A local Buchberger algorithm

ARIANE PÉLADAN-GERMA
École Polytechnique
Laboratoire Gage
91128 Palaiseau cedex
germa@ariana.polytechnique.fr

JORIS VAN DER HOEVEN
École Polytechnique
LIX
F-91128 Palaiseau cedex
vdhoeven@lix.polytechnique.fr

1 The algorithm

Let $A = K[x_1, \ldots, x_n]$ be the ring of polynomials in n indeterminates over an effective field K. This means that all elements of K can be represented by data structures, and that all field operations $(+, -, \cdot, /, =)$ can be performed by algorithms. We use the pure lexicographical order on monomials, with $x_1 < \cdots < x_n$. Let $S \supseteq K^\star$ be a multiplicative subset of A with an effective membership test.

In order to compute "pseudo-bases" of ideals of A/S, we use a classical reduction-completion approach. The keystone of this paper lies in our non-classical definitions of the pseudo-head $H(P)$ and the pseudo-leading-coefficient $C(P)$ of non-zero polynomials P: they are inspired both by Ritt-Wu's work and Buchberger's terminology.

Each non constant polynomial P in A can be written $P = I_P x_P^{d_P} + R_P$, where x_P is the greatest indeterminate involved in P, and d_P the highest order of P with respect to x_P. I_P is usually called the *initial* of P. Now we define $H(P)$ and $C(P)$ for non-zero polynomials:

- if $P \in S$ then $H(P) = 1$ and $C(P) = P$;
- if $P \notin S$ and $I_P \in S$ then $H(P) = x_P^{d_P}$ and $C(P) = I_P$;
- if $P \notin S$ and $I_P \notin S$ then $H(P) = x_P^{d_P} H(I_P)$ and $C(P) = C(I_P)$.

For example, let S be the set of polynomials that do not vanish at $x_1 = \ldots = x_n = 0$. If $P = (x_1 + 1)x_2 + x_1$, then $H(P) = x_2$ and $C(P) = x_1 + 1$. Now if $P = ((x_1 + 1)x_2 + x_1)x_3^2 + x_3 x_2$, then $H(P) = x_2 x_3^2$ and $C(P) = x_1 + 1$.

Suppose $Q \neq 0$, $Q \notin S$ and $P \neq 0$. We say that P is *reducible* with respect to Q if $H(P)$ is divisible by $H(Q)$. In this case, write $P = UH(Q) + V$, where $U, V \in A$, and no monomial appearing in V is divisible by $H(Q)$. P is then *elementary reduced* to $red(P, Q) = C(Q)P - UQ$ by Q. If $Q \in S$, then P is reducible with respect to Q and $red(P, Q) = 0$. It can be easily checked, although this is a little technical, that $H(red(P, Q)) < H(P)$ ($H(0) = -\infty$ by convention). Repeating the elementary reduction of P by Q, that is

$$P \to P_1 = red(P, Q) \to red(P_1, Q) \to \cdots,$$

we end up with a polynomial R such that $H(Q)$ does not divide $H(R)$ or $R = 0$. This process stops because the heads of the intermediate polynomials strictly decrease. This polynomial R is called the *pseudo-reduction* of P by Q and is denoted by $Red(P, Q)$. More generally, we can reduce P by a set E of polynomials by reducing P by $Q \in E$ as long as we can. Although the result R of this procedure is not necessarily unique, we will denote $R = Red(P, E)$, by abuse of language. Note that R belongs to the ideal $(P, E)_{A/S}$ generated by P and E in A/S and if $R = 0$, then $P \in (E)_{A/S}$.

