Do It Yourself: Buchberger and Janet Bases over effective rings

M.Ceria and T. Mora

1 Part 1: Moeller Lifting Theorem vs Buchberger Criteria

Buchberger Theory, classically formulated on the polynomial ring over a field [1, 2, 3], is possible, with suitable variations, in a more general framework. In particular, it has been generalized to non-necessarily commutative *monoid rings*, defined over a non-necessarily free monoid and over a principal ideal ring.
Such a generalization, passed through three important stages: Zacharias' representation of the canonical forms [29], Spears' theorem to give an extension to effectively given rings [26] and Moeller lifting theorem, which reformulates Buchberger's algorithm [15].

Consider first the classical case [1, 2, 3, 4] of the commutative polynomial ring $\mathbb{F}[X_1,\dots,X_n]$ over a field $\mathbb{F}$. In this case, the computation of a Groebner basis for an ideal $\mathbb{I} := (F)$ of $\mathbb{F}[X_1,\dots,X_n]$ is done by means of the so called Buchberger's *test/completion*: F is a Groebner basis of $\mathbb{I}$ if and only if, each S-polynomial between two elements of F, namely each element of the set

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

reduces to 0 with respect to F.

In the more general case of a free monoid ring $\mathbb{F}\langle X_1,\dots,X_n\rangle$, defined over the field $\mathbb{F}$, we have to do more or less the same thing, but S-polynomial are definitely more involved. The analogous of S-polynomials, in this framework, are *matches* and they can be potentially infinite.
For example, in general, we have the infinite matches

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

Anyway, we must remark that all the matches of the form described above can be avoided, thanks of *Buchberger's First Criterion*. In the language of liftings, introduced by Moeller, we say that these matches lift to the *trivial syzygy*

$$f_\alpha w f_{\alpha'} - f_\alpha w f_{\alpha'}.$$

The test/completion based on Moeller Lifting Theorem is well known to be definitely more efficient than Buchberger's test/completion. This is the reason

which moved good software implementations to demote the former test/completion algorithm.
We summarize now in a few words what Moeller Lifting Theorem says. Consider an ideal $\mathbb{I} := (F)$ and let $\mathbf{M}\{F\} := \{\mathbf{M}(f_\alpha) : f_\alpha \in F\}$ be the set of the leading monomials of the elements in F. Call $\mathfrak{GM}$ a minimal basis for the syzygies of the leading monomials in $\mathbf{M}\{F\}$.
Moeller Lifting Theorem says that *F is a Groebner basis for $\mathbb{I}$ if and only if each element in $\mathfrak{GM}$ lifts, by means of Buchberger's reduction, to a syzygy among elements in F.*

Thanks to this theorem, Gebauer and Moeller [8] could give their criteria to detect useless S-polynomials, namely those whose reduction has not to be computed, since - for some theoretical reason - they necessarily reduce to zero. The number of such useless S-polynomials, found by means of Gebauer-Moeller's criteria is the same as that found by means of Buchberger's criteria [4]. The difference is in the efficiency on finding them: Gebauer and Moeller do not need to verify the condition imposed by Buchberger's Second Criterion. This means avoiding the bottleneck represented by *listing* and *reordering* the S-polynomials (in the commutative case, they are $|F|^2$ with Buchberger's approach, while we have $n|F|$, according to an informal analysis on Gebauer-Moeller's approach).

2 Part 2: Buchberger Algorithm via Spear's Theorem, Zacharias' Representation, Weisspfenning Multiplication

Moeller Lifting Theorem, as well as Spear's Theorem [26], which essentially says that Buchberger Theory defined over a ring can be exported to the quotients, have been generalized in terms of filtration/valuation [27, 16, 19]. Thanks to that, [16] gives a framework such that Buchberger's Theory can be generalized to a setting which then specializes to three very important cases, such as monoid rings [13, 14], solvable polynomial rings [12] and Ore extensions [22, 5, 6, 20].

Anyway, we can see a weakness in [16], namely that everything works only for rings/modules admitting a representation as *vector spaces over a field.*

The universal property gives us something different: a ring can be represented as stated by Spear's Theorem, namely as *a quotient of a monoid ring over the integers.*

We should remark that in the setting of a monoid ring over the integers, Buchberger's Theory is well established [15].
Moreover, Zacharias' thesis [29] gives the natural setting to describe the canonical forms of the elements of any ring which could be presented as a 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.

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 it is possible to present each ring with identity $\mathcal{A}$ as a quotient $\mathcal{A} = \mathcal{Q}/\mathcal{I}$ of a free monoid ring $\mathcal{Q}$ modulo a bilateral ideal $\mathcal{I} \subset \mathcal{Q}$.

Therefore, if we want to impose a Buchberger Theory/Algorithm, based on Möller's Lifting Theorem over any effective associative ring what we have to do is to present effectively $\mathcal{A}$ and its elements via Zacharias canonical forms and use Spear's Theorem in order to equip $\mathcal{A}$ with the natural filtration of $\mathcal{Q}$.

