Algebraic Property Testing: A Survey

Madhu Sudan
MIT

Algebraic Property Testing: Personal Perspective

Madhu Sudan
MIT

Algebraic Property Testing: Personal Perspective

Madhu Sudan
MIT

Property Testing

- Distance: $\delta(f,g) = \Pr_{x\in D}[f(x) \neq g(x)]$
  $\delta(f,\mathcal{F}) = \min_{g\in\mathcal{F}}\{\delta(f,g)\}$
  $f \approx_\epsilon g$ if $\delta(f,g) \leq \epsilon$.
- Definition:
  $\mathcal{F}$ is (k,ϵ,δ)-locally testable if
  $\exists$ a k-query tester T s.t.
  $f \in \mathcal{F} \quad \Rightarrow \quad T^f$ accepts w.p. $\geq 1-\epsilon$
  $\delta(f,\mathcal{F}) \geq \delta \Rightarrow \quad T^f$ rejects w.p. $\geq \epsilon$.
- Notes: k-locally testable implies $\exists \epsilon, \delta > 0$
  locally testable implies $\exists k = O(1)$
  One-sided error: Accept $f \in \mathcal{F}$ w.p. 1

Brief History

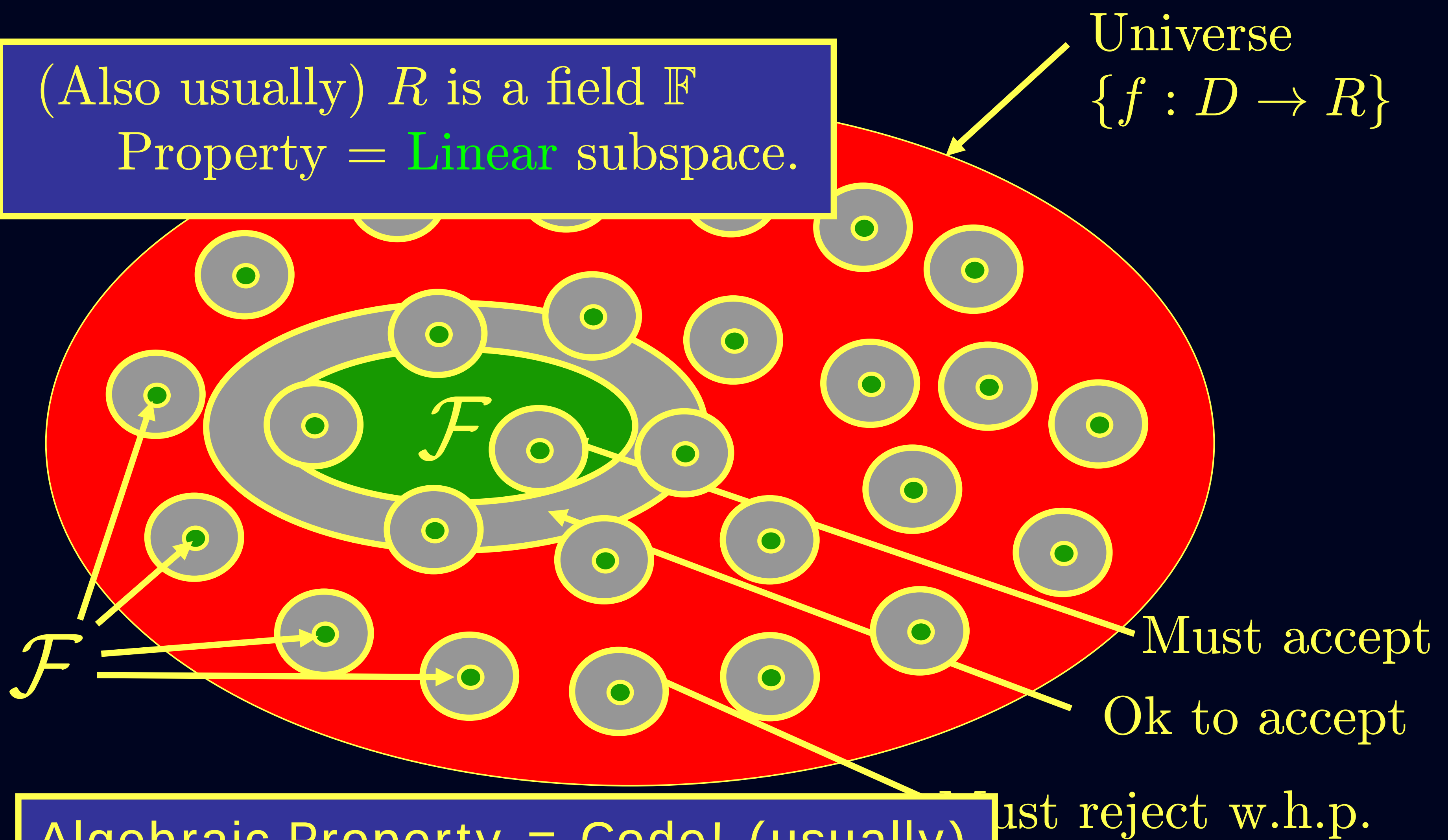
- [Blum,Luby,Rubinfeld – S'90]
  - Linearity + application to program testing
- [Babai,Fortnow,Lund – F'90]
  - Multilinearity + application to PCPs (MIP).
- [Rubinfeld+S.]
  - Low-degree testing + Formal Definition
- [Goldreich,Goldwasser,Ron]
  - Graph property testing.
- Since then … many developments
  - Graph properties
  - Statistical properties
  - More algebraic properties

Specific Directions in Algebraic P.T.

- More Properties
  - Low-degree ($d < q$) functions [RS]
  - Moderate-degree ($q < d < n$) functions
    - $q=2$: [AKKLR]
    - General q: [KR, JPRZ]
  - Long code/Dictator/Junta testing [PRS]
  - BCH codes (Trace of low-deg. poly.) [KL]
  - All nicely "invariant" properties [KS]
- Better Parameters (motivated by PCPs).
  - #queries, high-error, amortized query complexity, reduced randomness.

