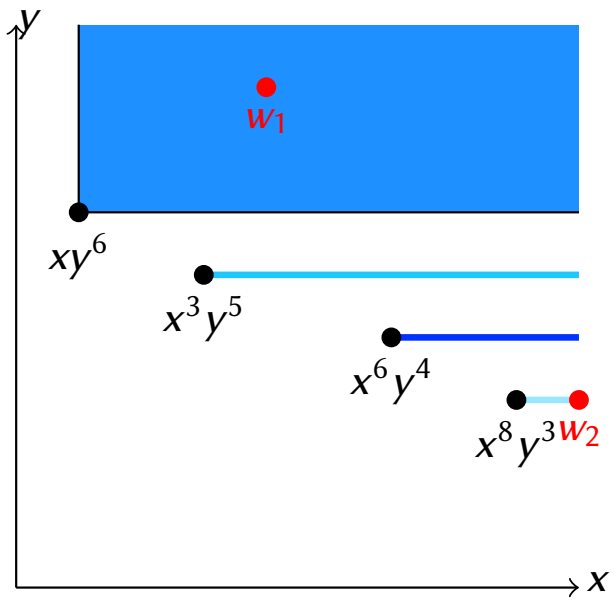
Do It Yourself:
Buchberger and Janet Bases over effective rings
Part 3: What happens to involutive bases?

Michela Ceria & Teo Mora

ICMS 2020

Involutive divisions and bases

- **Janet**: preliminary version of Buchberger Theory for polynomials over a field;
- **Gerdt-Blinkov**: *involutive divisions/bases* for efficiently compute Groebner bases.
- **Seiler**: involutive bases, toward solvable polynomial rings and distinction strong/weak involutive bases.



$F = \{f_1, \ldots, f_4\}$
$T(f_1) = x^8y^3$, $T(f_2) = x^6y^4$,
$T(f_3) = x^3y^5$, $T(f_4) = xy^6$.
Looking at their **cones**:

- w_1: reduced using f_4;
- w_2: reduced using f_1;

What is an involutive division?

1. noetherian rings, s.t. associated graded ring = commutative polynomials over a PIR; terms $\to$ twisted Tamari-Weispfenning multiplication $\Rightarrow$ involutive division over **monomials**;
2. $\mathcal{T}$: commutative terms; $\mathrm{M}(\mathcal{A})$: monomial set.

An **involutive division** Ł on $\mathrm{M}(\mathcal{A})$ is given, if

$\forall U \subset \mathrm{M}(\mathcal{A})$ finite and $\forall u \in U$: submonoid $Ł(u, U) \subseteq \mathrm{M}(\mathcal{A})$ s.t:

(A). If $w \in Ł(u, U)$ and $v|w$, then $v \in Ł(u, U)$.

(B). If $u, v \in U$ and $uŁ(u, U) \cap vŁ(v, U) \neq \emptyset$, then $u \in vŁ(v, U)$ or $v \in uŁ(u, U)$.

(C). If $v \in U$ and $v \in uŁ(u, U)$, then $Ł(v, U) \subseteq Ł(u, U)$.

(D). If $V \subseteq U$, then $Ł(u, U) \subseteq Ł(u, V)$ for all $u \in V$.

Things do not commute: the cone uŁ(u,U)

$u = c_u\tau_u \in U, c_u \in R \setminus \{0\}, \tau_u \in \mathcal{T}$: **how are we multiplying?**

LE: $Ł(u,U) * u = \{c_v\tau_v * u = c_v\alpha_{\tau_v}(c_u)\varpi(\tau_v,\tau_u)\tau_u \circ \tau_v : c_v \in R \setminus \{0\}, \tau_v \in \mathcal{T}\}$,

RI: $u * Ł(u,U) = \{u * c_v\tau_v = c_u\alpha_{\tau_u}(c_v)\varpi(\tau_u,\tau_v)\tau_u \circ \tau_v : c_v \in R \setminus \{0\}, \tau_v \in \mathcal{T}\}$,

RE: $Ł(u,U) \diamond u = \{c_v\tau_v \diamond u = c_v c_u \varpi(\tau_u,\tau_v)\tau_u \circ \tau_v : c_v \in R \setminus \{0\}, \tau_v \in \mathcal{T}\}$.

