A NEW HENSELIAN CONSTRUCTION AND ITS APPLICATION TO POLYNOMIAL GCDS OVER DIRECT PRODUCTS OF FIELDS

François Boulier   Marc Moreno Maza   Cosmin Oancea

Abstract

Let K be a field of multivariate rational functions over an infinite field. Let L be a direct product of fields extending K by a tower of algebraic extensions. We propose a modular algorithm for computing polynomial gcds over L based on a Hensel lifting strategy. The rational reconstruction is avoided by *guessing* the denominator of the gcd before the lifting step. The algorithm is probabilistic but succeeds with probability one. Our implementation shows a significant improvement with respect to other methods.

Introduction

Let k be an infinite field and let R be an integral domain which is either the ring $\mathbb{Z}$ of integers or a ring $k[t_1, \ldots, t_n]$ of multivariate polynomials over k. Let $L_0 = K$ be the field of fractions of R. Let $x_1 < \cdots < x_p$ be ordered variables and let $m_1, \ldots, m_p$ be non-constant polynomials in $R[x_1, \ldots, x_p]$. Let i be any integer in the range $1 \cdots p$. We assume that the greatest variable occurring in m_i is x_i and that the leading coefficient $\mathrm{lc}(m_i, x_i)$ of m_i w.r.t. x_i lies in R. Let L_i be the simple algebraic extension defined by m_i over L_{i-1}. In other words, the ring L_i is the residue class ring $L_i = L_{i-1}[x_i]/\langle m_i \rangle$. We assume that the polynomial m_i generates a radical ideal in $L_{i-1}[x_i]$. We define $L = L_p$. Let y be an additional variable and let f_1, f_2 be polynomials in $L[y]$ with regular (i.e. not zero-divisors) leading coefficients. It is known that every ring L_i is a direct product of fields. Therefore, it makes sense to consider the gcds of f_1, f_2 in $L[y]$ (although a monic gcd of f_1, f_2 may not always exist even if f_1, f_2 are both monic). See [MR95] for more detail.

Langemyr and McCallum provides in [LM89] an algorithm for computing gcds in $L[y]$ for the case where L is a field, $R = \mathbb{Z}$ and $p = 1$. This algorithm is improved by Encarnación in [Enc94]. In [MR95] the authors proposed an algorithm for the general case where L is not necessarily a field, p may be greater than 1 and R is any integral domain. This non-modular algorithm combines subresultant theory and the following remark.

In order to compute a gcd of f_1, f_2 in $L[y]$ one can apply the *D5 principle* [DDD85] to the Euclidean algorithm in $L[y]$. That is, running the Euclidean algorithm in $L[y]$ as if L was a field but checking that the leading coefficient of every intermediate remainder is regular. When a zero-divisor is met, then a decomposition $L_1 \oplus L_2$ of L has been found and the computations should split into two branches: one in $L_1[y]$ and one $L_2[y]$. We denote by g_{monic} the polynomial of $L[y]$ obtained by this process. Again, the polynomial g_{monic} is not necessarily monic but for every field F factor of L the projection of g_{monic} in $F[y]$ is monic.

Let us regard now the set $M = \{m_1, \ldots, m_p\}$ as a regular chain in $R[x_1, \ldots, x_p]$. We define $U = R[x_1, \ldots, x_p]/\mathrm{Sat}(M)$ where $\mathrm{Sat}(M)$ is the saturated ideal of M. See [ALM99] for the notions related to regular chains. One can run the subresultant algorithm in $U[y]$ as if U was an integral domain but checking that the leading coefficient of every intermediate pseudo-remainder is regular. If no zero-divisor is met during this process, then we obtain a polynomial $g_{\mathrm{subres}} \in U[y]$ such that g_{monic} and g_{subres} are equal in $L[y]$ up to a multiplicative factor which is a regular element of L. This alternative approach is introduced in [Mor99].

Monagan and van Hoeij have proposed two modular algorithms for the case where L is a field. The first one in [HM02] assumes that $R = \mathbb{Z}$ holds. The second one in [HM04] applies to the case where $R = k[t_1, \ldots, t_n]$ but assumes $p = 1$. Both algorithms are based on the Chinese remaindering algorithm and the rational reconstruction.

