Is more than 50% error a hard limit? : No

$\boxed{\text{Th}}$ [Sudan '97] If P has $d^\circ \leq \frac{\sqrt{q}}{200}$ & $|G| \geq \frac{q}{100}$ then there is an efficient algo which finds all P agreeing with F, $\geq 1\%$ of the time.

"list decoding".

$\boxed{\text{X}}$ The permanent lemma.

Let $A = (a_{ij})$ be a $n \times n$ matrix over $\mathbb{F}$.

(*) The same technique shows:

Prop| Every ~~n x~~ $(p-1)n+1 \times n$ matrix A with coefficients in $\mathbb{F}$ has a non zero $\{0,1\}$ vector $x \in \{0,1\}^{(p-1)n+1}$ s.t.

$$A.x = 0$$

(in other words a nontrivial subset sum of the columns is 0)

$$A \begin{pmatrix} \\ \\ \end{pmatrix}_{(p-1)n+1}$$

Rem:

(Central in complexity theory; Permanent hard / Determinant easy), it has very few applications.

$\boxed{\text{Th}}$ (Alon's permanent lemma)

$A = (a_{ij})$ coef in $\mathbb{F}$ $n \times n$. If $per(A) \neq 0$, there exists $x \in \{0,1\}^n$ s.t. Ax has all its coordinates $\neq 0$

Pf Form the polynomial $P(x_1, \dots, x_n) = \prod_{i=1}^{n} (a_{i1}x_1 + a_{i2}x_2 + \dots + a_{in}x_n)$

Note that the coef. of $x_1 \dots x_n$ is exactly $Per(A)$

By Comb null, since each x_i can take value in $\{0,1\}$ & $|\{0,1\}| >$ ~~coef~~ $\exp(x_i)$ in $x_1 \dots x_n$, P does not vanish on $\{0,1\}^n$.

$P(x) \neq 0$ means no coordinate of Ax is 0 ☒

Systèmes d'équations polynomiales

I Modélisation.

Tout pb. de décision discret se code facilement en sys d'équations.

(i) 3-SAT Formula $(x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_4)$

$$x_1^2 - 1 = 0 \quad (x_1-1)(x_2-1)(x_3-1)=0$$
$$x_2^2 - 1 = 0 \quad (x_1+1)(x_2-1)(x_4+1)=0$$
$$x_3^2 - 1 = 0$$
$$x_4^2 - 1 = 0$$

(ii) 2-Coloring Graph on vertices x_i & edges $x_i x_j$

$$V \left| \begin{array}{l} x_1^2 - 1 = 0 \\ \vdots \\ x_n^2 - 1 = 0 \end{array} \right. \qquad E \left| \; x_i + x_j = 0 \quad \forall \text{edge } x_i x_j \right.$$

etc... when the system is feasible, a certificat VRAI est une assignation des x_i. Comment certifier FAUX ?

II Certificats.

Prop The dimension of the space of polynomials of degree $\leq d$ with n variables is $\binom{n+d}{n}$

Pf A basis is given by the monomials $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$

Nb de façon d'écrire $\alpha_1 + \dots + \alpha_n \leq d$ avec $\alpha_i \geq 0$ entiers.

= Nb de mots sur $\{0,1\}$ avec n "1" et d "0".

Ex $d = 4$ $n = 5$

$$\underbrace{00}_{\alpha_1}1\underbrace{0}_{\alpha_2}1\underbrace{}_{\alpha_3}1\underbrace{0}_{\alpha_4}1\underbrace{}_{\alpha_5}1 \rightarrow x_1 x_3 \qquad 1000101110 \quad x_1^3 x_5 \qquad \otimes$$

