

Additive Combinatorics and Computational Complexity

Luca Trevisan

U.C. Berkeley

Ongoing joint work with Omer Reingold,

Madhur Tulsiani, Salil Vadhan

- Combinatorics:
 - Studies: Graphs, hypergraphs, set systems
 - Considers: cuts, subgraphs, intersections
 - Typical question:
 - max number of edges in triangle free graph
- Additive combinatorics
 - Studies: subsets of abelian groups (e.g. primes)
 - Considers: properties that can be described with linear equations
 - Typical question:
 - largest subset of integers in $\{1, \dots, N\}$ with no length-3 arithmetic progression

- Additive number theory
 - Questions about primes which can be formulated as systems of linear equations
- Does $y=x+2$ have infinitely many solutions in primes?
- Does $x+y=2n$ have solutions in primes for all $n \geq 2$?
- Are there infinitely many non-trivial solutions in primes to
 - $x-y=y-z$
 - $y-z=z-w$

- Additive number theory
 - Questions about primes which can be formulated as systems of linear equations
- Some questions better approached in broader generality, separating combinatorics and number theory
 1. Under what conditions does a set of integers possess a desired property?
 2. Do the primes satisfy such conditions?
[number theory needed only here]

- Additive combinatorics has seen a confluence of
 - Graph and hypergraph theory
 - Analysis
 - Ergodic theory
- Techniques have been applied in theoretical computer science to
 - Property testing
 - Pseudorandomness and derandomization
 - PCP
 - Lower bounds
 - ...

- Additive combinatorics
 - Graph and hypergraph theory
 - Regularity Lemmas
 - > property testing [Alon-....]
 - Analysis
 - Regularity Lemmas in groups
 - > PCP [Khot-O'Donnell]
 - Gowers-Balog-Szemerédi Thm
 - > low-degree testing [Samorodnitsky]
 - Gowers Uniformity
 - > PCP [Samorodnitsky-T],
 - > pseudorandomness [Bogdanov-Viola]
 - > direct product thms [Viola-Wigderson],
 - ...
 - Ergodic theory
 - ???

- Arithmetic Combinatorics

Subsets of rings, properties defined via addition and multiplication

- Sum-product Theorems

- Applications to Computer Science:

- Expanders, extractors

- [Barak-Impagliazzo-Wigderson,...]

- Additive (and arithmetic) Combinatorics
- What do the very different techniques have in common?
 - Randomness versus structure
[Terence Tao, ICM 2006 Lecture]
- Why so useful in (theoretical) computer science?
 - ??
 - In different language, notions of
 - pseudorandomness,
 - indistinguishability,
 - property testing,
 - compact representations (sketches),
 - approximation,
 - worst-case analysis,
 - . . .

- Additive (and arithmetic) Combinatorics

<http://www.cs.princeton.edu/theory/index.php/Main/AdditiveCombinatoricsMinicourse>

[Barak, Charikar, T., Wigderson]

- Google: additive combinatorics princeton

In this talk

- The structure of the proof of the Green-Tao Theorem
- A look at a key combinatorial step
- Complexity-theoretic interpretation
- New “complexity-theoretic” proofs
new results in complexity theory

Green-Tao (2004)

- “The primes contain arbitrarily long arithmetic progressions”

199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089

Green-Tao (2004)

- “The primes contain arbitrarily long arithmetic progressions”
- Previously, two lines of attack:
 - The primes are dense
Erdos (conj): all sets of density $1/\ln N$ have long APs
 - The primes are pseudorandom
Hardy-Littlewood (conj): primes satisfy linear systems as often as random sets of density $1/\ln N$

Density

- *Erdos (conj)*: if A is set of integers such that $\sum 1/a$ diverges, then A has long APs
[~equivalent: if A has density $1/\ln N$, then long APs]
- *Erdos-Turan (conj, 1940s)*: if A has constant density, then A has long APs
 - [Szemerédi, 1970s] density $1/\log^* \log^* N$
 - [Furstenberg, 1970s] density $o(1)$
 - [Gowers, 1998-01] density $1/\log \log N$

Pseudorandomness

- *Hardy-Littlewood*: take a system of linear equations
e.g.
$$y-x = z-y$$
$$z-y = w-z$$
- Then approximately as many solutions in primes as in “a random set of density $1/\ln N$ ”
- Twin primes conjecture: $y-x=2$

Pseudorandomness

- Hopeless for now
- Strong results for “almost primes:” integers with few, large, factors
- E.g.: $y-x=2$ has infinitely many solutions, x prime, y at most two factors

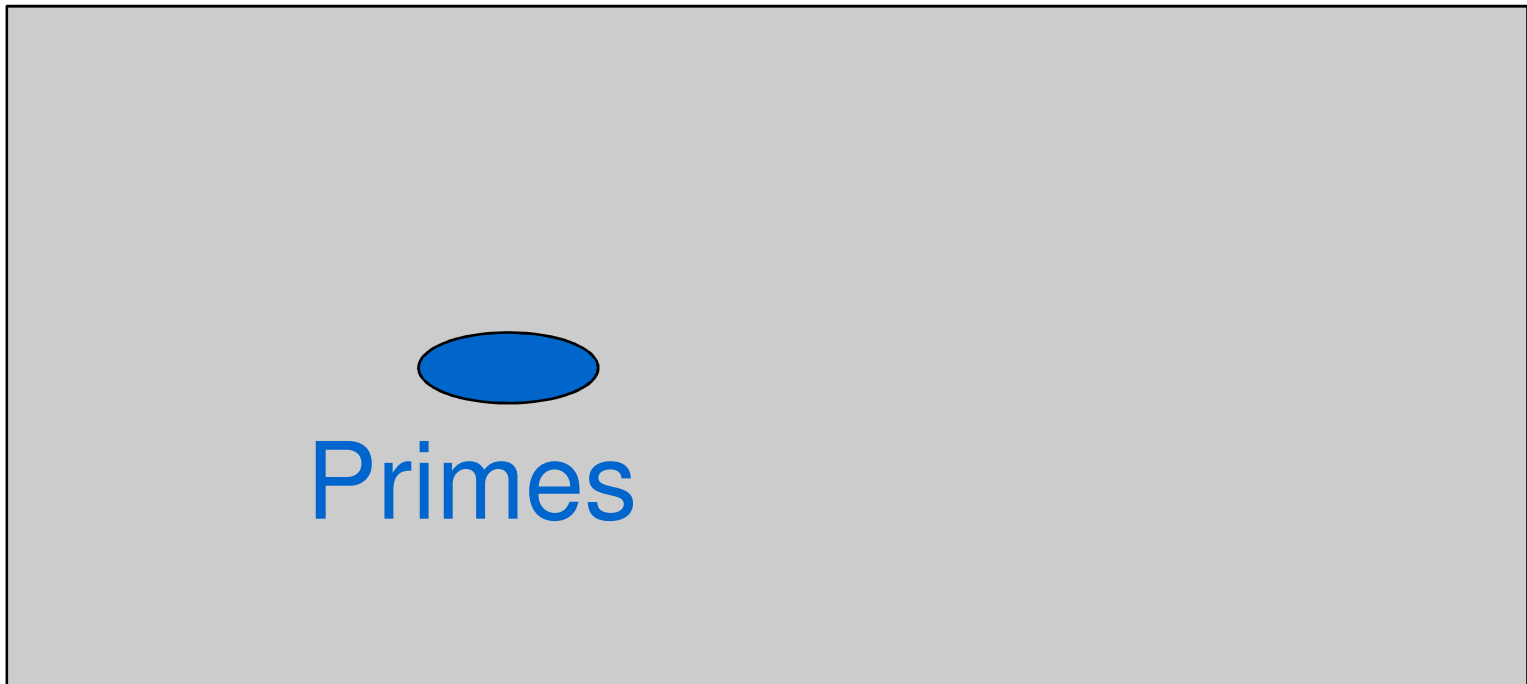
Green-Tao Idea

- Pseudorandomness works only for almost primes
- Density works only for $o(1)$ density
- Combine the two

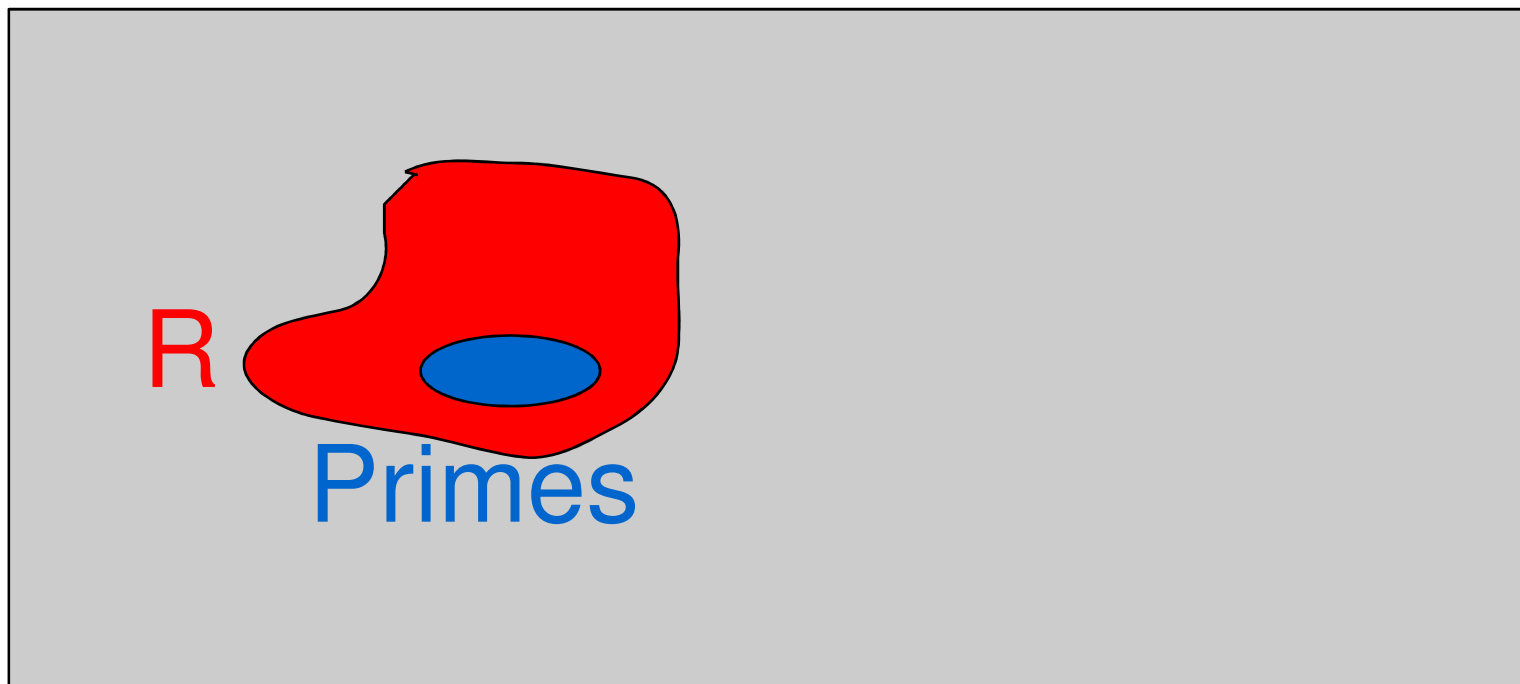
Green-Tao Proof

1. Thm: primes have const density in almost primes
2. Thm: almost primes are pseudorandom
3. Thm: [Main]
if R is pseudorandom
and D has constant density in R ,
then there is M of constant density
indistinguishable from D
4. Thm: [Szemerédi] M has long APs
5. so does D