In this paper, we propose an algorithm which applies to case where L is not necessarily a field, p may be greater than 1 and $R = k[t_1, \ldots, t_n]$ (as those of [MR95] and [Mor99]) but which is a modular algorithm (as those of [HM02] and [HM04]). A preliminary implementation shows that our new algorithm can process problems that were out of the scope of the algorithms of [MR95] and [Mor99]. We rely on a new Henselian construction presented in Section 1. Our approach avoids the rational reconstruction by *guessing* the denominator of the gcd, as discussed in Section 2. In addition, our algorithm is probabilistic (in the sense that it may run forever) but succeeds (in a finite number of steps) with probability one. The proof (not reported here) of this latter fact relies on subresultant theory, in particular on the results of [El 03], and a key notion that we introduce now.

Checking the regularity of an element in U is made by running the subresultant algorithm in $(R[x_1, \ldots, x_{\ell-1}]/\mathrm{Sat}(m_1, \ldots, m_{\ell-1}))[x_\ell]$ for some $\ell \in \{1, \ldots, p\}$. This leads to the following concept. We call the *history* of g_{subres} the sequence denoted by $\mathrm{history}(g_{\mathrm{subres}})$ of the degrees of all intermediate pseudo-remainders appearing when computing g_{subres} (including those pseudo-remainders involved when testing the regularity of an element). Similarly we define $\mathrm{history}(g_{\mathrm{monic}})$ and observe that $\mathrm{history}(g_{\mathrm{subres}})$ and $\mathrm{history}(g_{\mathrm{monic}})$ coincide.

1 A new Henselian construction

Let $\mathcal{M}_0$ be a maximal ideal of R of the form $\langle t_1 - t_{1,0}, \ldots, t_n - t_{n,0} \rangle$. We denote by $R_{\mathcal{M}_0}$ the residue class field $R/\mathcal{M}_0$ and by $M_0 = \{m_{1,0}, \ldots, m_{p,0}\}$ the image of the regular chain M in $R_{\mathcal{M}_0}[x_1, \ldots, x_p]$. We assume that no $\mathrm{lc}(m_i, x_i)$ is null modulo $\mathcal{M}_0$ such that M_0 is a regular chain in $(R/\mathcal{M}_0)[x_1, \ldots, x_p]$. Observe that M_0 is also a lexicographical Gröbner basis for the monomial ordering induced by $x_1 < \cdots < x_p$ and that $\mathrm{Sat}(M_0)$ is just the ideal generated by M_0. Finally, we denote by $U_{\mathcal{M}_0}$ the residue class ring $R_{\mathcal{M}_0}[x_1, \ldots, x_p]/\mathrm{Sat}(M_0)$.

Theorem 1.1. *Assume that* $\mathrm{Sat}(M_0)$ *is radical (as it is the case for* $\mathrm{Sat}(M)$*) such that* $U_{\mathcal{M}_0}$ *is a direct product of fields. Let* $f \in R[x_1, \ldots, x_p][y]$ *and* f_0 *be its image in* $R_{\mathcal{M}_0}[x_1, \ldots, x_p][y]$. *Let* $c_g, c_h \in R[x_1, \ldots, x_p]$ *be units of* L *such that* $\mathrm{lc}(f, y) = c_g\, c_h$. *Let* $d_1, \ldots, d_n$ *be positive* *integers. Let g_0 and h_0 be polynomials in $R_{\mathcal{M}_0}[x_1,\ldots,x_p][y]$ with respective degrees d_g and d_h and such that g_0 and h_0 are relatively prime in $U_{\mathcal{M}_0}[y]$, their product g_0h_0 is equal to f_0 in $U_{\mathcal{M}_0}[y]$, and their leading coefficients $\mathrm{lc}(f_0,y)$ and $\mathrm{lc}(g_0,y)$ are units in $U_{\mathcal{M}_0}$ equal respectively to c_g and c_h in $U_{\mathcal{M}_0}$. Then, there exists at most one couple (g,h) of polynomials in $L[y]$ such that*

(i) f *equals* $g\,h$ *in* $L[y]$,

(ii) g_0 *and* h_0 *are the respective images of* g *and* h *in* $U_{\mathcal{M}_0}[y]$,

(iii) $\mathrm{lc}(g) = c_g$ *and* $\mathrm{lc}(h) = c_h$,

(iv) *For every* $i = 1,\ldots,n$ *we have* $\max(\deg(g,t_i),\deg(h,t_i)) \leq d_i$.

In addition, if it exists, such couple (g,h) can be constructed effectively in $R[x_1,\ldots,x_p][y]$.

