Lecture 10: Complexity of Ideal Membership Problem

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

February 10, 2021

Overview

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

Ideal Membership Problem

- **Input:** $g_1, \ldots, g_s,\ f \in \mathbb{F}[x_1, \ldots, x_n]$ $\deg(g_i)$, $\deg(f) \leq d$
- **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

$$f = g_1 \cdot \underline{h_1} + \cdots + g_s \underline{h_s}$$

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

$$f = g_1 \cdot \underline{h_1} + \cdots + g_s \underline{h_s}$$

- 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 (doubly exponential)

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!

$$f = g_1 h_1 + \cdots + g_s h_s \qquad (*)$$

$$\deg(f), \deg(g_i) \le d \qquad \deg(h_i) \le \boxed{D}$$

$$\bar{\alpha} \in \{0, 1, \ldots, D\}^n \qquad \bar{x}^{\bar{\alpha}}$$

$$\underbrace{f_{\bar{\alpha}}}_{\text{input}} = \sum_{i=1}^{s} \sum_{\bar{\beta} \le \bar{\alpha}} \underbrace{g_{i\bar{\beta}}}_{\text{input}} \cdot \underbrace{h_{i\,\bar{\alpha}-\bar{\beta}}}_{\text{unknowns}}$$

coefficient of $\bar{x}^{\alpha}$ in $(*)$

gives us D^n equations (linear)

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_i would give us a space complexity of:

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

D doubly-exponential $\Rightarrow$ 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

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

$$G = (g_{ij}) \in \mathbb{F}[x]^{s \times t}$$

$$G \begin{pmatrix} h_1 \\ \vdots \\ h_t \end{pmatrix} = \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_s \end{pmatrix}$$

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 $y_1, \ldots, y_s$:

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

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 $i \in [s], j \in [t]$, $\deg(g_{ij}), \deg(f_i) \leq d$

$\boxed{s \leq t}$

- **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 $\mathrm{f} = (f_i) \in \mathbb{F}[x]^s$

Special Case: Univariate Polynomials

- Assume now our input $g_{ij},\ f_i \in \mathbb{F}[x]$ where $i \in [s], j \in [t]$, $\deg(g_{ij}), \deg(f_i) \leq d$ $s \leq t$
- 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 $\mathrm{f} = (f_i) \in \mathbb{F}[x]^s$
- 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 $\mathrm{f} = (f_i) \in \mathbb{F}[x]^s$
- Can assume that M has full row rank (thus $s \leq t$), otherwise we remove dependencies
- If $s = t$ then M is invertible over $\mathbb{F}(x)$ and our solution would be $h = M^{-1}\mathrm{f}$ over $\mathbb{F}(x)$

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 $\mathrm{f} = (f_i) \in \mathbb{F}[x]^s$
- 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 $h = M^{-1}\mathrm{f}$
- 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 $\underbrace{r = t - s}_{\text{remaining columns}}$

Special Case: Univariate Polynomials

- We have

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

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

$$M(h) = (f)$$

$$\overbrace{A\begin{pmatrix} h_1 \\ \vdots \\ h_s \end{pmatrix}} = (f) - \sum_{i=1}^{r} \underline{h_{s+i}} \cdot v_i$$

$\uparrow$ for any choice of h_{s+i}

get a solution over $\mathbb{F}(x)$ by inverting A

Special Case: Univariate Polynomials

- We have
$$M = \begin{pmatrix} A & v_1 & v_2 & \cdots & v_r \end{pmatrix}$$
where $A \in \mathbb{F}[x]^{s \times s}$ is invertible and $r = t - s$
- Let $h = (y_1, \ldots, y_s, z_1, \ldots, z_r)$ then
$$A \cdot y = f - \sum_{i=1}^{r} z_i v_i$$

$$y = A^{-1}\left(f - \sum_{i=1}^{r} z_i v_i\right)$$

Special Case: Univariate Polynomials

- We have
$$M = \begin{pmatrix} A & v_1 & v_2 & \cdots & v_r \end{pmatrix}$$
where $A \in \mathbb{F}[x]^{s \times s}$ is invertible and $r = t - s$
- Let $h = (y_1, \ldots, y_s, z_1, \ldots, z_r)$ then
$$A \cdot y = f - \sum_{i=1}^{r} z_i v_i$$
- z_i's are the "free variables" and y_j's are the "pivot variables"
$$y = A^{-1} \cdot (f - \sum_{i=1}^{r} z_i v_i)$$

