Primes via Zeroes :

interactive proofs for testing primality of natural classes of ideals

Abhibhav Garg
UWaterloo

Rafael Oliveira
Uwaterloo

Nitin Saxena
IIT Kanpur

Polynomial Systems

given: $f_1, f_2, \dots, f_m \in \mathbb{Z}[x_1, x_2, \dots, x_n]$,

$$Z(f_1, \dots, f_m) := \{\alpha \in \mathbb{C}^n \mid f_1(\alpha) = \dots = f_m(\alpha) = 0\}$$

Polynomial Systems

$$Z(f_1, \dots, f_m) := \{\alpha \in \mathbb{C}^n \mid f_1(\alpha) = \dots = f_m(\alpha) = 0\}$$

Is $Z(f_1, \dots, f_m)$ empty ? Polynomial system satisfiability.

NP-hard (arithmetisation of 3-SAT).

PSPACE

AM (assuming GRH) [Koiran 97]

Irreducibility of zero sets.

Every variety Z is a finite union of irreducible varieties $Z = \bigcup_{i=1}^{r} Z_i$

↳ not a union of two proper varieties.

Irreducibility of zero sets.

Every variety Z is a finite union of irreducible varieties $Z = \bigcup_{i=1}^{r} Z_i$

→ not a union of two proper varieties.

Algebraic Geometry starts with this decomposition, and is the study of irreducible varieties.

Irreducibility of zero sets.

Every variety Z is a finite union of irreducible varieties $Z = \bigcup_{i=1}^{r} Z_i$

→ not a union of two proper varieties.

Algebraic Geometry starts with this decomposition, and is the study of irreducible varieties.

Computationally, decomposing varieties seems to be hard, but how hard exactly?

Background: Ideals, radicals and primality

Ideal: ideal generated by $f_1, \ldots, f_m$ is

$$I(f_1, \ldots, f_m) := \{h \mid h = \sum f_i g_i\}$$

Background: Ideals, radicals and primality

Ideal: ideal generated by $f_1, \ldots, f_m$ is

$$I(f_1, \ldots, f_m) := \{h \mid h = \sum f_i g_i\}$$

$$Z(f_1, \ldots, f_m) = Z\left(I(f_1, \ldots, f_m)\right)$$

Two ideals can have the same zeroset:

for eg $Z(I(x^2(y-1))) = Z(I(x(y-1)))$

Background: Ideals, radicals and primality

Radical of an ideal:

$$\operatorname{rad}(I) = \{ h \mid h^a \in I,\ a \in \mathbb{N} \}.$$

$$Z(I) = Z(\operatorname{rad}(I)).$$

Nullstellensatz (Hilbert 1893) (Strong):

$$Z(f_1, \dots, f_m) = Z(h_1, \dots, h_s)$$

$$\Updownarrow$$

$$\operatorname{rad}(f_1, \dots, f_m) = \operatorname{rad}(h_1, \dots, h_s)$$

Background: Ideals, radicals and primality

Prime ideal: I is prime if

$h_1 \cdot h_2 \in I \Rightarrow h_1 \in I$ or $h_2 \in I$

Background: Ideals, radicals and primality

Prime ideal: I is prime if
$h_1 \cdot h_2 \in I \Rightarrow h_1 \in I$ or $h_2 \in I$

For radical ideals, I prime iff
$Z(f_1, \ldots, f_m)$ irreducible.

Main Theorems

Theorem (Gos):

Testing primality of radical ideals is in $\Sigma_3^P \cap \Pi_3^P$ assuming GRH

Testing primality of equidimensional CM ideals is in $\Sigma_3^P \cap \Pi_3^P$ assuming GRH

(captures complete intersection, dim 0)