For two polynomials $g,h \in R[x_1,\ldots,x_p][y]$ the equation $f = g\,h$ in $L[y]$ means f equals $g\,h$ modulo $\mathrm{Sat}(M)$. That is, there exist polynomials $r_1,\ldots,r_p \in R[x_1,\ldots,x_p][y]$ and a product λ of (powers of) the $\mathrm{lc}(m_i,x_i)$ such that

$$\lambda\,(f - g\,h) = r_1m_1 + \cdots + r_pm_p. \tag{1}$$

We assume that we have an initial guess for λ. If the construction to be described below does not succeed in computing g and h this implies either that no couple (g,h) of polynomials in $L[y]$ satisfying (i), (ii), (iii), (iv) exists or that λ was not adequate. However, the construction will show how λ must be corrected for a next *try*. This feature validates the whole process. Now, let λ_0 be the image of λ modulo $\mathcal{M}_0$. Because of the properties of M_0 described earlier, one can compute $r_{1,0},\ldots,r_{p,0} \in R_{\mathcal{M}_0}[x_1,\ldots,x_p][y]$ such that

$$\lambda_0\,(f_0 - g_0\,h_0) = r_{1,0}m_{1,0} + \cdots + r_{p,0}m_{p,0}. \tag{2}$$

The fact that g_0 and h_0 are relatively prime in $U_{\mathcal{M}_0}[y]$ means that there exist polynomials $\sigma_0,\pi_0 \in R_{\mathcal{M}_0}[x_1,\ldots,x_p][y]$ and polynomials $\rho_0,\tau_0,\theta_{1,0},\ldots,\theta_{p,0} \in R_{\mathcal{M}_0}[x_1,\ldots,x_p]$ such that

$$\sigma_0g_0 + \pi_0h_0 = \rho_0 \quad\text{and}\quad \rho_0\tau_0 = 1 + \theta_{1,0}m_{1,0} + \cdots + \theta_{p,0}m_{p,0}. \tag{3}$$

Note that all these polynomials can be effectively computed, for instance by the algorithms of [MR95]. For simplicity, we sketch the remaining of the construction of g and h for the case $n = 1$. The general case can be obtained by the techniques discussed in Section 6.7 of [GCL92]. We define $q = t_1 - t_{1,0}$. Then we set $g^{(1)} = (c_g - \mathrm{lc}(g_0,y))y^{d_g} + g_0$, $h^{(1)} = (c_h - \mathrm{lc}(h_0,y))y^{d_h} + h_0$, $r_1^{(1)} = r_{1,0}$, $\ldots$, $r_p^{(1)} = r_{p,0}$. For $1 \leq k \leq d_1 + 1$, we shall construct $g^{(k)},h^{(k)},r_1^{(k)},\ldots,r_p^{(k)} \in R[x_1,\ldots,x_p][y]$ such that $g^{(k)},h^{(k)},r_1^{(k)},\ldots,r_p^{(k)}$ are equal modulo q^k to the polynomials $g,h,r_1,\ldots,r_p$ to be computed, and $g^{(k)},h^{(k)},r_1^{(k)},\ldots,r_p^{(k)}$ are equal modulo q to $g^{(1)},h^{(1)},r_1^{(1)},\ldots,r_p^{(1)}$. To this end, we define

$$F(u,v,w_1,\ldots,w_p) = \lambda(f - u\,v) - w_1m_1 - \cdots - w_pm_p$$

where $u, v, w_1, \ldots, w_p$ are any polynomials in $R[x_1, \ldots, x_p][y]$. Proceeding by induction on $k \geq 1$ and using the Relations (1) and (2) one can easily show that

$$F(g^{(k)}, h^{(k)}, r_1^{(k)}, \ldots, r_p^{(k)}) \equiv F(g, h, r_1, \ldots, r_p) \equiv 0 \mod q^k. \tag{4}$$

Expressing $F(g^{(k+1)}, h^{(k+1)}, r_1^{(k+1)}, \ldots, r_p^{(k+1)})$ with the Taylor expansion of F around $g^{(k)}, h^{(k)}, r_1^{(k)}, \ldots, r_p^{(k)}$ and using Relation (4) leads to

$$\epsilon_k = \lambda_0 h_0 g_k + \lambda_0 g_0 h_k + r_{1,k} m_{1,0} + \ldots + r_{p,k} m_{p,0} \tag{5}$$

where $g_k, h_k, r_{1,k}, \ldots, r_{p,k}$ are the coefficients of q^k in $g^{(k)}, h^{(k)}, r_1^{(k)}, \ldots, r_p^{(k)}$ and where

$$\epsilon_k = \mathrm{eval}(\frac{E_k}{q^k}, t_1 = t_{1,0}) \quad \text{and} \quad E_k = F(g^{(k)}, h^{(k)}, r_1^{(k)}, \ldots, r_p^{(k)}). \tag{6}$$