Contrast w. Combinatorial P.T.

(Also usually) R is a field $\mathbb{F}$
Property = Linear subspace.



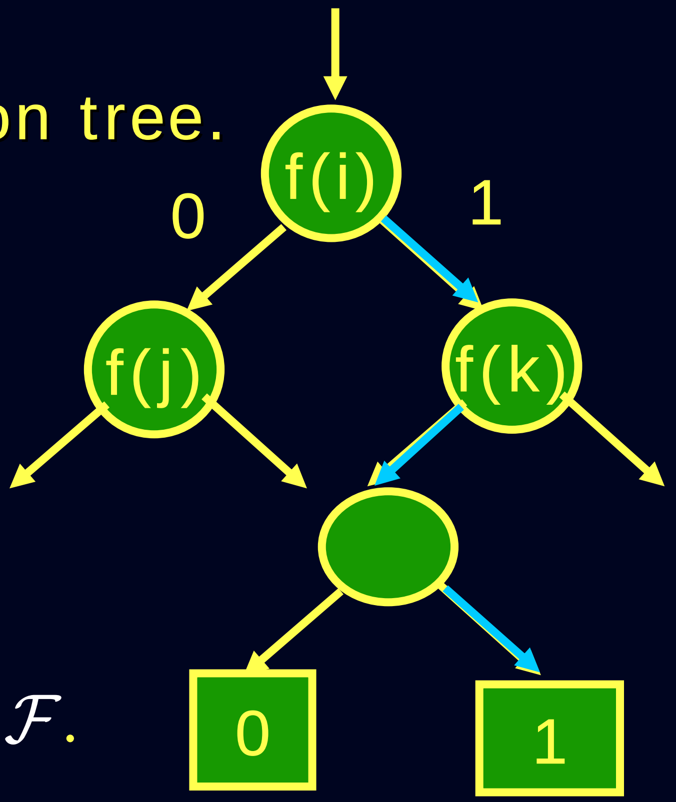
Algebraic Property = Code! (usually)

Goal of this talk

- Implications of linearity
  - Constraints, Characterizations, LDPC structure
  - One-sided error, Non-adaptive tests [BHR]
- Redundancy of Constraints
  - Tensor Product Codes
- Symmetries of Code
  - Testing affine-invariant codes
    - Yields basic tests for all known algebraic codes (over small fields).

Basic Implications of Linearity [BHR]

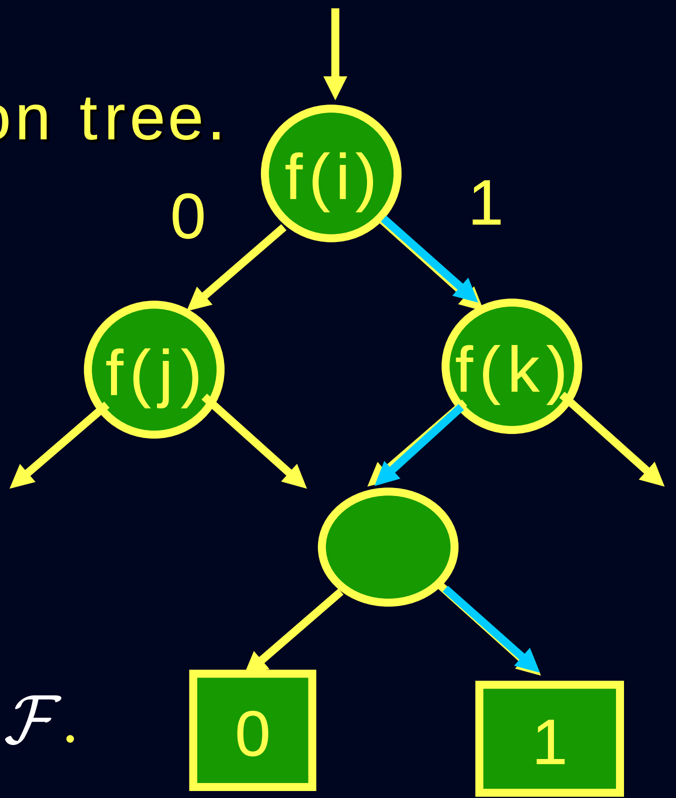
- Generic adaptive test = decision tree.



- Pick path followed by random $g \in \mathcal{F}$.
- Query f according to path.
- Accept iff f on path consistent with some $h \in \mathcal{F}$.
- Yields non-adaptive one-sided error test for linear $\mathcal{F}$.

Basic Implications of Linearity [BHR]

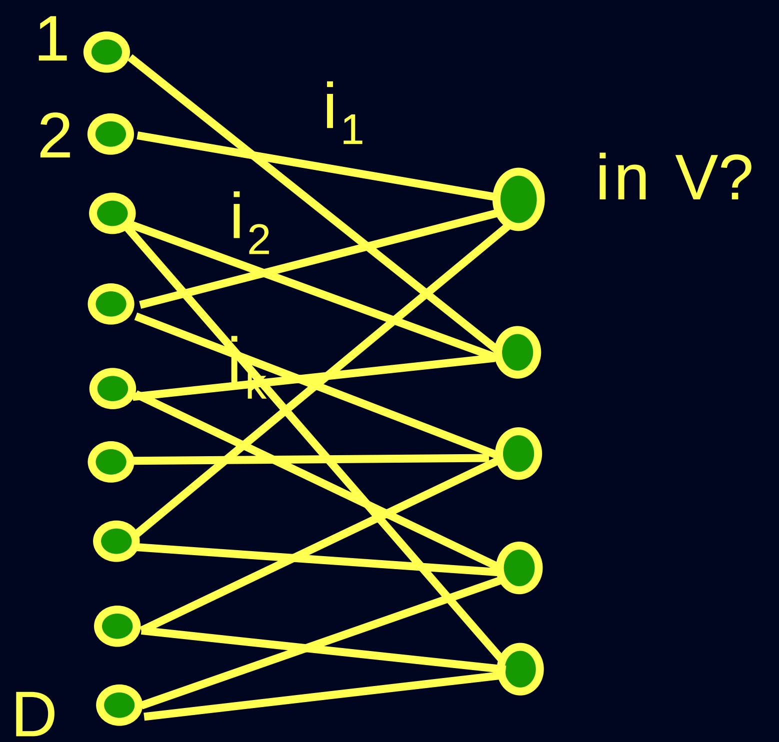
- Generic adaptive test = decision tree.



