Prime ideals and Non Commutative Gröbner Bases

José Gómez-Torrecillas
University of Granada

Alden-Biesen, September 2th., 2003
Some observations

• Many quantized algebras are iterated Ore extensions $k[x_1][x_2; \sigma_2, \delta_2] \cdots [x_n; \sigma_n, \delta_n]$

• Prime ideals are of current interest in Quantized Algebras (and in iterated differential operators algebras).

• Algorithmic structures based on Gröbner bases are available for noncommutative solvable polynomial rings [Kandri/Weispfenning:1990].

• How to exploit these computational skills to decide whether a given ideal is completely prime?

• There is a commutative primality test [Gianni/alt:], as a guide.


**Basic definitions**

- $T = A[x; \sigma, \delta]$ an Ore extension of an algebra $A$:
  - The powers $x^n \ n \geq 0$ form a left $A$–basis of $T$.
  - $xr = \sigma(r)x + \delta(r)$ (where $\sigma$ is an automorphism of $A$, $\delta$ is a $\sigma$–derivation).

- Let $I \triangleleft A[x; \sigma, \delta]$ be a (twosided) ideal. If $I \cap A$ is $\sigma$–stable (i.e. $\sigma(I \cap A) \subseteq I \cap A$) then we have an algebra map
  $$
  \pi : A[x; \sigma, \delta] \longrightarrow \frac{A}{I \cap A}[x; \sigma, \delta]
  $$
  $$
  ax^n \mapsto \overline{a}x^n,
  $$
  where $\overline{a} = a + I \cap A$.

- The ideal $I \triangleleft T$ is *completely prime* if $T/I$ is a domain.
A characterization of complete primeness

Proposition. Let $A$ be a noetherian domain and let $I$ be a two-sided ideal of $A[x; \sigma, \delta]$ with the property that $I \cap A$ is $\sigma$-stable. The following assertions are equivalent:

(i) $I$ is completely prime;

(ii) (1) $I \cap A$ is completely prime in $A$;

(2) with $S = A/(I \cap A)$, $Q$ the field of fractions of $S$, and $J = \pi(I)$ the image of $I$ in $S[x; \sigma, \delta]$,

(a) the generator $p$ of $Q[x; \sigma, \delta]J$ is irreducible in the euclidean domain $Q[x; \sigma, \delta]$;

(b) $Q[x; \sigma, \delta]J \cap S[x; \sigma, \delta] = J$. 

The INPUT is: generators $f_1, \ldots, f_s$ for an ideal $I$ of $R = k[x_1][x_2; \sigma_2, \delta_2] \cdots [x_n; \sigma_n, \delta_n]$.

The OUTPUT is: TRUE ($I$ is completely prime); FALSE ($I$ is not completely prime); NOT APPLY (the procedure does not apply to $I$).

1. Set $i = 0$, $R_0 = k$, $\sigma_1 = id$, $\delta_1 = 0$;

2. Set $R_{i+1} = R_i[x_{i+1}; \sigma_{i+1}, \delta_{i+1}]$, $I_i = I \cap R_i$;

3. If $\sigma_{i+1}(I_i) \notin I_i$, then return NOT APPLY and go to END;

4. Set $S_i = R_i/I_i$, $Q_i = Q_{cl}(S_i)$,
   $I_{i+1} = I \cap R_{i+1}$ and $J_{i+1} = \pi(I_{i+1})$;
5 Compute a generator $p_{i+1}$ for $Q_i[x_{i+1}; \sigma_{i+1}, \delta_{i+1}]J_{i+1}$;

6 If $p_{i+1} \neq 0$ and reducible in $Q_i[x_{i+1}; \sigma_{i+1}, \delta_{i+1}]$, then return FALSE and go to END;

7 Compute $\overline{J}_{i+1} =$ $Q_i[x_{i+1}; \sigma_{i+1}, \delta_{i+1}]J_{i+1} \cap S_i[x_{i+1}; \sigma_{i+1}, \delta_{i+1}]$;