Certificat d'infaisabilité

Gauss $Ax + By = b$	Farkas (1902)
$\nexists x \; Ax = b \iff$	$\nexists x \; Ax \leq b \iff$ (in $\mathbb{R}$)
$\exists y$ s.t. $\begin{cases} yA = 0 \\ yb = 1 \end{cases}$	$\exists y$ s.t. $\begin{cases} yA = 0 \\ yb = -1 \\ y \geq 0 \end{cases}$
Hilbert (1893)	**Stengle (1974)** (in $\mathbb{R}$)
$\nexists x \; p_1(x) = 0 \wedge \dots \wedge p_t(x) = 0$	$\nexists x \; p_1(x) \geq 0 \wedge \dots \; p_t(x) \geq 0$
$\iff \exists q_1 \dots q_t$ s.t. $\sum p_i q_i = 1$	$\exists \underbrace{q_0, q_1, q_2, q_{12}, q_3, q_{13}, \dots}_{(SOS)}$ t.q. $q_0 + q_1 p_1 + q_2 p_2 + q_{12} p_1 p_2 \dots = -1$

$\boxed{\text{Th}}$ Let $\mathbb{F}$ be algebraically close field, and $p_1, \dots, p_t \in \mathbb{F}[x_1, \dots, x_n]$, if there is no solution $x \in \mathbb{F}^n$ to $p_1(x) = 0 \wedge p_2(x) = 0 \wedge \dots \wedge p_t(x) = 0$, then there are polynomials $q_1, \dots, q_t$ s.t. $\sum_{i=1}^{t} q_i p_i = 1$ (or -1)

Remarksss:

① Observe that both cases exclude each other.

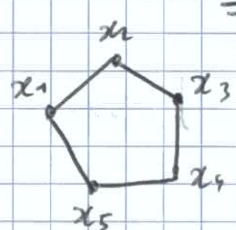
② $\mathbb{F}$ algebraically close is necessary for the case $t = 1$! $x^2 + 1 = 0$ in $\mathbb{R}$ has no certificate of this sort.

③ Let us illustrate on 2-COL (Exo: write modelization of 2-SAT)

x_i vertices $\quad x_i^2 - 1 = 0 \quad P_i$ $\qquad$ G 2-colorable

$x_i x_j$ edges $\quad x_i + x_j = 0 \quad P_{ij}$ $\qquad \iff$ $P_i, \dots, P_{ij}$ have common solution.

Certificate when G is <u>not</u> 2-col, for instance if G contains a cycle of length 5



$$Q_{12} P_{12} + Q_{23} P_{23} + Q_{34} P_{34} + Q_{45} P_{45}$$

$$\frac{x_1}{2}(x_1 + x_2) - \frac{x_1}{2}(x_2 + x_3) + \frac{x_1}{2}(x_3 + x_4) - \frac{x_1}{2}(x_4 + x_5)$$

$$+ \frac{x_1}{2}(x_5 + x_1) - (x_1^2 - 1) = 1$$

$$+ Q_{51} P_{51} + Q_1 \; P_1$$

④ Does this mean that 3-COL is in coNP (existence of certificate for NO). Unfortunately no, since the Q_i:

- can have large degree (but not here in fact → d° bounded by $2n$ since $x_i^3 = 1$.
- have potentially $\binom{3n}{n}$ monomials.

(5) Assume that the system has a bounded degree d certificate of NO (like 2-COL has degree 1) $\rightarrow$ certif is computable in poly time.

(Pf) Introduce variable for coefficient of all Q_i, $i = 1..t$.

$\rightarrow$ this gives $t \cdot \binom{n+d}{n} = O(n^d)$

$\rightarrow$ Solve the linear system. $\boxtimes$

(6) If the pb which is modelized (decision) always (provably) have degree $\leq d$ certificate, then this is a ~~decision~~ polytime decision algo (which does not return a solution in case of YES)

(7) Checking in polytime existence of certif of $d^\circ \leq d$ gives:

$\rightarrow$ either input has a solution

$\rightarrow$ or not, but the NS proof of it is rather complex (for this particular modelling.

$\rightarrow$ Gives a hierachy on coNP: Take your favorite modelling of 3-SAT.

(8) There is a cell missing!

Need to interpret $y \geq 0$ for multipliers Q_i.