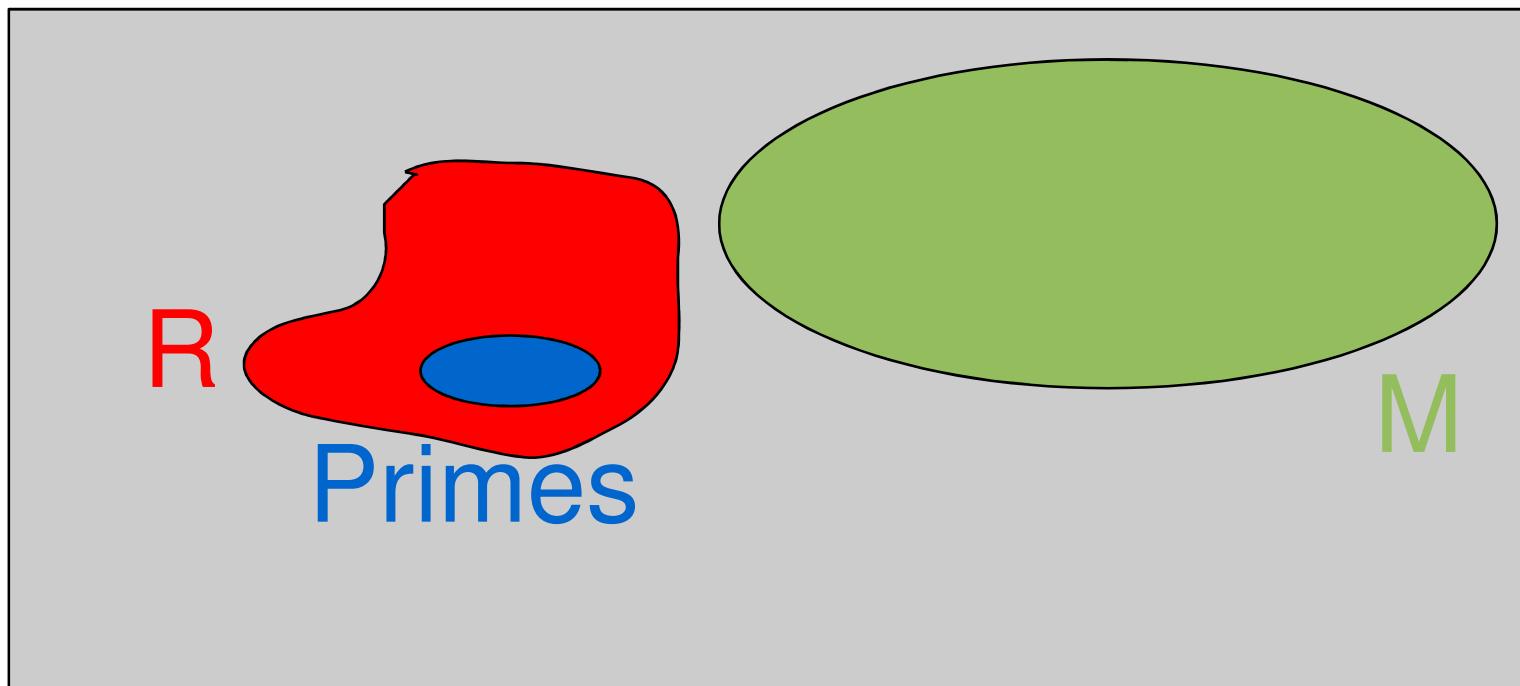
$\{1, \dots, N\}$



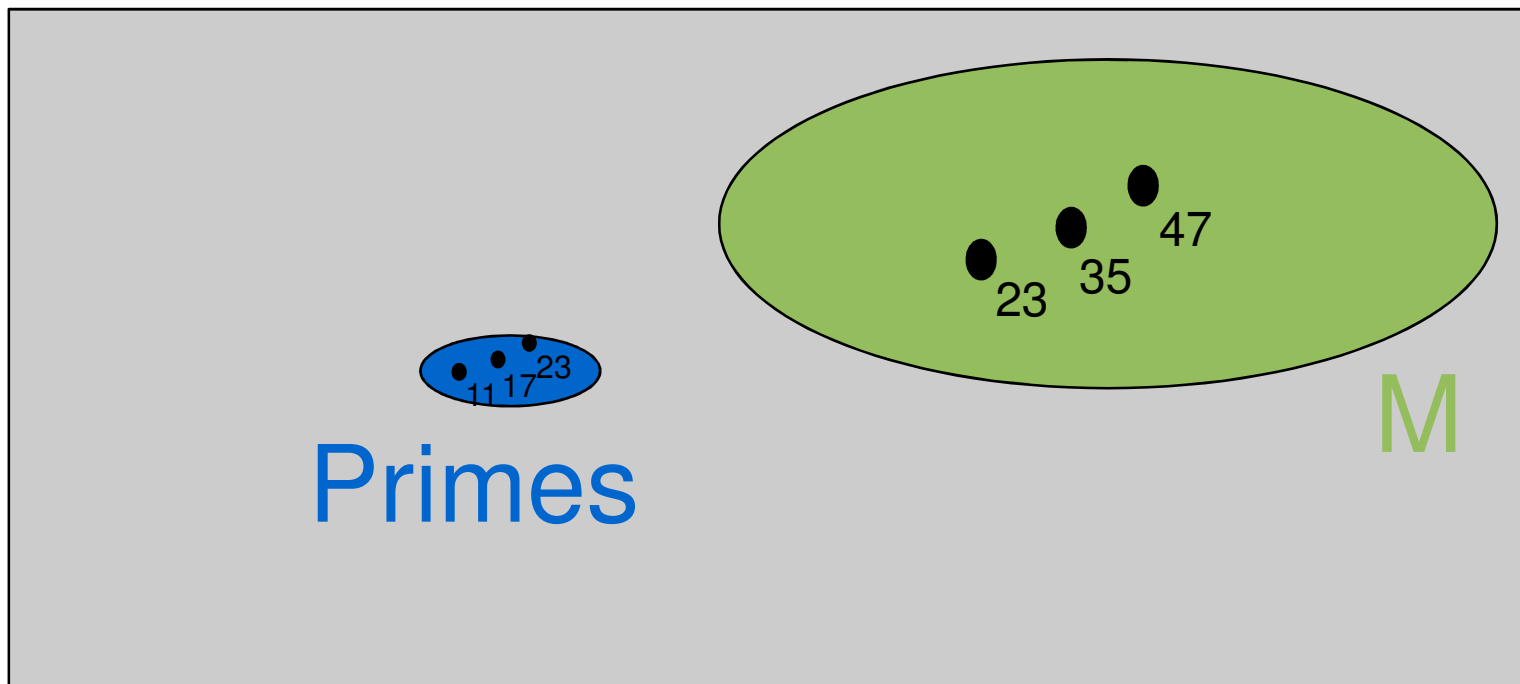
$\{1, \dots, N\}$



$\{1, \dots, N\}$



$\{1, \dots, N\}$



Key step

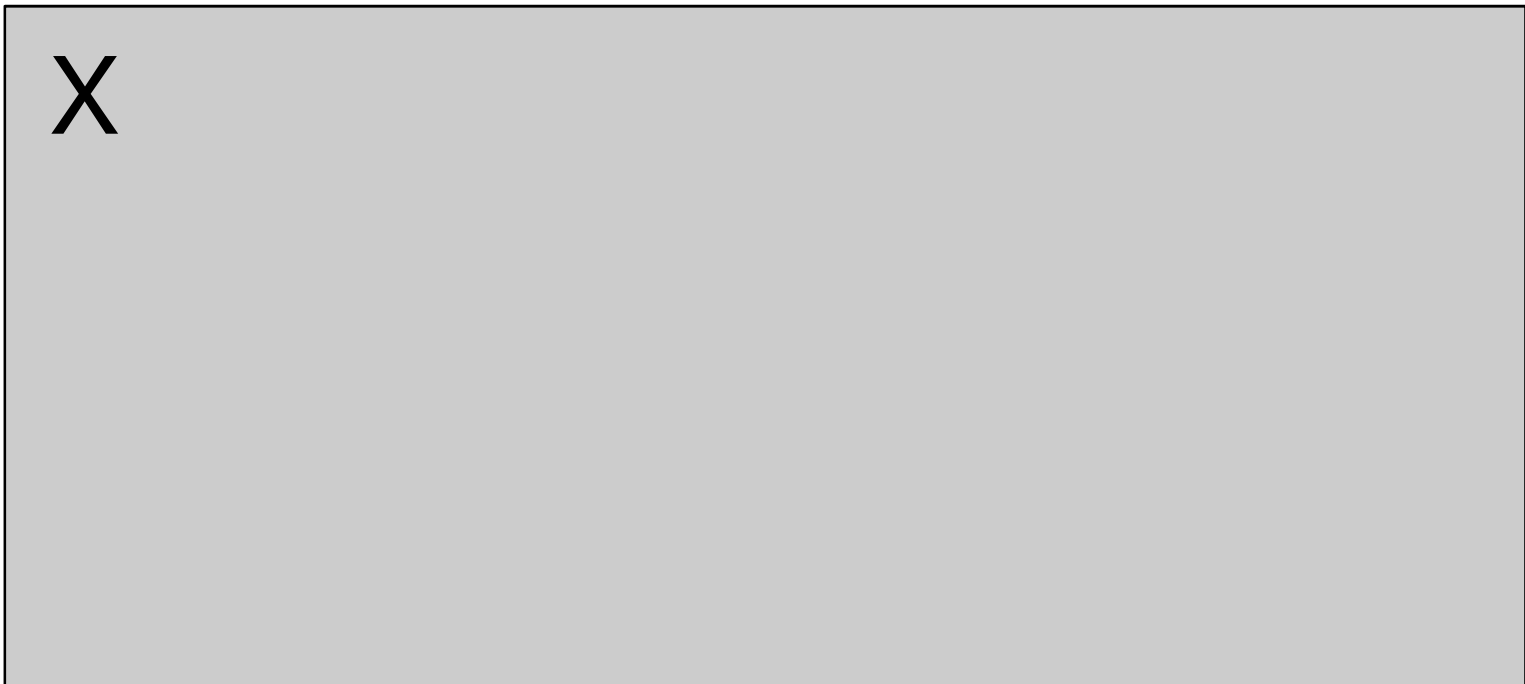
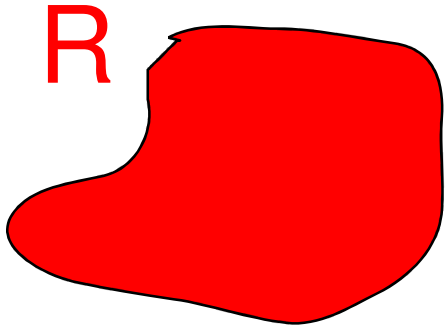
Dense Model Theorem:

