JTN 2015
Universidad de Valladolid
June 29-July 3, 2015

Local computation of resultants

Enric Nart

Universitat Autònoma de Barcelona, nart@mat.uab.cat

Let A be a Dedekind domain and let v be the valuation associated with a non-zero prime ideal $\mathfrak{m}$ of A.

We present a routine for the computation of the v-value of the resultant of two polynomials $f,g \in A[x]$, which does not require the computation of the resultant $\mathrm{Res}(f,g)$ itself. This may be useful in cases where the computation of $\mathrm{Res}(f,g)$ is inefficient because the polynomials have a large degree or very large coefficients.

The results appeared in [3].

The algorithm consists of a simultaneous application of the Montes algorithm [1, 2] to $f(x)$ and $g(x)$, and the accumulation of certain partial values of resultants, $\mathrm{Res}_{\mathbf{t}}(f,g)$, for all the types $\mathbf{t}$ considered along the flow of the algorithm, such that $\mathbf{t}$ divides both polynomials $f(x)$ and $g(x)$.

We obtain the following complexity estimation.

Theorem. *If the residue class field $\mathbb{F} = A/\mathfrak{m}$ has q elements, the computation of $v(\mathrm{Res}(f,g))$ requires*

$$O\left(n^{2+\varepsilon} + n^{1+\varepsilon}\delta \log q + n^{1+\varepsilon}\delta^{2+\varepsilon}\right)$$

operations in $\mathbb{F}$, where $n = \max\{\deg f, \deg g\}$, $\delta = v(\mathrm{Res}(f,g))$.

If $\mathbb{F}$ is small, the computation requires $O\left(n^{2+\varepsilon} + n^{1+\varepsilon}\delta^{2+\varepsilon}\right)$ word operations.

We have implemented our routine in the case $A = \mathbb{Z}$ and $v = v_p$ the p-adic valuation determined by a prime number p. It is included in the Magma package `+Ideals.m`. We present some numerical tests which have been done in a Linux server, with two Intel Quad Core processors, running at 3.0 Ghz, with 32Gb of RAM memory. Times are expressed in seconds.

We compare running times of our routine (abbreviated as `pRes` in the tables), with the `naive` routine that first computes $\mathrm{Res}(f,g)$, and then its p-valuation.

Example 1. Let $p > 5$ be a prime number, m a positive integer, $m < p/2$, and

$$f(x) = \left(x + p + p^2 + \cdots + p^{20}\right)^{10m} + p^{200m+1}.$$
$$g(x) = g_0(x)g_0(x+2)\cdots g_0(x+2(m-1)) + 2p^{110m}, \qquad g_0(x) := x^{10} + 2p^{11}.$$

p	$\deg f = \deg g$	$v_p(\mathrm{Res}(f,g))$	`pRes`	`naive`
7	30	300	0.01	0.94
11	50	500	0.00	19.58
23	100	1000	0.01	1060.03
31	150	1500	0.01	8433.39
43	200	2000	0.03	38430.25
101	500	5000	0.27	$>$ 24 hours

Example 2. Let $p > 3$ be a prime number. Consider $E_1(x) := x^2 + p$ and:

$$
\begin{aligned}
E_2(x) &= E_1(x)^2 + (p-1)p^3x \\
E_3(x) &= E_2(x)^3 + p^{11} \\
E_4(x) &= E_3(x)^3 + p^{29}xE_2(x) \\
E_5(x) &= E_4(x)^2 + (p-1)p^{42}xE_1(x)E_3(x)^2 \\
E_6(x) &= E_5(x)^2 + p^{88}xE_3(x)E_4(x) \\
E_7(x) &= E_6(x)^3 + p^{295}E_2(x)E_4(x)E_5(x) \\
E_8(x) &= E_7(x)^2 + (p-1)p^{632}xE_1(x)E_2(x)^2E_3(x)^2E_6(x)
\end{aligned}
$$

p	i	j	$v_p(\mathrm{Res}(E_i, E_j))$	`pRes`	`naive`
5	5	6	9557	0.04	0.23
5	5	7	28671	0.14	2.70
5	5	8	57342	0.61	13.76
5	6	7	57343	0.15	13.11
5	6	8	114686	0.67	66.12
5	7	8	344059	0.83	885.89
101	5	6	9557	0.05	1.95
101	5	7	28671	0.22	28.11
101	5	8	57342	1.12	150.30
101	6	7	57343	0.25	141.52
101	6	8	114686	1.31	746.78
101	7	8	344059	1.60	9335.33

References

[1] J. Guàrdia, J. Montes, E. Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, Journal de Théorie des Nombres de Bordeaux **23** (2011), no. 3, 667–696.

[2] J. Guàrdia, J. Montes, E. Nart, *Newton polygons of higher order in algebraic number theory*, Transactions of the American Mathematical Society **364** (2012), no. 1, 361–416.

[3] E. Nart, *Local computation of differents and discriminants*, Mathematics of Computation 83 (2014), no 287, 1513–1534.