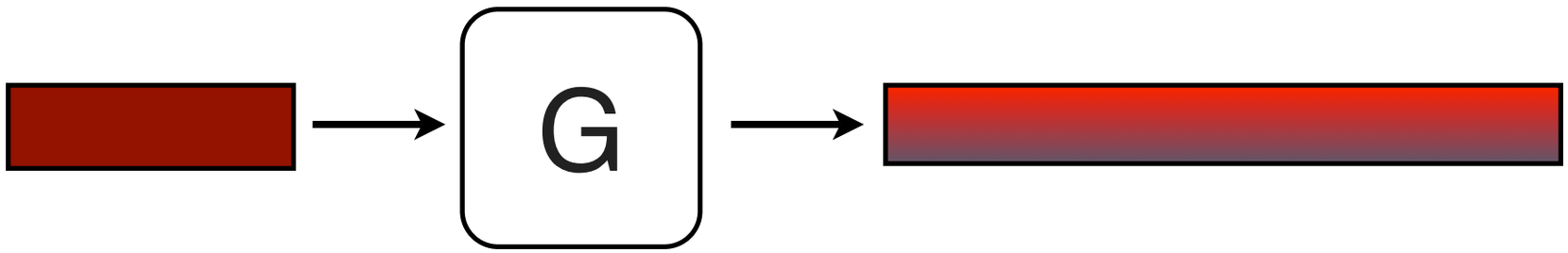
# Pseudorandomness in Computer Science and in Additive Combinatorics

Luca Trevisan
University of California, Berkeley

# this talk

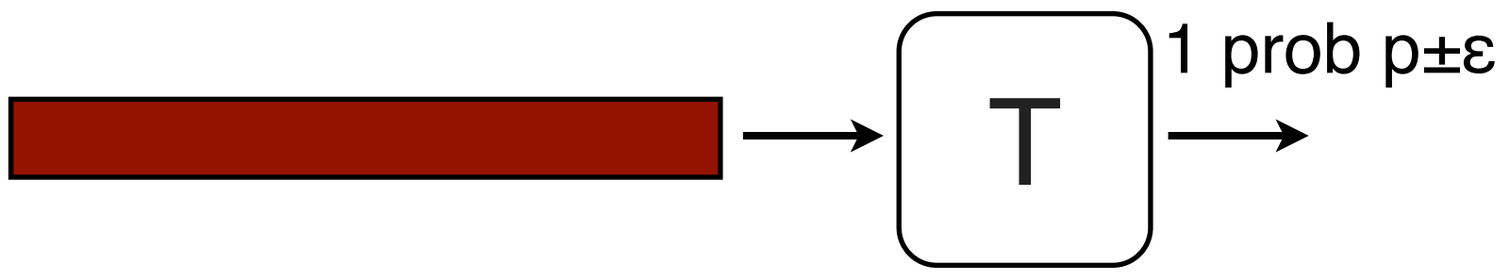
- explain what notions of pseudorandomness and indistinguishability arise in additive combinatorics
- how they relate to the TCS notions
- translate from language of norms, “decomposition” theorems, etc.

# pseudorandom generator



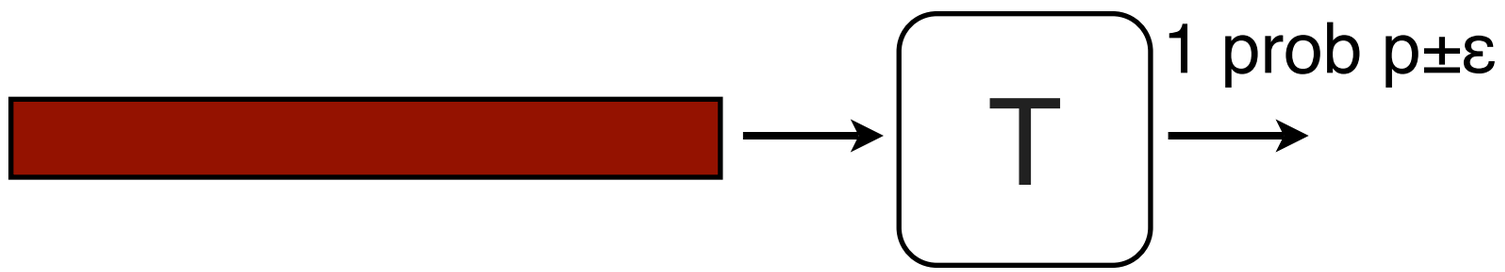

- deterministic procedure
- output longer than input
- when input is uniform, output “looks random”

