Low-Degree Testing

Madhu Sudan
MSR

Survey ... based on many works
Kepler’s Problem

Tycho Brahe (~1550-1600):
- Wished to measure planetary motion accurately.
- To confirm sun revolved around earth ... (+ other planets around sun)
- Spent 10% of Danish GNP

Johannes Kepler (~1575-1625s):
- Believed Copernicus’s picture: planets in circular orbits.
- Addendum: Ratio of orbits based on Löwner-John ratios of platonic solids.
- “Stole” Brahe’s data (1601).
- Worked on it for nine years.
- Disproved Addendum; Confirmed Copernicus (circle -> ellipse); discovered laws of planetary motion.

- Nine Years?
  - To check if data fits a low-degree polynomial?

Source: Michael Fowler, “Galileo & Einstein”, U. Virginia
Low-degree Testing

• Notation: \( \mathbb{F}_q = \) finite field of cardinality \( q \)

• Problem: Given \( f : \mathbb{F}_q^n \rightarrow \mathbb{F}_q \) and \( d \in \mathbb{N} \), is \( f \) “essentially” a deg. \( \leq d \) (\( n \)-var.) polynomial?
  – With few queries for values of \( f(\cdot) \)
  – “essentially”:
    • Must accept if \( \deg(f) \leq d \).
    • Reject w.h.p. if \( \delta(f, g) \geq .1 \), \( \forall g \) with \( \deg(g) \leq d \)
      \[- \delta(f, g) \triangleq q^{-n} \cdot |\{x \mid f(x) \neq g(x)\}|\]

\[ \deg(x^2 y^3) = 5 \]

\[ \delta(f, g) \triangleq q^{-n} \cdot |\{x \mid f(x) \neq g(x)\}| \]

Warning: Refinements and Variations later.
This talk

• Some motivations
• Some results
• Some proofs
Why Polynomials? Robustness!

• Polynomial Distance Lemma:
  – Let $f, g : \mathbb{F}_q^n \rightarrow \mathbb{F}_q$, w. $\deg(f), \deg(g) \leq d$, $f \neq g$
    • $d < q$: $\delta(f, g) \geq 1 - \frac{d}{q}$
    • Generally: $\delta(f, g) \geq q^{-\left(\frac{d}{q-1}\right)}$ (w.l.o.g. $\deg_{x_i}(f) < q$)
    ! No dependence on $n$!
  • $\delta_{d, q} \triangleq$ Min. Dist. Between degree $d$ polynomials over $\mathbb{F}_q$

• Used in Error-correcting Codes:
  – Information: Coefficients of polynomials
  – Encoding: Evaluations
  – Robust: Changing few values doesn’t cause ambiguity.
Formal Definitions and Parameters

• \((\ell, \varepsilon)\)-local low-degree test:
  - Selects queries \(Q = \{x_1, \ldots, x_{\ell}\} \subseteq \mathbb{F}_q^n\)
    and set \(S \subseteq \{h: Q \rightarrow \mathbb{F}\}\)
  - Accept iff \(f \mid_Q \in S\).
  - Guarantees:
    • \(\deg(f) \leq d \implies\) Accepts w.p. 1
    • \(\forall f, \Pr[\text{rejection}] \geq \varepsilon \cdot \delta_d(f)\)
    • \((\ell, \alpha)\)-robust if \(\forall f, \mathbb{E}_{Q,S}[\delta(f \mid_Q, S)] \geq \alpha \cdot \delta_d(f)\)

• General goal: Minimize \(\ell\), while maximizing \(\varepsilon, \alpha\)
What can be achieved? ($d = 1$)

- The functions: $\{c_0 + \sum_{i=1}^{n} c_i x_i \mid c_0 \ldots c_n \in \mathbb{F}_q\}$
  - $(n + 1)$-dimensional vector space over $\mathbb{F}_q$

- Distance: $\delta_{d,q} = 1 - \frac{1}{q}$

- $\ell, \epsilon, \alpha = ?$

- $\ell > 2$

- $\ell = 3$ achievable iff $q > 2$, with $\epsilon, \alpha > 0$

- $\ell = 4$: Test: $\alpha f(u) + \beta f(v) + \gamma f(v) = f(\alpha u + \beta v + \gamma w)$;
  - “Linearity Testing” [BlumLubyRubinfeld] ...
  - Achieves $\epsilon = 1$! [BellareCoppersmithHåstadKiwiSudan]
    - Proof ingredient: Discrete Fourier Analysis.
Generalizing to higher $d$

- Optimal locality = ?
- Test = ?
- Best soundness $\epsilon =$?
- Best robustness $\alpha =$?

