The Gowers Norm in the Testing of Boolean Functions

Victor Chen

Massachusetts Institute of Technology

April 23, 2009

Outline

Property testing

- dataset is massive, cannot be read in its entirety
- algorithm makes few queries into the input
- initiated in the the work of Blum, Luby, Rubinfeld

Property testing

- dataset is massive, cannot be read in its entirety
- algorithm makes few queries into the input
- initiated in the the work of Blum, Luby, Rubinfeld

In this talk, we focus on

- boolean function $f : \{0,1\}^n \to \{\text{True,False}\}$
- input is the truth table of f
- an algorithm can select an entry x and receive $f(x)$

Property testing

- dataset is massive, cannot be read in its entirety
- algorithm makes few queries into the input
- initiated in the the work of Blum, Luby, Rubinfeld

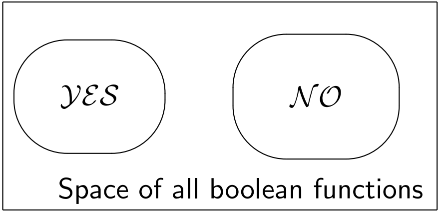
In this talk, we focus on

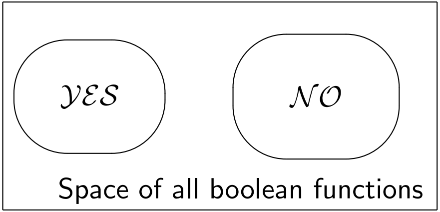
- boolean function $f : \{0,1\}^n \to \{\text{True,False}\}$
- input is the truth table of f
- an algorithm can select an entry x and receive $f(x)$

$f(s_1)$	$f(s_2)$	$f(s_3)$	$\cdots$	$f(s_{2^n})$

$$\begin{array}{c} \downarrow \\ \text{Alg} \end{array}$$

Definition of a testing algorithm



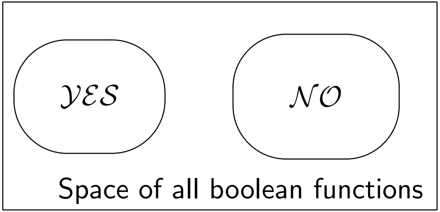


Definition

$T = T^f$ is a q-test for $(\mathcal{YES}, \mathcal{NO})$ if

- it makes at most q queries into f

Definition of a testing algorithm

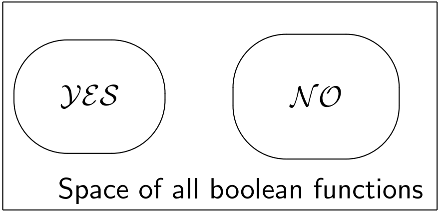


Definition

$T = T^f$ is a q-test for $(\mathcal{YES}, \mathcal{NO})$ if

- it makes at most q queries into f
- $\forall f \in \mathcal{YES}$, T always accepts

Definition of a testing algorithm

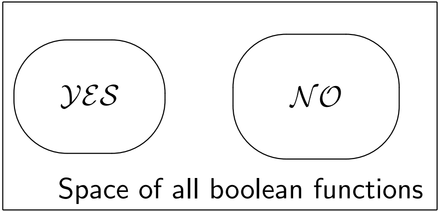


Definition

$T = T^f$ is a q-test for $(\mathcal{YES}, \mathcal{NO})$ if

- it makes at most q queries into f
- $\forall f \in \mathcal{YES}$, T always accepts
- $\forall f \in \mathcal{NO}$, T accepts w.p. < 1

Definition of a testing algorithm



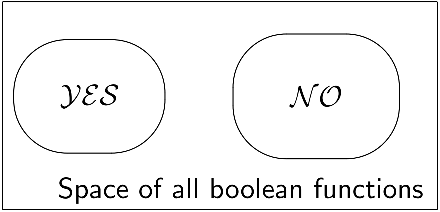
Definition

$T = T^f$ is a q-test for $(\mathcal{YES}, \mathcal{NO})$ if

- it makes at most q queries into f
- $\forall f \in \mathcal{YES}$, T always accepts
- $\forall f \in \mathcal{NO}$, T accepts w.p. < 1

- q fixed.

Definition of a testing algorithm



Definition

$T = T^f$ is a q-test for $(\mathcal{YES}, \mathcal{NO})$ if

- it makes at most q queries into f
- $\forall f \in \mathcal{YES}$, T always accepts
- $\forall f \in \mathcal{NO}$, T accepts w.p. < 1

- q fixed. if $f \in \mathcal{NO}$, f must be far from $\mathcal{YES}$

Outline

Dictatorship

- $f \in \mathcal{YES}$ if $f(x) = x(i)$

Dictatorship

- $f \in \mathcal{YES}$ if $f(x) = x(i)$
- motivation: dictatorship testing is a gadget in many PCP constructions (aka long code testing)

Dictatorship

- $f \in \mathcal{YES}$ if $f(x) = x(i)$
- motivation: dictatorship testing is a gadget in many PCP constructions (aka long code testing)
- introduced by Bellare, Goldreich, and Sudan
- studied by Parnas, Ron, Samorodnitsky in a combinatorial setting

Dictatorship

- $f \in \mathcal{YES}$ if $f(x) = x(i)$
- motivation: dictatorship testing is a gadget in many PCP constructions (aka long code testing)
- introduced by Bellare, Goldreich, and Sudan
- studied by Parnas, Ron, Samorodnitsky in a combinatorial setting

Our result:

A q-query (adaptive) test that
accepts w.p. 1 if $f \in \mathcal{YES}$

Dictatorship

- $f \in \mathcal{YES}$ if $f(x) = x(i)$
- motivation: dictatorship testing is a gadget in many PCP constructions (aka long code testing)
- introduced by Bellare, Goldreich, and Sudan
- studied by Parnas, Ron, Samorodnitsky in a combinatorial setting

Our result:

A q-query (adaptive) test that

accepts w.p. 1	if $f \in \mathcal{YES}$
accepts w.p. $\mathrm{poly}(q) \cdot 2^{-q}$	if $f \in \mathcal{NO}$.

connection to PCP

- $\mathcal{NO}$ must contain "anti-dictators"

connection to PCP

- $\mathcal{NO}$ must contain "anti-dictators"

  e.g. Majority, large parities, constant functions

connection to PCP

- $\mathcal{NO}$ must contain "anti-dictators"
  e.g. Majority, large parities, constant functions

- complement of $\mathcal{NO}$ must be "symmetry breaking" for the set $\{1, 2, \ldots, n\}$

connection to PCP

- $\mathcal{NO}$ must contain "anti-dictators"
  e.g. Majority, large parities, constant functions
- complement of $\mathcal{NO}$ must be "symmetry breaking" for the set $\{1, 2, \ldots, n\}$
- a symmetry breaking function helps in a PCP reduction

- $\mathcal{NO}$ must contain "anti-dictators"
  e.g. Majority, large parities, constant functions
- complement of $\mathcal{NO}$ must be "symmetry breaking" for the set $\{1, 2, \ldots, n\}$
- a symmetry breaking function helps in a PCP reduction

"meta theorem"

Under the unique games conjecture, a (q, c, s) dictatorship test translates into a PCP system with q queries, completeness $0.99c$, and soundness s.

What is a symmetry breaking function?

What is a symmetry breaking function?

- one that is at least $\left(\frac{1}{2} + \epsilon\right)$-close to a dictator

What is a symmetry breaking function?

- one that is at least $\left(\frac{1}{2}+\epsilon\right)$-close to a dictator
  does not include $x_1 + x_2$

What is a symmetry breaking function?

- one that is at least $\left(\frac{1}{2} + \epsilon\right)$-close to a dictator
  does not include $x_1 + x_2$
- [Håstad]: one that is close to a function depending only on a constant number of variables

What is a symmetry breaking function?

- one that is at least $\left(\frac{1}{2} + \epsilon\right)$-close to a dictator
  does not include $x_1 + x_2$
- [Håstad]: one that is close to a junta

What is a symmetry breaking function?

- one that is at least $\left(\frac{1}{2}+\epsilon\right)$-close to a dictator
  does not include $x_1 + x_2$

- [Håstad]: one that is close to a junta
  does not include $x_1 + \mathrm{Maj}(x_2, \ldots, x_n)$

What is a symmetry breaking function?

- one that is at least $\left(\frac{1}{2} + \epsilon\right)$-close to a dictator

  does not include $x_1 + x_2$

- [Håstad]: one that is close to a junta

  does not include $x_1 + \mathrm{Maj}(x_2, \ldots, x_n)$

- [DS,KKMO]: one that has an "influential variable"

Influence of variables

- The influence of variable i of f, $\mathrm{I}_i(f)$, is the expected variation of f on a random input whose i-th bit is flipped

Influence of variables

- The influence of variable i of f, $\mathrm{I}_i(f)$, is the expected variation of f on a random input whose i-th bit is flipped

- $f(x) = x_1 + x_2 + \ldots + x_n$.