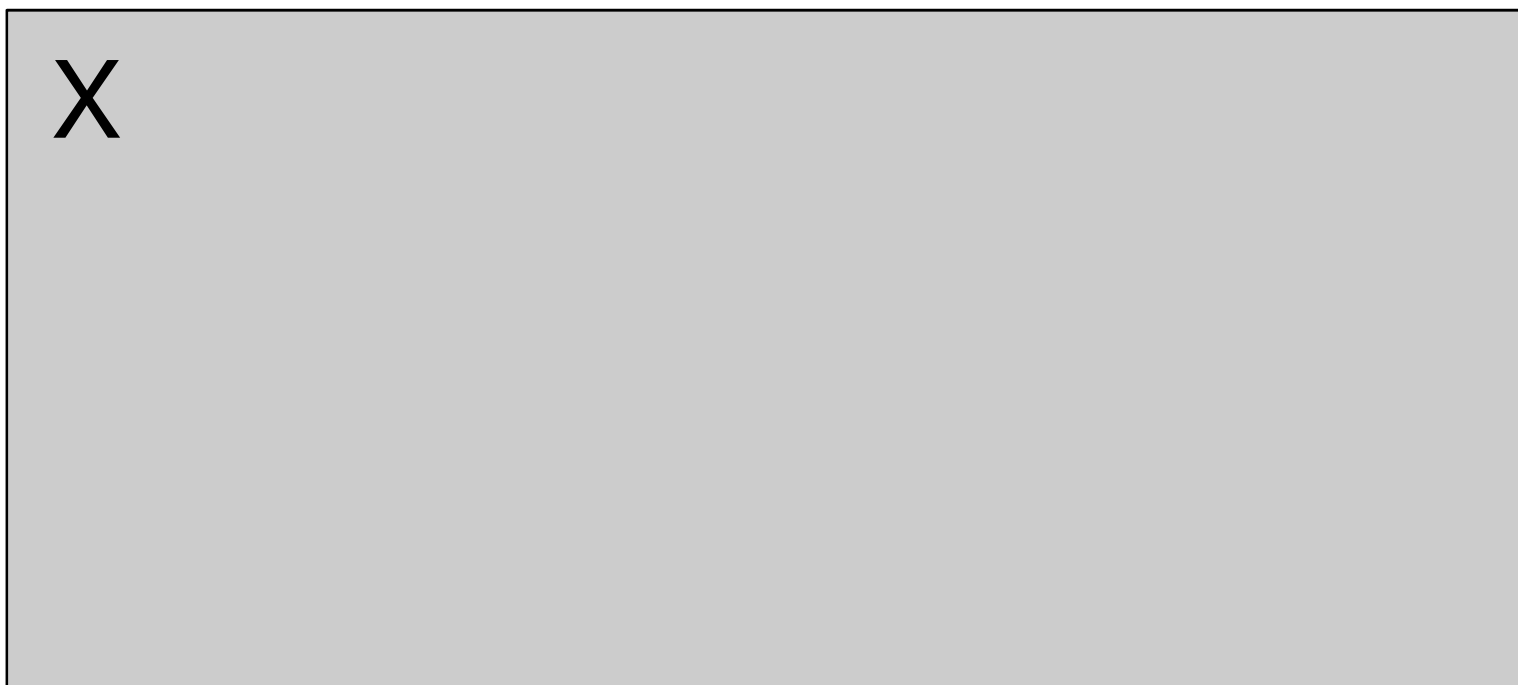
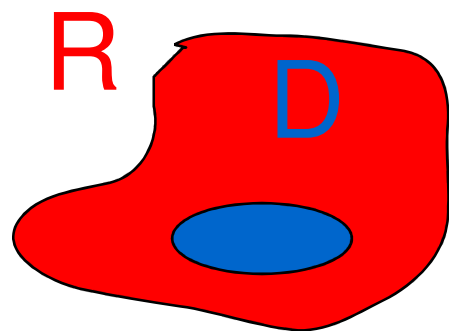
- If R pseudorandom in X
and D subset of R has size $\geq \delta |R|$
- Then there is M of size $\geq \delta |X|$ that is
indistinguishable from D

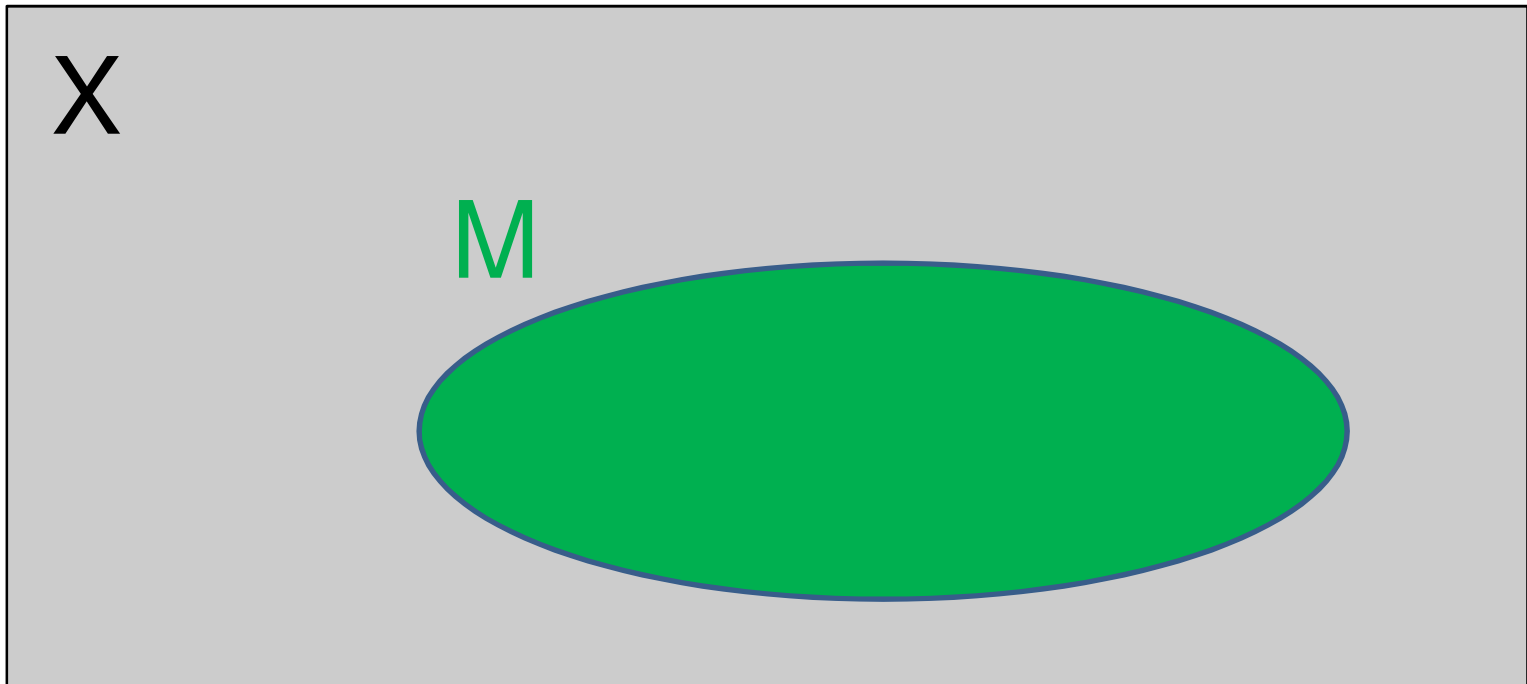
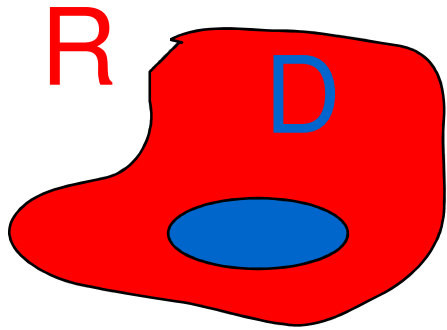
Key step

Dense Model Theorem:

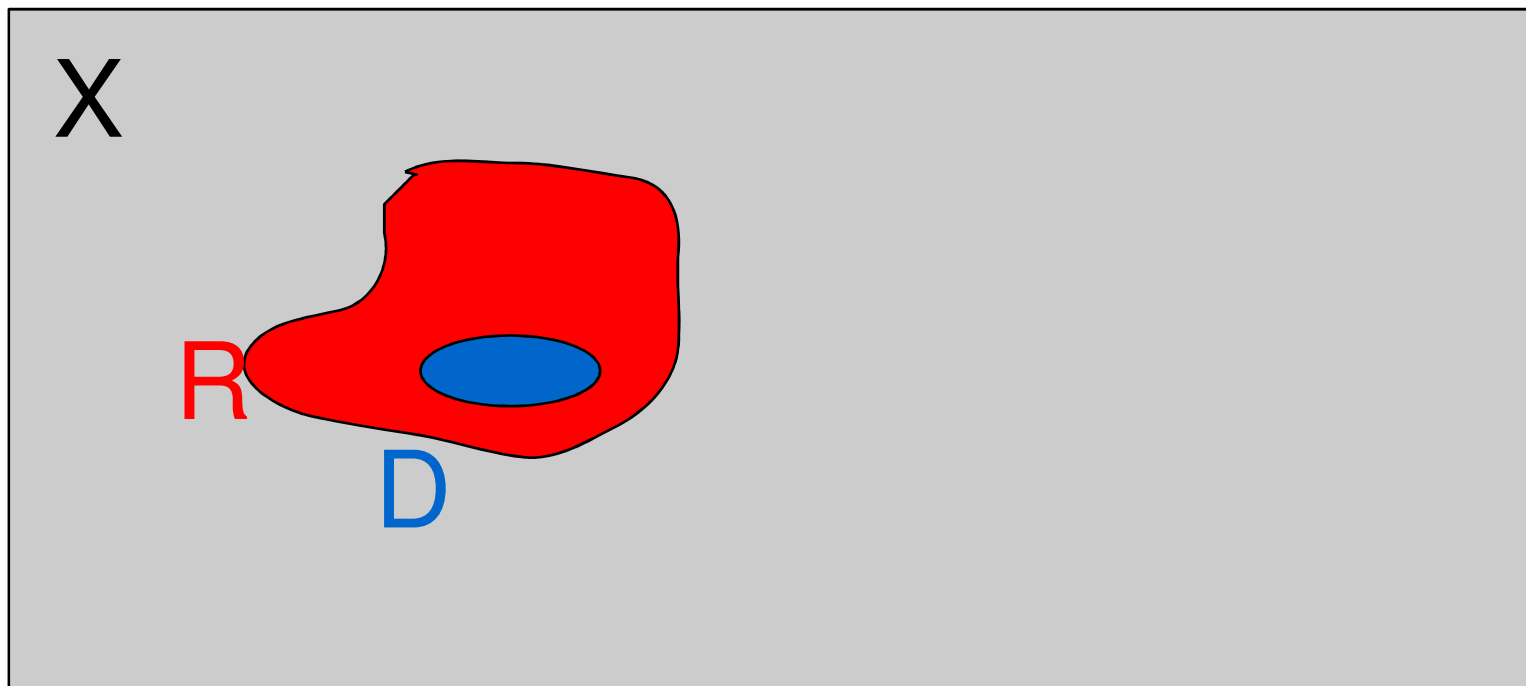
- If R is pseudorandom distribution in X and for all x , $D(x) \leq R(x) / \delta$
- Then there is M that is indistinguishable from D and for all x , $M(x) \leq 1 / \delta |X|$