Example:

$$XZ - Y^2$$
$$Y - Z^2$$
$$X - YZ$$

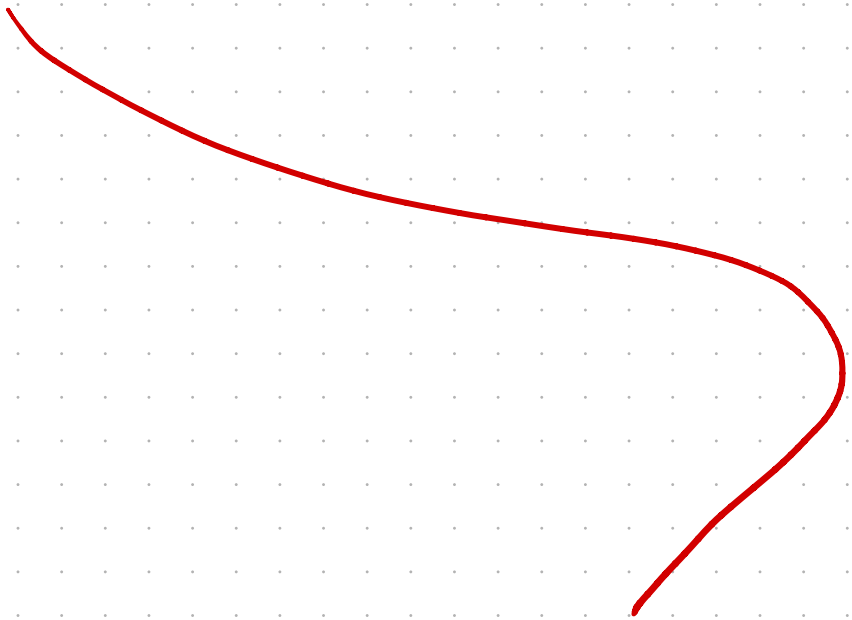
$$XZ - Y^2$$
$$Y - Z^2$$
$$X + YZ + 1$$

Example:

$XZ - Y^2$

$Y - Z^2$

$X - YZ$



$XZ - Y^2$

$Y - Z^2$

$X + YZ + 1$

$(-1,0,0)$

Complete intersection ≈

Cohen-Macaulay (CM) ideal ≈ $I = \langle f_1, \dots, f_m \rangle$

with f_i adding a constraint independent of the prior f_j's (in the sense of nonzero divisor ↗).

↳ $|$ regSequence of nonzerodiv. in $|\mathbb{F}[\vec{x}_n]/I| =: \operatorname{depth}(I)$,

$\leqslant \dim(\mathbb{F}[\vec{x}_n]/I) =: \operatorname{ht}(I) = \operatorname{codim}(I)$.

↳ CM: $\operatorname{depth}(I) = \operatorname{ht}(I)$.

e.g. minors of $\begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & 1 \end{pmatrix}$ are $f_1 = (x_1 y_2 - x_2 y_1)$, $f_2 = (x_1 - x_3 y_1)$,

$f_3 = (x_2 - x_3 y_2)$.

$I := \langle f_1, f_2, f_3 \rangle$ has — $\operatorname{ht}(I) = 3$

\ $\operatorname{depth}(I) = 3$ ⇒ CM [not complete intersection!]

\# generators $= 3 \neq n - \operatorname{ht}(I) = 2$.

non-CM ideal $\approx$ $\exists$ low-dim. "bad" prime P variety embedded in its ideal decomposition.

$\approx$ pts $P \in V(P)$ have a larger tangent space T_P.

$\approx$ singular pt. behavior in "our" algo.

e.g. $I = \langle x^2, xy \rangle = \langle x \rangle \cap \langle x, y \rangle$

pts. dim = 1 ; pts. dim = 1 ; pts. dim = 0 & embedded in $\langle x \rangle$

I has — $\text{depth}(I) = 0$ [$\langle x, y \rangle$ mod I has only zerodiv.]

$\text{ht}(I) = \dim \mathbb{F}[x,y]/I = 1$.

#generators $= 2$.

$\Rightarrow$ I is non-CM.

↳ To avoid the embedded prime / singularity issues, we work with special ideals in the algorithm.