Def: $Q \in \mathbb{R}[x_1, \dots, x_n]$ is a sum of square (sos) if it is a sum of square

☹ [The obvious $\sum Q_i P_i = -1$ with each Q_i sos does not work,

☹ Unlike univariate, we do not have $P(x) \geq 0 \Rightarrow P$ sos. Motzkin example:

$1 + x^2y^4 + x^4y^2 - 3y^2x^2$ is ≥ 0 but not sos

$\boxed{\text{Th}}$ (Stengle '74) positivstellensatz

Let $P_1, \dots, P_t \in \mathbb{R}[x_1, \dots, x_n]$. Then either:

- $\exists x \in \mathbb{R}^n$ s.t. $P_1(x) \geq 0 \,\&\, \dots \,\&\, P_t(x) \geq 0$
- Or $\forall I \subseteq \{1, \dots, n\}$ $\exists Q_I \in \mathbb{R}[x_1, \dots, x_n]$ sos such that

$$\sum_{I \subseteq \{1, \dots, n\}} Q_I \prod_{i \in I} P_i = -1$$

$\rightarrow$ leads to SOS hierarchy (could beat SDP for instance on MAX CUT pb).

{ What are the polynomials of the form $\sum Q_i P_i$??

$\boxed{X}$ Polynomial ideals

A subset $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ is a (polynomial) ideal if

- $0 \in I$
- $\forall p, q \in I \quad p+q \in I$
- $\forall p \in I \ \& \ q \in \mathbb{F}[x] \quad p \cdot q \in I$

Key examples:
- The set of polynomial vanishing on some fixed subset $X \subseteq \mathbb{F}^n$
- The ideal generated by $\{p_1, \ldots, p_\ell\}$, denoted by $\langle p_1, \ldots, p_\ell \rangle$ which is $\left\{ \sum q_i p_i : q_1, \ldots, q_\ell \in \mathbb{F}[x] \right\}$. Basic tool of poly method
- Ideals being close under $\cap$, one can consider $\langle P \rangle$ where P is an arbitrary subset, which is $\displaystyle\bigcap_{\substack{I \text{ ideal} \\ P \subseteq I}} I$.
- An ideal is principal if it is generated by one polynomial

Prop: Univariate polynomial ideals are principal.

Pf: $I \subseteq \mathbb{F}[x]$. Choose $p \in I \setminus \{\neq 0\}$ with minimum degree. Now for every $f \in I$ we have $f = qp + r$ with $d^\circ r < d^\circ p$ & $r = f - qp \in I$ thus $r = 0$ and $f \in \langle p \rangle$ $\boxtimes$

Rem: • NS says All $\{p_i\}$ vanish on some point

or

$$\langle p_1, \ldots, p_t \rangle = \mathbb{F}[x_1, \ldots, x_n]$$

- bivariate polynomial ideals are not necessarily ~~finitely generated~~ principal.

$\langle x^{11}, x^{10}y, x^9y^2, \ldots, xy^{10}, y^{11} \rangle$ cannot be generated by less than 12 poly.

Finite list? Yes:

Th (Hilbert finite basis theorem)

Every ideal of $\mathbb{F}[x_1, \ldots, x_n]$ is finitely generated.

The main ~~step~~ issue to generalize univariate proof is to find an invariant (like degree) which will strictly decrease at each step. We need here to (artificially) order all monomials. ~~in order~~ for this.

Def: A <u>monomial order</u> is a total order $\leq$ on all monomials x^α s.t.

- $1 \leq m \quad \forall$ monomials m
- $m_1 \leq m_2 \Rightarrow m.m_1 \leq m.m_2 \quad \forall m$

Remark: • $\leq$ is a linear extension of the divisibility partial order $\leq_d$ on monomials.

Indeed if $m_1 | m_2 \Rightarrow \left.\begin{array}{l} m_2 = m\, m_1 \\ 1 \leq m \end{array}\right\} \Rightarrow m_1 . 1 \leq m_1 . m$ $\boxtimes$

So, whatever the choice for $\leq$, we always have $xy^2 \leq x^2y^3$.

