Low Degree Testing

Seminar in Sublinear Algorithms

Matan Hamilis
matan.hamilis@gmail.com

Reichman University

January 24, 2023

The Plan

1. Introduction
   - Basic Terminology
   - Motivation
2. Background
   - Polynomials
   - Intuition
3. Characterizations
4. Tester

The Plan

1. Introduction
   - Basic Terminology
   - Motivation
2. Background
   - Polynomials
   - Intuition
3. Characterizations
4. Tester

The Plan

The Plan

Notation

- $\mathcal{F}$ denotes some field.
- A variable is denoted by a lowercase letter from the end of the alphabet (e.g x, y, z).
- A constant is denoted by a lowercase letter from the beginning of the alphabet (e.g a, b, c).
- A vector is an overlined lowercase latin letter (e.g $\bar{a}, \bar{x}$).
- $\bar{x}_i$ is the i^{th} coordinate of $\bar{x}$.

Univariate Monomials

Definition (Monomial)

Let x be a variable, and a be a non-zero constant and $d \in \mathbb{N}$. The term ax^d is called a degree d (univariate) monomial.

- When the degree is implicit in the context, we use the term “monomial” without mentioning the degree.
- a is also called coefficient.

Univariate Monomials

Definition (Monomial)

Let x be a variable, and a be a non-zero constant and $d \in \mathbb{N}$. The term ax^d is called a degree d (univariate) monomial.

- When the degree is implicit in the context, we use the term "monomial" without mentioning the degree.
- a is also called coefficient.

Univariate Monomials

Definition (Monomial)

Let x be a variable, and a be a non-zero constant and $d \in \mathbb{N}$. The term ax^d is called a degree d (univariate) monomial.

- When the degree is implicit in the context, we use the term "monomial" without mentioning the degree.
- a is also called coefficient.

Polynomials

Definition (Univariate Polynomial (Alt.))

Let $f : \mathcal{F} \to \mathcal{F}$ be a non-zero function. We say f is a univariate polynomial of degree d if it can be expressed as the non-empty sum of monomials of degree at most d.

- Note: We define the zero polynomial to be of degree ∞, so we shall disregard it in this talk.

Polynomials

Definition (Univariate Polynomial (Alt.))

Let $f : \mathcal{F} \to \mathcal{F}$ be a non-zero function. We say f is a univariate polynomial of degree d if it can be expressed as the non-empty sum of monomials of degree at most d.

- Note: We define the zero polynomial to be of degree ∞, so we shall disregard it in this talk.

Multivariate Monomials

Definition (Monomials)

Let a be a non-zero constant, $x_1, \ldots, x_m$ be m variables over $\mathcal{F}$ and let $d_1, \ldots, d_m \in \mathbb{N}$. Also let $d = \sum_i d_i$. The product $ax_1^{d_1} \cdots x_m^{d_m}$ is called a total degree d multivariate monomial.

- We also call d_i the degree of variable x_i in the monomial.

Example

- $x_1 x_2$ of total degree 2.
- x_1^3 of total degree 3.
- 10 of total degree 0.

Multivariate Monomials

Definition (Monomials)

Let a be a non-zero constant, $x_1, \ldots, x_m$ be m variables over $\mathcal{F}$ and let $d_1, \ldots, d_m \in \mathbb{N}$. Also let $d = \sum_i d_i$. The product $ax_1^{d_1} \cdots x_m^{d_m}$ is called a total degree d multivariate monomial.

- We also call d_i the degree of variable x_i in the monomial.

Example

- $x_1 x_2$ of total degree 2.
- x_1^3 of total degree 3.
- 10 of total degree 0.

Multivariate Monomials

Definition (Monomials)

Let a be a non-zero constant, $x_1, \ldots, x_m$ be m variables over $\mathcal{F}$ and let $d_1, \ldots, d_m \in \mathbb{N}$. Also let $d = \sum_i d_i$. The product $ax_1^{d_1} \cdots x_m^{d_m}$ is called a total degree d multivariate monomial.

- We also call d_i the degree of variable x_i in the monomial.

Example

- $x_1 x_2$ of total degree 2.
- x_1^3 of total degree 3.
- 10 of total degree 0.

Multivariate Polynomials

Definition ((Multivariate) Polynomial)

Let $m \in \mathbb{N}$ and let $f : \mathcal{F}^m \to \mathcal{F}$ be a non-zero function. We say f is a multivariate polynomial of degree d if it can be expressed as a non-empty sum of multivariate monomials of total degree $\leq d$.

Example

$f(x_1, x_2) = 3x_1 + 2x_2^2 x_1 + x_2 x_1$ is a multivariate polynomial of total degree 3.

Multivariate Polynomials

Definition ((Multivariate) Polynomial)

Let $m \in \mathbb{N}$ and let $f : \mathcal{F}^m \to \mathcal{F}$ be a non-zero function. We say f is a multivariate polynomial of degree d if it can be expressed as a non-empty sum of multivariate monomials of total degree $\leq d$.

Example

$f(x_1, x_2) = 3x_1 + 2x_2^2 x_1 + x_2 x_1$ is a multivariate polynomial of total degree 3.

Motivation

- Let $f : \mathcal{F}^m \to \mathcal{F}$ and $d \in \mathbb{N}$.
- Natural Question: Is f a degree $\leq d$ polynomial?
- Observation: We tackled a weaker form of this problem before. (Where?)

Motivation

- Let $f : \mathcal{F}^m \to \mathcal{F}$ and $d \in \mathbb{N}$.
- Natural Question: Is f a degree $\leq d$ polynomial?
- Observation: We tackled a weaker form of this problem before. (Where?)

Motivation

- Let $f : \mathcal{F}^m \to \mathcal{F}$ and $d \in \mathbb{N}$.
- Natural Question: Is f a degree $\leq d$ polynomial?
- Observation: We tackled a weaker form of this problem before. (Where?)

Linear Functions are Polynomials

- Linear functions are degree-1 polynomials.
- Following the BLR theorem, we have built a tester for linearity.
- A natural extension of linearity testing is low degree testing.
- Today: Low degree tester for both univariate and multivariate polynomials.

Linear Functions are Polynomials

- Linear functions are degree-1 polynomials.
- Following the BLR theorem, we have built a tester for linearity.
- A natural extension of linearity testing is low degree testing.
- Today: Low degree tester for both univariate and multivariate polynomials.

Linear Functions are Polynomials

- Linear functions are degree-1 polynomials.
- Following the BLR theorem, we have built a tester for linearity.
- A natural extension of linearity testing is low degree testing.
- Today: Low degree tester for both univariate and multivariate polynomials.

Linear Functions are Polynomials

- Linear functions are degree-1 polynomials.
- Following the BLR theorem, we have built a tester for linearity.
- A natural extension of linearity testing is low degree testing.
- Today: Low degree tester for both univariate and multivariate polynomials.

Notation

- $\mathcal{P}_d$ is the set of univariate polynomials of degree $\leq d$.
- $\mathcal{P}_{m,d}$ is the set of m-variate polynomials of degree $\leq d$.
- d denotes the degree of some polynomial, $d \leq \frac{|\mathcal{F}|}{2}$.
- $f : \mathcal{F}^m \to \mathcal{F}$ an m-variate function.

Notation

- $\mathcal{P}_d$ is the set of univariate polynomials of degree $\leq d$.
- $\mathcal{P}_{m,d}$ is the set of m-variate polynomials of degree $\leq d$.
- d denotes the degree of some polynomial, $d \leq \frac{|\mathcal{F}|}{2}$.
- $f : \mathcal{F}^m \to \mathcal{F}$ an m-variate function.

Notation

- $\mathcal{P}_d$ is the set of univariate polynomials of degree $\leq d$.
- $\mathcal{P}_{m,d}$ is the set of m-variate polynomials of degree $\leq d$.
- d denotes the degree of some polynomial, $d \leq \frac{|\mathcal{F}|}{2}$.
- $f : \mathcal{F}^m \to \mathcal{F}$ an m-variate function.

Notation

- $\mathcal{P}_d$ is the set of univariate polynomials of degree $\leq d$.
- $\mathcal{P}_{m,d}$ is the set of m-variate polynomials of degree $\leq d$.
- d denotes the degree of some polynomial, $d \leq \frac{|\mathcal{F}|}{2}$.
- $f : \mathcal{F}^m \to \mathcal{F}$ an m-variate function.

Basic Properties

Let f, g be two polynomials of degrees d_f, d_g respetively.

- The function $h = f + g$ is a polynomial of degree $\leq \max\{d_f, d_g\}$
- The function $h = f \cdot g$ is a polynomial of degree $d_f + d_g$

Basic Properties

Let f, g be two polynomials of degrees d_f, d_g respetively.

- The function $h = f + g$ is a polynomial of degree $\leq \max\{d_f, d_g\}$
- The function $h = f \cdot g$ is a polynomial of degree $d_f + d_g$

Basic Properties

Let f, g be two polynomials of degrees d_f, d_g respetively.

- The function $h = f + g$ is a polynomial of degree $\leq \max\{d_f, d_g\}$
- The function $h = f \cdot g$ is a polynomial of degree $d_f + d_g$

All Functions Are Polynomials

Lemma

The function $\pi_0 : \mathcal{F} \to \mathcal{F}$*:*

$$\pi_0(x) = \begin{cases} 1 & x = 0 \\ 0 & \textit{otherwise} \end{cases}$$

is a polynomial of degree at most $\leq |F| - 1$

All Functions Are Polynomials

Proof.

$$\pi_0(x) = \overbrace{\prod_{a \in \mathcal{F} \setminus \{0\}} \frac{a - x}{a}}^{|\mathcal{F}| - 1 \text{ polys of deg } 1}$$

$\square$

All Functions Are Polynomials

Lemma

For all $a \in \mathcal{F}$ the function $\pi_a : \mathcal{F} \to \mathcal{F}$:

$$\pi_a(x) = \begin{cases} 1 & x = a \\ 0 & otherwise \end{cases}$$

is a polynomial of degree at most $\leq |F| - 1$

All Functions Are Polynomials

Proof.

$$\pi_a(x) = \pi_0(x - a)$$

$\square$

All Functions Are Polynomials

Theorem

All univariate functions $f : \mathcal{F} \to \mathcal{F}$ can be written as polynomials of degree at most $|\mathcal{F}| - 1$

Proof.

$$f(x) = \sum_{a \in \mathcal{F}} f(a) \cdot \pi_a(x)$$

$\square$

All Functions Are Polynomials

Theorem

All univariate functions $f : \mathcal{F} \to \mathcal{F}$ can be written as polynomials of degree at most $|\mathcal{F}| - 1$

Proof.

$$f(x) = \sum_{a \in \mathcal{F}} f(a) \cdot \pi_a(x)$$

$\square$

All Functions Are Polynomials

Theorem

All multivariate functions $f : \mathcal{F}^m \to \mathcal{F}$ can be written as polynomials of degree at most $m \cdot (|\mathcal{F}| - 1)$

Proof.