# pseudorandom generator

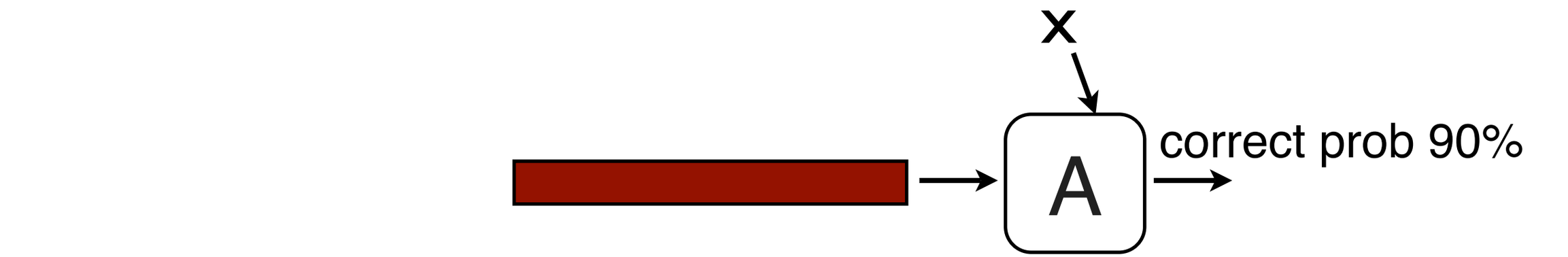

For every “efficient” test T

# pseudorandom generator

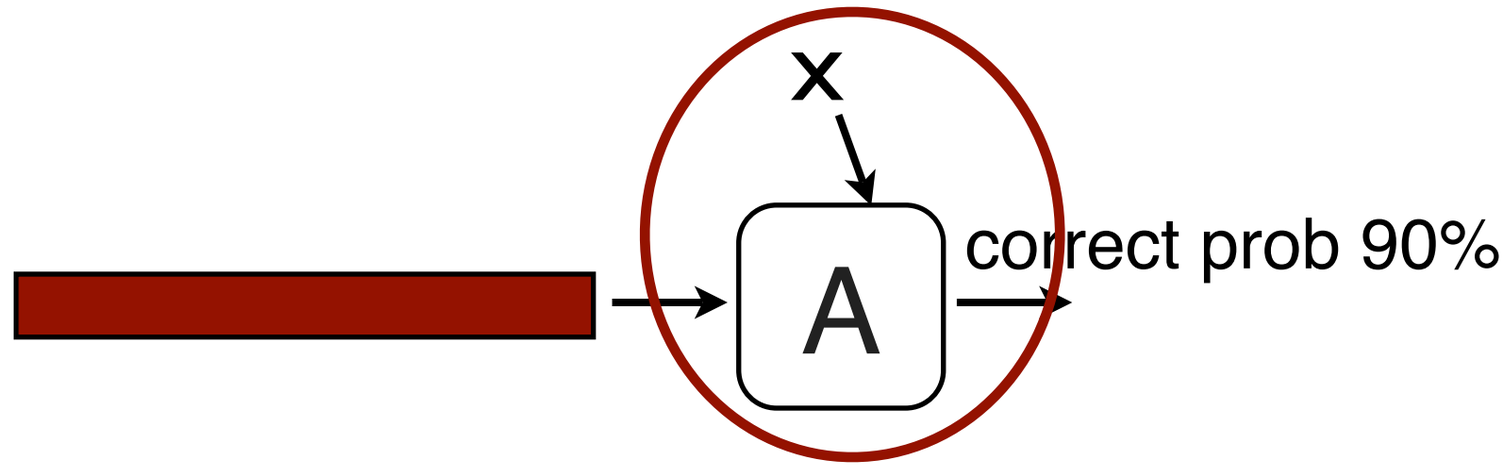



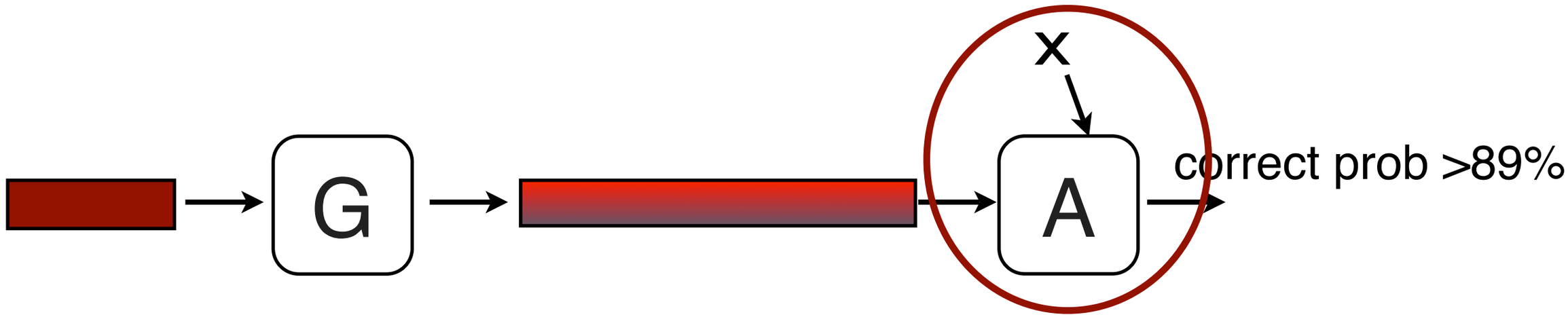

For every test T in a class ***C*** of functions
- Then we say G “ε-fools” ***C***