Multiples, divisors, multiplicativity

1. If $w = c_w\tau_w \in uŁ(u,U)$, $c_w \in R \setminus \{0\}, \tau_w \in \mathcal{T}$: $u|_Ł w$; w **(Ł-)involutive multiple** of u, u **(Ł-)involutive divisor** of w, and the unique monomial $v = c_v\tau_v$ s.t. $w = u * v$ **multiplicative** for u.

2. Involutive division $\to \{x_1,\dots,x_n\} = M_Ł(u,U) \sqcup NM_Ł(u,U)$: **multiplicative/non-multiplicative variables**.

Partition of variables $\to$ Involutive division if (B)-(D) satisfied for

$Ł(u,U) = \{cx_1^{h_1}\cdots x_n^{h_n} | c \in R\setminus\{0\}, (h_1,\dots,h_n) \in \mathbb{N}^n, x_i \in NM_Ł(u,U) \Rightarrow h_i = 0\}$

3. Multiplicative variables for polynomials = for leading monomials.

What questions we want to answer?

1. How to prove in the PIR case that **locally involutive implies involutive?**
2. How to extend **completion** - again - to the PIR case?
3. How to reformulate in our setting the algorithm by Seiler for computing **weak involutive bases**?

Completeness ... and how to find it

assume to be over a field

Given an involutive division Ł, $U \subset \mathrm{M}(\mathcal{A})$ is **involutive** (or **complete** with respect to Ł or Ł−involutive or Ł−complete) if

$$\cup_{u\in U}\, u\,\mathrm{M}(\mathcal{A}) = \cup_{u\in U}\, u\,\mathbf{Ł}(u, U)\,.$$

Ups... we are over a PIR!

$$\mathcal{N} := \cup_{u\in U}\, u\,\mathrm{M}(\mathcal{A}) \subset \mathbb{I}_2(U) \cap \mathrm{M}(\mathcal{A}) = \mathit{Span}_R\{\mathcal{N}\} \cap \mathrm{M}(\mathcal{A})$$

the equality being granted only if R is a field.

Solution

Force each element $u = c_u\tau_u \in U$, $c_u \in R \setminus \{0\}$, $\tau_u \in \mathcal{T}$, to satisfy

$$\mathbb{I}_2(c_u) = \mathcal{I}_{\tau_u} = \{Lc(f) : f \in \mathbb{I}_2(U), \mathbf{T}(f) = \tau_u\} \cup \{0\} \subset R.$$

What does "locally involutive" mean?

Prolongation:

Multiplication of $u \in U$ by a variable x_i: *multiplicative* / *non-multiplicative*.

Local involutivity

$U \subset \mathrm{M}(\mathcal{A})$ is **locally involutive** w.r.t. Ł if any non-multiplicative prolongation of any element in U has an involutive divisor in U:

$$\forall u \in U, \forall x_i \in NM_{\mathbf{Ł}}(u, U) \exists v \in U : v|_{\mathbf{Ł}}(u \cdot x_i).$$

Continuity is crucial!

Continuity

A division Ł is called **continuous** if $\forall U \subset \mathrm{M}(\mathcal{A})$ finite, the inequality $u_i \neq u_j, i \neq j$ holds for any finite sequence $u_1, \ldots u_k$ of elements in U s.t.

$$\forall i < k \exists x_j \in NM_{\text{Ł}}(u_i, U)) \textbf{ s.t. } u_{i+1}|_{\text{Ł}} u_i \cdot x_j.$$

Continuity is crucial!