↳ This ensures w.h.p.: $P \in Z(I) \Rightarrow$

$$\dim T_P = rk(\ker Jac_P(\bar{f})).$$

↳ which is related to $rk(Jac(\bar{f}) \bmod I)$

$$= rk \begin{pmatrix} \partial_{x_1} f_1, \dots, \partial_{x_n} f_1 \\ \vdots \\ \partial_{x_1} f_m, \dots, \partial_{x_n} f_m \end{pmatrix} \bmod I .$$

Lower Bound:

3CNF Φ $\xrightarrow{\text{arithmetization}}$ $\{f_1, \ldots, f_m\}$

Φ satisfiable $\Rightarrow$ $Z(f_1 \ldots, f_m) = \{\cdot \cdot \cdot\}$

Φ unsatisfiable $\Rightarrow$ $Z(f_1 \ldots, f_m) = \{\ \}$

Lower Bound: coNP hardness

3CNF Φ $\xrightarrow[+\text{ point}]{\text{arithmetization}}$ $\{g_1, \ldots, g_{m'}\}$

Φ satisfiable $\Rightarrow$ $Z(g_1, \ldots, g_{m'}) = \{\bullet, \bullet, \bullet\}$

Φ unsatisfiable $\Rightarrow$ $Z(g_1, \ldots, g_{m'}) = \{\bullet\}$

$I(g_1, \ldots, g_m)$ is radical, CM, dim 0

Previous Work:

General case hard: Best algorithms require Gröbner basis, EXPSPACE [Las05][Her26][GTZ88][EHV92]

Radical ideals: EXP [Gri86][Chi86]
PSPACE [BS07]

Complete intersection: EXP [DFGS91]

Constant codimension: RNC [BS10] if I is also radical.

Main tool: mod p reductions

Idea: roots of $f_1, \dots, f_m$ in $\mathbb{C}^n$ and $f_1 \bmod p, \dots, f_m \bmod p$ in $\mathbb{F}_p^n$ are related.

Main tool: mod p reductions

Suppose $f_1, \dots, f_m \in \mathbb{Z}[x_1, \dots, x_n]$.

Let $Z := Z(f_1, \dots, f_m) \subseteq \mathbb{C}^n$

Let $Z_p :=$ common zeroes of $\subseteq \mathbb{F}_p^n$
$f_1 \bmod p, \dots, f_m \bmod p$

Let $\overline{Z_p} :=$ common zeroes of $\subseteq \overline{\mathbb{F}_p}^n$.
$f_1 \bmod p, \dots, f_m \bmod p$

Koirans Proof of HN ∈ AM

If $Z(f_1, \ldots, f_m) = \emptyset$ then $Z_p = \emptyset$

for all except finitely many primes.

(Nullstellensatz)

If $Z(f_1, \ldots, f_m) \neq \emptyset$ then $Z_p \neq \emptyset$

for infinitely many primes.

(Nullstellensatz + number theory)

Koirans Proof of HNEAM

If $Z(f_1, \ldots, f_m) = \phi$ then $Z_p = \phi$

for all except expotentially many primes

(Koiran)

If $Z(f_1, \ldots, f_m) \neq \phi$ then $Z_p \neq \phi$

for primes with inverse exponential density.

(Koiran, assuming GRH)

Koirans Proof of $HN \in AM$

If $Z(f_1, \ldots, f_m) = \phi$ then $Z_p = \phi$

for all except expotentially many primes

(Koiran)

