Lecture 24: Complexity of Ideal Membership Problem

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

April 12, 2021

Overview

- Ideal Membership Problem & a Variant
- Univariate Case
- Multivariate Case
- EXPSPACE-completeness
- Conclusion
- Acknowledgements

Ideal Membership Problem

- **Input:** $g_1, \ldots, g_s,\ f \in \mathbb{F}[x_1, \ldots, x_n]$
- **Output:** is $f \in (g_1, \ldots, g_s)$?

Ideal Membership Problem

- **Input:** $g_1, \ldots, g_s,\ f \in \mathbb{F}[x_1, \ldots, x_n]$
- **Output:** is $f \in (g_1, \ldots, g_s)$?
- To solve this, we need to show the existence (or non-existence) of polynomials $h_1, \ldots, h_s$ such that

$$f = g_1 \cdot h_1 + \cdots + g_s h_s$$

Ideal Membership Problem

- **Input:** $g_1, \ldots, g_s, \; f \in \mathbb{F}[x_1, \ldots, x_n]$
- **Output:** is $f \in (g_1, \ldots, g_s)$?
- To solve this, we need to show the existence (or non-existence) of polynomials $h_1, \ldots, h_s$ such that

$$f = g_1 \cdot h_1 + \cdots + g_s h_s$$

- We know that if such polynomials exist then Groebner bases and the division algorithm will find them for us

Ideal Membership Problem

- **Input:** $g_1, \ldots, g_s, \; f \in \mathbb{F}[x_1, \ldots, x_n]$
- **Output:** is $f \in (g_1, \ldots, g_s)$?
- To solve this, we need to show the existence (or non-existence) of polynomials $h_1, \ldots, h_s$ such that

$$f = g_1 \cdot h_1 + \cdots + g_s h_s$$

- We know that if such polynomials exist then Groebner bases and the division algorithm will find them for us
- But today we will see a different algorithm for it - we will solve it by converting the polynomial system above into a *linear system* of equations

Ideal Membership Problem

- **Input:** $g_1, \ldots, g_s, \ f \in \mathbb{F}[x_1, \ldots, x_n]$
- **Output:** is $f \in (g_1, \ldots, g_s)$?
- To solve this, we need to show the existence (or non-existence) of polynomials $h_1, \ldots, h_s$ such that

$$f = g_1 \cdot h_1 + \cdots + g_s h_s$$

- We know that if such polynomials exist then Groebner bases and the division algorithm will find them for us
- But today we will see a different algorithm for it - we will solve it by converting the polynomial system above into a *linear system* of equations
- The complexity of today's algorithm comes from showing that if the h_i's exist, then they must exist in some "reasonable degree"
- So we need to upper bound the degree of the h_i's

Algorithm - Main Idea

$\beta_{i\bar{a}}\bar{x}^{a} \cdot \gamma_{i(\bar{e}-\bar{a})}\bar{x}^{\bar{e}-\bar{a}}$

- If we know upper bound on the degree of the h_i's then all we have left is a linear system!

$$f = g_1 \cdot h_1 + g_2 h_2 + \cdots + g_s h_s$$

inputs: $f, g_1, g_2, \ldots, g_s$ (degree d); $h_1, h_2, \ldots, h_s$: degree $\le D$

$$f = \sum_{\bar{e}} \alpha_{\bar{e}} \bar{x}^{\bar{e}}, \quad \alpha_{\bar{e}} \in \mathbb{F}$$

$$g_i = \sum_{\bar{e}} \beta_{i\bar{e}} \bar{x}^{\bar{e}}, \quad \beta_{i\bar{e}} \in \mathbb{F}$$

$$h_i = \sum_{\bar{e}} \gamma_{i\bar{e}} \bar{x}^{\bar{e}}$$

$\gamma_{i\bar{e}}$: variables of linear system

$\bar{e} = (1,2,3)$

$\bar{x} = (x_1, x_2, x_3)$

$\bar{x}^{\bar{e}} = x_1 x_2^2 x_3^3$

- write all monomials $\bar{x}^{\bar{e}}$, $\sum_{i=1}^{n} e_i \le D + d$
- for each monomial we are going to have a linear equation:

$$\alpha_{\bar{e}} = \sum_{i=1}^{s} \sum_{\bar{a} \le \bar{e}} \beta_{i\bar{a}} \cdot \gamma_{i(\bar{e}-\bar{a})}$$