- Pick path followed by random $g \in \mathcal{F}$.
- Query f according to path.
- Accept iff f on path consistent with some $h \in \mathcal{F}$.
- Yields non-adaptive one-sided error test for linear $\mathcal{F}$.

Constraints, Characterizations

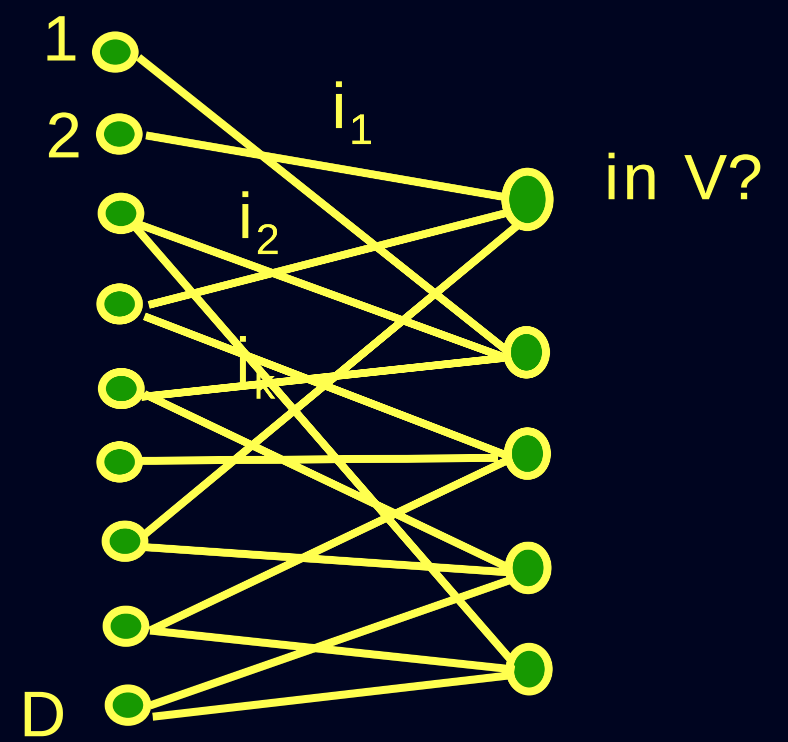
- Say test queries $i_1, \ldots, i_k$ accepts $\langle f(i_1), \ldots, f(i_k) \rangle \in V \neq \mathbb{F}^k$
- $(i_1, \ldots, i_k; V) =$ Constraint
  Every $f \in \mathcal{F}$ satisfies it.
- If every $f \notin \mathcal{F}$ rejected w. positive prob. then $\mathcal{F}$ characterized by constraints.



- Like LDPC Codes!

Constraints, Characterizations

- Say test queries $i_1, \ldots, i_k$ accepts $\langle f(i_1), \ldots, f(i_k) \rangle \in V \neq \mathbb{F}^k$
- $(i_1, \ldots, i_k; V)$ = Constraint. Every $f \in \mathcal{F}$ satisfies it.
- If every $f \notin \mathcal{F}$ rejected w. positive prob. then $\mathcal{F}$ characterized by constraints.



- Like LDPC Codes!

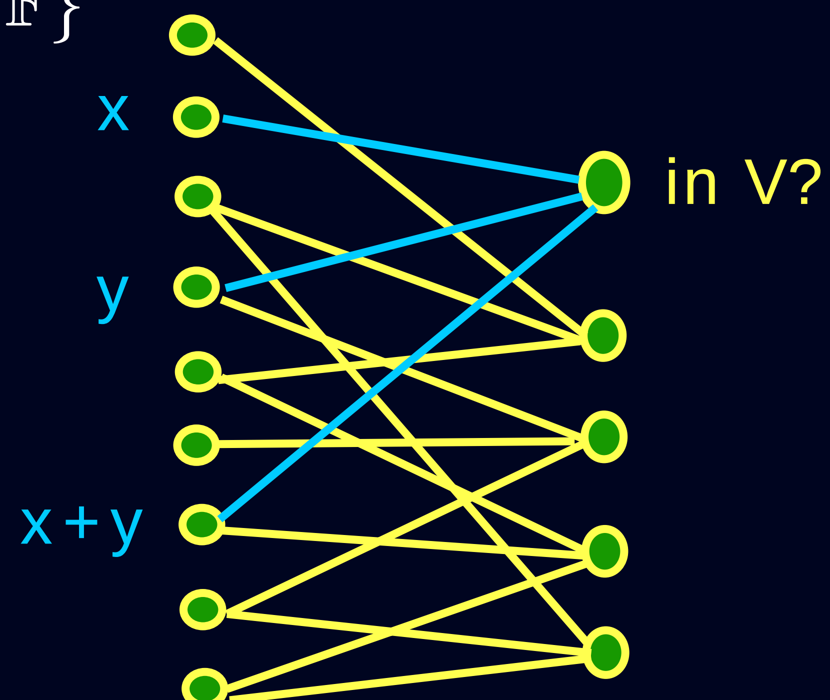
Example: Linearity Testing [BLR]

- Constraints:

$$C_{x,y} = (x, y, x+y; V) | x, y \in \mathbb{F}^n \text{ where}$$
$$V = \{(a, b, a+b) | a, b \in \mathbb{F}\}$$

- Characterization:

f is linear iff
$\forall x, y, C_{x,y}$ satisfied



Insufficiency of local characterizations

- [Ben-Sasson, Harsha, Raskhodnikova]
- There exist families $\mathcal{F}$ characterized by k-local constraints that are not o(|D|)-locally testable.
- Proof idea: Pick LDPC graph at random …
  (and analyze resulting property)

Why are characterizations insufficient?