- By induction on m. For $m = 1$ we're done.
- Assuming the claim holds for $m - 1$ we prove for m:

$$f(x_1, \ldots, x_{m-1}, x_m) = \sum_{a \in \mathcal{F}} \overbrace{f(x_1, \ldots, x_{m-1}, a)}^{\deg \leq (m-1)\cdot(|\mathcal{F}|-1)} \cdot \pi_a(x)$$

$\square$

All Functions Are Polynomials

Theorem

All multivariate functions $f : \mathcal{F}^m \to \mathcal{F}$ can be written as polynomials of degree at most $m \cdot (|\mathcal{F}| - 1)$

Proof.

- By induction on m. For $m = 1$ we're done.
- Assuming the claim holds for $m - 1$ we prove for m:

$$f(x_1, \ldots, x_{m-1}, x_m) = \sum_{a \in \mathcal{F}} \overbrace{f(x_1, \ldots, x_{m-1}, a)}^{\deg \le (m-1)\cdot(|\mathcal{F}|-1)} \cdot \pi_a(x)$$

$\square$

All Functions Are Polynomials

Theorem

All multivariate functions $f : \mathcal{F}^m \to \mathcal{F}$ can be written as polynomials of degree at most $m \cdot (|\mathcal{F}| - 1)$

Proof.

- By induction on m. For $m = 1$ we're done.
- Assuming the claim holds for $m - 1$ we prove for m:

$$f(x_1, \ldots, x_{m-1}, x_m) = \sum_{a \in \mathcal{F}} \overbrace{f(x_1, \ldots, x_{m-1}, a)}^{\deg \le (m-1)\cdot(|\mathcal{F}|-1)} \cdot \pi_a(x)$$

$\square$

Low Degree Polynomials

Observation

$\frac{|\mathcal{F}|-1}{|\mathcal{F}|}$*-fraction of the functions are of maximal degree.*

Observation

Only $\frac{1}{|\mathcal{F}|^{|\mathcal{F}|-1-d}}$ *fraction of the univariate functions are of degree* $\leq d$.

Definition (low degree polynomial)

A function f is a low degree polynomial if it is of degree $\leq d$.

Low Degree Polynomials

Observation

$\frac{|\mathcal{F}|-1}{|\mathcal{F}|}$*-fraction of the functions are of maximal degree.*

Observation

Only $\frac{1}{|\mathcal{F}|^{|\mathcal{F}|-1-d}}$ *fraction of the univariate functions are of degree* $\leq d$.

Definition (low degree polynomial)

A function f is a low degree polynomial if it is of degree $\leq d$.

Low Degree Polynomials

Observation

$\frac{|\mathcal{F}|-1}{|\mathcal{F}|}$-fraction of the functions are of maximal degree.

Observation

Only $\frac{1}{|\mathcal{F}|^{|\mathcal{F}|-1-d}}$ fraction of the univariate functions are of degree $\leq d$.

Definition (low degree polynomial)

A function f is a low degree polynomial if it is of degree $\leq d$.

Interpolation

- Let $f \in \mathcal{P}_d$ be a univariate polynomial of degree $\leq d$.
- Question: Given evaluations of f, can we reconstruct f's coefficients?
- Question: How many such evaluations do we need?

Theorem (Interpolation)

Let $f \in \mathcal{P}_d$ be a univariate polynomial of degree $\leq d$, then any $d+1$ samples of f suffice to reconstruct the $d+1$ coefficients of f.

Interpolation

- Let $f \in \mathcal{P}_d$ be a univariate polynomial of degree $\leq d$.
- Question: Given evaluations of f, can we reconstruct f's coefficients?
- Question: How many such evaluations do we need?

Theorem (Interpolation)

Let $f \in \mathcal{P}_d$ be a univariate polynomial of degree $\leq d$, then any $d+1$ samples of f suffice to reconstruct the $d+1$ coefficients of f.

Interpolation

- Let $f \in \mathcal{P}_d$ be a univariate polynomial of degree $\leq d$.
- Question: Given evaluations of f, can we reconstruct f's coefficients?
- Question: How many such evaluations do we need?

Theorem (Interpolation)

Let $f \in \mathcal{P}_d$ be a univariate polynomial of degree $\leq d$, then any $d+1$ samples of f suffice to reconstruct the $d+1$ coefficients of f.

Interpolation

- Let $f \in \mathcal{P}_d$ be a univariate polynomial of degree $\leq d$.
- Question: Given evaluations of f, can we reconstruct f's coefficients?
- Question: How many such evaluations do we need?

Theorem (Interpolation)

Let $f \in \mathcal{P}_d$ be a univariate polynomial of degree $\leq d$, then any $d+1$ samples of f suffice to reconstruct the $d+1$ coefficients of f.

Interpolation

Proof.

Assume we have $f(x_0)\dots f(x_d)$ for some distinct set of points $x_0\dots x_d$ then we can obtain f's coefficients $a_0,\dots,a_d$ by solving the following linear equation:

$$\begin{pmatrix} x_0^0 & x_0^1 & \cdots & x_0^d \\ x_1^0 & x_1^1 & \cdots & x_1^d \\ \vdots & \vdots & \ddots & \vdots \\ x_d^0 & x_d^1 & \cdots & x_d^d \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_d \end{pmatrix} = \begin{pmatrix} f(x_0) \\ f(x_1) \\ \vdots \\ f(x_d) \end{pmatrix}$$

$\square$

Roots of a Univariate Polynomials

Definition

Let $f : \mathcal{F}^m \to \mathcal{F} \in \mathcal{P}_{m,d}$ be a univariate polynomial. We say a point $x \in \mathcal{F}^m$ is a root of f if $f(x) = 0$.

Lemma

A univariate polynomial $f \in \mathcal{P}_d$ has a most d roots.

Roots of a Univariate Polynomials

Definition

Let $f : \mathcal{F}^m \to \mathcal{F} \in \mathcal{P}_{m,d}$ be a univariate polynomial. We say a point $x \in \mathcal{F}^m$ is a root of f if $f(x) = 0$.

Lemma

A univariate polynomial $f \in \mathcal{P}_d$ has a most d roots.

Roots of a Univariate Polynomials

Lemma

A univariate polynomial $f \in \mathcal{P}_d$ has a most d roots.

Proof.

- Assume f has $d+1$ roots, $x_0, \ldots, x_d$.
- Using the linear equation systems we obtain its coefficients:

$$\begin{pmatrix} x_0^0 & x_0^1 & \cdots & x_0^d \\ \vdots & \vdots & \ddots & \vdots \\ x_d^0 & x_d^1 & \cdots & x_d^d \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_d \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} f(x_0) \\ \vdots \\ f(x_d) \end{pmatrix}$$

- The only solution is $\bar{0}$, since the matrix is "Vandermonde" so it's invertible.
- Therefore $f \notin \mathcal{P}_d$ since it's the zero-polynomial, contradiction!

$\square$

Roots of a Univariate Polynomials

Lemma

A univariate polynomial $f \in \mathcal{P}_d$ has a most d roots.

Proof.

- Assume f has $d+1$ roots, $x_0, \ldots, x_d$.
- Using the linear equation systems we obtain its coefficients:

$$\begin{pmatrix} x_0^0 & x_0^1 & \cdots & x_0^d \\ \vdots & \vdots & \ddots & \vdots \\ x_d^0 & x_d^1 & \cdots & x_d^d \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_d \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} f(x_0) \\ \vdots \\ f(x_d) \end{pmatrix}$$

- The only solution is $\bar{0}$, since the matrix is "Vandermonde" so it's invertible.
- Therefore $f \notin \mathcal{P}_d$ since it's the zero-polynomial, contradiction!

□

Roots of a Univariate Polynomials

Lemma

A univariate polynomial $f \in \mathcal{P}_d$ has a most d roots.

Proof.

- Assume f has $d+1$ roots, $x_0, \ldots, x_d$.
- Using the linear equation systems we obtain its coefficients:

$$\begin{pmatrix} x_0^0 & x_0^1 & \cdots & x_0^d \\ \vdots & \vdots & \ddots & \vdots \\ x_d^0 & x_d^1 & \cdots & x_d^d \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_d \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} f(x_0) \\ \vdots \\ f(x_d) \end{pmatrix}$$

- The only solution is $\bar{0}$, since the matrix is "Vandermonde" so it's invertible.
- Therefore $f \notin \mathcal{P}_d$ since it's the zero-polynomial, contradiction!

$\square$

Roots of a Univariate Polynomials

Lemma

A univariate polynomial $f \in \mathcal{P}_d$ has a most d roots.

Proof.

- Assume f has $d+1$ roots, $x_0, \ldots, x_d$.
- Using the linear equation systems we obtain its coefficients:

$$\begin{pmatrix} x_0^0 & x_0^1 & \cdots & x_0^d \\ \vdots & \vdots & \ddots & \vdots \\ x_d^0 & x_d^1 & \cdots & x_d^d \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_d \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} f(x_0) \\ \vdots \\ f(x_d) \end{pmatrix}$$

- The only solution is $\bar{0}$, since the matrix is "Vandermonde" so it's invertible.
- Therefore $f \notin \mathcal{P}_d$ since it's the zero-polynomial, contradiction!

$\square$

Schwartz-Zippel Lemma

- What about number of roots of multivariate polynomial?
- The following is given without a proof.

Theorem

Let $p : \mathcal{F}^m \to \mathcal{F}$ be a non-zero m-variate polynomial of total degree d over finite field $\mathcal{F}$. Then,

$$\mathbf{Pr}_{x \in \mathcal{F}^m}[p(x) = 0] \leq \frac{d}{|\mathcal{F}|}$$

Schwartz-Zippel Lemma

- What about number of roots of multivariate polynomial?
- The following is given without a proof.

Theorem

Let $p : \mathcal{F}^m \to \mathcal{F}$ be a non-zero m-variate polynomial of total degree d over finite field $\mathcal{F}$. Then,

$$\mathbf{Pr}_{x \in \mathcal{F}^m}[p(x) = 0] \leq \frac{d}{|\mathcal{F}|}$$

Schwartz-Zippel Lemma

- What about number of roots of multivariate polynomial?
- The following is given without a proof.

Theorem

Let $p : \mathcal{F}^m \rightarrow \mathcal{F}$ be a non-zero m-variate polynomial of total degree d over finite field $\mathcal{F}$. Then,

$$\mathbf{Pr}_{x \in \mathcal{F}^m}[p(x) = 0] \leq \frac{d}{|\mathcal{F}|}$$

Intermission

- Reminder: Our goal is to build a tester for the property of a function being a low-degree polynomial.
- To give some intuition we shall begin with describing a tester for univariate polynomials.
- Next, we will present the full multivariate tester.

Intermission

- Reminder: Our goal is to build a tester for the property of a function being a low-degree polynomial.
- To give some intuition we shall begin with describing a tester for univariate polynomials.
- Next, we will present the full multivariate tester.

Intermission

- Reminder: Our goal is to build a tester for the property of a function being a low-degree polynomial.
- To give some intuition we shall begin with describing a tester for univariate polynomials.
- Next, we will present the full multivariate tester.

