Algebraic vs functional independence

(with A. Pandey & A. Sinhababu)

- <u>Defn:</u> • Polynomials $f_1, \ldots, f_m \in \mathbb{F}[\overline{x}_n]$ are <u>alg. dep.</u> if $\exists$ an <u>annihilating polynomial</u> $0 \neq A \in \mathbb{F}[\overline{y}_m]$ s.t. $A(\overline{f}_m) = 0$.

  • transcendence degree, <u>trdeg</u> of $\overline{f}_m$ is the max. number of alg. indep. polynomials in $\{f_1, \ldots, f_m\}$.

  ▷ $\mathrm{trdeg}(\overline{f}_m) \in [0, \ldots, n]$.

- For <u>linear</u> $f_1, \ldots, f_m$ these concepts specialize to linear dependence & linear rank.

- Eg. $\{x_1 + x_2, x_1^2 + x_2^2\}$ are alg. indep. over $\mathbb{F}$, unless $\mathrm{ch}\,\mathbb{F} = 2$.

  Over $\mathbb{F}_2$, the ann. poly. is $y_1^2 - y_2$.

<u>Motivation:</u> 1) It appears in commutative algebra &

geometry as <u>dimension</u>, eg. $\dim \mathbb{F}[\bar{x}_n] = n$.

- Appears in field theory as <u>trdeg</u> of extensions: $\mathrm{trdeg}[\mathbb{F}(\bar{x}_n) : \mathbb{F}(\bar{f}_m)]$
$$= n - \mathrm{trdeg}(\bar{f}_m).$$
- Gives interesting <u>matroid</u> examples.

2) • [Dvir, Gabizon, Wigderson '07] <u>extractors</u> for sources which are polynomial maps over $\mathbb{F}_q$.

- [Dvir, Gutfreund, Rothblum, Vadhan '11] use <u>entropy</u> of low-degree polynomials in a cryptographic application.
- [BMS'11, ASSS'12, Kumar Saraf '16] use trdeg for circuit lower bounds & hitting-set designs (PIT), for numerous models.

– In this talk, we'll only discuss the basic

<u>Qn 1</u>: Given circuits $\bar{f}_m$, test their alg. indep. in poly(s)-time ?

- Is Qn.1 even computable?

Criterion 0: [Perron '27] $\bar{f}_m$ alg. dep. $\Rightarrow \exists A(\bar{y}_m)$ of weighted-degree $\le \prod_i \deg(f_i)$.

- This optimal degree bound is shown by setting-up a linear system & using dimension arguments.

Corollary: For any $\mathbb{F}$, given size-s circuits $\bar{f}_m$, the ann-poly. has degree $s^{O(sm)}$. Alg. indep. testing $\in$ Pspace.

Criterion 1: [Jacobi 1841] For $\mathrm{ch}\,\mathbb{F}=0$,

$$\mathrm{trdeg}\,\bar{f}_m = \mathrm{rk}_{\mathbb{F}(\bar{x})} \left(\partial_j f_i\right)_{(i,j)\in[m]\times[n]}$$

Jacobian matrix

where $\partial_j f_i := \partial f_i / \partial x_j \in \mathbb{F}[\bar{x}_n]$.

Pf: Consider the derivatives of $A(\bar{f}_m)$. $\square$

Corollary: For $\mathrm{ch}\,\mathbb{F}=0$, alg. indep. testing $\in$ RP.

- Jacobian failure: • $\partial x^p = 0$ if $ch\, \mathbb{F} = p > 0$.
  • Jacobian of $\{x^2y, xy^2\}$ over $\mathbb{F}_3$ is $rk = 1$.
  • Galois theory explains: $\mathbb{F}_3(x,y) \supset \mathbb{F}_3(f_1, f_2)$ is an inseparable extn. above.

Defn.: • $\mathbb{F}(\bar{x}_n)/\mathbb{F}(\bar{f}_m)$ is an insep. extn. if $\exists \alpha \in \mathbb{F}(\bar{x}_n)$ s.t. the min. ann. poly. $A(y_0, \bar{y}_m)$ of $\{\alpha, \bar{f}_m\}$ is insep. wrt y_0, i.e. $\partial_{y_0} A = 0$.
(equivalently, A is a poly. in y_0^p)

• It's insep. deg. is the least p^i s.t. $\forall \alpha \in \mathbb{F}(\bar{x}_n)$, that are algebraic over $\mathbb{F}(\bar{f}_m)$, α^{p^i} is sep. over $\mathbb{F}(\bar{f}_m)$.