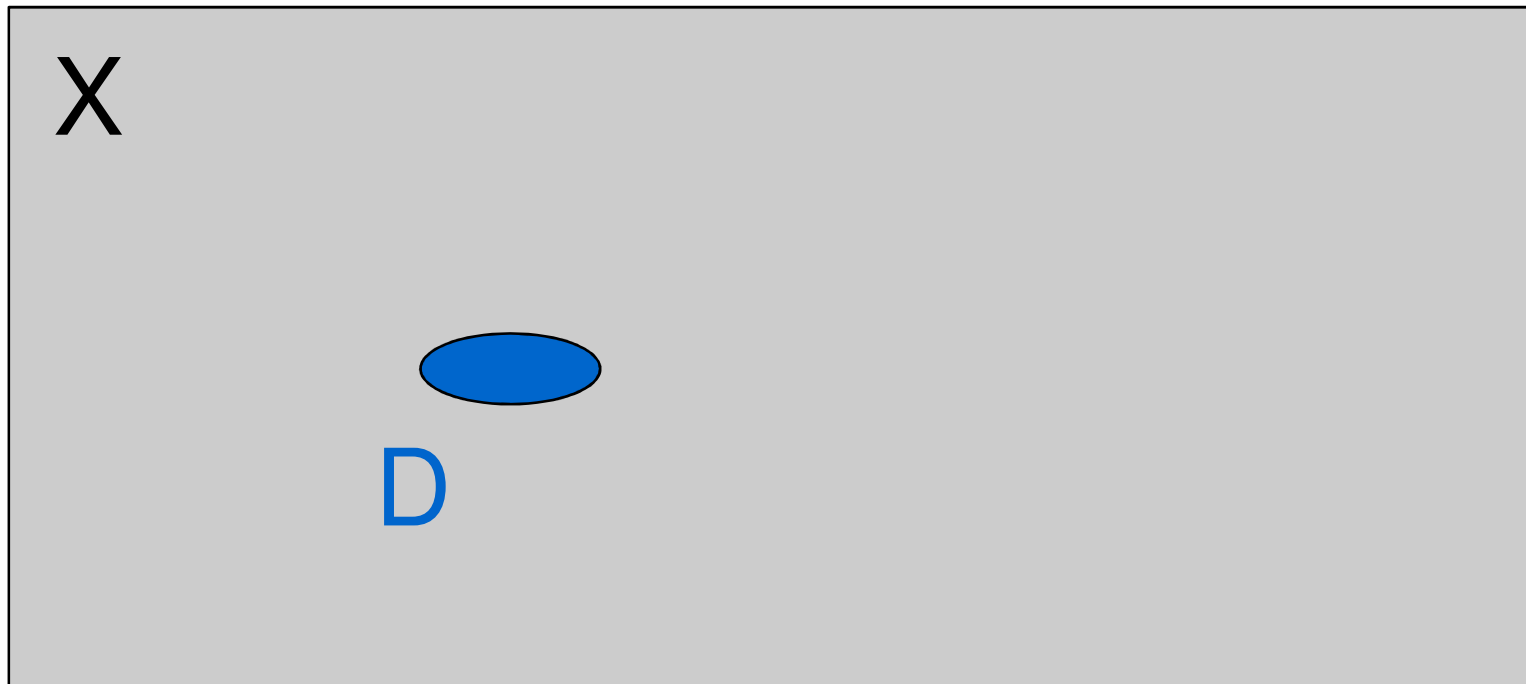




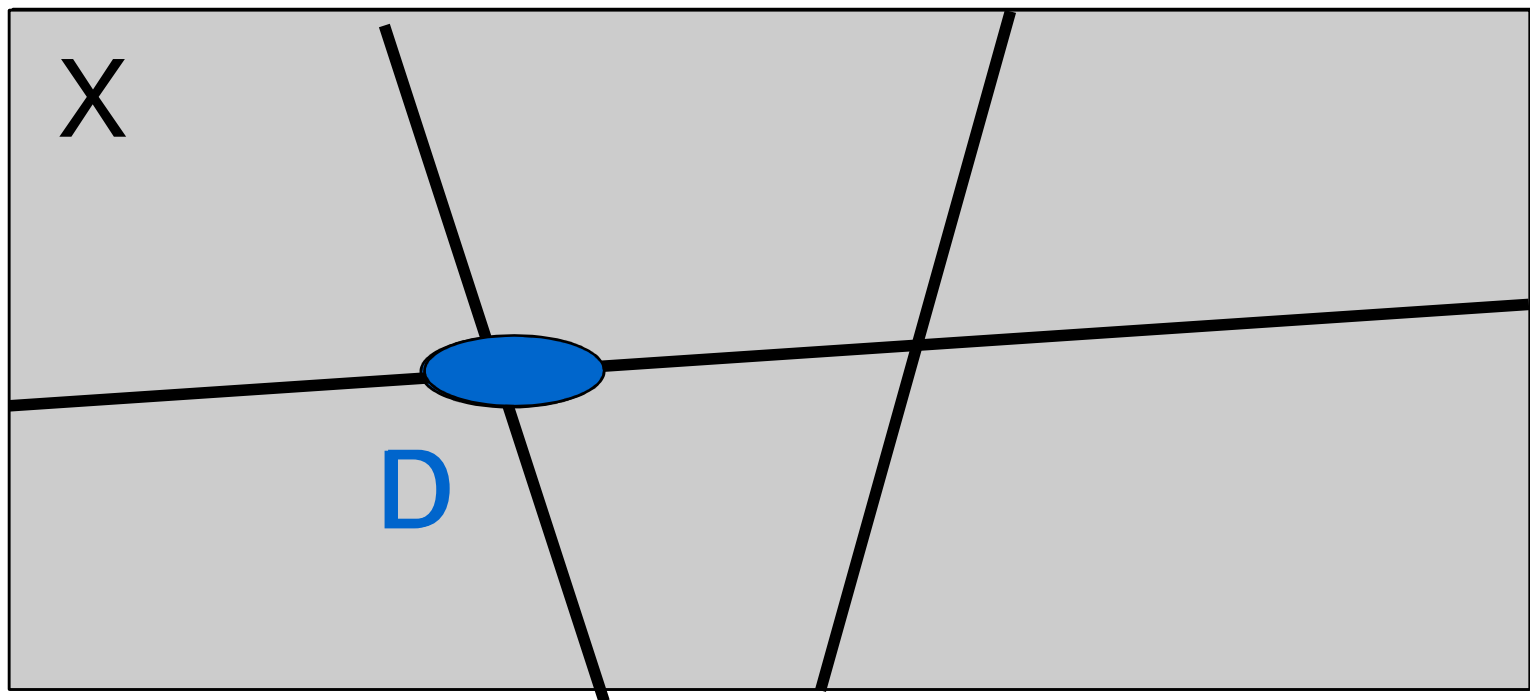
The Green-Tao(-Ziegler) proof



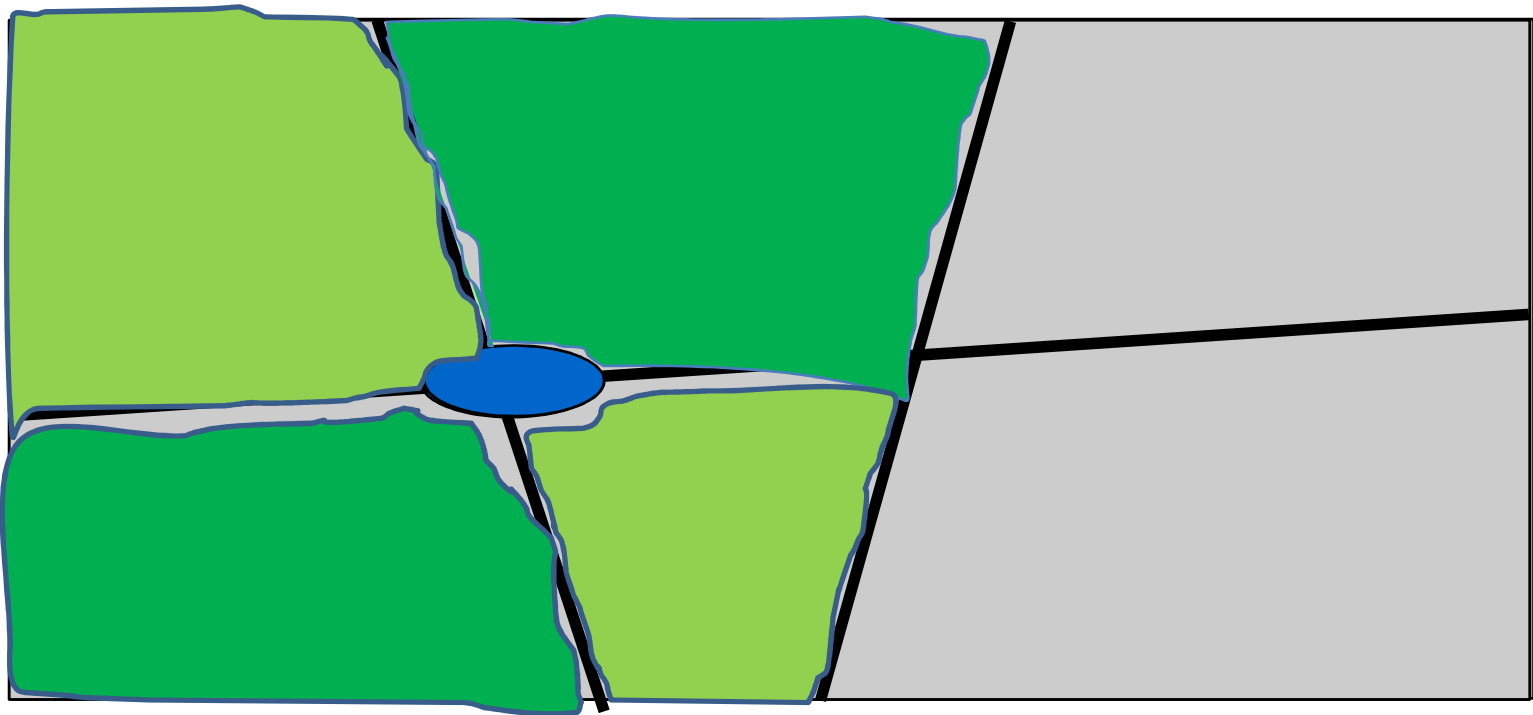
The Green-Tao(-Ziegler) proof



The Green-Tao(-Ziegler) proof



The Green-Tao(-Ziegler) proof



Find partition of X :

