Algebraic Property Testing

Tali Kaufman
Madhu Sudan
} MIT

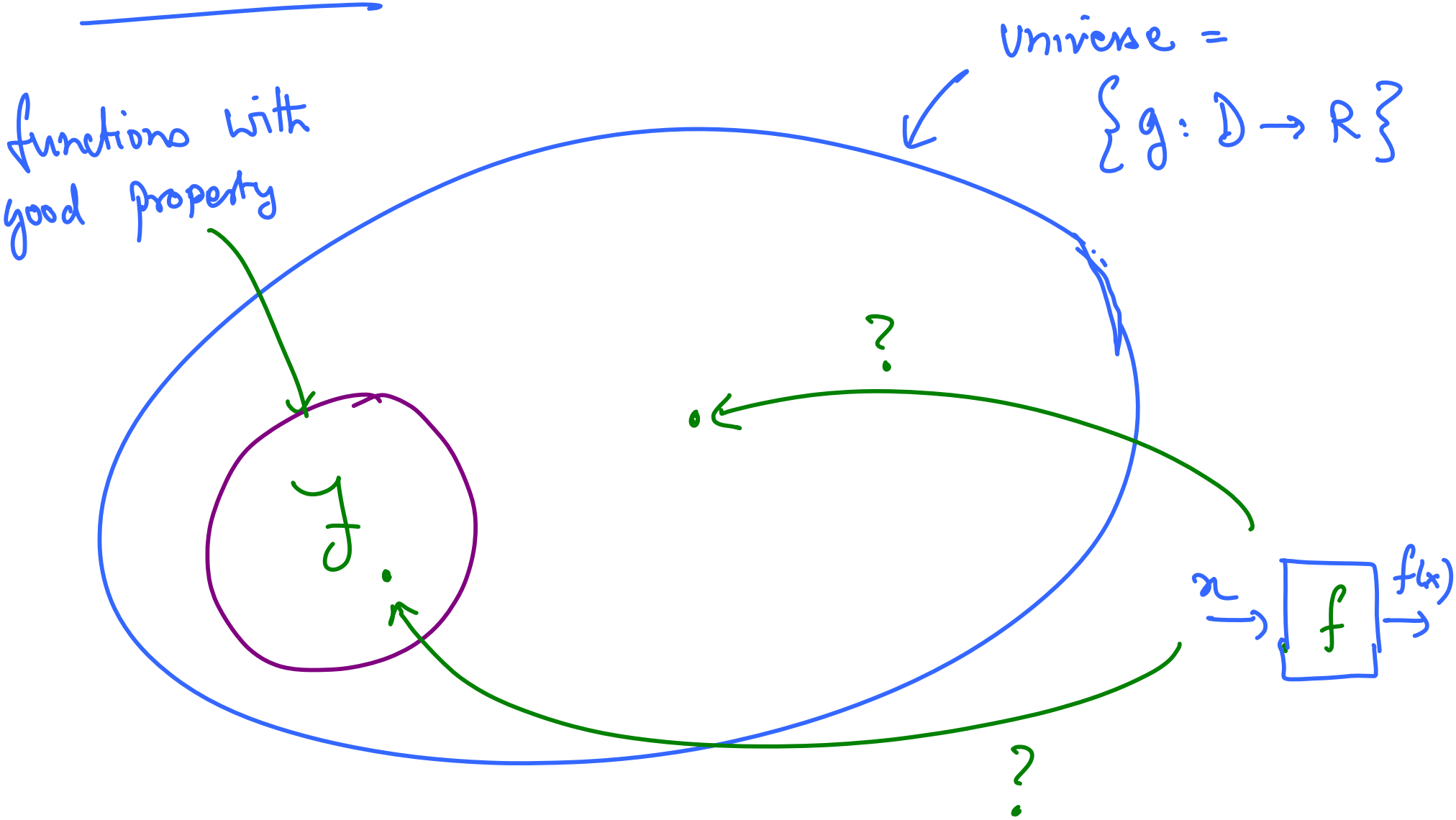
Outline

1. Property Testing : Definition
2. Brief History
3. Our Results
4. Blum-Luby-Rubinfeld Analysis
5. Sketch Of Our Analysis

Property Testing (Motivation)

- Have a program f.
- Safety Property for programs $\mathcal{F}$.
- Want quick (& dirty) test to see if program satisfies safety property.
  i.e. Does $f \in \mathcal{F}$?