In the case of solvable polynomial rings and Ore extensions, this filtration/graduation approach grants us that, in the left/right case, the arithmetics we need to apply Moeller's Lifting Theorem[6, 20] reduces to the arithmetics of the commutative polynomial ring; bilateral Groebner bases can be computed by means of Kandri-RodyWeispfenning completion[1]. This approach can be extended to the more general case of effective rings where also the bilateral case is "commutivized" adapting Weispfenning's notion of restricted Groebner bases [28] and introducing the commutativizing Weispfenning multiplication, as explained in [7].

3 Part 3: What happens to involutive bases?

Janet, in his 1920's paper [11] essentially introduced the notion of Groebner basis and also a computational algorithm [9, 10] to get such bases, and which is an anticipation of Buchberger's results and algorithm[2] [1, 2]. The idea stated by Janet is similar to the strongest formulation, given by Moeller Lifting Theorem [15] and this has been explicitly remarked by Schwartz in [24].

In Janet's approach, a finite set U of terms (the leading terms of a generating set for an ideal) is considered. To each term $u \in U$ is associated a set $M(u, U)$ of variables, called *multiplicative variables*[3] for u with respect to U.
A *completion procedure* grants that each term w in the semigroup ideal generated by U can be written as $w = ut$, where $u \in U$ and t is a product of powers of multiplicative variables for u with respect to U. In this case we say that u is the involutive divisor of w
In computing *involutive bases* namely Janet's analogous of Groebner bases, each term w should be reduced using the generating polynomial whose leading term $u \in U$ is the involutive divisor of w.

Since we have extended Buchberger's Theory and algorithm to each $\mathcal{R}$-module $\mathcal{A}$ [17, 7], where both $\mathcal{R}$ and $\mathcal{A}$ are assumed to be effectively given

[1]It essentially consists in extending the left Gröbner basis $G = \{g_1, \dots, g_n\}$ with $F := \{g_i \star X_j\}$ and computing the left Gröbner basis H of $G \cup F$ until $G = H$, which then is the bilateral basis of $\mathbb{I}_2(G)$.

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

[3]The complementary set of *non-multiplicative variables*, is denoted by $NM(u, U)$.

through their Zacharias representation [18], natural questions can be: *is it possible to have Janet's approach in more general settings? What are the conditions to be satisfied in order to do that?*
We started then investigating on these questions.

Janet completion is strongly based on combinatorial arguments; therefore, with the terminology of [17, 7], it is important that the associated graded ring $\mathcal{G}$ of $\mathcal{A}$ is an Ore-like extension [22, 6]. An interesting class of such kind of rings, much wider than solvable polynomial rings [12] (on which Seiler [25] applied Janet approach), has been proposed in the paper [20]:

$\mathcal{A} = \mathcal{R}\langle X_1, \dots, X_n, Y_1, \dots, Y_m\rangle/\mathcal{I}, \mathcal{I} = \mathbb{I}(G)$ 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 $\Gamma := \{X_1^{d_1} \cdots X_n^{d_n} Y_1^{e_1} \cdots Y_m^{e_m} | (d_1, \dots, d_n, e_1, \dots, e_m) \in \mathbb{N}^{n+m}\}$ induced by $X_1 < \dots < X_n < Y_1 < \dots < Y_m$ where a_{ij}, b_{jl}, c_{lk} are invertible elements in $\mathcal{R}$, $\upsilon_{jl} \in \{X_1^{d_1} \cdots X_j^{d_j} \mid (d_1, \dots, d_j) \in \mathbb{N}^j\}$, $d_{ij}, e_{jl}, f_{lk} \in \mathcal{A}$ with leading terms $\mathbf{T}(d_{ij}) < X_iX_j$, $\mathbf{T}(e_{jl}) < X_jY_l$, $\mathbf{T}(f_{lk}) < Y_kY_l$.
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 $\mathcal{D}$, over which $\mathcal{R} = \mathcal{D}\langle \overline{\mathbf{v}} \rangle / I$ is a module, is not a field but just a *principal ideal domain*[4]; as it was remarked by Seiler in the paper [25], at least we need to follow the standard approach proper of Buchberger Theory and make a distinction between *weak* and *strong* bases.

In the *strong* cases, basing on [23, 15, 21], we conjecture that the test/completion for involutiveness of a *continuous involutive division*[5], which in the field case ([10, Th.6.5]) is local involutiveness, should be reformulated as

Claim 1. *Let L be a continuous involutive division. A polynomial set F is strong L-involutive if*

[4]the PIR case is not much more complicated. Indeed, simply, we have to deal with proper annihilators.

[5]A division Ł is called *continuous* if for any finite set U of terms, the inequality $u_i \neq u_j, i \neq j$ holds for any finite sequence $u_1, \dots u_k$ of elements in U such that

$$\forall i < k \exists X_j \in NM(u_i, U) \text{ such that } u_{i+1} |_{\text{Ł}} u_i \cdot X_j. \tag{1}$$

- *for each* $f \in F$ *and each non-multiplicative variable* $x \in NM(\mathbf{M}(f), \mathbf{M}(F))$, *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 for the leading coefficients we have* $slc(f) + tlc(g) = \gcd(lc(f), lc(g))$,
- *for each* $f \in F$ *the related* A*-prolongation* af, a *being the annihilator of* $lc(f)$

all of them reduce 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)