A Characterization of Locally Testable Affine-Invariant Properties via Decomposition Theorems

Yuichi Yoshida

National Institute of Informatics and Preferred Infrastructure, Inc

June 9, 2014

Property Testing

Definition

$f : \{0,1\}^n \to \{0,1\}$ is *ϵ-far* from $\mathcal{P}$ if, for any $g : \{0,1\}^n \to \{0,1\}$ satisfying $\mathcal{P}$,

$$\Pr_x[f(x) \neq g(x)] \geq \epsilon.$$

Property Testing

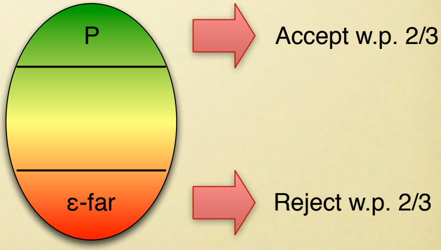
Definition

$f : \{0,1\}^n \to \{0,1\}$ is *ϵ-far* from $\mathcal{P}$ if, for any $g : \{0,1\}^n \to \{0,1\}$ satisfying $\mathcal{P}$,

$$\Pr_x[f(x) \neq g(x)] \geq \epsilon.$$

ϵ-tester for a property $\mathcal{P}$:

- Given $f : \{0,1\}^n \to \{0,1\}$ as a query access.
- Proximity parameter $\epsilon > 0$.



Local Testability

Definition

$\mathcal{P}$ is *locally testable* if, for any $\epsilon > 0$, there is an ϵ-tester with query complexity that only depends on ϵ.

Examples of locally testable properties:

- Linearity: $O(1/\epsilon)$ [BLR93]
- d-degree Polynomials: $O(2^d + 1/\epsilon)$ [AKK$^+$05, BKS$^+$10]
- Fourier sparsity [GOS$^+$11]
- Odd-cycle-freeness: $O(1/\epsilon^2)$ [BGRS12]
  $\nexists$ odd k and $x_1, \ldots, x_k$ such that $\sum_i x_i = 0$, $f(x_i) = 1$ for all i.
- k-Juntas: $O(k/\epsilon + k \log k)$ [FKR$^+$04, Bla09].

Affine-Invariant Properties

Definition

$\mathcal{P}$ is *affine-invariant* if a function $f : \mathbb{F}_2^n \to \{0, 1\}$ satisfies $\mathcal{P}$, then $f \circ A$ satisfies $\mathcal{P}$ for any bijective affine transformation $A : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

Examples: Linearity, low-degree polynomials, Fourier sparsity, odd-cycle-freeness.

Affine-Invariant Properties

Definition

$\mathcal{P}$ is *affine-invariant* if a function $f : \mathbb{F}_2^n \to \{0, 1\}$ satisfies $\mathcal{P}$, then $f \circ A$ satisfies $\mathcal{P}$ for any bijective affine transformation $A : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

Examples: Linearity, low-degree polynomials, Fourier sparsity, odd-cycle-freeness.

Q. Characterization of locally testable affine-invariant properties? [KS08]

Related Work

- Locally testable with one-sided error $\Leftrightarrow$ affine-subspace hereditary? [BGS10]
  Ex. Linearity, low-degree polynomials, odd-cycle-freeness.
  - $\Rightarrow$ is true. [BGS10]
  - $\Leftarrow$ is true (if the property has bounded complexity). [BFH$^+$13].

Related Work

- Locally testable with one-sided error $\Leftrightarrow$ affine-subspace hereditary? [BGS10]
  Ex. Linearity, low-degree polynomials, odd-cycle-freeness.
  - $\Rightarrow$ is true. [BGS10]
  - $\Leftarrow$ is true (if the property has bounded complexity). [BFH$^+$13].
- $\mathcal{P}$ is locally testable $\Rightarrow$ distance to $\mathcal{P}$ is estimable. [HL13]

Related Work

- Locally testable with one-sided error $\Leftrightarrow$ affine-subspace hereditary? [BGS10]
  Ex. Linearity, low-degree polynomials, odd-cycle-freeness.
  - $\Rightarrow$ is true. [BGS10]
  - $\Leftarrow$ is true (if the property has bounded complexity). [BFH$^+$13].
- $\mathcal{P}$ is locally testable $\Rightarrow$ distance to $\mathcal{P}$ is estimable. [HL13]
- $\mathcal{P}$ is locally testable $\Leftrightarrow$ regular-reducible. [This work]

