AXIOMATIC STRENGTH OF HITTING SETS FOR MULTIVARIATE POLYNOMIALS WITHIN BOUNDED ARITHMETIC

Albert Atserias
UPC Barcelona & CRM

based on joint work with

Iddo Tzameret
Imperial College London

POLYNOMIAL IDENTITIES

$$\boxed{\prod_{1\le i<j\le n}(x_j-x_i) - \sum_{1\le k\le n}(-1)^k \cdot \prod_{\substack{1\le i<j\le n\\ i\ne k,\, j\ne k}}(x_j-x_i)\, x_k^n \stackrel{?}{=} 0}$$

PIT : Given an n-variate $+, \times$ expression with constants in a field $\mathbb{F}$, does it compute the 0 polynomial?

Polynomial Identity Testing.

POLYNOMIAL IDENTITIES

"$E(x_1, \dots, x_n)$ computes the 0 polynomial":

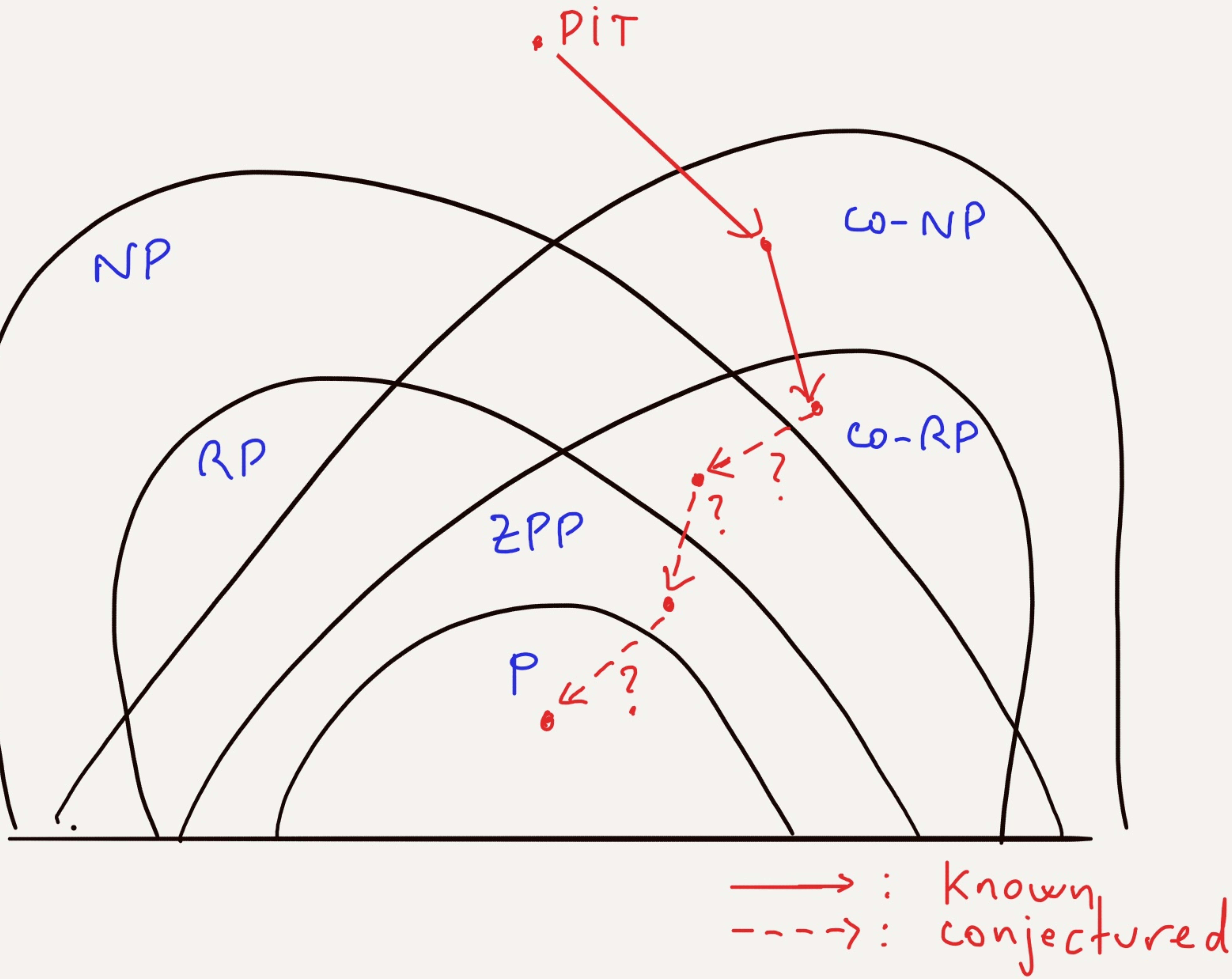
- interpretation 1: expanding out and grouping equal monomials, all coefficients become 0.