# application

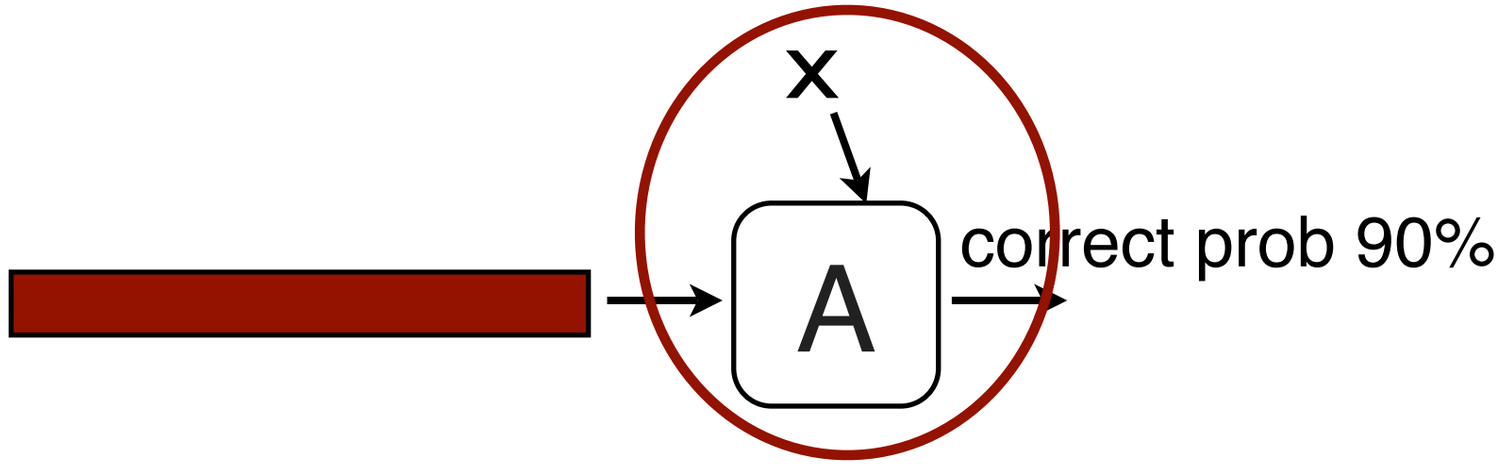


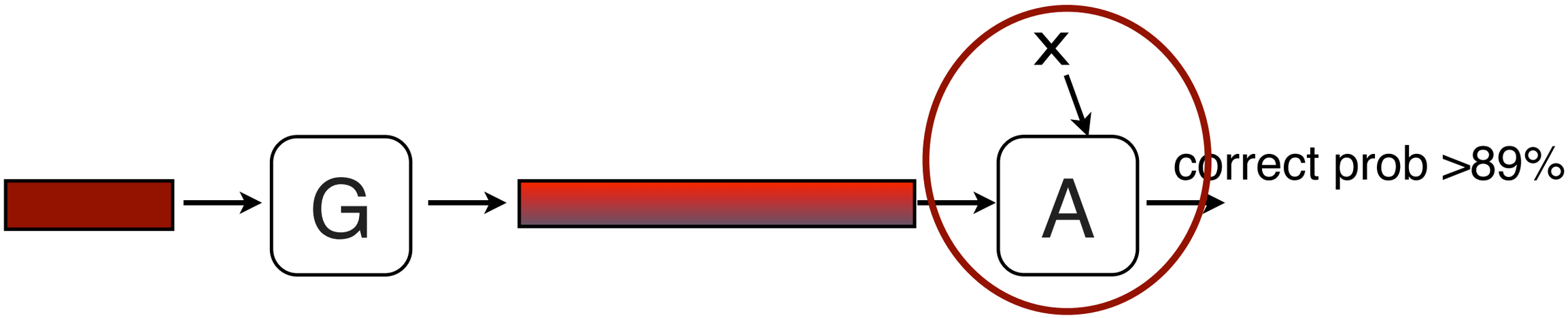

# application



# application




derandomization

# pseudorandomness

random variable X taking values in $\{0,1\}^n$ is
ε-pseudorandom for class of algorithms ***C***
if for every T in ***C***:

$$| \Pr [ T(X) = 1 ] - \Pr [ T(U_n) = 1 ] | \leq \varepsilon$$

( $U_n$ is uniform distribution over $\{0,1\}^n$ )

# indistinguishability

random variables X,Y taking values in $\{0,1\}^n$ are
ε-indistinguishable for class of algorithms ***C***
if for every T in ***C***:

$$| \Pr [ T(X) = 1 ] - \Pr [ T(Y) = 1 ] | \leq \varepsilon$$

# *pseudorandomness and graphs*

# quasirandom graph

[Thomason, Chung-Graham]

G=(V,E) is quasirandom if
for every sets A,B ⊆ V
# of edges between A,B is approximately

$$|E| \cdot |A| \cdot |B| \cdot 2 / |V|^2$$

# quasirandom graph

[Thomason, Chung-Graham]

G=(V,E) is ε-quasirandom if
for every sets $A,B \subseteq V$
# of edges between A,B is

$$|E| \cdot |A| \cdot |B| \cdot 2 / |V|^2 \pm \varepsilon \cdot |E|$$

# quasirandomness / indistinguishability

- Identify graph G=(V,E) with uniform distribution over E
- Define ***C*** to be class of functions
  $C_{A,B}$ (u,v) = 1 iff (u,v) crosses sets (A,B)
- Then G is ε-pseudorandom iff G and $K_{|V|}$ are ε-indistinguishable by ***C***

note: domain of functions in ***C*** is the set of all pairs of vertices

# *additive combinatorics*

# additive combinatorics

Like (Hungarian-style) combinatorics but

- graphs, hypergraphs
  -> sets of integers

- colorings, cuts, intersection
  -> properties definable using addition

# representative result

- Szemeredi's Theorem:
  - For every k, every δ, every subset $A \subseteq \{1,\ldots,N\}$ with $|A| > \delta N$
  - A contains a length-k arithmetic progression provided $N > N(\delta,k)$

At least 4 different proofs; each proof uses notions of "pseudorandomness"

# additive number theory

- Studies the existence and frequency of patterns in the primes that can be expressed using addition

- E.g.
  x,y prime such that x=y+2
  x,y,z,w prime such that y-x=z-y=w-z

# representative recent breakthroughs

[Green - Tao]

- The primes contain arbitrarily long arithmetic progressions [2004]

- Every system of linear equations of O(1) “complexity” has approximately as many solutions in primes as predicted by Hardy-Littlewood conjecture [ongoing]

# Roth's proof

Roth (1953) proved that if $A \subseteq \{1,...,N\}$ has size $\delta N$, and $N > \exp(\exp(1/\delta))$, then A must contain a length-3 progression.

Win-win argument:

- If A is "pseudorandom": done
  - then it has $\approx \delta^3 N^2$ progressions, like a random set of size |A|
- If A is not "pseudorandom": recurse
  - then enough to find progressions in $A' \subseteq \{1,...,N'\}$ of density $\delta+\delta^2$

# Roth-Meshulam

If $A \subseteq F^n$, $|A| = \delta |F^n|$, then if $\delta > 1/n$, A must have length-3 progression

Write Fourier expression of

$$\mathbf{E}_{x,y} A(x)A(x+y)A(x+y+y) = \Sigma_s \hat{A}(-2s)\, \hat{A}^2(s)$$

- it counts length-3 progressions
- It is $\delta^3$ plus an expression that is, in absolute value, at most $\delta \cdot \max |\hat{A}(s)|$

# Roth-Meshulam

# of length 3 progressions is at least

$N^2 \cdot ( \delta^3 - \delta \max | \hat{A}(s) | )$

1. If all coefficients $<< \delta^2$ we are done (pseudorandom case)
2. If a coefficient $> \delta^2$ then A correlates with a linear function and there is a sub-space of dimension n-1 on which A has density $> \delta+\delta^2$

# Gowers

Progressions of length 4?