Graph Property Testing

Definition

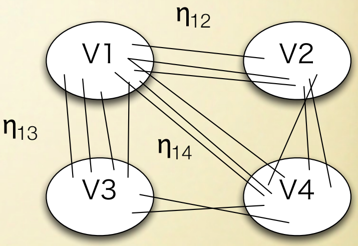
A graph $G = (V, E)$ is *ϵ-far* from a property $\mathcal{P}$ if we must add or remove at least $\epsilon|V|^2$ edges to make G satisfy $\mathcal{P}$.

Examples of locally testable properties:

- 3-Colorability [GGR98]
- H-freeness [AFKS00]
- Monotone properties [AS08b]
- Hereditary properties [AS08a]

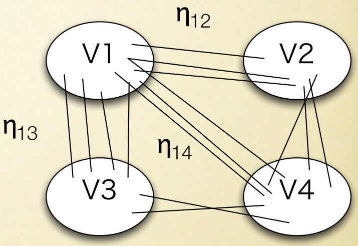
A Characterization of Locally Testable Graph Properties

Szemerédi's regularity lemma:
Every graph can be partitioned into a constant number of parts so that each pair of parts looks random.



A Characterization of Locally Testable Graph Properties

Szemerédi's regularity lemma:
Every graph can be partitioned into a constant number of parts so that each pair of parts looks random.

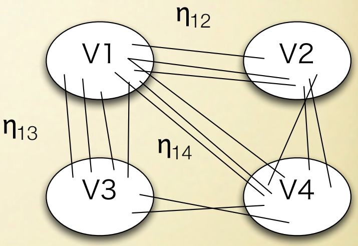


Theorem ([AFNS09])

A graph property $\mathcal{P}$ is locally testable
$\Leftrightarrow$ *whether $\mathcal{P}$ holds is determined only by the set of densities $\{\eta_{ij}\}_{i,j}$.*

A Characterization of Locally Testable Graph Properties

Szemerédi's regularity lemma:
Every graph can be partitioned into a constant number of parts so that each pair of parts looks random.



Theorem ([AFNS09])

A graph property $\mathcal{P}$ is locally testable
$\Leftrightarrow$ *whether $\mathcal{P}$ holds is determined only by the set of densities $\{\eta_{ij}\}_{i,j}$.*

Q. How can we extract such constant-size sketches from functions?

Constant Sketch for Functions

Theorem (Decomposition Theorem [BFH+13])

For any $\gamma > 0$, $d \geq 1$, and $r : \mathbb{N} \to \mathbb{N}$, there exists $\overline{C}$ such that: any function $f : \mathbb{F}_2^n \to \{0,1\}$ can be decomposed as $f = f' + f''$, where

Constant Sketch for Functions

Theorem (Decomposition Theorem [BFH+13])

For any $\gamma > 0$, $d \geq 1$, and $r : \mathbb{N} \to \mathbb{N}$, there exists $\overline{C}$ such that: any function $f : \mathbb{F}_2^n \to \{0,1\}$ can be decomposed as $f = f' + f''$, where

- *a **structured part** $f' : \mathbb{F}_2^n \to [0,1]$, where*
  - *$f' = \Gamma(P_1, \ldots, P_C)$ with $C \leq \overline{C}$,*
  - *$P_1, \ldots, P_C$ are "non-classical" polynomials of degree $< d$ and rank $\geq r(C)$.*
  - *$\Gamma : \mathbb{T}^C \to [0,1]$ is a function.*

Constant Sketch for Functions

Theorem (Decomposition Theorem [BFH+13])

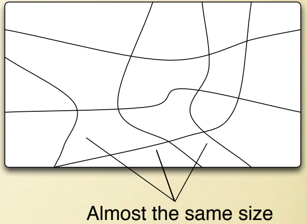
For any $\gamma > 0$, $d \geq 1$, and $r : \mathbb{N} \to \mathbb{N}$, there exists $\overline{C}$ such that: any function $f : \mathbb{F}_2^n \to \{0,1\}$ can be decomposed as $f = f' + f''$, where