8 If $\overline{J}_{i+1} \neq J_{i+1}$, then return FALSE and go to END;

9 Set $i = i + 1$, if $i = n$, then return TRUE, and go to END, else go to 2;

10 END.


Required Gröbner Bases Toolkit

We look for algorithms founded on Non-Commutative Gröbner Bases which allow the effective implementation of our primality test. The requirements of each step of the procedure are the following

2 Set $R_{i+1} = R_i[x_{i+1}, \sigma_{i+1}, \delta_{i+1}], I_i = I \cap R_i$;

Our non-commutative setting should include iterated Ore extensions (or at least a large class of them)

We should be able to do elimination of variables.

3 If $\sigma_{i+1}(I_i) \notin I_i$, then ...

We will need to solve the ideal membership problem. A Multivariable Division Algorithm is pertinent here for the computation of normal forms (or remainders) w.r.t. Gröbner Bases
4 Set $S_i = R_i/I_i$, $Q_i = Q_{cl}(S_i)$, $I_{i+1} = I \cap R_{i+1}$ and $J_{i+1} = \pi(I_{i+1})$;

5 Compute a generator $p_{i+1}$ for $Q_i[x_{i+1}; \sigma_{i+1}, \delta_{i+1}]J_{i+1}$

To handle effectively the projections $\pi(I_{i+1})$, and to compute the generators $p_{i+1}$, we need elimination of variables. Concretely, if $G$ is a Gröbner basis for $I$, then $G \cap R_i$ should be a Gröbner basis of $I_i$ for every $i$.

In this way, $p_{i+1} = \pi(g_{i+1})$, where $g_{i+1}$ is the element in $G_{i+1} \setminus G_i$ with minimal degree w.r.t. $x_{i+1}$. 
6 If \( p_{i+1} \neq 0 \) and reducible in \( Q_i[x_{i+1}; \sigma_{i+1}, \delta_{i+1}] \), then return FALSE and go to END;

This is the hardest step, as you need to check whether an one-variable invariant polynomial over a noncommutative skew polynomial ring is irreducible. No general method is known. Thus, our primality test reduces the problem of primality of ideals to the problem of irreducibility of one-variable invariant polynomials.

In any case, computing with left fractions in \( Q_i \) needs to handle effectively left Ore condition on \( S_i = R_i/I_i \). This requires the computation of Gröbner bases for left modules of syzygies.
7. Compute $\overline{J}_{i+1} = Q_i[x_{i+1}; \sigma_{i+1}, \delta_{i+1}]J_{i+1} \cap S_i[x_{i+1}; \sigma_{i+1}, \delta_{i+1}]$.

Here, one first computes

$$r_{i+1} = \sigma_{i+1}^{-\deg(g_{i+1})}(\text{lcc}(g_{i+1})),$$

where $\deg(g_{i+1})$ (resp. $\text{lcc}(g_{i+1})$) denotes the degree (resp. the leading coefficient) of $g_{i+1}$ with respect to $x_{i+1}$.

The intersection is shown to be equal to $\overline{J}_{i+1} = \pi(L_{i+1} \cap R_{i+1})$, where

$$L_{i+1} = R_{i+1}[y]I_{i+1} + R_{i+1}[y](1 - r_{i+1}y),$$

for $y$ a new commuting variable.
If $J_{i+1} \neq J_{i+1}$, then return FALSE & go to END;

But this is just to check that

$$I_{i+1} \subseteq L_{i+1} \cap R_{i+1},$$

which requires, again, elimination of variables, and to solve the membership problem.

