Weak Involutive bases over effective rings

Michela Ceria and Teo Mora

Abstract. We discuss the problems related with the extension of Janet theory to effectively given rings.

As remarked in 1992 by Schwartz [21], in 1920 after a cohoperation with Hilbert, Janet [11] introduced, under the name of complete/involutive bases both the notion of Gröbner bases and a computational algorithm which essentially anticipated Buchberger's [1, 2] Algorithm[1] (apparently in the strongest formulation given by Moller's Lifting Theorem [14]).
The recent extension of Buchberger Theory and Algorithm on each $\mathcal{R}$-module $\mathcal{A}$ [15, IV.50] [17, 5], where both $\mathcal{R}$ and $\mathcal{A}$ are assumed to be effectively given through their Zacharias representation [16] suggested us to investigate how far Janet's approach can be extended to more exotic settings. Clearly the combinatorial aspects of Janet completion necessarily require at least that, using the terminology of [15, IV.50], the associated graded ring $\mathcal{G}$ of $\mathcal{A}$ is an Ore-like extension [13, 6]; an interesting class of such rings, much wider than solvable polynomial rings [12] on which Seiler [22] applied Janet approach, has been recently proposed [18]: $\mathcal{A} = \mathcal{R}\langle X_1, \ldots, X_n, Y_1, \ldots, Y_m\rangle/\mathcal{I}, \mathcal{I} = \mathbb{I}(G)$ with

$$\begin{aligned} G &= \{X_jX_i - a_{ij}X_iX_j - d_{ij} : 1 \le i < j \le n\} \\ &\cup \{Y_lX_j - b_{jl}\upsilon_{jl}X_jY_l - e_{jl} : 1 \le j \le n, 1 \le l \le m\} \\ &\cup \{Y_kY_l - c_{lk}Y_lY_k - f_{lk} : 1 \le l < k \le m\} \end{aligned}$$

a Gröbner basis of $\mathcal{I}$ with respect to the lexicographical ordering $<$ on $\Gamma := \{X_1^{d_1}\cdots X_n^{d_n}Y_1^{e_1}\cdots Y_m^{e_m} | (d_1, \ldots, d_n, e_1, \ldots, e_m) \in \mathbb{N}^{n+m}\}$ induced by $X_1 < \ldots < X_n < Y_1 < \ldots < Y_m$ where

- a_{ij}, b_{jl}, c_{lk} are invertible elements in $\mathcal{R}$,
- $\upsilon_{jl} \in \{X_1^{d_1} \cdots X_j^{d_j} \mid (d_1, \ldots, d_j) \in \mathbb{N}^j\}$
- $d_{ij}, e_{jl}, f_{lk} \in \mathcal{A}$ with $\mathbf{T}(d_{ij}) < X_iX_j, \quad \mathbf{T}(e_{jl}) < X_jY_l, \quad \mathbf{T}(f_{lk}) < Y_kY_l$.

[1] Up to Second Buchberger Criterion [3] but probably including the other criteria proposed by Gebauer and Möller [8].

The associated graded ring $\mathcal{G}$ is obtained by setting $d_{ij} = e_{jl} = f_{lk} = 0$. We immediately remark that, unless we restrict to the case in which each $\upsilon_{jl} = \mathbf{1}_{\mathcal{A}}$, noetherianity is not sufficient to grant temination and finiteness.

Example 1. Simply consider Tamari's [23] ring $\mathbb{Q}\langle X, Y\rangle/\mathbb{I}(YX - X^2Y)$ where the principal ideal $\mathcal{I} = (X)$ has the infinite involutive basis $\{X^{2^i}Y^i, i \in \mathbb{N}\}$ each element having X as multiplicative variable.

Under this restriction, we obtain in any case a class of rings larger than solvable polynomial rings[2] even if $\mathcal{R}$ is assumed to be a field; there are in fact

- for each term $\tau \in \Gamma$ an automorphism $\alpha_\tau : \mathcal{R} \to \mathcal{R}$ and
- for each two terms $\tau_1, \tau_2 \in \Gamma$ an element $\varpi(\tau_2, \tau_1) \in \mathcal{R}$ so that the multiplicative $*$ arithmetic of $\mathcal{G}$ is defined by distributing the monomial product

$$a_1\tau_1 * a_2\tau_2 = a_i\alpha_{\tau_1}(a_2)\varpi(\tau_1, \tau_2)\tau_1 \circ \tau_2$$

where $\circ$ denote the classical multiplication in Γ.