• Examples include

- lexicographic order $\leq_{lex}$: $1 \leq x_2 \leq x_2^2 \leq x_2^3 \leq \ldots \leq x_1 \leq x_1x_2 \leq x_1x_2^2 \leq \ldots$
- deglex $\quad m_1 \leq_{deglex} m_2$ if $\begin{cases} d^\circ m_1 < d^\circ m_2 \\ \text{or} \\ d^\circ m_1 = d^\circ m_2 \ \& \ m_1 \leq_{lex} m_2 \end{cases}$

$\rightarrow 1 \leq x_2 \leq x_1 \leq x_2^2 \leq x_1x_2 \leq x_1^2 \leq x_2^3 \leq \ldots$

We will ~~need to~~ use $\leq$ to induct, so we need some well foundedness.

$\boxed{\text{Th}}$ (Dickson wqo) Given any ∞ sequence of monomials $m_1, m_2, \ldots \in \mathbb{F}[x_1 \ldots x_n]$ there exists an infinite non decreasing subsequence:

$m_{i_1} \leq_{div} m_{i_2} \leq_{div} m_{i_3} \leq \ldots$

Proof: Induction on n.

- For $n=1$, we just extract greedily $m_1 = m_{i_1} \leq m_{i_2} \leq \cdots \leq m_{i_k}$. If process stops on $m_{i_k} = x^j$, then all terms m_ℓ with $\ell > i_k$ belong to $\{1, \ldots, x^{j-1}\} \rightarrow$ we extract a constant ∞ sequence.
- For $n > 1$, write $(m_i) = (x_1^{d_i} . m_i')$

$\boxed{\text{☆ Argmax}}$ $\mapsto$ extract ∞ subsequence on (m_i')

$\mapsto$ extract ∞ subsequence of it which is non dec on x_1!

$\boxed{\text{Cor}}$ Any monomial order is well founded.

Pf: Assume that $m_1 > m_2 > m_3 \ldots$ is a strictly decreasing sequence, it contains an ∞ increasing $\leq_{div}$ sequence $\boxtimes$

Given a M.O. $\leq$

Def. Given a polynomial $p \in \mathbb{F}[x]$, its <u>leading monomial</u> is the monomial which is largest w.r.t. $\leq$. We denote it by $\mathrm{LM}(p)$.

A <u>Gröbner basis</u> of an ideal I is a set $\mathbb{B}$ of polynomials $\in I$ such that for every $q \in I$ $\exists p \in \mathbb{B}$ s.t. $\mathrm{LM}(p)$ divides $\mathrm{LM}(q)$.

<u>Prop:</u> If B is a GB, then $\langle B \rangle = I$

Pf: Let $q \in I$. Set $q = q_1$. $\exists p \in B$ s.t. $\underbrace{\mathrm{LM}(p)}_{:= m_1}$ divides $\underbrace{\mathrm{LM}(q)}_{:= m_2}$

*

$$\left.\begin{aligned} p &= \alpha_1 m_1 + \bar{p} \\ q &= \alpha_2 m_1 \cdot m + \bar{q} \end{aligned}\right) \text{Thus } \cancel{q - \frac{m\alpha_2}{\alpha_1} p =} \overbrace{\boxed{\bar{q} - \frac{m\alpha_2}{\alpha_1} \cdot \bar{p}}}^{q_1} \in I$$

* Assume that $q \in I \setminus \langle B \rangle$ for contr. & $\mathrm{LM}(q)$ min for $\leq$

& $\mathrm{LM}(\bar{q}) < \mathrm{LM}(q)$

& every monomial in in $\frac{m\alpha_2}{\alpha} \bar{p}$ is s.t.

$m \cdot \bar{m}$ with $\bar{m} < m_1$, thus $m\bar{m} < m m_1 = m_2$.

