R. Holtkamp, Berkeley

Gröbner bases of noncommutative power series

(with L. Gerritzen: Indag. Mathem.,N.S.9(4),1998)

K: commutative field, X: finite ordered set

noncommutative Gröbner bases
$\to$ Bergman, Bokut,Shirshov, Buchberger-Mora algorithm ... (ideals in $K\langle X\rangle$)

for ideals in $K[[X]]$: Becker-Weispfennig, Alonso-Mora-Raimondo,...

$K\langle\langle X\rangle\rangle$: (topological) K–algebra of power series in non–commuting variables from X
Elements: $f = \sum_{w\in W} c_w w$, coefficients $c_w \in K$, $W = W(X)$ monoid of words or monomials over X

The minimal element $\mu(f)$ of $supp(f) = \{w \in W : c_w \neq 0\}$ with respect to the degree–lexicographical ordering is called the initial or leading monomial of f; $c(f) := c_{\mu(f)}$.
For $n \in \mathbb{N}$ the two–sided ideal generated by all words $w \in W(X)$ of length n is denoted by J^n; $J = J^1$.

$K\langle\langle X\rangle\rangle$ is provided with the J–adic topology. For any $a \in K\langle\langle X\rangle\rangle$, a basis of neighborhoods of a for the J–adic topology is given by $\{J^n + a : n \in I\!N\}$.
Let p_n be the projection $K\langle\langle X\rangle\rangle \to K\langle\langle X\rangle\rangle / J^n$.
A subset $\Phi \subset K\langle\langle X\rangle\rangle$ of linearly independent elements is called J–adic basis of $K\langle\langle X\rangle\rangle$, if for all $n \in I\!N$ the set $\big\{\varphi \in \Phi : p_n(\varphi) \neq 0\big\}$ generates a K–vector subspace of $K\langle\langle X\rangle\rangle$ which is a complement of J^n in $K\langle\langle X\rangle\rangle$.
$W = W(X)$ is a J–adic basis of $K\langle\langle X\rangle\rangle$.

Remark. Ideals generated by single elements are almost never closed, e.g. the ideal generated by y in $K\langle\langle x, y\rangle\rangle$ is not closed.

Let X be a set and V a subset of the monoid $W = W(X)$ of words over X.

$M(V)$: the set of non–multiple words a in V (i.e. $a \notin WbW$ for all $a \neq b \in V$).
$M(V) = M(WVW)$ is the unique minimal set which generates WVW as a two–sided ideal in W; it is called the minimal ideal generator of WVW.
$M_r(V)$: the set of non–rightmultiple words in V.
The set $M_r(V) = M_r(VW)$ is called the minimal right ideal generator of VW.

Gröbner bases

Let I be a closed ideal in $K\langle\langle X\rangle\rangle$.

Proposition (reduced Gröbner basis G_I of I).
There is a unique subset $G_I \subset I$ such that
(i) $\mu(G_I) = M\big(\mu(I)\big)$
(ii) $supp(g) \subset \{\mu(g)\} \cup \big(W - \mu(I)\big)$ *for all* $g \in G_I$
(iii) g *is normed, i.e.* $c(g) = 1$ *for all* $g \in G_I$

Let $F \subset K\langle\langle X\rangle\rangle$ and $\Gamma \subset F$ be simple (with respect to leading monomials), i.e.
(i) $\mu(\Gamma) = M\big(\mu(\Gamma)\big)$
(ii) The restriction $\mu|\Gamma : \Gamma \to W(X)$ is injective.
We assume $\mu(\Gamma) = M\big(\mu(F)\big)$.

Criterion.
(The reduced simple system of) Γ *is the (reduced) Gröbner basis of the closed ideal* $I(F)$ *generated by* F*, if* $\Upsilon_\Gamma\big(F \cup D'(\Gamma)\big) = 0$*, where* $D'(\Gamma)$ *is the set of* S*-series (definition follows) and* Υ_Γ *the reduction operator induced by* Γ *(definition follows).*

S-series and Overlaps
(typical for nc Gröbner bases case):

$M_r\big(W\mu(\Gamma)\big) = \{b \cdot m : b \in W - W\mu(\Gamma)W, m \in \mu(\Gamma)$ and there is no $a = (a_0, a_1, a_2), a_i \in W - \{1\}$ such that $b \in Wa_0$, $a_0a_1 \in \mu(\Gamma)$, $a_1a_2 = m \in \mu(\Gamma)\}$.