Algorithm - Main Idea

- If we know upper bound on the degree of the h_i's then all we have left is a linear system!
- Since linear systems can be solved in *polylogarithmic space*, a degree bound of D on the h_i's, together with a degree bound of d for f_i, g would give us a space complexity of:

$$\text{poly}(n \log(D), \log(s))$$

$O(sD^n)$

Size of linear system:

equations = # monomials in n variables of degree $\leq D+d$

$= \binom{n-1+D+d}{n-1} \sim D^n$

variables = $s \cdot$ (# monomials in n variables of deg D (h_i))

$= s \cdot D^n$

Linear System of Polynomials

- **Input:** $g_{ij},\ f_i \in \mathbb{F}[x_1, \ldots, x_n]$ where $i \in [s], j \in [t]$, $\deg(g_{ij}), \deg(f_i) \leq d$
- **Output:** is there $h_1, \ldots, h_t$ such that

$$f_i = g_{i1}h_1 + \cdots + g_{it}h_t \quad \forall i \in [s]$$

$$\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1t} \\ g_{21} & g_{22} & \cdots & g_{2t} \\ \vdots & & & \\ g_{s1} & \cdots & & g_{st} \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_t \end{pmatrix} = \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_t \end{pmatrix}$$

Linear System of Polynomials

- **Input:** $g_{ij},\ f_i \in \mathbb{F}[x_1, \ldots, x_n]$ where $i \in [s], j \in [t]$, $\deg(g_{ij}), \deg(f_i) \leq d$
- **Output:** is there $h_1, \ldots, h_t$ such that

$$f_i = g_{i1}h_1 + \cdots + g_{it}h_t \quad \forall i \in [s]$$

- Can be reduced to ideal membership problem by adding extra variables $y_1, \ldots, y_s$:

$$f_1y_1 + \cdots + f_sy_s \in (y_1 \cdot g_{1j} + y_2 \cdot g_{2j} + \cdots + y_s \cdot g_{sj})_{j=1}^t$$

Linear System of Polynomials

- **Input:** $g_{ij},\ f_i \in \mathbb{F}[x_1, \ldots, x_n]$ where $i \in [s], j \in [t]$, $\deg(g_{ij}), \deg(f_i) \leq d$
- **Output:** is there $h_1, \ldots, h_t$ such that

$$f_i = g_{i1} h_1 + \cdots + g_{it} h_t \quad \forall i \in [s]$$

- Can be reduced to ideal membership problem by adding extra variables $y_1, \ldots, y_s$:

$$f_1 y_1 + \cdots + f_s y_s \in (y_1 \cdot g_{1j} + y_2 \cdot g_{2j} + \cdots + y_s \cdot g_{sj})_{j=1}^{t}$$

- It will be convenient to prove that this problem can be solved in EXPSPACE

Linear System of Polynomials

- **Input:** $g_{ij},\ f_i \in \mathbb{F}[x_1, \ldots, x_n]$ where $i \in [s], j \in [t]$, $\deg(g_{ij}), \deg(f_i) \leq d$
- **Output:** is there $h_1, \ldots, h_t$ such that

$$f_i = g_{i1} h_1 + \cdots + g_{it} h_t \quad \forall i \in [s]$$

- Can be reduced to ideal membership problem by adding extra variables $y_1, \ldots, y_s$:

$$f_1 y_1 + \cdots + f_s y_s \in (y_1 \cdot g_{1j} + y_2 \cdot g_{2j} + \cdots + y_s \cdot g_{sj})_{j=1}^{t}$$