Special Case: Univariate Polynomials

- We have
$$M = \begin{pmatrix} A & v_1 & v_2 & \cdots & v_r \end{pmatrix}$$
where $A \in \mathbb{F}[x]^{s \times s}$ is invertible and $r = t - s$
- Let $h = (y_1, \ldots, y_s, z_1, \ldots, z_r)$ then
$$A \cdot y = f - \sum_{i=1}^{r} z_i v_i$$
- z_i's are the "free variables" and y_j's are the "pivot variables"
$$y = A^{-1} \cdot (f - \sum_{i=1}^{r} z_i v_i)$$

$\leq (s-1)d$

$(s-1) \times (s-1)$

$\leq (s-1)d$

- By Cramer's rule $A^{-1} = \dfrac{\mathrm{Adj}(A)}{\det(A)}$ $\rightarrow \leq sd$

$\mathrm{Adj}(A)_{ij} = \boxed{A^{ij}}$

ratio of "low degree" polynomials

Special Case: Univariate Polynomials

- We have
$$M = \begin{pmatrix} A & v_1 & v_2 & \cdots & v_r \end{pmatrix}$$
where $A \in \mathbb{F}[x]^{s \times s}$ is invertible and $r = t - s$
- Let $h = (y_1, \ldots, y_s, z_1, \ldots, z_r)$ then
$$A \cdot y = f - \sum_{i=1}^{r} z_i v_i$$
- z_i's are the "free variables" and y_j's are the "pivot variables"
$$y = A^{-1} \cdot (f - \sum_{i=1}^{r} z_i v_i)$$
- By Cramer's rule $A^{-1} = \dfrac{\mathrm{Adj}(A)}{\det(A)}$
- Ratio of polynomials of low degree!

Special Case: Univariate Polynomials

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

$$a = A^{-1}(f - b_1 v_1 - \cdots - b_r v_r) = y + \mathrm{Adj}(A) \cdot (c_1 v_1 + \cdots + c_r v_r)$$

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

$$M\begin{pmatrix} y \\ z \end{pmatrix} = f$$

$$y = A^{-1}\left(f - \sum_{i=1}^{r} v_i z_i\right)$$

$$A^{-1}\left(f - \sum_{i=1}^{r} v_i b_i\right) = \overbrace{A^{-1}\left(f - \sum_{i=1}^{r} v_i z_i\right)}^{y} + \underbrace{\boxed{A^{-1}\det(A)}}_{\mathrm{adj}(A)} \sum_{i=1}^{r} v_i c_i$$

$\leftarrow$ polynomial matrix

Special Case: Univariate Polynomials

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

$$a = A^{-1}(f - b_1 v_1 - \cdots - b_r v_r) = y + \mathrm{Adj}(A) \cdot (c_1 v_1 + \cdots + c_r v_r)$$

  gives another polynomial solution to $M(a, b)^T = f$.
- 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 $< \ell := \deg(A) \leq sd$

$\mathbb{F}[x]$ Euclidean Domain

$$z_i = \det(A) \cdot c_i + \underbrace{b_i}_{\text{remainder}}$$

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

$$\ell := \deg(\det(A)) \leq sd$$

Special Case: Univariate Polynomials

- If $h = (y, z)$ is a *polynomial* solution to $Mh = f$, 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

$$a = A^{-1}(f - b_1 v_1 - \cdots - b_r v_r) = y + \mathrm{Adj}(A) \cdot (c_1 v_1 + \cdots + c_r v_r)$$

  gives another polynomial solution to $M(a, b)^T = f$.
- 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

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

$\deg(y) \leq td$ $\deg(z) \leq td$

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 $\mathbb{F}[x_1, \ldots, x_n] = \underbrace{\mathbb{F}[x_1, \ldots, x_{n-1}]}_{\text{coefficients}}\underbrace{[x_n]}_{\text{variable}}$

General Case

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

not Euclidean domain

- 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 $\mathbb{F}[x_1, \ldots, x_n] = \overbrace{\mathbb{F}[x_1, \ldots, x_{n-1}]}^{R}[x_n]$
- 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)

