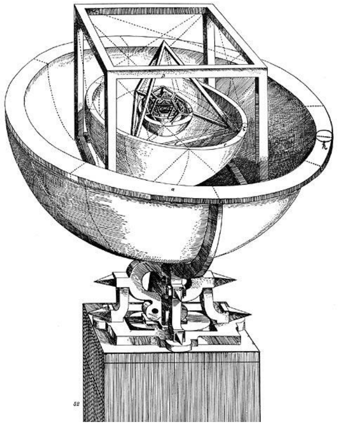
Low-Degree Testing

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.

Source: Michael Fowler, "Galileo & Einstein", U. Virginia

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

Low-degree Testing

- Notation: $\mathbb{F}_q =$ finite field of cardinality q
- Problem: Given $f: \mathbb{F}_q^n \to \mathbb{F}_q$ 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 $\deg(g) \leq d$
      - $\delta(f,g) \triangleq q^{-n} \cdot |\{x \mid f(x) \neq g(x)\}|$

$\deg(x^2 y^3) = 5$

$\deg\left(\sum m\right) = \max(\deg(m))$

Warning: Refinements and Variations later.

This talk

- Some motivations
- Some results
- Some proofs

Why Polynomials? Robustness!

- Polynomial Distance Lemma:
  - Let $f, g: \mathbb{F}_q^n \to \mathbb{F}_q$, w. $\deg(f), \deg(g) \le d$, $f \neq g$
    - $d < q$: $\delta(f,g) \ge 1 - \frac{d}{q}$
    - Generally: $\delta(f,g) \ge q^{-\left(\frac{d}{q-1}\right)}$ (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

- (ℓ, ϵ)-local low-degree test:
  - Selects queries $Q = \{x_1, \ldots, x_\ell\} \subseteq \mathbb{F}_q^n$

    and set $S \subseteq \{h: Q \to \mathbb{F}\}$
  - Accept iff $f|_Q \in S$.
  - Guarantees:
    - $\deg(f) \leq d \Rightarrow$ Accepts w.p. 1
    - $\forall f,\ \Pr[\text{rejection}] \geq \epsilon \cdot \delta_d(f)$
    - (ℓ, α)-robust if $\forall f, \mathbb{E}_{Q,S}[\delta(f|_Q, S)] \geq \alpha \cdot \delta_d(f)$
- General goal: Minimize ℓ while maximizing ϵ, α

$$\delta_d(f) \triangleq \min_{\{g | \deg(g) \leq d\}} \{\delta(f, g)\}$$

$$\frac{\epsilon}{\ell} \leq \alpha \leq \epsilon$$

local distance

vs.

global distance

What can be achieved? $(d = 1)$

- The functions: $\{c_0 + \sum_{i=1}^{n} c_i x_i | c_0 \dots c_n \in \mathbb{F}_q\}$
  - $(n+1)$-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 Π of Assertion T, encode Π using multivariate polynomial encoding;
    - Verify proof $\widehat{\Pi}$ by first a low-degree test; and then "more standard tests".

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]:
    - $G_{n,d,q} = (V, E)$;
      $V = \{f: \mathbb{F}_q^n \rightarrow \mathbb{F}_q, \deg(f) \leq d\}$;
      $(f, g) \in E \Leftrightarrow f - g$ (near)-maximally zero.
    - LDT $\Rightarrow G_{n,d,q}$ is a small-set expander!

Formal Definitions and Parameters

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

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.

$$\forall \text{ affine } A \text{ s.t. } \dim(A) = t, \deg\left(f\,\Big|_A\right) \leq d$$

$$\Rightarrow \deg(f) \leq d$$

- 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 $t_{q,d} = \left\lceil \frac{d+1}{q-\frac{q}{p}} \right\rceil$)

  $\Rightarrow$ Locality of test $\leq q^{\Theta\left(\frac{d}{q}\right)}$
- Codes + duality

  $\Rightarrow$ 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; $d \to \infty$; sound!

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

- Fix $\frac{d}{q} < 1$; $q \to \infty$; 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 $\mathbb{E}_A[\delta_d(f|_A)] \geq \alpha \cdot \delta_d(f)$.

