Property Testing Bounds for Linear and Quadratic Functions via Parity Decision Trees

A. Bhrushundi[1] S. Chakraborty[1] R. Kulkarni[2]

[1]Chennai Mathematical Institute
India

[2]Center for Quantum Technologies
Singapore

CSR 2014

Outline

Outline

What's property testing?

- Property - collection of combinatorial objects (graphs, functions etc.).
- This talk: Boolean functions, $f : \{0,1\}^n \to \{0,1\}$.
- Object A far from object B if A needs "lots" of modifications to become B.

Property Testing: Design randomized algorithms to determine if object in property, or "far" from it.

Catch: Read only part of the input!

What's property testing?

- Property - collection of combinatorial objects (graphs, functions etc.).
- This talk: Boolean functions, $f : \{0,1\}^n \to \{0,1\}$.
- Object A far from object B if A needs "lots" of modifications to become B.

Property Testing: Design randomized algorithms to determine if object in property, or "far" from it.

Catch: Read only part of the input!

What's property testing?

- Property - collection of combinatorial objects (graphs, functions etc.).
- This talk: Boolean functions, $f : \{0,1\}^n \to \{0,1\}$.
- Object A far from object B if A needs "lots" of modifications to become B.

Property Testing: Design randomized algorithms to determine if object in property, or "far" from it.

Catch: Read only part of the input!

What's property testing?

- Property - collection of combinatorial objects (graphs, functions etc.).
- This talk: Boolean functions, $f : \{0,1\}^n \to \{0,1\}$.
- Object A far from object B if A needs "lots" of modifications to become B.

Property Testing: Design randomized algorithms to determine if object in property, or "far" from it.

Catch: Read only part of the input!

What's property testing?

- Property - collection of combinatorial objects (graphs, functions etc.).
- This talk: Boolean functions, $f : \{0,1\}^n \to \{0,1\}$.
- Object A far from object B if A needs "lots" of modifications to become B.

Property Testing: Design randomized algorithms to determine if object in property, or "far" from it.

Catch: Read only part of the input!

Testing of Boolean functions

Let $\mathcal{P}$ be property of Boolean functions (linearity, monotonicity, k-junta, isomorphism ...).

Definition (ϵ-tester for a property $\mathcal{P}$)

Given 1^n, $f : \{0,1\}^n \to \{0,1\}$ as truth table, determine with probability $\geq 2/3$ if

- $f \in \mathcal{P}$, or
- $\forall g \in \mathcal{P}$, $dist(f, g) \geq \epsilon$,

by making queries to truth table.

Query complexity - $Q^{\epsilon}(\mathcal{P})$ - # queries by best ϵ-tester as function of n and ϵ.

Testing of Boolean functions

Let $\mathcal{P}$ be property of Boolean functions (linearity, monotonicity, k-junta, isomorphism ...).

Definition (ϵ-tester for a property $\mathcal{P}$)

Given 1^n, $f : \{0,1\}^n \to \{0,1\}$ as truth table, determine with probability $\geq 2/3$ if

- $f \in \mathcal{P}$, or
- $\forall g \in \mathcal{P}$, $dist(f,g) \geq \epsilon$,

by making queries to truth table.

Query complexity - $Q^{\epsilon}(\mathcal{P})$ - # queries by best ϵ-tester as function of n and ϵ.

Testing of Boolean functions

Let $\mathcal{P}$ be property of Boolean functions (linearity, monotonicity, k-junta, isomorphism ...).

Definition (ϵ-tester for a property $\mathcal{P}$)

Given 1^n, $f : \{0,1\}^n \to \{0,1\}$ as truth table, determine with probability $\geq 2/3$ if

- $f \in \mathcal{P}$, or
- $\forall g \in \mathcal{P}$, $dist(f,g) \geq \epsilon$,

by making queries to truth table.

Query complexity - $Q^{\epsilon}(\mathcal{P})$ - # queries by best ϵ-tester as function of n and ϵ.

Outline

Goal of property testing

- Study $Q^{\epsilon}(\mathcal{P})$ as function of n and ϵ.
- Difficult for arbitrary $\mathcal{P}$ - consider special cases!
- One such case - properties invariant under transformations on domain.
- Example: affine-invariant and linear-invariant properties.

Goal of property testing

- Study $Q^{\epsilon}(\mathcal{P})$ as function of n and ϵ.
- Difficult for arbitrary $\mathcal{P}$ - consider special cases!
- One such case - properties invariant under transformations on domain.
- Example: affine-invariant and linear-invariant properties.

Goal of property testing

- Study $Q^{\epsilon}(\mathcal{P})$ as function of n and ϵ.
- Difficult for arbitrary $\mathcal{P}$ - consider special cases!
- One such case - properties invariant under transformations on domain.
- Example: affine-invariant and linear-invariant properties.

Goal of property testing

- Study $Q^{\epsilon}(\mathcal{P})$ as function of n and ϵ.
- Difficult for arbitrary $\mathcal{P}$ - consider special cases!
- One such case - properties invariant under transformations on domain.
- Example: affine-invariant and linear-invariant properties.

Isomorphism testing

- A special case of invariant properties.
- Orbit of a single function under transformations.

Definition (ϵ-testing G-isomorphism to h)

Let $\mathcal{P}_h = \{h \circ T \mid T \in G\}$. ϵ-testing G-isomorphism to h is problem of ϵ-testing $\mathcal{P}_h$.

G could be S_n, $GL_n(\mathbb{F}_2)$ or $Aff_n(\mathbb{F}_2)$.

Isomorphism testing

- A special case of invariant properties.
- Orbit of a single function under transformations.

Definition (ϵ-testing G-isomorphism to h)

Let $\mathcal{P}_h = \{h \circ T \mid T \in G\}$. ϵ-testing G-isomorphism to h is problem of ϵ-testing $\mathcal{P}_h$.

G could be S_n, $GL_n(\mathbb{F}_2)$ or $Aff_n(\mathbb{F}_2)$.

Isomorphism testing

- A special case of invariant properties.
- Orbit of a single function under transformations.

Definition (ϵ-testing G-isomorphism to h)

Let $\mathcal{P}_h = \{h \circ T \mid T \in G\}$. ϵ-testing G-isomorphism to h is problem of ϵ-testing $\mathcal{P}_h$.

G could be S_n, $GL_n(\mathbb{F}_2)$ or $Aff_n(\mathbb{F}_2)$.