PICTORIALLY

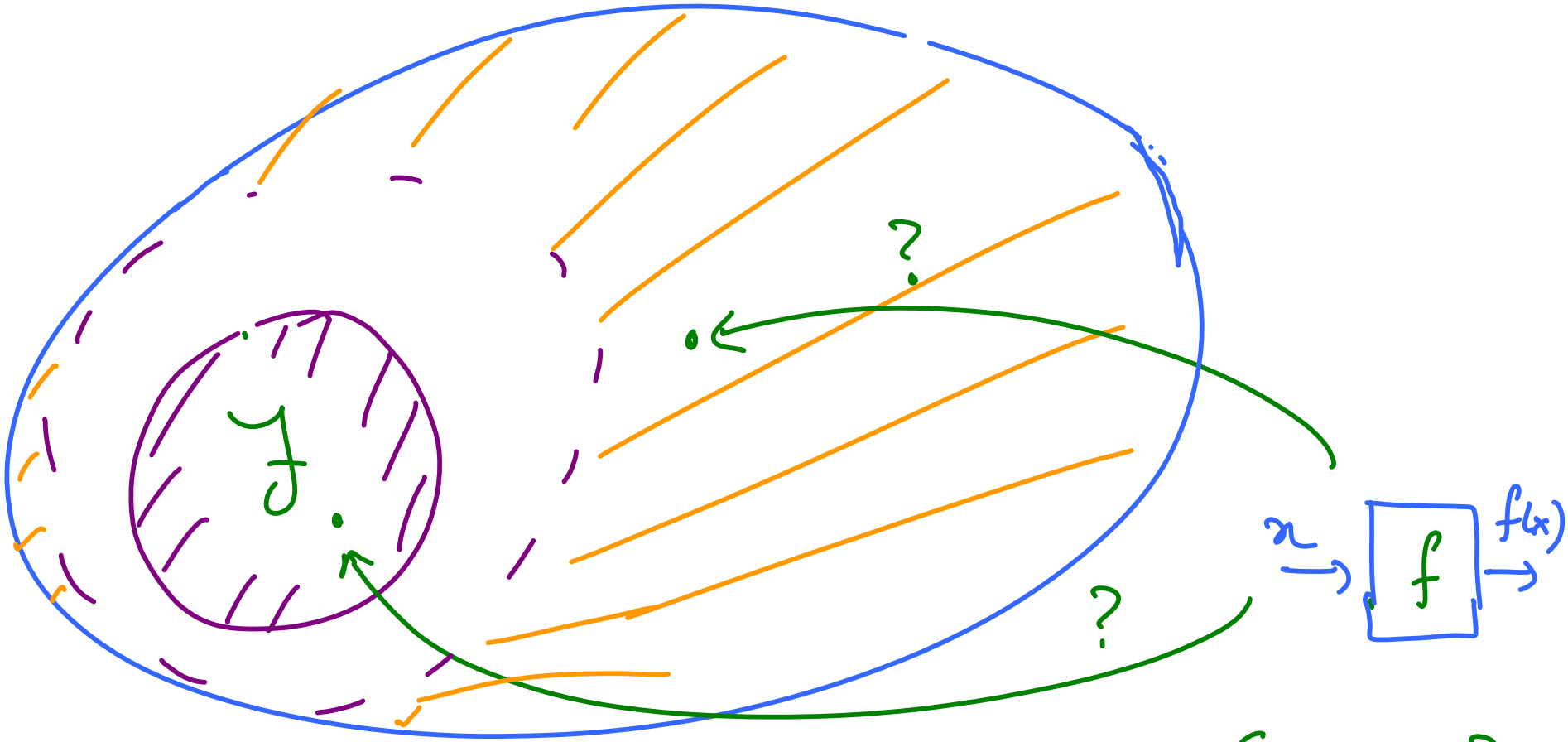


Quick + Dirtiness

- Have oracle access to f.
- Wish to access oracle very few ($O(1)$) times.
- Willing to be "flexible" with what is accepted.

Suffices to distinguish $f \in \mathcal{F}$ from f s.t $\delta(f, \mathcal{F}) \geq \epsilon$

PICTORIALLY



$$\delta(f,g) = \Pr_{x \in D}[f(x) \neq g(x)] \quad ; \quad \delta(f,\mathcal{F}) = \min_{g \in \mathcal{F}} \{\delta(f,g)\}$$

Example 1: Homomorphisms - [Blum Luby Rubinfeld]

- $D = G_1$ group ; $R = H$ group.
- $\mathcal{Y}$ = collection of homomorphisms from $G_1 \to H$

$$= \left\{ \phi : G_1 \to H \;\middle|\; \forall x, y \quad \phi(x) + \phi(y) = \phi(x+y) \right\}$$

- Tester for property:

Pick $x, y \in G_1$ at random & test

" is $f(x) + f(y) = f(x+y)$? "

[BLR Analysis]

- if f is a homomorphism, test always accepts (by defn.)
- if $\delta(f, \text{Hom}) \geq \epsilon$; then test rejects w.p. $\frac{2}{9} \cdot \epsilon$.

(non-trivial !!)

(actually show contrapositive ...

Rejection Prob. $(f) = \tau < \frac{2}{9} \Rightarrow \delta(f, \text{Hom}) \leq 2\tau$.

Example 2

- f represents graph G_f on vertex set D

  $i \leftrightarrow j \iff f(i,j) = 1$.

- $\mathcal{Y} = \{ f \mid G_f \text{ is 3-colorable} \}$

- Test = Pick $k = k(\epsilon)$ vertices at random.