- Eg. • insep. deg. of $\mathbb{F}_p(\bar{x}) / \mathbb{F}_p(x_1, x_1^2 + x_2^{p^2})$ is p^2.
  • " " " $\mathbb{F}_p(x_1, x_2^{p^2}) / \mathbb{F}_p(x_1, x_1^2 + x_2^{p^2})$ is 1.

Criterion 1' [Jacobian]: $\forall \mathbb{F}$, $\mathbb{F}(\bar{x}_n)/\mathbb{F}(\bar{f}_m)$ sep.
$\Rightarrow$ $\operatorname{trdeg} \bar{f}_m = rk_{\mathbb{F}(\bar{x}_n)} (\partial_j f_i)_{[m]\times[n]}$.

<u>Criterion 2</u>: [MSS'14] alg. indep. over $\mathbb{F}_q \in NP^{\#P}$.

<u>Pf</u>: The polys. are p-adically lifted beyond the insep. deg. p^i & we get a Jacobian-like invariant. $\square$

- Let $p^e :=$ insep. deg. $\mathbb{F}(\bar{x}_n)/\mathbb{F}(\bar{f}_m)$.
  Could we do indep. testing in poly(p^e)-time?

<u>Approx. Functional Dependence</u>

- (Kumar, Saraf CCC'16)'s work motivates the following definition.

<u>Defn</u>:
- Consider the formal power series ring $\mathbb{F}[[\bar{x}_n]]$, where the <u>precision</u> is by total degree. (Equiv., the filtration is by
  $$\cdots \to \mathbb{F}[\bar{x}_n]/\langle \bar{x}_n \rangle^3 \to \mathbb{F}[\bar{x}]/\langle \bar{x} \rangle^2 \to \mathbb{F}[\bar{x}]/\langle \bar{x} \rangle.)$$
- $f_0 \in \mathbb{F}[\bar{x}_n]$ <u>fn. deps.</u> on $\bar{f}_r$ if there is an $F \in \mathbb{F}[[\bar{y}_r]]$ s.t. $f_0 = F(\bar{f}_r)$ in $\mathbb{F}[[\bar{x}_n]]$.
  (Wlog assume $f_i(\bar{0}) = 0$, $i \in [0, .., r]$.)

Criterion 3: [PSS'16] $\bar{f}_m$ are alg. dep. iff $\exists i_0$, $f_{i_0}(\bar{x}+\bar{z}) - f_{i_0}(\bar{z})$ fn. deps. on $\{ f_j(\bar{x}+\bar{z}) - f_j(\bar{z}) \mid j \in [m] \setminus \{i_0\} \}$ for a random $\bar{z} \in \overline{\mathbb{F}}^n$.

Moreover, it suffices to consider fn. dep. up to $\deg = p^e$ precision. (i.e. mod $\langle \bar{x} \rangle^{p^e+1}$)

Corollary: Alg. indep. testing can be done in time polynomial in $s \cdot \binom{n+p^e}{n}$.

Proof: ($\Rightarrow$): Let $A(\bar{f}_m) = 0$. Since $A(\bar{y}_m)$ is

$p := \mathrm{ch}\,\mathbb{F} \rightarrow$ not a p-power, $\exists i_0$, say $=1$, s.t. $\partial_{y_1} A \neq 0$.

- Consider $A(f_1(\bar{x}+\bar{z}), \dots, f_m(\bar{x}+\bar{z})) = 0$

$\equiv_{\langle \bar{x} \rangle^2} A(H_1 f_1 + H_0 f_1, \dots, H_1 f_m + H_0 f_m)$,

where $H_0 f_i := f_i(\bar{z})$, $H_1 f_i := f_i(\bar{x}+\bar{z})^{\leq 1} - f_i(\bar{z})$.

truncate at deg = 1

- $\mathcal{H} f_i := f_i(\bar{x}+\bar{z}) - f_i(\bar{z})$.
- The idea now is to express $H_1 f_1$ as a fn. of $\{H_1 f_2, \dots, H_1 f_m\}$ mod $\langle \bar{x} \rangle^2$, & then repeat using Newton's iteration!