- It will be convenient to prove that this problem can be solved in EXPSPACE

Theorem (Hermann, Mayr-Meyer)

If the linear system of polynomials problem has a solution, then it has a solution in which

$$\deg(h_i) \leq (t \cdot d)^{2^n}$$

Remarks

- The above theorem proves that we can solve the ideal membership problem in EXPSPACE

Remarks

- The above theorem proves that we can solve the ideal membership problem in EXPSPACE
- We can assume that our base field $\mathbb{F}$ is infinite, without loss of generality.
- This is because a system of linear equations has a solution over an extension field $\mathbb{F} \subset \mathbb{K}$ if, and only if, it has a solution in $\mathbb{F}$
- **Practice problem:** prove this statement

Special Case: Univariate Polynomials

- Assume now our input $g_{ij},\ f_i \in \mathbb{F}[x]$ where $i \in [s], j \in [t]$, $\deg(g_{ij}), \deg(f_i) \leq d$
- is there $h_1, \ldots, h_t$ such that

$$f_i = g_{i1}h_1 + \cdots + g_{it}h_t \quad \forall i \in [s]$$

Special Case: Univariate Polynomials

- Assume now our input $g_{ij},\ f_i \in \mathbb{F}[x]$ where $i \in [s], j \in [t]$, $\deg(g_{ij}), \deg(f_i) \leq d$
- is there $h_1, \ldots, h_t$ such that

$$f_i = g_{i1}h_1 + \cdots + g_{it}h_t \quad \forall i \in [s]$$

- Let $M = (g_{ij}) \in \mathbb{F}[x]^{s \times t}$ and $\mathbf{f} = (f_i) \in \mathbb{F}[x]^s$

Special Case: Univariate Polynomials

- Assume now our input $g_{ij},\ f_i \in \mathbb{F}[x]$ where $i \in [s], j \in [t]$, $\deg(g_{ij}), \deg(f_i) \leq d$
- is there $h_1, \ldots, h_t$ such that

$$f_i = g_{i1}h_1 + \cdots + g_{it}h_t \quad \forall i \in [s]$$

- Let $M = (g_{ij}) \in \mathbb{F}[x]^{s \times t}$ and $\mathbf{f} = (f_i) \in \mathbb{F}[x]^s$
- Can assume that M has full row rank (thus $s \leq t$), otherwise we remove dependencies

Special Case: Univariate Polynomials

- Assume now our input $g_{ij},\ f_i \in \mathbb{F}[x]$ where $i \in [s], j \in [t]$, $\deg(g_{ij}), \deg(f_i) \leq d$
- is there $h_1, \ldots, h_t$ such that

$$f_i = g_{i1}h_1 + \cdots + g_{it}h_t \quad \forall i \in [s]$$

- Let $M = (g_{ij}) \in \mathbb{F}[x]^{s \times t}$ and $\mathbf{f} = (f_i) \in \mathbb{F}[x]^s$
- Can assume that M has full row rank (thus $s \leq t$), otherwise we remove dependencies
- If $s = t$ then M is invertible and our solution would be $\mathbf{h} = M^{-1}\mathbf{f}$

Special Case: Univariate Polynomials

- Assume now our input $g_{ij},\ f_i \in \mathbb{F}[x]$ where $i \in [s], j \in [t]$, $\deg(g_{ij}), \deg(f_i) \leq d$
- is there $h_1, \ldots, h_t$ such that

$$f_i = g_{i1}h_1 + \cdots + g_{it}h_t \quad \forall i \in [s]$$

- Let $M = (g_{ij}) \in \mathbb{F}[x]^{s \times t}$ and $\mathbf{f} = (f_i) \in \mathbb{F}[x]^s$
- Can assume that M has full row rank (thus $s \leq t$), otherwise we remove dependencies
- If $s = t$ then M is invertible and our solution would be $\mathbf{h} = M^{-1}\mathbf{f}$
- Rearranging columns, can write

$$M = \begin{pmatrix} A & v_1 & v_2 & \cdots & v_r \end{pmatrix}$$

where $A \in \mathbb{F}[x]^{s \times s}$ is invertible and $r = t - s$

square

Special Case: Univariate Polynomials

- We have
$$M = \begin{pmatrix} A & \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_r \end{pmatrix}$$
where $A \in \mathbb{F}[x]^{s \times s}$ is invertible and $r = t - s$