- Constraints too minimal.
  - Not redundant enough!
    - Proved formally in [Ben-Sasson, Guruswami, Kaufman, S., Viderman]
- Constraints too asymmetric.
  - Property must show some symmetry to be testable.
    - Not a formal assertion ... just intuitive.

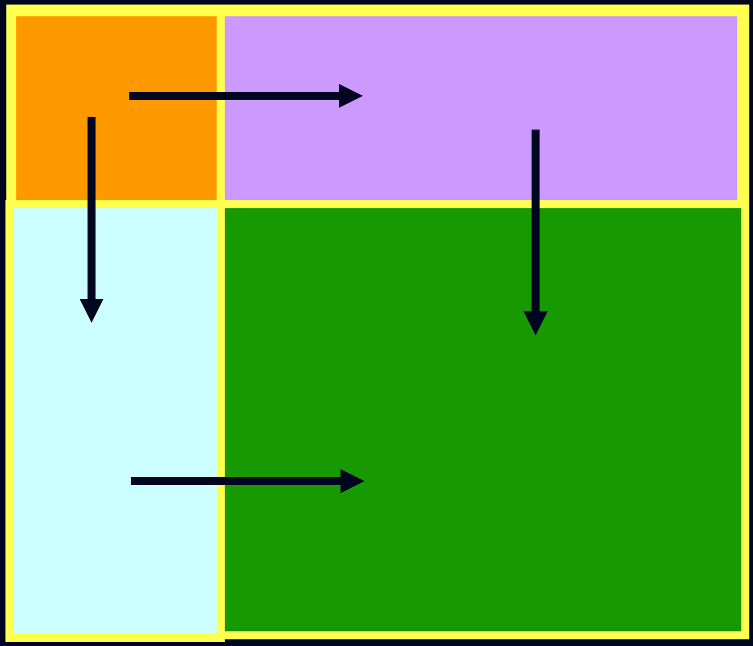
Redundancy?

- E.g. Linearity Test:
  – $\Omega(D^2)$ constraints on domain D
- Standard LDPC analysis:
  – $\text{Dimension}(\mathcal{F}) \approx D - m$ for m constraints.
  – Requires #constraints $< D$.
  – Does not allow much redundancy!
- What natural operations create redundant local constraints?
  - Tensor Products!

Tensor Products of Codes!

- Tensor Product: $\mathcal{F} \times \mathcal{G}$
  $= \{$ Matrices such every row in $\mathcal{F}$ and every column in $\mathcal{G}$ $\}$

- Redundancy?
  Suppose $\mathcal{F}$, $\mathcal{G}$ systematic
  First ℓ entries free
  rest determined by them.



Free

$\mathcal{F}$ determined

$\mathcal{G}$ determined

determined twice, by $\mathcal{F}$ and $\mathcal{G}$!

Testability of tensor product codes?

- Natural test:
  - Given Matrix M
    - Test if random row in F
    - Test if random column in G
- Claim:
  - If F, G codes of constant (relative) distance; then if test accepts w.h.p. then M is close to codeword of F x G
- Yields $O(\sqrt{n})$ local test for codes of length n.
  - Can we do better? Exploit local testability of F, G?

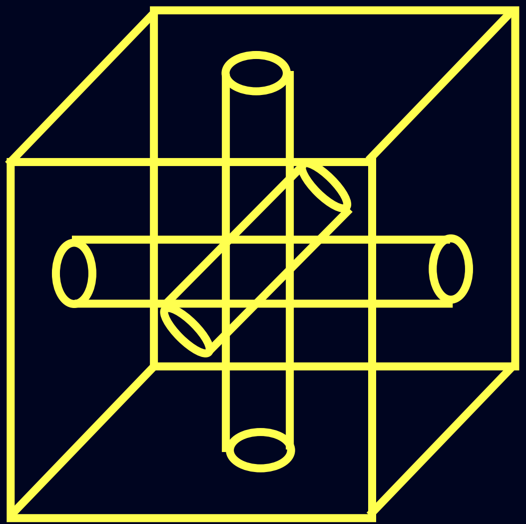
Robust testability of tensors?

- Natural test (if F,G locally testable):
  - Given Matrix M
    - Run Local Test for F on random row
    - Test that random row *close* to F
    - Run Local Test for G on random column
    - Test that random column *close* to G
- Suppose M close on most rows/columns to F, G. Does this imply M is close to F x G?
  - Generalizes test for bivariate polynomials. True for F, G = class of low-degree polynomials. [BFLS, Arora+Safra, Polishchuk+Spielman].
  - General question raised by [Ben-Sasson+S.]
  - [P. Valiant] Not true for every F, G !
  - [Dinur, S., Wigderson] True if F (or G) locally testable.

Tensor Products and Local Testability

- Robust testability allows easy induction (essentially from [BFL, BFLS]; see also [Ben-Sasson+S.])

  - Let $\mathcal{F}^n = n$-fold tensor of $\mathcal{F}$.



- Given $f : D^n \to \mathbb{F}$

  Natural test: Pick random axis-parallel line

  verify $f\big|_{\text{line}} \in \mathcal{F}$

Robust testability of tensors (contd.)