- i)* blocks are large and easily recognizable;
- ii)* D is indistinguishable from

- Sample $z \sim D$
- Let B be block of z
- Sample $x \sim B$

Above distribution is dense:

$$\Pr [x \text{ is sampled}] = \Pr [D \text{ in } B_x] / |B_x|$$

$$\Pr [D \text{ in } B_x] \leq \Pr [R \text{ in } B_x] / \delta$$

$$\Pr [R \text{ in } B_x] \leq |B_x| / |X| + \varepsilon$$

$$\Pr [x \text{ is sampled}] \leq 1/\delta|X| + \varepsilon/\delta|B_x|$$

Find partition of X : (i) blocks are large and easily recognizable; (ii) D is indistinguishable from:

- Sample $z \sim D$
- Let B be block of z
- Sample $x \sim B$

To find partition

- Start from trivial partition
- While distribution distinguishable from D
 - refine partition using level sets of distinguisher

Potential function argument:

- only need $\text{poly}(1/\varepsilon, 1/\delta)$ refinement steps
- upper bound on potential function uses pseudorandomness of R

Green-Tao(-Ziegler) Proof

Applies to computational setting

- R poly(ϵ, δ)-pseudorandom in X against circuits of size $O(S \cdot \exp(1/\delta, 1/\epsilon))$
- D is “ δ -dense” in R

Then there is M that is ϵ -indistinguishable from D by circuits of size S

Exponential loss: partition has exp many pieces

New Proof

[Reingold, T., Tulsiani, Vadhan, FOCS'08]

- R $\text{poly}(\epsilon, \delta)$ -pseudorandom in X against circuits of size $O(S^* \text{poly}(1/\delta, 1/\epsilon))$
- D is “ δ -dense” in R

Then there is M that is ϵ -indistinguishable from D by circuits of size S

Proof using linear programming duality

Same idea independently [Gowers, 2008]

New Proof

[Reingold, T., Tulsiani, Vadhan, FOCS'08]

As noted by Russell Impagliazzo, can also prove:

Suppose D is such that for every f of size $S \cdot \text{poly}(1/\delta, 1/\epsilon)$

$$\Pr[f(D)=1] \leq \Pr[f(U)] / \delta + \text{poly}(\epsilon)$$

Then there is M that is “ δ -dense”

and ϵ -indistinguishable from D by circuits of size S

Consequence of New Proof

[Reingold, T., Tulsiani, Vadhan, FOCS'08]

The following 3 properties of D are equivalent:

1. **Domination by pseudorandom distribution**
there is R indistinguishable from U
such that for all x , $D(x) \leq R(x)/\delta$
2. **“Pseudodensity”**
for all efficient f $\Pr[f(D)] \leq \Pr[f(U)]/\delta + \epsilon$
3. **Pseudoentropy (defined by Hastad-Impagliazzo-Luby-Levin)**
there is M indistinguishable from D
such that for all x , $M(x) \leq U(x)/\delta = 1/(\delta|X|)$

Consequence of New Proof

Suppose

- $G: \{0,1\}^{512} \rightarrow \{0,1\}^{100,000}$
is a cryptographic pseudorandom generator
- D is a distribution of seeds of entropy 510
(e.g. two digits are fixed)

Then there is a distribution M of entropy 99,998
which is indistinguishable from $G(D)$

New Proof

[Reingold, T., Tulsiani, Vadhan, FOCS'08; Gowers 2008]

Suppose Dense Model Theorem is false

Then there is D dense in pseudorandom R such that
for every dense model M there is a distinguisher

Then there is a distinguisher that works against all models

It can be used to distinguish R from Uniform
Contradiction

Comparison with Previous Proof

[Reingold, T., Tulsiani, Vadhan, FOCS'08; Gowers 2008]

Leads to computational application with
polynomial parameters

Green-Tao-Ziegler has **exponential** loss

The model is shown to exist **non-constructively**

Green-Tao-Ziegler **exhibits** model

Best of two worlds?

Comparison with Previous Proof

Impagliazzo
Hard Core Lemma



Min-max

“boosting”

Dense Model Theorem

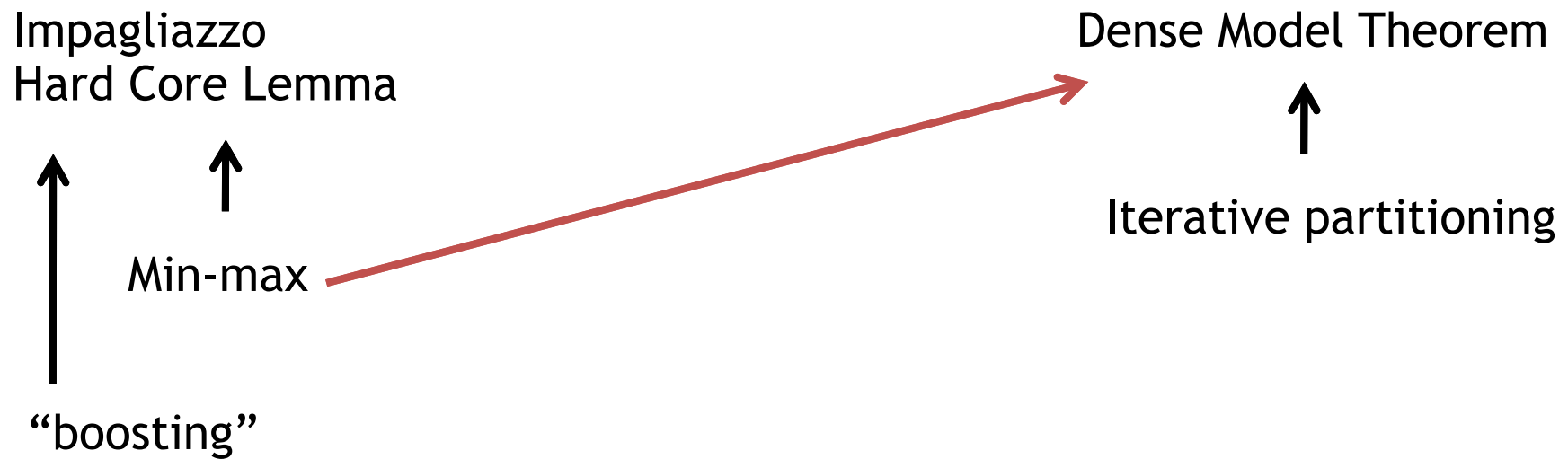


Iterative partitioning

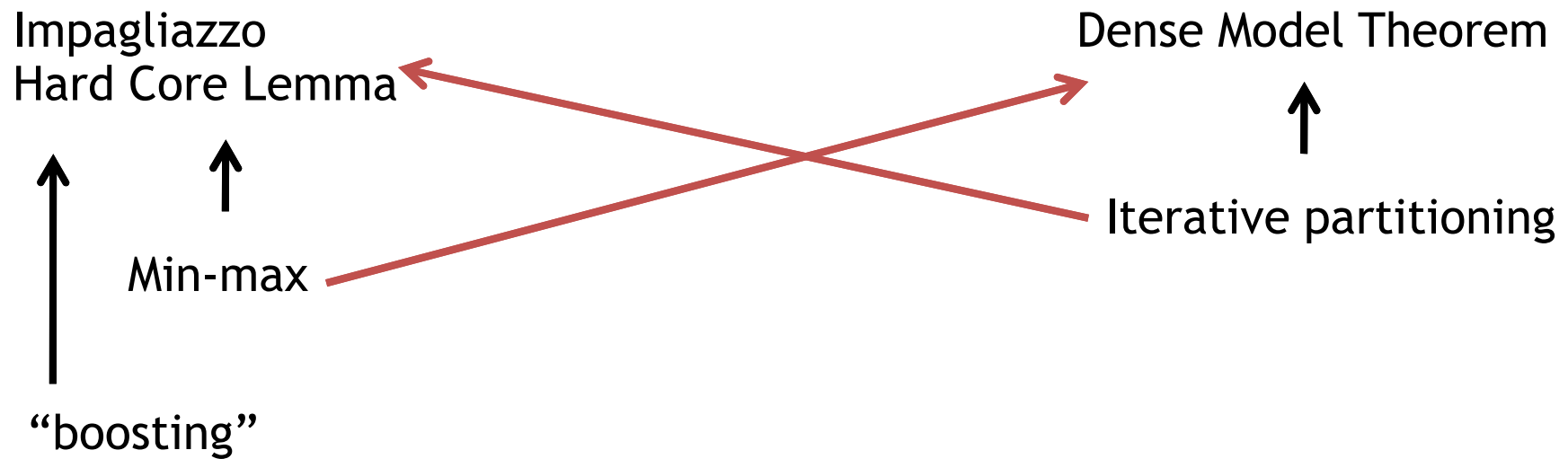
The Impagliazzo Hard-Core Lemma

- Suppose $g: \{0,1\}^n \rightarrow \{0,1\}$ is *weakly* hard-on-average:
for all f of size $S \cdot \text{poly}(1/\epsilon, 1/\delta)$
 $\Pr[f(x)=g(x)] \leq 1 - \delta$
- Then there is dense distribution on which g is strongly hard-on-average:
 - For all x , $H(x) \leq 1/\delta \cdot 2^n$ is such that
 - $\Pr_D[f(x) = g(x)] \leq 1/2 + \epsilon$ for all f of size S