Special Case: Univariate Polynomials

- We have
$$M = \begin{pmatrix} A & \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_r \end{pmatrix}$$
where $A \in \mathbb{F}[x]^{s \times s}$ is invertible and $r = t - s$
- Let $\mathbf{h} = (y_1, \ldots, y_s, z_1, \ldots, z_r)$ then

$$A \cdot \mathbf{y} = \mathbf{f} - \sum_{i=1}^{r} z_i \mathbf{v}_i$$

$$M \bar{h} = \bar{f}$$

$$M \bar{h} = A \bar{y} + \sum_{i=1}^{r} z_i \bar{v}_i = \bar{f}$$

$$\begin{pmatrix} A & \bar{v}_1 & \cdots & \bar{v}_r \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_s \\ z_1 \\ \vdots \\ z_r \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_s \end{pmatrix}$$

Special Case: Univariate Polynomials

- We have
$$M = \begin{pmatrix} A & \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_r \end{pmatrix}$$
where $A \in \mathbb{F}[x]^{s \times s}$ is invertible and $r = t - s$
- Let $\mathbf{h} = (y_1, \ldots, y_s, z_1, \ldots, z_r)$ then
$$A \cdot \mathbf{y} = \mathbf{f} - \sum_{i=1}^{r} z_i \mathbf{v}_i$$
- z_i's are the "free variables" and y_j's are the "pivot variables"
$$\mathbf{y} = A^{-1} \cdot (\mathbf{f} - \sum_{i=1}^{r} z_i \mathbf{v}_i)$$

determined

Special Case: Univariate Polynomials

- We have
$$M = \begin{pmatrix} A & \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_r \end{pmatrix}$$
where $A \in \mathbb{F}[x]^{s \times s}$ is invertible and $r = t - s$
- Let $\mathbf{h} = (y_1, \ldots, y_s, z_1, \ldots, z_r)$ then
$$A \cdot \mathbf{y} = \mathbf{f} - \sum_{i=1}^{r} z_i \mathbf{v}_i$$
- z_i's are the "free variables" and y_j's are the "pivot variables"
$$\mathbf{y} = A^{-1} \cdot (\mathbf{f} - \sum_{i=1}^{r} z_i \mathbf{v}_i)$$
- By Cramer's rule $A^{-1} = \dfrac{\text{Adj}(A)}{\det(A)}$ } ratio of two polynomials of small degree!

Special Case: Univariate Polynomials

- We have
$$M = \begin{pmatrix} A & \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_r \end{pmatrix}$$
where $A \in \mathbb{F}[x]^{s \times s}$ is invertible and $r = t - s$
- Let $\mathbf{h} = (y_1, \ldots, y_s, z_1, \ldots, z_r)$ then
$$A \cdot \mathbf{y} = \mathbf{f} - \sum_{i=1}^{r} z_i \mathbf{v}_i$$
- z_i's are the "free variables" and y_j's are the "pivot variables"
$$\mathbf{y} = A^{-1} \cdot (\mathbf{f} - \sum_{i=1}^{r} z_i \mathbf{v}_i)$$
- By Cramer's rule $A^{-1} = \dfrac{\text{Adj}(A)}{\det(A)}$
- Ratio of polynomials of low degree!