- Unnatural test (for F x F x F):
  - Given 3-d matrix M:
    - Pick random 2-d submatrix.
    - Verify it is close to F x F

- Theorem [BenSasson+S., based on Raz+Safra]: Distance to F x F x F proportional to average distance of random 2-d submatrix to F x F.

- [Meir]: “Linear-algebraic” construction of Locally Testable Codes (matching best known parameters) using this (and many other ingredients).

Redundant Characterizations (contd.)

- Redundant constraints necessary for testing [BGKSV]

- How to get redundancy?
  - Tensor Products
    - Sufficient to get some local testability
  - Invariances (Symmetries)
    - Sufficient?
  - Counting (See Tali's talk)

Testing by symmetries

Invariance & Property testing

- Invariances (Automorphism groups):

  For permutation $\pi : D \to D$, $\mathcal{F}$ is π-invariant if
  $f \in \mathcal{F}$ implies $f \circ \pi \in \mathcal{F}$.

  $\mathrm{Aut}(\mathcal{F}) = \{\pi \mid \mathcal{F} \text{ is } \pi\text{-invariant}\}$

  Forms group under composition.

- Hope: If Automorphism group is “large” (“nice”), then property is testable.

Examples

- Majority:
  - Aut group $= S_D$ (full group).
  - Easy Fact: If $\text{Aut}(\mathcal{F}) = S_D$ then $\mathcal{F}$ is poly$(R, 1/\epsilon)$-locally testable.
- Graph Properties:
  - Aut. group given by renaming of vertices
  - [AFNS, Borgs et al.] implies *regular* properties with this Aut group are testable.
- Algebraic Properties: What symmetries do they have?

Algebraic Properties & Invariances

- Properties:
  $D = \mathbb{F}^n$, $R = \mathbb{F}$ (Linearity, Low-degree, Reed-Muller)
  Or $D = \mathbb{K} \supseteq \mathbb{F}$, $R = \mathbb{F}$ (Dual-BCH) $(\mathbb{K}, \mathbb{F}$ finite fields)
- Automorphism groups?
  Linear transformations of domain.
  $\pi(x) = Ax$ where $A \in \mathbb{F}^{n \times n}$ (Linear-Invariant)
  Affine transformations of domain.
  $\pi(x) = Ax + b$ where $A \in \mathbb{F}^{n \times n}, b \in \mathbb{F}^n$ (Affine-Inv.)
- Question: Are Linear/Affine-Inv., Locally Characterized Props. Testable? ([Kaufman + S.])

Linear-Invariance & Testability

- Unifies previous studies on Alg. Prop. Testing.
  (And captures some new properties)

- Nice family of 2-transitive group of symmetries.

- Conjecture [Alon, Kaufman, Krivelevich, Litsyn, Ron] : Linear code with k-local constraint and 2-transitive group of symmetries must be testable.

Some Results [Kaufman + S.]

- Theorem 1: $\mathcal{F} \subseteq \{\mathbb{K}^n \to \mathbb{F}\}$ linear, linear-invariant,
  k-locally characterized
  implies $\mathcal{F}$ is $f(\mathbb{K}, k)$-locally testable.

- Theorem 2: $\mathcal{F} \subseteq \{\mathbb{K}^n \to \mathbb{F}\}$ linear, *affine*-invariant,
  has k-local *constraint*
  implies $\mathcal{F}$ is $f(\mathbb{K}, k)$-locally testable.

Examples of Linear-Invariant Families

- Linear functions from $\mathbb{F}^n$ to $\mathbb{F}$.
- Polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ of degree at most d
- Traces of Poly in $\mathbb{K}[x_1, \ldots, x_n]$ of degree at most d
- (Traces of) Homogenous polynomials of degree d
- $\mathcal{F}_1 + \mathcal{F}_2$, where $\mathcal{F}_1$, $\mathcal{F}_2$ are linear-invariant.
  Polynomials supported by degree $2, 3, 5, 7$ monomials.

What Dictates Locality of Characterizations?

- Precise locality not yet understood:
  Depends on p-ary representation of degrees.
  Example: $\mathcal{F}$ supported by monomials $x^{p^i+p^j}$
  behaves like degree two polynomial

- For affine-invariant family dictated (coarsely)
  by highest degree monomial in family

- For some linear-invariant families,
  can be *much* less than the highest degree monomial.

Example: $\mathbb{K} = \mathbb{F} = \mathbb{F}_7$; $\mathcal{F} = \mathcal{F}_1 + \mathcal{F}_2$

$\mathcal{F}_1$ = poly of degree at most 16

$\mathcal{F}_2$ = poly supported on monomials of degree $3 \mod 6$.

Degree$(\mathcal{F}) = \Omega(n)$; Locality$(\mathcal{F}) \leq 49$.

Property Testing from Invariances

Key Notion: Formal Characterization

– $\mathcal{F}$ has single-orbit characterization if $\exists$ a *single* constraint $C = (x_1, \ldots, x_k; V)$ such that $\{C \circ \pi\}_{\pi \in \mathrm{Aut}(\mathcal{F})}$ characterize $\mathcal{F}$.

Theorem: If $\mathcal{F}$ has single-orbit characterization by a k-local constraint (with some restrictions) then it is k-locally testable.

Rest of talk: Analysis (extending BLR)

BLR Analysis: Outline

- Have f s.t. $\Pr_{x,y}[f(x)+f(y) \neq f(x+y)] = \delta < 1/20$.
  Want to show f close to some $g \in \mathcal{F}$.
- Define $g(x) = \text{most likely}_y\{f(x+y) - f(y)\}$.
- If f close to $\mathcal{F}$ then g will be in $\mathcal{F}$ and close to f.
- But if f not close? g may not even be uniquely defined!
- Steps:
  - Step 0: Prove f close to g
  - Step 1: Prove *most likely* is overwhelming majority.
  - Step 2: Prove that g is in $\mathcal{F}$.