- How do the above depend on $n, q, d$?
Why Low-degree Testing?

• Polynomials: Makes data robust
• Low-degree Testing: Makes proofs robust
  – “Proof” = Data that makes “Theorem” obvious/verifiable
    [Gödel, Church, Turing, Cook, Levin]
  – “Robust Proof” = One that implies truth of theorem based on local tests (Holographic Proofs, Probabilistically Checkable Proofs)
    [Arora, Babai, Feige, Fortnow, Goldwasser, Levin, Lovasz, Lund, Rompel, Safra, Sipser, Szegedy]
  – (Mod Details):
    • To robustify Proof $\Pi$ of Assertion $T$, encode $\Pi$ using multivariate polynomial encoding;
    • Verify proof $\hat{\Pi}$ by first a low-degree test; and then “more standard tests”.

09/02/2015 CMSA: Low-degree Testing
Why low-degree testing - II

• Codes are extremal combinatorial objects
  – Lead to many other extremal objects (expanders, extractors, pseudo-random generators, condensers ...)
  – Low-degree testing: further embellishes such connections.
  – E.g. [BGHMRS]:
    • $G_{n,d,q} = (V, E)$;
      $V = \{ f : \mathbb{F}_q^n \to \mathbb{F}_q, \deg(f) \leq d \}$;
      $(f, g) \in E \iff f - g \text{ (near)-maximally zero.}$
    • LDT $\Rightarrow G_{n,d,q}$ is a small-set expander!
Formal Definitions and Parameters

• \((\ell, \epsilon)\)-local low-degree test:
  – Selects queries \(Q = \{x_1, \ldots, x_\ell\} \subseteq \mathbb{F}_q^n\)
  and set \(S \subseteq \{h: Q \rightarrow \mathbb{F}\}\)
  – Accept iff \(f|_Q \in S\).
  – Guarantees:
    • \(\deg(f) \leq d \Rightarrow \text{Accepts w.p. 1}\)
    • \(\forall f, \Pr[\text{rejection}] \geq \epsilon \cdot \delta_d(f)\)
    • \((\ell, \alpha)\)-robust if \(\forall f, \mathbb{E}_{Q,S}[\delta(f|_Q,S)] \geq \alpha \cdot \delta_d(f)\)

• General goal: Minimize \(\ell\), while maximizing \(\epsilon, \alpha\)
A natural test

- \( f: \mathbb{F}_q^n \to \mathbb{F}_q \) with \( \deg(f) \leq d \)
  \( \Rightarrow \) \( \forall \) affine subspaces \( A \subseteq \mathbb{F}_q^n \) s. t. \( \dim(A) = t, \deg(f|_A) \leq d \)

- Converse?

- Fact: \( \forall q, d \exists t = t_{q,d} \) s. t.
  \( \forall \) affine \( A \) s. t. \( \dim(A) = t, \deg(f|_A) \leq d \)
  \( \Rightarrow \) \( \deg(f) \leq d \)

- Natural test:
  - Pick random subspace \( A \) s. t. \( \dim(A) = \tilde{t} \geq t_{q,d} \)
    - Accept if \( \deg(f|_A) \leq d \).
Locality of subspace tests

• \( \frac{d+1}{q-1} \leq t_{q,d} \leq \frac{2(d+1)}{q-1} \). (Precisely \( t_{q,d} = \left\lceil \frac{d+1}{q^\frac{d}{q} - \frac{q}{p}} \right\rceil \))

\[ \Rightarrow \text{Locality of test} \leq q^{\Theta\left(\frac{d}{q}\right)} \]

• Codes + duality

\[ \Rightarrow \text{Locality of any non-trivial constraint} \geq q^{\Omega\left(\frac{d}{q}\right)} \]

• How good are the tests?
  – \( \epsilon = ? \); \( \alpha = ? \)
  – Does using \( \tilde{t} > t_{q,d} \) help?
Results

• (Disclaimer: Long history ... not elaborated below.)
• Fix \( q; \quad d \to \infty \); sound!