This leads to the following Diophantine equation over the direct product of fields $U_{\mathcal{M}_0}$

$$\epsilon_k = \lambda_0 h_0 g_k + \lambda_0 g_0 h_k. \tag{7}$$

Since the leading coefficients of g_k and h_k are set to be c_g and c_h we can assume that we are looking for (g_k, h_k) such that $\deg(g_k) < d_g = \deg(g_0)$ and $\deg(h_k) < d_h = \deg(h_0)$. Therefore, it is easy to check that Equation (7) admits a unique solution which can be computed by means of Relation (3). (Observe that we have the equality $\epsilon_k = \rho_0 \tau_0 \epsilon_k$ in $U_{\mathcal{M}_0}[y]$.) Finally, the coefficients $r_{1,k}, \ldots, r_{p,k}$ are obtained from Equation (5).

If some E_k becomes null, then the construction succeeds by returning $(g, h) = (g^{(k)}, h^{(k)})$. If no E_k is null, this may be because λ is not *big enough*. To deal with this difficulty, the error E_k should be computed by pseudo-dividing $f - g^{(k)} h^{(k)}$ w.r.t. M and comparing the actual λ used in this pseudo-division with the guessed λ. If the actual λ does not divide the guessed λ, then the construction should be started again with the correct λ.

2 Polynomial gcds over direct products of fields

Assume that the polynomials f_1 and f_2 admit a monic g_{monic} gcd in $L[y]$. The case where this assumption does not hold can be handled by splitting L. We describe now an algorithm which computes $\alpha \in R[x_1, \ldots, x_p]$ and $g, h \in R[x_1, \ldots, x_p][y]$ such that

(1) α is a regular element in U,

(2) g is equal to g_{monic} in $L[y]$ up to a multiplicative constant which is a unit of L,

(3) $\alpha f = gh$ holds in $U[y]$ and therefore in $L[y]$.

The key idea is to compute the *denominator* α before computing g. The computation of α is based on the following remark. Let $r_1 = f_1, r_2 = f_2, \ldots, r_i = q_{i+1}\, \overline{r_{i+1}} + r_{i+2}, \ldots, r_\ell$ be the Euclidean remainder sequence of f_1 and f_2 in $L[y]$ where $r_i = u_i \overline{r_i}$ and $u_i = \mathrm{lc}(r_i)$. With $e_i =$

$d_i - d_{i-1} + 1$ the following equalities are fraction-free: $u_{i+1}^{e_{i+1}} r_i = u_{i+1}^{e_{i+1}-1} q_{i+1} r_{i+1} + u_{i+1}^{e_{i+1}} r_{i+2}$. Therefore, we can choose $\alpha = u_2{}^{e_2} u_3{}^{e_3} \cdots u_\ell{}^{e_\ell} \mod \mathrm{Sat}(T)$. In practice, the degrees of α w.r.t. $t_1, \ldots, t_n$ are smaller than those of g. This is why reconstructing α before g is an efficient approach. We sketch now the main steps of our algorithm.

Step 1 Get an initial guess for the bounds $d_1, \ldots, d_n$ of Theorem 1.1. Get an initial guess N for the number of maximal ideals $\mathcal{M}_0$ that are needed in order to compute α by interpolation. Lastly, initialize a table T that we shall use for storing the history of a polynomial gcd of f_1 and f_2 in $U_{\mathcal{M}_0}[y]$, for every maximal ideal $\mathcal{M}_0$ that we use.

Step 2 Choose a maximal $\mathcal{M}_0$ such that the hypothesis of Section 1 hold.

Step 3 Compute $\alpha_0 \in R_{\mathcal{M}_0}[x_1, \ldots, x_p]$ regular element in $U_{\mathcal{M}_0}$ and $g_0, h_0 \in R_{\mathcal{M}_0}[x_1, \ldots, x_p][y]$ such that g_0 is a gcd of f_1, f_2 in $U_{\mathcal{M}_0}[y]$ and $\alpha_0 f = g_0 h_0$ holds in $U_{\mathcal{M}_0}[y]$. The computation of α_0 is based on the above remark for α.