  Accept if induced subgraph is 3-col.

[Goldreich Goldwasser Ron] Analysis

- f is 3-col $\Rightarrow$ Test accepts w.p. 1

  [obvious]

- f is ϵ-far from 3-col

  $\Rightarrow$ Test rejects w.p. $\Omega(\epsilon)$

  [non-trivial]

History

Algebraic Properties

- f is low-degree polynomial
- f is a Reed-Muller codeword
- f is a Dual-BCH codeword

But no general theorem

Combinatorial Properties

- f has dense cuts
- f has sparse cuts
- ⋮
- f is hereditary
- f is monotone

[ALON + SHAPIRA]

Our Results

Some general results in algebraic property testing.

Theorem 1: Let $\mathcal{F} \subseteq \{f : K^n \to \mathbb{F}\}$ be

- affine-invariant + $\mathbb{F}$-linear
- have k-local characterization

then $\mathcal{F}$ has k-query property tester.

Theorem 2: There exist many interesting $\mathcal{J}$ satisfying conditions of Theorem 1; in particular if $\mathcal{J}$ has an ℓ-local constraint $\Rightarrow$ $\mathcal{J}$ has a $R(\ell)$-local characterization (when $\mathbb{K} = \mathbb{F}$)

Notation used in Theorem 1

- K, F finite fields, $F \subseteq K$.
- $\mathcal{Y}$ is F-linear if $\forall\ f, g \in \mathcal{Y}$

  $\alpha, \beta \in F$

  $\alpha f + \beta g \in F$
- $\mathcal{Y}$ is affine-invariant if $\forall$ affine maps $A: K^n \to K^n$

  $\forall\ f \in \mathcal{Y}$

  - $f \circ A \in \mathcal{Y}$.