If A has small Fourier coefficients, it does not follow that A has $\delta^4$ progressions of length 4

Gowers has to introduce stronger notion of pseudorandomness

# Gowers uniformity

- f: $Z_N$ -> **R**

- Def:

  $\| f \|_{U^k} := ( \mathbf{E}_{x,y_1,\ldots,y_k} \prod_{S \subseteq \{1,\ldots,k\}} f(x + \sum_{i \in S} y_i) )^{1/2^k}$

- Main point:

  if $\| f - g \|_{U^k}$ is small, then

  $\mathbf{E}\, f(x)f(x+y_1) \cdots f(x+y_{k-1}) \approx \mathbf{E}\, g(x)g(x+y_1) \cdots g(x+y_{k-1})$

# Gowers uniformity

- Main point:
  if $\| f - g \|_{U^k}$ is small, then
  $\mathbf{E}\, f(x)f(x+y_1) \cdots f(x+y_{k-1}) \approx \mathbf{E}\, g(x)g(x+y_1) \cdots g(x+y_{k-1})$

- If $\| A - B \|_{U^k}$ is small, then A,B, have approximately same number of length-k progressions

- If A has density $\delta$, and $\| A - \delta \|_{U^k}$ is small,
  then A has $\approx \delta^k$ fraction of all length-k progressions

# Gowers's proof

$A \subseteq Z_N$, $|A| = \delta N$

- If $\|A - \delta\|_{U^k}$ is small, done
  - then A has $\approx \delta^{k+1}N^2$ length-(k+1) progressions (pseudorandom case)

- If $\|A - \delta\|_{U^k}$ is not small, recurse
  - reduce to finding progressions in $A' \subseteq Z_{N'}$ of density $\delta+\delta^{O(1)}$ (100 of 128 pages in the paper)

# Gowers norm as indistinguishability

- A,B (indicator functions of) sets
- $\| A - B \|_{U^k}$ small means A,B approximately same number of length-(k+1) progressions
- “Indistinguishable” by an “adversary” that counts progressions
- Does not immediately fit into TCS notion of indistinguishability

# Gowers inverse conjecture

ll f $ll_{Uk}$ is small iff for every “polynomial” p, f and p are not “correlated”

- ❤ The Gowers Inverse Conjecture recently changed its status to: *it’s complicated*

  [cf. Lovett-Meshulam-Samorodnitsky, Green-Tao, Bergelson-Tao-Ziegler, Tao-Ziegler]

# indistinguishability vs. correlation

- Let D1, D2 be two probability distributions
- D1,D2 are ε-indistinguishable by ***C*** iff for every function f in ***C***
- $| \mathbf{E}_{x \sim D1} f(x) - \mathbf{E}_{x \sim D2} f(x) | \leq \varepsilon$
- iff:

  $| \Sigma_x D1(x)f(x) - D2(x)f(x) | \leq \varepsilon$

# indistinguishability vs. correlation

- Let D1, D2 be two probability distributions
- D1,D2 are ε-indistinguishable by ***C*** iff for every function f in ***C***
- $| \mathbf{E}_{x \sim D1} f(x) - \mathbf{E}_{x \sim D2} f(x) | \leq \varepsilon$
- iff:

  $| \Sigma_x ( D1(x)-D2(x) ) f(x) | \leq \varepsilon$

# indistinguishability vs. correlation

- Let D1, D2 be two probability distributions
- D1,D2 are ε-indistinguishable by ***C*** iff for every function f in ***C***
- $| \mathbf{E}_{x \sim D1} f(x) - \mathbf{E}_{x \sim D2} f(x) | \leq \varepsilon$
- iff:
  $| < (D1\text{-}D2) , f > | \leq \varepsilon$

# view as a norm

- ***C*** is a class of bounded functions f: X -> [0,1]
- for a function g: X -> **R**,
  $\| g \|_{\boldsymbol{C}} := \max_{f \in \boldsymbol{C}} | \langle g,f \rangle |$
- Is always a norm; it is L1 if ***C*** is all bounded functions
- $\| h - g \|_{\boldsymbol{C}} \leq \varepsilon$ iff h,g ε-indistinguishable by ***C***

# inverse conjecture

- A,B indicator functions of (dense) sets
- A-B has small k-th Gowers norm
- iff $U_A$ , $U_B$ indistinguishable by degree (k-1) polynomials

# *primes in arithmetic progression*

# Green-Tao starting points

- Want to prove primes have arbitrarily long arithmetic progressions
- "Suffices" to prove:
  Primes - 1/log n
  has small Gowers norm
- Instead use facts:
  - "Almost primes" with few large factors have small Gowers norm, and are not much more than primes
  - Sets of integers of constant density have arbitrarily long arithmetic progressions