- interpretation 2: evaluating it at any $(b_1, \dots, b_n) \in \mathbb{F}^n$ we get value 0. ← when $\mathbb{F}$ is large

$1 \Leftrightarrow 2$

(not entirely trivial)

COMPLEXITY OF PIT (over Q, say)



FUNDAMENTAL THEOREM OF ALGEBRA (FTA)

Every non-zero degree-d univariate polynomial over $\mathbb{C}$ has exactly d roots in $\mathbb{C}$.

$\text{FTA}_{\geq}$: $\geq d$ roots : by algebraic closure of $\mathbb{C}$.

$\text{FTA}_{\leq}$: $\leq d$ roots : Euclidean division for polys.

available in <u>every</u> field

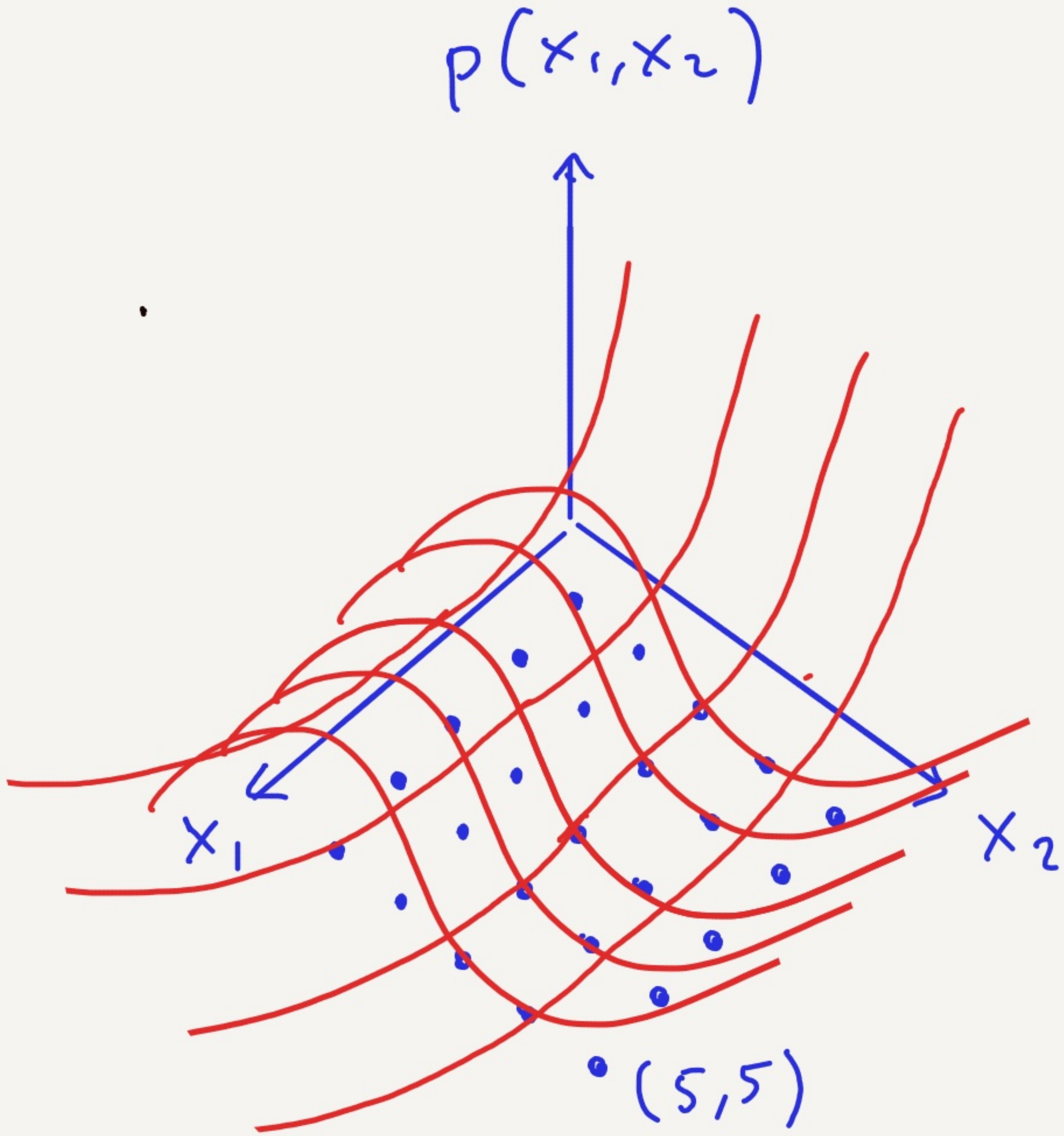
THE SCHWARTZ-ZIPPEL LEMMA

For every field $\mathbb{F}$,
every finite subset $S \subseteq \mathbb{F}$,
every number of variables n
every polynomial $p(\bar{x}) \in \mathbb{F}[x_1, \dots, x_n]$
if $p(\bar{x})$ is not the 0 polynomial
then

$$\Pr_{a_1, \dots, a_n \in_R S}\left[p(a_1, \dots, a_n) = 0 \right] \leq \frac{\deg(p) \cdot n}{|S|}$$

$\deg(p)$: maximum individual degree

