Do It Yourself: Buchberger and Janet Bases over effective rings

M.Ceria and T. Mora

Part 1

The classical Buchberger Theory and Algorithm in the framework of polynomial rings over a field [1, 2, 3] has been generalized to a framework that is even non-necessarily commutative, namely that of (non necessarily commutative) monoid rings over a (non necessarily free) monoid and a principal ideal ring. This has been done through a series of milestone papers: Zacharias' [29] approach to canonical forms, Spear's [26] theorem which extends Buchberger Theory to each effectively given ring, Möller's [15] reformulation of Buchberger Algorithm in terms of lifting.

Consider a field $\mathbb{F}$ and the (commutative) polynomial rings $\mathbb{F}[X_1, \dots, X_n]$ [1, 2, 3, 4] over it. In order to compute Gröbner bases, Buchberger test/completion is applied. It states that *a basis F is Gröbner if and only if each element in the set of all S-polynomials*

$$\left\{ S(f_{\alpha'}, f_\alpha) := \frac{\operatorname{lcm}(\mathbf{M}(f_\alpha), \mathbf{M}(f_{\alpha'}))}{\mathbf{M}(f_\alpha)} f_\alpha - \frac{\operatorname{lcm}(\mathbf{M}(f_\alpha), \mathbf{M}(f_{\alpha'}))}{\mathbf{M}(f_{\alpha'})} f_{\alpha'} : f_\alpha, f_{\alpha'} \in F \right\}$$

between two polynomials in F, reduces to 0.

The idea remains the same also in the more general setting of free monoid rings $\mathbb{F}\langle X_1, \dots, X_n\rangle$ over a field. Of course, the analogous of S-polynomials, i.e. *matches* are more complex, besides being potentially infinitely many; for instance,

$$\mathbf{M}(f_\alpha) w f_{\alpha'} - f_\alpha w \mathbf{M}(f_{\alpha'}), w \in \langle X_1, \dots, X_n\rangle.$$

These S-polynomials are not to be considered due to Buchberger's first Criterion, which states (in Möller's language) that such S-polynomial lifts to the trivial syzygy $f_\alpha w f_{\alpha'} - f_\alpha w f_{\alpha'}$.

As it is well known, both in the commutative and in the non-commutative setting, the test/completion based on the lifting theorem [15] is definitely more efficient than Buchberger test/completion, which is then discarded by the good implementations. Moeller lifting theorem says that *a generating set F is a Gröbner basis if and only if each element in a minimal basis of the syzygies among the leading monomials $\{\mathbf{M}(f_\alpha) : f_\alpha \in F\}$ lifts, via Buchberger reduction, to a syzygy among the elements of F.*

It is also worth to remark that the lifting theorem allowed [8] to give their (more efficient) criteria.

Gebauer-Moeller criteria detect at least as many "useless" pairs as Buchberger's two criteria [4], but *they do not need to verify whether a pair satisfies* *the conditions required by the Second Criterion and thus they avoid the consequent bottleneck* needed for listing and ordering the S-pairs (in the commutative case they are $(\#F)^2$, while a careful informal analysis in that setting suggests that the S-pairs needed by Gebauer–Möller Criterion are $n\#F$).

Part 2

The reformulation in the language of filtration-valuation terms [27, 16, 19] of Möller's Lifting Theorem and of Spear's [26] intuition that a Buchberger Theory defined in a ring can be exported to its quotients, allowed [16] to provide a framework in which Buchberger Theory may be generalized to a setting that specializes to useful cases such as monoid rings [13, 14], solvable polynomial rings [12] and Ore extensions [22, 5, 6, 20].

However, there was a weak point in [16]: the proposal of this paper could be applied only to rings/modules that were presented as vector spaces over a field. Differently, the universal property grants to a ring a representation accordingly to Spear's Theorem, *i.e.* as quotient of a monoid ring over the integers.

Anyway Buchberger Theory of monoid rings over the integers is strongly established [15] and Zacharias' Thesis [29] provided the natural setting for describing canonical forms of the elements of each ring which can be presented as quotient $\mathcal{A} = \mathcal{Q}/\mathcal{I}$ of a free monoid ring $\mathcal{Q} := \mathbb{Z}\langle\overline{\mathbf{Z}}\rangle$ over $\mathbb{Z}$ and the monoid $\langle\overline{\mathbf{Z}}\rangle$ of all words over the alphabet $\overline{\mathbf{Z}}$ modulo a bilateral ideal $\mathcal{I} \subset \mathcal{Q}$ of which a Gröbner basis is available.

Thus, since the universal property of the free monoid ring $\mathcal{Q} := \mathbb{Z}\langle\overline{\mathbf{Z}}\rangle$ over $\mathbb{Z}$ and the monoid $\langle\overline{\mathbf{Z}}\rangle$ of all words over the alphabet $\overline{\mathbf{Z}}$ grants that each ring with identity $\mathcal{A}$ can be presented as a quotient $\mathcal{A} = \mathcal{Q}/\mathcal{I}$ of a free monoid ring $\mathcal{Q}$ modulo a bilateral ideal $\mathcal{I} \subset \mathcal{Q}$, in order to impose a Buchberger Theory/Algorithm, based on Möller's Lifting Theorem over any effective associative ring it is enough to present effectively $\mathcal{A}$ and its elements via Zacharias canonical forms and use Spear's theorem in order to impose on $\mathcal{A}$ the natural filtration of $\mathcal{Q}$.