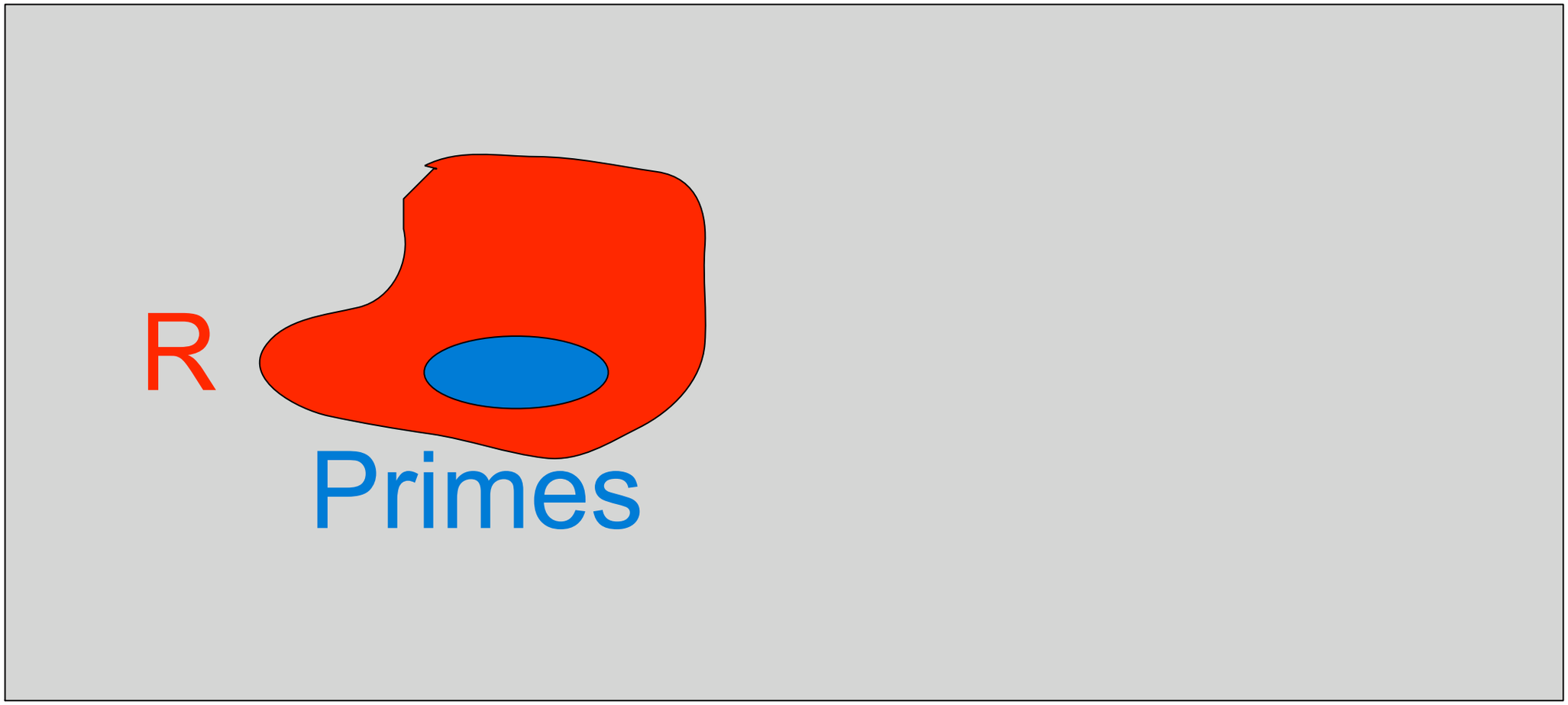
# Green-Tao main result

- If $R \subseteq Z_N$ is a (possibly tiny) pseudorandom set
  [i.e.: R - density(R) has small Gowers norm]
  and if $D \subseteq R$ has density $\delta$ in R