BLR Analysis: Step 0

- Define $g(x) =$ most likely $_y\{f(x+y) - f(y)\}$.

Claim: $\Pr_x[f(x) \neq g(x)] \leq 2\delta$

- Let $B = \{x | \Pr_y[f(x) \neq f(x+y) - f(y)] \geq \frac{1}{2}\}$
- $\Pr_{x,y}[$linearity test rejects $|x \in B] \geq \frac{1}{2}$

  $\Rightarrow \Pr_x[x \in B] \leq 2\delta$
- If $x \notin B$ then $f(x) = g(x)$

BLR Analysis: Step 1

$\text{Vote}_x(y)$

- Define $g(x) = \text{most likely}\ _y\{f(x+y) - f(y)\}$.
- Suppose for some x, $\exists$ two equally likely values. Presumably, only one leads to linear x, so which one?
- If we wish to show g linear, then need to rule out this case.

Lemma: $\forall\, x,\ \Pr_{y,z}[\text{Vote}_x(y) \neq \text{Vote}_x(z))] \leq 4\delta$

$\text{Vote}_x(y)$

BLR Analysis: Step 1

- Define $g(x) = \text{most likely}\ _y\{f(x+y) - f(y)\}$.
- Suppose for some x, $\exists$ two equally likely values.
  Presumably, only one leads to linear x, so which one?
- If we wish to show g linear,
  then need to rule out this case.

Lemma: $\forall\, x$, $\Pr_{y,z}[\text{Vote}_x(y) \neq \text{Vote}_x(z))] \leq 4\delta$

BLR Analysis: Step 1

Vote$_x(y)$

- Define $g(x) = \text{most likely}_y \{f(x+y) - f(y)\}$.

Lemma: $\forall\, x$, $\Pr_{y,z}[\text{Vote}_x(y) \neq \text{Vote}_x(z))] \leq 4\delta$

?	$f(y)$	$-f(x+y)$
$f(z)$	$f(y+z)$	$-f(y+2z)$
$-f(x+z)$	$-f(2y+z)$	$f(x+2y+2z)$

Prob. Row/column sum non-zero $\leq \delta$.

BLR Analysis: Step 1

$\mathrm{Vote}_x(y)$

- Define $g(x) = \text{most likely}_{\,y}\{f(x+y) - f(y)\}$.

Lemma: $\forall\, x$, $\Pr_{y,z}[\mathrm{Vote}_x(y) \neq \mathrm{Vote}_x(z))] \leq 4\delta$

?	$f(y)$	$-f(x+y)$
$f(z)$	$f(y+z)$	$-f(y+2z)$
$-f(x+z)$	$-f(2y+z)$	$f(x+2y+2z)$

Prob. Row/column sum non-zero $\leq \delta$.

BLR Analysis: Step 2 (Similar)

Lemma: If $\delta < \frac{1}{20}$, then $\forall\, x, y$, $g(x) + g(y) = g(x+y)$

$g(x)$	$g(y)$	$-g(x+y)$
$f(z)$	$f(y+z)$	$-f(y+2z)$
$-f(x+z)$	$-f(2y+z)$	$f(x+2y+2z)$

Prob. Row/column sum non-zero $\leq 4\delta$.

Our Analysis: Outline

- f s.t. $\Pr_L[\langle f(L(x_1),\ldots,f(L(x_k))\rangle \in V] = \delta \ll 1$.
- Define $g(x) = \alpha$ that maximizes $\Pr_{\{L|L(x_1)=x\}}[\langle \alpha, f(L(x_2)),\ldots,f(L(x_k))\rangle \in V]$
- Steps:
  - Step 0: Prove f close to g
  - Step 1: Prove "most likely" is overwhelming majority.
  - Step 2: Prove that g is in $\mathcal{F}$.

Our Analysis: Outline

- f s.t. $\Pr_L[\langle f(L(x_1),\ldots,f(L(x_k))\rangle \in V] = \delta \ll 1$.
- Define $g(x) = \alpha$ that maximizes
  $\Pr_{\{L|L(x_1)=x\}}[\langle \alpha, f(L(x_2)),\ldots,f(L(x_k))\rangle \in V]$

Same as before

- Steps:
  - Step 0: Prove f close to g
  - Step 1: Prove "most likely" is overwhelming majority.
  - Step 2: Prove that g is in $\mathcal{F}$.

$\text{Vote}_x(L)$

Matrix Magic?