Property Testing — Notation

- Since we present a tester in this talk, we remind a few useful notations.
- For functions $f, f' : \mathcal{F}^m \to \mathcal{F}$ the (normalized) distance between f, f' is defined:

$$\delta(f, f') = \frac{|\{x : f(x) \neq f'(x)\}|}{|\mathcal{F}|^m}$$

- For property Π the distance of a function f from Π is defined:

$$\Delta_\Pi(f) = \min_{f' \in \Pi}\{\delta(f, f')\}$$

Property Testing — Notation

- Since we present a tester in this talk, we remind a few useful notations.
- For functions $f, f' : \mathcal{F}^m \to \mathcal{F}$ the (normalized) distance between f, f' is defined:

$$\delta(f, f') = \frac{|\{x : f(x) \neq f'(x)\}|}{|\mathcal{F}|^m}$$

- For property Π the distance of a function f from Π is defined:

$$\Delta_\Pi(f) = \min_{f' \in \Pi}\{\delta(f, f')\}$$

Property Testing — Notation

- Since we present a tester in this talk, we remind a few useful notations.
- For functions $f, f' : \mathcal{F}^m \to \mathcal{F}$ the (normalized) distance between f, f' is defined:

$$\delta(f, f') = \frac{|\{x : f(x) \neq f'(x)\}|}{|\mathcal{F}|^m}$$

- For property Π the distance of a function f from Π is defined:

$$\Delta_\Pi(f) = \min_{f' \in \Pi}\{\delta(f, f')\}$$

Intuition

- For the univariate case consider the following tester:
  1. Samples $d+2$ points $x_1, \ldots, x_{d+2} \in \mathcal{F}$
  2. Interpolates a degree d polynomial p from $x_1, \ldots, x_{d+1}$ and $f(x_1), \ldots, f(x_{d+1})$
  3. Checks $p(x_{d+2}) = f(x_{d+2})$
- If f is low degree, the tester always accepts.
- If f is not low degree then probability of x_{d+2} being a point of disagreement between f and p is at least:

$$\frac{\delta(f,p)\cdot|\mathcal{F}|}{|\mathcal{F}|-(d+1)} > \delta(f,p) \geq \Delta_{\mathcal{P}_d}(f) = \epsilon$$

Intuition

- For the univariate case consider the following tester:
  1. Samples $d+2$ points $x_1, \ldots, x_{d+2} \in \mathcal{F}$
  2. Interpolates a degree d polynomial p from $x_1, \ldots, x_{d+1}$ and $f(x_1), \ldots, f(x_{d+1})$
  3. Checks $p(x_{d+2}) = f(x_{d+2})$
- If f is low degree, the tester always accepts.
- If f is not low degree then probability of x_{d+2} being a point of disagreement between f and p is at least:

$$\frac{\delta(f,p)\cdot|\mathcal{F}|}{|\mathcal{F}|-(d+1)} > \delta(f,p) \geq \Delta_{\mathcal{P}_d}(f) = \epsilon$$

Intuition

- For the univariate case consider the following tester:
  1. Samples $d+2$ points $x_1, \ldots, x_{d+2} \in \mathcal{F}$
  2. Interpolates a degree d polynomial p from $x_1, \ldots, x_{d+1}$ and $f(x_1), \ldots, f(x_{d+1})$
  3. Checks $p(x_{d+2}) = f(x_{d+2})$
- If f is low degree, the tester always accepts.
- If f is not low degree then probability of x_{d+2} being a point of disagreement between f and p is at least:

$$\frac{\delta(f,p) \cdot |\mathcal{F}|}{|\mathcal{F}| - (d+1)} > \delta(f,p) \geq \Delta_{\mathcal{P}_d}(f) = \epsilon$$

Intuition

- For the univariate case consider the following tester:
  1. Samples $d+2$ points $x_1, \ldots, x_{d+2} \in \mathcal{F}$
  2. Interpolates a degree d polynomial p from $x_1, \ldots, x_{d+1}$ and $f(x_1), \ldots, f(x_{d+1})$
  3. Checks $p(x_{d+2}) = f(x_{d+2})$
- If f is low degree, the tester always accepts.
- If f is not low degree then probability of x_{d+2} being a point of disagreement between f and p is at least:

$$\frac{\delta(f,p) \cdot |\mathcal{F}|}{|\mathcal{F}| - (d+1)} > \delta(f,p) \geq \Delta_{\mathcal{P}_d}(f) = \epsilon$$

Intuition

- For the univariate case consider the following tester:
  1. Samples $d+2$ points $x_1, \ldots, x_{d+2} \in \mathcal{F}$
  2. Interpolates a degree d polynomial p from $x_1, \ldots, x_{d+1}$ and $f(x_1), \ldots, f(x_{d+1})$
  3. Checks $p(x_{d+2}) = f(x_{d+2})$
- If f is low degree, the tester always accepts.
- If f is not low degree then probability of x_{d+2} being a point of disagreement between f and p is at least:

$$\frac{\delta(f,p) \cdot |\mathcal{F}|}{|\mathcal{F}| - (d+1)} > \delta(f,p) \geq \Delta_{\mathcal{P}_d}(f) = \epsilon$$

Intuition

- For the univariate case consider the following tester:
  1. Samples $d+2$ points $x_1, \ldots, x_{d+2} \in \mathcal{F}$
  2. Interpolates a degree d polynomial p from $x_1, \ldots, x_{d+1}$ and $f(x_1), \ldots, f(x_{d+1})$
  3. Checks $p(x_{d+2}) = f(x_{d+2})$
- If f is low degree, the tester always accepts.
- If f is not low degree then probability of x_{d+2} being a point of disagreement between f and p is at least:

$$\frac{\delta(f,p)\cdot|\mathcal{F}|}{|\mathcal{F}|-(d+1)} > \delta(f,p) \geq \Delta_{\mathcal{P}_d}(f) = \epsilon$$

Lower Bound?

Theorem

No univariate low-degree tester exists which makes less than $d + 2$ queries.

Proof.

(sketch, "Yao's minimax-principle") $d + 1$ queries convey no information. That is, given $d + 1$ queries' responses we can show that there exist two functions f_1, f_2 that both agree on the responses of the queries, but $\deg(f_1) \leq d$ and $\deg(f_2) = |\mathcal{F}| - 1$. $\square$

Lines

- It can be a bit difficult generalizing the foregoing tester for multivariate setting.
- We give an alternative tester that will form the basis for the generalized, multivariate tester.
- The alternative tester is based on querying the first $d+2$ points over a random line.
- A *line* is parametrized by two values $r, s \in \mathcal{F}$ and is made of the solutions $y$to the linear equation $y = r + s \cdot x$ for $x \in \mathcal{F}$.

Lines

- It can be a bit difficult generalizing the foregoing tester for multivariate setting.
- We give an alternative tester that will form the basis for the generalized, multivariate tester.
- The alternative tester is based on querying the first $d + 2$ points over a random line.
- A *line* is parametrized by two values $r, s \in \mathcal{F}$ and is made of the solutions $y$to the linear equation $y = r + s \cdot x$ for $x \in \mathcal{F}$.

Lines

- It can be a bit difficult generalizing the foregoing tester for multivariate setting.
- We give an alternative tester that will form the basis for the generalized, multivariate tester.
- The alternative tester is based on querying the first $d+2$ points over a random line.
- A *line* is parametrized by two values $r, s \in \mathcal{F}$ and is made of the solutions $y$to the linear equation $y = r + s \cdot x$ for $x \in \mathcal{F}$.

Lines

- It can be a bit difficult generalizing the foregoing tester for multivariate setting.
- We give an alternative tester that will form the basis for the generalized, multivariate tester.
- The alternative tester is based on querying the first $d+2$ points over a random line.
- A *line* is parametrized by two values $r, s \in \mathcal{F}$ and is made of the solutions $y$to the linear equation $y = r + s \cdot x$ for $x \in \mathcal{F}$.

Alternative Tester

- We devise the following tester:
  1. Sample $r, s \leftarrow \mathcal{F}$ uniformly.
  2. Query the points $\{r + s \cdot i\}_{i \in \{0,\dots,d+1\}}$.
  3. Make sure the $d + 2$ points interpolate into a degree d polynomial.
- Obviously, if f is low degree, the tester accepts.
- However, if f is ϵ-far from being low degree, how many random lines will fail the test?
- The answer to this question is special case of the following multivariate tester.
- It is also the core result of this talk.

Alternative Tester

- We devise the following tester:
  1. Sample $r, s \leftarrow \mathcal{F}$ uniformly.
  2. Query the points $\{r + s \cdot i\}_{i \in \{0,\ldots,d+1\}}$.
  3. Make sure the $d + 2$ points interpolate into a degree d polynomial.
- Obviously, if f is low degree, the tester accepts.
- However, if f is ϵ-far from being low degree, how many random lines will fail the test?
- The answer to this question is special case of the following multivariate tester.
- It is also the core result of this talk.

Alternative Tester

- We devise the following tester:
  1. Sample $r, s \leftarrow \mathcal{F}$ uniformly.
  2. Query the points $\{r + s \cdot i\}_{i \in \{0, \ldots, d+1\}}$.
  3. Make sure the $d + 2$ points interpolate into a degree d polynomial.
- Obviously, if f is low degree, the tester accepts.
- However, if f is ϵ-far from being low degree, how many random lines will fail the test?
- The answer to this question is special case of the following multivariate tester.
- It is also the core result of this talk.

Alternative Tester

- We devise the following tester:
    1. Sample $r, s \leftarrow \mathcal{F}$ uniformly.
    2. Query the points $\{r + s \cdot i\}_{i \in \{0, \ldots, d+1\}}$.
    3. Make sure the $d + 2$ points interpolate into a degree d polynomial.
- Obviously, if f is low degree, the tester accepts.
- However, if f is ϵ-far from being low degree, how many random lines will fail the test?
- The answer to this question is special case of the following multivariate tester.
- It is also the core result of this talk.

Alternative Tester

- We devise the following tester:
  1. Sample $r, s \leftarrow \mathcal{F}$ uniformly.
  2. Query the points $\{r + s \cdot i\}_{i \in \{0,\ldots,d+1\}}$.
  3. Make sure the $d + 2$ points interpolate into a degree d polynomial.
- Obviously, if f is low degree, the tester accepts.
- However, if f is ϵ-far from being low degree, how many random lines will fail the test?
- The answer to this question is special case of the following multivariate tester.
- It is also the core result of this talk.

Alternative Tester

- We devise the following tester:
  1. Sample $r, s \leftarrow \mathcal{F}$ uniformly.
  2. Query the points $\{r + s \cdot i\}_{i \in \{0,\ldots,d+1\}}$.
  3. Make sure the $d+2$ points interpolate into a degree d polynomial.
- Obviously, if f is low degree, the tester accepts.
- However, if f is ϵ-far from being low degree, how many random lines will fail the test?
- The answer to this question is special case of the following multivariate tester.
- It is also the core result of this talk.

Alternative Tester

- We devise the following tester:
  1. Sample $r, s \leftarrow \mathcal{F}$ uniformly.
  2. Query the points $\{r + s \cdot i\}_{i \in \{0,\dots,d+1\}}$.
  3. Make sure the $d + 2$ points interpolate into a degree d polynomial.
- Obviously, if f is low degree, the tester accepts.
- However, if f is ϵ-far from being low degree, how many random lines will fail the test?
- The answer to this question is special case of the following multivariate tester.
- It is also the core result of this talk.