Special Case: Univariate Polynomials

- If $\mathbf{h} = (\mathbf{y}, \mathbf{z})$ is a *polynomial* solution to $M\mathbf{h} = \mathbf{f}$, then for any $c_1, \ldots, c_r \in \mathbb{F}[x]$ we have that $b_i = z_i - c_i \cdot \det(A)$ and

$$\mathbf{a} = A^{-1}(\mathbf{f} - b_1\mathbf{v}_1 - \cdots - b_r\mathbf{v}_r) = y + \mathrm{Adj}(A) \cdot (c_1\mathbf{v}_1 + \cdots + c_r\mathbf{v}_r)$$

polynomial vector

gives another polynomial solution to $M(\mathbf{a}, \mathbf{b})^T = \mathbf{f}$.

from polynomial solution $\bar{h} = \begin{pmatrix} \bar{y} \\ \bar{z} \end{pmatrix}$ can construct another polynomial solution

$$b_i = z_i - c_i \det(A)$$

$$\bar{a} = A^{-1}(\bar{f} - b_1\bar{v}_1 - \cdots - b_n\bar{v}_n)$$

$$= \underbrace{A^{-1}(\bar{f} - z_1\bar{v}_1 - \cdots - z_n\bar{v}_n)}_{\bar{y}} + A^{-1} \cdot \det(A)(c_1\bar{v}_1 + \cdots + c_n\bar{v}_n)$$

$\frac{\mathrm{Adj}(A)}{\det}$

Special Case: Univariate Polynomials

- If $\mathbf{h} = (\mathbf{y}, \mathbf{z})$ is a *polynomial* solution to $M\mathbf{h} = \mathbf{f}$, then for any $c_1, \ldots, c_r \in \mathbb{F}[x]$ we have that $b_i = z_i - c_i \cdot \det(A)$ and

$$\mathbf{a} = A^{-1}(\mathbf{f} - b_1\mathbf{v}_1 - \cdots - b_r\mathbf{v}_r) = y + \mathrm{Adj}(A) \cdot (c_1\mathbf{v}_1 + \cdots + c_r\mathbf{v}_r)$$

  gives another polynomial solution to $M(\mathbf{a}, \mathbf{b})^T = \mathbf{f}$.
- Because we are in univariate case (thus we have Euclidean domain) we can assume that all z_i's are reduced modulo $\det(A)$ and thus have degree bounded by $< \ell :=$ ~~$\deg(A)$~~ $\leq sd$

  $\deg(\det(A))$

$\mathbb{F}[x]$ Euclidean Domain ∴ division with remainder

$z_i = c_i \det(A) + b_i$

$\deg(b_i) < \deg(\det(A))$

↑ Euclidean division

Special Case: Univariate Polynomials

- If $\mathbf{h} = (\mathbf{y}, \mathbf{z})$ is a *polynomial* solution to $M\mathbf{h} = \mathbf{f}$, then for any $c_1, \ldots, c_r \in \mathbb{F}[x]$ we have that $b_i = z_i - c_i \cdot \det(A)$ and

$$\mathbf{a} = A^{-1}(\mathbf{f} - b_1\mathbf{v}_1 - \cdots - b_r\mathbf{v}_r) = y + \mathrm{Adj}(A) \cdot (c_1\mathbf{v}_1 + \cdots + c_r\mathbf{v}_r)$$

  gives another polynomial solution to $M(\mathbf{a}, \mathbf{b})^T = \mathbf{f}$.
- Because we are in univariate case (thus we have Euclidean domain) we can assume that all z_i's are reduced modulo $\det(A)$ and thus have degree bounded by $< \ell := \deg(A) \leq sd$
- Thus, we have

$$\begin{aligned}
\deg(y) &\leq \deg(A^{-1}) + \deg(f - z_1 v_1 - \cdots - z_r v_r) \\
&= \deg(\mathrm{Adj}(A)) - \deg(\det(A)) + \max\left\{\deg(f), \deg(\sum_{i=1}^{r} z_i v_i)\right\} \\
&\leq (s-1)d - \ell + \max(d, \ell - 1 + d) < sd \leq td
\end{aligned}$$

$(s \leq t)$

Proved: if there is a solution there is one with degree $\leq sd$

General Case

- To prove the general case, we will simply apply induction with base case being univariate case.

