Topics in Complexity Theory 11 March, 2015

Lec. 13: Monomial Ordering

Lecturer: Neeraj Kayal *Scribe: Vineet Nair*

In this lecture we introduce the concept of monomial ordering and look at problems where it is useful.

Idea: Say we have two univariate polynomials:

$$f(x) = \alpha_0 + \alpha_1 x + ... + \alpha_d x^d$$

$$g(x) = \beta_0 + \beta_1 x + ... + \beta_e x^e$$

$$f(x)g(x) = \alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)x + ... + \alpha_d\beta_e x^{d+e}$$

Claim 13.0.1. *Given two univariate polynomials f and g of degree d and e respectively as above, the polynomial fg has degree d+e.*

Proof. We order the monomials in a univariate polynomial as follows: $x^i > x^j$ if $i > j$. x^i is the leading monomial in a polynomial h, if x^i is greater than all other monomials in h. It is easy to see that, f is a degree d polynomial iff the leading monomial in f is x^d. If the leading monomial in h_1 and h_2 is x^i and x^j then the leading monomial in h_1h_2 is $x^i.x^j = x^{i+j}$. Hence the leading monomial in fg is x^{d+e}. Hence degree of fg is d+e. $\square$

We wish to generalize the monomial ordering concept used in the above proof for univariate polynomials to multivariate monomials. Frome here on X represents the set of variables $X = \{x_1, x_2, ..., x_n\}$,$\overline{\alpha}$ represents the vector $(\alpha_1, \alpha_2, ..., \alpha_n)$ and $X^{\underline{\alpha}}$ represents the monomial $x_1^{\alpha_1}x_2^{\alpha_2}...x_n^{\alpha_n}$. We want to establish a variable ordering such that the following holds.

1. For any two monomials $X^{\underline{\alpha}}$ and $X^{\underline{\beta}}$ either $X^{\underline{\alpha}} > X^{\underline{\beta}}$ or $X^{\underline{\alpha}} < X^{\underline{\beta}}$.
2. For all α and β, $X^{\underline{\alpha}}X^{\underline{\beta}} > X^{\underline{\alpha}}$.
3. For any monomial $X^{\underline{\alpha}}$, there are a finite number of monomials samller than it, i.e $\{m : X^{\underline{\alpha}} > m\}$ is finite.

Examples of variable ordering

1. Pure lexicographic ordering:

In this the variables are ordered as $x_1 > x_2 > ... > x_n$ and for any two degree vectors $\overline{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n)$ and $\overline{\beta} = (\beta_1, \beta_2, ..., \beta_n)$ where $\overline{\alpha} \neq \overline{\beta}$
for $\alpha_1 \neq \beta_1$ and $\alpha_1 > \beta_1 \Rightarrow X^{\underline{\alpha}} > X^{\underline{\beta}}$
else for $\alpha_2 \neq \beta_1$ and $\alpha_2 > \beta_2 \Rightarrow X^{\underline{\alpha}} > X^{\underline{\beta}}$
.
.
.

else for $\alpha_n \neq \beta_n$ and $\alpha_n > \beta_n \Rightarrow X^{\underline{\alpha}} > X^{\underline{\beta}}$

2. Graded lexicographic ordering

For any two degree vectors $\overline{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n)$ and $\overline{\beta} = (\beta_1, \beta_2, ..., \beta_n)$ where $\overline{\alpha} \neq \overline{\beta}$

if $\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$ then $X^{\underline{\alpha}} > X^{\underline{\beta}}$

else if $\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$ then use pure lexicographic ordering to order $X^{\underline{\alpha}}, X^{\underline{\beta}}$.