Isomorphism testing

- A special case of invariant properties.
- Orbit of a single function under transformations.

Definition (ϵ-testing G-isomorphism to h)

Let $\mathcal{P}_h = \{h \circ T \mid T \in G\}$. ϵ-testing G-isomorphism to h is problem of ϵ-testing $\mathcal{P}_h$.

G could be S_n, $GL_n(\mathbb{F}_2)$ or $Aff_n(\mathbb{F}_2)$.

Outline

Testing k-linearity

- Isomorphism testing: $G = S_n$, $h = x_1 + x_2 + \ldots + x_k$.
- Known: upper bound $O(k \log k)$, lower bound $\Omega(k)$.
- Our result: new proof of $\Omega(k)$ lower bound.
- Advantage: earlier proofs not likely to be improved.
- Hope for closing gap.

Testing k-linearity

- Isomorphism testing: $G = S_n$, $h = x_1 + x_2 + \ldots + x_k$.
- Known: upper bound $O(k \log k)$, lower bound $\Omega(k)$.
- Our result: new proof of $\Omega(k)$ lower bound.
- Advantage: earlier proofs not likely to be improved.
- Hope for closing gap.

Testing k-linearity

- Isomorphism testing: $G = S_n$, $h = x_1 + x_2 + \ldots + x_k$.
- Known: upper bound $O(k \log k)$, lower bound $\Omega(k)$.
- Our result: new proof of $\Omega(k)$ lower bound.
- Advantage: earlier proofs not likely to be improved.
- Hope for closing gap.

Testing k-linearity

- Isomorphism testing: $G = S_n$, $h = x_1 + x_2 + \ldots + x_k$.
- Known: upper bound $O(k \log k)$, lower bound $\Omega(k)$.
- Our result: new proof of $\Omega(k)$ lower bound.
- Advantage: earlier proofs not likely to be improved.
- Hope for closing gap.

Testing k-linearity

- Isomorphism testing: $G = S_n$, $h = x_1 + x_2 + \ldots + x_k$.
- Known: upper bound $O(k \log k)$, lower bound $\Omega(k)$.
- Our result: new proof of $\Omega(k)$ lower bound.
- Advantage: earlier proofs not likely to be improved.
- Hope for closing gap.

Testing affine-isomorphism

- Trivial upper bound for G-isomorphism testing to any function h: $O(\log |G|)$.
- Consider $G = Aff_n$. Can trivial upper bound - $O(n^2)$ - be improved?
- Our result: $IP_n(x) = x_1x_2 + x_3x_4 + \ldots x_{n-1}x_n$ needs $\Omega(n^2)$.

Testing affine-isomorphism

- Trivial upper bound for G-isomorphism testing to any function h: $O(\log |G|)$.
- Consider $G = Aff_n$. Can trivial upper bound - $O(n^2)$ - be improved?
- Our result: $IP_n(x) = x_1x_2 + x_3x_4 + \ldots x_{n-1}x_n$ needs $\Omega(n^2)$.

Testing affine-isomorphism

- Trivial upper bound for G-isomorphism testing to any function h: $O(\log |G|)$.
- Consider $G = Aff_n$. Can trivial upper bound - $O(n^2)$ - be improved?
- Our result: $IP_n(x) = x_1x_2 + x_3x_4 + \ldots x_{n-1}x_n$ needs $\Omega(n^2)$.

Testing affine-isomorphism

- Trivial upper bound for G-isomorphism testing to any function h: $O(\log |G|)$.
- Consider $G = Aff_n$. Can trivial upper bound - $O(n^2)$ - be improved?
- Our result: $IP_n(x) = x_1x_2 + x_3x_4 + \ldots x_{n-1}x_n$ needs $\Omega(n^2)$.

Main techniques

- Associate Boolean function $E_{\mathcal{P}}$ with property $\mathcal{P}$ of linear/quadratic functions.
- $Q^{\epsilon}(\mathcal{P}) \geq$ Randomized parity decision tree complexity of $E_{\mathcal{P}}$ (denoted by $R_{\oplus}(E_{\mathcal{P}})$).
- Lower bound $R_{\oplus}(E_{\mathcal{P}})$ using communication complexity.

Main techniques

- Associate Boolean function $E_{\mathcal{P}}$ with property $\mathcal{P}$ of linear/quadratic functions.
- $Q^{\epsilon}(\mathcal{P}) \geq$ Randomized parity decision tree complexity of $E_{\mathcal{P}}$ (denoted by $R_{\oplus}(E_{\mathcal{P}})$).
- Lower bound $R_{\oplus}(E_{\mathcal{P}})$ using communication complexity.

Main techniques

- Associate Boolean function $E_{\mathcal{P}}$ with property $\mathcal{P}$ of linear/quadratic functions.
- $Q^{\epsilon}(\mathcal{P}) \geq$ Randomized parity decision tree complexity of $E_{\mathcal{P}}$ (denoted by $R_{\oplus}(E_{\mathcal{P}})$).
- Lower bound $R_{\oplus}(E_{\mathcal{P}})$ using communication complexity.