- $d/q \to 0$; 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:
  - $f_a(x) \triangleq f(x+a) - f(a)$ "discrete derivative"
  - $\deg(f) \le d \Rightarrow \deg(f_a) \le d-1$
  - … $\Rightarrow$ $\deg\left(f_{a1,\ldots,a(d+1)}\right) < 0 \Rightarrow f_{a1,\ldots,a(d+1)} = 0$
  - Rejection Prob. $\triangleq \rho(f) = \Pr_{a1\ldots a(d+1)}\left[f_{a1\ldots a(d+1)}\right] \neq 0$
  - $(1-2\rho(f))^{\frac{1}{2^d}}$ 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]:
    - $f = Sym_{2^t}(x_1 \ldots x_n);\ d = 2^t - 1;$
    - $\delta_d(f) = \frac{1}{2} - o_n(1);\ \rho(f) \le \frac{1}{2} - 2^{-7}$

Theorem 1 (contd.)

- So $\rho(f) \nrightarrow \frac{1}{2}$ 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. $\exists H$ s.t. $\deg(f|_H) > d$: defn of testing dimension.
2. $\Pr_H[\deg(f|_H) \leq d] \geq \frac{1}{q} \quad \Leftarrow \deg_{x_i}(f) < q - 1.$
3. … What we needed: $\#\{H \text{ s.t. } \deg(f|_H) \leq d\} \leq O(2^{\mathrm{d}})$

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

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 $B \subseteq \{h: \mathbb{F}_q^t \to \mathbb{F}_q\}$ base family (affine-invariant)
  - Its n-dim lift is
    $$B^{\uparrow n} \triangleq C = \{f: \mathbb{F}_q^n \to \mathbb{F}_q \mid \forall \text{ affine } A, \dim(A) = t, f|_A \in B\}$$
- Lifted families of functions are "nice"
  - Inherit distance of base family (almost)
  - Generalize low-degree property: $B = \left\{h: \mathbb{F}_q^{t_{q,d}} \to \mathbb{F}_q \mid \deg(h) \le d\right\}$
  - 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 ⇒

  Robustness of $B^{\uparrow 4} > 0$ ⇒ Robustness of $B^{\uparrow n} > 0$

- How to analyze robustness of the test for constant n?

Tensors: Key to understanding Lifts

- Given $F \subseteq \{f: S \to \mathbb{F}_q\}$ and $G \subseteq \{g: T \to \mathbb{F}_q\}$,
  $$F \otimes G = \{h: S \times T \to \mathbb{F}_q \mid \forall x, y, h(\cdot, y) \in F \,\&\, h(x, \cdot) \in G\}$$
- $F^{\otimes n} = F \otimes F \otimes \cdots \otimes F$
- $B^{\uparrow n} \subseteq B^{\otimes n}$; $B^{\uparrow n} = \cap_T T(B^{\otimes n})$ (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 $B^{\uparrow 4}$ by querying 2-d subspace.
- Let $C_a = \{f \mid f|_{\text{line}} \in B$ for coordinate parallel line, and line in direction a}
- $B^{\uparrow 4} = \cap_a C_a$;
- C_a not a tensor code, but modification of tensor analysis works!
- $\cup_a C_a \subseteq B^{\otimes 4}$ 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
  - Manuel Blum, Michael Luby, Ronitt Rubinfeld: Self-Testing/Correcting with Applications to Numerical Problems. J. Comput. Syst. Sci. 47(3): 549-595 (1993)
  - Mihir Bellare, Don Coppersmith, Johan Håstad, Marcos A. Kiwi, Madhu Sudan: Linearity testing in characteristic two. IEEE Transactions on Information Theory 42(6): 1781-1795 (1996)
- Page 9 (See references in survey below)
  - **Probabilistically Checkable Proofs**, Madhu Sudan. *Communications of the ACM*, 52(3):76-84, March 2009.
- Page 14
  - **Optimal testing of Reed-Muller codes**. Arnab Bhattacharyya, Swastik Kopparty, Grant Schoenebeck, Madhu Sudan, and David Zuckerman. *Electronic Colloquium on Computational Complexity*, Technical Report TR 09-086, October 2, 2009.
  - **Optimal testing of multivariate polynomials over small prime fields**. Elad Haramaty, Amir Shpilka, and Madhu Sudan. *SIAM Journal on Computing,* 42(2): 536--562, April 2013.
  - **Absolutely Sound Testing of Lifted Codes**. Elad Haramaty, Noga Ron-Zewi and Madhu Sudan. *Electronic Colloquium on Computational Complexity*, Technical Report TR 13-030, February 20, 2013.
  - Alan Guo, Elad Haramaty, Madhu Sudan: Robust testing of lifted codes with applications to low-degree testing. Electronic Colloquium on Computational Complexity (ECCC) 22: 43 (2015)
  - 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