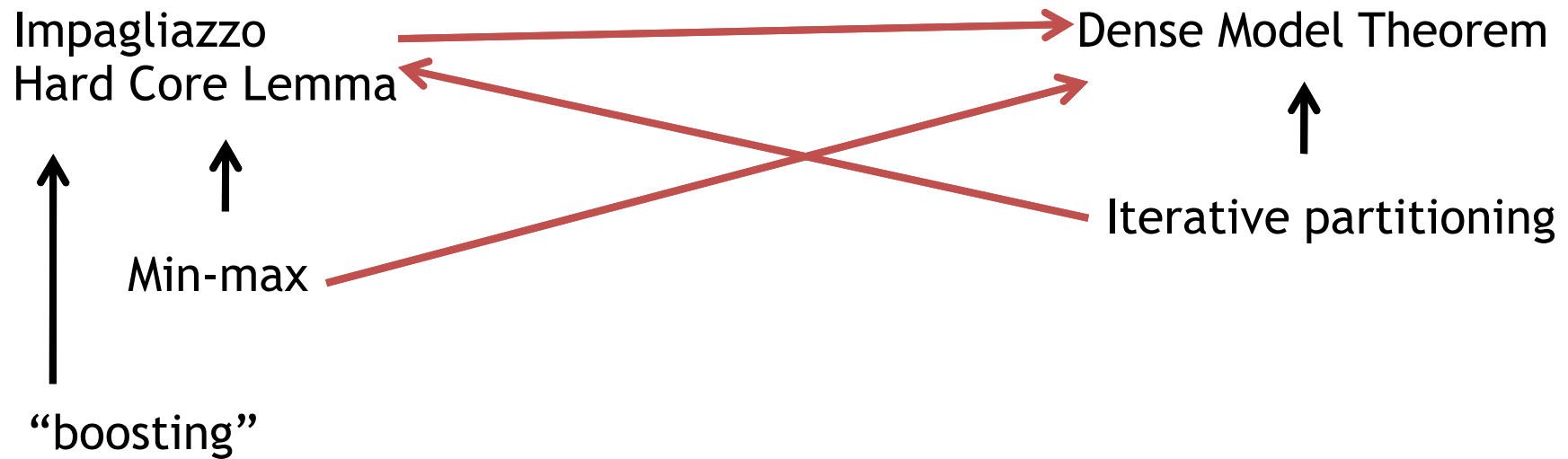
Comparison with Previous Proof



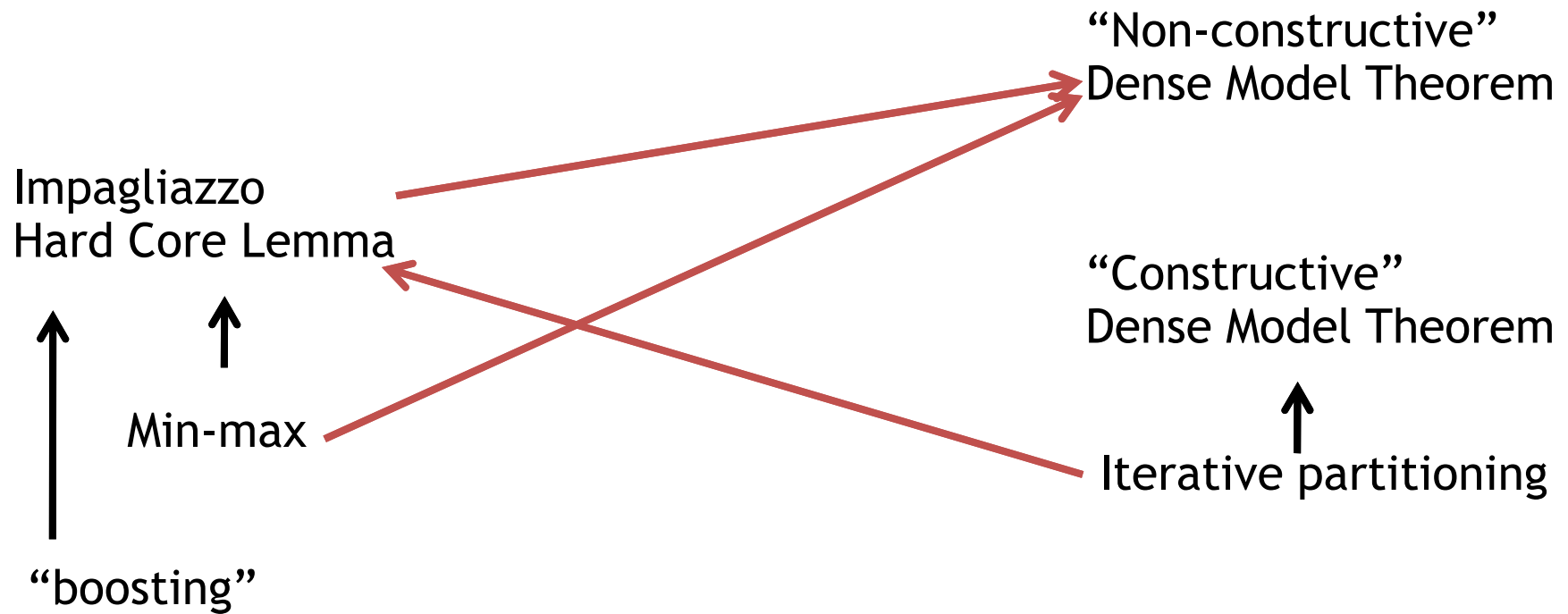
Comparison with Previous Proof



Comparison with Previous Proof

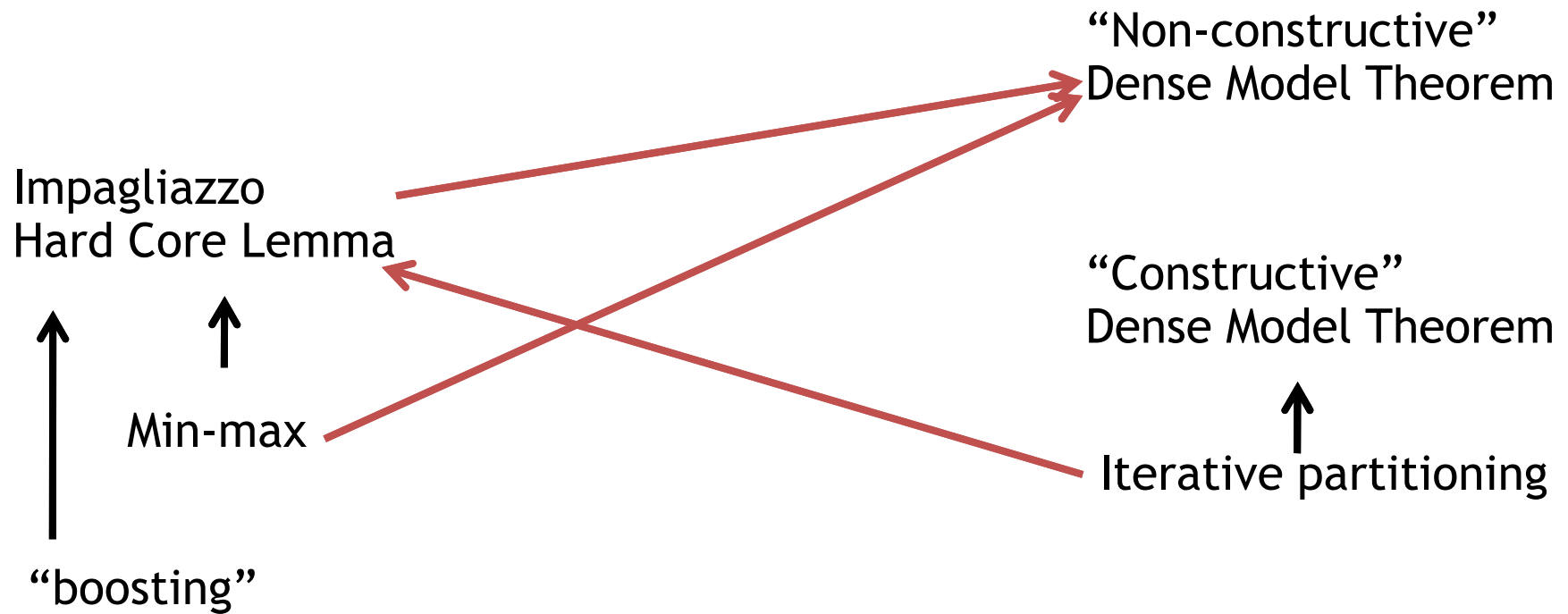


Comparison with Previous Proof

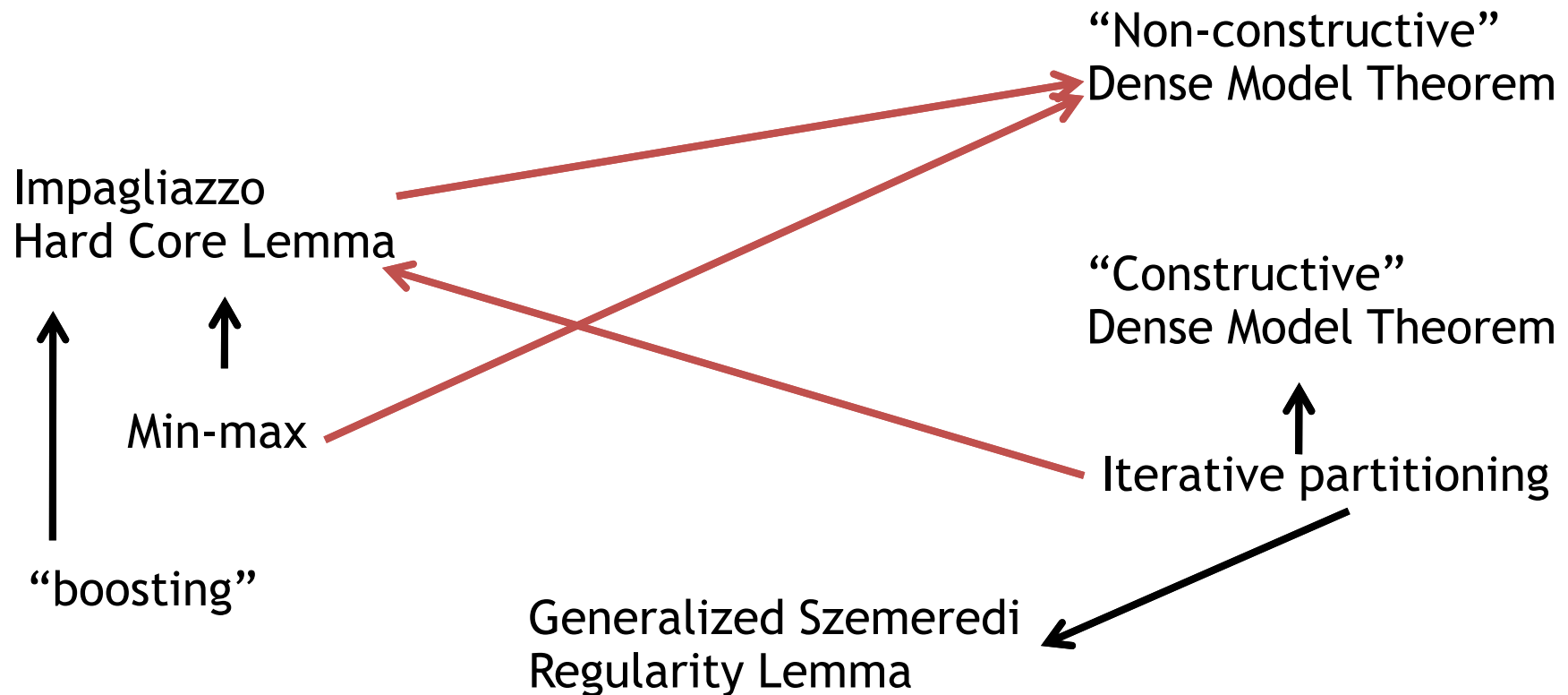


Ongoing work by T., Tulsiani, Vadhan

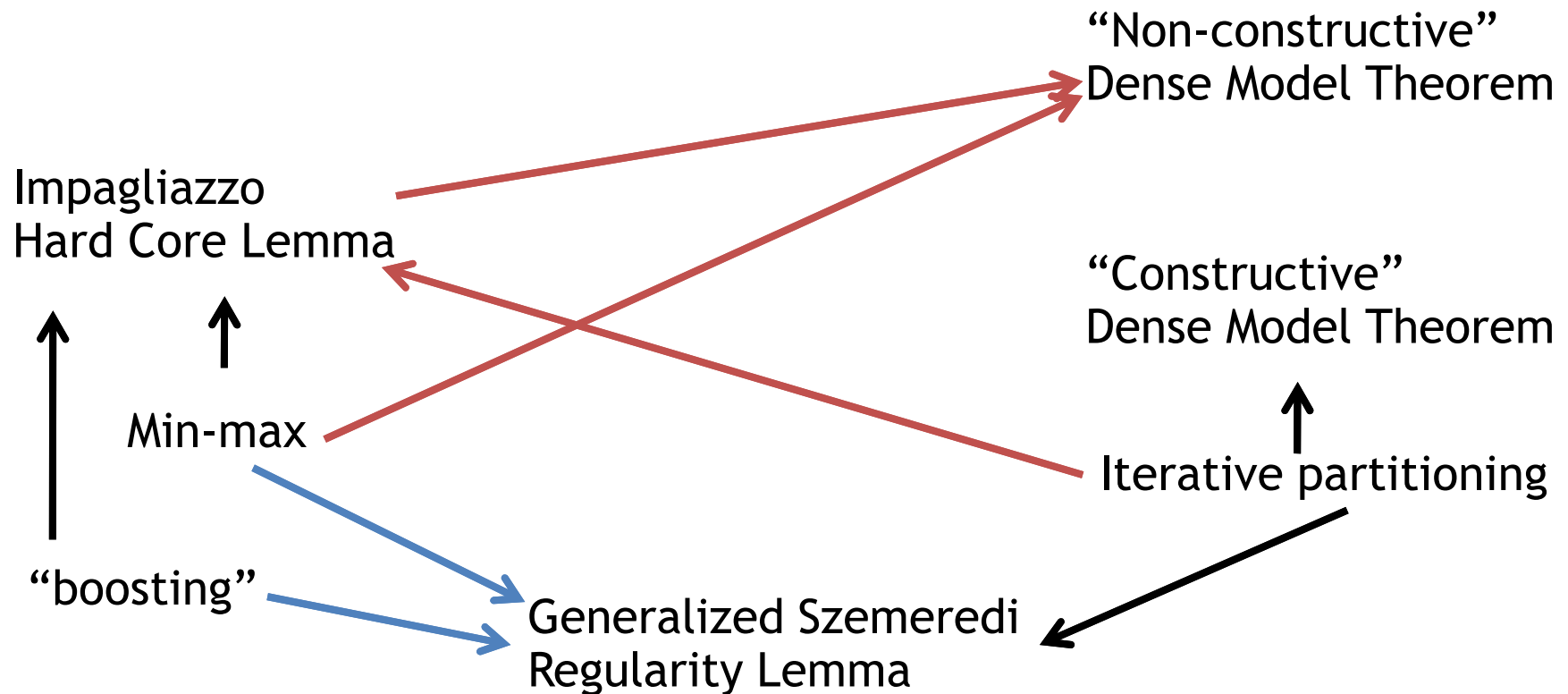
Comparison with Previous Proof



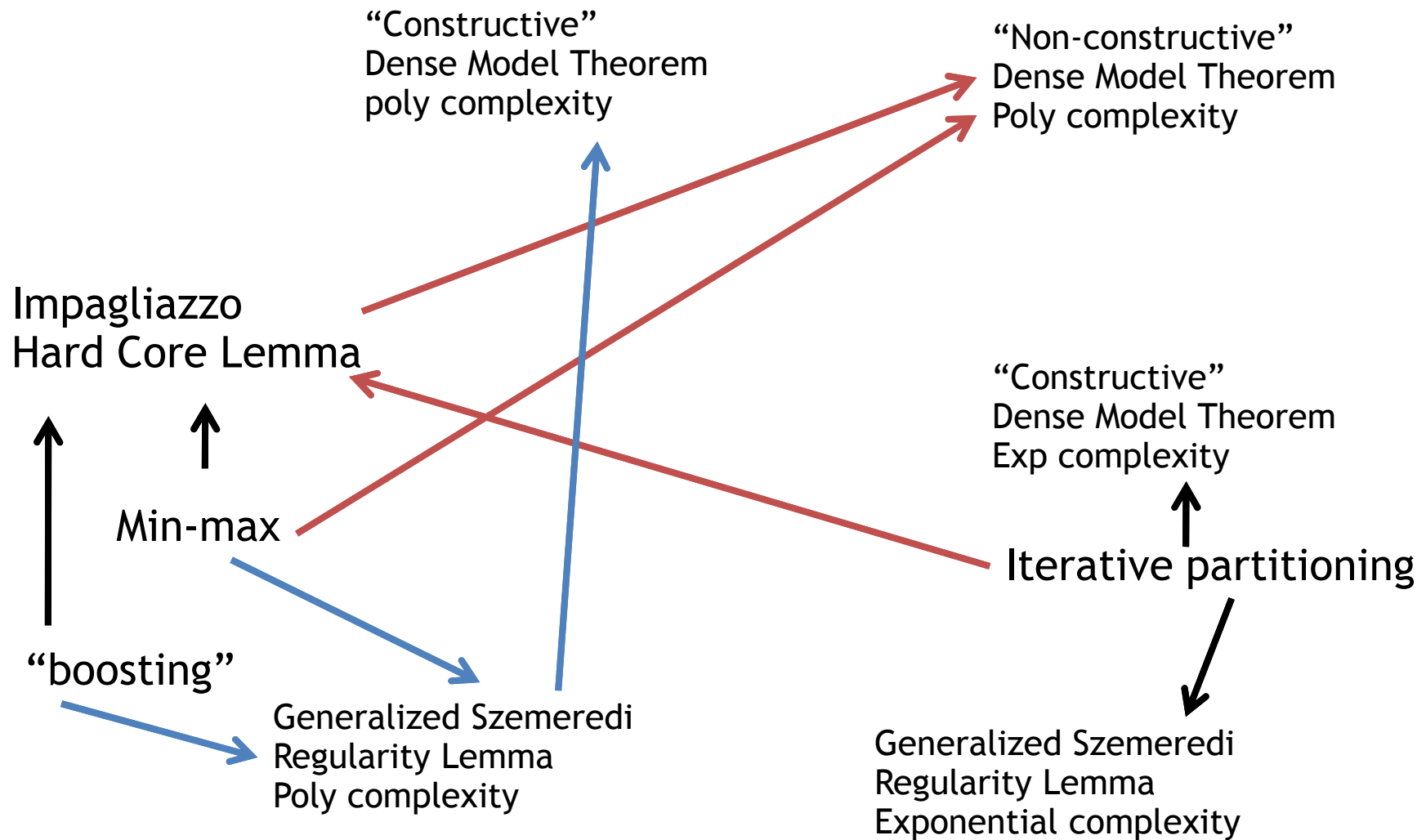
Comparison with Previous Proof



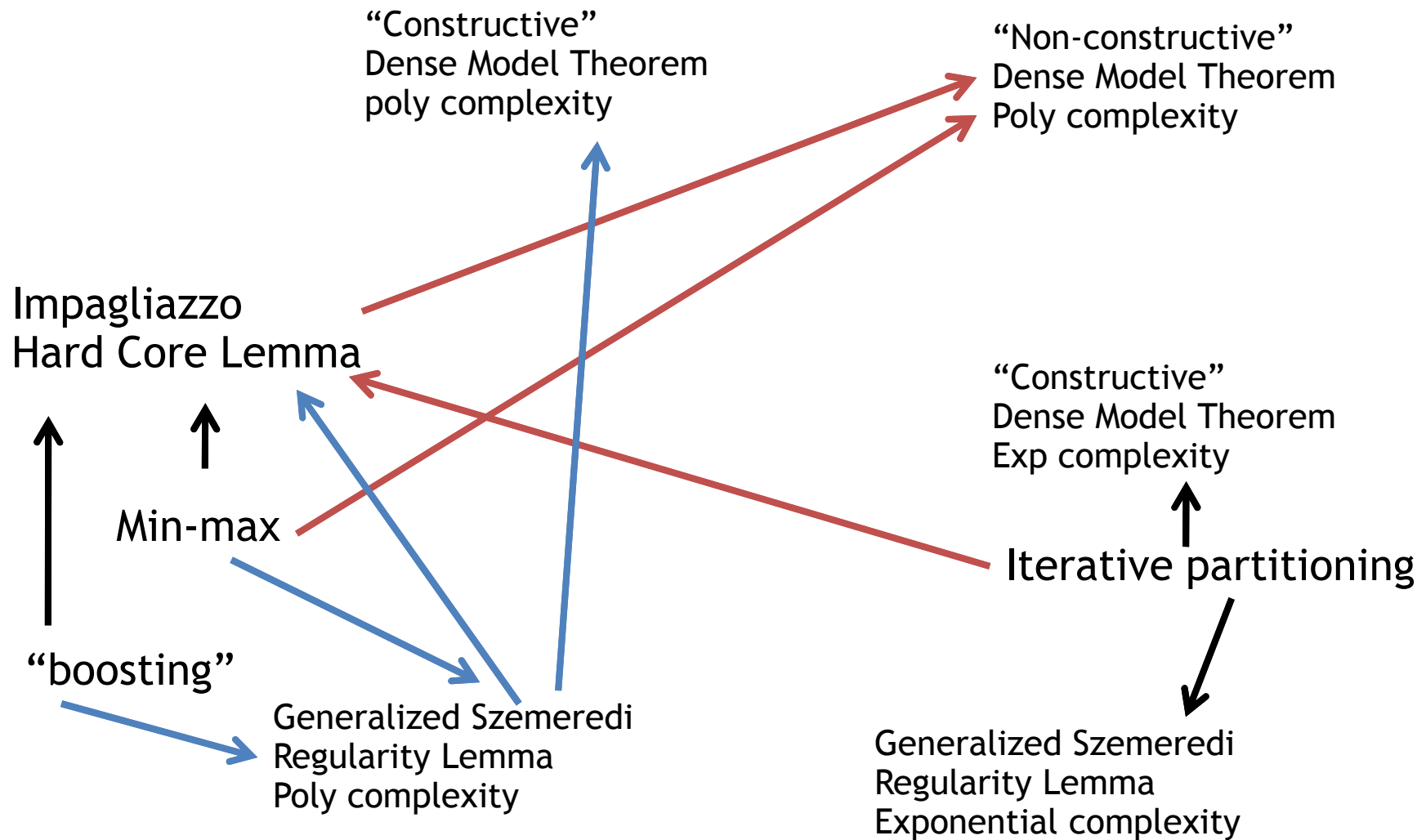
Comparison with Previous Proof



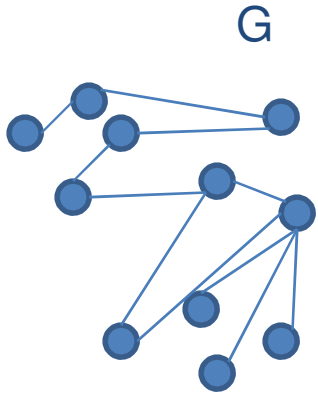
Comparison with Previous Proof



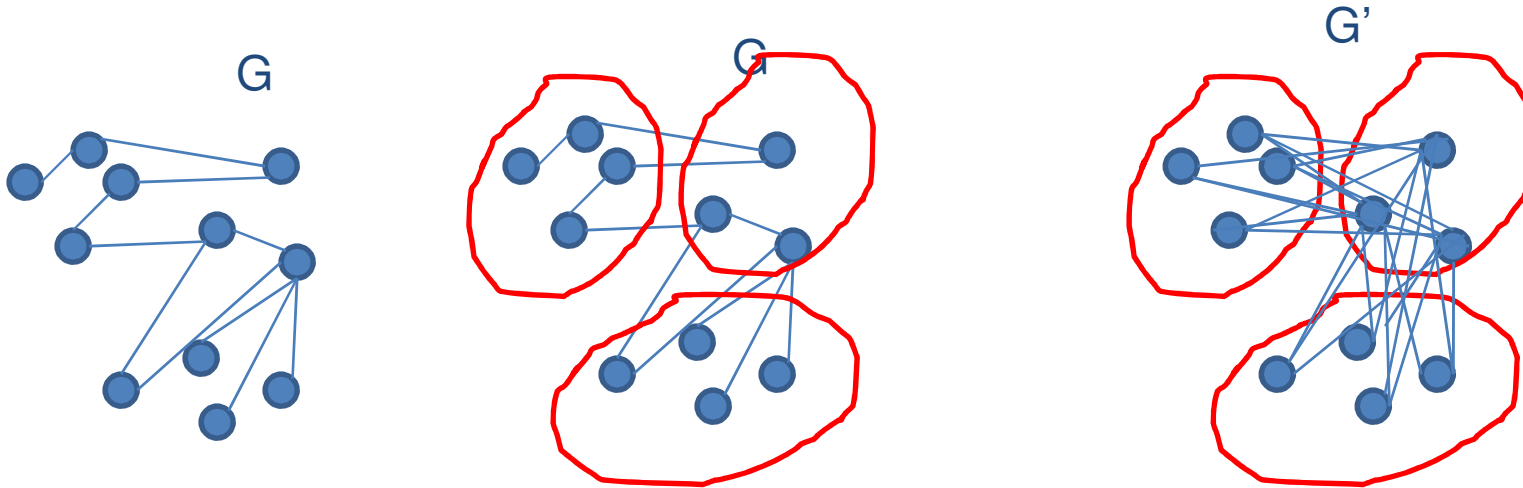
Comparison with Previous Proof



Regularity Lemma



Regularity Lemma



Given: dense graph G , approximation ε

Find partition of vertices into $O_{\varepsilon}(1)$ blocks

G is indistinguishable by cuts from graph G' that has weighted complete bipartite subgraph between blocks

Abstract Version

- Finite space X [edges of complete graph]
- $g: X \rightarrow [0,1]$ [graph]
- ε
- $F = \{ f \}, f: X \rightarrow [0,1]$ [char functions of cuts]
- Can find approximating function