Influence of variables

- The influence of variable i of f, $\mathrm{I}_i(f)$, is the expected variation of f on a random input whose i-th bit is flipped

- $f(x) = x_1 + x_2 + \ldots + x_n$. not symmetry breaking

Influence of variables

- The influence of variable i of f, $\mathrm{I}_i(f)$, is the expected variation of f on a random input whose i-th bit is flipped

Influence of variables

- The influence of variable i of f, $\mathrm{I}_i(f)$, is the expected variation of f on a random input whose i-th bit is flipped
- For $0 < \rho < \frac{1}{2}$, noise operator $T_\rho(f)(x) = \mathbb{E}_{\eta \in D_\rho} f(x + \eta)$,

Influence of variables

- The influence of variable i of f, $\mathrm{I}_i(f)$, is the expected variation of f on a random input whose i-th bit is flipped

- For $0 < \rho < \frac{1}{2}$, noise operator $T_\rho(f)(x) = \mathbb{E}_{\eta \in D_\rho} f(x + \eta)$,
  each bit of η is 1 w.p. ρ.

Influence of variables

- The influence of variable i of f, $\mathrm{I}_i(f)$, is the expected variation of f on a random input whose i-th bit is flipped
- For $0 < \rho < \frac{1}{2}$, noise operator $T_\rho(f)(x) = \mathbb{E}_{\eta \in D_\rho} f(x + \eta)$,

Influence of variables

- The influence of variable i of f, $\mathrm{I}_i(f)$, is the expected variation of f on a random input whose i-th bit is flipped
- For $0 < \rho < \frac{1}{2}$, noise operator $T_\rho(f)(x) = \mathbb{E}_{\eta \in D_\rho} f(x + \eta)$,
- ρ-attenuated influence of variable i is $\mathrm{I}_i(T_\rho(f))$.

Influence of variables

- The influence of variable i of f, $\mathrm{I}_i(f)$, is the expected variation of f on a random input whose i-th bit is flipped
- For $0 < \rho < \frac{1}{2}$, noise operator $T_\rho(f)(x) = \mathbb{E}_{\eta \in D_\rho} f(x + \eta)$,
- ρ-attenuated influence of variable i is $\mathrm{I}_i(T_\rho(f))$.
    - maximized at $\rho = 0$

Influence of variables

- The influence of variable i of f, $\mathrm{I}_i(f)$, is the expected variation of f on a random input whose i-th bit is flipped
- For $0 < \rho < \frac{1}{2}$, noise operator $T_\rho(f)(x) = \mathbb{E}_{\eta \in D_\rho} f(x + \eta)$,
- ρ-attenuated influence of variable i is $\mathrm{I}_i(T_\rho(f))$.
  - maximized at $\rho = 0$
  - $f(x) = x_1 + \ldots + x_n$. $\mathrm{I}_i(T_\rho(f)) = o(1)$.

Influence of variables

- The influence of variable i of f, $\mathrm{I}_i(f)$, is the expected variation of f on a random input whose i-th bit is flipped
- For $0 < \rho < \frac{1}{2}$, noise operator $T_\rho(f)(x) = \mathbb{E}_{\eta \in D_\rho} f(x + \eta)$,
- ρ-attenuated influence of variable i is $\mathrm{I}_i(T_\rho(f))$.
  - maximized at $\rho = 0$
  - $f(x) = x_1 + \ldots + x_n$. $\qquad \mathrm{I}_i(T_\rho(f)) = o(1)$.
  - $f(x) = x_1 + \mathrm{Maj}(x_2, \ldots, x_n)$. $\qquad \mathrm{I}_1(T_\rho(f)) > 0$.

Influence of variables

- The influence of variable i of f, $\mathrm{I}_i(f)$, is the expected variation of f on a random input whose i-th bit is flipped
- For $0 < \rho < \frac{1}{2}$, noise operator $T_\rho(f)(x) = \mathbb{E}_{\eta \in D_\rho} f(x + \eta)$,
- ρ-attenuated influence of variable i is $\mathrm{I}_i(T_\rho(f))$.
  - maximized at $\rho = 0$
  - $f(x) = x_1 + \ldots + x_n$. $\mathrm{I}_i(T_\rho(f)) = o(1)$.
  - $f(x) = x_1 + \mathrm{Maj}(x_2, \ldots, x_n)$. $\mathrm{I}_1(T_\rho(f)) > 0$.
- Upshot: any function has a finite number of variables with positive ρ-attenuated influence

Our result

- A function is symmetry breaking if there exists $i \in [n]$, $0 < \rho < \frac{1}{2}$ $\mathrm{I}_i(T_\rho f) > 0$

Our result

- A function is symmetry breaking if there exists $i \in [n]$, $0 < \rho < \frac{1}{2}$ $\mathrm{I}_i(T_\rho f) > 0$
- $f \in \mathcal{NO}$ if f is not symmetry breaking

Our result

- A function is symmetry breaking if there exists $i \in [n]$, $0 < \rho < \frac{1}{2}$ $\mathrm{I}_i(T_\rho f) > 0$

- $f \in \mathcal{NO}$ if f is not symmetry breaking

- Previous Works: q-query PCP system with completeness 1, soundness $2^{O(\sqrt{q})} \cdot 2^{-q}$.

- [Samorodnitsky+Trevisan06]: q-query dictatorship test with completeness $1 - \epsilon$, soundness $(q+1) \cdot 2^{-q}$.

Our result

- A function is symmetry breaking if there exists $i \in [n]$, $0 < \rho < \frac{1}{2}$ $\mathrm{I}_i(T_\rho f) > 0$
- $f \in \mathcal{NO}$ if f is not symmetry breaking

- Previous Works: q-query PCP system with completeness 1, soundness $2^{O(\sqrt{q})} \cdot 2^{-q}$.
- [Samorodnitsky+Trevisan06]: q-query dictatorship test with completeness $1 - \epsilon$, soundness $(q+1) \cdot 2^{-q}$.

Theorem (C08)

A q-query (adaptive) dictatorship test with completeness 1 and soundness $O(q^3 \cdot 2^{-q})$.

Outline

1. Introduction
   - Dictatorship testing
   - Testing graph free
2. Technique overview
3. Design & analysis of dictatorship test
4. Design & analysis of graph free test

A graph-free test

- Property of triangle-free

A graph-free test

- Property of triangle-free
  - $f \in \mathcal{YES}_{C_3}$ if f has no Schur triple ("triangle")

A graph-free test

- Property of triangle-free
  - $f \in \mathcal{YES}_{C_3}$ if f has no Schur triple ("triangle")
    i.e., no x, y such that $f(x) = f(y) = f(x + y) = 1$

A graph-free test

- Property of triangle-free
  - $f \in \mathcal{YES}_{C_3}$ if f has no Schur triple ("triangle")
  - $f \in \mathcal{NO}_\epsilon$ if f is ϵ-far from any function in $\mathcal{YES}$

A graph-free test

- Property of triangle-free
  - $f \in \mathcal{YES}_{C_3}$ if f has no Schur triple ("triangle")
  - $f \in \mathcal{NO}_\epsilon$ if f is ϵ-far from any function in $\mathcal{YES}$
- [Green]: a 3-query triangle-free test with completeness 1, soundness < 1.

A graph-free test

- Property of triangle-free
  - $f \in \mathcal{YES}_{C_3}$ if f has no Schur triple ("triangle")
  - $f \in \mathcal{NO}_\epsilon$ if f is ϵ-far from any function in $\mathcal{YES}$
- [Green]: a 3-query triangle-free test with completeness 1, soundness < 1.
- can this be generalized?

A graph-free test

- Property of triangle-free
  - $f \in \mathcal{YES}_{C_3}$ if f has no Schur triple ("triangle")
  - $f \in \mathcal{NO}_\epsilon$ if f is ϵ-far from any function in $\mathcal{YES}$
- [Green]: a 3-query triangle-free test with completeness 1, soundness < 1.
- can this be generalized?

Our result: joint with Bhattacharyya, Sudan, Xie

Let G be a graph with k edges. There is a k-query "G-free" test with completeness 1 and soundness < 1.

Motivation: property testing

Linear invariance

$\mathcal{YES}$ is linear-invariant if for every linear transformation L on $\{0,1\}^n$,

Motivation: property testing

Linear invariance

$\mathcal{YES}$ is linear-invariant if for every linear transformation L on $\{0,1\}^n$, if $f \in \mathcal{YES}$, then $f \circ L \in \mathcal{YES}$.

Motivation: property testing

Linear invariance

$\mathcal{YES}$ is linear-invariant if for every linear transformation L on $\{0,1\}^n$, if $f \in \mathcal{YES}$, then $f \circ L \in \mathcal{YES}$.

- example: low-degree testing

Motivation: property testing

Linear invariance

$\mathcal{YES}$ is linear-invariant if for every linear transformation L on $\{0,1\}^n$, if $f \in \mathcal{YES}$, then $f \circ L \in \mathcal{YES}$.

- example: low-degree testing
- [Kaufman, Sudan]: studied families of algebraic properties

Motivation: property testing

Linear invariance

$\mathcal{YES}$ is linear-invariant if for every linear transformation L on $\{0,1\}^n$, if $f \in \mathcal{YES}$, then $f \circ L \in \mathcal{YES}$.