Theorem 1: [BKSSZ,HSS,HRS] \( \forall q \exists \epsilon = \epsilon_q > 0 \), s.t. \( \forall d, n, f \) the \( t_{q,a} \)-dimensional test rejects \( f \) w.p. \( \geq \epsilon \cdot \delta_d(f) \)

• Fix \( \frac{d}{q} < 1; \quad q \to \infty \); robust!

Theorem 2: [GHS] \( \forall \delta > 0 \exists \alpha > 0 \) s.t. \( \forall q, d, n, f \) w. \( d < (1 - \delta)q \), the 2-dim. test satisfies \( \mathbb{E}_A[\delta_d(f|_A)] \geq \alpha \cdot \delta_d(f) \).

• \( \frac{d}{q} \to 0; \quad \text{Maximal robustness} \)

Theorem 3: [RS] \( \forall \alpha < 1, \exists \delta < 1 \) s.t. \( \forall q, d, n, f \) w. \( d < (1 - \delta)q \), the 2-dim. test satisfies \( \mathbb{E}_A[\delta_d(f|_A)] \geq \alpha \cdot \delta_d(f) \).
Theorem 1: Context + Ideas

- Fix $q = 2$.
- Alternative view of test:
  - $f_a(x) \equiv f(x + a) - f(a)$ “discrete derivative”
  - $\deg(f) \leq d \Rightarrow \deg(f_a) \leq d - 1$
  - $\Rightarrow \deg(f_{a_1,\ldots,a(d+1)}) < 0 \Rightarrow f_{a_1,\ldots,a(d+1)} = 0$
  - Rejection Prob. $\triangleq \rho(f) = \Pr_{a_1\ldots a(d+1)}[f_{a_1\ldots a(d+1)}] \neq 0$
  - $(1 - 2\rho(f))\frac{1}{2^d}$ special case of “Gowers norm”
  - Strong “Inverse Conjecture” $\Rightarrow \rho(f) \to \frac{1}{2}$ as $\delta_d(f) \to \frac{1}{2}$.
  - Falsified by [LovettMeshulamSamorodnitsky],[GreenTao]:
    - $f = \text{Sym}_{2^t}(x_1 \ldots x_n); d = 2^t - 1$;
    - $\delta_d(f) = \frac{1}{2} - o_n(1); \rho(f) \leq \frac{1}{2} - 2^{-7}$
Theorem 1 (contd.)

• So $\rho(f) \to \frac{1}{2}$ as $\delta(f) \to \frac{1}{2}$; but is $\rho(f) > 0$?

• Prior to [BKSSZ]: $\rho(f) > 4^{-d}$

• [BKSSZ] Lemma: $\rho(f) \geq \min\{\epsilon_2, 2^d \cdot \delta(f)\}$

• Key ingredient in proof:
  – Suppose $\delta_d(f) > 2^{-d}$
  – On how many “hyperplanes” $H$ can $\deg(f|_H) \leq d$?
Hyperplanes

\[ \delta_d(f) > 2^{-d} \Rightarrow \#\{H \text{ s.t. } \deg(f|_H) \leq d\} \leq ? \]

1. \( \exists H \text{ s.t. } \deg(f|_H) > d \): defn of testing dimension.

2. \( \Pr_{H}[\deg(f|_H) \leq d] \geq \frac{1}{q} \iff \deg_{x_i}(f) < q - 1 \).

3. ... What we needed: \( \#\{H \text{ s.t. } \deg(f|_H) \leq d\} \leq O(2^d) \)
General $q$

- Lemma: $\forall q \exists c$ s.t. if $\delta_d(f) \geq q^{-t_{q,d}}$ then $\#\{H \text{ s.t. } \deg(f|_H) \leq d\} \leq c \cdot q^{t_{q,d}}$

- Ingredients in proof:
  - $q = 2$: Simple symmetry of subspaces, linear algebra.
  - $q = 3$: Roth’s theorem ...
  - General $q$: Density Hales-Jewett theorem

09/02/2015 CMSA: Low-degree Testing 18 of 25
Theorem 2: Ideas

Theorem 2: [GHS] \( \forall \delta > 0 \exists \alpha > 0 \) s.t. \( \forall q, d, n, f \) w. \( d < (1 - \delta)q \), the 2-dim. test satisfies \( \mathbb{E}_A[\delta_d(f|_A)] \geq \alpha \cdot \delta_d(f) \).