Continuity

A division Ł is called **continuous** if $\forall U \subset \mathrm{M}(\mathcal{A})$ finite, the inequality $u_i \neq u_j, i \neq j$ holds for any finite sequence $u_1, \ldots u_k$ of elements in U s.t.

$$\forall i < k \exists x_j \in NM_{\mathbf{Ł}}(u_i, U)) \textbf{ s.t. } u_{i+1}|_{\mathbf{Ł}} u_i \cdot x_j.$$

local involutivity $\Rightarrow$ involutivity

If an involutive division Ł is continuous then local involutivity of any set U implies involutivity:

$$\mathcal{N} = \cup_{u \in U} u\, \mathrm{M}(\mathcal{A}) = \cup_{u \in U} u\, \mathbf{Ł}(u, U).$$

Local involutivity $\Rightarrow$ involutivity

For every $u = c_u\tau_u \in U, c_u \in R \setminus \{0\}, \tau_u \in \mathcal{T}$ and $v = c_v\tau_v \in \mathrm{M}(\mathcal{A}), c_v \in R \setminus \{0\}, \tau_v \in \mathcal{T}$ we show that there is $m = c_m\tau_m \in U, c_m \in R \setminus \{0\}, \tau_m \in \mathcal{T}$ such that

$$m|_{\text{Ł}}\, u * v = c_u\alpha_{\tau_u}(c_v)\varpi(\tau_u,\tau_v)\tau_u \circ \tau_v =: t = c_t\tau_t,$$
$$\textbf{with } \tau_t = \tau_u \circ \tau_v \textbf{ and } c_t = c_u\alpha_{\tau_u}(c_v)\varpi(\tau_u,\tau_v).$$

If $u|_{\text{Ł}}\, u * v$ we are done.

Local involutivity $\Rightarrow$ involutivity

$m|_{\text{Ł}}\, u * v = c_u \alpha_{\tau_u}(c_v)\varpi(\tau_u, \tau_v)\tau_u \circ \tau_v =: t = c_t \tau_t$, **with** $\tau_t = \tau_u \circ \tau_v$ **and** $c_t = c_u \alpha_{\tau_u}(c_v)\varpi(\tau_u, \tau_v)$.

Otherwise, since $c_u \mid c_t$, $\exists x_{k_1} \in NM_{\text{Ł}}(u, U)$ s.t. $x_{k_1} | \tau_v \xrightarrow{\text{loc. invol.}} u \cdot x_{k_1}$ has involutive divisor $w_1 = c_{w_1}\tau_{w_1} \in U$.
Note that $u * x_{k_1} = c_u \varpi(\tau_u, x_{k_1}) u \circ x_{k_1}$ and that

$$\tau_u * \tau_v = \tau_u * \left(x_{k_1} * \frac{\tau_v}{x_{k_1}} \right) = (\tau_u * x_{k_1}) * \frac{\tau_v}{x_{k_1}} \implies$$

$$\varpi(\tau_u, \tau_v) = \varpi(\tau_u, x_{k_1}) \varpi\left(\tau_u * x_{k_1}, \frac{\tau_v}{x_{k_1}} \right)$$

so that $c_{w_1} \mid c_u \varpi(\tau_u, x_{k_1}) \mid c_u \alpha_{\tau_u}(c_v)\varpi(\tau_u, \tau_v) = c_t$.

Local involutivity $\Rightarrow$ involutivity

$m|_{Ł} u * v = c_u \alpha_{\tau_u}(c_v)\varpi(\tau_u, \tau_v)\tau_u \circ \tau_v =: t = c_t \tau_t$, **with** $\tau_t = \tau_u \circ \tau_v$ **and** $c_t = c_u \alpha_{\tau_u}(c_v)\varpi(\tau_u, \tau_v)$.

Thus either $w_1|_{Ł}(u * v)$ and we are done, or there are $x_{k_2} \in NM_{Ł}(w_1, U)$ and $w_2 = c_2\tau_{w_2} \in U$ such that $x_{k_2} \mid \frac{\tau_u \circ \tau_v}{\tau_{w_1}}$ and $v_2|_{Ł}(v_1 \cdot x_{k_2})$.