Alternative Tester

- We devise the following tester:
  1. Sample $r, s \leftarrow \mathcal{F}$ uniformly.
  2. Query the points $\{r + s \cdot i\}_{i \in \{0,\ldots,d+1\}}$.
  3. Make sure the $d + 2$ points interpolate into a degree d polynomial.
- Obviously, if f is low degree, the tester accepts.
- However, if f is ϵ-far from being low degree, how many random lines will fail the test?
- The answer to this question is special case of the following multivariate tester.
- It is also the core result of this talk.

Multivariate Tester

- In the multivariate setting we are given $f : \mathcal{F}^m \to \mathcal{F}$.
- We will apply the line-based approach.

Definition

A *line* in $\mathcal{F}^m$ is a ($|\mathcal{F}|$ long) sequence of the form $\left(\bar{x} + i\bar{h}\right)_{i \in \mathcal{F}}$ for some $\bar{x}, \bar{h} \in \mathcal{F}^m$.

- It's easy to see that if f is low degree, then its restriction to any line is a low degree univariate polynomial.
- We'll later see that the opposite direction is also correct, if restriction to all lines is low degree univariate, then f is low degree.

Multivariate Tester

- In the multivariate setting we are given $f : \mathcal{F}^m \to \mathcal{F}$.
- We will apply the line-based approach.

Definition

A *line* in $\mathcal{F}^m$ is a ($|\mathcal{F}|$ long) sequence of the form $\left(\bar{x} + i\bar{h}\right)_{i \in \mathcal{F}}$ for some $\bar{x}, \bar{h} \in \mathcal{F}^m$.

- It's easy to see that if f is low degree, then its restriction to any line is a low degree univariate polynomial.
- We'll later see that the opposite direction is also correct, if restriction to all lines is low degree univariate, then f is low degree.

Multivariate Tester

- In the multivariate setting we are given $f : \mathcal{F}^m \to \mathcal{F}$.
- We will apply the line-based approach.

Definition

A *line* in $\mathcal{F}^m$ is a ($|\mathcal{F}|$ long) sequence of the form $\left(\bar{x} + i\bar{h}\right)_{i \in \mathcal{F}}$ for some $\bar{x}, \bar{h} \in \mathcal{F}^m$.

- It's easy to see that if f is low degree, then its restriction to any line is a low degree univariate polynomial.
- We'll later see that the opposite direction is also correct, if restriction to all lines is low degree univariate, then f is low degree.

Multivariate Tester

- In the multivariate setting we are given $f : \mathcal{F}^m \to \mathcal{F}$.
- We will apply the line-based approach.

Definition

A *line* in $\mathcal{F}^m$ is a ($|\mathcal{F}|$ long) sequence of the form $\left(\bar{x} + i\bar{h}\right)_{i\in\mathcal{F}}$ for some $\bar{x}, \bar{h} \in \mathcal{F}^m$.

- It's easy to see that if f is low degree, then its restriction to any line is a low degree univariate polynomial.
- We'll later see that the opposite direction is also correct, if restriction to all lines is low degree univariate, then f is low degree.

Multivariate Tester

- In the multivariate setting we are given $f : \mathcal{F}^m \to \mathcal{F}$.
- We will apply the line-based approach.

Definition

A *line* in $\mathcal{F}^m$ is a ($|\mathcal{F}|$ long) sequence of the form $\left(\bar{x} + i\bar{h}\right)_{i \in \mathcal{F}}$ for some $\bar{x}, \bar{h} \in \mathcal{F}^m$.

- It's easy to see that if f is low degree, then its restriction to any line is a low degree univariate polynomial.
- We'll later see that the opposite direction is also correct, if restriction to all lines is low degree univariate, then f is low degree.

Suggestion (or dead end?)

- It would be natural to suggest the following multivariate tester:
  1. Select a random line in $\mathcal{F}^m$.
  2. Test that f restricted to the line is low degree univariate.
- Obviously, if f is low degree, the tester accepts.
- But if f is ϵ-far, how many lines will result in a rejection?

Suggestion (or dead end?)

- It would be natural to suggest the following multivariate tester:
  1. Select a random line in $\mathcal{F}^m$.
  2. Test that f restricted to the line is low degree univariate.
- Obviously, if f is low degree, the tester accepts.
- But if f is ϵ-far, how many lines will result in a rejection?

Suggestion (or dead end?)

- It would be natural to suggest the following multivariate tester:
  1. Select a random line in $\mathcal{F}^m$.
  2. Test that f restricted to the line is low degree univariate.
- Obviously, if f is low degree, the tester accepts.
- But if f is ϵ-far, how many lines will result in a rejection?

Suggestion (or dead end?)

- It would be natural to suggest the following multivariate tester:
    1. Select a random line in $\mathcal{F}^m$.
    2. Test that f restricted to the line is low degree univariate.
- Obviously, if f is low degree, the tester accepts.
- But if f is ϵ-far, how many lines will result in a rejection?

Suggestion (or dead end?)

- It would be natural to suggest the following multivariate tester:
  1. Select a random line in $\mathcal{F}^m$.
  2. Test that f restricted to the line is low degree univariate.
- Obviously, if f is low degree, the tester accepts.
- But if f is ϵ-far, how many lines will result in a rejection?

Intuition - Summary

- Spoiler: The multivariate tester is exactly the tester we've just seen.
- We'll have to prove two main theorems.
- First, that in the univariate case, taking to a random line and testing the first $d + 2$ points has good rejection probability.
- Second, in the multivariate when reducing the test to the univariate case via a random line, then with good probability most lines will reject.

Intuition - Summary

- Spoiler: The multivariate tester is exactly the tester we've just seen.
- We'll have to prove two main theorems.
- First, that in the univariate case, taking to a random line and testing the first $d+2$ points has good rejection probability.
- Second, in the multivariate when reducing the test to the univariate case via a random line, then with good probability most lines will reject.

Intuition - Summary

- Spoiler: The multivariate tester is exactly the tester we've just seen.
- We'll have to prove two main theorems.
- First, that in the univariate case, taking to a random line and testing the first $d + 2$ points has good rejection probability.
- Second, in the multivariate when reducing the test to the univariate case via a random line, then with good probability most lines will reject.

Intuition - Summary

- Spoiler: The multivariate tester is exactly the tester we've just seen.
- We'll have to prove two main theorems.
- First, that in the univariate case, taking to a random line and testing the first $d+2$ points has good rejection probability.
- Second, in the multivariate when reducing the test to the univariate case via a random line, then with good probability most lines will reject.

Notation

- $L_{\bar{x},\bar{h}} \stackrel{\text{def}}{=} \left(\bar{x} + i\bar{h}\right)_{i \in \mathcal{F}}$, a line parametrized by $\bar{x}, \bar{h}$.

Definition

The restriction of f to the line $L_{\bar{x},\bar{h}}$ is a the polynomial p such that $p(i) = f\left(\bar{x} + i\bar{h}\right)$ for every $i \in \mathcal{F}$.

Local Characterization (Multivariate Polynomials)

Theorem

Let $|F| > 2d$. The function $f : \mathcal{F}^m \to \mathcal{F}$ is in $\mathcal{P}_{m,d}$ if and only if for every $\bar{x}, \bar{h} \in \mathcal{F}^m$ there exists a degree-d univariate polynomial $p_{\bar{x},\bar{h}}$ such that $p_{\bar{x},\bar{h}} = f\left(\bar{x} + i\bar{h}\right)$ for every $i \in \mathcal{F}$.

Proof $\Rightarrow$

Proof.

First direction is simple. For every $\bar{x} = (x_1, \ldots, x_m)$ and $\bar{h} = (h_1, \ldots, h_m)$ we have:

$$f\left(\bar{x} + z\bar{h}\right) = f(x_1 + zh_1, \ldots, x_m + zh_m)$$

is univariate of degree d in z. $\square$

Proof $\Leftarrow$

Proof.

The other direction is less trivial, we'll use the induction + probabilistic method.

- Assume $\deg(f) \leq 2d < |\mathcal{F}|$ for now.
- For any all $\bar{h} \in \mathcal{F}$, let $g_{\bar{h}}(z) = f(z\bar{h})$, the restriction of f to line $L_{0,\bar{h}}$.
- $g_{\bar{h}}$ is of degree $\leq d$.
- The coefficient of $z^{\deg(f)}$ is a (multivariate) polynomial in $\bar{h}$ of degree $\leq 2d$, $c(\bar{h})$.
- Therefore, from Schwartz-Zippel lemma $\mathbf{Pr}_{\bar{h}\in\mathcal{F}^m}\left[c(\bar{h}) \neq 0\right] > 1 - \frac{\deg(f)}{|\mathcal{F}|} > 0$.
- Since the probability over $\bar{h}$ is positive, there exists such $\bar{h}^*$ for which $d \geq \deg(g_{\bar{h}^*}) = \deg(f)$.

$\square$

Proof $\Leftarrow$

Proof.

The other direction is less trivial, we'll use the induction + probabilistic method.

- Assume $\deg(f) \leq 2d < |\mathcal{F}|$ for now.
- For any all $\bar{h} \in \mathcal{F}$, let $g_{\bar{h}}(z) = f(z\bar{h})$, the restriction of f to line $L_{0,\bar{h}}$.
- $g_{\bar{h}}$ is of degree $\leq d$.
- The coefficient of $z^{\deg(f)}$ is a (multivariate) polynomial in $\bar{h}$ of degree $\leq 2d$, $c(\bar{h})$.
- Therefore, from Schwartz-Zippel lemma $\mathbf{Pr}_{\bar{h}\in\mathcal{F}^m}[c(\bar{h}) \neq 0] > 1 - \frac{\deg(f)}{|\mathcal{F}|} > 0$.
- Since the probability over $\bar{h}$ is positive, there exists such $\bar{h}^*$ for which $d \geq \deg(g_{\bar{h}^*}) = \deg(f)$.

$\square$

Proof $\Leftarrow$

Proof.

The other direction is less trivial, we'll use the induction + probabilistic method.

- Assume $\deg(f) \leq 2d < |\mathcal{F}|$ for now.
- For any all $\bar{h} \in \mathcal{F}$, let $g_{\bar{h}}(z) = f(z\bar{h})$, the restriction of f to line $L_{0,\bar{h}}$.
- $g_{\bar{h}}$ is of degree $\leq d$.
- The coefficient of $z^{\deg(f)}$ is a (multivariate) polynomial in $\bar{h}$ of degree $\leq 2d$, $c(\bar{h})$.
- Therefore, from Schwartz-Zippel lemma $\mathbf{Pr}_{\bar{h}\in\mathcal{F}^m}\left[c(\bar{h}) \neq 0\right] > 1 - \frac{\deg(f)}{|\mathcal{F}|} > 0$.
- Since the probability over $\bar{h}$ is positive, there exists such $\bar{h}^*$ for which $d \geq \deg(g_{\bar{h}^*}) = \deg(f)$.

$\square$

Proof $\Leftarrow$

Proof.

The other direction is less trivial, we'll use the induction + probabilistic method.