$\rightarrow \mathrm{LM}(q_1) < \mathrm{LM}(q)$ so $q_1 \in \langle B \rangle$, but we have $q = \underbrace{q_1 + \frac{m\alpha_2}{\alpha_1} p_1}_{\in \langle B \rangle}$ ☒

We are now ready for:

Pf <u>Hilbert basis th.</u>

Consider I ideal of $\mathbb{F}[x_1 .. x_n]$. Pick $\leq$ a monomial order ~~We have $\langle I \rangle = I$, and thus I is a GB of I. Consider now a GB B which set of leading monomials $\mathrm{LM}(B)$ is~~. Consider the set $\mathrm{LM}(I)$ of all leading monomials of polynomials of I. The set of minimal elts for $\leq_{div}$ of $\mathrm{LM}(I)$ is finite, by Dickson Lemma. Consider M then $p_1, .., p_t \in I$ s.t. $\{\mathrm{LM}(p_1), .., \mathrm{LM}(p_t)\} = M$. Observe that every $p \in I$ satisfies $\exists i = 1..t$ s.t. $\mathrm{LM}(p_i)$ divides $\mathrm{LM}(p)$. Therefore $\mathrm{LM}(p_i) \leq \mathrm{LM}(p)$ and then B is a GB. Finally $\langle p_1, .., p_t \rangle = I$. ☒

<u>Quick word on varieties</u>

Let $p_1, .., p_t$ be polynomials in $\mathbb{C}[x_1 .. x_n]$. The (affine algebraic) variety $V(\{p_1, .., p_t\})$ is the set $\{x \in \mathbb{C}^n : p_i(x) = 0 \ \forall i\}$.

As we have seen NS tells us that

$$V(p_1 \dots p_n) = \emptyset \text{ iff } \langle p_1, \dots, p_n \rangle = \mathbb{C}[x]$$

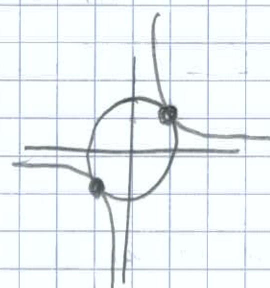
Recall that if $X \subseteq \mathbb{C}^n$, $I(X)$ is the ideal of poly vanishing on X.
We clearly have $I(V(p_1, \dots, p_n)) \supseteq \langle p_1, \dots, p_n \rangle$ but it could be that some polynomial $q \notin \langle p_1, \dots, p_n \rangle$ is such that $q^k \in \langle p_1, \dots, p_\ell \rangle$. Hence it would also vanish on $V(p_1, \dots, p_\ell)$ and thus the inclusion can be strict. The strong form of NS tells it is the only possibility.

<u>Def:</u> I ideal, we denote by $V(I)$ the set $\{x \in \mathbb{C}^n : p(x) = 0 \ \forall p \in I\}$

- we denote by $\sqrt{I} := \{p \text{ s.t. } \exists k, p^k \in I\}$

$\boxed{\text{Th}}$ Strong form of NS. $\mathbb{F}$ algebraically closed,
$\forall I \subseteq \mathbb{F}[x_1, \dots, x_n]$ we have $\sqrt{I} = \cancel{\subseteq} I(V(I))$

$$I = \langle x^2 + y^2 - 2, xy - 1 \rangle$$
$$= \langle x^2 + y^2 - 2, y^3 - 2y + x \rangle$$
$$= \langle y^4 - 2y^2 + 1, x - 2y + y^3 \rangle$$



$\langle y^2 - 1, x^2 - 1, xy - 1 \rangle$ $\underline{xy}$

<u>R trick</u> $g \in \sqrt{\langle p_1, \dots, p_\ell \rangle} \iff \langle p_1, \dots, p_\ell, 1 - y g \rangle$

g vanishes on $V(\langle p_1 \dots p_\ell \rangle)$ in $\mathbb{F}[x_1, \dots, x_n, y]$

$\Downarrow \langle p_1, \dots, p_\ell, 1 - y g \rangle$ in $\mathbb{F}[x_1, \dots, x_n, y]$
$= \langle 1 \rangle$

$$\underline{\sum q_i p_i + q - y q g} = 1$$

$q \neq 0$ $\quad q = a + y b \quad y = \dfrac{1}{g(x_1 \dots x_n)}$

$\sum q_i \left(\frac{1}{g}, x_1, \dots, x_n\right) p_i = 1 \quad q_i = a_i + y b_i$

$\Rightarrow \sum \frac{1}{g^{r_i}} h_i p_i = 1 \Rightarrow \dfrac{\sum h_i' p_i}{g^r} = 1 \quad \otimes$