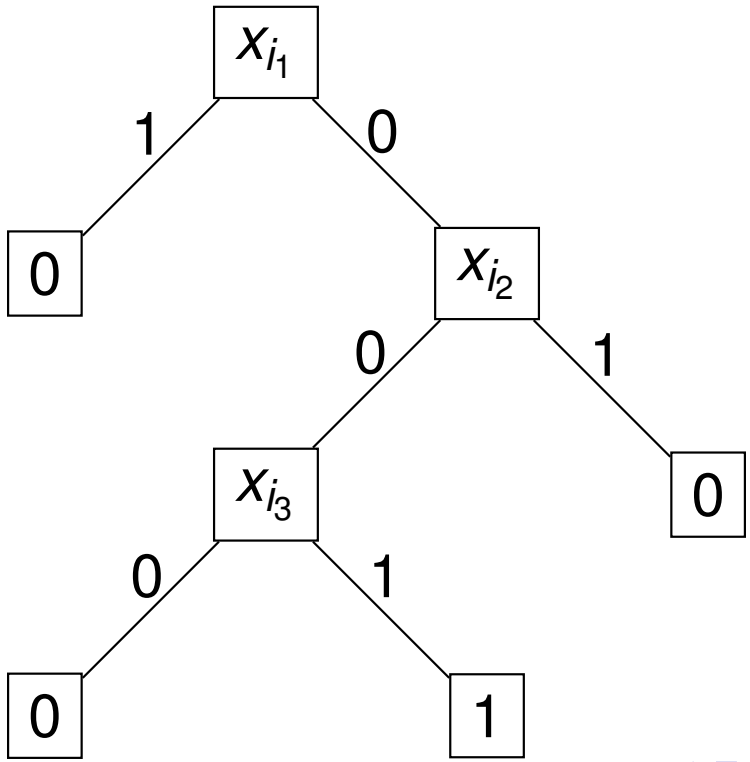
Outline

Decision trees

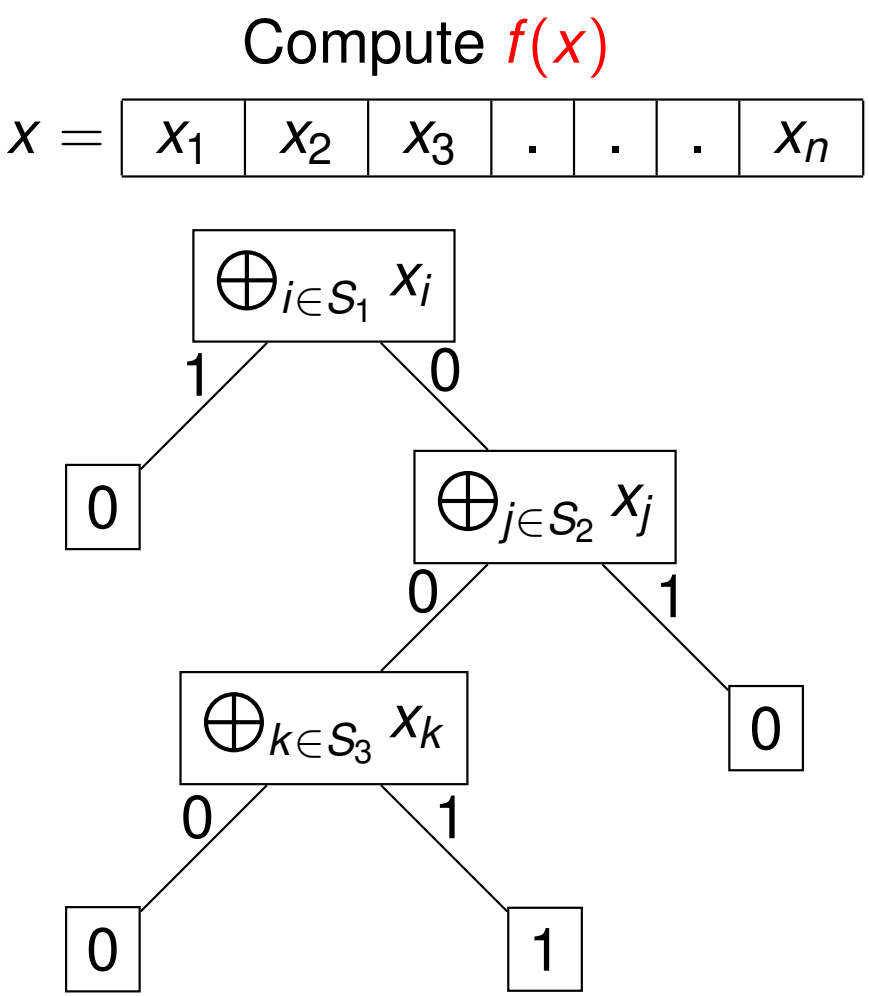
$f : \{0,1\}^n \to \{0,1\}$

Compute $f(x)$

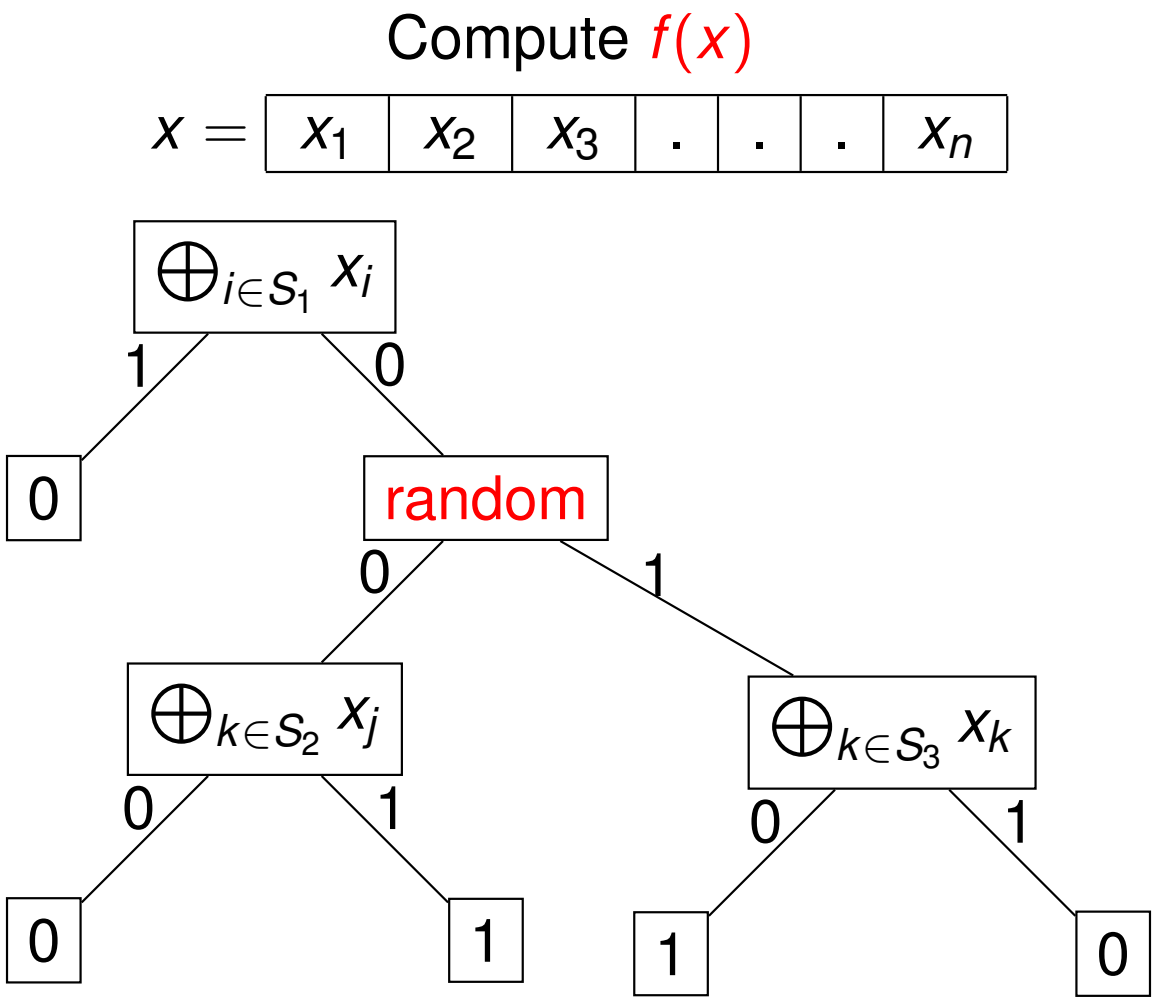
$x =$ | x_1 | x_2 | x_3 | . | . | . | x_n |



Parity decision trees



Randomized parity decision trees



Randomized parity decision trees - contd.