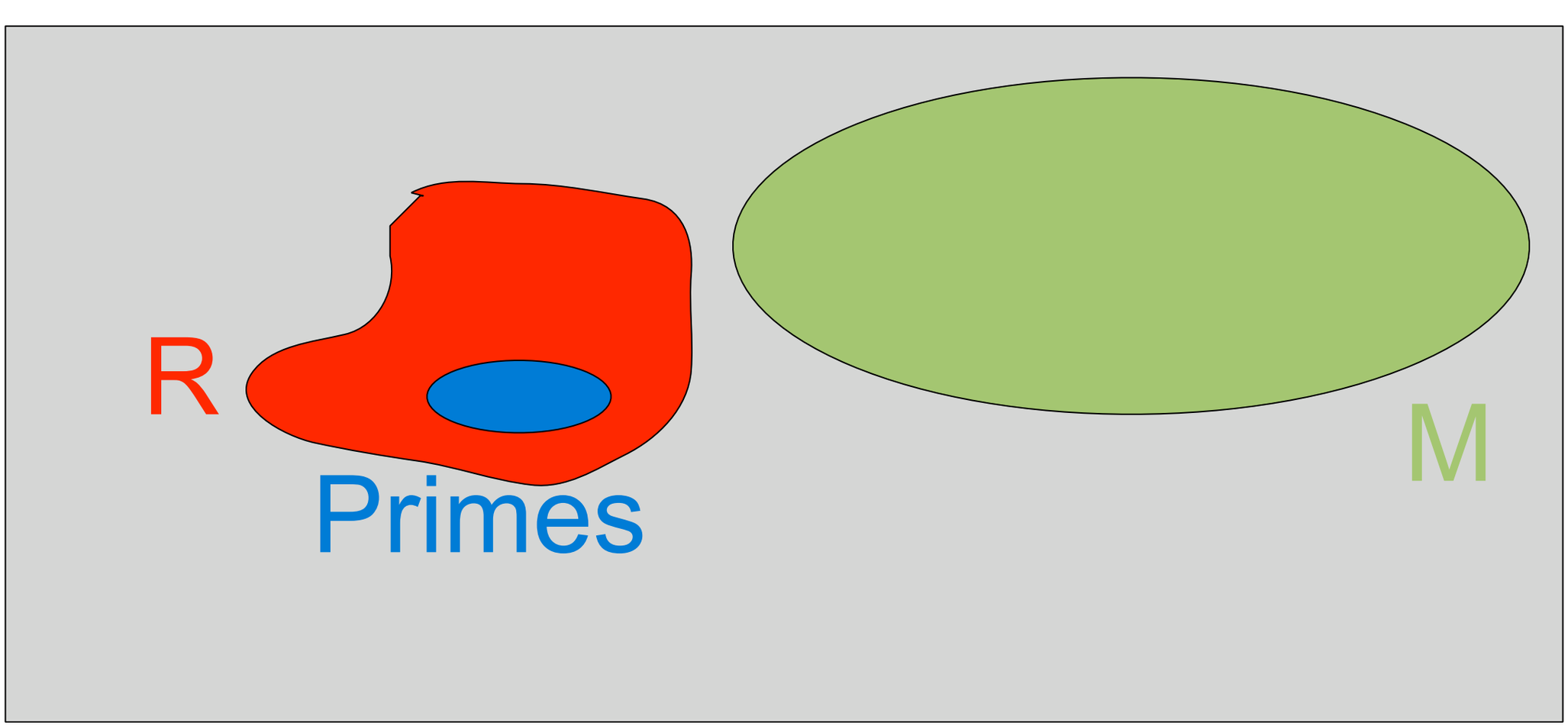
- Then there is $M \subseteq Z_N$ of size $> \delta N/2$ such that M and D are indistinguishable
  [i.e. M - scalingfactor $\cdot$ D has small Gowers norm]