- Assume $\deg(f) \leq 2d < |\mathcal{F}|$ for now.
- For any all $\bar{h} \in \mathcal{F}$, let $g_{\bar{h}}(z) = f(z\bar{h})$, the restriction of f to line $L_{0,\bar{h}}$.
- $g_{\bar{h}}$ is of degree $\leq d$.
- The coefficient of $z^{\deg(f)}$ is a (multivariate) polynomial in $\bar{h}$ of degree $\leq 2d$, $c(\bar{h})$.
- Therefore, from Schwartz-Zippel lemma $\mathbf{Pr}_{\bar{h}\in\mathcal{F}^m}[c(\bar{h}) \neq 0] > 1 - \frac{\deg(f)}{|\mathcal{F}|} > 0$.
- Since the probability over $\bar{h}$ is positive, there exists such $\bar{h}^*$ for which $d \geq \deg(g_{\bar{h}^*}) = \deg(f)$.

$\square$

Proof $\Leftarrow$

Proof.

The other direction is less trivial, we'll use the induction + probabilistic method.

- Assume $\deg(f) \leq 2d < |\mathcal{F}|$ for now.
- For any all $\bar{h} \in \mathcal{F}$, let $g_{\bar{h}}(z) = f(z\bar{h})$, the restriction of f to line $L_{0,\bar{h}}$.
- $g_{\bar{h}}$ is of degree $\leq d$.
- The coefficient of $z^{\deg(f)}$ is a (multivariate) polynomial in $\bar{h}$ of degree $\leq 2d$, $c(\bar{h})$.
- Therefore, from Schwartz-Zippel lemma $\mathbf{Pr}_{\bar{h}\in\mathcal{F}^m}[c(\bar{h}) \neq 0] > 1 - \frac{\deg(f)}{|\mathcal{F}|} > 0$.
- Since the probability over $\bar{h}$ is positive, there exists such $\bar{h}^*$ for which $d \geq \deg(g_{\bar{h}^*}) = \deg(f)$.

$\square$

Proof $\Leftarrow$

Proof.

The other direction is less trivial, we'll use the induction + probabilistic method.

- Assume $\deg(f) \le 2d < |\mathcal{F}|$ for now.
- For any all $\bar{h} \in \mathcal{F}$, let $g_{\bar{h}}(z) = f(z\bar{h})$, the restriction of f to line $L_{0,\bar{h}}$.
- $g_{\bar{h}}$ is of degree $\le d$.
- The coefficient of $z^{\deg(f)}$ is a (multivariate) polynomial in $\bar{h}$ of degree $\le 2d$, $c(\bar{h})$.
- Therefore, from Schwartz-Zippel lemma $\mathbf{Pr}_{\bar{h}\in\mathcal{F}^m}\left[c(\bar{h}) \neq 0\right] > 1 - \frac{\deg(f)}{|\mathcal{F}|} > 0$.
- Since the probability over $\bar{h}$ is positive, there exists such $\bar{h}^*$ for which $d \ge \deg(g_{\bar{h}^*}) = \deg(f)$.

$\square$

Proof $\Leftarrow$

Proof.

- We now prove that $\leq 2d$.
- For each $e \in \{0, \ldots, d\}$ let $f_e(x_1, \ldots, x_{m-1}) = f(x_1, \ldots, x_{m-1}, e)$.
- $f_e(\bar{x})$ is an $m-1$-variate polynomial, by induction hypothesis (of the whole theorem), it is of degree $\leq d$.
- For any $e \in \{0, \ldots, d\}$, let $\delta_e(x)$ by a degree d polynomial such that $\delta_e(e) = 1$ and $\delta_e(e') = 0$ for $e' \in \{0, \ldots, d\} \setminus \{e\}$.

$\square$

PROOF $\Leftarrow$

- For any $e_1, \dots, e_{m-1}$ it holds that:

$$f(e_1, \dots, e_{m-1}, x) = \sum_{e=0}^{d} \delta_e(x) f_e(e_1, \dots, e_{m-1})$$

- Notice both sides are degree d polynomials that agree on $d+1$ points: $\{0, \dots, d\}$.
- Since the foregoing equality holds for all $e_1, \dots, e_{m-1}$ we conclude:

$$f(x_1, \dots, x_{m-1}, x_m) = \sum_{e=0}^{d} \overbrace{\delta_e(x_m)}^{\deg \leq d} \overbrace{f_e(x_1, \dots, x_{m-1})}^{\deg \leq d}$$

Proof $\Leftarrow$

- For any $e_1, \ldots, e_{m-1}$ it holds that:

$$f(e_1, \ldots, e_{m-1}, x) = \sum_{e=0}^{d} \delta_e(x) f_e(e_1, \ldots, e_{m-1})$$

- Notice both sides are degree d polynomials that agree on $d+1$ points: $\{0, \ldots, d\}$.
- Since the foregoing equality holds for all $e_1, \ldots, e_{m-1}$ we conclude:

$$f(x_1, \ldots, x_{m-1}, x_m) = \sum_{e=0}^{d} \overbrace{\delta_e(x_m)}^{\deg \leq d} \overbrace{f_e(x_1, \ldots, x_{m-1})}^{\deg \leq d}$$

Proof $\Leftarrow$

- For any $e_1, \ldots, e_{m-1}$ it holds that:

$$f(e_1, \ldots, e_{m-1}, x) = \sum_{e=0}^{d} \delta_e(x) f_e(e_1, \ldots, e_{m-1})$$

- Notice both sides are degree d polynomials that agree on $d+1$ points: $\{0, \ldots, d\}$.
- Since the foregoing equality holds for all $e_1, \ldots, e_{m-1}$ we conclude:

$$f(x_1, \ldots, x_{m-1}, x_m) = \sum_{e=0}^{d} \overbrace{\delta_e(x_m)}^{\deg \leq d} \overbrace{f_e(x_1, \ldots, x_{m-1})}^{\deg \leq d}$$

Conclusions

- We've seen a "local" characterization of multivariate polynomial as a conjunction of $|\mathcal{F}|^{2m}$ constraints.
- However, these constraints are still not local, as the multivariate polynomial restricted to any line still refers to $|F|$ values of the tested function as a univariate polynomial.
- We will now give a local characterization of univariate polynomials as a conjunction of $|F|^2$ constraints, each referring only to $d+2$ values of the function.

Conclusions

- We've seen a "local" characterization of multivariate polynomial as a conjunction of $|\mathcal{F}|^{2m}$ constraints.
- However, these constraints are still not local, as the multivariate polynomial restricted to any line still refers to $|F|$ values of the tested function as a univariate polynomial.
- We will now give a local characterization of univariate polynomials as a conjunction of $|F|^2$ constraints, each referring only to $d+2$ values of the function.

Conclusions

- We've seen a "local" characterization of multivariate polynomial as a conjunction of $|\mathcal{F}|^{2m}$ constraints.
- However, these constraints are still not local, as the multivariate polynomial restricted to any line still refers to $|F|$ values of the tested function as a univariate polynomial.
- We will now give a local characterization of univariate polynomials as a conjunction of $|F|^2$ constraints, each referring only to $d + 2$ values of the function.

A claim on deriviatives

- We start with a claim on *deriviatives*.

Definition

For a function $g : \mathcal{F} \to \mathcal{F}$, the deriviative of g is the function g' such that: $g'(x) \stackrel{\text{def}}{=} g(x+1) - g(x)$

Theorem

A function g is of degree exactly $d > 0$ if and only if its deriviate is of degree exactly $d-1$.

A claim on deriviatives

- We start with a claim on *deriviatives*.

Definition

For a function $g : \mathcal{F} \to \mathcal{F}$, the deriviative of g is the function g' such that:
$g'(x) \stackrel{\text{def}}{=} g(x+1) - g(x)$

Theorem

A function g is of degree exactly $d > 0$ if and only if its deriviate is of degree exactly $d-1$.

A claim on deriviatives

- We start with a claim on *deriviatives*.

Definition

For a function $g : \mathcal{F} \to \mathcal{F}$, the deriviative of g is the function g' such that:
$g'(x) \stackrel{\text{def}}{=} g(x+1) - g(x)$

Theorem

A function g is of degree exactly $d > 0$ if and only if its deriviate is of degree exactly $d - 1$.

Proof about derivatives

Proof.

Write $g(x) = \sum_{j=0}^{d} c_j x^j$

$$g'(x) = \sum_{j=0}^{d} c_j \cdot (x+1)^j - \sum_{j=0}^{d} c_j \cdot x^j$$

$$= \sum_{j=0}^{d} c_j \cdot \left((x+1)^j - x^j\right)$$

$$= \sum_{j=0}^{d} c_j \cdot \sum_{k=0}^{j-1} \binom{j}{k} \cdot x^k \qquad \Leftarrow \text{coefficient of } x^{d-1} \text{ is } c_d \cdot d \neq 0$$

$\square$

Local Characterization - Univariate Polynomials

- Notation: $\alpha_i = (-1)^{i+1} \cdot \binom{d+1}{i}$

Theorem

A univariate polynomial $g : \mathcal{F} \to \mathcal{F}$ has degree $\leq d < |\mathcal{F}|$ if any only if for every $e \in \mathcal{F}$ it holds that:

$$\sum_{i=0}^{d+1} \alpha_i \cdot g(e+i) = 0$$

Proof

Proof.

- By induction on d. If $d = 0$ the function is constant, therefore $-g(e) + g(e+1) = 0$ for all $e \in \mathcal{F}$.
- For induction step, $\deg(g) = d$ therefore $\deg(g') = d - 1$
- From induction hypothesis, since $\deg(g') = d - 1$ then $\sum_{i=0}^{d} (-1)^{i+1} \cdot \binom{d}{i} \cdot g'(e+i) = 0$ for all $e \in \mathcal{F}$.
- So we know that $\deg(g) = d$ if and only if

$$\sum_{i=0}^{d} (-1)^{i+1} \cdot \binom{d}{i} \cdot (g(e+i+1) - g(e+i)) = 0$$

$\square$

Proof

Proof.

- By induction on d. If $d = 0$ the function is constant, therefore $-g(e) + g(e+1) = 0$ for all $e \in \mathcal{F}$.
- For induction step, $\deg(g) = d$ therefore $\deg(g') = d - 1$
- From induction hypothesis, since $\deg(g') = d - 1$ then $\sum_{i=0}^{d} (-1)^{i+1} \cdot \binom{d}{i} \cdot g'(e+i) = 0$ for all $e \in \mathcal{F}$.
- So we know that $\deg(g) = d$ if and only if

$$\sum_{i=0}^{d} (-1)^{i+1} \cdot \binom{d}{i} \cdot (g(e+i+1) - g(e+i)) = 0$$

$\square$

Proof

Proof.

- By induction on d. If $d = 0$ the function is constant, therefore $-g(e) + g(e+1) = 0$ for all $e \in \mathcal{F}$.
- For induction step, $\deg(g) = d$ therefore $\deg(g') = d - 1$
- From induction hypothesis, since $\deg(g') = d - 1$ then $\sum_{i=0}^{d} (-1)^{i+1} \cdot \binom{d}{i} \cdot g'(e+i) = 0$ for all $e \in \mathcal{F}$.
- So we know that $\deg(g) = d$ if and only if

$$\sum_{i=0}^{d} (-1)^{i+1} \cdot \binom{d}{i} \cdot (g(e+i+1) - g(e+i)) = 0$$

$\square$

Proof

Proof.