- $\mathcal{T}$ computes f if $\forall x \Pr[\mathcal{T}(x) = f(x)] \geq \frac{2}{3}$.
- Probability over values of random nodes.
- Depth of $\mathcal{T}$ = Max # query nodes along any path.
- $R_{\oplus}(f)$ = Depth of "best" $\mathcal{T}$ computing f.

Randomized parity decision trees - contd.

- $\mathcal{T}$ computes f if $\forall x \Pr[\mathcal{T}(x) = f(x)] \geq \frac{2}{3}$.
- Probability over values of random nodes.
- Depth of $\mathcal{T}$ = Max # query nodes along any path.
- $R_{\oplus}(f)$ = Depth of "best" $\mathcal{T}$ computing f.

Randomized parity decision trees - contd.

- $\mathcal{T}$ computes f if $\forall x \Pr[\mathcal{T}(x) = f(x)] \geq \frac{2}{3}$.
- Probability over values of random nodes.
- Depth of $\mathcal{T}$ = Max # query nodes along any path.
- $R_{\oplus}(f)$ = Depth of "best" $\mathcal{T}$ computing f.

Randomized parity decision trees - contd.

- $\mathcal{T}$ computes f if $\forall x \Pr[\mathcal{T}(x) = f(x)] \geq \frac{2}{3}$.
- Probability over values of random nodes.
- Depth of $\mathcal{T}$ = Max # query nodes along any path.
- $R_{\oplus}(f)$ = Depth of "best" $\mathcal{T}$ computing f.

Outline

Properties of linear functions

- View linear functions as strings.
- E.g. $x_1 + x_3 + x_5 \in \mathbb{F}_2[x_1, x_2, x_3, x_4, x_5]$ as 10101.
- Also, $y \in \{0,1\}^n$ gives $f_y \in \mathbb{F}_2[x_1, \ldots, x_n]$.

$\mathcal{P}$ of linear functions $\longleftrightarrow$ $E_{\mathcal{P}} : \{0,1\}^n \to \{0,1\}$

$$E_{\mathcal{P}}(y) = 1 \Leftrightarrow f_y \in \mathcal{P}$$

Properties of linear functions

- View linear functions as strings.
- E.g. $x_1 + x_3 + x_5 \in \mathbb{F}_2[x_1, x_2, x_3, x_4, x_5]$ as 10101.
- Also, $y \in \{0,1\}^n$ gives $f_y \in \mathbb{F}_2[x_1, \ldots, x_n]$.

$\mathcal{P}$ of linear functions $\longleftrightarrow$ $E_{\mathcal{P}} : \{0,1\}^n \to \{0,1\}$

$$E_{\mathcal{P}}(y) = 1 \Leftrightarrow f_y \in \mathcal{P}$$

Properties of linear functions

- View linear functions as strings.
- E.g. $x_1 + x_3 + x_5 \in \mathbb{F}_2[x_1, x_2, x_3, x_4, x_5]$ as 10101.
- Also, $y \in \{0,1\}^n$ gives $f_y \in \mathbb{F}_2[x_1, \ldots, x_n]$.

$\mathcal{P}$ of linear functions $\longleftrightarrow$ $E_{\mathcal{P}} : \{0,1\}^n \to \{0,1\}$

$$E_{\mathcal{P}}(y) = 1 \Leftrightarrow f_y \in \mathcal{P}$$

Properties of linear functions

- View linear functions as strings.
- E.g. $x_1 + x_3 + x_5 \in \mathbb{F}_2[x_1, x_2, x_3, x_4, x_5]$ as 10101.
- Also, $y \in \{0,1\}^n$ gives $f_y \in \mathbb{F}_2[x_1, \ldots, x_n]$.

$\mathcal{P}$ of linear functions $\longleftrightarrow$ $E_{\mathcal{P}} : \{0,1\}^n \to \{0,1\}$

$$E_{\mathcal{P}}(y) = 1 \Leftrightarrow f_y \in \mathcal{P}$$

Properties of linear functions - contd.

Claim:

1/2-tester $\mathcal{T}$ for $\mathcal{P} \longrightarrow$ RPDT $\mathcal{T}'$ for $E_{\mathcal{P}}$

Proof:
(Input to $\mathcal{T}'$ is y)

- $\mathcal{T}$ queries f_y at $x \rightarrow \mathcal{T}'$ queries $\bigoplus_{\{i|x_i=1\}} y_i$
- Coin toss by $\mathcal{T} \rightarrow$ random node in $\mathcal{T}'$.
- $\mathcal{T}$ accepts $\rightarrow$ '1' leaf in $\mathcal{T}'$.

Note: can prove converse - RPDT $\mathcal{T}' \rightarrow 1/2$-tester $\mathcal{T}$.

$$Q^{1/2}(\mathcal{P}) = R_{\oplus}(E_{\mathcal{P}})$$

Properties of linear functions - contd.

Claim:

1/2-tester $\mathcal{T}$ for $\mathcal{P} \longrightarrow$ RPDT $\mathcal{T}'$ for $E_{\mathcal{P}}$

Proof:

(Input to $\mathcal{T}'$ is y)

- $\mathcal{T}$ queries f_y at $x \rightarrow \mathcal{T}'$ queries $\bigoplus_{\{i|x_i=1\}} y_i$
- Coin toss by $\mathcal{T} \rightarrow$ random node in $\mathcal{T}'$.
- $\mathcal{T}$ accepts $\rightarrow$ '1' leaf in $\mathcal{T}'$.