In resume, we need to recognize our iterated Ore extensions within a class of algebras with a good notion of Gröbner basis, enjoying the following algorithmic structures:

- A Multivariable Division Algorithm
- Buchberger’s Algorithm for computing of left and twosided Gröbner bases
- Elimination of variables
- Modules of Syzygies and Gröbner bases for modules
Basic algorithms for solvable polynomial rings

Solvable polynomial rings were first introduced by [ElFrom:1983], and Gröbner bases over them by [Kandri/Weispfenning:1990]. The basic algorithms we need in our Primality Test appeared for the first time as follows:

- **A Multivariable Division Algorithm**

- **Buchberger’s Algorithms for one and twosided ideals** [Kandri/Weispfenning:1990]

- **Elimination of variables** [Kredel:1992]

- **Modules of Syzygies and Gröbner bases for modules** [Kredel:1992]


Our Primality Test works in the following setting:

- \( R \) an iterated Ore extension
  \[ R_0 \subset R_1 \subset \cdots \subset R_n = R, \]

where

- \( R_0 = k \) is a field (or \( R_0 = k \) a division ring)
- \( R_1 = k[x_1] \) is a polynomial algebra (or \( R_1 = k[x_1; \sigma_1, \delta_1] \), an Ore extension)
- \( R_{i+1} = R_i[x_{i+1}; \sigma_{i+1}, \delta_{i+1}] \).

All \( \sigma_i \)'s are assumed to be automorphisms.

Assume for every \( 1 \leq i < j \leq n \) there is \( 0 \neq q_{ji} \in k \) such that

\[ \sigma_j(x_i) - q_{ji}x_i = s_{ji} \in R_{i-1}. \]

This is just to say that \( R \) is a solvable polynomial ring with respect to the lexicographical order with \( x_1 <_{\text{lex}} \cdots <_{\text{lex}} x_n \).
Primality Test

Given generators $f_1, \ldots, f_m$ of a two-sided ideal $I$ of $R$, we proceed as follows.

1.- Compute a Gröbner basis $G$ for $I$, then $G_i = G \cap R_i$ is a Gröbner basis for $I_i = I \cap R_i$, for $i = 0, \ldots, n$.
2.- Set $i = 0$.
3.- If $\text{rem}(\sigma_{i+1}(g), G_i) \neq 0$ for some $g \in G_i$, then the test does not apply for $I$.
4.- If $G_{i+1} \setminus G_i$ is not empty, then pick $g_{i+1} \in G_{i+1} \setminus G_i$ with minimal degree in $x_{i+1}$. If $g_{i+1}$ is reducible in $Q_i[x_{i+1}; \sigma_{i+1}, \delta_{i+1}]$, then $I$ is not completely prime.
5.- Compute $r_{i+1} = \sigma_{i+1}^{-m}(c)$, where $c = \text{lc}_{x_{i+1}}(g_{i+1})$, $m = \text{deg}_{x_{i+1}}(g_{i+1})$.
6.- Compute a Gröbner $\Gamma_{i+1}$ basis in $R_{i+1}[y]$ for the left ideal $L_{i+1}$ generated by $G_{i+1} \cup \{1 - r_{i+1}y\}$.
7.- If $\text{rem}(g, G_{i+1}) \neq 0$ for some $g \in \Gamma_{i+1} \cap R_{i+1}$, then $I$ is not completely prime.
8.- If $i + 1 = n$, then $I$ is completely prime.
9.- Set $i = i + 1$ and go to 3.
Two special cases When some of the contractions $I_i$ is not $\sigma_{i+1}$–stable, then the test does not apply. There are two special cases where this unpleasant contingency does not appear.

Iterated differential operators algebras (including enveloping algebras of solvable Lie algebras), which are of the form

$$k[x_1][x_2; \delta_2] \cdots [x_n; \delta_n].$$

Affine quantum spaces (i.e., coordinate rings of affine quantum spaces), which are of the form $R = k[x_1][x_2; \sigma_2] \cdots [x_n; \sigma_n]$, where $\sigma_j(x_i) = q_{ji}x_i$.

For ideals $I$ such that $I \cap \{x_1, \ldots, x_n\} = \emptyset$, if $I_i$ is not $\sigma_{i+1}$–stable for some $i$, then $I$ is not completely prime, so the test applies for $I$.