- *a* ***structured part*** *$f' : \mathbb{F}_2^n \to [0,1]$, where*
  - *$f' = \Gamma(P_1, \ldots, P_C)$ with $C \leq \overline{C}$,*
  - *$P_1, \ldots, P_C$ are "non-classical" polynomials of degree $< d$ and rank $\geq r(C)$.*
  - *$\Gamma : \mathbb{T}^C \to [0,1]$ is a function.*
- *a* ***pseudo-random part*** *$f'' : \mathbb{F}_2^n \to [-1,1]$*
  - *The Gowers norm $\|f''\|_{U^d}$ is at most γ.*

Factors

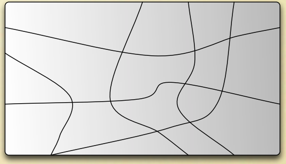
Polynomial sequence $(P_1, \ldots, P_C)$ partitions $\mathbb{F}_2^n$ into atoms $\{x \mid P_1(x) = b_1, \ldots, P_C(x) = b_C\}$.

$\mathbb{F}_2^n =$



The decomposition theorem says:

$f =$



$+\Upsilon$

$\Gamma(P_1, \ldots, P_C)$

What is the Gowers Norm?

Definition

Let $f : \mathbb{F}_2^n \to \mathbb{C}$. The *Gowers norm of order d* for f is

$$\|f\|_{U^d} := \left(\mathop{\mathbf{E}}_{x,y_1,\ldots,y_d} \prod_{I \subseteq \{1,\ldots,d\}} J^{|I|} f(x + \sum_{i \in I} y_i) \right)^{1/2^d},$$

where J denotes complex conjugation.

- $\|f\|_{U^1} = |\mathbf{E}_x f(x)|$
- $\|f\|_{U^1} \leq \|f\|_{U^2} \leq \|f\|_{U^3} \leq \cdots$
- $\|f\|_{U^d}$ measures correlation with polynomials of degree $< d$.

Correlation with Polynomials of Degree $< d$

Proposition

For any polynomial $P : \mathbb{F}_2^n \to \{0,1\}$ of degree $< d$, $\|(-1)^P\|_{U^d} = 1$.

Correlation with Polynomials of Degree $< d$

Proposition

For any polynomial $P : \mathbb{F}_2^n \to \{0,1\}$ of degree $< d$, $\|(-1)^P\|_{U^d} = 1$.

However, the converse does not hold when $d \geq 4$...

Correlation with Polynomials of Degree $< d$

Proposition

For any polynomial $P : \mathbb{F}_2^n \to \{0,1\}$ *of degree* $< d$, $\|(-1)^P\|_{U^d} = 1$.

However, the converse does not hold when $d \geq 4$...

Definition

$P : \mathbb{F}_2^n \to \mathbb{T}$ is a *non-classical polynomial of degree* $< d$ if $\|\exp(2\pi i \cdot f)\|_{U^d} = 1$.

It turns out that the range of P is $\mathbb{U}_{k+1} := \{0, \frac{1}{2^{k+1}}, \ldots, \frac{2^{k+1}-1}{2^{k+1}}\}$ for some k (= *depth*).

Is This Really a Constant-size Sketch?

- Structured part: $f' = \Gamma(P_1, \ldots, P_C)$.
- Γ indeed has a constant-size representation, but $P_1, \ldots, P_C$ may not have (even if we just want to specify the coset $\{P \circ A\}$).
- The rank of $(P_1, \ldots, P_C)$ is high
  $\Rightarrow$ Their degrees and depths determine almost everything.
  Ex. the distribution of the restriction of f to a random affine subspace.

Regularity-Instance

Formalize "f has some specific structured part".

Definition

A *regularity-instance* I is a tuple of

- an error parameter $\gamma > 0$,
- a structure function $\Gamma : \prod_{i=1}^{C} \mathbb{U}_{h_i+1} \to [0,1]$,
- a complexity parameter $C \in \mathbb{N}$,
- a degree-bound parameter $d \in \mathbb{N}$,
- a degree parameter $\mathbf{d} = (d_1, \ldots, d_C) \in \mathbb{N}^C$ with $d_i < d$,
- a depth parameter $\mathbf{h} = (h_1, \ldots, h_C) \in \mathbb{N}^C$ with $h_i < \frac{d_i}{p-1}$, and
- a rank parameter $r \in \mathbb{N}$.