- By induction on d. If $d = 0$ the function is constant, therefore $-g(e) + g(e+1) = 0$ for all $e \in \mathcal{F}$.
- For induction step, $\deg(g) = d$ therefore $\deg(g') = d - 1$
- From induction hypothesis, since $\deg(g') = d - 1$ then $\sum_{i=0}^{d} (-1)^{i+1} \cdot \binom{d}{i} \cdot g'(e+i) = 0$ for all $e \in \mathcal{F}$.
- So we know that $\deg(g) = d$ if and only if

$$\sum_{i=0}^{d} (-1)^{i+1} \cdot \binom{d}{i} \cdot (g(e+i+1) - g(e+i)) = 0$$

$\square$

Proof

$$
\begin{aligned}
0 &= \sum_{i=0}^{d} (-1)^{i+1} \cdot \binom{d}{i} \cdot (g(e+i+1) - g(e+i)) \\
&= \sum_{i=0}^{d} (-1)^{i+1} \cdot \binom{d}{i} \cdot g(e+i+1) - \sum_{i=0}^{d} (-1)^{i+1} \cdot \binom{d}{i} \cdot g(e+i) \\
&= \sum_{j=1}^{d+1} (-1)^{j} \cdot \binom{d}{j-1} \cdot g(e+j) - \sum_{i=0}^{d} (-1)^{i+1} \cdot \binom{d}{i} \cdot g(e+i) \\
&= g(e) + (-1)^{d+1} \cdot g(e+d+1) + \sum_{i=1}^{d} (-1)^{i} \cdot \left(\binom{d}{i-1} + \binom{d}{i} \right) \cdot g(e+i) \\
&= -\sum_{i=0}^{d+1} (-1)^{i+1} \binom{d+1}{i} \cdot g(e+i) \quad \square
\end{aligned}
$$

Tester

- The previous two characterizations result in the following tester:
  1. Sample uniformly $\bar{x}, \bar{h} \in \mathcal{F}^m$.
  2. Query f at $\bar{x}, \bar{x} + \bar{h}, \ldots, \bar{x} + (d+1)\bar{h}$.
  3. Accept if and only if
  $$\sum_{i=0}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) = 0$$
- We now move to the analysis of this tester.

Tester

- The previous two characterizations result in the following tester:
  1. Sample uniformly $\bar{x}, \bar{h} \in \mathcal{F}^m$.
  2. Query f at $\bar{x}, \bar{x} + \bar{h}, \ldots, \bar{x} + (d+1)\bar{h}$.
  3. Accept if and only if

$$\sum_{i=0}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) = 0$$

- We now move to the analysis of this tester.

Tester

- The previous two characterizations result in the following tester:
  1. Sample uniformly $\bar{x}, \bar{h} \in \mathcal{F}^m$.
  2. Query f at $\bar{x}, \bar{x} + \bar{h}, \ldots, \bar{x} + (d+1)\bar{h}$.
  3. Accept if and only if

$$\sum_{i=0}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) = 0$$

- We now move to the analysis of this tester.

Tester

- The previous two characterizations result in the following tester:
  1. Sample uniformly $\bar{x}, \bar{h} \in \mathcal{F}^m$.
  2. Query f at $\bar{x}, \bar{x} + \bar{h}, \ldots, \bar{x} + (d+1)\bar{h}$.
  3. Accept if and only if

$$\sum_{i=0}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) = 0$$

- We now move to the analysis of this tester.

Tester

- The previous two characterizations result in the following tester:
  1. Sample uniformly $\bar{x}, \bar{h} \in \mathcal{F}^m$.
  2. Query f at $\bar{x}, \bar{x} + \bar{h}, \ldots, \bar{x} + (d+1)\bar{h}$.
  3. Accept if and only if
  $$\sum_{i=0}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) = 0$$
- We now move to the analysis of this tester.

Analysis - Main Theorem

Theorem

Let $\delta_0 = 1/(d+2)^2$. Then, our tester is a (one sided-error) POT with detection probability $\min(\delta, \delta_0)/2$*, where δ denotes the distance of the given function from $\mathcal{P}_{m,d}$*

Main Theorem - Approach

- From previous characterizations if $f \in \mathcal{P}_{m,d}$ we accept with probability 1.
- The approach to prove soundness is similar to the BLR theorem.
- We will show the if the tester rejects with probability $\rho < \delta_0/2$ then f, the input, is 2ρ-close to $\mathcal{P}_{m,d}$.
- This will be done by "correcting" f on at most $2\rho \cdot |\mathcal{F}|^m$ values into a low-degree polynomial.

Main Theorem - Approach

- From previous characterizations if $f \in \mathcal{P}_{m,d}$ we accept with probability 1.
- The approach to prove soundness is similar to the BLR theorem.
- We will show the if the tester rejects with probability $\rho < \delta_0/2$ then f, the input, is 2ρ-close to $\mathcal{P}_{m,d}$.
- This will be done by "correcting" f on at most $2\rho \cdot |\mathcal{F}|^m$ values into a low-degree polynomial.

Main Theorem - Approach

- From previous characterizations if $f \in \mathcal{P}_{m,d}$ we accept with probability 1.
- The approach to prove soundness is similar to the BLR theorem.
- We will show the if the tester rejects with probability $\rho < \delta_0/2$ then f, the input, is 2ρ-close to $\mathcal{P}_{m,d}$.
- This will be done by "correcting" f on at most $2\rho \cdot |\mathcal{F}|^m$ values into a low-degree polynomial.

Main Theorem - Approach

- From previous characterizations if $f \in \mathcal{P}_{m,d}$ we accept with probability 1.
- The approach to prove soundness is similar to the BLR theorem.
- We will show the if the tester rejects with probability $\rho < \delta_0/2$ then f, the input, is 2ρ-close to $\mathcal{P}_{m,d}$.
- This will be done by "correcting" f on at most $2\rho \cdot |\mathcal{F}|^m$ values into a low-degree polynomial.

Correcting f

- The way f is corrected at point $f(\bar{x})$ into a low degree polynomial is according to the most frequent value of:

$$\left\{ \sum_{i \in [d+1]} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) \right\}_{\bar{h} \in \mathcal{F}^m}$$

- It remains to show that this "corrected" function is a low degree polynomial.
- And that this function is 2ρ-close to f.

CORRECTING f

- The way f is corrected at point $f(\bar{x})$ into a low degree polynomial is according to the most frequent value of:

$$\left\{ \sum_{i \in [d+1]} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) \right\}_{\bar{h} \in \mathcal{F}^m}$$

- It remains to show that this "corrected" function is a low degree polynomial.
- And that this function is 2ρ-close to f.

Correcting f

- The way f is corrected at point $f(\bar{x})$ into a low degree polynomial is according to the most frequent value of:

$$\left\{ \sum_{i \in [d+1]} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) \right\}_{\bar{h} \in \mathcal{F}^m}$$

- It remains to show that this "corrected" function is a low degree polynomial.
- And that this function is 2ρ-close to f.

Simplified Version

- Imagine as if f is obtained by taking a degree $\leq d$ polynomial p and "corrupting" it on less than $|\mathcal{F}|^m/2(d+1)$ points.
- What happens when f is fed to our tester?
- Case 1: $\rho \geq \delta$, then we have a rejection probability proprtional to the distance.

Simplified Version

- Imagine as if f is obtained by taking a degree $\leq d$ polynomial p and "corrupting" it on less than $|\mathcal{F}|^m/2(d+1)$ points.
- What happens when f is fed to our tester?
- Case 1: $\rho \geq \delta$, then we have a rejection probability proprtional to the distance.

Simplified Version

- Imagine as if f is obtained by taking a degree $\leq d$ polynomial p and "corrupting" it on less than $|\mathcal{F}|^m/2(d+1)$ points.
- What happens when f is fed to our tester?
- Case 1: $\rho \geq \delta$, then we have a rejection probability proprtional to the distance.

Simplified Version

- Case 2: $\rho < \delta$ then the probability of $\sum_{i\in[d+1]} \alpha_i f\left(\bar{x} + i\bar{h}\right) = \sum_{i\in[d+1]} \alpha_i p\left(\bar{x} + i\bar{h}\right)$ is at least $1 - (d+1)\cdot\rho > 1/2$, from union bound.
- Since the probability is greather than 1/2, then this is the most common value for f, which means this is the value of the "corrected" f.
- Since $p(\bar{x})$ is a polynomial of degree $\leq d$, the right-hand-side equals $p(\bar{x})$.

Simplified Version

- Case 2: $\rho < \delta$ then the probability of $\sum_{i\in[d+1]} \alpha_i f\left(\bar{x} + i\bar{h}\right) = \sum_{i\in[d+1]} \alpha_i p\left(\bar{x} + i\bar{h}\right)$ is at least $1 - (d+1)\cdot\rho > 1/2$, from union bound.
- Since the probability is greather than $1/2$, then this is the most common value for f, which means this is the value of the "corrected" f.
- Since $p(\bar{x})$ is a polynomial of degree $\leq d$, the right-hand-side equals $p(\bar{x})$.

Simplified Version

- Case 2: $\rho < \delta$ then the probability of $\sum_{i\in[d+1]} \alpha_i f\left(\bar{x} + i\bar{h}\right) = \sum_{i\in[d+1]} \alpha_i p\left(\bar{x} + i\bar{h}\right)$ is at least $1 - (d+1)\cdot\rho > 1/2$, from union bound.
- Since the probability is greather than $1/2$, then this is the most common value for f, which means this is the value of the "corrected" f.
- Since $p(\bar{x})$ is a polynomial of degree $\leq d$, the right-hand-side equals $p(\bar{x})$.