Let P, Q be nonzero elements of $K[x_1, \ldots, x_n]$. Let i be the lowest index such that $C(P)$ and $C(Q)$ are both in $A_i = K[x_1, \cdots, x_{i-1}]$. We write $P = C_i(P)H_i(P) + R(P)$, where $H_i(P)$ is highest monomial occurring in P, when considered as a polynomial in $x_i, \cdots, x_n$ with coefficients in A_i. Similarly, we write $Q = C_i(Q)H_i(Q) + R(Q)$. Then the *S-polynomial* of P and Q is defined by $SPol(P, Q) := \dfrac{C_i(Q)H_i(Q)}{gcd(H_i(P), H_i(Q))}P - \dfrac{C_i(P)H_i(P)}{gcd(H_i(P), H_i(Q))}Q$. This definition enables us to assert that $H(SPol(P, Q)) < lcm(H(P), H(Q))$. Note also that $Spol(P, Q) \in (P, Q)$ and *a fortiori* $Spol(P, Q) \in (P, Q)_{A/S}$.

We now apply Buchberger's algorithm (see [CLO 92], [Buch 65]) with our alternative definitions of heads, leading coefficients, reduction, and S-polynomials. We recall hereafter a compact but non optimized version of this algorithm.

Algorithm Pseudo_Groebner_basis
Input: a finite set E of non zero polynomials in A.
Output: a pseudo-Groebner basis G of the ideal generated by E in A/S.

$G := E$
repeat
    $G' := G$
    for each $P \in G'$
        $R := Red(P, G - \{P\})$
        if $R \neq 0$ **then** $G := G \cup \{R\}$
    for each pair $P \neq Q$ in G' **do**
        $R := Red(SPol(P, Q), G')$
        if $R \neq 0$ **then** $G := G \cup \{R\}$
until $G = G'$

The ideals generated by the heads of the elements of the successive values of G form a strictly increasing sequence of ideals, whence the algorithm terminates. The sets E and G generate in A/S the same ideal $I_{A/S}$. Indeed, we only insert elements that are already in $(E)_{A/S}$ into G. G is not a Groebner basis, but has the property that if P is in A and $Red(P, G) = 0$, then $P \in I_{A/S}$. The computation of G enables us to quickly extract much information about $I_{A/S}$, without obtaining a complete description of $I_{A/S}$. Notice that if G contains a polynomial in S, then $I_{A/S}$ is trivial, and every polynomial in A is reduced to zero by G.

Our algorithm reduces to the usual Buchberger algorithm if $S = K^\star$; that is the reason why we call G a pseudo-Groebner basis rather than a pseudo-Ritt basis.

2 An application

In this section, we present a generalization of Shackell's first algorithm for testing identities between formal power series (see [Sh 89]). This algorithm detects identities like $\sin^2 z + \cos^2 z = 1$ from the differential relations $\sin' z = \cos z$ and $\cos' z = -\sin z$ and the initial conditions $\sin z = 0$ and $\cos z = 1$ (at $z = 0$). In our generalization of Shackell's algorithm, we can also detect identities between formal power series in several variables. Here the variables may themselves satisfy non-degenerate functional equations (see [VdH 96] for details).

Moreover, Shackell's algorithm uses Groebner bases, and he gave an example where this may lead to a drastic complexity. This motivated our introduction of pseudo-Groebner bases.

With the notations from the previous section, we assume that we have a set $\Delta = \{\partial_1, \cdots, \partial_k\}$ of partial derivations on A. Classically, $\partial_1, \ldots, \partial_k$ commute, but this is not necessary here: allowing non commutation makes it possible to impose functional relations among the coordinate functions. We take S of the form $S = \{P \in A | \varepsilon(P) \neq 0\}$, where $\varepsilon : A \to K$ is a given ring homomorphism. We call ε the *evaluation mapping* on A; ε specifies the initial conditions mentioned above. An element $P \in A$ is said to be *zero-equivalent*, if $\varepsilon(\partial_{i_1} \cdots \partial_{i_p} P) = 0$, for all p and $i_1, \cdots, i_p \in \{1, \cdots, k\}$. In the above example, we take $A = K[\sin z, \cos z]$, $k = 1$, $\partial_1 \sin z = \cos z$, $\partial_1 \cos z = -\sin z$, $\varepsilon(\sin z) = 0$ and $\varepsilon(\cos z) = 1$. Now $P = \sin^2 z + \cos^2 z - 1$ is zero-equivalent although $P \neq 0$ as a polynomial in $\sin z, \cos z$. The following algorithm is a generalization of Shackell's algorithm:

Algorithm zero_equivalence
Input: A polynomial $P \in A$.
Output: Answer to the question whether P is zero-equivalent.

if $\varepsilon(P) \neq 0$ **then return false**
$G := \{P\}$
while $\exists i\ \exists Q \in G \quad Red(\partial_i Q, G) \neq 0$ **do**
  if $\varepsilon(\partial_i Q) \neq 0$ **then return false**
  $G :=$ Pseudo_Groebner_basis$(G \cup \{\partial_i Q\})$
return true

Let us prove the termination and the correctness of this algorithm. The ideals generated by the heads of the polynomials in the successive values of G form a strictly increasing chain of ideals. This proves the termination. As to the correctness, it is clear that if the algorithm answers negatively, then P is not zero-equivalent. If the algorithm answers positively, then let G be the pseudo-Groebner basis at the end of the algorithm. We have $Red(\partial_i Q, G) = 0$, for each $1 \leq i \leq k, Q \in G$. In particular, $\Delta G \subseteq (G)_{A/S}$, where $(G)_{A/S}$ denotes the ideal in A/S generated by G. This implies that $(G)_{A/S}$ is stable by Δ. Since all elements of G evaluate to zero, so do all elements of $(G)_{A/S}$. Hence all elements of $(G)_{A/S}$ — which contains P — are zero-equivalent.

The interest of the our pseudo-Buchberger algorithm is illustrated by the following example, due to Shackell: we take $A = K[f_1, f_2, f_3, f_4]$, $k = 1$, $\partial_1 f_1 = 1$, $\partial_1 f_2 = f_2$, $\partial_1 f_3 = 2f_1 f_3$, $\partial_1 f_4 = 2f_1 f_4$, $\varepsilon(f_1) = 0$, $\varepsilon(f_2) = \varepsilon(f_3) = \varepsilon(f_4) = 1$. Then the polynomial $P = (f_1^M + f_2)(f_3 - f_4)$ is zero-equivalent since $f_3 - f_4$ is. However, Shackell's algorithm needs $O(M)$ steps to conclude this, whereas ours terminates after one step: $\partial_1 P$ is pseudo-reduced to zero by P. For more details about zero-equivalence algorithms, and alternative tests, we refer to [Pél 95], [Pél 97] and [VdH 97].

3 Bibliography

[Buch 65] B. Buchberger. Ein Algorithmus zum auffinden der Basiselemente des Restklassenringes nach einem null-dimensionalen Polynomideal. *PhD. thesis, University of Innsbruck.*

[CLO 92] D. Cox, J. Little, D. O' Shea. *Ideals, varieties and algorithms.* Springer-Verlag, New York.

[DL 89] J. Denef, L. Lipshitz. Decision problems for differential equations. *Journal of Symbolic Logic, Vol 54(3) (p. 941- 950).*

[Lo 87] A. Logar. Constructions over localizations of rings. *Le Mathematiche, Vol. 42 (p. 131-149).*

[MPT 92] T. Mora, G. Pfister, C. Traverso. An introduction to the tangent cone algorithm. *Advances in computing research (1992), vol. 6 (p. 199-270).*

[Pél 95] A. Péladan-Germa. Testing identities of series defined by algebraic partial differential equations. *Lect. Notes in Comp. Science 948 (p. 393-407).*

[Pél 97] A. Péladan-Germa. Tests effectifs de nullité dans des extensions d'anneaux différentiels. *PhD. Thesis, École Polytechnique, France.*

[Sh 89] J. Shackell. Zero-equivalence in function fields defined by algebraic differential equations. *Trans. of the AMS, Vol. 336, Number 1 (p. 151-171).*

[VdH 97] J. van der Hoeven. Automatic asymptotics. *PhD. Thesis, École polytechnique, France.*

[Wu 87] W.T. Wu. A Zero structure theorem for polynomial equation solving and its applications. *Proceedings of ISSAC'88, Roma, Springer Verlag.*