$R[x]$ not Euclidean domain

$$f(x) = (\underbrace{x^d}_{\text{unit coefficient}} + \text{lower order terms})\, q(x) + r(x)$$

$\deg(r) < d$

$a_D x^D$

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. (use here that $\mathbb{F}$ infinite)

$\alpha_i \in \mathbb{F}$

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 $x_i \leftarrow x_i + \underline{\alpha_i x}_n$, which gives us an isomorphism from $\mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}[x_1, \ldots, x_n]$ preserving degree.
- Since $\det(A) \neq 0$, a generic linear map as above will make

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

$$\det(A) = \sum_{\sigma \in S_n} (-1)^{\sigma} \cdot \prod_{i=1}^{n} a_{i\sigma(i)}(x_1, \ldots, x_n) = \sum_{|\bar{\beta}| \leq \ell} a_{\bar{\beta}} \cdot \bar{x}^{\bar{\beta}}$$

$$\det(A) = \sum_{|\beta| \le \ell} a_\beta \cdot \prod_{i=1}^{n} (x_i)^{\beta_i}$$

$$\widehat{\det(A)} = \sum_{|\beta| \le \ell} a_\beta x_n^{\beta_n} \prod_{i=1}^{n-1} (x_i + \alpha_i x_n)^{\beta_i}$$

$$= \sum_{|\beta| \le \ell} \left(a_\beta \cdot \prod_{i=1}^{n-1} \alpha_i^{\beta_i} \cdot x_n^{\beta_1+\beta_2+\cdots+\beta_n} + \text{lower deg terms in } x_n \right)$$

$$= \underbrace{\sum_{|\beta| = \ell} \left(a_\beta \prod_{i=1}^{n-1} \alpha_i^{\beta_i} \right)}_{\neq 0 \,\in\, \mathbb{F}} \cdot x_n^{\ell} + \text{lower deg in } x_n$$

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 $\deg_n(h_i) \leq t \cdot d$

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 $\boxed{\deg_n(h_i) \leq t \cdot d}$
- But that reduces to the following linear system of equations!

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

$$f_i = g_{i1} h_1 + \cdot + g_{it} h_t$$

$$f_{im} x_n^m = H_m^{(n)} [g_{i1} h_1 + \cdots + g_{it} h_t]$$

hom. components of deg m (variable x_n)

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 $\leq d$

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 $\deg_n(h_i) < t \cdot d$
- 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

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

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

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

- Thus our recursion becomes

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

Recursion

$$D(n,d,t) \leq D\left(n-1, \underline{d}, \underline{\frac{(td)^2}{d}}\right) + td$$

$$\leq D\left(n-2, d, \left(\frac{(td)^2}{d}\right)^2 d\right) + \frac{(td)^2}{d} \cdot d + td$$

$$= D\left(n-2, d, \frac{(td)^{2^2}}{d}\right) + (td)^2 + (td)$$

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

$$\Longrightarrow \quad (td)^{2^n}$$

$\square$

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 $\sigma_i\sigma_j = \sigma_j\sigma_i$

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 $\Sigma = \{\sigma_1, \dots, \sigma_r\}$, 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 $\alpha = \beta$?

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 $\sigma_i \sigma_j = \sigma_j \sigma_i$ $\quad x^\alpha - x^\beta \in (S)$ $\quad \gamma = \delta \in S$
- **Input:** two words $\alpha, \beta \in \Sigma^*$ $\quad \bar{x}^\gamma - \bar{x}^\delta$
- **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 $\quad \gamma = (\gamma_1, .., \gamma_n) = \sigma_1^{\gamma_1} .. \sigma_n^{\gamma_n}$

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

Conclusion

- Different algorithm for Ideal Membership Problem and its analysis
- Reduced it to linear system solving!
- Saw degree bounds for the Ideal Membership Problem
- Would be interesting to see an analysis of the Groebner basis algorithm – in case anyone wants to learn and teach it
- EXPSPACE territory

- what are natural problems encoding other complexity classes?
- Can we have a finer-grained complexity theory of AG-problems?

Acknowledgement

- Lecture based entirely on the book by CLO: Ideals, varieties and algorithms (see course webpage for a copy - or get online version through UW library)