Note: can prove converse - RPDT $\mathcal{T}' \rightarrow 1/2$-tester $\mathcal{T}$.

$$Q^{1/2}(\mathcal{P}) = R_{\oplus}(E_{\mathcal{P}})$$

Properties of linear functions - contd.

Claim:

1/2-tester $\mathcal{T}$ for $\mathcal{P} \longrightarrow$ RPDT $\mathcal{T}'$ for $E_{\mathcal{P}}$

Proof:
(Input to $\mathcal{T}'$ is y)

- $\mathcal{T}$ queries f_y at $x \rightarrow \mathcal{T}'$ queries $\bigoplus_{\{i|x_i=1\}} y_i$
- Coin toss by $\mathcal{T} \rightarrow$ random node in $\mathcal{T}'$.
- $\mathcal{T}$ accepts $\rightarrow$ '1' leaf in $\mathcal{T}'$.

Note: can prove converse - RPDT $\mathcal{T}' \rightarrow 1/2$-tester $\mathcal{T}$.

$$Q^{1/2}(\mathcal{P}) = R_{\oplus}(E_{\mathcal{P}})$$

Properties of linear functions - contd.

Claim:

1/2-tester $\mathcal{T}$ for $\mathcal{P} \longrightarrow$ RPDT $\mathcal{T}'$ for $E_{\mathcal{P}}$

Proof:
(Input to $\mathcal{T}'$ is y)

- $\mathcal{T}$ queries f_y at $x \rightarrow \mathcal{T}'$ queries $\bigoplus_{\{i|x_i=1\}} y_i$
- Coin toss by $\mathcal{T} \rightarrow$ random node in $\mathcal{T}'$.
- $\mathcal{T}$ accepts $\rightarrow$ '1' leaf in $\mathcal{T}'$.

Note: can prove converse - RPDT $\mathcal{T}' \rightarrow$ 1/2-tester $\mathcal{T}$.

$$Q^{1/2}(\mathcal{P}) = R_{\oplus}(E_{\mathcal{P}})$$

Properties of linear functions - contd.

Claim:

1/2-tester $\mathcal{T}$ for $\mathcal{P} \longrightarrow$ RPDT $\mathcal{T}'$ for $E_{\mathcal{P}}$

Proof:
(Input to $\mathcal{T}'$ is y)

- $\mathcal{T}$ queries f_y at $x \rightarrow \mathcal{T}'$ queries $\bigoplus_{\{i|x_i=1\}} y_i$
- Coin toss by $\mathcal{T} \rightarrow$ random node in $\mathcal{T}'$.
- $\mathcal{T}$ accepts $\rightarrow$ '1' leaf in $\mathcal{T}'$.

Note: can prove converse - RPDT $\mathcal{T}' \rightarrow$ 1/2-tester $\mathcal{T}$.

$$Q^{1/2}(\mathcal{P}) = R_{\oplus}(E_{\mathcal{P}})$$

Properties of linear functions - contd.

Claim:

1/2-tester $\mathcal{T}$ for $\mathcal{P} \longrightarrow$ RPDT $\mathcal{T}'$ for $E_{\mathcal{P}}$

Proof:
(Input to $\mathcal{T}'$ is y)

- $\mathcal{T}$ queries f_y at $x \rightarrow \mathcal{T}'$ queries $\bigoplus_{\{i|x_i=1\}} y_i$
- Coin toss by $\mathcal{T} \rightarrow$ random node in $\mathcal{T}'$.
- $\mathcal{T}$ accepts $\rightarrow$ '1' leaf in $\mathcal{T}'$.

Note: can prove converse - RPDT $\mathcal{T}' \rightarrow 1/2$-tester $\mathcal{T}$.

$$Q^{1/2}(\mathcal{P}) = R_{\oplus}(E_{\mathcal{P}})$$

Properties of linear functions - contd.

Claim:

1/2-tester $\mathcal{T}$ for $\mathcal{P} \longrightarrow$ RPDT $\mathcal{T}'$ for $E_{\mathcal{P}}$

Proof:
(Input to $\mathcal{T}'$ is y)

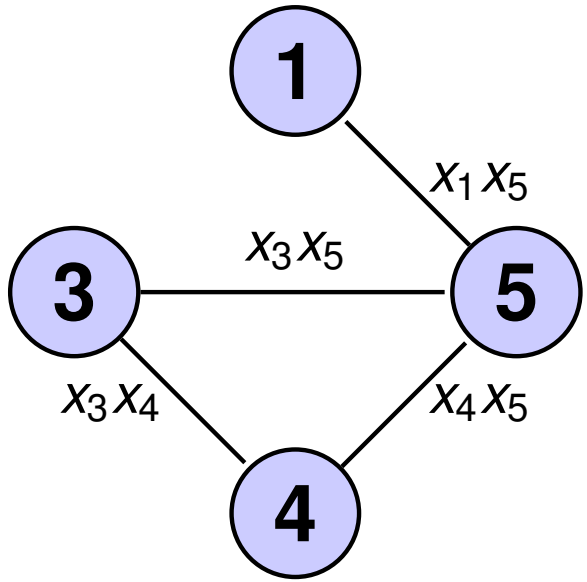
- $\mathcal{T}$ queries f_y at $x \rightarrow \mathcal{T}'$ queries $\bigoplus_{\{i|x_i=1\}} y_i$
- Coin toss by $\mathcal{T} \rightarrow$ random node in $\mathcal{T}'$.
- $\mathcal{T}$ accepts $\rightarrow$ '1' leaf in $\mathcal{T}'$.

Note: can prove converse - RPDT $\mathcal{T}' \rightarrow 1/2$-tester $\mathcal{T}$.

$$Q^{1/2}(\mathcal{P}) = R_{\oplus}(E_{\mathcal{P}})$$

Properties of quadratic functions

homogeneous quadratic functions $\longleftrightarrow$ graphs



$$x_1x_5 + x_3x_4 + x_3x_5 + x_4x_5 \in \mathbb{F}_2[x_1, \ldots, x_5]$$

Properties of quadratic functions

$\mathcal{P}$ of quadratic functions $\longrightarrow$ $E_{\mathcal{P}} : \{0,1\}^{n^2} \to \{0,1\}$

$$E_{\mathcal{P}}(G) = 1 \Leftrightarrow f_G \in \mathcal{P}$$

Claim:

1/4-tester $\mathcal{T}$ for $\mathcal{P} \longrightarrow$ RPDT $\mathcal{T}'$ for $E_{\mathcal{P}}$

Proof:

- $\mathcal{T}$ queries f_G at $x \to \mathcal{T}'$ queries induced graph $\{i | x_i = 1\}$
- Coin toss by $\mathcal{T} \to$ random node in $\mathcal{T}'$.
- $\mathcal{T}$ accepts $\to$ '1' leaf in $\mathcal{T}'$.

$$Q^{1/4}(\mathcal{P}) \geq R_{\oplus}(E_{\mathcal{P}})$$

Note: only one direction works!