EXAMPLE



$\mathbb{F} = \mathbb{R}$

$S = \{1,2,3,4,5\}$

$n = 2$

$d = 3$

$$p(x_1,x_2) = (x_1^2+2)(x_2^2-9)(x_2-4)$$

$$= x_1^2x_2^3 - 4x_1^2x_2^2 - 9x_1^2x_2 + 2x_2^3 + 36x_1^2 - 8x_2^2 - 18x_2 + 72$$

STRATEGY FOR A NEW PROOF [AT'25]

Given $p(\bar{x})$ and $\bar{b} \in \mathbb{F}^n$ we define

$$f_{p,\bar{b}} : S^{n-1} \times [d] \times [n] \longrightarrow S^n$$

which is:

(1) onto $ROOTS_p^S \subseteq S^n$ if $p(\bar{b}) \neq 0$.

(2) explicit and poly-time given any such $\bar{b}$

(3) invertible in poly-time given any such $\bar{b}$

$$\longrightarrow |ROOTS_p^S| := |\{\bar{a} \in S^n : p(\bar{a}) = 0\}| \leq |S|^{n-1} \cdot d \cdot n$$

FEASIBLE PROOF

Q: What is the weakest subtheory of PA

(1) that proves $PIT \in P/poly$ or $PIT \in co\text{-}RP$

(2) that proves Schwartz-Zippel ?

$$PV_1 \subseteq S^1_2 \subseteq T^1_2 \subseteq S^2_2 \subseteq T^2_2 \subseteq S^3_2 \subseteq \dots \subseteq BA$$