Back to Reality

- We can't assume that f is constructed that way.
- Instead, f satisfies:

$$\mathbf{Pr}_{\bar{x},\bar{h}\in\mathcal{F}^m}\left[\overbrace{\sum_{i=0}^{d+1}\alpha_i\cdot f\left(\bar{x}+i\bar{h}\right)=0}^{\triangle}\right]=1-\rho$$

- For $\rho<\delta_0/2=1/2(d+2)^2$.
- $\triangle \iff f(\bar{x})=\sum_{i\in[d+1]}\alpha_i\cdot f\left(\bar{x}+i\bar{h}\right)$

Back to Reality

- We can't assume that f is constructed that way.
- Instead, f satisfies:

$$\mathbf{Pr}_{\bar{x},\bar{h}\in\mathcal{F}^m}\left[\overbrace{\sum_{i=0}^{d+1}\alpha_i\cdot f\left(\bar{x}+i\bar{h}\right)=0}^{\triangle}\right]=1-\rho$$

- For $\rho < \delta_0/2 = 1/2(d+2)^2$.
- $\triangle \iff f(\bar{x}) = \sum_{i\in[d+1]}\alpha_i\cdot f\left(\bar{x}+i\bar{h}\right)$

Back to Reality

- We can't assume that f is constructed that way.
- Instead, f satisfies:

$$\mathbf{Pr}_{\bar{x},\bar{h}\in\mathcal{F}^m}\left[\overbrace{\sum_{i=0}^{d+1}\alpha_i\cdot f\left(\bar{x}+i\bar{h}\right)=0}^{\triangle}\right]=1-\rho$$

- For $\rho<\delta_0/2=1/2(d+2)^2$.
- $\triangle \iff f(\bar{x})=\sum_{i\in[d+1]}\alpha_i\cdot f\left(\bar{x}+i\bar{h}\right)$

Back to Reality

- We can't assume that f is constructed that way.
- Instead, f satisfies:

$$\mathbf{Pr}_{\bar{x},\bar{h}\in\mathcal{F}^m}\left[\overbrace{\sum_{i=0}^{d+1}\alpha_i\cdot f\left(\bar{x}+i\bar{h}\right)=0}^{\triangle}\right]=1-\rho$$

- For $\rho<\delta_0/2=1/2(d+2)^2$.
- $\triangle \iff f(\bar{x})=\sum_{i\in[d+1]}\alpha_i\cdot f\left(\bar{x}+i\bar{h}\right)$

The Corrected Function

- Let S be a set.
- Let $\texttt{MFO}_{e \in S}\{v(e)\}$ be the *most frequently occuring* value of $v(e)$, ties are broken arbitrarily.
- From a function f we construct a "corrected" function g as:

$$g(\bar{x}) \stackrel{\text{def}}{=} \texttt{MFO}_{\bar{h} \in \mathcal{F}^m} \left\{ \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) \right\}$$

- From the assumption on f, we get that $g(\bar{x}) = f(\bar{x})$ with good probability on a random $\bar{x}$.

The Corrected Function

- Let S be a set.
- Let $\mathtt{MFO}_{e \in S}\{v(e)\}$ be the *most frequently occuring* value of $v(e)$, ties are broken arbitrarily.
- From a function f we construct a "corrected" function g as:

$$g(\bar{x}) \stackrel{\text{def}}{=} \mathtt{MFO}_{\bar{h} \in \mathcal{F}^m} \left\{ \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) \right\}$$

- From the assumption on f, we get that $g(\bar{x}) = f(\bar{x})$ with good probability on a random $\bar{x}$.

The Corrected Function

- Let S be a set.
- Let $\mathtt{MFO}_{e\in S}\{v(e)\}$ be the *most frequently occuring* value of $v(e)$, ties are broken arbitrarily.
- From a function f we construct a "corrected" function g as:

$$g(\bar{x}) \stackrel{\text{def}}{=} \mathtt{MFO}_{\bar{h}\in\mathcal{F}^m}\left\{\sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)\right\}$$

- From the assumption on f, we get that $g(\bar{x}) = f(\bar{x})$ with good probability on a random $\bar{x}$.

The Corrected Function

- Let S be a set.
- Let $\mathtt{MFO}_{e \in S}\{v(e)\}$ be the *most frequently occuring* value of $v(e)$, ties are broken arbitrarily.
- From a function f we construct a "corrected" function g as:

$$g(\bar{x}) \stackrel{\text{def}}{=} \mathtt{MFO}_{\bar{h} \in \mathcal{F}^m} \left\{ \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) \right\}$$

- From the assumption on f, we get that $g(\bar{x}) = f(\bar{x})$ with good probability on a random $\bar{x}$.

Claims about g

- We'll prove the following claims on g:
- Closeness: g is 2ρ-close to f.
- Strong Majority:

$$\forall \bar{x} \in \mathcal{F}^m : \mathbf{Pr}_{\bar{h} \in \mathcal{F}^m}\left[g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) \right] \geq 1 - 2(d+1)\rho$$

.

- Low Degree: $g \in \mathcal{P}_{m,d}$.

Claims about g

- We'll prove the following claims on g:
- Closeness: g is 2ρ-close to f.
- Strong Majority:

$$\forall \bar{x} \in \mathcal{F}^m : \mathbf{Pr}_{\bar{h} \in \mathcal{F}^m}\left[g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)\right] \geq 1 - 2(d+1)\rho$$

.

- Low Degree: $g \in \mathcal{P}_{m,d}$.

Claims about g

- We'll prove the following claims on g:
- Closeness: g is 2ρ-close to f.
- Strong Majority:

$$\forall \bar{x} \in \mathcal{F}^m : \mathbf{Pr}_{\bar{h} \in \mathcal{F}^m}\left[g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) \right] \geq 1 - 2(d+1)\rho$$

.

- Low Degree: $g \in \mathcal{P}_{m,d}$.

Claims about g

- We'll prove the following claims on g:
- Closeness: g is 2ρ-close to f.
- Strong Majority:

$$\forall \bar{x} \in \mathcal{F}^m : \mathbf{Pr}_{\bar{h} \in \mathcal{F}^m}\left[g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) \right] \geq 1 - 2(d+1)\rho$$

.

- Low Degree: $g \in \mathcal{P}_{m,d}$.

Closeness

Theorem

The function g is 2ρ-close to f.

Proof.

- A point $\bar{x}$ is bad if $g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)$ for less than half of choices of $\bar{h}$.
- A good point satisfies $f(\bar{x}) = g(\bar{x})$.
- Let B denote the set of all bad points.

$$\begin{aligned}\rho &= \mathbf{Pr}[\text{reject } f] \\ &\geq \mathbf{Pr}[\text{reject } f \mid \bar{x} \in B] \cdot \mathbf{Pr}[\bar{x} \in B] \\ &\geq \frac{1}{2} \cdot \mathbf{Pr}[\bar{x} \in B]\end{aligned}$$

- $\delta(f, g) = \mathbf{Pr}_{\bar{x} \in \mathcal{F}^m}[f(\bar{x}) \neq g(\bar{x})] \leq \mathbf{Pr}[\bar{x} \in B] \leq 2\rho$.

$\square$

Closeness

Theorem

The function g is 2ρ-close to f.

Proof.

- A point $\bar{x}$ is bad if $g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)$ for less than half of choices of $\bar{h}$.
- A good point satisfies $f(\bar{x}) = g(\bar{x})$.
- Let B denote the set of all bad points.

$$\begin{aligned}\rho &= \mathbf{Pr}[\text{reject } f] \\ &\geq \mathbf{Pr}[\text{reject } f \mid \bar{x} \in B] \cdot \mathbf{Pr}[\bar{x} \in B] \\ &\geq \frac{1}{2} \cdot \mathbf{Pr}[\bar{x} \in B]\end{aligned}$$

- $\delta(f, g) = \mathbf{Pr}_{\bar{x} \in \mathcal{F}^m}[f(\bar{x}) \neq g(\bar{x})] \leq \mathbf{Pr}[\bar{x} \in B] \leq 2\rho.$

□

Closeness

Theorem

The function g is 2ρ-close to f.

Proof.

- A point $\bar{x}$ is bad if $g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)$ for less than half of choices of $\bar{h}$.
- A good point satisfies $f(\bar{x}) = g(\bar{x})$.
- Let B denote the set of all bad points.

$$\begin{aligned}\rho &= \mathbf{Pr}[\text{reject } f] \\ &\geq \mathbf{Pr}[\text{reject } f \mid \bar{x} \in B] \cdot \mathbf{Pr}[\bar{x} \in B] \\ &\geq \frac{1}{2} \cdot \mathbf{Pr}[\bar{x} \in B]\end{aligned}$$

- $\delta(f, g) = \mathbf{Pr}_{\bar{x} \in \mathcal{F}^m}[f(\bar{x}) \neq g(\bar{x})] \leq \mathbf{Pr}[\bar{x} \in B] \leq 2\rho.$

□

Closeness

Theorem

The function g is 2ρ-close to f.

Proof.

- A point $\bar{x}$ is bad if $g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)$ for less than half of choices of $\bar{h}$.
- A good point satisfies $f(\bar{x}) = g(\bar{x})$.
- Let B denote the set of all bad points.

$$
\begin{aligned}
\rho &= \mathbf{Pr}[\text{reject } f] \\
&\geq \mathbf{Pr}[\text{reject } f \mid \bar{x} \in B] \cdot \mathbf{Pr}[\bar{x} \in B] \\
&\geq \frac{1}{2} \cdot \mathbf{Pr}[\bar{x} \in B]
\end{aligned}
$$

- $\delta(f, g) = \mathbf{Pr}_{\bar{x} \in \mathcal{F}^m}[f(\bar{x}) \neq g(\bar{x})] \leq \mathbf{Pr}[\bar{x} \in B] \leq 2\rho.$

Closeness

Theorem

The function g is 2ρ-close to f.

Proof.

- A point $\bar{x}$ is bad if $g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)$ for less than half of choices of $\bar{h}$.
- A good point satisfies $f(\bar{x}) = g(\bar{x})$.
- Let B denote the set of all bad points.

$$\begin{aligned}\rho &= \mathbf{Pr}[\text{reject } f] \\ &\geq \mathbf{Pr}[\text{reject } f \mid \bar{x} \in B] \cdot \mathbf{Pr}[\bar{x} \in B] \\ &\geq \frac{1}{2} \cdot \mathbf{Pr}[\bar{x} \in B]\end{aligned}$$

- $\delta(f, g) = \mathbf{Pr}_{\bar{x} \in \mathcal{F}^m}[f(\bar{x}) \neq g(\bar{x})] \leq \mathbf{Pr}[\bar{x} \in B] \leq 2\rho$.

$\square$

Strong Majority

Theorem

$$\forall \bar{x} \in \mathcal{F}^m : \mathbf{Pr}_{\bar{h}\in\mathcal{F}^m}\left[g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)\right] \geq 1 - 2(d+1)\rho$$

Proof.

- Let $Z_{\bar{x}} = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)$ be a random variable where $\bar{h} \in \mathcal{F}^m$ is chosen uniformly at random.
- The rejection probability is ρ.
- Therefore: $\mathbf{Pr}_{\bar{x}\in\mathcal{F}^m}[f(\bar{x}) = Z_{\bar{x}}] = 1 - \rho$
- This means that for a typical $\bar{x}$ we have $Z_{\bar{x}} = f(\bar{x})$ with high probability.
- Therefore, $Z_{\bar{x}} = g(\bar{x})$ for such $\bar{x}$'s as well W.H.P.

□

Strong Majority

Theorem

$\forall \bar{x} \in \mathcal{F}^m : \mathbf{Pr}_{\bar{h} \in \mathcal{F}^m}\left[g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)\right] \geq 1 - 2(d+1)\rho$

Proof.

- However, we want to prove this claim for any $\bar{x}$.
- Therefore, we have to show that for all $\bar{x}$ the most common value of $Z_{\bar{x}}$ is **very** common.
- From now on, fix some $\bar{x} \in \mathcal{F}^m$

$\square$

Strong Majority

Theorem

$\forall \bar{x} \in \mathcal{F}^m : \mathbf{Pr}_{\bar{h} \in \mathcal{F}^m}\left[g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)\right] \geq 1 - 2(d+1)\rho$

Proof.