Step 4 If the history of g_0 matches at least $N - 1$ other gcd computation histories in T then interpolate their α_0's into an α and go to **Step 5** otherwise go to **Step 2**.

Step 5 Apply the construction of Section 1. If it succeeds then return (α, g, h) otherwise revise (i.e. increase) the estimation of $d_1, \ldots, d_n, N$ and go to **Step 2**.

Definition 2.1. We say that $\mathcal{M}_0$ is a

lc-bad prime if one of the leading coefficients $\mathrm{lc}(m_1, x_1), \ldots, \mathrm{lc}(m_p, x_p)$ is zero modulo $\mathcal{M}_0$ or $U_{\mathcal{M}_0}$ is not a product of fields, or one of the leading coefficients $\mathrm{lc}(f_1, y), \mathrm{lc}(f_1, y)$ is not regular modulo $\mathcal{M}_0$,

fail prime if $\mathcal{M}_0$ is not lc-bad but a *subresultant gcd* could not be computed modulo $\mathcal{M}_0$ because a zero-divisor was found,

unlucky prime if $\mathcal{M}_0$ is not a lc-bad or fail prime but the history of the subresultant gcd of f_1, f_2 in $U_{\mathcal{M}_0}[y]$ is different from the history of the subresultant gcd of f_1, f_2 in $U[y]$ (the one we called g_{subres} above),

good prime if $\mathcal{M}_0$ is not a lc-bad prime, nor a fail prime, nor an unlucky prime.

Theorem 2.2. *Assume $\mathcal{M}_0$ is not a lc-bad prime. Then, $\mathcal{M}_0$ is a good prime with a probability one and the subresultant gcd of f_1, f_2 computed for this specialization is the image of g_{subres}. In particular, for the case $R = k[t]$ (i.e. $n = 1$) there is only a finite number of specializations that are not good primes.*

Theorem 2.3. *Assume $\mathcal{M}_0$ is a good prime. Then, the polynomial g_0 (computed in $U_{\mathcal{M}_0}[y]$) divided by $\mathrm{lc}(g_0, y)$ is the image modulo $\mathcal{M}_0$ of the polynomial g_{monic} (computed in $L[y]$).*

References

[ALM99] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *J. Symb. Comp.*, 28(1-2):105–124, 1999.

[DDD85] J. Della Dora, C. Discrescenzo, and D. Duval. About a new method method for computing in algebraic number fields. In *Proc. EUROCAL 85 Vol. 2*, volume 204 of *Lect. Notes in Comp. Sci.*, pages 289–290. Springer-Verlag, 1985.

[El 03] M. El Kahoui. An elementary approach to subresultants theory. *J. Symb. Comp.*, 35:281–292, 2003.

[Enc94] M. J. Encarnación. On a modular algorithm for computing gcds of polynomials over algebraic number fields. In *Proc. ISSAC'94*, pages 58–65. ACM Press, 1994.

[GCL92] K.O. Geddes, S.R. Czapor, and G. Labahn. *Algorithms for Computer Algebra.* Kluver Acadenic Publishers, 1992.

[HM02] M. van Hoeij and M. Monagan. A modular gcd algorithm over number fields presented with multiple extensions. In Teo Mora, editor, *Proc. ISSAC 2002*, pages 109–116. ACM Press, July 2002.

[HM04] M. van Hoeij and M. Monagan. Algorithm for polynomial gcd computation over algebraic function fields. (accepted for ISSAC 2004), 2004.

[LM89] L. Langemyr and S. McCallum. The computation of polynomial greatest common divisors over an algebraic number field. *J. Symbolic Comp*, 8:429–448, 1989.

[Mor99] M. Moreno Maza. On triangular decompositions of algebraic varieties. Technical Report TR 4/99, NAG Ltd, Oxford, UK, 1999. Presented at the MEGA-2000 Conference, Bath, England.

[MR95] M. Moreno Maza and R. Rioboo. Polynomial gcd computations over towers of algebraic extensions. In *Proc. AAECC-11*, pages 365–382. Springer, 1995.

François Boulier
Université Lille 1
59655 Villeneuve d'Ascq
France
boulier@lifl.fr

Marc Moreno Maza
Université Lille 1
&
University of Western Ontario
moreno@orcca.on.ca

Cosmin Oancea
University of Western Ontario
London N6A 5B7
Canada
oancea@orcca.on.ca