- example: low-degree testing
- [Kaufman, Sudan]: studied families of algebraic properties
  attributed testability primarily to linear-invariance

Motivation: property testing

Linear invariance

$\mathcal{YES}$ is linear-invariant if for every linear transformation L on $\{0,1\}^n$, if $f \in \mathcal{YES}$, then $f \circ L \in \mathcal{YES}$.

- example: low-degree testing
- [Kaufman, Sudan]: studied families of algebraic properties
  attributed testability primarily to linear-invariance
- these properties are also *linear*. Is this necessary?

Motivation: property testing

Linear invariance

$\mathcal{YES}$ is linear-invariant if for every linear transformation L on $\{0,1\}^n$, if $f \in \mathcal{YES}$, then $f \circ L \in \mathcal{YES}$.

- example: low-degree testing
- [Kaufman, Sudan]: studied families of algebraic properties
  attributed testability primarily to linear-invariance
- these properties are also *linear*. Is this necessary?
- No. Property of triangle-free is linear-invariant & non-linear

Motivation: combinatorics

Removal lemma for graphs

(folklore) If a graph on n vertices has $o(n^3)$ triangles, then $o(n^2)$ edges can be removed so that the graph has no triangle.

Motivation: combinatorics

Removal lemma for graphs

[AFKS] Let H be a fixed graph. If a graph on n vertices has $o(n^{|E(H)|})$ copies of H, then $o(n^2)$ edges can be removed so that the graph has no copies of H.

Removal lemma for graphs

[AFKS] Let H be a fixed graph. If a graph on n vertices has $o(n^{|E(H)|})$ copies of H, then $o(n^2)$ edges can be removed so that the graph has no copies of H.

- contrapositive of removal lemma easily implies a testing algorithm

Motivation: combinatorics

Removal lemma for graphs

[AFKS] Let H be a fixed graph. If a graph on n vertices has $o(n^{|E(H)|})$ copies of H, then $o(n^2)$ edges can be removed so that the graph has no copies of H.

- contrapositive of removal lemma easily implies a testing algorithm
  [AFKS], [AS] . . . : strong characterization of which graph properties are testable

Motivation: combinatorics

Removal lemma for graphs

[AFKS] Let H be a fixed graph. If a graph on n vertices has $o(n^{|E(H)|})$ copies of H, then $o(n^2)$ edges can be removed so that the graph has no copies of H.

- contrapositive of removal lemma easily implies a testing algorithm [AFKS], [AS] . . . : strong characterization of which graph properties are testable
- main tool: Szemerédi's regularity lemma

Removal lemma for graphs

[AFKS] Let H be a fixed graph. If a graph on n vertices has $o(n^{|E(H)|})$ copies of H, then $o(n^2)$ edges can be removed so that the graph has no copies of H.

- contrapositive of removal lemma easily implies a testing algorithm
  [AFKS], [AS] . . . : strong characterization of which graph properties are testable
- main tool: Szemerédi's regularity lemma
- applications: additive combinatorics, e.g. arithmetic progressions

Green's removal lemma for functions

Green's removal lemma for functions

Theorem (Green)

Let $A = \{x : f(x) = 1\}$. $N = 2^n$. *If* A *has* $o(N^2)$ *Schur triples, then* $o(N)$ *points can be removed from* A *so that* A *has no Schur triple.*

Green's removal lemma for functions

Theorem (Green)

Let $A = \{x : f(x) = 1\}$. $N = 2^n$. *If* A *has* $o(N^2)$ *Schur triples, then* $o(N)$ *points can be removed from* A *so that* A *has no Schur triple.*

- lemma easily implies a testing algorithm

Green's removal lemma for functions

Theorem (Green)

Let $A = \{x : f(x) = 1\}$. $N = 2^n$. *If* A *has* $o(N^2)$ *Schur triples, then* $o(N)$ *points can be removed from* A *so that* A *has no Schur triple.*

- lemma easily implies a testing algorithm
- main tool: a regularity lemma for functions

Green's removal lemma for functions

Theorem (Green)

Let $A = \{x : f(x) = 1\}$. $N = 2^n$. *If* A *has* $o(N^2)$ *Schur triples, then* $o(N)$ *points can be removed from* A *so that* A *has no Schur triple.*

- lemma easily implies a testing algorithm
- main tool: a regularity lemma for functions
- motivated by a number theoretic conjecture

Green's conjecture

- Let M be an r by k matrix (rank r) over $\{0, 1\}$.

Green's conjecture

- Let M be an r by k matrix (rank r) over $\{0,1\}$.
- f is M-free if no $\vec{x} = (x_1, \ldots, x_k) \in \mathbb{F}_{2^n}^k$ such that

Green's conjecture

- Let M be an r by k matrix (rank r) over $\{0, 1\}$.
- f is M-free if no $\vec{x} = (x_1, \ldots, x_k) \in \mathbb{F}_{2^n}^k$ such that
  - $f(x_1), \ldots, f(x_k) = 1$
  - $M \cdot \vec{x} = \vec{0}$.

Green's conjecture

- Let M be an r by k matrix (rank r) over $\{0,1\}$.
- f is M-free if no $\vec{x} = (x_1, \ldots, x_k) \in \mathbb{F}_{2^n}^k$ such that
  - $f(x_1), \ldots, f(x_k) = 1$
  - $M \cdot \vec{x} = \vec{0}$.

triangle-free: $r = 1$, $k = 3$, $M = (1, 1, 1)$.

Green's conjecture

- Let M be an r by k matrix (rank r) over $\{0, 1\}$.
- f is M-free if no $\vec{x} = (x_1, \ldots, x_k) \in \mathbb{F}_{2^n}^k$ such that
  - $f(x_1), \ldots, f(x_k) = 1$
  - $M \cdot \vec{x} = \vec{0}$.

  triangle-free: $r = 1$, $k = 3$, $M = (1, 1, 1)$.

Green's conjecture

Let $A = \{x : f(x) = 1\}$. $N = 2^n$.

Green's conjecture

- Let M be an r by k matrix (rank r) over $\{0, 1\}$.
- f is M-free if no $\vec{x} = (x_1, \ldots, x_k) \in \mathbb{F}_{2^n}^k$ such that
  - $f(x_1), \ldots, f(x_k) = 1$
  - $M \cdot \vec{x} = \vec{0}$.

  triangle-free: $r = 1$, $k = 3$, $M = (1, 1, 1)$.

Green's conjecture

Let $A = \{x : f(x) = 1\}$. $N = 2^n$.
If A has $o(N^{k-r})$ copies of M, then $o(N)$ points can be removed from A so that A is M-free.

Summary of known results

- [this work]: M-free testable when M is "graphic"

Summary of known results

- [this work]: M-free testable when M is "graphic"
- [Král', Serra, Vena]: M-free testable when M is graphic

Summary of known results

- [this work]: M-free testable when M is "graphic"
- [Králʼ, Serra, Vena]: M-free testable when M is graphic
- [KSV2],[Shapira]: building on [KSV], M-free testable for arbitrary M

Summary of known results

- [this work]: M-free testable when M is "graphic"
- [Král', Serra, Vena]: M-free testable when M is graphic
- [KSV2],[Shapira]: building on [KSV], M-free testable for arbitrary M
- differences: ours – Fourier analytic
  [KSV] – graph-theoretic
  [KSV2], [Shapira] – hypergraph-theoretic

Summary of known results

- [this work]: M-free testable when M is "graphic"
- [Král', Serra, Vena]: M-free testable when M is graphic
- [KSV2],[Shapira]: building on [KSV], M-free testable for arbitrary M
- differences: ours – Fourier analytic
  [KSV] – graph-theoretic
  [KSV2], [Shapira] – hypergraph-theoretic
- similiarities: regularity lemmas, notions of pseudorandomness

Definition of graphic matrix

An r by k matrix M over $\{0, 1\}$ is graphic if

Definition of graphic matrix

An r by k matrix M over $\{0, 1\}$ is graphic if

- there exists a graph G on k edges

Definition of graphic matrix

An r by k matrix M over $\{0, 1\}$ is graphic if

- there exists a graph G on k edges
- each edge is associated with an integer from $[k]$

Definition of graphic matrix

An r by k matrix M over $\{0, 1\}$ is graphic if

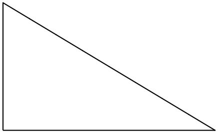
- there exists a graph G on k edges
- each edge is associated with an integer from $[k]$
- the indicator vector of each cycle C in G lies in the span of the rows of M

Definition of graphic matrix

An r by k matrix M over $\{0,1\}$ is graphic if

- there exists a graph G on k edges
- each edge is associated with an integer from $[k]$
- the indicator vector of each cycle C in G lies in the span of the rows of M