- Write $0 \underset{\langle \bar{x} \rangle^2}{\equiv} A(H_1 f_1 + H_0 f_1, \ldots) = \sum_{i=0}^{d} a_i \cdot (H_1 f_1 + H_0 f_1)^i$,

where $a_i = a_i(\mathcal{H} f_2, \mathcal{H} f_3, \ldots)$ is a polynomial.

$\because H_1 f_1 \in \langle \bar{x} \rangle$

$\Rightarrow$

$$0 \equiv_{\langle \bar{x} \rangle^2} \sum_{i=0}^{d} a_i \cdot (H_0 f_1)^i + \sum_{i=0}^{d} i a_i \cdot (H_0 f_1)^{i-1} \cdot (H_1 f_1)$$

$$\Rightarrow H_1 f_1 \equiv \frac{-\sum_i a_i (H_0 f_1)^i}{\sum_i i a_i (H_0 f_1)^{i-1}} \bmod \langle \bar{x} \rangle^2 .$$

- Note: Not all $i a_i$ are $0 \in \mathbb{F}$, & $H_0 f_j$ is 'random' as we think of $\bar{z}$ as a random point.

$\Rightarrow$ the denominator above is actually a unit in $\mathbb{F}[\bar{x}] / \langle \bar{x} \rangle^2$.

$\Rightarrow$ We've expressed $\mathcal{H} f_1$ as a polynomial in $\{\mathcal{H} f_2, \ldots, \mathcal{H} f_m\}$ mod $\langle \bar{x} \rangle^2$.

- Next, consider $H_2 f_1 := f_1(\bar{x}+\bar{z})^{\leq 3} - f_1(\bar{x}+\bar{z})^{\leq 1}$ $H_{\leq 1} f_i :=$
- Repeat the above with

$0 \equiv A(H_2 f_1 + H_{\leq 1} f_1, \mathcal{H} f_2, \ldots, \mathcal{H} f_m) \bmod \langle \bar{x} \rangle^4$.

• Note that $H_2 f_1 \in \langle\bar{x}\rangle^2$ & we get a higher precision value as:

$$H_2 f_1 \equiv -\frac{\sum_i a_i (H_{\leq 1} f_1)^i}{\sum_i i a_i (H_{\leq 1} f_1)^{i-1}} \mod \langle\bar{x}\rangle^4 .$$

$\Rightarrow$ We've expressed $\mathcal{H}f_1$ as a polynomial in $\{\mathcal{H}f_2, \dots, \mathcal{H}f_m\} \mod \langle\bar{x}\rangle^4$.

This can be repeated ad infinitum.

($\Leftarrow$): • Suppose $\bar{f}_m$ are alg. indep.

• Wlog assume $m=n$.

$\Rightarrow \forall i \in [n]$, x_i alg. deps. on $\bar{f}_n$.

• In fact, $\forall i$, $x_i^{p^e}$ " " " separably.

$\Longrightarrow \mathcal{H}x_i^{p^e} = x_i^{p^e}$ fn. deps. on $\{\mathcal{H}f_1, \dots, \mathcal{H}f_n\}$.

• Suppose $\mathcal{H}f_{i_0}$ fn. deps. on the other $\mathcal{H}f_j$'s.

$\Rightarrow \forall i \in [n]$, $x_i^{p^e}$ fn. deps. on $\{\mathcal{H}f_1, \dots\} \setminus \{\mathcal{H}f_{i_0}\}$.

This leads to a contradiction by trdeg/deg-lex. □

Applns: 1) VNP has $\Sigma\Pi^{(k)}\Sigma\Pi$ complexity $= n^{\Omega(\sqrt{d})}$.

2) Quasipoly-hsg for $\Sigma\Pi^{(k)}\Sigma\Pi^{\delta}$, if $k\delta$ = polylog & $p >$ ind-deg.