General Case

- To prove the general case, we will simply apply induction with base case being univariate case.
- We will look at the ring $\mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[x_1, \ldots, x_{n-1}][x_n]$

coefficients are polynomials in n-1 variables

univariate polynomial in x_n

General Case

- To prove the general case, we will simply apply induction with base case being univariate case.
- We will look at the ring $\mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[x_1, \ldots, x_{n-1}][x_n]$
- All the previous steps of the univariate case work the same way, apart from when we used the *Euclidean Algorithm* to reduce the degree of the polynomials over the variable x (which now will be x_n)

General Case

- To prove the general case, we will simply apply induction with base case being univariate case.
- We will look at the ring $\mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[x_1, \ldots, x_{n-1}][x_n]$
- All the previous steps of the univariate case work the same way, apart from when we used the *Euclidean Algorithm* to reduce the degree of the polynomials over the variable x (which now will be x_n)
- But Euclidean Divison still works if the polynomials are *monic* in x_n (so all we need is that $\det(A)$ be monic over x_n)

det(A) monic in x_n ⇒ we can control degree in x_n

R[x] not necessarily Euclidean domain

$f(x) = x^d +$ lower order terms

$g(x) = q(x) \cdot f(x) + r(x)$, $\deg r < d$

$g(x) = a_D x^D + \cdots$

$g(x) - a_D \cdot x^{D-d} f$

General Case

- To prove the general case, we will simply apply induction with base case being univariate case.
- We will look at the ring $\mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[x_1, \ldots, x_{n-1}][x_n]$
- All the previous steps of the univariate case work the same way, apart from when we used the *Euclidean Algorithm* to reduce the degree of the polynomials over the variable x (which now will be x_n)
- But Euclidean Divison still works if the polynomials are *monic* in x_n (so all we need is that $\det(A)$ be monic over x_n)
- To achieve that, we can do a generic linear change of variables of the form $x_i \leftarrow x_i + \alpha_i x_n$, which gives us an isomorphism from $\mathbb{F}[x_1, \ldots, x_n] \rightarrow \mathbb{F}[x_1, \ldots, x_n]$ preserving degree.

$x_i \longmapsto x_i + \alpha_i x_n$

General Case

- To prove the general case, we will simply apply induction with base case being univariate case.
- We will look at the ring $\mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[x_1, \ldots, x_{n-1}][x_n]$
- All the previous steps of the univariate case work the same way, apart from when we used the *Euclidean Algorithm* to reduce the degree of the polynomials over the variable x (which now will be x_n)
- But Euclidean Divison still works if the polynomials are *monic* in x_n (so all we need is that $\det(A)$ be monic over x_n)
- To achieve that, we can do a generic linear change of variables of the form $x_i \leftarrow x_i + \alpha_i x_n$, which gives us an isomorphism from $\mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}[x_1, \ldots, x_n]$ preserving degree. $\alpha_i \in \mathbb{F}$
- Since $\det(A) \neq 0$, a generic linear map as above will make

$$\det(A) = \alpha x_n^\ell + \quad \text{(other terms of } x_n \text{ degree } < \ell)$$

$\in \mathbb{F}$

$\alpha \cdot x_n^\ell$

$\det(A)(x_1, \ldots, x_n)$

$\det(A)(\alpha_1 x_n, \alpha_2 x_n, \ldots, \alpha_{n-1} x_n, x_n) \neq 0$

General Case

- As in the univariate case, and because we can make $\det(A)$ monic in x_n we can reduce to solutions where $\deg_n(h)$ is upper bounded by $t \cdot d$

General Case

- As in the univariate case, and because we can make $\det(A)$ monic in x_n we can reduce to solutions where $\deg_n(h)$ is upper bounded by $t \cdot d$
- So now, enough to only look for solutions where $\deg_n(h_i) \leq t \cdot d$