Notation (cohtd.)

- $\mathcal{J}$ has <u>ℓ-local constraint</u> if $\exists\ x_1, \ldots x_\ell$ & $C \subsetneq \mathbb{F}^\ell$

s.t. $\forall\ f \in \mathcal{J}$

$$\langle f(x_1), f(x_2), \ldots f(x_\ell) \rangle \in C$$

- $\mathcal{J}$ has <u>ℓ-local characterization</u> if the above condition is "if and only if".

Example:

$K = F = GF(2)$;

$\mathcal{F}$ = Homomorphisms from $\mathbb{F}_2^n \to \mathbb{F}_2$

- $\mathcal{F}$ is linear
- $\mathcal{F}$ is affine-inv.
- $\mathcal{F}$ has 3-local characterization

$$x_1 = e_1 \; ; \; x_2 = e_2 \; ; \; x_3 = e_1 + e_2$$

$$S = \{(000), (011), (101), (110)\}$$

Our Results

Some general results in algebraic property testing.

Theorem 1: Let $\mathcal{F} \subseteq \{f : K^n \to \mathbb{F}\}$ be

- affine-invariant + $\mathbb{F}$-linear
- have k-local characterization

then $\mathcal{F}$ has k-query property tester.

Theorem 2: There exist many interesting $\mathcal{J}$ satisfying conditions of Theorem 1; in particular if $\mathcal{J}$ has an ℓ-local constraint $\Rightarrow$ $\mathcal{J}$ has a $R(\ell)$-local characterization (when $\mathbb{K} = \mathbb{F}$)

Rest Of Talk

- BLR Analysis.
- Our Analysis (Sketch).

BLR (recalled)

- $f : G \to H$

$$\Pr_{x,y}\left[f(x) + f(y) \neq f(x+y) \right] = \epsilon < \frac{2}{9}$$

- $\Rightarrow \exists \ \phi : G \to H$, homomorphism

s.t. $\Pr\left[f(x) \neq \phi(x) \right] \leq 2\epsilon$

Construction of ϕ

- Only function that can work is

$$\phi(x) \triangleq \underset{y}{\text{plurality}} \left\{ f(x+y) - f(y) \right\}$$

- Questions:
  - Is ϕ close to f?
  - Is ϕ a homomorphism?

Easy Part: ϕ is close to f

Let $\text{Bad} = \left\{ x \;\middle|\; \Pr_y \left[f(x+y) - f(y) \neq f(x) \right] \geq \frac{1}{2} \right\}$

1. $x \notin \text{BAD} \Rightarrow \phi(x) = f(x)$

2. $\epsilon = \Pr_{x,y} \left[f(x+y) - f(y) \neq f(x) \right]$

$$\geq \Pr_x \left[x \in \text{BAD} \right] \cdot \Pr \left[\searrow \;\middle|\; x \in \text{BAD} \right]$$

$$\geq \Pr_x \left[x \in \text{BAD} \right] \cdot \frac{1}{2}$$

$\boxtimes$

Hard Part: Structure in ϕ

- Can't prove structure if ϕ is not well-defined ("plurality")
- Is ϕ well-defined?

$$\phi(x) \overset{?}{=} f(x+y_1) - f(y_1)$$

$$\overset{?}{=} f(x+y_2) - f(y_2)$$

Hard Part : Structure in ϕ

- Can't prove structure if ϕ is not well-defined ("plurality")
- Is ϕ well-defined? [Lets fill this matrix]

$\phi(x)$ $\overset{?}{=}$ $f(x+y_2)$	$f(x+y_1)$	$-f(y_1)$
$f(x+y_2)$	$f(x+y_1+y_2)$	$-f(y_1)$
$-f(y_2)$	$-f(y_2)$	0

