The permanent lemma.

Let \( A = (d_{ij}) \) be a matrix over \( \mathbb{F} \).

The same technique shows:

**Prop.** Every \((p-1)n^{n+1}\times n\) matrix \( A \) with coefficients in \( \mathbb{F} \) has a non zero \( \mathbb{F}/2 \)-vector \( \mathbf{x} \in \mathbb{F}/2^{(p-1)n + 1} \) s.t.

\[ A \mathbf{x} = 0 \]

(in other words a subet sum of the columns is 0).

\[ A = \left( \begin{array}{cccc} 
\vdots \\
\vdots \\
\vdots \\
\vdots \\
\vdots \\
\vdots \\
\end{array} \right) \]

Rem. (Central in complexity theory. Permanent hard. Determinant easy.) It has very few applications.

**Th.** (Alon's permanent lemma)

\( A = (d_{ij}) \) cochain \( n \times n \). If \( \text{per}(A) \neq 0 \), there exists \( \mathbf{x} \in \mathbb{F}/2^n \) s.t.

\( A \mathbf{x} \) has all its coordinates \( \neq 0 \).

**Pe.** Form the polynomial \( P(x_1, \ldots, x_n) = \prod_{i=1}^{n} (a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n) \)

Note that the coeff. of \( x_1x_n \) is exactly \( \text{Pa}(A) \).

By comb null, since each \( x_i \) can take values in 0,1,2,3, \( \text{exp}(x_i) \) in \( 2x_i - x_i^2 \), \( P \) does not vanish in \( \mathbb{F}/2^{15} \).

\( P(x) \neq 0 \) means no coordinate of \( A \mathbf{x} \) is 0.
Systèmes d'équations polynomiaux

I. Modélisation.
Tout problème direct se code facilement au syst d'équat-s de décision.

(i) 3-SAT
Formula \((x_1 \lor x_2 \lor x_3) \land (\neg x_4 \lor x_5 \lor \neg x_6)\)

\[\begin{align*}
x_1^2 - 1 &= 0 \\
x_2^2 + 1 &= 0 \\
x_3^2 + 1 &= 0 \\
x_4^2 - 1 &= 0 \\
x_5^2 - 1 &= 0 \\
x_6^2 - 1 &= 0
\end{align*}\]

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

\[\begin{align*}
x_1^2 - 1 &= 0 \\
x_2^2 - 1 &= 0
\end{align*}\]

\[\begin{align*}\lor \quad E \quad |\quad x_i \lor x_j = 0 \quad \text{Vedge} \quad x_i x_j
\end{align*}\]

etc... when the system is feasible, a certificate VRAI est une assignment 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 \(x_1^d x_2^{d-1} \ldots x_n^d\)

\(d\) de fact: décrire \(x_1^d \ldots + x_n^d\) avec \(d\) \(d\) entiers.

\(=\) Nb de mots sur \(30,14\) avec \(n^d\) et \(d^0\)

Ex. \(d = 4\) \(n = 5\)

\[\begin{align*}
0010110110 &\rightarrow x_1 x_3 \\
x_4 x_5 x_6 x_7 &\rightarrow 100010110 \quad x_4 x_5 \&
\end{align*}\]
Gauss\[Ax+By=b\]
\[\iff\]
Farkas (1902)
\[\text{exists } A \text{ s.t. } \begin{cases} g A = 0 \\ g b = -1 \end{cases} \]
\[\iff\]
Farkas (1902)
\[\text{exists } A \text{ s.t. } \begin{cases} g A = 0 \\ g b = -1 \end{cases} \]
\[\iff\]
\[\exists y \text{ s.t. } y A = 0 \quad \exists y \text{ s.t. } y b = -1 \]
\[\iff\]
\[\exists y \text{ s.t. } y A = 0 \quad \exists y \text{ s.t. } y b = -1 \]
\[\iff\]
\[\exists y \text{ s.t. } y A = 0 \quad \exists y \text{ s.t. } y b = -1 \]
\[\iff\]
\[\exists y \text{ s.t. } y A = 0 \quad \exists y \text{ s.t. } y b = -1 \]

Hilbert (1983) \[p_1(x) = 0 \land \ldots \land p_n(x) = 0\]
\[\iff\]
Stengle (1974) \[\begin{cases} p_1(x) > 0 \\ \ldots \\ p_n(x) > 0 \end{cases} \]
\[\iff\]
\[\exists q_1, q_2, q_3, q_4, q_5, q_6 \text{ s.t. } \sum_{i=1}^{6} q_i p_i = 1 \quad \text{or} \quad -1 \]