If $I \cap \{x_1, \ldots, x_n\} \neq \emptyset$, then, factoring out $R$ by the ideal generated by the variables contained in $I$, we are in the former case.
An example

Let $R$ be the algebra over $k$ generated by $x, y, z, t$ with relations

\begin{align*}
    yx &= xy \quad zy = yz + x \\
    zx &= xz \quad ty = yt + y \quad ; \\
    tx &= xt \quad tz = zt - z
\end{align*}

which is the iterated Ore extension

$$R = k[x, y][z; \delta][t; \theta],$$

with $\delta(x) = 0, \delta(y) = x, \theta(x) = 0, \theta(y) = y, \theta(z) = -z.$

Let $I$ be the twosided ideal generated by $x^2 + y^2 + z^2 + t^2 + 1$. A Gröbner basis of $I$ is $G = \{x, y, z, t^2 + 1\}$.

$I_2 = \langle x, y \rangle$ is (completely) prime in $k[x, y]$; $Q_2 = S_2 = k$.

$I_3 = \langle x, y, z \rangle$, $g_3 = z$ which is irreducible in $Q_2[z; \delta]$. Moreover, $\Gamma_3 = \{x, y, z, 1-u\}$, where
$u$ is a commuting variable. Thus, $\Gamma_3 \cap R_3 = G_3$, and $I_3$ is c.p.

$S_3 = Q_3 = k$ and $t^2 + 1$ is irreducible iff $\sqrt{-1} \notin k$. Moreover $\Gamma_4 = \{x, y, z, 1 + t^2, 1 - u\}$, for $u$ commuting. Thus, $\Gamma_4 \cap R_4 = G_4$, and $I$ is completely prime if and only if $\sqrt{-1} \notin k$.

**Note:** The computations of the Gröbner bases has been done with the package [Greuel/alt:2003]

PBW rings and solvable polynomial rings

By $\mathbb{N}^n$ we will denote the free abelian monoid with generators $\varepsilon_1, \ldots, \varepsilon_n$. The elements of $\mathbb{N}^n$ will be $n$–tuples $\alpha = (\alpha_1, \ldots, \alpha_n)$ of non-negative integers, and the sum is defined componentwise.

Let $x_1, \ldots, x_n$ be elements of a ring $R$ which contains a division ring $k$. The elements of the form $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ are called standard terms.

**Definition.** The ring $R$ is said to be left polynomial (over $k$ in $x_1, \ldots, x_n$) if the set $\{x^\alpha; \alpha \in \mathbb{N}^n\}$ is a basis of $R$ as a left $k$–vectorspace.

This means that every element $f$ of $R$ has a unique standard representation

$$f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha.$$  

For $0 \neq f \in R$, define the Newton diagram of $f$ as

$$\mathcal{N}(f) = \{\alpha \in \mathbb{N}^n; c_\alpha \neq 0\}.$$
Let \( \preceq \) be an *admissible order* on \( \mathbb{N}^n \), namely, a total monoid order with \( 0 \prec \alpha \) for every \( \alpha \in \mathbb{N}^n \).

The *exponent* of \( f \) is defined by

\[
\exp(f) = \max_{\preceq} N(f).
\]

The standard representation of any \( f \in R \) thus becomes

\[
f = c_{\exp(f)}x^{\exp(f)} + \sum_{\alpha \prec \exp(f)} c_{\alpha}x^{\alpha}.
\]

**Observation:** The well-known algorithmic structures based on Gröbner bases over commutative polynomial ring would be adapted whenever \( \exp(fg) = \exp(f) + \exp(g) \) for \( f, g \in R \). This is what happens for solvable polynomial rings.
**Left PBW rings**

**Theorem.** [Bueso/alt:2001b] Let $R$ be a left polynomial ring over $k$ in $x_1, \ldots, x_n$. The following statements are equivalent for an admissible order $\preceq$ on $\mathbb{N}^n$:

(i) $\exp(fg) = \exp(f) + \exp(g)$ for every $f, g \in R$;

(ii) (a) for every $1 \leq i < j \leq n$ there exist $0 \neq q_{ji} \in k$ and $p_{ji} \in R$ with $\exp(p_{ji}) \prec \exp(x_i x_j)$ such that $x_j x_i = q_{ji} x_i x_j + p_{ji}$;

(b) for every $1 \leq i \leq n$ and every $0 \neq a \in k$ there exists $0 \neq q_{ai} \in k$ and $p_{ai} \in R$ with $\exp(p_{ai}) \prec \exp(x_i)$ such that $x_i a = q_{ia} x_i + p_{ai}$.

