Advanced Coding Theory and Cryptography

Notes by: Alex Pellegrini

Contents

Chapter 1

An introduction to Gröbner bases

Theorem 2.1.10 (Hilbert's Basis Theorem)

Proof. We proceed by induction on the number of variables. Let $I \subset A[X]$ be an ideal not finitely generated, we may assume it can be constructed by an infinite sequence $(f_i)_{i \in \mathbb{N}}$ of independent polynomials of minimal degree. "Independent" means that $f_i \in I \setminus J_i$ where we set $J_i :=< f_0, \dots, f_{i-1} >$. Now let $a_i := lc(f_i)$ be the leading coefficient of f_i and consider $J := a_0, a_1, \dots \subset A$. We know that J can be a basis for an ideal in A but since A is a Noetherian ring we have that there exists a finite basis for such ideal, say $J =< a_1, \dots, a_N >$. We claim that $I =< f_1, \dots, f_N >=: I'$.
Suppose by contrary that this is not true then take a polynomial $f_{N+1} \ni$, we want to show that it is a linear combination of elements of I':

$$a_{N+1} = u_1 a_1 + u_2 a_2 + \cdots + u_N a_N$$

Consider

$$g := \sum_{i=1}^{N} u_i f_i x^{deg(f_{N+1}) - deg(f_i)} \in I'$$

it has the same degree and same leading coefficient as f_{N+1}. Now $f_{N+1} - g \notin I'$ and has degree strictly less than f_{N+1} contraddicting its minimality. Therefore $f_{N+1} - g$ must be 0 and $f_{N+1} \in I'$.

The induction follows since we can consider $A[X_1, \dots, X_m] = A'[X_m]$ where $A' := [X_1, \dots, X_{m-1}]$ which we know is a Noetherian ring. □

Lemma 2.1.13 (Dickson's Lemma)

Proof. We proceed by induction on the number of variable, by first proving the case with one variable. So we are considering $\mathcal{M} = \{X_1^\alpha | \alpha \in \mathbb{N}\}$, and

$T \subset \mathcal{M}$ a semigroup ideal. Since every $t_i \in T$ is of the form $t = X_1^{\alpha_i}$ we consider $\beta = \min\{\alpha_i | X_1^{\alpha_i} \in T\}$. We claim that $T =< X_1^{\beta} >$. Indeed let $t_j \in T$ then it is of the form $t_j = X_1^{\alpha_j}$ so $\frac{t_j}{t_i} = X_1^{\alpha_j - \beta}$ is well defined where $\alpha_j - \beta > 0$ by minimality of β. We can take $\gamma = \alpha_j - \beta$ hence:

$$t_j = X_1^{\beta} \cdot X_1^{\gamma} \in < X_1^{\beta} >= T$$

We prove the more general case so let be $m \in \mathbb{N}$ arbitrary and assume the lemma proved for $m-1$.
Let $T \subset \mathcal{M} = \{X_1^{a_1} \cdots X_m^{a_m} \mid (a_1, \ldots, a_m) \in \mathbb{N}^m\}$. Consider also the projection map $\pi(X_1^{a_1} \cdots X_m^{a_m}) = X_1^{a_1} \cdots X_{m-1}^{a_{m-1}}$. By induction hypothesis $\pi(T)$ is a finitely generated semigroup ideal so we can find a basis, say $\pi(T) =< t_1, \ldots, t_k >$. Now let:

$$A_i := \min\{a_m \mid X_m^{a_m} | t, t \in T, \pi(t) = t_i\} \quad \forall i = 1, \ldots, k$$

and furthermore

$$A := \min\{a_m \mid X_m^{a_m} \in T\}$$

We claim that $T =< t_1 X_m^{A_1}, \ldots, t_k X_m^{A_k}, X_m^{A} >$ which is a finite set.
So pick an arbitrary $t \in T$ so $t = \pi(t) X_m^{a_{m_t}}$ for some $a_{m_t} \in \mathbb{N}$, we know that $\exists t_i$ such that $\pi(t) = s \cdot t_i$, therefore $t = s \cdot t_i \cdot X_m^{a_{m_t}}$ and by minimality of A_i we obtain that for:

$$t = s \cdot t_i \cdot X_m^{a_{m_t}} = s \cdot t_i \cdot X_m^{A_i} \cdot X_m^{\gamma}$$

for $\gamma = a_{m_t} - A_i$. Now $\forall t \in T$ we have proved that $t \in < t_i \cdot X_m^{A_i} >$ which is contained in $< t_1 X_m^{A_1}, \ldots, t_k X_m^{A_k}, X_m^{A} >$ □

Theorem 2.1.14

Proof. $\Rightarrow$ Let $f \in I$ then we can write:

$$f = \sum_{i=1}^{k} f_i \cdot p_i = f_1 \cdot p_1 + f_2 \cdot p_2 + \ldots + f_k \cdot p_k, \ f_i \in \mathcal{P}$$

So evaluating $f(A)$ means to evaluate every p_i so:

$$f(A) = f_1 \cdot p_1(A) + f_2 \cdot p_2(A) + \ldots + f_k \cdot p_k(A) =$$

$$= f_1 \cdot 0 + f_2 \cdot 0 + \cdots + f_k \cdot 0 = 0$$

$\Leftarrow$ Trivial by setting $f = p_i \ \forall i = 1, \ldots, k$

□