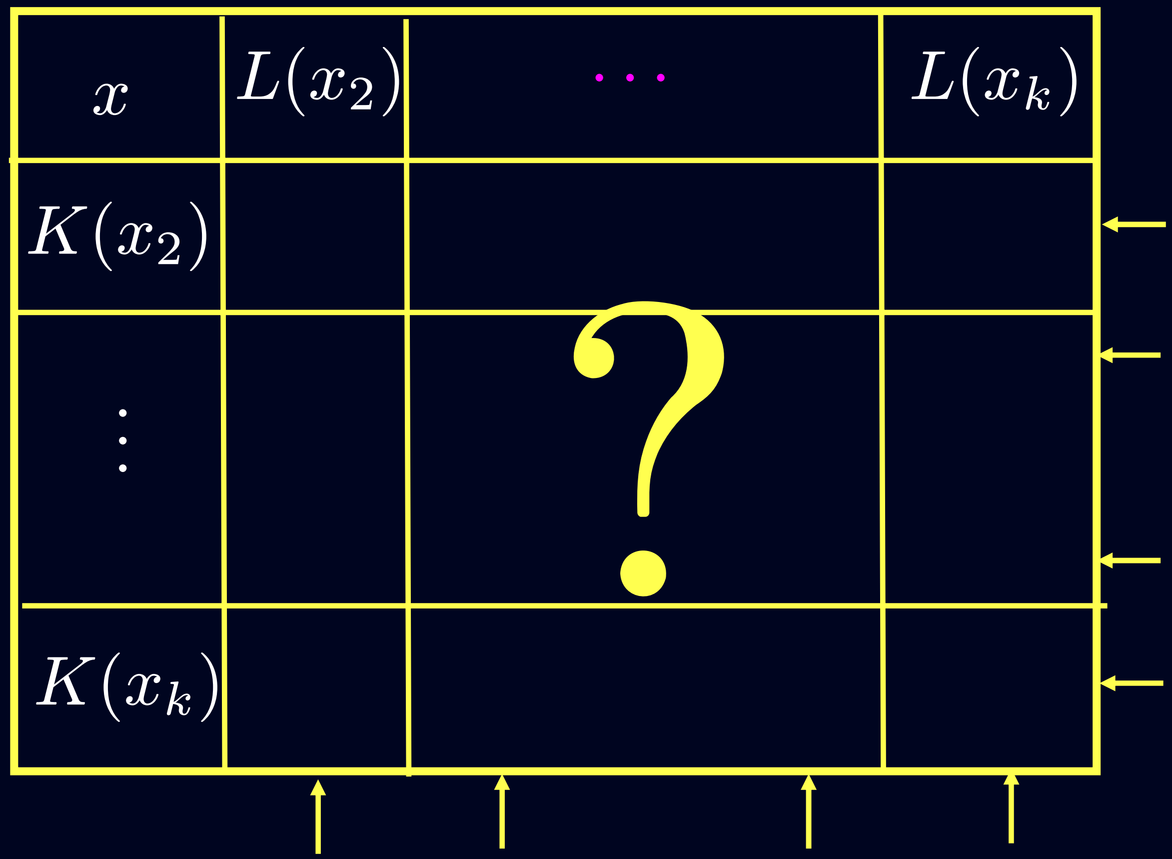
- Define $g(x) = \alpha$ that maximizes

$$\Pr_{\{L \mid L(x_1)=x\}}[\langle \alpha, f(L(x_2)), \ldots, f(L(x_k))\rangle \in V]$$

Lemma: $\forall\, x$, $\Pr_{L,K}[\text{Vote}_x(L) \neq \text{Vote}_x(K))] \leq 2(k-1)\delta$

x	$L(x_2)$	$\cdots$	$L(x_k)$
$K(x_2)$			
$\vdots$		?	
$K(x_k)$			

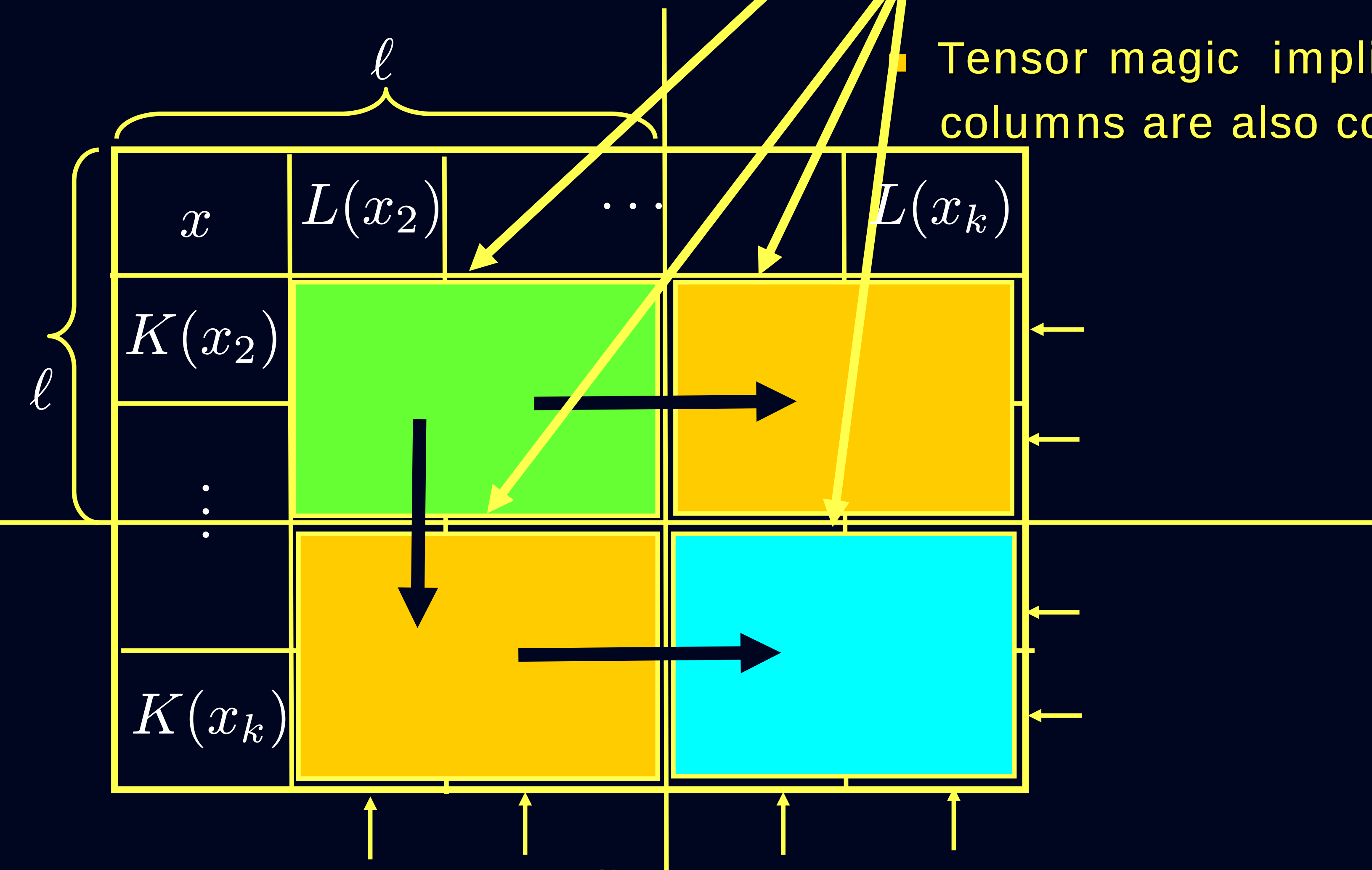
Matrix Magic?