Already under this restriction and even assuming $\mathcal{R}$ to be a field, the classical

Theorem 2. [9, Th.4.10] [10, Th.2.10] *If an involutive division is left(/right/restricted) continuous then left(/right/restricted) local involutivity of any set U implies its left(/right/restricted) involutivity.*

is not obvious [7]: it can be proved by means of Jacobi-like formulas which can be deduced on effective rings via associativity. The main problem arises when the coefficient ring $\mathcal{D}$, on which $\mathcal{R} = \mathcal{D}\langle\overline{\mathbf{v}}\rangle/I$ is a module, is not a field but just a PID[3]; as it was remarked by Seiler [22] one needs at least to follow the standard approach in Buchberger Theory and speak of *weak* and *strong* bases.

Example 3. [20] In the ideal $\mathcal{I} := \mathbb{I}(g_1, g_2) \subset \mathbb{Z}[X, Y], g_1 := 3X, g_2 := 2Y$, it holds $\mathcal{I} \ni g_3 := XY = g_1Y - g_2X$ while $3X \nmid XY$ and $2Y \nmid XY$.

As a consequence the characterization of a set U to be *involutive/complete with respect to an involutive division* L which in the field case [9, Def.4.1] [10, Def.2.4] simply requires that $\cup_{u\in U} u\, L(u, U) = \cup_{u\in U} u\,\Gamma \subset \Gamma$ must be reconsidered since we should require a formulation $\cup_{u\in U} u\, L(u, U) = \cup_{u\in U} u\,\mathsf{M}(\mathcal{A}) \subset \mathsf{M}(\mathcal{A}) := \{ct : t \in \Gamma, c \in \mathcal{R} \setminus \{0\}\}$ but, in general $\mathcal{N} := \cup_{u\in U} u\,\mathsf{M}(\mathcal{A}) \subsetneq \mathbb{I}(U) \cap \mathsf{M}(\mathcal{A}) = \mathrm{Span}_{\mathcal{R}}\{\mathcal{N}\} \cap \mathsf{M}(\mathcal{A})$.
For the moment we have postponed the investigation of the *strong* case and we [7] have adapted the terminology from the *terms* Γ with coefficients over a field to the *monomials* $\mathsf{M}(\mathcal{A})$, the coefficients being over an effectively given ring $\mathcal{R}$ and applied *Weispfenning multiplication* [24, 5] in order to deduce twosided (and subbilateral) bases from restricted ones, but mainly we have considered only the easiest *weak* case. In this setting, of course, we loose one stength of involutiveness, namely that any monomial $w \in \mathsf{M}(\mathcal{A})$ has at most one $L-$involutive divisor in U,

---

[2] where each α_τ is the identity and each $\varpi(\tau_2, \tau_1) = 1$ so that $a_1\tau_1 * a_2\tau_2 = a_1a_2\tau_1 \circ \tau_2$.
[3] the PIR case simply requires to deal with proper annihilators.

a property which can be granted, via *strong* bases, only when $\mathcal{R}$ itself is a PIR. Therefore reduction of a monomial $c\tau \in \mathsf{M}(\mathcal{A})$ must be performed considering all potential divisors $c_i\tau_i \in U$ such that $\tau_i \mid \tau$, $\tau = \upsilon_i \circ \tau_i$ and looking for relations $c = \sum_i a_i \alpha_{\upsilon_i} \varpi(\upsilon_i, \tau_i)$ and reduction be performed via classical Buchberger reduction.

In the *strong* cases, on the basis of [20, 14, 19], we guess that the test/completion for involutivity of a continuous involutive division, which in the field case (Theorem 2) is local involutivity, should be reformulated as

Claim 4. [10, Th.6.5] *Let L be a continuous involutive division. A polynomial set F is strong L-involutive if*

- *for each $f \in F$ and each non-multiplicative variable $x \in NM_L(lc(f), lc(F))$, the related J-prolongation $f \cdot x_i$,*
- *for each $f, g \in F$ the related P-prolongation $s\frac{lcm(\mathbf{T}(f),\mathbf{T}(g))}{\mathbf{T}(f)} f + t\frac{lcm(\mathbf{T}(g)g,\mathbf{T}(g))}{\mathbf{T}(f)}$, where c, s are the Bezout values such that $slc(f) + tlc(g) = \gcd(lc(f), lc(g)$,*
- *for each $f \in F$ the related A-prolongation af, a being the annihilator of $lc(f)$*

reduce all of them to zero modulo F.

There is still some research required in the strong case when $\mathcal{R}$ itself is PID; we need to investigate whether both the classical [9, 10] approach and the recent RID [4] suggestion are able to recover the division structure of polynomial domains.