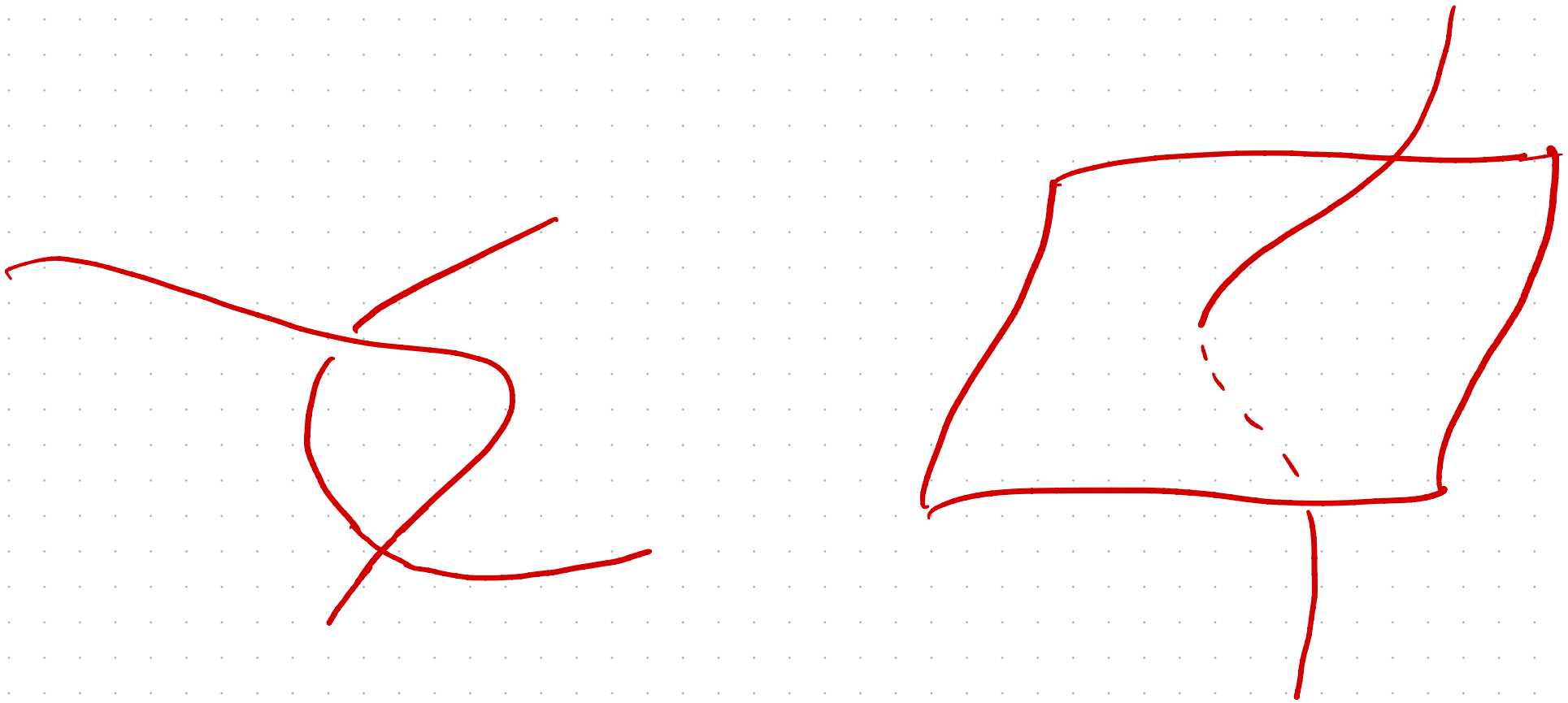
If $Z(f_1, \ldots, f_m) \neq \phi$ then $Z_p \neq \phi$

for primes with inverse exponential density.

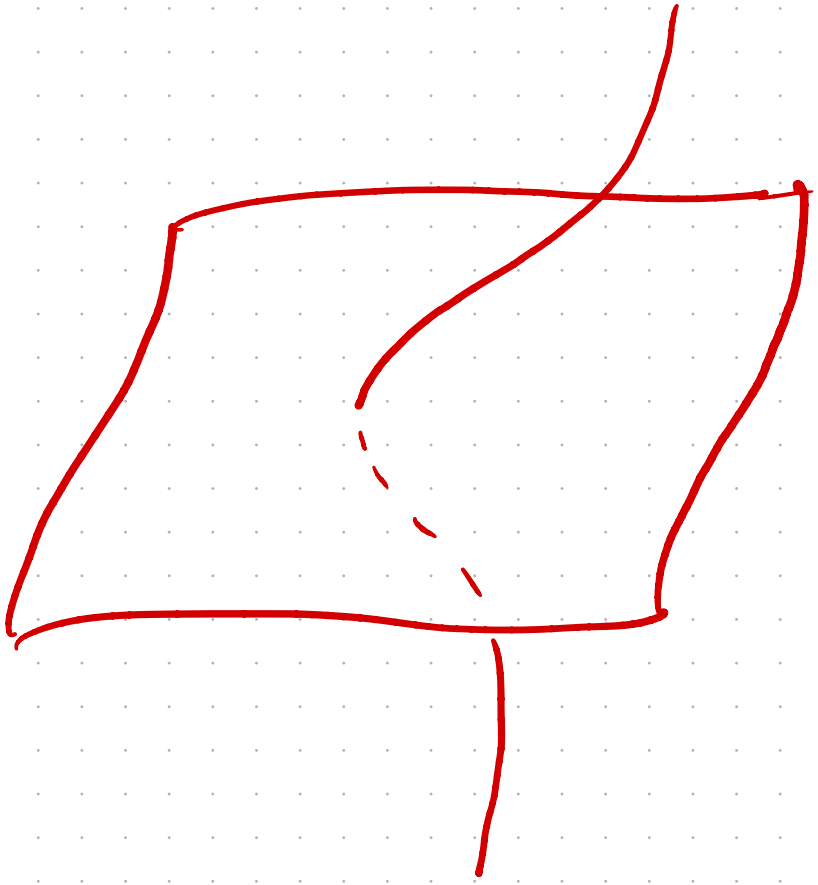
(Koiran, assuming GRH)