$M\bar{h} = \bar{f}$ $\qquad$ $\deg_n(h_i) \leq td$

General Case

- As in the univariate case, and because we can make $\det(A)$ monic in x_n we can reduce to solutions where $\deg_n(h)$ is upper bounded by $t \cdot d$
- So now, enough to only look for solutions where $\deg_n(h_i) \leq t \cdot d$
- But that reduces to the following linear system of equations!

$$f_{im}x_n^m = H_m^{(n)}[g_{i1}h_1 + \cdots + g_{it}h_t] \quad \forall i \in [s], m \in [td+d]$$

↳ homogeneous component in x_n of degree m

$$M\bar{h} = \bar{f} \qquad \deg_n(h_i) \leq t \cdot d$$

$$\bar{f} = \bar{f}^{(0)} + x_n \bar{f}^{(1)} + \cdots + x_n^{t\cdot d+d} \bar{f}^{(td+d)}$$

$$\bar{f}^{(j)} \in \mathbb{F}[x_1, \dots, x_{n-1}]^s \qquad \bar{f}^{(j)} = \begin{pmatrix} f_{1j} \\ f_{2j} \\ \vdots \\ f_{sj} \end{pmatrix}$$

$$f_i = f_{i0} + f_{i1}x_n + \cdots + f_{i(td+d)} x_n^{td+d}$$

General Case

- As in the univariate case, and because we can make $\det(A)$ monic in x_n we can reduce to solutions where $\deg_n(h)$ is upper bounded by $t \cdot d$
- So now, enough to only look for solutions where $\deg_n(h_i) \leq t \cdot d$
- But that reduces to the following linear system of equations!

$$f_{im} x_n^m = H_m^{(n)}[g_{i1} h_1 + \cdots + g_{it} h_t] \quad \forall i \in [s], m \in [td + d]$$

- System above has $s(t+1)d$ equations of polynomials in $\mathbb{F}[x_1, \ldots, x_{n-1}]$ of degree $\leq d$

one less variable

General Case

- As in the univariate case, and because we can make $\det(A)$ monic in x_n we can reduce to solutions where $\deg_n(h)$ is upper bounded by $t \cdot d$
- So now, enough to only look for solutions where $\deg_n(h_i) \leq t \cdot d$
- But that reduces to the following linear system of equations!

$$f_{im} x_n^m = H_m^{(n)}[g_{i1} h_1 + \cdots + g_{it} h_t] \quad \forall i \in [s], m \in [td + d]$$

- System above has $s(t+1)d$ equations of polynomials in $\mathbb{F}[x_1, \ldots, x_{n-1}]$ of degree $\leq d$
- And $\leq t \cdot td$ unknowns - given by the coefficients

$$h_k = \sum_{i=0}^{td-1} h_{ki} x_n^i$$

new variable vector

td new vectors

General Case

- As in the univariate case, and because we can make $\det(A)$ monic in x_n we can reduce to solutions where $\deg_n(h)$ is upper bounded by $t \cdot d$
- So now, enough to only look for solutions where $\deg_n(h_i) \leq t \cdot d$
- But that reduces to the following linear system of equations!

$$f_{im}x_n^m = H_m^{(n)}[g_{i1}h_1 + \cdots + g_{it}h_t] \quad \forall i \in [s], m \in [td + d]$$

- System above has $s(t+1)d$ equations of polynomials in $\mathbb{F}[x_1, \ldots, x_{n-1}]$ of degree $\leq d$
- And $\leq t \cdot td$ unknowns - given by the coefficients

$$h_k = \sum_{i=0}^{td-1} h_{ki} x_n^i$$

degree bound on variable x_n

- Thus our recursion becomes

$$D(n, d, t) \leq D(n-1, d, t^2 d) + td = D(n-1, d, (td)^2/d) + td$$

n variables, degree, dimension of poly-system

$s(t+1)d \sim t^2 d$

Recursion

$$D(n,d,t) \le D(n-1, d, t^2 d) + td$$

$$\le D\left(n-2, d, \underbrace{(t^2 d)^2 \cdot d}_{t^4 d^3 = \frac{(td)^4}{d}}\right) + \frac{(td)^2}{d} + td$$