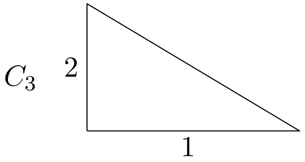
C_3



Definition of graphic matrix

An r by k matrix M over $\{0, 1\}$ is graphic if

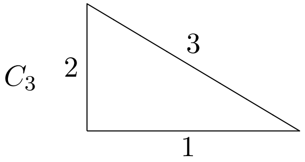
- there exists a graph G on k edges
- each edge is associated with an integer from $[k]$
- the indicator vector of each cycle C in G lies in the span of the rows of M



Definition of graphic matrix

An r by k matrix M over $\{0,1\}$ is graphic if

- there exists a graph G on k edges
- each edge is associated with an integer from $[k]$
- the indicator vector of each cycle C in G lies in the span of the rows of M

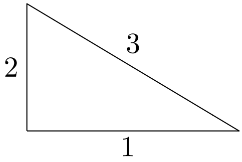


Definition of graphic matrix

An r by k matrix M over $\{0,1\}$ is graphic if

- there exists a graph G on k edges
- each edge is associated with an integer from $[k]$
- the indicator vector of each cycle C in G lies in the span of the rows of M

C_3



$$M = (1,1,1)$$

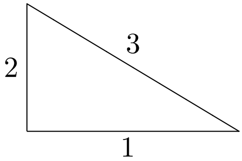
Definition of graphic matrix

An r by k matrix M over $\{0,1\}$ is graphic if

- there exists a graph G on k edges
- each edge is associated with an integer from $[k]$
- the indicator vector of each cycle C in G lies in the span of the rows of M

generalizes a natural link between a Schur triple and a triangle

C_3



$$M = (1, 1, 1)$$

Definition of graphic matrix

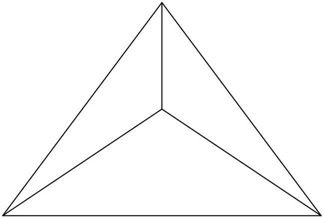
An r by k matrix M over $\{0, 1\}$ is graphic if

- there exists a graph G on k edges
- each edge is associated with an integer from $[k]$
- the indicator vector of each cycle C in G lies in the span of the rows of M

Definition of graphic matrix

An r by k matrix M over $\{0, 1\}$ is graphic if

- there exists a graph G on k edges
- each edge is associated with an integer from $[k]$
- the indicator vector of each cycle C in G lies in the span of the rows of M

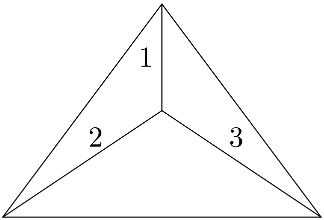


K_4

Definition of graphic matrix

An r by k matrix M over $\{0, 1\}$ is graphic if

- there exists a graph G on k edges
- each edge is associated with an integer from $[k]$
- the indicator vector of each cycle C in G lies in the span of the rows of M

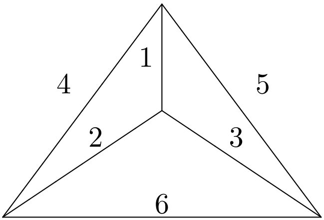


K_4

Definition of graphic matrix

An r by k matrix M over $\{0,1\}$ is graphic if

- there exists a graph G on k edges
- each edge is associated with an integer from $[k]$
- the indicator vector of each cycle C in G lies in the span of the rows of M

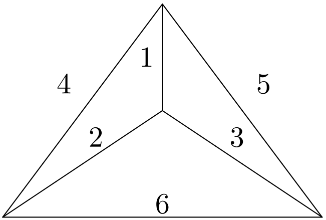


K_4

An r by k matrix M over $\{0,1\}$ is graphic if

- there exists a graph G on k edges
- each edge is associated with an integer from $[k]$
- the indicator vector of each cycle C in G lies in the span of the rows of M

$$M = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$



K_4

Our result

Theorem (Bhattacharyya,C',Sudan,Xie)

Our result

Theorem (Bhattacharyya,C',Sudan,Xie)

- *for any fixed* G*, a* $|E(G)|$*-query test for* $(\mathcal{YES}_G, \mathcal{NO}_\epsilon)$ *with completeness* 1 *and soundness* $\tau(\epsilon)$

Our result

Theorem (Bhattacharyya,C',Sudan,Xie)

- *for any fixed* G*, a* $|E(G)|$*-query test for* $(\mathcal{YES}_G, \mathcal{NO}_\epsilon)$ *with completeness* 1 *and soundness* $\tau(\epsilon)$
- *infinitely many (semantic) properties that are testable*

Our result

Theorem (Bhattacharyya,C',Sudan,Xie)

- *for any fixed* G*, a* $|E(G)|$*-query test for* $(\mathcal{YES}_G, \mathcal{NO}_\epsilon)$ *with completeness* 1 *and soundness* $\tau(\epsilon)$
- *infinitely many (semantic) properties that are testable*
  $$\ldots \mathcal{YES}_{C_7} \subsetneq \mathcal{YES}_{C_5} \subsetneq \mathcal{YES}_{C_3}$$

Our result

Theorem (Bhattacharyya,C',Sudan,Xie)

- *for any fixed* G*, a* $|E(G)|$*-query test for* $(\mathcal{YES}_G, \mathcal{NO}_\epsilon)$ *with completeness* 1 *and soundness* $\tau(\epsilon)$
- *infinitely many (semantic) properties that are testable*
  $$\ldots \mathcal{YES}_{C_7} \subsetneq \mathcal{YES}_{C_5} \subsetneq \mathcal{YES}_{C_3} \subsetneq \mathcal{YES}_{K_5} \subsetneq \mathcal{YES}_{K_{12}} \ldots$$

Our result

Theorem (Bhattacharyya,C',Sudan,Xie)

- *for any fixed* G*, a* $|E(G)|$*-query test for* $(\mathcal{YES}_G, \mathcal{NO}_\epsilon)$ *with completeness* 1 *and soundness* $\tau(\epsilon)$
- *infinitely many (semantic) properties that are testable*

Our result

Theorem (Bhattacharyya,C',Sudan,Xie)

- *for any fixed* G, *a* $|E(G)|$*-query test for* $(\mathcal{YES}_G, \mathcal{NO}_\epsilon)$ *with completeness* 1 *and soundness* $\tau(\epsilon)$
- *infinitely many (semantic) properties that are testable*
- *For any* k, *a* C_k*-free test with arbitary* $0/1$ *pattern*

Our result

Theorem (Bhattacharyya,C',Sudan,Xie)

- *for any fixed* G*, a* $|E(G)|$*-query test for* $(\mathcal{YES}_G, \mathcal{NO}_\epsilon)$ *with completeness* 1 *and soundness* $\tau(\epsilon)$
- *infinitely many (semantic) properties that are testable*
- *For any* k*, a* C_k*-free test with arbitary* $0/1$ *pattern*
  implies alternate proofs that linearity and affinity are testable

Our result

Theorem (Bhattacharyya,C',Sudan,Xie)

- *for any fixed G, a $|E(G)|$-query test for $(\mathcal{YES}_G, \mathcal{NO}_\epsilon)$ with completeness 1 and soundness $\tau(\epsilon)$*
- *infinitely many (semantic) properties that are testable*
- *For any k, a C_k-free test with arbitary $0/1$ pattern*
  implies alternate proofs that linearity and affinity are testable

Can only guarantee $\tau(\epsilon) \geq 2^{-O(W(\frac{1}{\epsilon}))}$,
where $W(t)$ denotes a tower of twos with height t

Outline

1. Introduction
   - Dictatorship testing
   - Testing graph free
2. Technique overview
3. Design & analysis of dictatorship test
4. Design & analysis of graph free test

Designing a testing algorithm: a perspective

Designing a testing algorithm: a perspective

- $\mathcal{YES}$: typically well-defined

Designing a testing algorithm: a perspective

- $\mathcal{YES}$: typically well-defined
  e,g. linear functions, polynomials

Designing a testing algorithm: a perspective

- $\mathcal{YES}$: typically well-defined
  e,g. linear functions, polynomials
- $\mathcal{NO}$: often defined in relation to $\mathcal{YES}$

Designing a testing algorithm: a perspective

- $\mathcal{YES}$: typically well-defined
  e,g. linear functions, polynomials
- $\mathcal{NO}$: often defined in relation to $\mathcal{YES}$
  contains objects very "different" from those in $\mathcal{YES}$

Designing a testing algorithm: a perspective

- $\mathcal{YES}$: typically well-defined
  e,g. linear functions, polynomials
- $\mathcal{NO}$: often defined in relation to $\mathcal{YES}$
  contains objects very "different" from those in $\mathcal{YES}$
- define a notion of "local structure"

Designing a testing algorithm: a perspective

- $\mathcal{YES}$: typically well-defined
  e,g. linear functions, polynomials
- $\mathcal{NO}$: often defined in relation to $\mathcal{YES}$
  contains objects very "different" from those in $\mathcal{YES}$
- define a notion of "local structure"

Test T:

- selects a random local structure.
- accepts iff f has no structure.

