Advanced Robotics

Lecture 9

pajdla@cmp.felk.cvut.cz

Theorem A: Let $G = \{g_1, \dots, g_t\}$ be the Groebner basis constructed by the Buchberger algorithm from polynomials $\{f_1, \dots, f_s\} \in \mathbb{C}[x_1, \dots, x_n]$. Then $V(\{f_1, \dots, f_s\}) = V(\{g_1, \dots, g_t\})$.

Proof: $=$ means $\subseteq$ and $\supseteq$

$\supseteq$: $a \in V(G) \Rightarrow g_i(a) = 0,\ i = 1, \dots, t \Rightarrow f_1(a) = g_1(a) = 0, \dots, f_s(a) = g_s(a) = 0$

$\subseteq$: $a \in V(\{f_1, \dots, f_s\}) \Rightarrow a \in V(G)$. By induction over the order in which are $g \in G$ generated.

1) $g_1, \dots, g_s = f_1, \dots, f_s \Rightarrow g_1(a) = \dots = g_s(a) = 0$

2) Let us show that the following implication holds for every m

$g_1, \dots, g_{m-1} = 0 \Rightarrow g_m = 0$

$g_m = \overline{S(g_k, g_l)}^{(g_1, \dots, g_{m-1})} \Rightarrow S(g_k, g_l) = b_1 g_1 + \dots + b_t g_{m-1} + g_m$

$$(c_1 g_k + c_2 g_l)(a) = (b_1 g_1 + \dots + b_t g_{m-1})(a) + g_m(a)$$

$$0 = 0 + g_m(a)$$

Theorem 1: Let $f_i \in \mathbb{C}[x_1, \dots, x_n]$, $i = 1, \dots, s$. If the equations $f_i(x_1, \dots, x_n) = 0$ $i = 1, \dots, s$ have a finite number of solutions, then $I(\{f_1, \dots, f_s\})$ contains polynomials in one variable $h_j \in \mathbb{C}[x_j]$, $j = 1, \dots, n$.

Proof: Let $\{(a_1^{(m)}, \dots, a_n^{(m)})\}_{m=1,\dots,M}$ be the set of the solutions. Define

$$g_j(x_j) = (x_j - a_j^{(1)})(x_j - a_j^{(2)}) \cdots (x_j - a_j^{(M)}) \quad , \quad j = 1, \dots, n$$

Notice that $g_j(x) \in I(V(\{f_1, \dots, f_s\}))$ since for all m holds

$$g_j((a_1^{(m)}, a_2^{(m)}, \dots, a_n^{(m)})) = (a_j^{(m)} - a_j^{(1)}) \cdots (a_j^{(m)} - a_j^{(2)}) \cdots \underbrace{(a_j^{(m)} - a_j^{(m)})}_{=0} \cdots (a_j^{(m)} - a_j^{(M)}) = 0$$

It follows from the Hilbert Nullstellensatz that there is $k \geq 1$ such that $g_j^k(x_j) \in I(\{f_1, \dots, f_s\})$.

Hilbert's Nullstellensatz

Let k be an algebraically closed field (e.g. $\mathbb{C}$).
If $f, f_1, \dots, f_s \in k[x_1, \dots, x_n]$ are such that
$f \in I(V(\{f_1, \dots, f_s\}))$, then there exists
an integer $m \geq 1$ such that

$$f^m \in I(\{f_1, \dots, f_s\})$$

(and conversely).

Proof: CLO page 170

Theorem 2 Let $f_i \in \mathbb{C}[x_1, \dots, x_n]$, $i = 1, \dots, s$ and let G be a Groebner basis computed from $\{f_1, \dots, f_s\}$ by the Buchberger algorithm. If the equations $f_i(x_1, \dots, x_n) = 0$ $\quad i = 1, \dots, s$ have a finite number of solutions, then for every $i \in 1, \dots, n$ there is $g \in G$ and $k \geq 0$ such that

$$LM(g) = x_i^k.$$

Proof:

It follows from Theorem 1 that for every $i \in 1, \dots, n$, there is $f \in I(\{f_1, \dots, f_s\})$ such that $f \in \mathbb{C}[x_i]$. Polynomial f is generated by $\{f_1, \dots, f_s\}$, and therefore there are polynomials h_i such that $f = \sum_{i=1}^{s} h_i f_i$. G is computed from $\{f_1, \dots, f_s\}$ and thus $f_i \in G$. There holds $\overline{f}^{G} = 0$. Therefore there must be $g \in G$ such that $LT(g)$ divides $LT(f) \in \mathbb{C}[x_i]$. That is possible only if $LT(g) \in \mathbb{C}[x_i]$, i.e., $LT(g) = x_i^k$, $k \geq 0$.

Theorem 3: Let G be a Groebner basis constructed by the Buchberger algorithm w.r.t. $x_1 >_{lex} \cdots >_{lex} x_n$ from polynomials $\{f_1, \ldots, f_s\} \in \mathbb{C}[x_1, \ldots, x_n]$ for which equations $\{f_i = 0\}_{i=1,\ldots,s}$ have a finite number of solutions. Then G contains a polynomial $g \in \mathbb{C}[x_n]$.

Proof:

It follows from Theorem 2 that there is $g \in G$ such that $LM_{>_{lex}}(g) \in \mathbb{C}[x_n]$. Any other monomial of g is strictly smaller than $LM(g)$. Therefore it cannot contain any other variable than x_n.