$\phi(x)$ $\overset{?}{=}$	$-f(x+y_1)$	$+f(y_1)$
$\overset{?}{=}$ $-f(x+y_2)$	$f(x+y_1+y_2)$	$-f(y_1)$
$+f(y_2)$	$-f(y_2)$	0

- Last row & column sum to zero
- Middle row & column likely sum to zero
  [over choice of y_1, y_2]
- So top row sums to zero $\Rightarrow$ first column sums to zero

ϕ is a homomorphism

Claim 1: $\forall x \Pr_{y_1, y_2}\left[f(x+y_1) - f(y_1) \neq f(x+y_2) - f(y_2) \right] \leq 2\epsilon$

(just proved)

Claim 2: $\forall x \Pr_{y}\left[\phi(x) \neq f(x+y) - f(y) \right] \leq 2\epsilon$

(immediate from Claim 1)

Claim 3: $\forall x, y \quad \phi(x) + \phi(y) = \phi(x+y)$

(proof: more Matrix magic)

$\phi(x)$	$\phi(y)$	$-\phi(x+y)$
$-f(x+z_1)$	$-f(y+z_2)$	$f(x+y+z_1+z_2)$
$f(z_1)$	$f(z_2)$	$-f(z_1+z_2)$

- Bottom rows likely to sum to zero
- All columns likely to sum to zero

$\Rightarrow$ ☒

Generalizing to linear-invariant families

Given : $f: \mathbb{K}^n \to \mathbb{F}$ s.t.

$$\Pr_A \left[\langle f(Ax_1) \ldots f(Ax_\ell) \rangle \notin C \right] \leq \epsilon$$

Need : 1. Definition of ϕ.