Analysis of a testing algorithm: a perspective

Analysis of a testing algorithm: a perspective

- $f \in \mathcal{YES}$: easy to analyze

Analysis of a testing algorithm: a perspective

- $f \in \mathcal{YES}$: easy to analyze
  show f has no local structure

Analysis of a testing algorithm: a perspective

- $f \in \mathcal{YES}$: easy to analyze
- $f \in \mathcal{NO}$: requires a more delicate argument

Analysis of a testing algorithm: a perspective

- $f \in \mathcal{YES}$: easy to analyze
- $f \in \mathcal{NO}$: requires a more delicate argument

  show f has many local structures

Analysis of a testing algorithm: a perspective

- $f \in \mathcal{YES}$: easy to analyze
- $f \in \mathcal{NO}$: requires a more delicate argument

Proof strategy:

Analysis of a testing algorithm: a perspective

- $f \in \mathcal{YES}$: easy to analyze
- $f \in \mathcal{NO}$: requires a more delicate argument

Proof strategy:

- Fix $\delta > 0$. If f is a random function with density δ,

Analysis of a testing algorithm: a perspective

- $f \in \mathcal{YES}$: easy to analyze
- $f \in \mathcal{NO}$: requires a more delicate argument

Proof strategy:

- Fix $\delta > 0$. If f is a random function with density δ, easy to analyze

Analysis of a testing algorithm: a perspective

- $f \in \mathcal{YES}$: easy to analyze
- $f \in \mathcal{NO}$: requires a more delicate argument

Proof strategy:

- Fix $\delta > 0$. If f is a random function with density δ, easy to analyze
- Define a notion of pseudorandomness to relate

Analysis of a testing algorithm: a perspective

- $f \in \mathcal{YES}$: easy to analyze
- $f \in \mathcal{NO}$: requires a more delicate argument

Proof strategy:

- Fix $\delta > 0$. If f is a random function with density δ, easy to analyze
- Define a notion of pseudorandomness to relate

$$\Pr[\text{Test accepts} | f \in \mathcal{NO}]$$

Analysis of a testing algorithm: a perspective

- $f \in \mathcal{YES}$: easy to analyze
- $f \in \mathcal{NO}$: requires a more delicate argument

Proof strategy:

- Fix $\delta > 0$. If f is a random function with density δ, easy to analyze
- Define a notion of pseudorandomness to relate

$$\Pr[\text{Test accepts} | f \in \mathcal{NO}]$$

$$\text{to} \quad \Pr[\text{Test accepts} | f \text{ random}]$$

Analysis of a testing algorithm: a perspective

- $f \in \mathcal{YES}$: easy to analyze
- $f \in \mathcal{NO}$: requires a more delicate argument

Proof strategy:

- Fix $\delta > 0$. If f is a random function with density δ, easy to analyze
- Define a notion of pseudorandomness to relate

$$\Pr[\text{Test accepts} | f \in \mathcal{NO}]$$

$$\Pr[\text{Test accepts} | \quad f \quad \text{pseudorandom}]$$

$$\text{to} \quad \Pr[\text{Test accepts} | f \text{ random}]$$

Analysis of a testing algorithm: a perspective

- $f \in \mathcal{YES}$: easy to analyze
- $f \in \mathcal{NO}$: requires a more delicate argument

Proof strategy:

- Fix $\delta > 0$. If f is a random function with density δ, easy to analyze
- Define a notion of pseudorandomness to relate

$$\begin{aligned} &\Pr[\text{Test accepts} | f \in \mathcal{NO}] \\ \approx \quad &\Pr[\text{Test accepts} | \Phi(f) \text{ pseudorandom}] \\ \text{to} \quad &\Pr[\text{Test accepts} | f \text{ random}] \end{aligned}$$

Analysis of a testing algorithm: a perspective

- $f \in \mathcal{YES}$: easy to analyze
- $f \in \mathcal{NO}$: requires a more delicate argument

Proof strategy:

- Fix $\delta > 0$. If f is a random function with density δ, easy to analyze
- Define a notion of pseudorandomness to relate

$$\begin{aligned} &\Pr[\text{Test accepts} | f \in \mathcal{NO}] \\ \approx \quad &\Pr[\text{Test accepts} | \Phi(f) \text{ pseudorandom}] \\ \text{to} \quad &\Pr[\text{Test accepts} | f \text{ random}] \end{aligned}$$

where $\Phi(f)$ is some "extension of f" dependent on $(\mathcal{YES}, \mathcal{NO})$

A notion of pseudorandomness

f is degree $(d-1)$-pseudorandom if its d-th Gowers norm is $o(1)$

A notion of pseudorandomness

f is degree $(d-1)$-pseudorandom if its d-th Gowers norm is $o(1)$

The Gowers norm

A notion of pseudorandomness

f is degree $(d-1)$-pseudorandom if its d-th Gowers norm is $o(1)$

The Gowers norm

- For every $d \in \mathbb{Z}^+, d \geq 2$, a d-th norm is defined on functions

A notion of pseudorandomness

f is degree $(d-1)$-pseudorandom if its d-th Gowers norm is $o(1)$

The Gowers norm

- For every $d \in \mathbb{Z}^+, d \geq 2$, a d-th norm is defined on functions
- $d = 2$ corresponds to f's Fourier transform

A notion of pseudorandomness

f is degree $(d-1)$-pseudorandom if its d-th Gowers norm is $o(1)$

The Gowers norm

- For every $d \in \mathbb{Z}^+, d \geq 2$, a d-th norm is defined on functions
- $d = 2$ corresponds to f's Fourier transform
- norms are monotonically increasing

A notion of pseudorandomness

f is degree $(d-1)$-pseudorandom if its d-th Gowers norm is $o(1)$

The Gowers norm

- For every $d \in \mathbb{Z}^+, d \geq 2$, a d-th norm is defined on functions
- $d = 2$ corresponds to f's Fourier transform
- norms are monotonically increasing
- Roughly, f with $o(1)$ d-th Gowers norm is equivalent to f having $o(1)$ correlation with every degree $d-1$ polynomials

A notion of pseudorandomness

f is degree $(d-1)$-pseudorandom if its d-th Gowers norm is $o(1)$

The Gowers norm

- For every $d \in \mathbb{Z}^+, d \geq 2$, a d-th norm is defined on functions
- $d = 2$ corresponds to f's Fourier transform
- norms are monotonically increasing
- Roughly, f with $o(1)$ d-th Gowers norm is equivalent to f having $o(1)$ correlation with every degree $d-1$ polynomials

A notion of pseudorandomness

f is degree $(d-1)$-pseudorandom if its d-th Gowers norm is $o(1)$

The Gowers norm

- For every $d \in \mathbb{Z}^+, d \geq 2$, a d-th norm is defined on functions
- $d = 2$ corresponds to f's Fourier transform
- norms are monotonically increasing
- Roughly, f with $o(1)$ d-th Gowers norm is equivalent to f having $o(1)$ correlation with every degree $d-1$ polynomials

roughly: due to values of d, field characteristic, roots of unity, etc

The Gowers uniformity norm $\|f\|_{U_d}$

The Gowers uniformity norm $\|f\|_{U_d}$

Definition

- $\|f\|_{U_2} = ||\hat{f}||_4$
  i.e., U_2 norm is the L_4 norm of f's Fourier transform

- Inductively, define $\|f\|_{U_{d+1}}^{2^{d+1}} = \mathbb{E}_h \|\Delta_h f\|_{U_d}^{2^d}$,

  where $\Delta_h f(x) = f(x)f(x+h)$ denotes the discrete derivative of f.

The Gowers uniformity norm $\|f\|_{U_d}$

Definition

- $\|f\|_{U_2} = ||\hat{f}||_4$
  i.e., U_2 norm is the L_4 norm of f's Fourier transform
- Inductively, define $\|f\|_{U_{d+1}}^{2^{d+1}} = \mathbb{E}_h \|\Delta_h f\|_{U_d}^{2^d}$,

  where $\Delta_h f(x) = f(x)f(x+h)$ denotes the discrete derivative of f.

- Expanding, $\|f\|_{U_2}^4 = \mathbb{E}_{x,y,z}[f(x)f(x+y)f(x+z)f(x+y+z)]$
- monotonicity: $\|f\|_{U_2} \leq \|f\|_{U_3} \leq \dots$

Generalized von-Neumann type theorems

- statements that show certain "estimations of f" are bounded above by the Gowers norm of f

Generalized von-Neumann type theorems

- statements that show certain "estimations of f" are bounded above by the Gowers norm of f
- [Gowers:] Let $A \subseteq [N]$ with density δ.

Generalized von-Neumann type theorems

- statements that show certain "estimations of f" are bounded above by the Gowers norm of f

- [Gowers:] Let $A \subseteq [N]$ with density δ.
  If $\|1_A - \delta\|_{U_{k-1}} = o(1)$, then A has approximately $\delta^k N^2$ k-term AP.