Leading Monomial and Trailing Monomial:

Given

$$f = \sum_{\overline{\alpha} \in \mathbb{Z}^n} a_{\overline{\alpha}} X^{\overline{\alpha}}$$

we say a monomial $X^{\overline{\alpha}}$ is the leading monomial of f, represented as LM(f) if for all $X^{\overline{\beta}} > X^{\overline{\alpha}}$, $a_{\overline{\beta}} = 0$. Similarly we can define the trailing monomial of f, represented as TM(f) if for all $X^{\overline{\beta}} < X^{\overline{\alpha}}$, $a_{\overline{\beta}} = 0$.

Claim 13.0.2. *Given two multivariate polynomials f and g, LM(fg)=LM(f)LM(g).*

Proof. Say for contradiction LM(fg)$\neq$LM(f)LM(g). Let $X^{\overline{\alpha}}$ and $X^{\overline{\beta}}$ be the leading monomial of LM(f) and LM(g) respectively. Let LM(fg)=$X^{\overline{\alpha_1}}X^{\overline{\beta_1}}$ where $X^{\overline{\alpha_1}}$ and $X^{\overline{\beta_1}}$ are monomials in f and g respectively. Hence either $X^{\overline{\alpha_1}} < X^{\overline{\alpha}}$ or $X^{\overline{\beta_1}} < X^{\overline{\beta}}$. W.l.o.g assume $X^{\overline{\alpha_1}} < X^{\overline{\alpha}}$. This implies $\overline{\alpha_1} < \overline{\alpha}$ (since the ordering is implicitly on the degree vectors). Since $X^{\overline{\alpha_1}}X^{\overline{\beta_1}}$ is the leading monomial, $\overline{\alpha_1} + \overline{\beta_1} > \overline{\alpha} + \overline{\beta}$. But $X^{\overline{\alpha}}$ and $X^{\overline{\beta}}$ are the leading monomials of LM(f) and LM(g) respectively, hence $\overline{\alpha} + \overline{\beta} > \overline{\alpha_1} + \overline{\beta_1}$. Thus we get a contradiction. □

We will see a couple of examples where we can use monomial ordering to solve the problem.

1. Show that the monomial x^2y^3 cannot be expressed as a power of any polynomial, i.e $x^2y^3 \neq f^e$ where f is polynomial and $e \neq 1$.

Say for contradiction $x^2y^3 = f^e$. This implies LM(x^2y^3)=LM(f^e)=LM(f)^e. Thus $x^2y^3 = x^{em}y^{en}$. Since gcd(2,3)=1 we have $e = 1$, $m = 2$ and $y = 3$. Hence a contradiction. This method also extends to show $x^2y^3 + \alpha_t x^2y^2 + ... + \alpha_0 x_0$ is not power of any polynomial.

2.Suppose we have two multivariate polynomials $f(\underline{X})$ and $g(\underline{X})$ where $\underline{X} = \{x_1, x_2, ..., x_n\}$ and we need to determine whether $f(\underline{X})$ and $g(\underline{X})$ have a common root.

Observe that if $f(\underline{X})$ and $g(\underline{X})$ have a common root then deg(gcd($f(\underline{X}), g(\underline{X})$)) > 0. Hence we perform euclids algorithm on $f(\underline{X})$ and $g(\underline{X})$ to determine their gcd. Suppose deg($f(\underline{X})$)) $>$ deg($g(\underline{X})$). We divide $f(\underline{X})$ by $g(\underline{X})$. Say we get

$$f(\underline{X}) = g(\underline{X})q(\underline{X}) + r(\underline{X})$$

where $q(\underline{X})$ and $r(\underline{X})$ are the qoutient and remainder polynomials respectively. We know $\gcd(f(\underline{X}), g(\underline{X}))$ $= \gcd(g(\underline{X}), r(\underline{X}))$. In multivariate case we need to determine which of the polynomials $g(\underline{X})$ or $r(\underline{X})$ is smaller to continue the recursion. $r(\underline{X})$ is smaller than $g(\underline{X})$ iff $\mathrm{LM}(r(\underline{X})) < \mathrm{LM}(g(\underline{X}))$.