CS5760: Topics in Cryptanalysis **3 July 2025**

Lecture 10: Signatures and Gröbner Bases

Instructor: Maria Francis *Scribe: Gautam Singh*

10.1 F5 Algorithm

The F5 algorithm proposed by Faugere in 2002 ensures no zero reduction will happen for *regular sequences* of polynomials $\langle f_1, \ldots, f_s \rangle$ in a polynomial ring $k[x_1, \ldots, x_n]$. Eder proposed an algorithm to lift this seuqence of polynomials to a module $k[x_1, \ldots, x_n]^s$.

10.2 Notations

Suppose R is a polynomial ring over a field k in n variables. Define R^m to be a free R-module with standard basis $e_1, \ldots, e_m$. Any polynomial of R^m can be written as $f = \sum_{i=1}^{m} f_i e_i$ where $f_i \in R$. Modules can be thought to be the ring counterparts of vector spaces, that is, the coefficients are polynomials instead of field elements. As a corollary, a module may or may not have a basis. A *free module* has a basis.

All the module elements $\alpha \in R^m$ can be uniquely written as a finite sum $\alpha = \sum_{ae_i \in \mathcal{N}} ae_i$ where $a \in R$ and $\mathcal{N}$ is a minimal set. The ae_i's are called *module terms*.

In a module, two orderings are required: one for R and the other for R^m. The orderings should be compatible, that is, if $a \leq b$ in R then $ae_i \leq be_i$ in R^m.

If $\alpha = \sum_{i=1}^{m} a_i e_i$ is a module element with $a_i \in R$, then we can define the homomorphism $\alpha \mapsto \bar{\alpha}$ where $\bar{\alpha} = \sum_{i=1}^{m} a_i f_i$. An element α is called a *syzygy* if $\bar{\alpha} = 0$. The module of all syzygies of $f_1, \ldots f_s$ is denoted by $\mathrm{Sy}(f_1, \ldots, f_s)$.

10.3 Signatures

The signature of $\alpha \in R^m$ is defined as the leading term of α with respect to the ordering on R^m. For $\alpha \in R^m$, we define the *sig-poly* pair of α as $(S(\alpha), \bar{\alpha}) \in R^m \times R$. Over fields, $\alpha, \beta \in R^m$ are equal up to sig-poly pairs if $S(\alpha) = S(k\beta)$ and $\bar{\alpha} = k\bar{\beta}$ for some field element $k \neq 0$.

A typical module monomial ordering is as follows. Assume a monomial order $<$ on R and let ae_i, be_j be two module monomials in R^m. The *POT ordering* gives priority to position over the term. Here, $ae_i < be_j$ iff $i < j$ or $i = j$ and $a < b$. The *TOP ordering* gives priority to the term over the position. Here, $ae_i < be_j$ iff $a < b$ or $a = b$ and $i < j$.

10.4 Signature Reduction

Definition 10.1. Let $\alpha \in R^m$ and t be a term in $\bar{\alpha}$. Then, we can *s-reduce* t by $\beta \in R^m$ if

1. There exists a monomial b such that $\mathrm{lt}(\bar{b\beta}) = t$.
2. $S(b\beta) < S(\alpha)$.

We insist that $S(b\beta) < S(\alpha)$ since an equality can result in cancelling the signatures or leading terms. This is called a *signature drop*.

Lemma 10.1. *Let $\alpha, \beta \in R^m$ and $\mathcal{G}$ be a signature Gröbner basis upto a signature $S(\alpha) = S(\beta)$. If α and β are s-reduced, then either $\mathrm{lt}(\bar{\alpha}) = \mathrm{lt}(\bar{\beta})$ or $\bar{\alpha} = \bar{\beta} = 0$.*

Lemma 10.2 (Singular Criterion)**.** *For any signature T we need to handle exactly one $a\alpha \in R^m$ from $\mathcal{G}$ such that $S(a\alpha) = T$.*