$D(V) := \big\{a = (a_0, a_1, a_2) : a_0a_1, a_1a_2 \in M(V)$, $a_i \in W - \{1\}\big\}$ is called the set of overlaps of $V \subset W$.

For any pair (a, f), where $a = (a_0, a_1, a_2) \in D\big(\mu(\Gamma)\big)$ and $f = (f_1, f_2) \in \Gamma \times \Gamma$ with $\mu(f_1) = a_0a_1, \mu(f_2) = a_1a_2$, let $h(a, f) := c(f_1)a_0f_2 - c(f_2)f_1a_2$ and denote by $D'(\Gamma)$ the set of all $h(a, f)$ (S–series).

Example.
Let $X = \{x, y\}, y < x$ and let $k \in I\!N, k \geq 3$.
The equation $y^2 = x^k$ in $K\langle x, y\rangle$ can be viewed as the equation of a noncommutative Neil parabola.
The same equation $f = 0, f = y^2 - x^k$, generates an ideal $I(f) \in K\langle\langle x, y\rangle\rangle$.
We have $\mu(f) = y^2$. The set of overlaps $D(y^2)$ is $\{(y, y, y)\}$.
We compute the S-series $h = (y^2 - x^k)y - y(y^2 - x^k) = yx^k - x^ky$. Now $\Upsilon_{\{f\}}(h) = h \neq 0$.
$\{f\}$ is not a Gröbner basis of $I(f)$.

Proposition (reduction operator induced by Γ, typical for the nc power series case).

For Γ simple, let $g : \mu(\Gamma) \to \Gamma$ be the inverse map of the bijective map $\mu|\Gamma : \Gamma \to \mu(\Gamma)$ and let

$P(\Gamma) := \big\{ bg(v)w : bv \in M_r\big(W\mu(\Gamma)\big), w \in W \big\}.$

Then there is a unique continuous K–linear projection operator $\Upsilon_\Gamma : K\langle\langle X\rangle\rangle \to K\langle\langle X\rangle\rangle$ with

(i) $Ker(\Upsilon_\Gamma)$ is the closed K–subspace generated by $P(\Gamma)$

(ii) $Im(\Upsilon_\Gamma)$ is the closed K–subspace generated by $W - W\mu(\Gamma)W$

It holds: $\mu\big(\Upsilon_\Gamma(f)\big) \geq \mu(f)$ and

$$\Upsilon_\Gamma(f_1 f_2) = \Upsilon_\Gamma\big(\Upsilon_\Gamma(f_1) f_2\big) \text{ for } f_1, f_2 \in K\langle\langle X\rangle\rangle$$

For every simple subset Γ of $K\langle\langle X\rangle\rangle - \{0\}$, we get the reduced simple system $\tilde{\Gamma}$ associated to Γ (normed, simple, $\mu(\tilde{\Gamma}) = \mu(\Gamma)$, $\Upsilon_{\tilde{\Gamma}} = \Upsilon_\Gamma$ and $supp(h) \subset \{\mu(h)\} \cup \big(W - W\mu(\tilde{\Gamma})W\big)$ for all $h \in \tilde{\Gamma}$).

Sketch of Proof (Proposition): For Γ simple, $\Phi(\Gamma) = P(\Gamma) \cup \big(W - W\mu(\Gamma)W\big)$ is a J–adic basis of $K\langle\langle X\rangle\rangle$.

Procedure and Applications

We sketch a procedure which computes for any given system $F \subset K\langle\langle X\rangle\rangle$ the reduced Gröbner basis G_F (a system of bilinear combinations $\sum_{i=1}^{r} h_i f_i h_i'$ with $f_i \in F,\ h_i, h_i' \in K\langle\langle X\rangle\rangle$) of the closed two–sided ideal $I = I(F)$ generated by F in $K\langle\langle X\rangle\rangle$:

We compute the reduced Gröbner basis G_n of $I + J^n$ (step by step). Assume that G_n has been computed.
Let $G_n' = \{g \in G_n : deg(\mu(g)) \leq n-1\}$.
It is easy to find a lifting $\Gamma_n = \{\hat{g} : g \in G_n'\}$ of G_n' into I, i.e. $\Gamma_n \subset I$ simple and $\mu(\Gamma_n) = \mu(G_n')$.