Theorem: Let $\mathbb{F}$ be an algebraically closed field, and $p_1, \ldots, p_6 \in \mathbb{F}[x_1, \ldots, x_6]$, if there is no solution $x \in \mathbb{F}^6$ to $p_1(x) = 0 \land \ldots \land p_6(x) = 0$, then there are polynomials $q_1, \ldots, q_6$ s.t. \[\sum_{i=1}^{6} q_i p_i = 1 \quad \text{or} \quad -1 \]

Remarks:
1. Observe that both cases exclude each other.
2. If algebraically closed is necessary for the case $6 - 1$, $x^2 + 1$ in $\mathbb{R}$ has no certificate of this sort.
3. Let us illustrate an 2-COL (Example write modularization of 2-SAT).
4. Let us illustrate an 2-COL (Example write modularization of 2-SAT).

Certificate when $G$ is not 2-col, for instance if $G$ contains a cycle of length 5:

\[
\begin{align*}
Q_{12} P_{12} + Q_{23} P_{23} + Q_{34} P_{34} + Q_{45} P_{45} + Q_{51} P_{51} + Q_{61} P_{61} = 1 \\
\frac{x_1}{2} (x_1 + x_2) + \frac{x_2}{2} (x_2 + x_3) + \frac{x_3}{2} (x_3 + x_4) + \frac{x_4}{2} (x_4 + x_5) + \frac{x_5}{2} (x_5 + x_6) + \frac{x_6}{2} (x_6 + x_1)
\end{align*}
\]

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 have in fact $d^6$ bounded
     by $2^n$), since $x_i^2 = 1$.
5. Assume that the system has a bounded degree certificate of NO (like 2-COL has degree 1) \( \Rightarrow \) certif is computable in poly-time.

\[ P_{\text{r}} \] introduce variable for coefficient of all \( Q_i, i=1, \ldots \).

\[ \text{this gives } e_n (n+d) = O(n^d) \]

\[ \Rightarrow \text{solve the linear system (probably)} \]

6. If the pb which is modelled always have degree \( d \) certificate, then this is a decision poly-time decision algo (which does not return a)

\[ \text{solution process of YES} \]

\[ \text{Chaining in poly-time existence of certif of } d^0 \leq d \text{ gives:} \]

\[ \Rightarrow \text{either input has a solution} \]

\[ \Rightarrow \text{or not, but the NS proof of it is rather complex (for this particular modelling)} \]

\[ \Rightarrow \text{Gives a hierarchy on coNP: Take your favorite modelling of 3-SAT} \]

8. There is a cell missing! Need to interpret \( y \geq 0 \) for multipliers \( Q_i \).

**Def.** \( Q \in R[x_1, \ldots, x_n] \) is a sum of square (sos) if it is a sum of square.

\[ \text{The obvious } \leq Q_i = -1 \text{ with each } Q_i \text{ sos does not work,} \]

\[ \text{Unlike univariate, we do not have } P(x) \geq 0 \Rightarrow P \text{ sos. Note in example:} \]

\[ 1 + x^2 y^2 + x^4 y^2 - 3 y^2 x^2 \geq 0 \text{ but not sos} \]

\[ \text{Th.} (\text{Stengle '74}) \text{ positive semidefinite} \]

Let \( p_1, \ldots, p_e \in R[x_1, \ldots, x_n] \). Then either:

\[ \exists \bar{x} \in R^n \text{ s.t. } p_1(x) \geq 0 \land \ldots \land p_e(x) \geq 0 \]

\[ \text{or} \forall \bar{x} \in \bar{x}_1, \ldots, x_n \exists \bar{Q}_i \in R[x_1, \ldots, x_n] \text{ sos such that} \]

\[ \leq Q_i = -1 \]

\[ i \in \{1, \ldots, e\} \]

\[ \Rightarrow \text{leads to sos hierarchy (could beat SDP for instance on MAX CUT pb).} \]

\[ ? \text{What are the polynomials of the form } \leq Q_i P_i \text{ ??} \]
Polynomial ideals

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

1. \( 0 \in I \)
2. \( \forall p, q \in I \) \( p + q \in I \)
3. \( \forall p \in I \) \( \forall q \in \mathbb{F}[x_1, \ldots, x_n] \) \( p \cdot q \in I \)

Key examples:
1. The set of polynomial vanishing on some fixed subset \( \mathbb{X} \subseteq \mathbb{F}^n \)
2. The ideal \( \langle p_1, \ldots, p_k \rangle \), denoted by \( \prod_{i=1}^k p_i \)
3. \( \langle p \rangle \) which is \( \{ \sum c_i p_i : c_i \in \mathbb{F} [x_1, \ldots, x_n] \} \)

- Ideals being close under \( \cap \), one can consider \( \bigcap_{I \in \mathcal{I}} I \) for an arbitrary subset, which is \( \bigcup_{I \in \mathcal{I}} I \)
- An ideal is principal if it is generated by one polynomial

Prop: Univariate polynomial ideals are principal.