2. Closeness of ϕ to f.

3. Structure of ϕ.

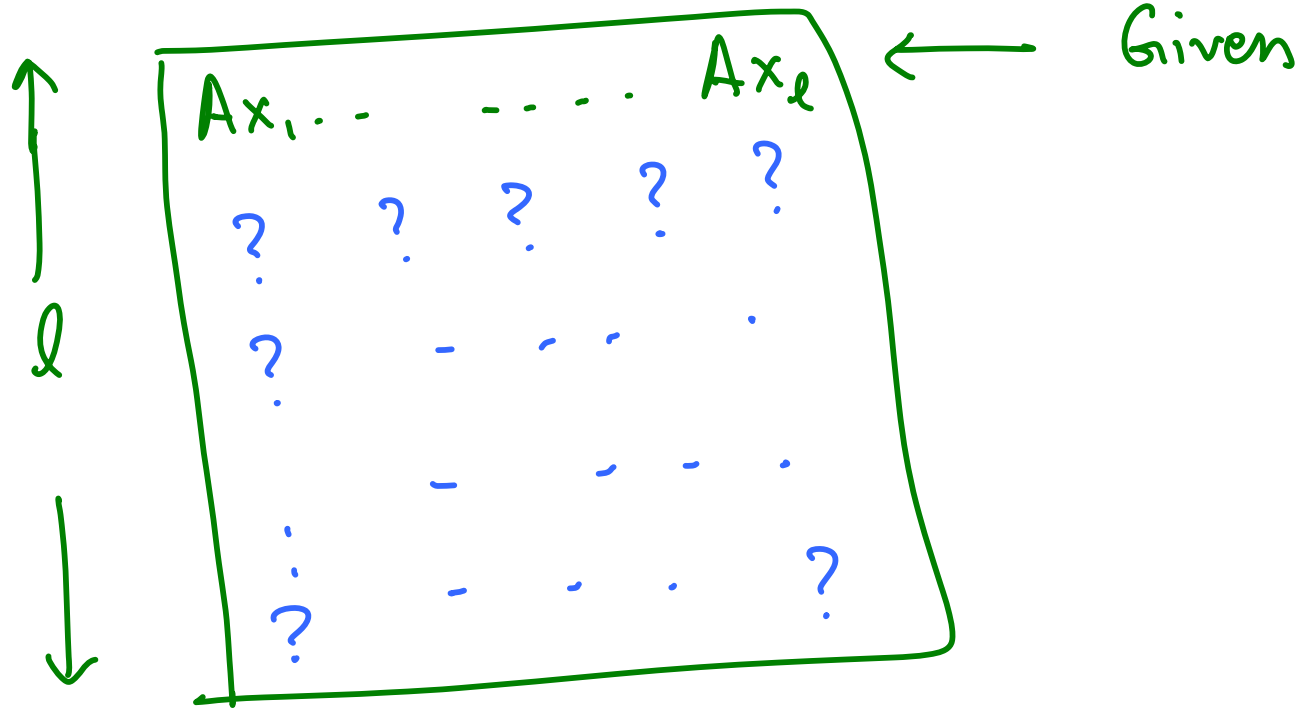
Definition of ϕ

$$\phi(x) = \underset{A \mid Ax_1 = x}{\text{plurality}} \left\{ \underline{\alpha}(A) \;\middle|\; \langle \underline{\alpha}, f(Ax_2) \ldots f(Ax_\ell) \rangle \in C \right\}$$

Closeness of ϕ to f

Same as before.

Matrix Magic ?



← Given

Want : • rows/columns to be of the form $A'x_1 \ldots A'x_\ell$

• rows/columns as random as possible.

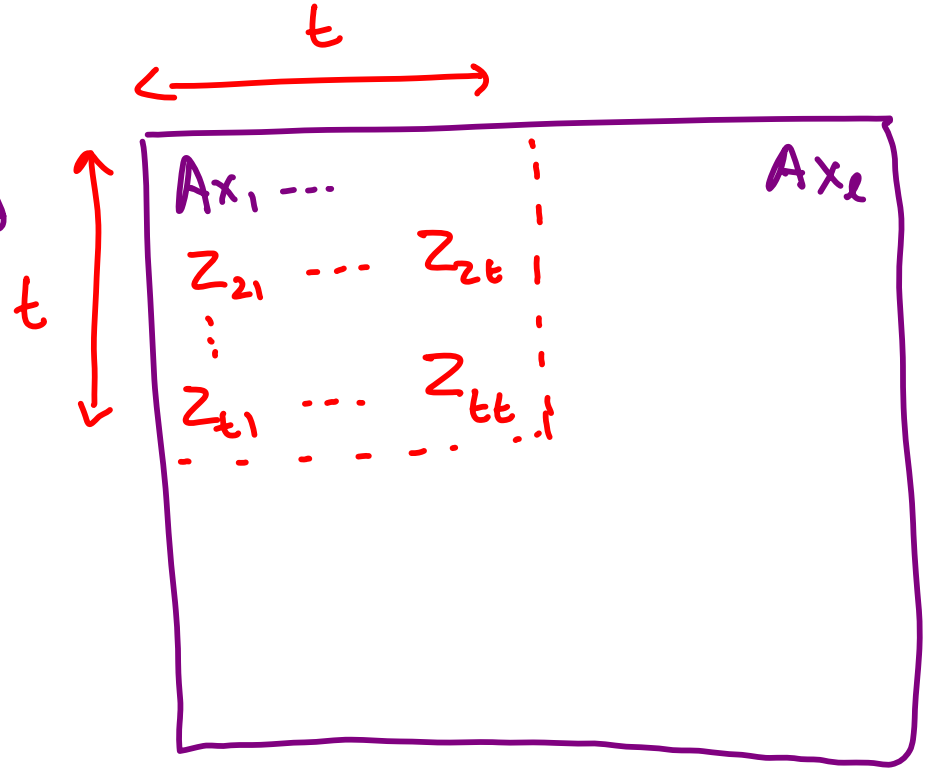
How to do this ?