Properties of quadratic functions

$\mathcal{P}$ of quadratic functions $\longrightarrow$ $E_{\mathcal{P}} : \{0,1\}^{n^2} \to \{0,1\}$

$$E_{\mathcal{P}}(G) = 1 \Leftrightarrow f_G \in \mathcal{P}$$

Claim:

1/4-tester $\mathcal{T}$ for $\mathcal{P} \longrightarrow$ RPDT $\mathcal{T}'$ for $E_{\mathcal{P}}$

Proof:

- $\mathcal{T}$ queries f_G at $x \to \mathcal{T}'$ queries induced graph $\{i | x_i = 1\}$
- Coin toss by $\mathcal{T} \to$ random node in $\mathcal{T}'$.
- $\mathcal{T}$ accepts $\to$ '1' leaf in $\mathcal{T}'$.

$$Q^{1/4}(\mathcal{P}) \geq R_{\oplus}(E_{\mathcal{P}})$$

Note: only one direction works!

Properties of quadratic functions

$\mathcal{P}$ of quadratic functions $\longrightarrow$ $E_{\mathcal{P}} : \{0,1\}^{n^2} \to \{0,1\}$

$$E_{\mathcal{P}}(G) = 1 \Leftrightarrow f_G \in \mathcal{P}$$

Claim:

1/4-tester $\mathcal{T}$ for $\mathcal{P} \longrightarrow$ RPDT $\mathcal{T}'$ for $E_{\mathcal{P}}$

Proof:

- $\mathcal{T}$ queries f_G at $x \to \mathcal{T}'$ queries induced graph $\{i | x_i = 1\}$
- Coin toss by $\mathcal{T} \to$ random node in $\mathcal{T}'$.
- $\mathcal{T}$ accepts $\to$ '1' leaf in $\mathcal{T}'$.

$$Q^{1/4}(\mathcal{P}) \geq R_{\oplus}(E_{\mathcal{P}})$$

Note: only one direction works!

Properties of quadratic functions

$\mathcal{P}$ of quadratic functions $\longrightarrow$ $E_{\mathcal{P}} : \{0,1\}^{n^2} \to \{0,1\}$

$$E_{\mathcal{P}}(G) = 1 \Leftrightarrow f_G \in \mathcal{P}$$

Claim:

1/4-tester $\mathcal{T}$ for $\mathcal{P} \longrightarrow$ RPDT $\mathcal{T}'$ for $E_{\mathcal{P}}$

Proof:

- $\mathcal{T}$ queries f_G at $x \to \mathcal{T}'$ queries induced graph $\{i | x_i = 1\}$
- Coin toss by $\mathcal{T} \to$ random node in $\mathcal{T}'$.
- $\mathcal{T}$ accepts $\to$ '1' leaf in $\mathcal{T}'$.

$$Q^{1/4}(\mathcal{P}) \geq R_{\oplus}(E_{\mathcal{P}})$$

Note: only one direction works!

Properties of quadratic functions

$\mathcal{P}$ of quadratic functions $\longrightarrow$ $E_{\mathcal{P}} : \{0,1\}^{n^2} \to \{0,1\}$

$$E_{\mathcal{P}}(G) = 1 \Leftrightarrow f_G \in \mathcal{P}$$

Claim:

1/4-tester $\mathcal{T}$ for $\mathcal{P} \longrightarrow$ RPDT $\mathcal{T}'$ for $E_{\mathcal{P}}$

Proof:

- $\mathcal{T}$ queries f_G at $x \to \mathcal{T}'$ queries induced graph $\{i | x_i = 1\}$
- Coin toss by $\mathcal{T} \to$ random node in $\mathcal{T}'$.
- $\mathcal{T}$ accepts $\to$ '1' leaf in $\mathcal{T}'$.

$$Q^{1/4}(\mathcal{P}) \geq R_{\oplus}(E_{\mathcal{P}})$$

Note: only one direction works!

Properties of quadratic functions

$\mathcal{P}$ of quadratic functions $\longrightarrow$ $E_{\mathcal{P}} : \{0,1\}^{n^2} \to \{0,1\}$

$$E_{\mathcal{P}}(G) = 1 \Leftrightarrow f_G \in \mathcal{P}$$

Claim:

1/4-tester $\mathcal{T}$ for $\mathcal{P} \longrightarrow$ RPDT $\mathcal{T}'$ for $E_{\mathcal{P}}$

Proof:

- $\mathcal{T}$ queries f_G at $x \to \mathcal{T}'$ queries induced graph $\{i | x_i = 1\}$
- Coin toss by $\mathcal{T} \to$ random node in $\mathcal{T}'$.
- $\mathcal{T}$ accepts $\to$ '1' leaf in $\mathcal{T}'$.

$$Q^{1/4}(\mathcal{P}) \geq R_{\oplus}(E_{\mathcal{P}})$$

Note: only one direction works!

Properties of quadratic functions

$\mathcal{P}$ of quadratic functions $\longrightarrow$ $E_{\mathcal{P}} : \{0,1\}^{n^2} \to \{0,1\}$

$$E_{\mathcal{P}}(G) = 1 \Leftrightarrow f_G \in \mathcal{P}$$

Claim:

1/4-tester $\mathcal{T}$ for $\mathcal{P} \longrightarrow$ RPDT $\mathcal{T}'$ for $E_{\mathcal{P}}$

Proof:

- $\mathcal{T}$ queries f_G at $x \to \mathcal{T}'$ queries induced graph $\{i | x_i = 1\}$
- Coin toss by $\mathcal{T} \to$ random node in $\mathcal{T}'$.
- $\mathcal{T}$ accepts $\to$ '1' leaf in $\mathcal{T}'$.

$$Q^{1/4}(\mathcal{P}) \geq R_{\oplus}(E_{\mathcal{P}})$$

Note: only one direction works!