- \( I \subseteq \mathbb{F}[x] \). Choose \( p \in I \) with minimum degree. Now for every \( f \in I \) we have \( f = q \cdot p + r \) with \( d_r < d_p \) and \( r \in I \) thus \( r = 0 \) and \( f \in \langle p \rangle \)

Remark: NS says all \( p_i \) vanish on some point

\( \langle p_1, \ldots, p_k \rangle = \mathbb{F}[x_1, \ldots, x_k] \) principal.

- Bivariate polynomial ideals are not necessarily finitely generated.

\( \langle x^n, x^y, x^g, \ldots, xy, y^n \rangle \) cannot be generated by less than 12 polynomials.

Finite list? Yes:

\[ \{ \text{Hilbert finite basis theorem} \} \]

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

The main step to generalize univariate proofs is to find an invariant (like degree) which will strictly decrease at each step. We need here to (artificially) order all monomials.
Def: A monomial order is a total order $\leq$ on all monomials $x^\alpha$ s.t.

1. $1 \leq m$ for all monomials $m$
2. $m_1 \leq m_2 \Rightarrow m_1 m_2 \leq m_2 m_1$ for all monomials $m_1$, $m_2$

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

Indeed, if $m_1 \mid m_2 \Rightarrow m_2 = m_1 m_2' \Rightarrow m_1, 1 \leq m_1, m$.

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

Examples include
- lexicographic order $\leq_{lex}$: $1 \leq x_1 \leq x_2 \leq x_3 \leq \ldots$, $x_i \leq x_j$ for $i < j$
- degree lexicographic order $\leq_{deglex}$: $m_1 \leq_{deglex} m_2$ if $d^0 m_1 < d^0 m_2$ or $d^0 m_1 = d^0 m_2$ and $m_1 \leq_{lex} m_2$

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

Th (Dickson wgo) Given any $\omega$ sequence of monomials $M_1, M_2, \ldots \in \mathbb{C}[x, x_2]$ there exists an infinite decreasing subsequence.

$m_1 \leq \text{div } M_1 \leq \text{div } M_2 \leq \ldots$

Proof: Induction on $n$.

1. For $n = 1$, we just extract greedily $m_1 = m_{i_1} \leq m_{i_2} \leq \ldots \leq m_{i_k}$. If the process stops on $M_{i_k} = x^{\alpha}$, then all terms $m_\ell$ with $\ell > i_k$ belong to $\{1, \ldots, x^{\alpha - 1}\}$.

2. For $n > 1$, write $(M_i) = (x^{\alpha_i}, m_i)$

$\Rightarrow$ extract infinite subsequence on $(m_i)$

$\Rightarrow$ extract $\omega$ subsequence of it which is non-decreasing $\leq_{\text{div}}$.

Conversely, any monomial order is well-founded.

Corollary: Assume that $m_1 > m_2 > m_3 \ldots$ is a strictly decreasing sequence, it contains an $\omega$ increasing $\leq_{\text{div}}$ sequence $\Rightarrow$
Given a PID \( \mathcal{O} \), a monomial leading monomial is the monomial which is largest w.r.t. \( \leq \). We denote it by \( \text{LM}(p) \).

A Gröbner basis of an ideal \( I \) is a set \( B \) of polynomials \( \in I \) such that for every \( q \in I \) \( \exists p \in B \) s.t. \( \text{LM}(p) \) divides \( \text{LM}(q) \).

Prop: If \( B \) is a GB, then \( \langle B \rangle = I \).

Let \( q \in I \). Set \( q = q_2 + \sum_{i=1}^{n} q_i \) \( \in \text{LM}(q) \) \( \in I \)

\[ p = x_1 m_1 + \cdots + x_n m_n \]

\[ q = x_1 m_1 + \cdots + x_n m_n + q_n \]

Thus \( q = x_1 m_1 + \cdots + x_n m_n + q_n \)

Assume that \( q \in I \), \( \langle B \rangle \) & \( \text{LM}(q) \) \( < \text{LM}(q) \)

\[ \text{min } \text{for } q \in I \text{ such that } m_1 \text{ divides } \text{LM}(q) \text{ is s.t. } m_1 < m_2 \]

Thus \( \text{min } \in I \) \( \leq \text{min } \in I \) \( \leq \text{min } \in I \)

\[ \text{LM}(q_1) < \text{LM}(q) \text{ so } q_1 \in \langle B \rangle \text{ but we have } q = q_1 + \frac{m m_2}{m_1} q_2 \]

We are now ready for:

Hilbert basis th.