- When \( d < q \), polynomials are good codes!
- Is this sufficient for low-degree testing?
  - Investigated in computational complexity since 90s.
  - Linearity insufficient. [Folklore]
  - Local constraints insufficient. [BHR05]
  - Symmetry: Automorphisms of domain preserving space of functions?
    - Cyclicity: Insufficient [BSS]
    - Affine-invariance: Weakly sufficient [KS] \( (\epsilon \geq \exp(-d)) \)
Theorem 2 (contd.)

- “Lifted families” [GuoKoppartyS.14]
  - Fix $B \subseteq \{ h: \mathbb{F}_q^t \rightarrow \mathbb{F}_q \}$ base family (affine-invariant)
  - Its $n$-dim lift is
    $$B^\uparrow n \equiv C = \{ f: \mathbb{F}_q^n \rightarrow \mathbb{F}_q \mid \forall \text{ affine } A, \dim(A) = t, f|_A \in B \}$$
- Lifted families of functions are “nice”
  - Inherit distance of base family (almost)
  - Generalize low-degree property: $B = \{ h: \mathbb{F}_q^{tq,d} \rightarrow \mathbb{F}_q \mid \deg(h) \leq d \}$
  - Yield new codes of “high rate”
- Have a natural test: “Pick random $t$-dim subspace $A$ and test if $\delta(f|_A) \in B$”
  - Does this test work? [Haramaty, Ron-Zewi, S.14] – Yes, with $\epsilon = \epsilon_q$
  - Is the test robust?
    - Don’t know, but ...
    - The $(2t)$-dim test is! [Guo,Haramaty,S’15] with $\alpha = \alpha(\delta(B))$
- Low-degree testing (Theorem 2) follows.
Testing Lifted Codes - 1

• For simplicity $B \subseteq \{h: \mathbb{F}_q \to \mathbb{F}_q\}$ ($t = 1$).

• General geometry + symmetry $\Rightarrow$

  Robustness of $B^\uparrow 4 > 0 \Rightarrow$ Robustness of $B^\uparrow n > 0$

• How to analyze robustness of the test for constant $n$?
Tensors: Key to understanding Lifts

• Given $F \subseteq \{f : S \rightarrow \mathbb{F}_q\}$ and $G \subseteq \{g : T \rightarrow \mathbb{F}_q\}$,
  
  $F \otimes G = \{h : S \times T \rightarrow \mathbb{F}_q | \forall x, y, h(\cdot, y) \in F \& h(x, \cdot) \in G\}$

• $F \otimes^n = F \otimes F \otimes \cdots \otimes F$

• $B^\uparrow_n \subseteq B \otimes^n ; B^\uparrow_n = \cap_T T(B \otimes^n)$ (affine transform $T$)

• $(n - 1)$-dim test for $B \otimes^n$: Fix coordinate at random and test if $f(\cdots, x_i, \cdots) \in B \otimes^{(n-1)}$

• [Viderman’13]: Test is $\alpha \delta_{(B), n}$-robust.

• Hope: Use $B^\uparrow_n = \cap_T T(B \otimes^n)$ to show that testing for random $T(B \otimes^n)$ suffices;
  
  $- \delta_A(f), \delta_B(f)$ small $\not\equiv \delta_{A \cap B} (f)$ small 😞
Actual Analysis

• Say testing $B^{4}$ by querying 2-d subspace.
• Let $C_a = \{ f \mid f|_{\text{line}} \in B \text{ for coordinate parallel line, and line in direction } a\}$
• $B^{4} = \bigcap_{a} C_a$ ;
• $C_a$ not a tensor code, but modification of tensor analysis works!
• $\bigcup_{a} C_a \subseteq B^{4}$ is still an error-correcting code.
  – So $\delta_{C_a}(f), \delta_{C_b}(f)$ small $\Rightarrow \delta_{C_a\cap C_b}(f)$ small!
• Putting things together $\Rightarrow$ Theorem 2.
Wrapping up

• Low-degree testing:
  – Basic, easy to state, problem.
  – Quite useful in complexity, combinatorics.
  – Powerful theorems known.

• Other connections?
Thank You!
(Appendix) References

- Page 7

- Page 9 (See references in survey below)

- Page 14
  - Ran Raz, Shmuel Safra: A Sub-Constant Error-Probability Low-Degree Test, and a Sub-Constant Error-Probability PCP Characterization of NP. *STOC* 1997: 475-484

09/02/2015
CMSA: Low-degree Testing
26 of 25