 $A(x) = h(f_1(x), \dots, f_k(x)), k = \text{poly}(1/\varepsilon), f_i() \text{ in } F$
- Such that for all f in F
 $| \mathbf{E} f(x)g(x) - \mathbf{E} f(x)A(x) | = \leq \varepsilon$

Abstract Version

- Finite space X [edges of complete graph]
- $g: X \rightarrow [0,1]$ [graph]
- ε
- $F = \{ f \}$, $f: X \rightarrow [0,1]$ [char functions of cuts]

- Can find approximating function
 $A(x) = h(f_1(x), \dots, f_k(x))$, $k = \text{poly}(1/\varepsilon)$, $f_i() \in F$
in standard proof, h has $\exp(1/\varepsilon)$ complexity
- Such that for all f in F
$$| \mathbf{E} f(x)g(x) - \mathbf{E} f(x)A(x) | = \langle f, g-A \rangle \leq \varepsilon$$

Abstract Version

- Finite space X [edges of complete graph]
- $g: X \rightarrow [0,1]$ [graph]
- ε
- $F = \{ f \}, f: X \rightarrow [0,1]$ [char functions of cuts]

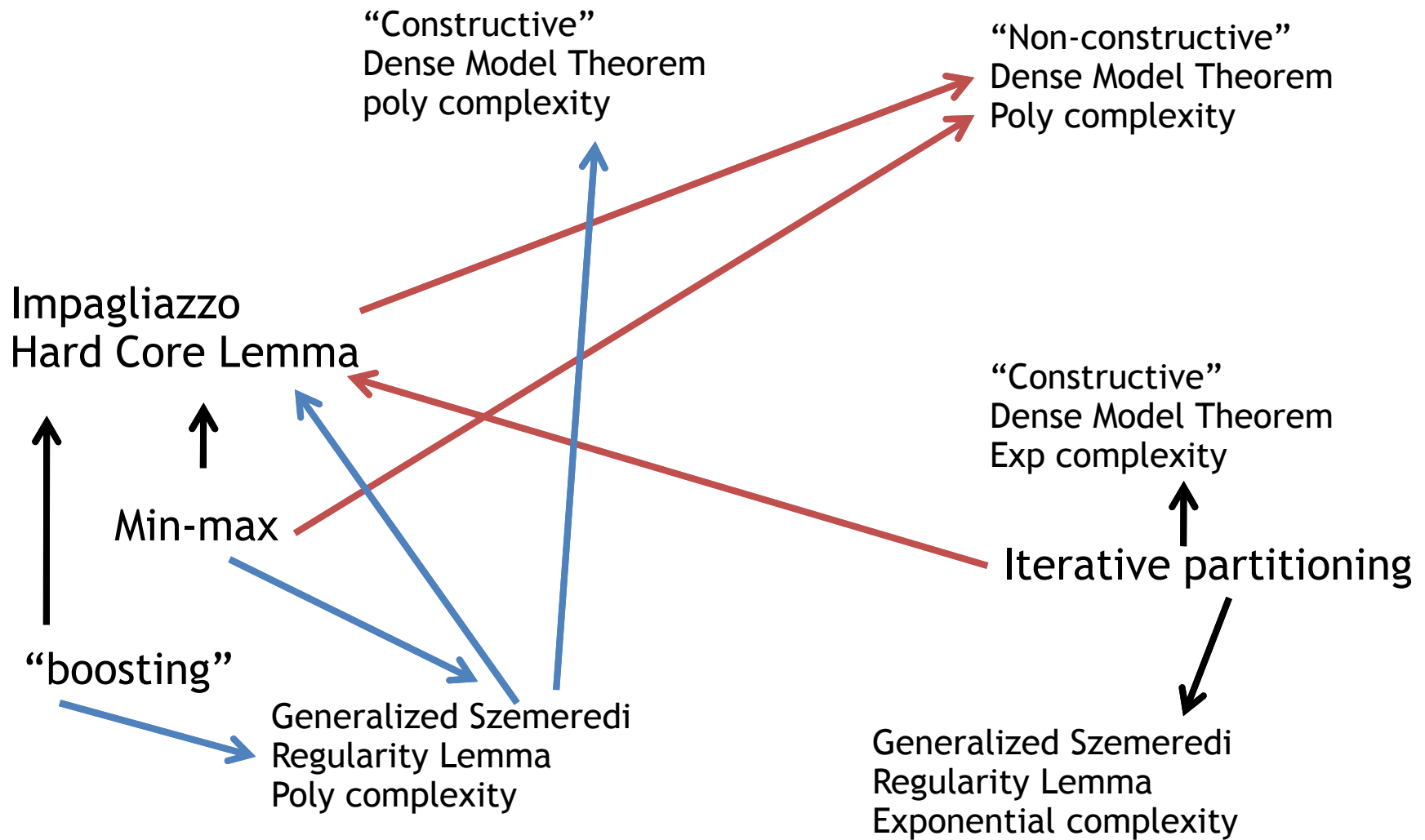
- Can find approximating function
 $A(x) = h(f_1(x), \dots, f_k(x)), k = \text{poly}(1/\varepsilon), f_i() \text{ in } F$
in new “boosting” proof, h has $\text{poly}(1/\varepsilon)$ complexity
- Such that for all f in F
 $| \mathbf{E} f(x)g(x) - \mathbf{E} f(x)A(x) | = \langle f, g-A \rangle \leq \varepsilon$

Rephrasing

- Finite space $X = \{0,1\}^n$