$PV_1 + dWPHP(PV)$

$S^1_2 + dWPHP(PV)$

induction for P-predicates

induction for PH-predicates

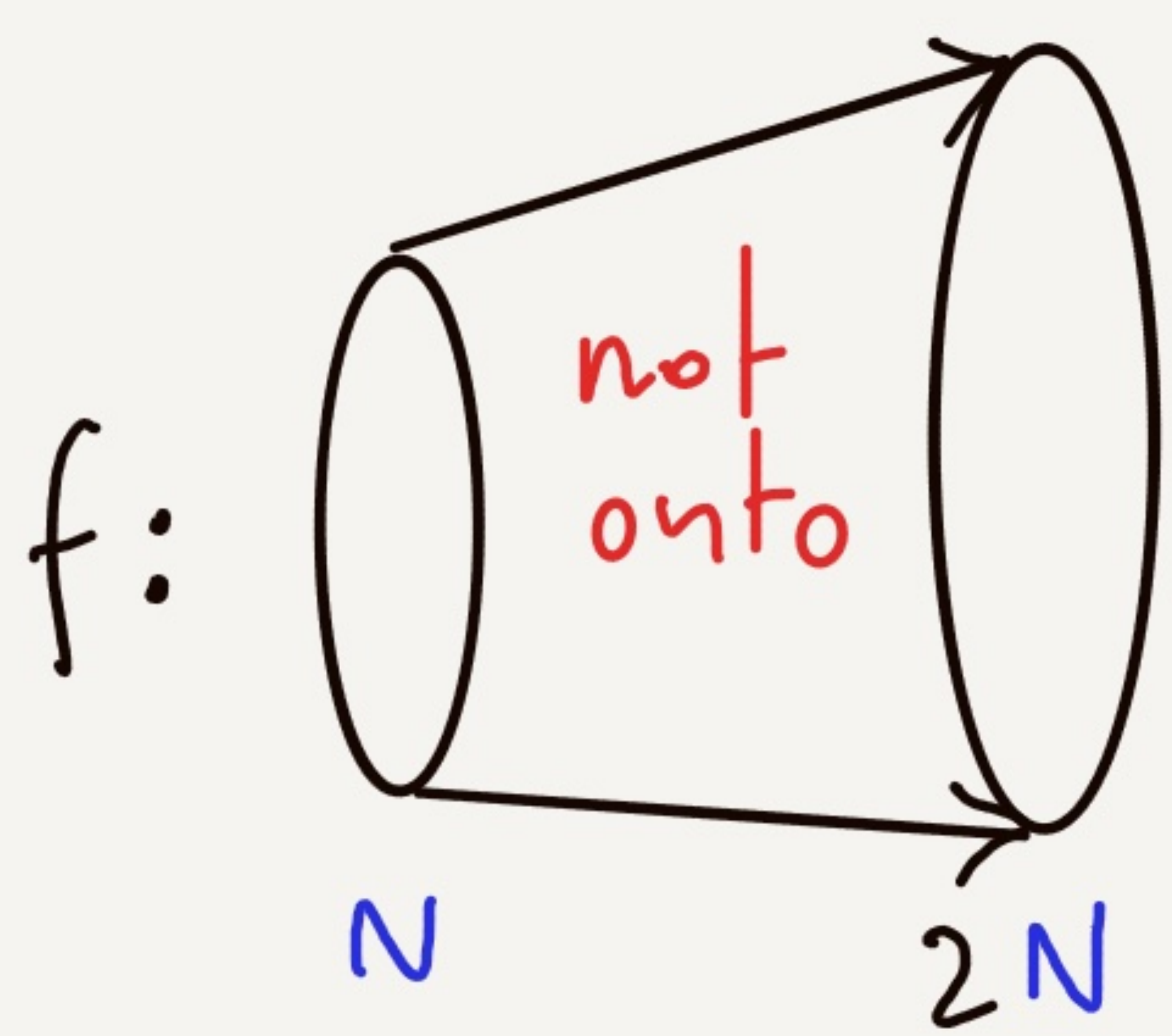
$S^1_2 + dWPHP(PV)$ [Wilkie] [Krajicek'01] [Jerabek'05]

- basic axioms for $+, \times, \leq, \#, |\cdot|$
- axioms for PV (poly-time) algorithms
- Length-induction for all NP-predicates

Σ^b_1-LIND

and

- Dual Weak Pigeonhole Principle for PV-function



$dWPHP^{2N}_N(f) :=$
$\exists y < 2N \ \forall x < N \ f(x) \neq y$

STATING & PROVING THE SZ-LEMMA

$$S^1_2 \vdash \forall n, d, q \in Log$$
$$\forall F \in AlgCkt(n, d)$$
$$\forall \bar{b} \in \mathbb{Z}^n \quad \forall \bar{c} \in [q]^n$$

$$F(\bar{b}) \neq 0 \wedge F(\bar{c}) = 0 \longrightarrow$$
$$\exists \bar{a} \in [q]^{n-1} \, \exists u \in [d] \times [n] \;\; f_{F, \bar{b}}(\bar{a}, u) = \bar{c}$$

Read: if a non-root exists then many non-roots exist (or $d \geq q/n$)

$\boxed{\text{many}: \; q^n \left(1 - \frac{dn}{q}\right)}$

APPLICATION 1 : PIT $\in$ co-NP

$S^1_2 + \mathrm{dWPHP(PV)} \vdash$

$\forall n, d, q \in \mathrm{Log} \quad q > 2dn \longrightarrow$

$\forall P \in \mathrm{AlgCkt}(n,d)$

$(\exists \bar{a} \in \mathbb{Z}^n \;\; P(\bar{a}) \neq 0) \longrightarrow (\exists \bar{b}^* \in [q]^n \;\; P(\bar{b}^*) \neq 0)$