Generalized von-Neumann type theorems

- statements that show certain "estimations of f" are bounded above by the Gowers norm of f

- [Samorodnitsky, S.&Trevisan06]: The acceptance probability of the AKKLR test for degree d polynomials is bounded above by the $(d+1)$-th Gowers norm

Generalized von-Neumann type theorems

- statements that show certain "estimations of f" are bounded above by the Gowers norm of f
- [Green&Tao:] A system of linear equations with "complexity d" is bounded above by the $(d+1)$-th Gowers norm

System of linear equations with low complexity

Theorem (Green & Tao)

Suppose the system of linear equations $L_1, \ldots, L_k$ over variables $x_1, \ldots, x_m$ has "complexity d."

System of linear equations with low complexity

Theorem (Green & Tao)

Suppose the system of linear equations $L_1, \ldots, L_k$ over variables $x_1, \ldots, x_m$ has "complexity d." Then

$$\mathop{\mathbb{E}}_{x_1,\ldots,x_m}\left[\prod_{i\in[k]} f_i(L_i(x_1,\ldots,x_m))\right] \le \min_{i\in[k]} \|f_i\|_{U_{d+1}}$$

System of linear equations with low complexity

$L_1, \ldots, L_k$ has complexity d if d is the minimum s.t. for each $i \in [k]$,

System of linear equations with low complexity

$L_1, \ldots, L_k$ has complexity d if d is the minimum s.t. for each $i \in [k]$,

can cover $\{L_j\}_{j \neq i}$ by $d+1$ classes such that L_i does not lie in the span of each class

System of linear equations with low complexity

$L_1, \ldots, L_k$ has complexity d if d is the minimum s.t. for each $i \in [k]$,

can cover $\{L_j\}_{j \neq i}$ by $d+1$ classes such that L_i does not lie in the span of each class

Examples:

- variables x, y, $L_1(x,y) = x$, $L_2(x,y) = y$, $L_3(x,y) = x + y$

System of linear equations with low complexity

$L_1, \ldots, L_k$ has complexity d if d is the minimum s.t. for each $i \in [k]$,

can cover $\{L_j\}_{j \neq i}$ by $d+1$ classes such that L_i does not lie in the span of each class

Examples:

- variables x, y, $L_1(x,y) = x$, $L_2(x,y) = y$, $L_3(x,y) = x + y$
  has complexity 1

System of linear equations with low complexity

$L_1, \ldots, L_k$ has complexity d if d is the minimum s.t. for each $i \in [k]$,

can cover $\{L_j\}_{j \neq i}$ by $d+1$ classes such that L_i does not lie in the span of each class

Examples:

- variables x, y, $L_1(x,y) = x$, $L_2(x,y) = y$, $L_3(x,y) = x+y$
  has complexity 1
- variables x, y, z, linear equations $x, y, z, x+y, y+z, x+z, x+y+z$

System of linear equations with low complexity

$L_1, \ldots, L_k$ has complexity d if d is the minimum s.t. for each $i \in [k]$,

can cover $\{L_j\}_{j \neq i}$ by $d+1$ classes such that L_i does not lie in the span of each class

Examples:

- variables x, y, $L_1(x,y) = x$, $L_2(x,y) = y$, $L_3(x,y) = x + y$
  has complexity 1
- variables x, y, z, linear equations $x, y, z, x+y, y+z, x+z, x+y+z$
  has complexity 2

System of linear equations with low complexity

$L_1, \ldots, L_k$ has complexity d if d is the minimum s.t. for each $i \in [k]$,

can cover $\{L_j\}_{j \neq i}$ by $d+1$ classes such that L_i does not lie in the span of each class

Examples:

- variables x, y, $L_1(x,y) = x$, $L_2(x,y) = y$, $L_3(x,y) = x+y$
  has complexity 1
- variables x, y, z, linear equations $x, y, z, x+y, y+z, x+z, x+y+z$
  has complexity 2
- variables x, y, z, linear equations $x, y, z, x+y, y+z, x+z$; K_4

System of linear equations with low complexity

$L_1, \dots, L_k$ has complexity d if d is the minimum s.t. for each $i \in [k]$,

can cover $\{L_j\}_{j \neq i}$ by $d+1$ classes such that L_i does not lie in the span of each class

Examples:

- variables x, y, $L_1(x,y) = x$, $L_2(x,y) = y$, $L_3(x,y) = x+y$
  has complexity 1
- variables x, y, z, linear equations $x, y, z, x+y, y+z, x+z, x+y+z$
  has complexity 2
- variables x, y, z, linear equations $x, y, z, x+y, y+z, x+z$; K_4
  has complexity 1

Outline

Proof overview

- Find a basic dictatorship test that has completeness 1 and soundness $\frac{1}{2}$.

Proof overview

- Find a basic dictatorship test that has completeness 1 and soundness $\frac{1}{2}$.
- Iterate this basic test by reusing queries from previous iterations.

Proof overview

- Find a basic dictatorship test that has completeness 1 and soundness $\frac{1}{2}$.
- Iterate this basic test by reusing queries from previous iterations.
- Apply von-Neumann type theorem and the following lemma:

Proof overview

- Find a basic dictatorship test that has completeness 1 and soundness $\frac{1}{2}$.
- Iterate this basic test by reusing queries from previous iterations.
- Apply von-Neumann type theorem and the following lemma:

ST Lemma:

For balanced function f, if for all $i \in [n]$ $\mathrm{I}_i(f) = o(1)$, then for all $d \in \mathbb{Z}^+$, $\|f\|_{U_d} = o(1)$.

Basic test with completeness 1

- many 3-query test in the literature: Håstad 97, GLST 98, Khot & Saket 05, O'Donell & Wu 09

Basic test with completeness 1

- many 3-query test in the literature: Håstad 97, GLST 98, Khot & Saket 05, O'Donell & Wu 09
- monomial testing: Parnas, Ron, Samorodnitsky 02

Basic test with completeness 1

- many 3-query test in the literature: Håstad 97, GLST 98, Khot & Saket 05, O'Donell & Wu 09
- monomial testing: Parnas, Ron, Samorodnitsky 02
- essentially checks if $f(y) \wedge f(z) = f(y \wedge z)$.

Basic test with completeness 1

Test with access to $f : \{0,1\}^n \to \{\text{-}1,1\}$

Basic test with completeness 1

Test with access to $f : \{0,1\}^n \to \{\text{-}1,1\}$

1. Pick x_i, x_j, y, z uniformly at random from $\{0,1\}^n$.

Basic test with completeness 1

Test with access to $f : \{0,1\}^n \to \{\text{-}1,1\}$

1. Pick x_i, x_j, y, z uniformly at random from $\{0,1\}^n$.
2. Accept iff

$$f(x_i)f(x_j)(f(y) \wedge f(z)) = f(x_i + x_j + y \wedge z)$$

[Håstad & Khot 02]; too inefficient for us

Basic test with completeness 1

Test with access to $f : \{0,1\}^n \to \{\text{-}1,1\}$

1. Pick x_i, x_j, y, z uniformly at random from $\{0,1\}^n$.
2. Accept iff

$$f(x_i)f(x_j) = f(x_i + x_j + y \wedge z)$$

[Håstad 97]; imperfect completeness

Basic test with completeness 1

Test with access to $f : \{0,1\}^n \to \{\text{-}1,1\}$

1. Pick x_i, x_j, y, z uniformly at random from $\{0,1\}^n$.
2. Query $f(y)$.
3. Accept iff

$$f(x_i)f(x_j) = f(x_i + x_j + y \wedge z)$$

Basic test with completeness 1

Test with access to $f : \{0,1\}^n \to \{\text{-}1,1\}$

1. Pick x_i, x_j, y, z uniformly at random from $\{0,1\}^n$.
2. Query $f(y)$.
3. Let $w = \frac{1-f(y)}{2}$. Accept iff

$$f(x_i)f(x_j) = f(x_i + x_j + (w\vec{1} + y) \wedge z).$$

Basic test with completeness 1

Test with access to $f : \{0,1\}^n \to \{\text{-}1,1\}$

1. Pick x_i, x_j, y, z uniformly at random from $\{0,1\}^n$.
2. Query $f(y)$.
3. Let $w = \frac{1-f(y)}{2}$. Accept iff

$$f(x_i)f(x_j) = f(x_i + x_j + (w\vec{1} + y) \wedge z).$$

[GLST 98]

Running dependent iterations of basic test

- idea due to Trevisan 98

Running dependent iterations of basic test

- idea due to Trevisan 98
- Pick $x_1, \dots, x_k \in \{0,1\}^n$.

Running dependent iterations of basic test

- idea due to Trevisan 98
- Pick $x_1, \ldots, x_k \in \{0,1\}^n$.
- Consider a graph $G = ([k], E)$

Running dependent iterations of basic test

- idea due to Trevisan 98
- Pick $x_1, \ldots, x_k \in \{0,1\}^n$.
- Consider a graph $G = ([k], E)$
- Accept iff for each $(i,j) \in E$, $f(x_i)f(x_j) = f(x_i + x_j)$.

Running dependent iterations of basic test

- idea due to Trevisan 98
- Pick $x_1, \ldots, x_k \in \{0,1\}^n$.
- Consider a graph $G = ([k], E)$
- Accept iff for each $(i,j) \in E$, $f(x_i)f(x_j) = f(x_i + x_j)$.