- Given distribution D such that $D(x) \leq 1/\delta 2^n$
(min-entropy $\geq n - \log 1/\delta$)
- There is samplable distribution M :
 - Also $M(x) \leq 1/\delta 2^n$
 - M is (S,ϵ) indistinguishable from D
 - Samplable (and computable) by circuits of size $S^* \text{poly}(1/\epsilon, 1/\delta)$


Derive the Hard Core Lemma




- Given: g weakly hard on average
- Find efficient approximation A of g
- Easy to prove:
 g is very hard on average on distribution in which point x has probability proportional to $|A(x) - g(x)|$
- Also easy to prove direct product lemma, Yao's XOR lemma, and other complexity result from "polynomial complexity regularity lemma"



Returning to big picture

- Additive combinatorics

- Graph theory
regularity lemma  Graph Property Testing


- Analysis
Gowers Uniformity  Pseudorandomness
 Direct Product Theorems
 PCP




- Ergodic Theory
???

- Finitary Ergodic Theory
??

Returning to the big picture

- Additive combinatorics

- Graph theory
regularity lemma  Graph Property Testing

- Analysis
Gowers Uniformity  Pseudorandomness
 Direct Product Theorems
 PCP

- Ergodic Theory
???

- Finitary Ergodic Theory
??  Average-case complexity
pseudorandomness