CS5760: Topics in Cryptanalysis **7 July 2025**

Lecture 11: Gröbner Bases over Rings

Instructor: Maria Francis *Scribe: Gautam Singh*

11.1 Gröbner Bases over Principal Ideal Domains (PIDs)

Here, we consider the univariate polynomial ring $\mathbb{Z}(x)$. The ordering in $\mathbb{Z}$ is $a_1 < a_2$ if $|a_1| < |a_2|$ or if $|a_1| = |a_2|$ and a_1 is negative.

Definition 11.1 (Reduction)**.** We say that $f \xrightarrow{g} h$ if $\mathrm{lm}(g) \mid \mathrm{lm}(f)$ and $\exists a, b \in \mathbb{Z}$ such that $\mathrm{lc}(f) = a\mathrm{lc}(g) + b$ where $a \neq 0$ and $b < \mathrm{lc}(f)$.

11.2 Strong and Weak Gröbner Basis

Definition 11.2 (Strong Gröbner Basis)**.** A set of polynomials $G = (g_1, \dots, g_t)$ is a *strong Gröbner basis* for an ideal I if for any $f \in I \setminus \{0\}$, $\exists a, g \in G$ such that $\mathrm{lt}(g) \mid \mathrm{lt}(f)$.

To construct a strong Gröbner basis, we required to construct a G-polynomial in addition to an S-polynomial.

Definition 11.3 (S/G-Polynomial)**.** Let $f, g \in R[x]$. WLOG let $\mathrm{lc}(f) < \mathrm{lc}(g)$. Let $t = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$. Define

$$t_f = \frac{t}{\mathrm{lm}(f)}, \quad t_g = \frac{t}{\mathrm{lm}(g)}. \tag{11.1}$$

Similarly, let $a = \mathrm{lcm}(\mathrm{lc}(f), \mathrm{lc}(g))$. Define

$$a_f = \frac{a}{\mathrm{lc}(f)}, \quad a_g = \frac{a}{\mathrm{lc}(g)}. \tag{11.2}$$

Then, the S polynomial of f and g is defined as

$$S(f, g) = a_f t_f f - a_g t_g g. \tag{11.3}$$

Let $b = \gcd(\mathrm{lc}(f), \mathrm{lc}(g))$. Then, by the Extended Euclidean algorithm, we have $b = b_f \mathrm{lc}(f) + b_g \mathrm{lc}(g)$ for some b_f, b_g. Then, the G-polynomial of f and g is given by

$$G(f, g) = b_f t_f f - b_g t_g g. \tag{11.4}$$

Definition 11.4 (S/G-Pairs)**.** Let $\{f_1, \dots, f_m\}$ be the set R^m. Let $\alpha, \beta \in R^m$. We assume that $\mathrm{lc}(\bar{\alpha}) < \mathrm{lc}(\bar{\beta})$. Let $t = \mathrm{lcm}(\mathrm{lm}(\bar{\alpha}), \mathrm{lm}(\bar{\beta}))$. Define

$$t_\alpha = \frac{t}{\mathrm{lm}(\bar{\alpha})}, \quad t_\beta = \frac{t}{\mathrm{lm}(\bar{\beta})}. \tag{11.5}$$

Let $a = \mathrm{lcm}(\mathrm{lc}(\bar{\alpha}), \mathrm{lc}(\bar{\beta}))$. Define

$$a_\alpha = \frac{a}{\mathrm{lc}(\bar{\alpha})}, \quad a_\beta = \frac{a}{\mathrm{lc}(\bar{\beta})}. \tag{11.6}$$

Then, the S-pair of α and β is defined as

$$\mathrm{Spair}(\alpha, \beta) = a_\alpha t_\alpha \alpha - a_\beta t_\beta \beta. \tag{11.7}$$

Let $b = \gcd(\mathrm{lc}(\bar{\alpha}), \mathrm{lc}(\bar{\beta}))$. Then, the G-pair of α and β is defined as

$$\mathrm{Gpair}(\alpha, \beta) = b t_\alpha \alpha - b t_\beta \beta. \tag{11.8}$$

Definition 11.5 (S-Reduction)**.** Let $\alpha, \beta \in R^m$. We say that β s-reduces to α if $\bar{\beta}$ reduces $\bar{\alpha}$ and $\mathrm{Sig}(\alpha) > \mathrm{Sig}(\beta)$ where $\mathrm{lc}(\bar{\alpha}) = a\mathrm{lc}(\bar{\beta}) + b$ for some $a, b \in R$ where $a \neq 0$ and $b < \mathrm{lc}(\bar{\alpha})$.