Today

1. Complexity of Ideal Membership
   - ExpSpace hardness
   - Degree upper bounds.

2. Hilbert Nullstellensatz
I. A - ExpSpace Hardness

**Known Hard Problem**

**CWEP**: Commutative Word Equivalence Problem

**Input**: $\Sigma$, $|\Sigma| = n$

- **Rules**: $\alpha_i = \beta_i$  \(i = 1, \ldots, m\)
  
  $\alpha_i, \beta_i \in \Sigma^*$

- **(Implicit)**: $\sigma T = T \sigma$

  \(\forall \sigma, T \in \Sigma\)

- $\alpha, \beta \in \Sigma^*$

**Task**: Determine if $\alpha = \beta$.

**Using commutativity and equivalence rules.**
Reduction

Let $\leq = \sigma_1 \ldots \sigma_n$

$\#_i(w) = \# \text{ of occurrences of } \sigma_i \text{ in } w$

$\alpha_j = \beta_j$ $\Rightarrow f_j(x_1, \ldots, x_n)$

$$f(x_1, \ldots, x_n) = \prod_{i=1}^{\#(\alpha)} x_i - \prod_{i=1}^{\#(\beta)} x_i$$

Claim: $f \in \text{Ideal } (f_1, \ldots, f_m)$

$\Leftrightarrow \alpha = \beta \Leftrightarrow \{ \alpha_j = \beta_j \}_{j=1}^m$

Proof: Omitted.
1. B: Degree Bounds

Recall: \( f \in I(f_1, \ldots, f_m) \)

\[ \iff \exists q_1, \ldots, q_m \in K[x_1, \ldots, x_n] \text{ s.t.} \]

\[ f = \sum q_i \]

To make bound "constructive" we need an upper bound on degree of \( q_1, \ldots, q_m \).

[Assume \( \deg(f, f_1, \ldots, f_m) \leq d \)]

Combined with polylog space algorithms for solving linear equations over field, we get complexity \( \text{SPACE} \left( \text{POLYLOG} \left( \text{Degree bound} \right) \right) \)
Two views of Ideal Membership

I. Linear equation over a ring

\[ \exists g_1, \ldots, g_m \in R = \mathbb{K}[x_1, \ldots, x_n] \text{ s.t. } \]
\[ f = \sum_{i} \alpha_i g_i \]
\[ \uparrow \]
\[ \text{one big linear equation} \]

II. Many linear equations over a field \( K \)

\[ \exists \{ \alpha_{i, \delta} \} \quad \delta = 1, \ldots, m \quad \forall \alpha_i \leq D_n \text{ s.t. } \]
\[ \forall \beta \in (\mathbb{Z}^{\geq 0})^n, \quad \exists \beta_i \leq D_n + d \]
\[ f_{\beta} = \sum_{i, \delta} \alpha_{i, \delta} f_{i, \beta - \alpha} \]
\[ (f_{\beta}, f_{i, \beta}, \alpha_{i, \delta} \text{ denote coefficients of } f, f_i, \alpha_i) \]
Want to know: When does existence of solution to $I$ imply existence of solution to $II$ with parameter $D_n$.

Strategy:
- Build common generalized problem $II(i)$.
- $II(n) = I$
- $II(0) = II$
- Variable elimination:
  $II(i+1)$ has solution with $m_{i+1}$ equations & degree $D_{i+1}$
  $\Rightarrow II(i)$ has solution with $m_i = \text{poly}(m_{i+1}, D_{i+1})$
  & $D_i = \text{poly}(m_{i+1}, D_{i+1})$
$\Pi(i)$: $j$-variable linear system.

**Given:** $f_\beta, f_i, \rho \in K[x_{i-1}, x_i]$

\[
\exists g_i, \alpha \in K[x_{i-1}, x_i], \quad \exists ! i \leq \rho
\]

\[
f_\beta = \prod_{i=1}^{\rho} g_i, \alpha
\]

---

**Lemma:** $\Pi(i+1)$ instance with $M$ equations of degree $D$ has solution $\Rightarrow$ corresponding $\Pi(i+1)$ instance has solution with degree $\text{poly}(m, D) \leq$ equations $\text{poly}(n, \rho)$
key supporting lemma: \((L1)\)

- Given linear system \(Ax = b\),
  
  \[ A \in \mathbb{R}[z]^{m \times m}, \quad b \in \mathbb{R}[z]^{m} \]
  
  \[ \max \{ \deg(A_{i,j}), \deg(b_{i}) \} \leq D \]

  - \(A\) has full rank minor with monic determinant.

  - Then \(Ax = b\) has solution \(\Rightarrow\) it has a solution with \(\deg(x_{i}) \leq \text{poly}(mD)\).
Proof of L1

w.l.o.g. \[ A = \begin{bmatrix} \hat{A} & B \\ \vdots & \vdots \\ C & D \end{bmatrix} \]

where \( \hat{A} \) is full rank & \( \text{det}(\hat{A}) = \text{monic} \).

Solution looks like

\[ x = \begin{bmatrix} x_1 \\ \vdots \\ x_2 \end{bmatrix}, \quad b = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \]

Note, by rank, that (if solution exists)

\[ \begin{bmatrix} \hat{A} & B \\ C & D \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \]

\[ \Rightarrow \begin{bmatrix} C & D \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} b_2 \end{bmatrix} \]

so, can ignore \[ [C \quad D], \quad [b_2] \].
Want to show that W.L.O.G. \( \text{deg} (x_1) \leq \text{small} \).

\[
x_1 = \hat{A}^{-1} (b_1 - Bx_2)
\]

So \( \text{deg} (x_1) \leq \text{deg} \left( \text{Adj} (A) + \text{deg} b_1 + \text{deg} (B) + \text{deg} (x_2) \right) \)

\[
\left[ \text{using } \hat{A}^{-1} = \frac{\text{Adj} (A)}{\det (A)} \right]
\]

So reduces to show, can reduce \( \text{deg}(x_2) \).

Now use the fact

\( (x_1, x_2) \) solution \( \Rightarrow \) so is

\[
( x_1 + \text{Adj} (\hat{A}) B y_2, x_2 - \det (\hat{A}) y_2 )
\]
So can reduce $\deg(x_2) \leq \deg(\text{det}(\mathbf{A})) \leq m^k$.

From above, follows that $\deg(x_1) \leq O(m^0)$ also.

How to use lemma L1?

How to ensure $\text{det}(\mathbf{A})$ is monic?

Idea: Generic/Random invertible linear transform.
22: Given \( A x = b \) with \( A, b \in \mathbb{K}[x_1, \ldots, x_j] \)

let \( T \) be an invertible affine transform
from \( \mathbb{K}^j \to \mathbb{K}^j \)

then

1. \( x \) is solution to \((A, b)\) \(\iff\)

\( x(T) \) is solution to \( (A(T), b(T)) \);

\( \deg (x(T)) = \deg (x) \).

2. \( \) w.h.p. over choice of \( T \)

\( \det (\tilde{A}(T)) \) is monic in \( x_j \).

Combining L5 & L2, we get proof of [Hermann's] bound on \( \deg g, \ldots, g_m \).