Satisfying a Regularity-Instance

Definition

Let $I = (\gamma, \Gamma, C, d, \mathbf{d}, \mathbf{h}, r)$ be a regularity-instance.
f *satisfies I* if it is of the form

$$f(x) = \Gamma(P_1(x), \ldots, P_C(x)) + \Upsilon(x),$$

where

- P_i is a polynomial of degree d_i and depth h_i,
- $(P_1, \ldots, P_C)$ has rank at least r,
- $\|\Upsilon\|_{U^d} \leq \gamma$.

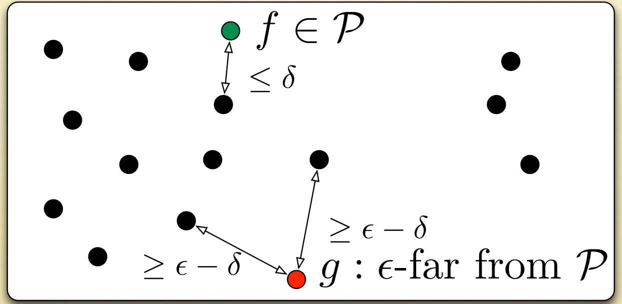
Testing the Property of Satisfying a Regularity-Instance

Theorem

Let $\epsilon > 0$ and $I = (\gamma, \Gamma, C, d, \mathbf{d}, \mathbf{h}, r)$ be a regularity-instance with $r \geq r(\epsilon, \gamma, C, d)$. Then, there is an ϵ-tester for the property of satisfying I with a constant number of queries.

Regular-Reducibility

A property $\mathcal{P}$ is *regular-reducible* if for any $\delta > 0$, there exists a set $\mathcal{R}$ of constant number of high-rank regularity-instances with constant parameters such that:



Our Characterization

Theorem

An affine-invariant property $\mathcal{P}$ is locally testable

$$\Updownarrow$$

$\mathcal{P}$ is regular-reducible.

Proof Sketch

- Regular-reducible $\Rightarrow$ Locally testable
  Combining the testability of regularity-instances and [HL13], we can estimate the distance to $\mathcal{R}$.
- Locally testable $\Rightarrow$ Regular-reducible
  The behavior of a tester depends only on the distribution of the restriction to a random affine subspace. Since Γ, $\mathbf{d}$, and $\mathbf{h}$ determines the distribution, we can find $\mathcal{R}$ using the tester.

Testability of the Property of Satisfying a Regularity-Instance

Input: $f : \mathbb{F}_2^n \to \{0,1\}$, $I = (\gamma, \Gamma, C, d, \mathbf{d}, \mathbf{h}, r)$, and $\epsilon > 0$.

1: Set δ small enough and m large enough.
2: Take a random affine embedding $A : \mathbb{F}_2^m \to \mathbb{F}_2^n$.
3: **if** $f \circ A$ is δ-close to satisfying I **then** accept.
4: **else** reject.

Testability of the Property of Satisfying a Regularity-Instance

Input: $f : \mathbb{F}_2^n \to \{0,1\}$, $I = (\gamma, \Gamma, C, d, \mathbf{d}, \mathbf{h}, r)$, and $\epsilon > 0$.

1: Set δ small enough and m large enough.
2: Take a random affine embedding $A : \mathbb{F}_2^m \to \mathbb{F}_2^n$.
3: **if** $f \circ A$ is δ-close to satisfying I **then** accept.
4: **else** reject.

Q. If f satisfies I, $f \circ A$ is close to I?
Q. If f is far from I, $f \circ A$ is far from I?

If f satisfies I

- $f(x) = \Gamma(\mathbf{P}(x)) + \Upsilon(x)$ with $\|\Upsilon(x)\|_{U^d} \leq \gamma$.
- $f(Ax)$ almost satisfies I:
  - $f(Ax) = \Gamma(\mathbf{P}(Ax)) + \Upsilon(Ax)$ with $\|\Upsilon(Ax)\|_{U^d} \leq \gamma + o(\gamma)$.
  - $\mathbf{P}(Ax)$ meets the requirement of I.
- By perturbing $f(Ax)$ up to δ-fraction, we obtain a function satisfying I.

If f is ϵ-far from I

We will show that "$f \circ A$ is δ-close to I" implies "f is ϵ-close to I."

