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

Yuichi Yoshida
National Institute of Informatics and Preferred Infrastructure, Inc

November 29, 2013
Property Testing

**Definition**

\( f : \{0, 1\}^n \rightarrow \{0, 1\} \) is \( \epsilon \)-far from \( \mathcal{P} \) if, for any \( g : \{0, 1\}^n \rightarrow \{0, 1\} \) satisfying \( \mathcal{P} \),

\[
\Pr_{x}[f(x) \neq g(x)] \geq \epsilon.
\]
Property Testing

Definition

\[ f : \{0, 1\}^n \to \{0, 1\} \] is \( \varepsilon \)-far from \( \mathcal{P} \) if, for any \( g : \{0, 1\}^n \to \{0, 1\} \) satisfying \( \mathcal{P} \),

\[ \Pr_{x}[f(x) \neq g(x)] \geq \varepsilon. \]

\( \varepsilon \)-tester for a property \( \mathcal{P} \):

- Given \( f : \{0, 1\}^n \to \{0, 1\} \) as a query access.
- Proximity parameter \( \varepsilon > 0 \).
Local Testability

**Definition**

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

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]
  \[ \forall \text{ odd } k \text{ and } x_1, \ldots, x_k \text{ such that } \sum_i x_i = 0, f(x_i) = 1 \text{ for all } i. \]
- $k$-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 ⇔ affine-subspace hereditary? [BGS10]
  
  **Ex.** Linearity, low-degree polynomials, odd-cycle-freeness.
  - ⇒ is true. [BGS10]
  - ⇐ is true (if the property has bounded complexity). [BFH+13].
Related Work

- Locally testable with one-sided error $\Leftrightarrow$ affine-subspace hereditary? \cite{BGS10}

  *Example.* Linearity, low-degree polynomials, odd-cycle-freeness.
  - $\Rightarrow$ is true. \cite{BGS10}
  - $\Leftarrow$ is true (if the property has bounded complexity). \cite{BFH+13}.

- $\mathcal{P}$ is locally testable $\Rightarrow$ distance to $\mathcal{P}$ is estimable. \cite{HL13}
Related Work

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

Definition

A graph \( G = (V, E) \) is \( \epsilon \)-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]
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 $\iff$ 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 $\iff$ 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?
Theorem (Decomposition Theorem [BFH+13])

For any $\gamma > 0$, $d \geq 1$, and $r : \mathbb{N} \rightarrow \mathbb{N}$, there exists $C$ such that:

any function $f : \mathbb{F}_2^n \rightarrow \{0, 1\}$ can be decomposed as $f = f' + f''$, where

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

The Gowers norm $\|f''\|_{U^d}$ is at most $\gamma$. 

Yuichi Yoshida (NII and PFI)
Theorem (Decomposition Theorem [BFH+13])

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

- a **structured part** $f' : \mathbb{F}_2^n \rightarrow [0, 1]$, 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 $\geq r(C)$.
  - $\Gamma : \mathbb{T}^C \rightarrow [0, 1]$ is a function.

- a pseudo-random part $f'' : \mathbb{F}_2^n \rightarrow [-1, 1]$.
- The Gowers norm $\|f''\|_{U^d}$ is at most $\gamma$. 

Yuichi Yoshida (NII and PFI)
Constant Sketches 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 $\gamma$. 
Factors

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

The decomposition theorem says:

\[
\mathbb{F}_2^n = \Gamma(P_1, \ldots, P_C) + \Upsilon
\]
What is the Gowers Norm?

**Definition**

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

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

where $J$ denotes complex conjugation.

- $\|f\|_{U^1} = |\mathbb{E}_x f(x)|$
- $\|f\|_{U^1} \leq \|f\|_{U^2} \leq \|f\|_{U^3} \leq \cdots$
- $\|f\|_{U^d}$ 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 \(P : \mathbb{F}_2^n \rightarrow \{0, 1\}\) 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 $P : \mathbb{F}_2^n \rightarrow \{0, 1\}$ of degree $< d$, $\|(-1)^P\|_{U^d} = 1$. However, the converse does not hold when $d \geq 4$...*

**Definition**

$P : \mathbb{F}_2^n \rightarrow \mathbb{T}$ is a *non-classical polynomial of degree (less than) $d$* if

\[ \|\exp(2\pi i \cdot f)\|_{U^d} = 1. \]

It turns out that the range of $P$ is $U_{k+1} := \{0, \frac{1}{2^{k+1}}, \ldots, \frac{2^{k+1}-1}{2^{k+1}}\}$ for some $k$ (= *depth*).
Is This Really a Constant-size Sketch?

