Algebraic Property Testing

Madhu Sudan

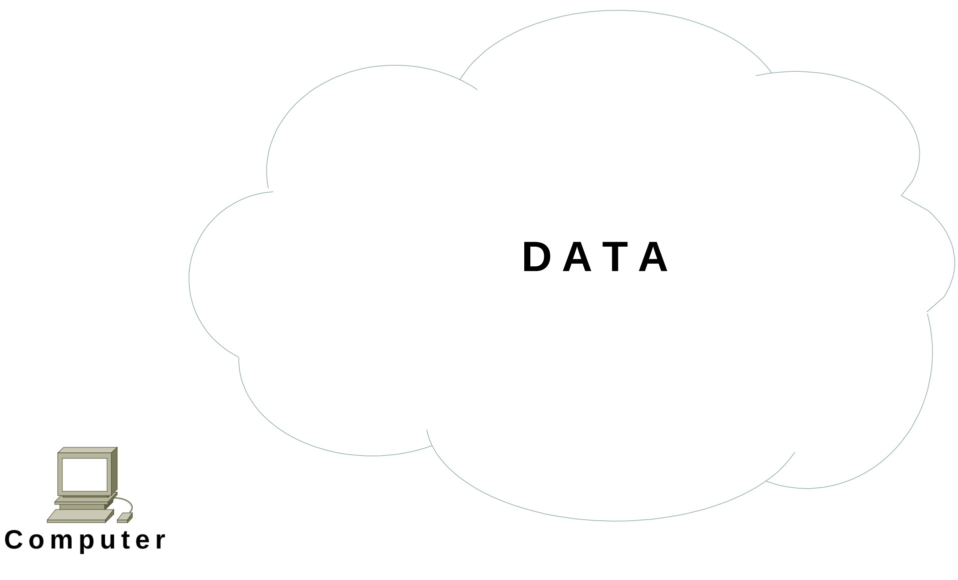
October 13, 2007

1 Introduction

- What is Property Testing?
- What is "algebraic" Property Testing?
- Why it is interesting?
- Brief History
- Linearity (or Homomorphism) Testing

2 Property Testing

Modern theme in algorithmic research:



We have:

- small computer
- big amounts of data
- small amount of time

We want to:

- make some estimations
- we can't scan all data
- do not have enough time to read data - need "Quick & Dirty Solution"!

2.1 Data=?

Function $f : \mathcal{D} \to \mathcal{R}$, where $\mathcal{D}$ is a finite set and $\mathcal{R}$ is a finite range.
We treat function f as a "box":

$$x \to \boxed{\text{f}} \to f(x)$$

We will mainly consider cases of $f : \mathcal{G} \to \mathcal{H}$, where $\mathcal{G}$ is a finite abelian group and $\mathcal{H}$ is a subgroup of $\mathcal{G}$.
Special cases of the above are: $f : \mathbb{F}^n \to \mathbb{F}$

2.2 Property=?

Specified by a set $\mathfrak{F} \subseteq \{f : \mathcal{D} \to \mathcal{R}\}$ of functions that satisfy our desired property.

2.3 Quick?

$$\boxed{\text{f}} \to \boxed{\begin{matrix}\text{Test}\\ \mathfrak{F},\mathcal{D},\mathcal{R}\end{matrix}} \to \begin{matrix}\text{YES? if } f \in \mathfrak{F}\\ \text{NO? if } f \notin \mathfrak{F}\end{matrix}$$

With very few queries into $\boxed{\text{f}}$ i.e. $o(|\mathcal{D}|)$ or even $\mathcal{O}(1)$.
Simple example:

$$\mathfrak{F} = \{f | f(0) = 0\}$$

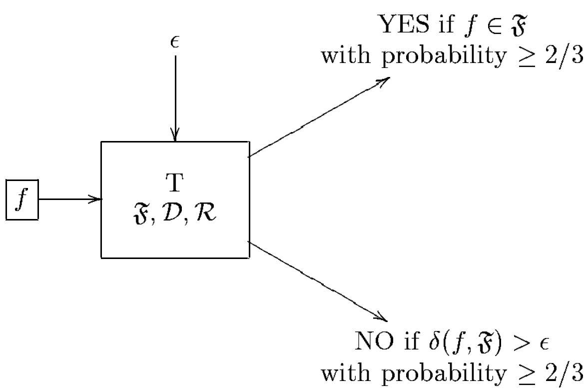
More interesting families $\mathfrak{F}$:
if $f \in \mathfrak{F}$, $f_{x,a} \triangleq f_{xa}(y) = \begin{cases} f(y) & \text{except } x = y \\ a & \text{if } x = y \end{cases}$
$\forall_{x \& a \neq f(x)} f_{x,a} \notin \mathfrak{F}$
In other words, if $f \in \mathfrak{F}$ and g disagrees with f in one place, then $g \notin \mathfrak{F}$.

