On Polynomial Gcds over Direct Products of Fields Given by Towers of Simple Extensions

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

Marc Moreno Maza
Cosmin Oancea
University of Western Ontario
London N6A 5B7
Canada
moreno@orcca.on.ca
coancea@orcca.on.ca

July 2004

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 present 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 may not stop but does terminate with *probability one*. Our implementation shows a significant improvement with respect to other methods.

- We want to compute the solutions of $f_1 = f_2 = 0$ where $f_1 = y^2 + (t-1)xy - tx^2$ and $f_2 = y^2 - ty$ for $t < x < y$.
- Their resultant w.r.t. x is $m = t^2x^4 + (-t^3 + t^2)x^3 - t^3x^2$.
- Dividing f_1 w.r.t. f_2

$$\begin{array}{c|c} f_1 & f_2 \\ \hline f_3 & 1 \end{array} \quad \text{where} \quad f_3 = ((t-1)x + t)y - tx^2$$

- The lead. coef. $\mathrm{lc}(f_3)$ is invertible modulo m. Multiplying f_3 (modulo m) by this inverse leads to

$$y + \frac{t-1}{t}\, x^3 + \frac{-t^2 + t - 1}{t}\, x^2$$

- The next division shows that this latter polynomial is a gcd of f_1 and f_2 modulo m. The polynomials (m, f_3) describe the solutions of the input system.

Let $L_0 = K$ be the field of fractions of an integral domain R. ($R = \mathbb{Z}$ or $R = k[t_1, \ldots, t_n]$ for a field k.) Let $x_1 < \cdots < x_p$ be variables.

> **for** $i = 1, \ldots, p$ **repeat**
>
> **let** $m_i \in L_{i-1}[x_i]$ **with** $\mathrm{lc}(m_i, x_i) \in R$ **and** $\langle m_i \rangle_{L_{i-1}[x_i]}$ radical
>
> **define** $L_i = L_{i-1}[x_i]/\langle m_i \rangle$

Define $L = L_p$ and $T = \{m_1, \ldots, m_p\}$. Let $f_1, f_2 \in L[y]$.

Theorem 1 *A Noetherian ring is a direct product of fields iff every nonzero element is either invertible or a non-nilpotent zero-divisor.*

Corollary 1 *L is a direct product of fields.*

Definition 1 *For a commutative ring $\mathbb{A}$ and $f_1, f_2, g \in \mathbb{A}[y]$ the polynomial g is a gcd of f_1 and f_2 if* $\boxed{\langle f_1, f_2 \rangle =_{\mathrm{Fr}(A)[y]} \langle g \rangle}$ *where $\mathrm{Fr}(A)$ is the total ring of fractions of $\mathbb{A}$.*

Corollary 2 *All pair $f_1, f_2 \in L[y]$ admit gcds in the above sense.*

- Assume f_1, f_2 quasi-monic (i.e. $\mathrm{lc}(f_i)$ is regular in L) and assume f_1, f_2 admit a quasi-monic gcd in $L[y]$.
- Their **monic gcd** $g_{\mathrm{monic}} \in L[y]$ can be obtained by applying the *D5 principle* to the *Euclidean Algorithm*. 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 $L = L_1 \oplus L_2$ has been found and the computations continue in $L_1[y]$ and $L_2[y]$. (J. Della Dora and C. Discrescenzo and D. Duval, 1985)
- Let $U = (R[x_1, \ldots, x_p]/\mathrm{Sat}(T))$ where $\mathrm{Sat}(T)$ is the saturated ideal of T. We have $L = \mathrm{Fr}(U)$. The **subresultant gcd** g_{srgcd} of f_1, f_2 in $U[y]$ can be computed by applying the *D5 principle*. That is running 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.

An Example

- Without modular methods, the polynomial g_{monic} is much more expensive to compute than g_{srgcd} (Aubry & Moreno Maza, 1999).
- But g_{srgcd} is not necessarily primitive in $U[y]$ and its expression may be much larger than g_{monic}.
- With $n = 1$, $t = t_1$, $p = 1$, $x_1 = x$ and $m_1 = m$ consider

$$f_1 = ty^{12} + (tx+1)y^7 + (t^2x^2 - 1)y^5 - t^2$$

$$f_2 = y^{10} + (tx^2 + x)y^5 - t$$

$$m = t^3x^3 + t^2x^2 - tx + t^3 - 1.$$

- Then we have

$$\begin{array}{rcl} g_{\text{monic}} & = & y^5 + x + 1/t \\ g_{\text{srgcd}} & = & ((t^6 + 8t^3 - 4t^2)x^2 + (-4t^5 + t^4)x + 7t^4 - 3t^3 - 8t + 4)y^5 \\ & & +(-4t^5 + t^4)x^2 + (4t^4 - 2t^3)x - t^6 + t^2 \end{array}$$