For $f \in F$, we have $\Upsilon_{\Gamma_n}(f) \equiv 0 \bmod J^n$. For $h \in D'(G_n)$, also $\Upsilon_{\Gamma_n}(h) \equiv 0 \bmod J^n$.
There is a unique $q_n(f) \in K\langle\langle X\rangle\rangle$ with $supp\big(q_n(f)\big) \subset \{w \in W : deg(w) = n\}$ such that $\Upsilon_{\Gamma_n}(f) - q_n(f) \in J^{n+1}$ and there is a unique $t_n(h) \in K\langle\langle X\rangle\rangle$ with $supp\big(t_n(h)\big) \subset \{w \in W : deg(w) = n\}$ such that $\Upsilon_{\Gamma_n}(h) - t_n(h) \in J^{n+1}$.
"Adding" all $q_n(f), t_n(h)$ to the set Γ_n, we get $G_{n+1}^{(')}$.

To obtain G_F, we look at $\bigcup_{n=1}^{\infty} \mu(G_n')$.

Example.
Let $X = \{x, y\}, y < x$ and let $k \in I\!N, k \geq 3$. Let $f = y^2 - x^k$, see above: We note that $\{y^2 - x^k\} \cup \big\{w \in W - Wy^2W : deg(w) = n+1\big\}$ is a Gröbner basis of $I + J^{n+1}$ for $n \leq k$ only.

Proposition.

(i) *For all $k \geq 3$, a Gröbner basis for $I(x^k - y^2)$ in $K\langle\langle x, y\rangle\rangle$ is given by $G_I = \{y^2 - x^k, yx^k - x^k y\}$ and a J–adic K–basis of $\hat{A} := K\langle\langle x, y\rangle\rangle / I(x^k - y^2)$ is given by*
$B := W - W\mu(G_I)W = \Big\{x^\tau \big(\prod_{i=1}^m yx^{\varepsilon_i}\big) y^\sigma : 0 \leq \sigma \leq 1, 0 \leq \tau, 0 \leq m, 1 \leq \varepsilon_i \leq k-1\Big\}.$

(ii) *$A_{poly} := K\langle x, y\rangle / I(x^k - y^2)$ canonically embeds into $\hat{A}$.*

Example. Let $X = \{x, y\}, y < x$.
If $F = \{f\}$ and f is homogeneous then the algorithm to determine the reduced Gröbner basis of $I(F)$ in $K\langle\langle x, y\rangle\rangle$ with $y < x$ coincides with the Buchberger–Mora algorithm for ideals in the free algebra $K\langle x, y\rangle$ with $x < y$. For example, if $f = y^2 - xy$, we get an infinite Gröbner basis $\{yx^n y - xy^{n+1} : n \in I\!N\}$ (compare [Ufnarovski]).

Proposition. *Let* $\Gamma \subset K\langle\langle X\rangle\rangle - \{0\}$ *be simple (and without units). We define* $H := \{g \in \tilde{\Gamma} : ord(g) = 1\}$, $X' = X - \mu(H)$ *and denote by* Γ' *the subset of* $K\langle\langle X'\rangle\rangle$ *consisting of all* $f \in \tilde{\Gamma} - H$.
Then $K\langle\langle X\rangle\rangle/I(\Gamma) \cong K\langle\langle X'\rangle\rangle/I(\Gamma')$.

Lemma.
A Gröbner basis of $(1-x)^{-1}\big(K\langle x,y\rangle/I(y^2-x^3)\big) := K\langle x,y,t\rangle/I\big(y^2-x^3,\ 1-t(1-x), 1-(1-x)t\big)$ *is given by* $\{x^3-y^2,\ y^2x-xy^2,\ tx-t+1,\ xt-t+1,\ ty^2+x^2+x+1-t,\ y^2t+x^2+x+1-t\}$.

Proposition. $(1-x)^{-1}K\langle x,y\rangle/I(x^3-y^2)$ *canonically embeds into* $K\langle\langle x,y\rangle\rangle/I(y^2-x^3)$.
(Here $t \mapsto \sum_{m=0}^{\infty} x^m$*).*