Consider an ideal \( I \) of \( \mathbb{F}[x_1, \ldots, x_n] \), let \( \langle B \rangle \) be its GB and thus \( \langle B \rangle \) is a GB of \( I \). Consider now a GB \( B \) which is a set of leading monomials of polynomials \( \in I \). The set of minimal elements for \( \leq \) of \( \text{LM}(I) \) is finite, by Dickson's Lemma. Consider then \( p_1, \ldots, p_k \in I \) s.t. \( \{ \text{LM}(p_1), \ldots, \text{LM}(p_k) \} = \mathbb{N} \), observe that every \( p \in I \) satisfies \( \exists i \) s.t. \( \text{LM}(p_i) \) divides \( \text{LM}(p) \). Therefore \( \text{LM}(p_i) \in \text{LM}(p) \) and thus \( B \) is a GB. Finally \( \langle p_1, \ldots, p_k \rangle = I \).

Quickword on varieties

Let \( p_1, \ldots, p_k \) be polynomials in \( \mathbb{C}[x_1, \ldots, x_n] \). The (affine algebraic) variety \( V(p_1, \ldots, p_k) \) is the set \( \{ x \in \mathbb{C}^n : p_i(x) = 0 \forall i \} \).
As we have seen, NS tells us that

\[ V(p_1, \ldots, p_n) = \emptyset \iff \langle p_1, \ldots, p_n \rangle = \mathbb{C}^n \]

Recall that if \( \mathfrak{a} \subseteq \mathbb{C}^n \), \( I(\mathfrak{a}) \) is the ideal of polynomials vanishing on \( \mathfrak{a} \).

We clearly have \( I(V(p_1, \ldots, p_n)) \supseteq \langle p_1, \ldots, p_n \rangle \) but it could be that some polynomial \( q \notin \langle p_1, \ldots, p_n \rangle \) is such that \( q^k \in \langle p_1, \ldots, p_n \rangle \). Hence, it would also vanish on \( V(p_1, \ldots, p_n) \) and thus the inclusion can be strict. The strong form of NS tells it is the only possibility.

**Def:** Ideal: we denote by \( V(\mathfrak{a}) \) the set \( \{ x \in \mathbb{C}^n : p(x) = 0 \ \forall p \in \mathfrak{a} \} \).

We denote by \( \sqrt{\mathfrak{a}} = \{ p \in \mathbb{C}[x] : p^k \in \mathfrak{a} \} \).

**Strong form of NS:** Algebraically closed, \( V(\mathfrak{a}) \subseteq \mathbb{C}[x_1, \ldots, x_n] \) we have \( \sqrt{\mathfrak{a}} = \mathfrak{a}^{V(I(\mathfrak{a}))} \).

\[
\mathfrak{a} = \langle x^2 + y^2 - 2, xy - 1 \rangle \\
= \langle x^2 + y^2 - 2, y^2 - 2y + x \rangle \\
= \langle y^2 - 2y + 1, x - 2y + y^3 \rangle \\
= \langle y^2 - 1, x - 1, xy - 1 \rangle
\]

We want to show \( g \in \sqrt{\langle p_1, p_2 \rangle} \iff \langle p_1, p_2, 1 - y^2 g \rangle \) vanishes on \( V(\langle p_1, p_2 \rangle) \) in \( \mathbb{C}[x_1, \ldots, x_n, y] \).

\[
\langle p_1, p_2, 1 - y^2 g \rangle \text{ in } \mathbb{C}[x_1, \ldots, x_n, y]
\]

\[
\sum q_i \psi_i + q - y^2 g = 1
\]

We have \( q \neq 0 \), \( q = a + yb \), \( y = \frac{1}{q_1(x_1, \ldots, x_n)} \).

\[
\sum q_i \left( \frac{a_i}{q_1}, x_1, \ldots, x_n \right) \psi_i = 1 \\
q_i = a_i + yb_i
\]

\[
\Rightarrow \sum \frac{a_i}{q_1} \psi_i = 1 \Rightarrow \frac{\sum a_i \psi_i}{q_1} = 1 \quad \text{Q.E.D.}
\]