Solution $\{Ax_1 \dots Ax_\ell \mid A\}$

$= \left\{ \left(y_1 \dots y_t, \sum \lambda_j^{(t+1)} y_j, \dots \sum \lambda_j^{(\ell)} y_j\right) \;\middle|\; y_1 \dots y_\ell \in K^n \right\}$

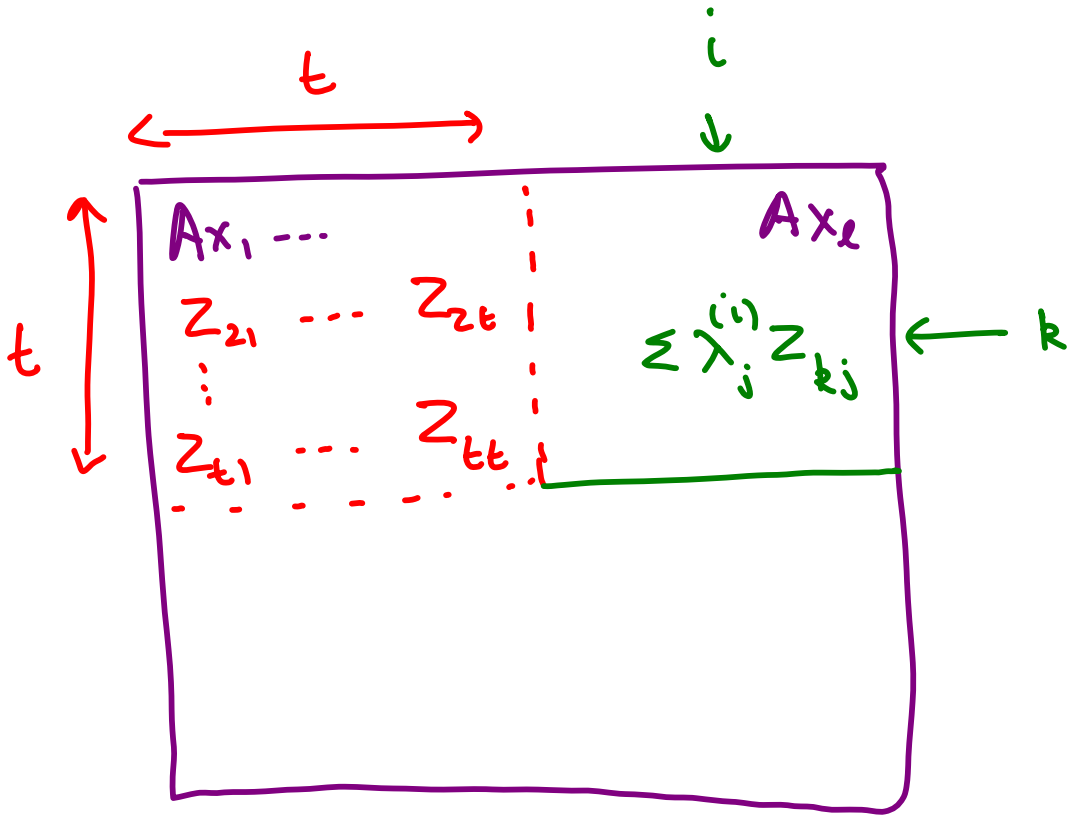
for some $\lambda_j^{(i)} \in K$

Matrix filling



1. Pick z_{ij} at random

2. Now Extend to right using $\lambda_j^{(i)}$'s



3. Now extend to bottom rows similarly.

4. Claim: Bottom rows still of form $(A'x_1 \ldots A'x_\ell)$
(simple linear algebra) ⊠

Conclusions

- Simple proof combining
  [Blum Luby Rubinfeld]
  [Rubinfeld S.]
  [Alon Krivelevich Kaufman Litsyn Ron]
  [Kaufman Ron] / [?]
- Main Question: How local are the local constraints?
- Alon's Conjecture: if 2-transitive class of functions has local constraint ⇒ testable.