$\mathrm{dWPHP}^{2N}_{N}(f_{P,\bar{a}}) \equiv \exists \bar{b} \in [q]^n \;\; (\bar{b} \notin \mathrm{ROOTS}_P^{[q]^n})$

for $\quad N := q^{n-1} \cdot d \cdot n$

APPLICATION 2 : PIT $\in$ P/poly

$S^1_2 + dWPHP(PV) \vdash$

$$\forall n, d, q, s \in Log \quad q > 2dn \longrightarrow$$
$$\exists C \in BoolCkt(s, poly(n, q, s))$$
$$\forall P \in AlgCkt(n, d, s)$$
$$C(P) = 1 \rightarrow \forall \bar{b} \in \mathbb{Z}^n \quad P(\bar{b}) = 0$$
$$\wedge\, C(P) = 0 \rightarrow \exists \bar{b} \in [q]^n \; P(\bar{b}) \neq 0$$

$$C(P) := \bigwedge_{i=1}^{r} [P(h_i) = 0]$$

with $h_1, \dots, h_r$ given

by $dWPHP^{2N}_{N}\left(\left(f_{-,-}\right)^{\otimes r}\right)$

with $r \geq s+1$
we argue by
independence
and
union bound

$$2^s \cdot 2^{-r} < 1$$

COLLECTIONS OF CKTS

Let $\mathcal{C}(n,d,s,m) \subseteq \mathrm{AlgCkt}(n,d,s)$ be a collection of algebraic circuits of description size m.

Ex: $\mathcal{C} = \{ \det(X_G) : \quad G = (L \,\dot\cup\, R,\ E \subseteq L \times R) \}$

$$\det(X_G) = \sum_{m \in M_G} (-1)^{\mathrm{ord}(m)} \prod_{u \in L} x_{u, m(u)}$$

symbolic adjacency matrix $(x_e : e \in E)$

perfect matchings

description size: $O(|E| \cdot \log(|L| + |R|))$

HITTING SET PRINCIPLE

Fact: For such $e(n,d,s,m)$, there exist hitting sets of size $m + n \cdot \log(q)$.

Def: $HS(PV) := \{ HS(f) : f \in PV \}$

$HS(f) :=$

$$\forall e \ \forall n, d, s, q, r, m \in Log$$
$$q > 2nd \wedge r > m + n \cdot |q| \longrightarrow \exists H = (\bar{h}_1, \dots, \bar{h}_r) \in ([q]^n)^r$$
$$\forall x \in \{0,1\}^m \ \forall P = f_e(x) \in AlgCkt(n,d,s)$$
$$(\exists \bar{a} \in \mathbb{Z}^n \ P(\bar{a}) \neq 0) \longrightarrow (\exists i < r \ \ P(\bar{h}_{i+1}) \neq 0).$$

HS(PV) $\longleftrightarrow$ dWPHP(PV)

$S^1_2 \vdash$ dWPHP(PV) $\longleftrightarrow$ HS(PV)

Pf:

$\rightarrow$: two applications of dWPHP(f_{SZ})

- one for small witnesses
- one for hitting set itself.

built from f, k

$\leftarrow$: assume $\neg$ dWPHP$^{2k}_{k}(f) \wedge$ HS(PV)

- by amplification, $\neg$ dWPHP$^{2^{m^3}}_{2^m}(h)$
- define $\mathcal{C}(n, d, s, m)$ with $s = m^3$ to cover $\mathrm{Img}(h)$ in their roots.
- contradiction follows from HS($\mathcal{C}$) and diagonalization.

THE CHOICE OF $\mathcal{C}(n,d,s,m)$

$$\mathcal{C}(n,d,s,m) := \{ A_x(z_1,\dots,z_n) : x \in \{0,1\}^m \}$$

where

$$\boxed{A_x(z_1,\dots,z_n) := \prod_{i\in[r]} \sum_{j\in[n]} \Big(z_j - \sum_{k\in[|q|]} h(x)_{i,j,k} \cdot 2^{k-1} \Big)^2}$$

$|||$ ⟵ both $=0$ or both $\neq 0$

"$z_1 \cdots z_n \notin H(x)$"

$$x \in \{0,1\}^m \xrightarrow{h} y \in \{0,1\}^{m^3}$$

$$y = h(x) = \mathrm{enc}(H(x))$$

$$\hookrightarrow (h_1(x),\dots,h_r(x)) \in ([q]^n)^r$$

WRAP UP SLIDE

- We gave a new proof of SZ-Lemma
- This gives $PIT \in P/poly$ & co-NP in the theory $S^1_2 + dwPHP(PV)$
- Indeed $S^1_2 \vdash dwPHP(PV) \longleftrightarrow HS(PV)$

Intriguing: Hitting sets for depth-3 families suffice !!

$\Pi\Sigma\Pi_{\leq \text{polylog}}$