Example 5. For the ideal $\mathcal{I} := \mathbb{I}\left(8X, 4X^3, 2X^6, 36Y^2, 6Y^3, Y^4\right) \subset \mathbb{Z}[X,Y]$ a (minimal) strong Gröbner basis is $\bar{U} := \{8X, 4X^3, 2X^6, 36Y^2, 4XY^2, 6Y^3, 2XY^3, Y^4\}$; with respect the Janet/Pommaret division a strong minimal involutive basis is

$$\begin{aligned} \tilde{U} &:= \left\{8X^{1+i}Y^j, 0 \le i \le 1, 0 \le j \le 1\right\} \cup \left\{4X^{3+i}Y^j, 0 \le i \le 2, 0 \le j \le 1\right\} \\ \cup & \quad \left\{2X^6Y^j, 0 \le j \le 3\right\} \cup \left\{36Y^2, 6Y^3, Y^4\right\} \cup \left\{4X^{1+i}Y^2, 0 \le i \le 4\right\} \cup \left\{2X^{1+i}Y^3, 0 \le i \le 4\right\} \end{aligned}$$

with

τ	$M(\tau)$	$NM(\tau)$
Y^4	$\{X, Y\}$	$\emptyset$
$\left\{2X^6Y^j, 0 \le j \le 3\right\}$	$\{X\}$	$\{Y\}$
$\emptyset$	$\{Y\}$	$\{X\}$
$\tilde{U} \setminus \{2X^6, 2X^6Y, 2X^6Y^2, 2X^6Y^3, Y^4\}$	$\emptyset$	$\{X, Y\}$

References

[1] Buchberger B., *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph. D. Thesis, Innsbruck (1965)

[2] Buchberger B., *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleischunssystem*, Aeq. Math. **4** (1970), 374–383

[3] Buchberger B., *A Criterion for Detecting Unnecessary Reduction in the Construction of Gröbner bases*, L. N. Comp. Sci **72** (1979), 3–21, Springer

[4] Ceria, M., *Combinatorial decompositions for monomial ideals*, preprint

[5] Ceria, M., Mora, T. *Buchberger-Weispfenning Theory for Effective Associative Rings*, J. Symb. Comp., special issue for ISSAC 2015, 83, pp. 112-146.

[6] Ceria, M., Mora, T., *Buchberger-Zacharias Theory of Multivariate Ore Extensions*, Journal of Pure and Applied Algebra Volume 221, Issue 12, December 2017, Pages 2974-3026

[7] Ceria, M., Mora, T. *Weak Involutive bases over effective rings*, submitted to ISSAC2019

[8] Gebauer R., Möller H.M., *A fast Variant of Buchbgerger's Algorithm*, Preprint (1985)

[9] Gerdt V.P., Blinkov Y.A. *Involutive bases of Polynomial Ideals*, Math. Comp. Simul. **45** (1998), 543–560

[10] Gerdt V.P., Blinkov Y.A. *Minimal involutive bases*, Math. Comp. Simul. **45** (1998), 519–541

[11] Janet M. , *Sur les systèmes d'équations aux dérivées partielles* J. Math. Pure et Appl., **3** (1920), 65–151

[12] Kandri-Rody, A., Weispfenning, W., *Non-commutative Gröbner Bases in Algebras of Solvable Type*, J. Symb. Comp. **9** (1990), 1–26

[13] Ore O., *Theory of non-commutative polynomials* , Ann. Math. **34** (1933), 480–508

[14] Möller H.M., *On the construction of Gröbner bases using syzygies*, J. Symb. Comp. **6** (1988), 345–359

[15] T. Mora, *Solving Polynomial Equation Systems* 4 Vols., Cambridge University Press, I (2003), II (2005), III (2015), IV (2016)

[16] T. Mora, *Zacharias Representation of Effective Associative Rings*

[17] F. Mora, *De Nugis Groebnerialium 4: Zacharias, Spears, Möller* Proc. ISSAC'15 (2015), 191–198, ACM

[18] B. Nguefack, E. Pola, *Effective Buchberger-Zacharias-Weispfenning theory of skew polynomial extensions of restricted bilateral coherent rings*, J. Symb. Comp.

[19] Norton G.H., Sălăgean A., *Strong Gröbner bases for polynomials over a principal ideal ring*, Bull. Austral. Math. Soc. **64** (2001), 505–528

[20] Pan L., *On the D-bases of polynomial ideals over principal ideal domains*, J. Symb. Comp. **7** (1988), 55–69

[21] Schwartz F., *Reduction and Completion Algorithm for Partial Differential Equations*, Proc. ISSAC'92 (1992), 49–56 ACM

[22] Seiler W.M. *A Combinatorial Approach to Involution and δ-Regularity I: Involutive Bases in Polynommial Algebras of Solvable Type* J. AAECC **20** (2009), 207–259

[23] Tamari D. *On a certain Classification of rings and semigroups* Bull. A.M.S. **54** (1948), 153–158

[24] Weispfenning, V. *Finite Gröbner bases in non-noetherian Skew Polynomial Rings* Proc. ISSAC'92 (1992), 320–332, A.C.M.

Michela Ceria
Department of Computer Science, University of Milan, Italy
e-mail: michela.ceria@gmail.com

Teo Mora
Department of Mathematics, University of Genoa, Italy
e-mail: theomora@disi.unige.it