We then say that $R$ is a left PWB ring. All basic algorithms work over them [Bueso/alt:2001b, Bueso/alt:2003].


Solvable polynomial rings are left PWB

The “relations” in a left PBW ring are of the type

\[(PWB1) \ x_jx_i = q_{ji}x_ix_j + p_{ji} \text{ with } 0 \neq q_{ji} \in k, \exp(p_{ji}) \prec \exp(x_ix_j);\]

\[(PBW2) \ x_ia = q_{ai}x_i + p_{ai} \text{ (}0 \neq a \in k\text{)} \text{ with } 0 \neq q_{ai} \in k, \exp(p_{ai}) \prec \exp(x_i).\]

When \(p_{ai} \in k\) we obtain Solvable Polynomial Rings \([Kredel:1992]\).

When \(k\) is commutative and it is contained in the center of \(R\) (and, so, \(q_{ai} = a, p_{ai} = 0\)) we obtain Solvable Polynomial Algebras \([Kandri/Weispfenning:1990]\).

**Example** Let \(R = k[t][x; \delta], \text{ where } k = \mathbb{C}(u), \delta(u) = tu, \delta(t) = 1.\)

\[
\begin{align*}
x t & = tx + 1 \\
t r(u) & = r(u)t & (r(u) \in \mathbb{C}(u)) \\
x r(u) & = r(u)x + ur'(u)t & (r(u) \in \mathbb{C}(u))
\end{align*}
\]

For any ordering with \((1,0) \prec (0,1), \text{ we have } \exp(ur'(u)t) = (1,0) \prec (0,1) = \exp(x) \text{ or, shortly, if } t \prec x \text{ then } ur'(u)t \prec x, \text{ } R \text{ is a left PBW ring but not a solvable polynomial ring, as } ur'(u)t \notin k.\]
Solvable polynomial algebras and filtrations.
The following result locates solvable polynomial algebras within the class of (positively) filtered algebras.

**Theorem.** [Bueso/alt:2001c] The following conditions are equivalent for an associative and unitary algebra $R$ over a field $k$.

(i) $R$ is a filtered algebra whose associated graded algebra is an $n$–dimensional (graded) quantum affine space;

(ii) $R$ is a solvable polynomial algebra with respect to some admissible ordering on $\mathbb{N}^n$;

(iii) $R$ is a filtered algebra with a finite-dimensional filtration whose associated graded algebra is an $n$–dimensional (graded) quantum affine space.

From filtrations to solvable polynomial algebras

Let $R$ be a filtered $k$–algebra with a quantum affine space as associated graded algebra $\text{gr}(R)$. Thus $R$ is endowed with an ascending chain $FR = \{F_nR \mid n \geq 0\}$ of vector subspaces, the filtration of $R$, satisfying for all $n, m \geq 0$

1. $1 \in F_0R$,
2. $(F_nR)(F_mR) \subseteq F_{n+m}R$,
3. $R = \bigcup_{n \geq 0} F_nR$,

in such a way that

$$\text{gr}(R) = \bigoplus_{n \geq 0} F_nR/F_{n-1}R,$$

is generated by homogeneous elements $y_1, \ldots, y_n$ subject to the relations $y_jy_i = q_{ji}y_iy_j$, where $0 \neq q_{ji} \in k$ for $1 \leq i < j \leq n$. 

Let $u_i = \deg y_i$ and chose $x_1, \ldots, x_n \in R$ are such that $x_i = y_i + F_{u_i-1}R$ for $1 \leq i \leq n$ then

$$F_sR = \sum_{|\alpha|_u \leq s} k x^\alpha,$$

where $u = (u_1, \ldots, u_n)$ and $|\alpha|_u = u_1 \alpha_1 + \cdots + u_n \alpha_n$.