Outline

Enter communication complexity

- Alice has x and Bob has y, want to compute $f(x \oplus y)$.
- $RCC(f(x \oplus y))$ - randomized communication complexity of computing $f(x \oplus y)$.
- Can show: $R_{\oplus}(f) \geq \frac{1}{2} RCC(f(x \oplus y))$.
- Hint: simple simulation!

Enter communication complexity

- Alice has x and Bob has y, want to compute $f(x \oplus y)$.
- $RCC(f(x \oplus y))$ - randomized communication complexity of computing $f(x \oplus y)$.
- Can show: $R_{\oplus}(f) \geq \frac{1}{2} RCC(f(x \oplus y))$.
- Hint: simple simulation!

Enter communication complexity

- Alice has x and Bob has y, want to compute $f(x \oplus y)$.
- $RCC(f(x \oplus y))$ - randomized communication complexity of computing $f(x \oplus y)$.
- Can show: $R_{\oplus}(f) \geq \frac{1}{2} RCC(f(x \oplus y))$.
- Hint: simple simulation!

Enter communication complexity

- Alice has x and Bob has y, want to compute $f(x \oplus y)$.
- $RCC(f(x \oplus y))$ - randomized communication complexity of computing $f(x \oplus y)$.
- Can show: $R_{\oplus}(f) \geq \frac{1}{2} RCC(f(x \oplus y))$.
- Hint: simple simulation!

Outline

$\Omega(k)$ lower bound for k-linearity

- Suppose $\mathcal{P}$ is set of k-linear functions.
- $E_{\mathcal{P}} : \{0,1\}^n \to \{0,1\}$ is such that $E_{\mathcal{P}}(y) = 1 \Leftrightarrow wt(y) = k$.
- $Q^{1/2}(\mathcal{P}) = R_{\oplus}(E_{\mathcal{P}})$
- $R_{\oplus}(E_{\mathcal{P}}) \geq \frac{1}{2} RCC(E_{\mathcal{P}}(x \oplus y))$.
- Known: $RCC(E_{\mathcal{P}}(x \oplus y)) = \Omega(k)$ (Set Disjointness).

$\Omega(k)$ lower bound for k-linearity

- Suppose $\mathcal{P}$ is set of k-linear functions.
- $E_{\mathcal{P}} : \{0,1\}^n \to \{0,1\}$ is such that $E_{\mathcal{P}}(y) = 1 \Leftrightarrow wt(y) = k$.
- $Q^{1/2}(\mathcal{P}) = R_{\oplus}(E_{\mathcal{P}})$
- $R_{\oplus}(E_{\mathcal{P}}) \geq \frac{1}{2} RCC(E_{\mathcal{P}}(x \oplus y))$.
- Known: $RCC(E_{\mathcal{P}}(x \oplus y)) = \Omega(k)$ (Set Disjointness).

$\Omega(k)$ lower bound for k-linearity

- Suppose $\mathcal{P}$ is set of k-linear functions.
- $E_{\mathcal{P}} : \{0,1\}^n \to \{0,1\}$ is such that $E_{\mathcal{P}}(y) = 1 \Leftrightarrow wt(y) = k$.
- $Q^{1/2}(\mathcal{P}) = R_{\oplus}(E_{\mathcal{P}})$
- $R_{\oplus}(E_{\mathcal{P}}) \geq \frac{1}{2} RCC(E_{\mathcal{P}}(x \oplus y))$.
- Known: $RCC(E_{\mathcal{P}}(x \oplus y)) = \Omega(k)$ (Set Disjointness).

$\Omega(k)$ lower bound for k-linearity

- Suppose $\mathcal{P}$ is set of k-linear functions.
- $E_{\mathcal{P}} : \{0,1\}^n \to \{0,1\}$ is such that $E_{\mathcal{P}}(y) = 1 \Leftrightarrow wt(y) = k$.
- $Q^{1/2}(\mathcal{P}) = R_{\oplus}(E_{\mathcal{P}})$
- $R_{\oplus}(E_{\mathcal{P}}) \geq \frac{1}{2} RCC(E_{\mathcal{P}}(x \oplus y))$.
- Known: $RCC(E_{\mathcal{P}}(x \oplus y)) = \Omega(k)$ (Set Disjointness).

$\Omega(k)$ lower bound for k-linearity

- Suppose $\mathcal{P}$ is set of k-linear functions.
- $E_{\mathcal{P}} : \{0,1\}^n \to \{0,1\}$ is such that $E_{\mathcal{P}}(y) = 1 \Leftrightarrow wt(y) = k$.
- $Q^{1/2}(\mathcal{P}) = R_{\oplus}(E_{\mathcal{P}})$
- $R_{\oplus}(E_{\mathcal{P}}) \geq \frac{1}{2} RCC(E_{\mathcal{P}}(x \oplus y))$.
- Known: $RCC(E_{\mathcal{P}}(x \oplus y)) = \Omega(k)$ (Set Disjointness).

Why our proof is interesting?

- Possibility to avoid Set Disjointness.
- Directly compute $R_{\oplus}(E_{\mathcal{P}})$.
- $O(k)$ upper bound on $R_{\oplus}(E_{\mathcal{P}}) \Rightarrow Q^{1/2}(\mathcal{P}) = O(k)$.
- Interesting because $1/2$-testing and ϵ-testing believed to be equally hard for k-linearity.

Why our proof is interesting?

- Possibility to avoid Set Disjointness.
- Directly compute $R_{\oplus}(E_{\mathcal{P}})$.
- $O(k)$ upper bound on $R_{\oplus}(E_{\mathcal{P}}) \Rightarrow Q^{1/2}(\mathcal{P}) = O(k)$.
- Interesting because $1/2$-testing and ϵ-testing believed to be equally hard for k-linearity.

Why our proof is interesting?

- Possibility to avoid Set Disjointness.
- Directly compute $R_{\oplus}(E_{\mathcal{P}})$.
- $O(k)$ upper bound on $R_{\oplus}(E_{\mathcal{P}}) \Rightarrow Q^{1/2}(\mathcal{P}) = O(k)$.
- Interesting because $1/2$-testing and ϵ-testing believed to be equally hard for k-linearity.

Why our proof is interesting?

- Possibility to avoid Set Disjointness.
- Directly compute $R_{\oplus}(E_{\mathcal{P}})$.
- $O(k)$ upper bound on $R_{\oplus}(E_{\mathcal{P}}) \Rightarrow Q^{1/2}(\mathcal{P}) = O(k)$.
- Interesting because $1/2$-testing and ϵ-testing believed to be equally hard for k-linearity.