2.4 Dirtiness

$\delta(f,g) \triangleq Pr_{x \leftarrow_u \mathcal{D}}[f(x) \neq g(x)]$ - normalised Hamming Distance.
It has all required properties of a metrics function:

- $\delta(f,f) = 0$
- $\delta(f,g) + \delta(g,h) \geq \delta(f,h)$
- $\delta(f,g) = \delta(g,f)$

$\delta(f,\mathfrak{F}) = \min_{g \in \mathfrak{F}}\{\delta(f,g)\}$ - smallest distance of family



2.5 Polling = Property Test (symmetric property)

$\mathcal{D} =$ population of the country
$\mathcal{R} = \{\text{Red}, \text{Blue}\}$
$f(x) =$ vote of x
$\mathfrak{F} = \{f(x) | \text{majority}(f) = \text{Red}\}$

$$\text{Property test} = \begin{cases} \text{YES} & \text{if majority is RED} \\ \text{NO} & \text{if} \leq 49\% \text{ of votes are RED} \\ \text{arbitrary} & \text{otherwise} \end{cases}$$

If $f \in \mathfrak{F}$ and $\pi : \mathcal{D} \to \mathcal{D}$ is $1 \leftrightarrow 1$, then $f \circ \pi \in \mathfrak{F}$ - symmetric property.

2.6 History

- '90: Blum, Luby, Rubinfeld: *Linearity of functions (homomorphisms of groups)*
- '96: Goldreich, Goldwasser, Ron: *Graph theoretic properties*
- .
- Alon, Shopira, ...: *Exactly which graph properties are testable*

2.6.1 Graph property

$\mathcal{D} = [n] \times [n]$, where $[n] = \{1, 2, \ldots, n\}$
$\mathcal{R} = \{0, 1\}$
$f(i, j) = 1$ if there is an edge between i and j.
$\pi : [n] \rightarrow [n]$ is $1 \leftrightarrow 1$
$\forall_{f \in \mathfrak{F}} f_\pi(i, j) = f(\pi(i), \pi(j)) \Rightarrow f_\pi \in \mathfrak{F}$

3 Homomorphism Testing

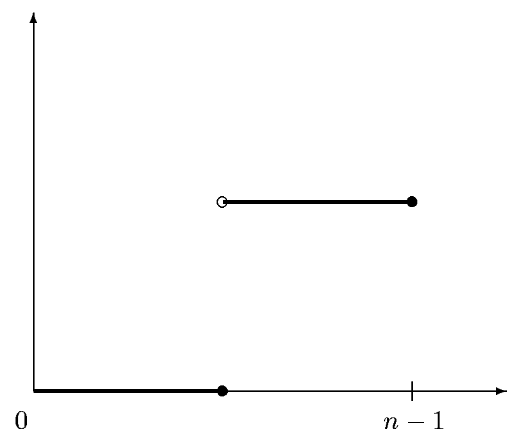
$f : \mathcal{G} \rightarrow \mathcal{H}$, where $\mathcal{G}$ is a finite abelian group
$\mathfrak{F} = \mathfrak{F}_{\text{hom}} = \{\Phi : \mathcal{G} \rightarrow \mathcal{H} \text{ s.t. } \forall_{x,y \in \mathcal{G}} \Phi(x) + \Phi(y) = \Phi(x+y)\}$

3.1 Linearity Testing

$\mathcal{D} = \mathbb{F}_p^n$
$\mathbb{F}_p$ - finite field of size p (p prime)
$\mathcal{R} = \mathbb{F}_p$
Even more special:

- $\mathbb{F}_2^n \rightarrow \mathbb{F}_2$
- $\Phi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is a homomorphism
- $\mathbb{F}_2^n = (x_1, \ldots, x_n)$
- $\Phi(x)$ is a homomorphism iff $\exists_{a_1, a_2, \ldots, a_n \in \mathbb{F}_2}$ s.t. $\Phi(x) = \sum_i a_i x_i \pmod 2$

Let $\mathcal{G} = \mathcal{H} = \mathbb{Z}_n$.
Φ is a homomorphism iff $\forall_x \Phi(x) + \Phi(1) = \Phi(x+1)$
$\exists_f$ s.t. $Pr_x[f(x+1) = f(x) + f(1)] = 99,9\%$, but $\delta(f, \mathfrak{F}) \leq \frac{1}{2}$



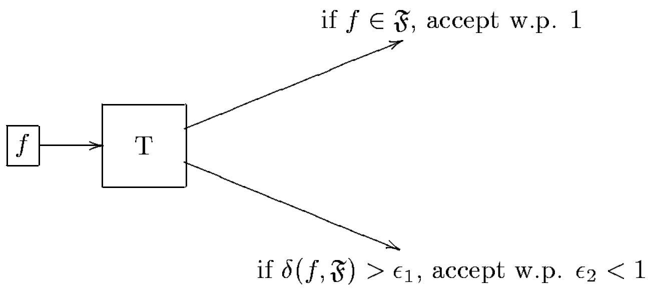
3.1.1 Simple Exercises

1. Give a function $f : \mathbb{Z}_n \to \mathbb{Z}_n$ s.t. $Pr_x[f(x+1) = f(x) + f(1)] \to 1$, but $\delta(f, \mathfrak{F}) \to 1$

2. Prove that for every pair of homomorphisms $\Phi, \Psi : \mathcal{G} \to \mathcal{H}$, $\delta(\Phi, \Psi) \geq \frac{1}{2}$

3.2 Homomorphism Test

Pick $x, y \leftarrow_u \mathcal{G}$ and test if $f(x) + f(y) = f(x+y)$.
If $f \in \mathbb{F}$, then $Pr[\text{acceptance}] = 1$.



where ϵ_1 and ϵ_2 are some constants.