This gap is enough to invoke Goldwasser Sipser set lower bound protocol to show $HN \in AM$.

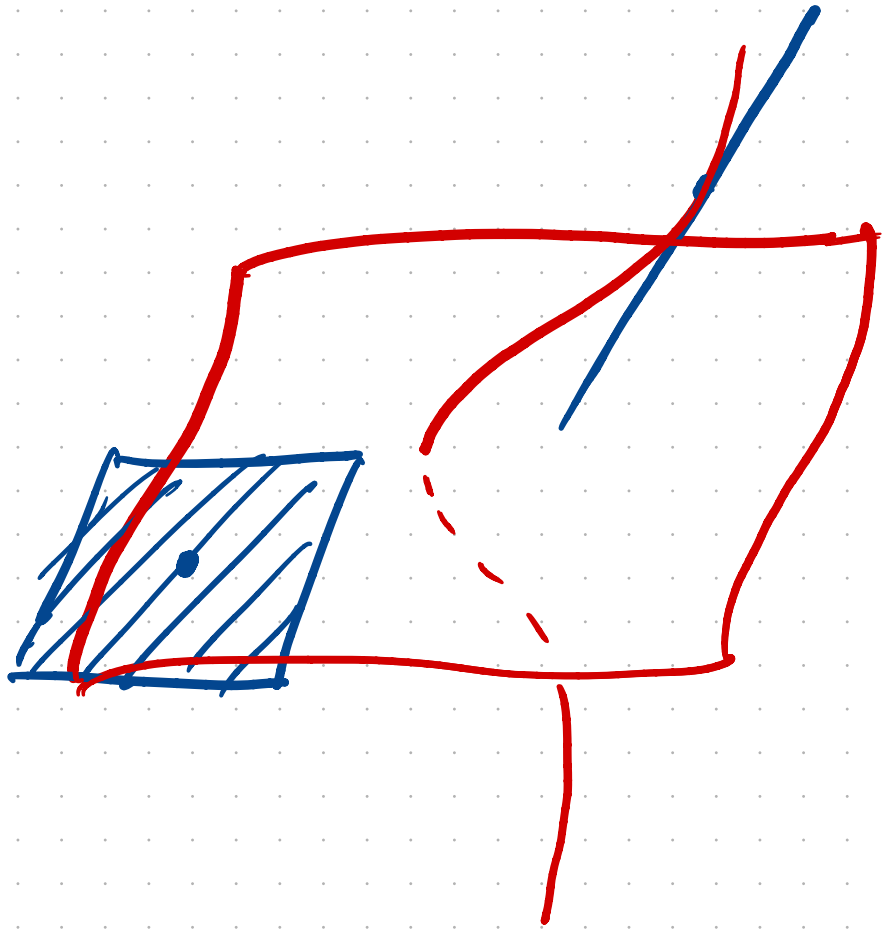
Radical Ideals that are not prime



Radical ideal primality problem.