- We will use the property that *the probability for the most common value to appear is lower bound by the collision probability.*
- Let S be a set and $\mathtt{MFO}_S$ be the most frequent occuring value in S.
- $\overbrace{\mathbf{Pr}_{u,v \in S}[u = v]}^{\text{collision probability}} = \sum_{v \in S} \mathbf{Pr}_{u \in S}[u = v]^2 \leq \overbrace{\sum_{v \in S} \mathbf{Pr}_{u \in S}[u = v]}^{\text{sum} = 1} \mathbf{Pr}_{u \in S}[u = \mathtt{MFO}_S] = \mathbf{Pr}_{u \in S}[u = \mathtt{MFO}_S]$
- In our context $S = \left\{\sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) \mid \bar{h} \in \mathcal{F}^m\right\}$ and $\mathtt{MFO}_S = g(\bar{x})$.

$\square$

Strong Majority

Theorem

$\forall \bar{x} \in \mathcal{F}^m : \mathbf{Pr}_{\bar{h} \in \mathcal{F}^m}\left[g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)\right] \geq 1 - 2(d+1)\rho$

Proof.

- So, to lower bound $\mathbf{Pr}[g(\bar{x}) = Z_{\bar{x}}]$ we will give a lower bound on the collision probability of $Z_{\bar{x}}$ which is:
- $\mathbf{Pr}_{\bar{h}_1, \bar{h}_2 \in \mathcal{F}^m}\left[\sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}_1\right) = \sum_{j=1}^{d+1} \alpha_j \cdot f\left(\bar{x} + i\bar{h}_2\right)\right]$

$\square$

Strong Majority

Theorem

$\forall \bar{x} \in \mathcal{F}^m : \mathbf{Pr}_{\bar{h} \in \mathcal{F}^m}\left[g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)\right] \geq 1 - 2(d+1)\rho$

Proof.

- Since $\bar{h}_1, \bar{h}_2$ are random, then $\bar{x} + i\bar{h}_1$ is also random and so is $\bar{x} + j\bar{h}_2$.
- Therefore, we can apply our assumption (on ρ being the rej. prob. of f) on random line starting at random point in random direction.
- The random points will be $\bar{x} + i\bar{h}_1$ for $i \in [d+1]$ with direction $\bar{h}_2$ and points $\bar{x} + j\bar{h}_2$ with direction $\bar{h}_1$.
- These lines intersect at points $\bar{x} + i\bar{h}_1 + j\bar{h}_2$, we will use these intersections soon.

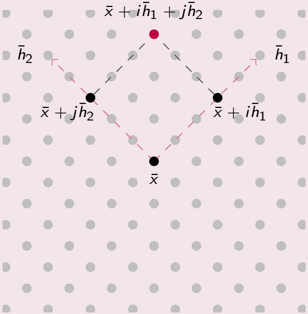
$\square$

Strong Majority

Theorem

$$\forall \bar{x} \in \mathcal{F}^m : \mathbf{Pr}_{\bar{h}\in\mathcal{F}^m}\left[g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)\right] \geq 1 - 2(d+1)\rho$$

Proof.



□

Strong Majority

Theorem

$\forall \bar{x} \in \mathcal{F}^m : \mathbf{Pr}_{\bar{h} \in \mathcal{F}^m}\left[g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)\right] \geq 1 - 2(d+1)\rho$

Proof.

- For random $\bar{h}_1, \bar{h}_2$ we have $\bar{x} + i\bar{h}_1$ and $\bar{x} + j\bar{h}_2$ are random for every $i, j \in [d+1]$. This implies:

$$\forall i \in [d+1] : \mathbf{Pr}_{\bar{h}_1, \bar{h}_2 \in \mathcal{F}^m}\left[f\left(\bar{x} + i\bar{h}_1\right) = \sum_{j=1}^{d+1} \alpha_j \cdot f\left(\left(\bar{x} + i\bar{h}_1\right) + j\bar{h}_2\right)\right] = 1 - \rho$$

$$\forall j \in [d+1] : \mathbf{Pr}_{\bar{h}_1, \bar{h}_2 \in \mathcal{F}^m}\left[f\left(\bar{x} + j\bar{h}_2\right) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\left(\bar{x} + j\bar{h}_2\right) + i\bar{h}_1\right)\right] = 1 - \rho$$

$\square$

Strong Majority

Theorem

$\forall \bar{x} \in \mathcal{F}^m : \mathbf{Pr}_{\bar{h} \in \mathcal{F}^m}\left[g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)\right] \geq 1 - 2(d+1)\rho$

Proof.

- If we use a union bound over $i \in [d+1]$ in the first eq. and over $j \in [d+1]$ in the second one we get:

$$\mathbf{Pr}_{\bar{h}_1, \bar{h}_2 \in \mathcal{F}^m}\left[\sum_{i=1}^{d+1} \alpha_i f\left(\bar{x} + i\bar{h}_1\right) = \sum_{i=1}^{d+1}\sum_{j=1}^{d+1} \alpha_i \alpha_j \cdot f\left(\bar{x} + i\bar{h}_1 + j\bar{h}_2\right)\right] = 1 - (d+1) \cdot \rho$$

$$\mathbf{Pr}_{\bar{h}_1, \bar{h}_2 \in \mathcal{F}^m}\left[\sum_{j=1}^{d+1} \alpha_j f\left(\bar{x} + j\bar{h}_2\right) = \sum_{j=1}^{d+1}\sum_{i=1}^{d+1} \alpha_j \alpha_i \cdot f\left(\bar{x} + i\bar{h}_1 + j\bar{h}_2\right)\right] = 1 - (d+1) \cdot \rho$$

□

Strong Majority

Theorem

$\forall \bar{x} \in \mathcal{F}^m : \mathbf{Pr}_{\bar{h} \in \mathcal{F}^m}\left[g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right) \right] \geq 1 - 2(d+1)\rho$

Proof.

- Union bounding over the previous two equations together, we get:

$$\underbrace{\mathbf{Pr}_{\bar{h}_1, \bar{h}_2 \in \mathcal{F}^m}\left[\overbrace{\sum_{i=1}^{d+1} \alpha_i f\left(\bar{x} + i\bar{h}_1\right)}^{\text{sample from } Z_{\bar{x}}} = \overbrace{\sum_{j=1}^{d+1} \alpha_j f\left(\bar{x} + j\bar{h}_2\right)}^{\text{sample from } Z_{\bar{x}}} \right]}_{\text{collision probability of } Z_{\bar{x}}} = 1 - 2(d+1) \cdot \rho$$

$\square$

Strong Majority

Theorem

$\forall \bar{x} \in \mathcal{F}^m : \mathbf{Pr}_{\bar{h} \in \mathcal{F}^m}\left[g(\bar{x}) = \sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)\right] \geq 1 - 2(d+1)\rho$

Proof.

- We have given a lower bound on the collision probability of $Z_{\bar{x}}$.
- This is a lower bound on $\mathbf{Pr}_{\bar{h} \in \mathcal{F}^m}\left[g(\bar{x}) = \overbrace{\sum_{i=1}^{d+1} \alpha_i \cdot f\left(\bar{x} + i\bar{h}\right)}^{=\text{sample from } Z_{\bar{x}}}\right]$
- Finally, QED.

$\square$

Low Degree

Theorem

$g \in \mathcal{P}_{m,d}$.

Proof.

- g is low degree $\iff$ for all $\bar{x}, \bar{h} \in \mathcal{F}^m$: $\sum_{i=0}^{d+1} \alpha_i \cdot g\left(\bar{x} + i\bar{h}\right) = 0$.
- Fix $\bar{x}, \bar{h}$ for the rest of the proof.

$\square$

Low Degree

Theorem

$g \in \mathcal{P}_{m,d}$.

Proof.

- Let $\bar{h}_1, \bar{h}_2$ be uniform and independently chosen from $\mathcal{F}^m$.
- Therefore, for every $i \in [d+1]$ $\bar{h}_1 + i\bar{h}_2$ is uniform in $\mathcal{F}^m$ and from "Strong Majority" lemma:

$$\mathbf{Pr}_{\bar{h}_1,\bar{h}_2 \in \mathcal{F}^m}\left[g\left(\bar{x} + i\bar{h}\right) = \sum_{j=1}^{d+1} \alpha_j \cdot f\left(\left(\bar{x} + i\bar{h}\right) + j\left(\bar{h}_1 + i\bar{h}_2\right)\right)\right] \geq 1 - 2(d+1)\rho$$

$\square$

Low Degree

Theorem

$g \in \mathcal{P}_{m,d}$.

Proof.

- Also, for all $j \in [d+1]$ both $\bar{x} + j\bar{h}_1$ and $\bar{h} + j\bar{h}_2$ are uniformly distributed in $\mathcal{F}^m$.
- Therefore, from ρ being the rejection probability of the tester for f we get:

$$\mathbf{Pr}_{\bar{h}_1,\bar{h}_2 \in \mathcal{F}^m}\left[\sum_{i=0}^{d+1} \alpha_i f\left(\left(\bar{x} + j\bar{h}_1\right) + i\left(\bar{h} + j\bar{h}_2\right)\right) = 0\right] = 1 - \rho$$

$\square$

Low Degree

Theorem

$g \in \mathcal{P}_{m,d}$.

Proof.

- By adding up the above equations for all $j \in [d+1]$ and rephrasing the agument to f, we get:

$$\mathbf{Pr}_{\bar{h}_1,\bar{h}_2 \in \mathcal{F}^m}\left[\sum_{j=1}^{d+1} \alpha_j \sum_{i=0}^{d+1} \alpha_i f\left(\left(\bar{x} + i\bar{h}\right) + j\left(\bar{h}_1 + i\bar{h}_2\right)\right) = 0\right] = 1 - (d+1)\rho$$

- Overall, from union bounding, we get...

$\square$

Low Degree

Theorem

$g \in \mathcal{P}_{m,d}$.

Proof.

$$\mathbf{Pr}_{\bar{h}_1,\bar{h}_2\in\mathcal{F}^m}\left[\sum_{i=0}^{d+1}\alpha_i g\left(\bar{x}+i\bar{h}\right)=\sum_{i=0}^{d+1}\alpha_i\sum_{j=1}^{d+1}\alpha_j f\left(\left(\bar{x}+i\bar{h}\right)+j\left(\bar{h}_1+i\bar{h}_2\right)\right)=0\right]$$

$$\geq 1-(d+2)\cdot 2(d+1)\rho-(d+1)\cdot\rho$$

$$=1-(2d+5)(d+1)\rho$$

$$>0 \quad \texttt{//since} \;\; \rho\geq 1/2(d+2)^2$$

$\square$

Low Degree

Theorem

$g \in \mathcal{P}_{m,d}$.

Proof.

- There we get that:

$$\mathbf{Pr}_{\bar{h}_1, \bar{h}_2 \in \mathcal{F}^m}\left[\sum_{i=0}^{d+1} \alpha_i g\left(\bar{x} + i\bar{h}\right) = 0\right] > 0$$

- Since the event is fixed (ind. of $\bar{h}_1, \bar{h}_2$), the probability is therefore 1.

□

Recap

- We have shown that f is 2ρ-far from g if the detection probability is below some constant threshold.
- We have shown that g in that case is a low degree polynomial.
- The tester doesn't depend on the distance.
- The tester always accepts low degree polynomials.
- Therefore: We have a one-sided error POT for low degree polynomials.

Fin.

Thank you!