$\{1,\ldots,N\}$

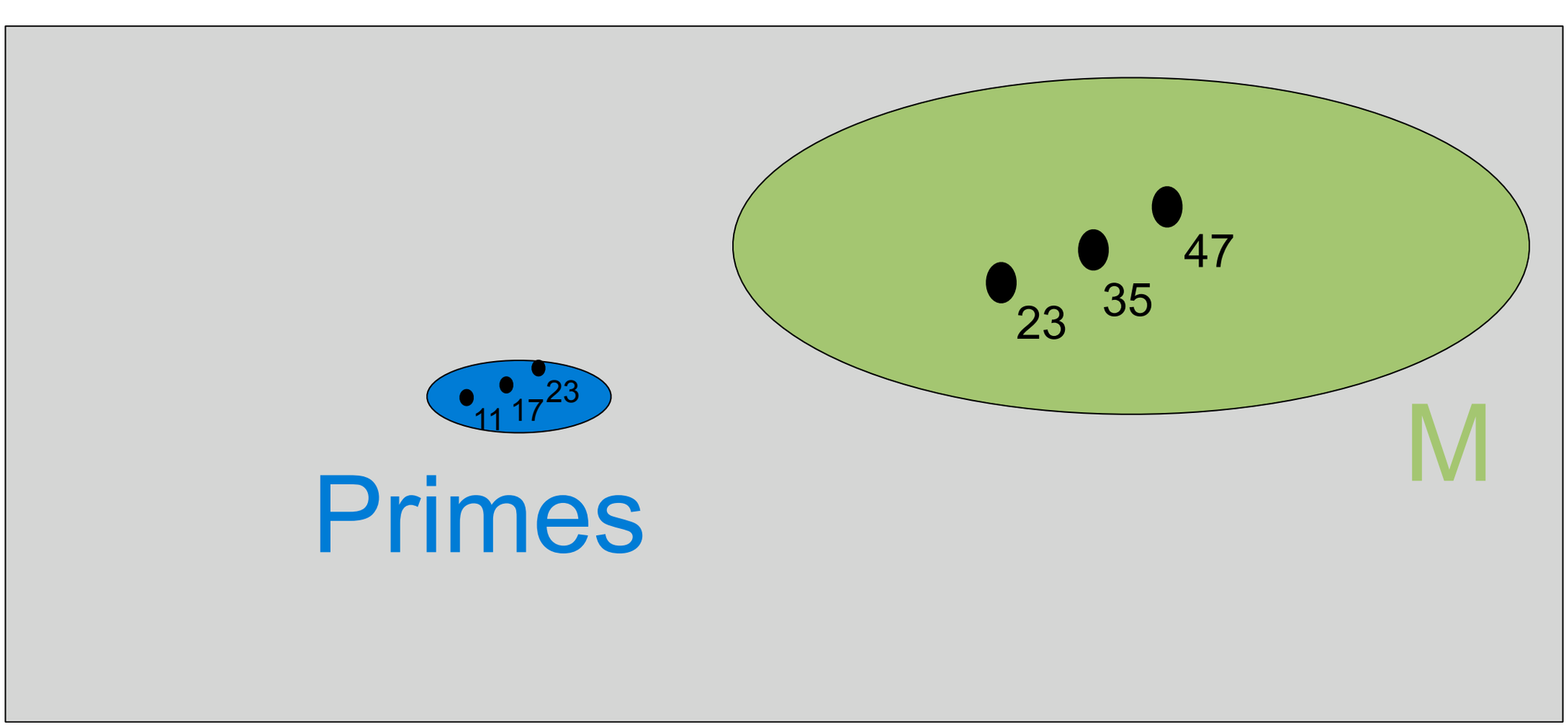
$\{1,\ldots,N\}$



$\{1,\ldots,N\}$



$\{1,\ldots,N\}$



# dense model theorem

[Green Tao] [Tao Ziegler]

r: X -> [0,M] **E**r=1 (indicator function of almost-primes)

g:X -> [0,M], $g \leq r$, **E**g = δ (primes)

***C*** class of functions f: X -> [0,1], ε

Then either there is h: X -> [0,1], **E**h $\geq$ δ/2, s.t.

$\forall f \in \boldsymbol{C}$ . $|\langle (h-g), f \rangle| \leq \varepsilon$

or $\exists\, d \in \boldsymbol{C'}$ . $|\langle (r - 1), d \rangle| \geq \varepsilon'$

# dense model theorem

- Can be proved in a computational setting [Reingold T Tulsiani Vadhan 2008]
- E.g. If G is a pseudorandom generator mapping t bits into n bits
- X is a distribution of entropy t-2
- There is distribution of M of entropy n-2 that is indistinguishable from G(X)
- Useful to secure against key leakage c.f. [Dziembowsky-Pietrzak]

# *decomposition theorems*

# simulators

- Typical scenario in cryptography:
  - distribution X quite complicated
    - efficient simulator algorithm S()
    - X and output of S() are indistinguishable

- E.g. Zero Knowledge

# decomposition results in add comb

Many theorems have form:

given g arbitrary function, ***C*** class of functions

can write

$g = g_s + g_r$

where: $g_s$ is “structured” (related to ***C***)

$g_r$ has low correlation with ***C***

# decomposition results in add comb

Many theorems have form:

given g arbitrary function, ***C*** class of functions

can write

$g = g_s + g_r$

where: $g_s$ is “structured” (related to ***C***)

$g_r$ has low correlation with ***C***

Means:
there is simulator $g_s$ for g that is indistinguishable.

# where are we going with this?

- some arguments in additive combinatorics more transparent using language of distributions, adversaries and indistinguishability
- arguments in complexity, cleaner and more general using language of functions, inner products and norms
- each side suggests generalizations
- complexity: min-max, boosting; add comb: partitions ECCC TR08-45, TR08-103 w/ Tulsiani & Vadhan

# good end-of-summer reads

Terry Tao:

- *The dichotomy between structure and randomness*
  ICM 2006 Lecture

- *Structure and randomness in combinatorics*
  FOCS 2007 Tutorial