$$\le D\left(n-k, d, \frac{(td)^{2^k}}{d}\right) + O\left(\frac{(td)^{2^{k-1}}}{d}\right)$$

$$\le \frac{(td)^{2^n}}{d} \le (td)^{2^n}$$

∎

EXPSPACE Completeness

- Since EXPSPACE is far from efficient, one may wonder if this is the best we can do, and it turns out the answer is yes.
- Mayr and Meyer also proved that the ideal membership problem is EXPSPACE-complete

EXPSPACE Completeness

- Since EXPSPACE is far from efficient, one may wonder if this is the best we can do, and it turns out the answer is yes.
- Mayr and Meyer also proved that the ideal membership problem is EXPSPACE-complete
- Reduced from the *commutative semigroup problem* (which they prove to be EXPSPACE hard) to ideal membership problem

EXPSPACE Completeness

- Since EXPSPACE is far from efficient, one may wonder if this is the best we can do, and it turns out the answer is yes.
- Mayr and Meyer also proved that the ideal membership problem is EXPSPACE-complete
- Reduced from the *commutative semigroup problem* (which they prove to be EXPSPACE hard) to ideal membership problem
- **Setup:** finite alphabet $\Sigma = \{\sigma_1, \ldots, \sigma_r\}$, set of rewriting rules S (of the form $\alpha = \beta$ where $\alpha, \beta \in \Sigma^*$) where S contains the rules

$\sigma_i \sigma_j = \sigma_j \sigma_i$ commutative rules

$\sigma_1 \sigma_2$

$\sigma_1^3 \sigma_2 \sigma_3 = \sigma_1 \sigma_1 \sigma_2 \sigma_1 \sigma_3 \in \Sigma^*$

$\sigma_i \sigma_j = \sigma_j \sigma_i$

EXPSPACE Completeness

- Since EXPSPACE is far from efficient, one may wonder if this is the best we can do, and it turns out the answer is yes.
- Mayr and Meyer also proved that the ideal membership problem is EXPSPACE-complete
- Reduced from the *commutative semigroup problem* (which they prove to be EXPSPACE hard) to ideal membership problem
- **Setup:** finite alphabet $\Sigma = \{\sigma_1, \ldots, \sigma_r\}$, set of rewriting rules S (of the form $\alpha = \beta$ where $\alpha, \beta \in \Sigma^*$) where S contains the rules $\sigma_i \sigma_j = \sigma_j \sigma_i$
- **Input:** two words $\alpha, \beta \in \Sigma^*$
- **Output:** is $\alpha = \beta$?

Commutative
semigroup
problem

EXPSPACE Completeness

- Since EXPSPACE is far from efficient, one may wonder if this is the best we can do, and it turns out the answer is yes.
- Mayr and Meyer also proved that the ideal membership problem is EXPSPACE-complete
- Reduced from the *commutative semigroup problem* (which they prove to be EXPSPACE hard) to ideal membership problem
- **Setup:** finite alphabet $\Sigma = \{\sigma_1, \ldots, \sigma_r\}$, set of rewriting rules S (of the form $\alpha = \beta$ where $\alpha, \beta \in \Sigma^*$) where S contains the rules $\sigma_i \sigma_j = \sigma_j \sigma_i$
- **Input:** two words $\alpha, \beta \in \Sigma^*$
- **Output:** is $\alpha = \beta$?
- To reduce to ideal membership problem, need to rewrite the rules of S with polynomials, which they write as polynomials of the form $x^\alpha - x^\beta$, then need to encode all these "relation polynomials" into a small ideal

Conclusion

- Different algorithm for Ideal Membership Problem and its analysis
- Reduced it to linear system solving!
- Saw degree bounds for the Ideal Membership Problem

Acknowledgement

- Lecture based entirely on Madhu's notes, lecture 14

http://people.csail.mit.edu/madhu/FT98/