In the case of solvable polynomial rings and Ore extensions, the filtration/graduation approach grants that, in the left/right case the arithmetics required by Möller's Lifting Theorem [6, 20] boils down to the arithmetics of polynomial commutative ring. The computation of bilateral Gröbner bases can be performed via Kandri-Rody—Weispfenning completion[1]. A more efficient solution is obtained by means of restricted Gröbner bases [28] and the related Weispfenning multiplication [7].

Part 3

In 1920 Janet [11] introduced both the notion of Gröbner bases and a computational algorithm [9, 10] which essentially anticipated Buchberger's [1, 2]

[1] Extend the left Gröbner basis $G = \{g_1, \ldots, g_n\}$ with $F := \{g_i \star X_j\}$ and compute the left Gröbner basis H of $G \cup F$ until $G = H$ which then is the bilateral basis of $\mathbb{I}_2(G)$.

Algorithm[2]. Janet's idea is quite similar to the strongest formulation given by Moller's Lifting Theorem [15]. This has been explicitly remarked by Schwartz [24].
Our extension of Buchberger Theory and Algorithm on each $\mathcal{R}$-module $\mathcal{A}$ [17, 7], where both $\mathcal{R}$ and $\mathcal{A}$ are assumed to be effectively given through their Zacharias representation [18] suggested us to investigate whether and under which conditions Janet's approach can be extended to more general settings.

Janet completion has a strong combinatorial component. Therefore we need that, with the terminology of [17, 7], the associated graded ring $\mathcal{G}$ of $\mathcal{A}$ is an Ore-like extension [22, 6]; an interesting class of such rings, much wider than solvable polynomial rings [12] on which Seiler [25] applied Janet approach, has been recently proposed [20]:
$\mathcal{A} = \mathcal{R}\langle X_1, \ldots, X_n, Y_1, \ldots, Y_m\rangle/\mathcal{I}, \mathcal{I} = \mathbb{I}(G)$ with

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

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 $\mathbf{T}(d_{ij}) < X_iX_j, \quad \mathbf{T}(e_{jl}) < X_jY_l, \quad \mathbf{T}(f_{lk}) < Y_kY_l$. The associated graded ring $\mathcal{G}$ can be obtained setting $d_{ij} = e_{jl} = f_{lk} = 0$. Unless we restrict to the case in which each $\upsilon_{jl} = \mathbf{1}_{\mathcal{A}}$, noetherianity is not sufficient to grant temination and finiteness.

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 [25] one needs at least to follow the standard approach in Buchberger Theory and speak about *weak* and *strong* bases.

In the *strong* cases, basing on [23, 15, 21], we guess that the test/completion for involutiveness of a continuous involutive division, which in the field case ([10, Th.6.5]) is local involutivity, should be reformulated as

Claim 1. *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 t, s are the Bézout values such that $slc(f)+tlc(g) = \gcd(lc(f), lc(g))$,*

[2] Up to Second Buchberger Criterion [4] but probably including the other criteria proposed by Gebauer and Möller [8].

[3] the PIR case is not so complicated; indeed it simply requires to deal with proper annihilators.

- *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.

References

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

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

[3] B. Buchberger, *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory*, in Bose N.K. (Ed.) *Multidimensional Systems Theory* (1985), 184–232, Reider

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

[5] J. Bueso, J. Gomez-Torrecillas, and A. Verschoren. *Methods in Non-Commutative Algebra*. Kluwer, 2003.

[6] M. Ceria and T. Mora, *Buchberger-Zacharias Theory of Multivariate Ore Extensions*, J.P.A.A.**221**, 2974-3026 (2017).

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

[8] R. Gebauer and H.M. Möller, *On an Installation of Buchbgerger's Algorithm.* J. Symb. Comp. **6**, 275–286 (1988).

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

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

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

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

[13] K. Madlener and B. Reinert, *String Rewriting and Gröbner bases – A General Approach to Monoid and Group Rings*, Progress in Computer Science and Applied Logic **15** (1991), 127–180, Birkhäuser

[14] K. Madlener and B. Reinert, *Computing Gröbner bases in monoid and group rings*, Proc.ISSAC '93, ACM (1993), 254–263

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

[16] T. Mora, *Seven variations on standard bases*, (1988)
`ftp://ftp.disi.unige.it/person/MoraF/PUBLICATIONS/7Varietions.tar.gz`

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

[18] T. Mora, *Zacharias Representation of Effective Associative Rings*, J. Symb. Comp. (to appear).

[19] E. Mosteig, M. Sweedler, *Valuations and filtrations*, J. Symb. Comp. **34** (2002), 399–435

[20] B. Nguefack and E. Pola, *Effective Buchberger-Zacharias-Weispfenning theory of skew polynomial extensions of restricted bilateral coherent rings*, J. Symb. Comp. (to appear)

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

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

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

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

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

[26] D.A. Spear, *A constructive approach to commutative ring theory*, in *Proc. of the 1977 MACSYMA Users' Conference*, NASA CP-2012 (1977), 369–376

[27] M. Sweedler, *Ideal bases and valuation rings*, Manuscript (1986) available at `http://math.usask.ca/fvk/Valth.html`

[28] V. Weispfenning, Finite Gröbner bases in non-noetherian Skew Polynomial Rings. In: Proc.ISSAC '92. ACM, pp. 320–332 (1992).

[29] G. Zacharias, *Generalized Gröbner bases in commutative polynomial rings*, Bachelor's thesis, M.I.T. (1978)