- Upshot: reduce the number of queries, soundness decreases exponentially w.r.t. $|E|$

Running dependent iterations of basic test

- idea due to Trevisan 98
- Pick $x_1, \ldots, x_k \in \{0,1\}^n$.
- Consider a graph $G = ([k], E)$
- Accept iff for each $(i,j) \in E$, $f(x_i)f(x_j) = f(x_i + x_j)$.

- Upshot: reduce the number of queries, soundness decreases exponentially w.r.t. $|E|$
- We will use a complete hypergraph following [ST06]

Design of a hypergraph dictatorship test

Consider a hypergraph $H = ([k], E)$.

Design of a hypergraph dictatorship test

Consider a hypergraph $H = ([k], E)$.

H-Test, with access to $f : \{0,1\}^n \rightarrow \{\text{-}1, 1\}$

Design of a hypergraph dictatorship test

H-Test, with access to $f : \{0,1\}^n \to \{\text{-}1,1\}$

1. Pick $\{x_i\}_{i \in [k]}$ uniformly at random from $\{0,1\}^n$.
2. $$\prod_{i \in e} [f(x_i)] = f\left(\sum_{i \in e} x_i\right).$$

Design of a hypergraph dictatorship test

H-Test, with access to $f : \{0,1\}^n \to \{\text{-}1, 1\}$

1. Pick $\{x_i\}_{i \in [k]}$ uniformly at random from $\{0,1\}^n$.
2. $$\prod_{i \in e} [f(x_i)] = f\left(\sum_{i \in e} x_i\right).$$

accepts large parities, $f(x) = (-1)^{x_1 + \ldots + x_n}$

Design of a hypergraph dictatorship test

H-Test, with access to $f : \{0,1\}^n \to \{\text{-}1,1\}$

1. Pick $\{x_i\}_{i\in[k]}$ uniformly at random from $\{0,1\}^n$.
2. Pick $\rho > 0$. Pick $\{z_a\}_{a\in[k]\cup[E]}$ such that each bit of z_a is 1 w.p. ρ.
3. $$\prod_{i\in e}[f(x_i+z_i)] = f\left(\sum_{i\in e} x_i + z_e\right).$$

Design of a hypergraph dictatorship test

H-Test, with access to $f : \{0,1\}^n \to \{\text{-}1,1\}$

1. Pick $\{x_i\}_{i\in[k]}$ uniformly at random from $\{0,1\}^n$.
2. Pick $\rho > 0$. Pick $\{z_a\}_{a\in[k]\cup[E]}$ such that each bit of z_a is 1 w.p. ρ.
3. $$\prod_{i\in e}\left[f(x_i+z_i)\right] = f\left(\sum_{i\in e} x_i + z_e\right).$$

[ST06] test; has imperfect completeness

Design of a hypergraph dictatorship test

H-Test, with access to $f : \{0,1\}^n \to \{\text{-}1, 1\}$

1. Pick $\{x_i\}_{i \in [k]}$ uniformly at random from $\{0,1\}^n$.
2. Pick $\{y_i\}_{i \in [k]}$ uniformly at random from $\{0,1\}^n$.
3. Pick $\rho > 0$. Pick $\{z_a\}_{a \in [k] \cup [E]}$ such that each bit of z_a is 1 w.p. ρ.
4. For each $i \in [k]$, query $f(y_i)$.
5. Accept iff for $e \in E$,

$$\prod_{i \in e} [f(x_i + z_i)] = f\left(\sum_{i \in e} x_i + z_e\right).$$

Design of a hypergraph dictatorship test

H-Test, with access to $f : \{0,1\}^n \to \{\text{-}1,1\}$

1. Pick $\{x_i\}_{i\in[k]}$ uniformly at random from $\{0,1\}^n$.
2. Pick $\{y_i\}_{i\in[k]}$ uniformly at random from $\{0,1\}^n$.
3. Pick $\rho > 0$. Pick $\{z_a\}_{a\in[k]\cup[E]}$ such that each bit of z_a is 1 w.p. ρ.
4. For each $i \in [k]$, query $f(y_i)$.
5. Let $w_i = \frac{1-f(y_i)}{2}$. Accept iff for $e \in E$,

$$\prod_{i\in e} [f(x_i + z_i)] = f\left(\sum_{i\in e} x_i + z_e\right).$$

Design of a hypergraph dictatorship test

H-Test, with access to $f : \{0,1\}^n \to \{\text{-}1,1\}$

1. Pick $\{x_i\}_{i\in[k]}$ uniformly at random from $\{0,1\}^n$.
2. Pick $\{y_i\}_{i\in[k]}$ uniformly at random from $\{0,1\}^n$.
3. Pick $\rho > 0$. Pick $\{z_a\}_{a\in[k]\cup[E]}$ such that each bit of z_a is 1 w.p. ρ.
4. For each $i \in [k]$, query $f(y_i)$.
5. Let $w_i = \frac{1-f(y_i)}{2}$. Accept iff for $e \in E$,

$$\prod_{i\in e}\left[f(x_i + (w_i\vec{1} + y_i) \wedge z_i)\right] =$$

$$f\left(\sum_{i\in e} x_i + \left(\sum_{i\in e}(w_i\vec{1} + y_i)\right) \wedge z_e\right).$$

Analysis of hypergraph dictatorship test

- Use a complete hypergraph on k vertices.

Analysis of hypergraph dictatorship test

- Use a complete hypergraph on k vertices.
- Suppose $f \in \mathcal{NO}$, i.e., for all $i \in [n]$, $\mathrm{I}_i(T_\rho(f)) = o(1)$.

Analysis of hypergraph dictatorship test

- Use a complete hypergraph on k vertices.
- Suppose $f \in \mathcal{NO}$, i.e., for all $i \in [n]$, $\mathrm{I}_i(T_\rho(f)) = o(1)$.
- Goal: Show prob. of acceptance is $q^3 \cdot 2^{-q} + o(1)$.

Analysis of hypergraph dictatorship test

- Use a complete hypergraph on k vertices.
- Suppose $f \in \mathcal{NO}$, i.e., for all $i \in [n]$, $\mathrm{I}_i(T_\rho(f)) = o(1)$.
- Goal: Show prob. of acceptance is $q^3 \cdot 2^{-q} + o(1)$.

"Extension" Φ_ρ

For every $f : \{0,1\}^n \to \{\text{-}1, 1\}$, define $\Phi_\rho(f) : \{0,1\}^{2n} \to [-1, 1]$ to be

$$\Phi_\rho(f)(x, y) = \mathop{\mathbb{E}}_{z \in \mathcal{D}_\rho} f(x + y \wedge z)$$

Analysis continued

- for $i \in [n]$, $\mathrm{I}_i(T_\rho(f)) \approx \mathrm{I}_i(\Phi_\rho(f))$.

Analysis continued

- for $i \in [n]$, $\mathrm{I}_i(T_\rho(f)) \approx \mathrm{I}_i(\Phi_\rho(f))$.
- Since $f \in \mathcal{NO}$, we conclude for each $i \in [n]$, $\mathrm{I}_i(\Phi_\rho(f)) = o(1)$.

Analysis continued

- for $i \in [n]$, $\mathrm{I}_i(T_\rho(f)) \approx \mathrm{I}_i(\Phi_\rho(f))$.
- Since $f \in \mathcal{NO}$, we conclude for each $i \in [n]$, $\mathrm{I}_i(\Phi_\rho(f)) = o(1)$.
- By ST Lemma, $\|\Phi_\rho(f)\|_{U_d} = o(1)$ for all fixed d.

Analysis continued

- for $i \in [n]$, $\mathrm{I}_i(T_\rho(f)) \approx \mathrm{I}_i(\Phi_\rho(f))$.
- Since $f \in \mathcal{NO}$, we conclude for each $i \in [n]$, $\mathrm{I}_i(\Phi_\rho(f)) = o(1)$.
- By ST Lemma, $\|\Phi_\rho(f)\|_{U_d} = o(1)$ for all fixed d.
- Arithmetize the prob. of acceptance p to show that

$$p \leq q^3 \cdot 2^{-q} + \Pr[k\text{-deg AKKLR test accepts } \Phi_\rho(f)]$$

Analysis continued

- for $i \in [n]$, $\mathrm{I}_i(T_\rho(f)) \approx \mathrm{I}_i(\Phi_\rho(f))$.
- Since $f \in \mathcal{NO}$, we conclude for each $i \in [n]$, $\mathrm{I}_i(\Phi_\rho(f)) = o(1)$.
- By ST Lemma, $\|\Phi_\rho(f)\|_{U_d} = o(1)$ for all fixed d.
- Arithmetize the prob. of acceptance p to show that

$$p \leq q^3 \cdot 2^{-q} + \Pr[k\text{-deg AKKLR test accepts } \Phi_\rho(f)]$$

- By generalized von-Neumann,

$$\Pr[k\text{-deg AKKLR test accepts } \Phi_\rho(f)] \leq \|\Phi_\rho(f)\|_{U_{k+1}}$$

Outline

M-free test

Let M be an r by k matrix over $\{0, 1\}$.

M-free test

Let M be an r by k matrix over $\{0, 1\}$.