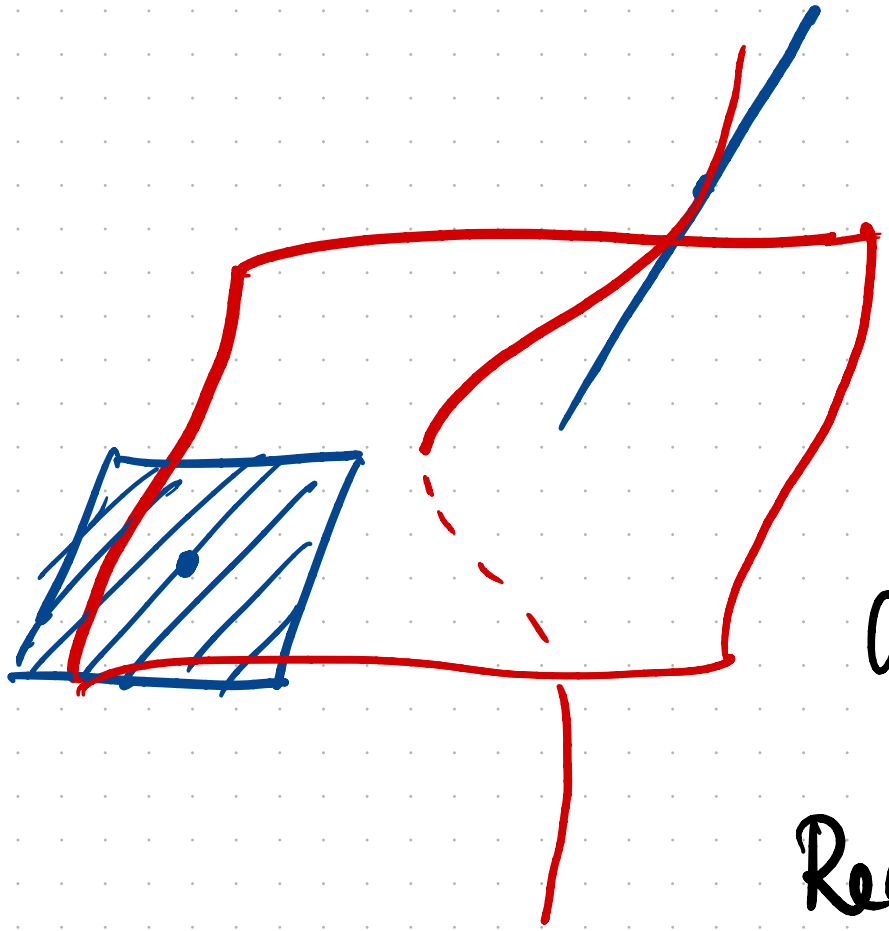


Radical ideal primality problem.



Tangent Space

Radical ideal primality problem.



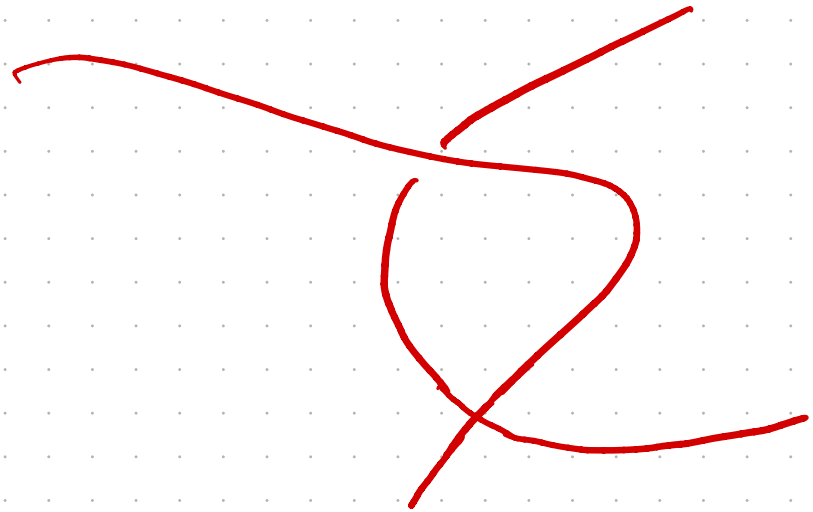
Tangent Space

$$\dim T_p = \operatorname{rk} \ker \operatorname{Jac}_p(\bar{f})$$

Requires radical ideal.