- Want marked rows to be random constraints.
- Suppose $x_1, \ldots, x_\ell$ linearly independent; and rest dependent on them.

Matrix Magic?

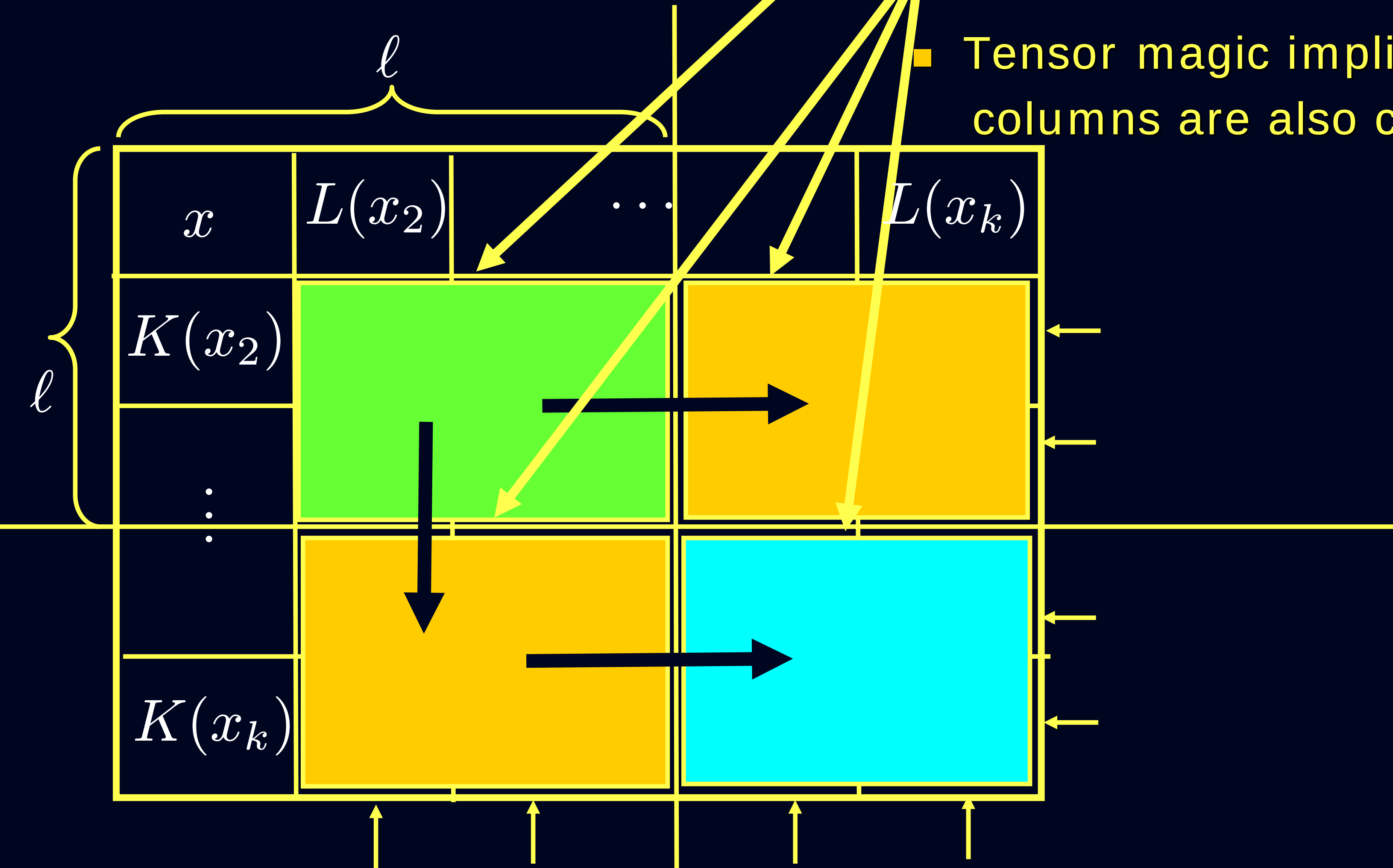
- Fill with random entries
- Fill so as to form constraints
- Tensor magic implies final columns are also constraints.



- Suppose $x_1, \ldots, x_\ell$ linearly independent; and rest dependent on them.

Matrix Magic?

- Fill with random entries
- Fill so as to form constraints
- Tensor magic implies final columns are also constraints!



- Suppose $x_1, \ldots, x_\ell$ linearly independent; and rest dependent on them.

Summarizing

- Affine invariance + single-orbit characterizations imply testing.
- Unifies analysis of linearity test, basic low-degree tests, moderate-degree test (all A.P.T. except dual-BCH?)

Concluding thoughts - 1

- Didn't get to talk about
  - PCPs, LTCs (though we did implicitly)
  - Optimizing parameters
  - Parameters

- In general
  - Broad reasons why property testing works worth examining.
  - Tensoring explains a few algebraic examples.
  - Invariance explains many other algebraic ones.

    (More about invariances in [Grigorescu,Kaufman,S. '08], [GKS'09])

Concluding thoughts - 2

- Invariance:
  - Seems to be a nice lens to view all property testing results (combinatorial, statistical, algebraic).
  - Many open questions:
    - What groups of symmetries aid testing?
    - What additional properties needed?
      - Local constraints?
      - Linearity?
    - Does sufficient symmetry imply testability?
      - Give an example of a non-testable property with a k-single orbit characterization.

Thank You!