Thus, the algebra $R$ is a solvable polynomial algebra with relations

$$Q \equiv x_j x_i = q_{ji} x_i x_j + p_{ji} \quad \text{with} \quad \exp(p_{ji}) <_u \epsilon_i + \epsilon_j$$

Then admissible ordering $\preceq_u$ is given by

\[
\alpha \preceq_u \beta \iff \begin{cases} 
|\alpha|_u < |\beta|_u \\
\text{or} \\
|\alpha|_u = |\beta|_u \text{ and } \alpha \preceq_{\text{lex}} \beta
\end{cases}
\]

where $\preceq_{\text{lex}}$ denotes the lexicographical order with $\epsilon_1 <_{\text{lex}} \cdots <_{\text{lex}} \epsilon_n$. 
A criterion of solvability. Let us now consider an algebra $R$ with generators $x_1, \ldots, x_n$ and relations

$$Q = \{ x_j x_i = q_{ji} x_i x_j + p_{ji}, \ 1 \leq i < j \leq n \},$$

for some standard polynomials $p_{ji}$. Define

$$C_{ji} = \mathcal{N}(p_{ji}) - \epsilon_i - \epsilon_j,$$

and the finite subset $C_Q$ of $\mathbb{Z}^n$

$$C_Q = \bigcup_{1 \leq i < j \leq n} C_{ji} \cup \{-\epsilon_1, \ldots, -\epsilon_n\}$$

Let us also define the (open) polyhedron

$$\Phi_Q = \{ w \in \mathbb{R}^n_+ : \langle w, \gamma \rangle < 0 \ \forall \ \gamma \in C_Q \}$$

**Theorem.** There is an admissible order $\prec$ on $\mathbb{N}^n$ such that $\exp(p_{ji}) \prec \exp(x_i x_j)$ for every $1 \leq i < j \leq n$ if and only if $\Phi_Q$ is not empty. In such a case, $\Phi_Q$ contains vectors with strictly positive integer components.
Filtering solvable polynomial algebras. The following result shows how to find a finite-dimensional filtration with a quantum affine space as associated graded algebra on any solvable polynomial algebra.

**Theorem.** Let $R$ be a solvable polynomial algebra with relations

$$Q = \left\{ x_j x_i = q_{ji} x_i x_j + p_{ji}, \ 1 \leq i < j \leq n \right\},$$

such that $\exp(p_{ji}) \prec \exp(x_i x_j)$ for some admissible ordering $\preceq$. Let $w = (w_1, \ldots, w_n) \in \Phi_Q$ with strictly positive components. Then $R$ is filtered by finite dimensional vector subspaces $F_n(R) = \sum_{|\alpha| w \leq n} kx^\alpha$, and the associated graded algebra $\text{gr}(R)$ is an $n$–dimensional quantum space.
Ring theoretical properties of solvable polynomial algebras So, the class of solvable polynomial algebras coincides with the class of positively filtered algebras (by finite-dimensional vector spaces, if desired) with quantum affine spaces as associated graded algebras. Combining results by J. E. Björk, E. K. Ekström, A. K. Fields, JGT, T.H. Lenagan, T. Levasseur, J. McConnell, J.C. Robson, A. Roy, P. Tauvel (other combinations could also work) we have:

**Theorem.** Let $R$ be a solvable polynomial algebra. Then
1. $R$ is a noetherian domain.
2. The Gelfand-Kirillov dimension is exact on short exact sequences of f.g. $R$–modules.
3. $R$ is left and right partitive w.r.t. the GK dimension.
4. The Krull dimension of a f.g. module is bounded by the G.K. dimension.
5. $R$ satisfies the Nullstellensatz.
6. $R$ has finite global dimension.
7. $R$ is Auslander-Regular.
8. $R$ is Cohen-Macaulay w.r.t. GK dimension.