- δ-close: $f(Ax) \approx \Gamma(\mathbf{P}'(x))$.
- Decomposition: $f(x) \approx \Sigma(\mathbf{R}(x))$.
  $\Rightarrow f(Ax) \approx \Sigma(\mathbf{R}'(x))$, where $\mathbf{R}' = \mathbf{R} \circ A$.

If f is ϵ-far from I

We will show that "$f \circ A$ is δ-close to I" implies "f is ϵ-close to I."

- δ-close: $f(Ax) \approx \Gamma(\mathbf{P}'(x))$.
- Decomposition: $f(x) \approx \Sigma(\mathbf{R}(x))$.
  $\Rightarrow f(Ax) \approx \Sigma(\mathbf{R}'(x))$, where $\mathbf{R}' = \mathbf{R} \circ A$.

$$\Sigma(\mathbf{R}'(x)) \approx \Gamma(\mathbf{P}'(x)).$$

If f is ϵ-far from I

We will show that "$f \circ A$ is δ-close to I" implies "f is ϵ-close to I."

- δ-close: $f(Ax) \approx \Gamma(\mathbf{P}'(x))$.
- Decomposition: $f(x) \approx \Sigma(\mathbf{R}(x))$.
  $\Rightarrow f(Ax) \approx \Sigma(\mathbf{R}'(x))$, where $\mathbf{R}' = \mathbf{R} \circ A$.

$$\Sigma(\mathbf{R}'(x)) \approx \Gamma(\mathbf{P}'(x)).$$

We can find an extension $\overline{\mathbf{R}'}$ of $\mathbf{R}'$ (of high rank) such that:

$$P_i = \Gamma_i(\overline{\mathbf{R}'}(x)) \text{ for some } \Gamma_i.$$

$$\Rightarrow \Sigma(\mathbf{R}'(x)) \approx \Gamma(\Gamma_1(\overline{\mathbf{R}'}(x)), \ldots, \Gamma_C(\overline{\mathbf{R}'}(x))).$$

If f is ϵ-far from I

Lemma

The identity holds for every value in the range of $\overline{\mathbf{R}'}$.

If f is ϵ-far from I

Lemma

The identity holds for every value in the range of $\overline{\mathbf{R}'}$.

We can replace $\overline{\mathbf{R}'}$ (on m variables) by a polynomial sequence $\overline{\mathbf{R}}$ on n variables such that $\overline{\mathbf{R}} \circ A = \overline{\mathbf{R}'}$.
$\Rightarrow f(x) \approx \Sigma(\mathbf{R}(x)) \approx \Gamma(\Gamma_1(\overline{\mathbf{R}}(x)), \ldots, \Gamma_C(\overline{\mathbf{R}}(x))) := \Gamma(\mathbf{P}(x))$.

If f is ϵ-far from I

Lemma

The identity holds for every value in the range of $\overline{\mathbf{R}'}$.

We can replace $\overline{\mathbf{R}'}$ (on m variables) by a polynomial sequence $\overline{\mathbf{R}}$ on n variables such that $\overline{\mathbf{R}} \circ A = \overline{\mathbf{R}'}$.

$\Rightarrow f(x) \approx \Sigma(\mathbf{R}(x)) \approx \Gamma(\Gamma_1(\overline{\mathbf{R}}(x)), \ldots, \Gamma_C(\overline{\mathbf{R}}(x))) := \Gamma(\mathbf{P}(x))$.

Lemma

With high probability $\mathbf{P}(x)$ is consistent with I.

$\Rightarrow$ f is ϵ-close to satisfying I.

$\Rightarrow$ Contradiction.

Conclusions

- Easily extendable to $\mathbb{F}_p$ for a prime p.
- Query complexity is actually unknown due to the Gowers inverse theorem. Other parts involve Ackermann-like functions.

Conclusions

- Easily extendable to $\mathbb{F}_p$ for a prime p.
- Query complexity is actually unknown due to the Gowers inverse theorem. Other parts involve Ackermann-like functions.
  $\Rightarrow$ Obtaining a tower-like function is a big improvement!

Open Problems

- Characterization based on function (ultra)limits?
- locally testable with one-sided error $\Leftrightarrow$ affine-subspace hereditary? [BFH+13]
- Characterization of linear-invariant properties?
- Study other groups?
  - Abelian $\Rightarrow$ higher order Fourier analysis developed [Sze12].
  - Non-Abelian $\Rightarrow$ representation theory?
- Why is affine invariance easier to deal with than permutation invariance?