• Structured part: $f' = \Gamma(P_1, \ldots, P_C)$.
• $\Gamma$ indeed has a constant-size representation, but $P_1, \ldots, P_C$ may not have.
• 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.
Formalize “$f$ has some specific structured part”.

**Definition**

A *regularity-instance* $I$ is a tuple of

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

Definition

Let $I = (\gamma, \Gamma, C, d, d, h, r)$ 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 $r$,
- $\|\Upsilon\|_{U^d} \leq \gamma$.

Can we test the property of satisfying $I$?
Testing the Property of Satisfying a Regularity-Instance

Theorem

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

**Theorem**

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

Q. Is this really meaningful? There might not exist a polynomial sequence of rank at least $r$ as it depends on many parameters...
Testing the Property of Satisfying a Regularity-Instance

**Theorem**

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

**Q.** Is this really meaningful? There might not exist a polynomial sequence of rank at least $r$ as it depends on many parameters...

**Lemma (Polynomial regularity lemma [BFH+13])**

For any $d \in \mathbb{N}$ and $r : \mathbb{N} \rightarrow \mathbb{N}$, there is a function $\bar{C} : \mathbb{N}$ s.t. there is a polynomial sequence $P$ with $|P| \leq \bar{C}$, degree $\leq d$, and rank $\geq r(|P|)$. 
A property $\mathcal{P}$ is **regular-reducible** if for any $\delta > 0$, there exists a set $\mathcal{R}$ of constant number of regularity-instances with constant parameters and a **high rank** (depending on $\delta$) such that:
Our Characterization

**Theorem**

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

$\iff$

$\mathcal{P}$ 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 $\Gamma$, $\mathbf{d}$, and $\mathbf{h}$ determines the distribution, we can find $\mathcal{R}$ using the tester.
Testability of the Property of Satisfying a Regularity-Instance

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

1. Set $\delta$ 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 $\delta$-close to satisfying $I$ **then** accept.
4. **else** reject.
Testability of the Property of Satisfying a Regularity-Instance

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

1. Set $\delta$ small enough and $m$ large enough.
2. Take a random affine embedding $A : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$.
3. If $f \circ A$ is $\delta$-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 \( I \)

- \( f(x) = \Gamma(P(x)) + \Upsilon(x) \) with \( \| \Upsilon(x) \|_{U_d} \leq \gamma \).
- \( f(Ax) \) almost satisfies \( I \):
  - \( f(Ax) = \Gamma(P(Ax)) + \Upsilon(Ax) \) with \( \| \Upsilon(Ax) \|_{U_d} \leq \gamma + o(\gamma) \).
  - \( P(Ax) \) meets the requirement of \( I \).
- By perturbing \( f(Ax) \) up to \( \delta \)-fraction, we obtain a function satisfying \( I \).
If \( f \) is \( \epsilon \)-far from \( I \)

- Suppose that \( f \circ A \) is \( \delta \)-close to satisfying \( I \) with high probability.
  - \( \delta \)-close: \( f(Ax) = \Gamma(P'(x)) + \Upsilon'(x) + \Delta'(x) \).
  - Decomposition:
    \[
    f(x) = \Sigma(R(x)) + \text{noise} \Rightarrow f(Ax) = \Sigma(R(Ax)) + \text{noise}.
    \]
- We “lift” \( P' \cup (R \circ A) \) to \( P \cup R \) using the high-rank conditions.
  - \( \Sigma(R(x)) = \Gamma(P(x)) + \Upsilon(x) \) with \( \|\Upsilon\|_{U^d} \leq \gamma + o(\gamma) \).
  - \( P \) meets the requirement of \( I \).
- By perturbing \( f \) up to \( \epsilon \)-fraction, we get a function satisfying \( I \), 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 requires Ackermann-type complexity.
Conclusions

• Easily extendable to $\mathbb{F}_p$ for a prime $p$.

• Query complexity is actually unknown due to the Gowers inverse theorem. Other parts requires Ackermann-type complexity.

Open Problems

• $\mathcal{P}$ is locally testable with one-sided error $\Leftrightarrow \mathcal{P}$ is affine-subspace hereditary? [BFH+13]

• Characterizations of proximity oblivious testing?

• Why is affine-invariance easier to deal with than permutation-invariant properties?