Outline

Testing affine-isomorphism to $IP_n(x)$

- $IP_n(x) = x_1x_2 + x_3x_4 + \ldots + x_{n-1}x_n$
- $Aff_n(\mathbb{F}_2)$ = Invertible affine transformations.
- Want to test $\mathcal{P} = \{IP_n(x) \circ T | \ T \in Aff_n\}$.
- Consider $\mathcal{P}' = \{IP_n(x) \circ T + c | \ T \in Aff_n, \ c \in \mathbb{F}_2\}$.
- Easy to see: $Q^\epsilon(\mathcal{P}) \geq Q^\epsilon(\mathcal{P}')$.

Testing affine-isomorphism to $IP_n(x)$

- $IP_n(x) = x_1x_2 + x_3x_4 + \ldots + x_{n-1}x_n$
- $Aff_n(\mathbb{F}_2)$ = Invertible affine transformations.
- Want to test $\mathcal{P} = \{IP_n(x) \circ T | \ T \in Aff_n\}$.
- Consider $\mathcal{P}' = \{IP_n(x) \circ T + c | \ T \in Aff_n, \ c \in \mathbb{F}_2\}$.
- Easy to see: $Q^\epsilon(\mathcal{P}) \geq Q^\epsilon(\mathcal{P}')$.

Testing affine-isomorphism to $IP_n(x)$

- $IP_n(x) = x_1x_2 + x_3x_4 + \ldots + x_{n-1}x_n$
- $Aff_n(\mathbb{F}_2)$ = Invertible affine transformations.
- Want to test $\mathcal{P} = \{IP_n(x) \circ T |\ T \in Aff_n\}$.
- Consider $\mathcal{P}' = \{IP_n(x) \circ T + c |\ T \in Aff_n,\ c \in \mathbb{F}_2\}$.
- Easy to see: $Q^\epsilon(\mathcal{P}) \geq Q^\epsilon(\mathcal{P}')$.

Testing affine-isomorphism to $IP_n(x)$

- $IP_n(x) = x_1x_2 + x_3x_4 + \ldots + x_{n-1}x_n$
- $Aff_n(\mathbb{F}_2)$ = Invertible affine transformations.
- Want to test $\mathcal{P} = \{IP_n(x) \circ T |\ T \in Aff_n\}$.
- Consider $\mathcal{P}' = \{IP_n(x) \circ T + c |\ T \in Aff_n,\ c \in \mathbb{F}_2\}$.
- Easy to see: $Q^\epsilon(\mathcal{P}) \geq Q^\epsilon(\mathcal{P}')$.

Testing affine-isomorphism to $IP_n(x)$

- $IP_n(x) = x_1x_2 + x_3x_4 + \ldots + x_{n-1}x_n$
- $Aff_n(\mathbb{F}_2)$ = Invertible affine transformations.
- Want to test $\mathcal{P} = \{IP_n(x) \circ T |\ T \in Aff_n\}$.
- Consider $\mathcal{P}' = \{IP_n(x) \circ T + c |\ T \in Aff_n,\ c \in \mathbb{F}_2\}$.
- Easy to see: $Q^\epsilon(\mathcal{P}) \geq Q^\epsilon(\mathcal{P}')$.

An $\Omega(n^2)$ lower bound for $1/4$-testing

- Sufficient to lower bound $Q^{1/4}(\mathcal{P}')$.
- We show: $E_{\mathcal{P}'} : \{0,1\}^{n^2} \to \{0,1\}$ s.t. $E_{\mathcal{P}'}(G) = 1 \Leftrightarrow Adj(G) \in GL_n(\mathbb{F}_2)$.
- $Q^{1/4}(\mathcal{P}') \geq R_{\oplus}(E_{\mathcal{P}'}) \geq \frac{1}{2} RCC(E_{\mathcal{P}'}(x \oplus y))$.
- Follows from known result: $RCC(E_{\mathcal{P}'}(x \oplus y)) = \Omega(n^2)$.

An $\Omega(n^2)$ lower bound for $1/4$-testing

- Sufficient to lower bound $Q^{1/4}(\mathcal{P}')$.
- We show: $E_{\mathcal{P}'} : \{0,1\}^{n^2} \to \{0,1\}$ s.t. $E_{\mathcal{P}'}(G) = 1 \Leftrightarrow Adj(G) \in GL_n(\mathbb{F}_2)$.
- $Q^{1/4}(\mathcal{P}') \geq R_{\oplus}(E_{\mathcal{P}'}) \geq \frac{1}{2} RCC(E_{\mathcal{P}'}(x \oplus y))$.
- Follows from known result: $RCC(E_{\mathcal{P}'}(x \oplus y)) = \Omega(n^2)$.

An $\Omega(n^2)$ lower bound for $1/4$-testing

- Sufficient to lower bound $Q^{1/4}(\mathcal{P}')$.
- We show: $E_{\mathcal{P}'} : \{0,1\}^{n^2} \to \{0,1\}$ s.t. $E_{\mathcal{P}'}(G) = 1 \Leftrightarrow Adj(G) \in GL_n(\mathbb{F}_2)$.
- $Q^{1/4}(\mathcal{P}') \geq R_{\oplus}(E_{\mathcal{P}'}) \geq \frac{1}{2} RCC(E_{\mathcal{P}'}(x \oplus y))$.
- Follows from known result: $RCC(E_{\mathcal{P}'}(x \oplus y)) = \Omega(n^2)$.

An $\Omega(n^2)$ lower bound for $1/4$-testing

- Sufficient to lower bound $Q^{1/4}(\mathcal{P}')$.
- We show: $E_{\mathcal{P}'} : \{0,1\}^{n^2} \to \{0,1\}$ s.t. $E_{\mathcal{P}'}(G) = 1 \Leftrightarrow Adj(G) \in GL_n(\mathbb{F}_2)$.
- $Q^{1/4}(\mathcal{P}') \geq R_{\oplus}(E_{\mathcal{P}'}) \geq \frac{1}{2} RCC(E_{\mathcal{P}'}(x \oplus y))$.
- Follows from known result: $RCC(E_{\mathcal{P}'}(x \oplus y)) = \Omega(n^2)$.

Summary

- Relating property testing complexity to parity decision tree complexity.
- New proof for $\Omega(k)$ lower bound k-linearity testing.
- $\Omega(n^2)$ lower bound for testing affine-isomorphism to $IP_n(x)$.
- Matches trivial upper bound.

THANK YOU