Going on, we obtain the sequence $u, w_1, w_2, \ldots$ of elements in U satisfying continuity. By construction, each element of the sequence divides $u \circ v$. Since all the elements are distinct and $u \circ v$ has a finite number of distinct divisors, it follows that the above sequence in U is finite, and, hence, it ends up with an involutive divisor of $u * v$.

Completion

An Ł−involutive $\tilde{U} \subseteq \mathsf{M}(\mathcal{A})$ is an Ł−**completion** of $U \subseteq \tilde{U}$ if

$$\mathcal{N} = \cup_{u \in \tilde{U}} u \, \text{Ł}(u, U).$$

Easy to find

- first: $U = \tilde{U}$
- if $\exists u = c_u \tau_u \in \tilde{U}$ and $x \in NM_{\text{Ł}}(u, \tilde{U})$ s.t. $u \cdot x$ has no involutive divisors in $\tilde{U}$
- Choose such u and x with the lowest $\tau_u \circ Z$ w.r.t. $<$:
  $\tilde{U} := \tilde{U} \cup \{u \cdot Z\}$

Weak involutive bases

Let Ł be an involutive division on $\mathrm{M}(\mathcal{A})$, and F a finite set of polynomials. Then:

I. p is **Ł−weak-reducible** mod F if p has a monomial $u = c_u\tau_u \in \mathrm{M}(\mathcal{A})$, $\tau_u \in \mathcal{T}$, $c_u \in R \setminus \{0\}$, s.t. $c_u = \sum_i \mathrm{Lc}(f_i)\alpha_{\mathbf{T}(f_i)}(c_{v_i})\varpi(\mathbf{T}(f_i), \tau_{v_i})$ and $\tau_u = \mathbf{T}(f_i) \circ \tau_{v_i}$ for each i, where $v_i = c_{v_i}\tau_{v_i} \in \text{Ł}(\mathbf{M}(f_i), \mathbf{M}(F))$, $\tau_{v_i} \in \mathcal{T}$, $c_{v_i} \in R \setminus \{0\}$.

II. p is **in Ł−weak-normal form modulo** F if p is not Ł−reducible modulo F.

We denote $wNF_{\text{Ł}}(p, F)$ the weak-normal form of a polynomial p modulo F.

Weak involutive bases

Only an adapting-matter!

Since the definition of normal forms and reduction are a **verbatim reformulation** of the related notions in Buchberger Theory, a weak version can then be easily deduced by a verbatim reformulation of the notions and algorithms of Buchberger Theory

Weak involutive bases

$U \subseteq \mathrm{M}(\mathcal{A})$ is **Ł−autoreduced** if $u\text{Ł}(u, U) \cap v\text{Ł}(v, U) = \emptyset$, $\forall u, v \in U, u \neq v$.
A finite polynomial set F is **Ł−autoreduced** if $\mathbf{M}(F)$ is Ł−autoreduced and every $f \in F$ does not contain monomials involutively multiple of any element in $\mathbf{M}(F)$.

Weak-involutive

An Ł−autoreduced set F is weak-involutive with respect to a continuous weak-involutive division Ł if and only if the following conditions of local involutivity hold

$$wNF(f \cdot x_i, F) = 0 \forall f \in F \textbf{ and } x_i \in NM_{\text{Ł}}(\mathbf{M}(f), \mathbf{M}(F)).$$

Weak-involutive bases

Finally, it is sufficient to directly apply the version of Buchberger Algorithm over effective rings based on Möller Lifting Theorem, to obtain an algorithm for producing an involutive basis; the redundancy removal which in the classical setting is forced by a reformulation of Buchberger Criteria, in this setting is directly granted by Möller Lifting Theorem which subsumed the Gebauer-Möller Criteria.