Finding a point with small tangent space reduces to system satisfiability.

One / Many curve case.



One / Many curve case.

If Z is one curve, is $\bar{Z}_p$ one curve for many primes ?

If Z is many curves, is $\bar{Z}_p$ many curves for many primes ?

How can we detect the number of curves just via $\mathbb{F}_p$ roots ?

One / Many curve case.

If Z is one curve, is $\bar{Z}_p$ one curve for many primes ?

If Z is many curves, is $\bar{Z}_p$ many curves for many primes ?

Bertini - Noether theorem.

How can we detect the number of curves just via $\mathbb{F}_p$ roots ?

Lang - Weil bounds.

Lang Weil bounds

Thm (Lang, Weil): if C is a $\mathbb{F}_p$-definable irreducible curve in $\overline{\mathbb{F}_p}^n$, then C has $p \pm 3D\sqrt{p}$ points in $\mathbb{F}_p^n$.

Lang Weil bounds

Thm (Lang, Weil): if C is a $\mathbb{F}_p$-definable irreducible curve in $\overline{\mathbb{F}_p}^n$, then C has $p \pm 3D\sqrt{p}$ points in $\mathbb{F}_p^n$.

If $\overline{Z_p}$ is irreducible, then $|Z_p| < p + 3D\sqrt{p}$

If $\overline{Z_p}$ is reducible and has at least two $\mathbb{F}_p$-definable components then $|Z_p| > 2p - 6D\sqrt{p}$.

Effective Bertini Noether + $\mathbb{F}_p$ definability

Thm (QOS):

If Z is irreducible, then $\overline{Z}_p$ is irreducible for all but exponentially many primes.

If Z is reducible, then $\overline{Z}_p$ is reducible, and has at least two $\mathbb{F}_p$ definable components for primes with inverse exponential density, assuming GRH.

Inv. exp. density of primes p happens because

e.g. $f := \prod_{i=1}^{d=2^b} (x_1 - a_i \cdot x_2)$ with $a_i \in \mathbb{Q}$ &
$f \in \mathbb{Z}[x_1, x_2]$.

$|Gal_{\mathbb{Q}}(f)| \approx d! \Rightarrow \{p \mid f \bmod p \text{ splits completely}\}$
has density $\approx \frac{1}{d!} \approx \frac{1}{\exp(\exp(s))}$.

While, $\{p \mid f \bmod p$ has ≥ 2 roots$\}$ has
density $\approx \frac{1}{d^2} \approx \frac{1}{\exp(s)}$.

Proof Sketch:

Z irreducible $\Rightarrow$ $\overline{Z}_p$ irreducible

By Noether Normalization, we can reduce to curves in $\mathbb{C}^2$.

Requires new height bounds for elimination ideal generators.

Effective Noether equations [Kal 85] to show that irreducibility of curves in $\mathbb{C}^2$ is preserved mod p.

Proof Sketch:

Z reducible $\Rightarrow$ $\overline{Z}_p$ reducible + two $\overline{\mathbb{F}}_p$ definable components

Factoring algorithm $\mathbb{Z}[\text{Kal}\ \&\ \Sigma]$ to find components of Z that are definable over small extensions of $\mathbb{Q}$.

Algebraic number theoretic tools to show that these components are preserved mod p.

Requires height bounds etc for algebraic numbers.

□

Summary:

We give interactive proofs for primality testing of natural classes of ideals, and reduce the gap between upper and lower bounds.

The main technical result is an effective bound on the sets of bad primes for irreducibility and reducibility, assuming GRH.

Open problems:

* What makes problems in computational algebraic geometry and computational commutative algebra hard?

* Most problems involve Gröbner basis, which are worst case EXPSPACE hard. Is this always required to handle the embedded primes?

* Could (HN over $\overline{\mathbb{F}_p}$) be solved below PSPACE?