Related Work

Authors	K	T	L	strategy
Langemyr, McCallum, 1989 Encarnaciòn, 1994	$\mathbb{Q}$	$p = 1$	Field	Modular, Subresultant-based
Kalkbrener, 1993	any K	any p	any L	Non-modular, PRS
Moreno Maza, Rioboo, 1995	any $\mathrm{Fr}(R)$ $\mathbb{Q}$ is meant	any p	DP of fields	Non-modular Subresultant-based
Boulier, Lehobey Moreno Maza, 1999	$\mathbb{Q}$	any p	DP of fields	Hensel (+CRA) + Rational Rec.
van Hoeij, Monagan, 2002	$\mathbb{Q}$	any p	Field	CRA + Rational Rec.
van Hoeij, Monagan, 2004	$\mathbb{Q}(t_1, \ldots, t_n)$	$p = 1$	Field	CRA + Rational Rec.
This poster 2004	$\mathbb{Q}(t_1, \ldots, t_n)$	any p	DP of fields	Hensel (+CRA) No Rational Reconstruction

Overview of the Algorithm

- **Assume** R is $\mathbb{Q}[t_1, \ldots, t_n]$ and L may not be a field.
- **Input** $f_1, f_2 \in R[x_1, \ldots, x_p][y]$ are quasi-monic and admit a quasi-monic gcd in $L[y]$.
- **Output** $\alpha \in R[x_1, \ldots, x_p]$ and $g, h \in R[x_1, \ldots, x_p][y]$ such that
  (1) α is a regular element in U,
  (2) g is a quasi-monic gcd of f_1, f_2 in $L[y]$,
  (3) $\alpha f = gh$ holds in $U[y]$ and therefore in $L[y]$.
- **Main steps**
  - Guess α and the degrees of g, h w.r.t. $t_1, \ldots, t_n$.
  - Compute g_0, h_0 modulo some $\mathcal{M}_0 = \langle t_1 - a_1, \ldots, t_n - a_n \rangle$.
  - Try lifting $\boxed{\alpha f = g_0 h_0 \mod \mathcal{M}_0, \mathrm{Sat}(T)}$ to $\boxed{\alpha f = gh \mod \mathrm{Sat}(T)}$ where $f \in \{f_1, f_2\}$.
  - If failure, then increase accuracy for α and the degrees.

- Recall $U = (R[x_1, \ldots, x_p]/\mathrm{Sat}(T))$, the *fraction-free place.*

- 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 $\ell \in \{1, \ldots, p\}$.

$\Longrightarrow$ This leads to the following *key-idea.*

- The *history* of g_{subres} is 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.

- We also store in $\mathrm{history}(g_{\mathrm{subres}})$ events like *regularity-test*, *zero-divisor-found*, ...

- Similarly we define $\mathrm{history}(g_{\mathrm{monic}})$ and observe that $\mathrm{history}(g_{\mathrm{subres}})$ and $\mathrm{history}(g_{\mathrm{monic}})$ coincide.

How to Compute α before g?

- We specialize by maximal ideals $\mathcal{M}_0 = \langle t_1 - a_1, \ldots, t_n - a_n \rangle$ in R such that $U_{\mathcal{M}_0} = (R/\mathcal{M}_0[x_1, \ldots, x_p]/\mathrm{Sat}(T))$ remains a product of fields.
- In practice $\deg(\alpha, t_i) \ll \deg(g, t_i)$ holds for $i = 1, \ldots, n$.
- Hence, the *denominator* α can be reconstructed earlier than g.
- For estimating α we start from the trivial 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 Euclid. rem. sequence in $L[y]$ where $r_i = u_i \overline{r_i}$ and $u_i = \mathrm{lc}(r_i)$.
  - With $e_i = d_i - d_{i-1} + 1$ these 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 $\alpha = {u_2}^{e_2} {u_3}^{e_3} \cdots {u_\ell}^{e_\ell} \mod \mathrm{Sat}(T)$.

△ This *rough estimate* is refined using histories which track inversions.

△ We estimate α by interpolating α_0's which have the same history.

△ A *sub-resultant+CRA* based approach would lead to bigger degrees w.r.t. $t_1, \ldots, t_n$ and thus to a bigger α.

Definition 2 *We say that $\mathcal{M}_0$ is a*

lc-bad prime *if one of the leading coefficients* $\mathrm{lc}(m_1, x_1)$, *. . . ,* $\mathrm{lc}(m_p, x_p)$ *is zero modulo $\mathcal{M}_0$ or $L_{\mathcal{M}_0}$ 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 quasi-monic 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_{srgcd} above),*

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

Theorem 2 *Assume that k is an infinite field and let $\mathcal{M}_0$ a specialization. Then, $\mathcal{M}_0$ is a good prime with* **probability one** *and the subresultant gcd of f_1, f_2 computed for this specialization is the image of g_{srgcd}. 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 3 *Assume that k is an infinite field and that $\mathcal{M}_0$ is a good prime. Then, the polynomial g_0 (coomputed in $U_{\mathcal{M}_0}[y]$) is the image modulo $\mathcal{M}_0$ of the polynomial g_{monic} (coomputed in $L[y]$).*

We rely on the work of El Kahoui *An elementary approach to sub-resultant theory* (JSC, 2003) which provides a *Block Structure Theorem* over non-integral domains.