M-free test

Let M be an r by k matrix over $\{0,1\}$.

M-free test, with access to f:

1. Pick $\vec{x} = x_1, \ldots, x_k$ uniformly from $\{0,1\}^n$ such that $M\vec{x} = 0$.
2. Reject iff $f(x_1), \ldots, f(x_k) = 1$.

M-free test

Let M be an r by k matrix over $\{0,1\}$.

M-free test, with access to f:

1. Pick $\vec{x} = x_1, \ldots, x_k$ uniformly from $\{0,1\}^n$ such that $M\vec{x} = 0$.
2. Reject iff $f(x_1), \ldots, f(x_k) = 1$.

If f is M-free, test always accepts.

Green's regularity lemma

- a function f is ϵ-pseudorandom if $\|f - \mathbb{E} f\|_{U_2} \leq \epsilon$

Green's regularity lemma

- a function f is ϵ-pseudorandom if $\|f - \mathbb{E}\, f\|_{U_2} \leq \epsilon$
- a collection of functions is ϵ-pseudorandom if all but at most ϵ-fraction of the functions are ϵ-pseudorandom

Green's regularity lemma

- a function f is ϵ-pseudorandom if $\|f - \mathbb{E} f\|_{U_2} \leq \epsilon$
- a collection of functions is ϵ-pseudorandom if all but at most ϵ-fraction of the functions are ϵ-pseudorandom
- Extension $\Phi(f)$: sends f into a collection of functions $\{f_{g+H}\}_{g \in \{0,1\}^n}$.

Green's regularity lemma

- a function f is ϵ-pseudorandom if $\|f - \mathbb{E} f\|_{U_2} \leq \epsilon$
- a collection of functions is ϵ-pseudorandom if all but at most ϵ-fraction of the functions are ϵ-pseudorandom
- Extension $\Phi(f)$: sends f into a collection of functions $\{f_{g+H}\}_{g \in \{0,1\}^n}$. where

  H is a subspace of $\{0,1\}^n$

  f_{g+H} is the restriction of f to the affine subspace $g + H$

Green's regularity lemma

- a function f is ϵ-pseudorandom if $\|f - \mathbb{E} f\|_{U_2} \leq \epsilon$
- a collection of functions is ϵ-pseudorandom if all but at most ϵ-fraction of the functions are ϵ-pseudorandom
- Extension $\Phi(f)$: sends f into a collection of functions $\{f_{g+H}\}_{g \in \{0,1\}^n}$.

Green's regularity lemma

- a function f is ϵ-pseudorandom if $\|f - \mathbb{E} f\|_{U_2} \leq \epsilon$
- a collection of functions is ϵ-pseudorandom if all but at most ϵ-fraction of the functions are ϵ-pseudorandom
- Extension $\Phi(f)$: sends f into a collection of functions $\{f_{g+H}\}_{g \in \{0,1\}^n}$.

Theorem (Green)

Let $\epsilon > 0$, $f : \{0,1\}^n \to \{0,1\}$.

Green's regularity lemma

- a function f is ϵ-pseudorandom if $\|f - \mathbb{E} f\|_{U_2} \leq \epsilon$
- a collection of functions is ϵ-pseudorandom if all but at most ϵ-fraction of the functions are ϵ-pseudorandom
- Extension $\Phi(f)$: sends f into a collection of functions $\{f_{g+H}\}_{g \in \{0,1\}^n}$.

Theorem (Green)

Let $\epsilon > 0$, $f : \{0,1\}^n \to \{0,1\}$.
There exists a subspace H of constant co-dimension such that $\Phi(f) = \{f_{g+H}\}$ is ϵ-pseudorandom.

Analysis of graph-free test

- Suppose f is ϵ-far from M-free.

Analysis of graph-free test

- Suppose f is ϵ-far from M-free.
- Apply Φ from regularity lemma to obtain $\{f_{g+H}\}$.

Analysis of graph-free test

- Suppose f is ϵ-far from M-free.
- Apply Φ from regularity lemma to obtain $\{f_{g+H}\}$.
- Define the following reduced function f^R:

Analysis of graph-free test

- Suppose f is ϵ-far from M-free.
- Apply Φ from regularity lemma to obtain $\{f_{g+H}\}$.
- Define the following reduced function f^R:

For each $g \in \{0,1\}^n$,

Analysis of graph-free test

- Suppose f is ϵ-far from M-free.
- Apply Φ from regularity lemma to obtain $\{f_{g+H}\}$.
- Define the following reduced function f^R:

For each $g \in \{0,1\}^n$,

1. if f_{g+H} is not $\ll \epsilon$-pseudorandom or has density $\ll \epsilon$,

Analysis of graph-free test

- Suppose f is ϵ-far from M-free.
- Apply Φ from regularity lemma to obtain $\{f_{g+H}\}$.
- Define the following reduced function f^R:

For each $g \in \{0,1\}^n$,

1. if f_{g+H} is not $\ll \epsilon$-pseudorandom or has density $\ll \epsilon$, set $f^R_{g+H} = 0$.

Analysis of graph-free test

- Suppose f is ϵ-far from M-free.
- Apply Φ from regularity lemma to obtain $\{f_{g+H}\}$.
- Define the following reduced function f^R:

For each $g \in \{0,1\}^n$,

1. if f_{g+H} is not $\ll \epsilon$-pseudorandom or has density $\ll \epsilon$,
   set $f^R_{g+H} = 0$.
2. Else, set $f^R_{g+H} = f_{g+H}$.

Analysis (page 2)

- Since $\delta(f, f^R) \leq \epsilon$, there exist $x_1, \ldots, x_k$ such that $f^R(x_1), \ldots, f^R(x_k) = 1$.

Analysis (page 2)

- Since $\delta(f, f^R) \leq \epsilon$, f^R has a M-pattern.

Analysis (page 2)

- Since $\delta(f, f^R) \leq \epsilon$, f^R has a M-pattern.
- By construction of f^R, each f_{x_i+H} is dense and pseudorandom

Analysis (page 2)

- Since $\delta(f, f^R) \le \epsilon$, f^R has a M-pattern.
- By construction of f^R, each f_{x_i+H} is dense and pseudorandom

Analysis (page 2)

- Since $\delta(f, f^R) \leq \epsilon$, f^R has a M-pattern.
- By construction of f^R, each f_{x_i+H} is dense and pseudorandom

Observation

If M is graphic, then the rows of M form a complexity 1 system of linear forms.

Analysis (page 2)

- Since $\delta(f, f^R) \leq \epsilon$, f^R has a M-pattern.
- By construction of f^R, each f_{x_i+H} is dense and pseudorandom

Observation

If M is graphic, then the rows of M form a complexity 1 system of linear forms.

- Count the fraction of M-patterns across the functions f_{x_i+H}.

Analysis (page 2)

- Since $\delta(f, f^R) \leq \epsilon$, f^R has a M-pattern.
- By construction of f^R, each f_{x_i+H} is dense and pseudorandom

Observation

If M is graphic, then the rows of M form a complexity 1 system of linear forms.

- Count the fraction of M-patterns across the functions f_{x_i+H}.
- By generalized von-Neumann, this is $\approx$ the expected number of M patterns in a random function,

Analysis (page 2)

- Since $\delta(f, f^R) \leq \epsilon$, f^R has a M-pattern.
- By construction of f^R, each f_{x_i+H} is dense and pseudorandom

Observation

If M is graphic, then the rows of M form a complexity 1 system of linear forms.

- Count the fraction of M-patterns across the functions f_{x_i+H}.
- By generalized von-Neumann, this is $\approx$ the expected number of M patterns in a random function, which is > 0

Analysis (page 2)

- Since $\delta(f, f^R) \leq \epsilon$, f^R has a M-pattern.
- By construction of f^R, each f_{x_i+H} is dense and pseudorandom

Observation

If M is graphic, then the rows of M form a complexity 1 system of linear forms.

- Count the fraction of M-patterns across the functions f_{x_i+H}.
- By generalized von-Neumann, this is $\approx$ the expected number of M patterns in a random function, which is > 0
- Since H has constant co-dimension, test rejects with positive probability.

Future direction

Open question:

- a q-query PCP with completeness 1, soundness $\mathrm{poly}(q) \cdot 2^{-q}$?

Future direction

Open question:

- a q-query PCP with completeness 1, soundness $\mathrm{poly}(q) \cdot 2^{-q}$?
- an analytic proof of Green's conjecture

Future direction

Open question:

- a q-query PCP with completeness 1, soundness $\mathrm{poly}(q) \cdot 2^{-q}$?
- an analytic proof of Green's conjecture

  decomposition theorem $\rightarrow$ hypergraph $\rightarrow$ testability

Future direction

Open question:

- a q-query PCP with completeness 1, soundness $\mathrm{poly}(q) \cdot 2^{-q}$?
- an analytic proof of Green's conjecture

  decomposition theorem $\longrightarrow$ hypergraph $\longrightarrow$ testability
- prove some form of inverse for Gowers norm

  a low-degree polynomial test with soundness $\frac{1}{2}$.