Strong involutive bases

In the present setting for each element $g_i \in F \subset \mathcal{A}^m$ and each monomail $ct \in \mathrm{M}(\mathcal{A})$ we have

$$\begin{aligned} ct * \mathbf{M}(g_i) &= ct * c_i\tau_i\mathbf{e}_{\iota_i} = c\alpha_t(c_i)\varpi(t,\tau_i)\Upsilon(t,\tau_i)t \circ \tau_i\mathbf{e}_{\iota_i} \text{ and} \\ ct \diamond \mathbf{M}(g_i) &= cc_i\varpi(\tau_i,t)\Upsilon(\tau_i,t)\tau_i t\mathbf{e}_{\iota_i} \end{aligned}$$

Given $g_{j_1}, g_{j_2} \in F \subset \mathcal{A}^m$, even if $\mathbf{e}_{\iota_{j_1}} = \mathbf{e}_{\iota_{j_1}}$ (or $m = 1$), in our setting we do not hope that exists a least common multiple between $\mathbf{M}(g_{j_1})$ and $\mathbf{M}(g_{j_1})$; however as remarked by Wespfenning, if there is a syzygy

$$\mathbf{M}(g_{j_1}) * c_1\upsilon_1 = \mathbf{M}(g_{j_2}) * c_2\upsilon_2$$

among them, then such least common multiple exists and there are terms $\upsilon(j_1,j_2)_{j_1}, \upsilon(j_1,j_2)_{j_2} \in \mathcal{T}$ satisfyng

$$\begin{aligned} &\mathbf{T}(g_{j_1}) \circ \upsilon(j_1,j_2)_{j_1} = \mathbf{T}(g_{j_1}\upsilon(j_1,j_2)_{j_1}) = lcm(\mathbf{T}(g_{j_1}), \mathbf{T}(g_{j_2})) = \\ &\mathbf{T}(g_{j_2})\upsilon(j_1,j_2)_{j_2} = \mathbf{T}(g_{j_2}) \circ \upsilon(j_1,j_2)_{j_2}. \end{aligned}$$

Strong involutive bases: conjecture

Let Ł be a continuous involutive division. A polynomial set

$$F := \{g_1, \ldots, g_u\} \subset \mathcal{A}^m, g_i = \mathbf{M}(g_i) - p_i =: c_i \tau_i \mathbf{e}_{\iota_i} - p_i$$

is strong Ł-involutive if and only if:

- for each $f \in F$ and each non-multiplicative variable $x_i \in NM_{Ł}(\mathbf{M}(f), \mathbf{M}(F))$, the related J-prolongation $J(f, x_i) := f \cdot x_i$, satisfies $sNF(J(f, x_i), F) = 0$;
- for each $g_{j_1}, g_{j_2} \in F$ the related P-prolongation

$$P(g_{j_1}, g_{j_2}) := g_{j_1} \star \alpha^{-1}_{\tau_{j_1}}(s) \upsilon(j_1, j_2)_{j_1} + g_{j_2} \star \alpha^{-1}_{\tau_{j_2}}(t) \upsilon(j_1, j_2)_{j_2},$$

  where s, t are the Bézout values such that
  $sc_{j_1} \varpi(\tau_{j_1}, \upsilon(j_1, j_2)_{j_1}) + tc_{j_2} \varpi(\tau_{j_2}, \upsilon(j_1, j_2)_{j_2}) =$
  $\gcd(c_{j_1} \varpi(\tau_{j_1}, \upsilon(j_1, j_2)_{j_1}), c_{j_2} \varpi(\tau_{j_2}, \upsilon(j_1, j_2)_{j_2}))$
  satisfies $sNF(P(g_{j_1}, g_{j_2}), F) = 0$;
- for each $g_i \in F$ the related A-prolongation $A(g_i) := f_i \alpha^{-1}_T(g_i)(a)$, a being the annihilator of $lc(gi)$, satisfies $sNF(A(g_i), F) = 0$.

Thank you
for your attention!