Lifting a Modular Factorization (I)

- Let $f \in R[x_1, \ldots, x_p][y]$ with image f_0 in $R_{\mathcal{M}_0}[x_1, \ldots, x_p][y]$.
- Let $g_0, h_0 \in R_{\mathcal{M}_0}[x_1, \ldots, x_p][y]$ such that $f_0 = g_0 h_0$ holds in $U_{\mathcal{M}_0}[y]$, the polynomials g_0 and h_0 are relatively prime in $U_{\mathcal{M}_0}[y]$ and $\mathrm{lc}(f_0, y)$ and $\mathrm{lc}(g_0, y)$ are units in $U_{\mathcal{M}_0}$.
- We look for $f, g \in R[x_1, \ldots, x_p][y]$ such that $f = gh$ in $L[y]$. That is, there exists $\lambda \in R$ and $r_1, \ldots, r_p \in R[x_1, \ldots, x_p][y]$ such that
$$\boxed{\lambda\,(f - g\,h) = r_1 m_1 + \cdots + r_p m_p.}$$
- In our case $\mathrm{lc}(g)$ and $\mathrm{lc}(h)$ can be set in advance.
- In addition we assume to have *guesses* for λ and for $d_1, \ldots, d_n$ degree bounds in $t_1, \ldots, t_n$ for f, g.
- The lifting procedure may fail if the guess λ is wrong but it will correct it for a next *try*.
- Similarly, the algorithm and histories refine $\alpha, d_1, \ldots, d_n$.

- Since $f_0 = g_0 h_0$ holds in $U_{\mathcal{M}_0}[y]$ we have
$\boxed{\lambda_0\,(f_0 - g_0\,h_0) = r_{1,0} m_{1,0} + \cdots + r_{p,0} m_{p,0}.}$
- Since g_0 and h_0 are relatively prime in $U_{\mathcal{M}_0}[y]$ we have
$\boxed{\sigma_0 g_0 + \pi_0 h_0 = \rho_0}$ and $\boxed{\rho_0 \tau_0 = 1 + \theta_{1,0} m_{1,0} + \cdots + \theta_{p,0} m_{p,0}.}$
- We define $\boxed{F(u, v, w_1, \ldots, w_p) = \lambda(f - u\,v) - w_1 m_1 - \cdots - w_p m_p.}$
- See (Geddes, Czapor, Labahn, 1992) for related constructions.
- Restricting here to $n = 1$, considering $(q = t_1 - t_{1,0})$-expansions
$\boxed{\epsilon_k = \lambda_0 h_0 g_k + \lambda_0 g_0 h_k + r_{1,k} m_{1,0} + \ldots + r_{p,k} m_{p,0}}$ where
$\boxed{\epsilon_k = \mathrm{eval}(\frac{E_k}{q^k}, t_1 = t_{1,0})}$ and $\boxed{E_k = F(g^{(k)}, h^{(k)}, r_1^{(k)}, \ldots, r_p^{(k)})}$
- This leads to $\boxed{\epsilon_k = \lambda_0 h_0 g_k + \lambda_0 g_0 h_k}$ over the direct product of fields $U_{\mathcal{M}_0}$ which can be solved uniquely.

- We have **not implemented yet** modular methods for the coefficients. That is, currently, every computation is over $\mathbb{Q}$.
- Our current Hensel lifting implementation works in $R[x_1, \ldots, x_p][y]$ and computes the $r_1, \ldots, r_p$ whereas one **could work directly** in $U_{\mathcal{M}_0}[y]$.

$$
\begin{array}{lllll}
f_1 & = & g(y^a x + txy^{a-1} + tx^a + t^2) \mod m, & g & = & y^2 + xy + t \\
f_2 & = & g(y^a x - txy^{a-1} + tx^a + t) \mod m, & m & = & x^a + n(x+t)
\end{array}
$$

a	New approach	sub-resultants
6	7.5	3
8	39	46
10	151	390
12	572	2375
14	1643	$+\infty$

We have other data sets confirming these results.

- $\triangle$ Assume f_1, f_2 *do not admit* a quasi-monic gcd. Then, the computation of a g_0 (modulo a specialization $\mathcal{M}_0$) will hit a zero-divisor with *probability one*.

$\Longrightarrow$ L **must** be decomposed and histories will raise which polynomial f in T must be factorized. Then, one of the modular factorizations of f is *lifted* by our Hensel lifting procedure!

- $\triangle$ We have presented here a first modular method for computing polynomial gcds over a direct product of fields given by multiple extensions and with transcendental quantities $(t_1, \ldots, t_n)$. If α is small, the cost of our algorithm is essentially that of the lifting!

- $\triangle$ Our preliminary implementation provides already a significant performance improvement w.r.t. the sub-resultant based approach. This preliminary implementation does not reduce yet computations over $\mathbb{Q}$ to over $\mathbb{Z}/p\mathbb{Z}$. Once this is implemented, performances should improve greatly!