

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

François Boulier	Marc Moreno Maza	Cosmin Oancea
Université Lille 1	University of Western Ontario	
France	Canada	
boulier@lifl.fr	moreno@orcca.on.ca	coancea@orcca.on.ca

10 May 2004

Extended Abstract

Let k be an infinite field and let R be an integral domain which is either the ring \mathbb{Z} of integers or the multivariate polynomial ring $k[t_1, \dots, t_n]$. Let $L_0 = K$ be the field of fractions of R . Let $x_1 < \dots < x_p$ be ordered variables and let m_1, \dots, m_p be non-constant polynomials in $R[x_1, \dots, x_p]$. Let i be any integer in the range $1 \dots p$. We assume that the greatest variable occurring in m_i is x_i and that the leading coefficient $\text{lc}(m_i, x_i)$ 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} (that is $L_i = L_{i-1}[x_i]/\langle m_i \rangle$) where the ideal $\langle m_i \rangle$ is assumed to be radical. 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 $L[y]$. Assume that f_1, f_2 admit a monic gcd g_{monic} in $L[y]$.

Let us regard now the set $M = \{m_1, \dots, m_p\}$ as a regular chain in $R[x_1, \dots, x_p]$. We define $U = R[x_1, \dots, x_p]/\text{Sat}(M)$ where $\text{Sat}(M)$ is the saturated ideal of M . 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 $g_{\text{subres}} \in U[y]$ 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 approach is introduced in [MR95].

Monagan and van Hoeij have proposed two modular algorithm 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 $R = k[t_1, \dots, t_n]$ but assumes $p = 1$. Both algorithms are based on the Chinese remaindering algorithm and rational reconstruction.

In this poster, we propose an algorithm which applies to the case where L is not necessarily a field, p may be greater than 1 and $R = k[t_1, \dots, t_n]$. A preliminary implementation shows that our new algorithm can process problems that were out of the scope of the previous algorithms. We rely on a new Henselian construction presented in Theorem 0.1.

Let \mathcal{M}_0 be a maximal ideal of R of the form $\langle t_1 - t_{1,0}, \dots, t_n - t_{n,0} \rangle$. We denote by $R_{\mathcal{M}_0}$ the residue class field R/\mathcal{M}_0 and by $M_0 = \{m_{1,0}, \dots, m_{p,0}\}$ the image of the regular chain M in $R_{\mathcal{M}_0}[x_1, \dots, x_p]$. We assume that no $\text{lc}(m_i, x_i)$ is null modulo \mathcal{M}_0 . Finally, we denote by $U_{\mathcal{M}_0}$ the residue class ring $R_{\mathcal{M}_0}[x_1, \dots, x_p]/\text{Sat}(M_0)$.

Theorem 0.1. *Assume that $\text{Sat}(M_0)$ is radical (as it is the case for $\text{Sat}(M)$) such that $U_{\mathcal{M}_0}$ is a direct product of fields. Let $f \in R[x_1, \dots, x_p][y]$ and f_0 be its image in $R_{\mathcal{M}_0}[x_1, \dots, x_p][y]$. Let $c_g, c_h \in R[x_1, \dots, x_p]$ be units of L such that $\text{lc}(f, y) = c_g c_h$. Let d_1, \dots, d_n be positive integers. Let g_0 and h_0 be polynomials in $R_{\mathcal{M}_0}[x_1, \dots, x_p][y]$ 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 $g_0 h_0$ is equal to f_0 in $U_{\mathcal{M}_0}[y]$, and their leading coefficients $\text{lc}(f_0, y)$ and $\text{lc}(g_0, y)$ 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 gh in $L[y]$,
- (ii) g_0 and h_0 are the respective images of g and h in $U_{\mathcal{M}_0}[y]$,
- (iii) $\text{lc}(g) = c_g$ and $\text{lc}(h) = c_h$,
- (iv) for every $i = 1, \dots, n$ 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 $R[x_1, \dots, x_p][y]$.

Again, 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 . Our new gcd algorithm computes $\alpha \in R[x_1, \dots, x_p]$ and $g, h \in R[x_1, \dots, x_p][y]$ 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 guess the *denominator* α before computing g which avoids the rational reconstruction. The main steps of our algorithm are

- Guess α and the degrees of g, h w.r.t. t_1, \dots, t_n .
- Compute g_0, h_0 modulo some $\mathcal{M}_0 = \langle t_1 - a_1, \dots, t_n - a_n \rangle$.
- Try lifting $\boxed{\alpha f = g_0 h_0 \text{ mod } \mathcal{M}_0, \text{Sat}(T)}$ to $\boxed{\alpha f = gh \text{ mod } \text{Sat}(T)}$ where $f \in \{f_1, f_2\}$.
- If failure, then increase accuracy for α and the degrees.

Our algorithm is probabilistic (in the sense that it may run forever) but succeeds (i.e. terminates in a finite number of steps) with probability one. In particular, in the case of a unique parameter ($n = 1$) there is only a finite number of specifications \mathcal{M}_0 that are not *good* for lifting.

References

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