ACM Communications in Computer Algebra, Vol 43, No. 3, Issue 181, September 2012

An Efficient Algorithm to Factorize Sparse Bivariate Polynomials over the Rationals *

Wenyuan Wu[1], Jingwei Chen[2], Yong Feng[1]
[1]Chongqing Institute of Green and Intelligent Technology, CAS, China
[2]Chengdu Institute of Computer Applications, CAS, China
wuwenyuan@cigit.ac.cn,velen.chan@163.com,yongfeng@cigit.ac.cn

Polynomial factorization is one of the central problems and also a successful story in computer algebra. In this poster, we give a summary of an algorithm, recently presented in the authors' manuscript [5], that uses both symbolic and numeric methods to exactly compute the irreducible factorization in $\mathbb{Z}[x, y]$, and therefore in $\mathbb{Q}[x, y]$, of any bivariate polynomial satisfying

Hypothesis. On $f \in \mathbb{Z}[x, y]$ and its *initial factors*, we assume that (i) f is squarefree, non-constant and monic in x; (ii) f has no univariate factors; (iii) the initial factors of f are mutually coprime.

There are a large number of algorithms to factorize sparse polynomials, such as probabilistic algorithm [6], supersparse (lacunary) algorithm [3], polytope method [1, 4, 2], etc. Our algorithm can be seen as a polytope method and is based on the *generalized Hensel lifting*, which preserves the sparsity, and a numerical combination before lifting.

We now sketch the algorithm. To factorize $f \in \mathbb{Z}[x, y]$ satisfying the hypothesis, firstly we factorize its *Newton polynomial* which essentially is a univariate polynomial; secondly we combine these factors to the right initial factors using a numerical method; lastly we lift the initial factors to the irreducible factors of f over $\mathbb{Z}$ without usual expression swell.

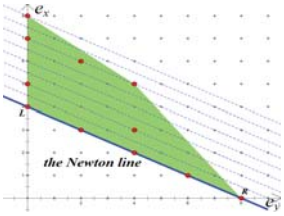

Figure 1: The polytope and the Newton line

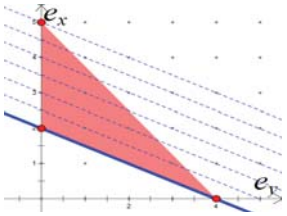

Figure 2: Lifting for G_2

Note that it is different from classical methods that we perform the combination step before the lifting step. We give a brief example here. Let f have two irreducible factors $G_1 = x^4 + 2\,x^2y + y^2 + 2\,y^3$ and $G_2 = x^4 - 4\,y^2 + 5\,y^5$. We first factorize its Newton polynomial $f^{(0)} = -4\,y^4 - 8\,x^2y^3 + 2\,x^6y - 3\,x^4y^2 + x^8$ (Each term of $f^{(0)}$ lies on the *Newton line*, i.e. LR in Fig. 1.) in $\mathbb{Z}[x, \hat{y}]$ as $g_1 \cdot g_2 \cdot g_3 \triangleq (x^2 + \hat{y}^2)^2 \cdot (x^2 + 2\,\hat{y}^2) \cdot (x^2 - 2\,\hat{y}^2)$, where $\hat{y} = y^{1/2}$. However, the initial

*This work was partially supported by NKBRPC (2011CB302400) and NSFC (11001040, 11171053).

factors here are $G_1^{(0)} = x^4 + 2\,x^2y + y^2$ and $G_2^{(0)} = x^4 - 4\,y^2$, respectively. Thus there exists a unique vector $\mu_i = (\mu_{j,i}) \in \{0,1\}^3$ such that $G_i^{(0)} = \prod_{j=1}^3 g_j^{\mu_{j,i}}$ for $i = 1, 2$, for instance $G_2^{(0)} = g_1^0 \cdot g_2^1 \cdot g_3^1$. After linearization by taking natural logarithm, we have $\mathrm{Ln}\, G_i^{(0)} = \sum_{j=1}^3 \mu_{j,i} \mathrm{Ln}\, g_j$. By uniformly random choosing some evaluation points, we can construct a numerical matrix equation $AU = B$, from which we get all $\mu_{j,i}$'s by rounding the solution U. Then we use the generalized Hensel lifting to lift each initial factor by $y^{1/2}$ in each step until the factorization completes (see Fig. 2).

We prove that the combination is correct under some error control conditions and that the generalized Hensel lifting always returns the irreducible factors of f in $\mathbb{Z}[x, y]$ provided that its initial factors are given. Moreover, the sparsity of the input polynomial is preserved during lifting.

From the complexity point of view, given a bivariate polynomial f in $\mathbb{Q}[x, y]$ satisfying the hypothesis, our algorithm reduces the computation of the irreducible factors of f over $\mathbb{Q}$ to the computation of univariate polynomials factorization with degree at most d_x over $\mathbb{Q}$ in $\tilde{\mathcal{O}}(Td_xd_y + s^\omega)$ arithmetic operations, where T is the number of non-zero terms of f, d_x and d_y are the degrees in x and y respectively, s is the number of the irreducible factors in $\mathbb{Q}[x, \hat{y}]$ of the Newton polynomial of f, and ω is the exponent of matrix multiplication. Note that our algorithm is probabilistic.

In Table 1, we compare some experimental results for the Maple's built-in function `factor` and our implementation `BiFactor` of our algorithm in Maple 14, where all univariate factorizations are directly computed by `factor`. All tests were run on Athlon 7750 processor (2.70 GHz) with 2GB memory. Time is shown in seconds. All test polynomials are of total degree d and constructed by multiplying two random polynomials with total degree $d/2$.

d	d_x	d_y	T	$time_{Maple}$	$time_{BiFactor}$
50	46	29	135	0.281	0.157
100	95	89	143	2.125	0.109
200	156	152	144	7.578	0.235
400	335	305	144	87.297	0.218
800	580	595	144	943.094	0.422
50	39	50	705	0.532	0.437
100	100	65	827	4.282	1.468
200	193	179	890	50.75	2.156
400	306	302	746	208.515	2.110
800	784	613	912	10301.844	4.578

Table 1: Experimental results

Our future work is to weaken the hypothesis and to generalize the method to polynomials with variables more than two.

References

[1] F. Abu Salem, S. Gao, and A. Lauder. Factoring polynomials via polytopes. In *ISSAC '04*, pages 4–11, Santander, Spain, 2004.

[2] J. Berthomieu and G. Lecerf. Reduction of bivariate polynomials from convex-dense to dense, with application to factorizations. *Mathematics of Computation*, 81(279):1799–1821, 2012.

[3] E. Kaltofen and P. Koiran. On the complexity of factoring bivariate supersparse (lacunary) polynomials. In *ISSAC '05*, pages 208–215, Beijing, China, 2005.

[4] M. Weimann. A lifting and recombination algorithm for rational factorization of sparse polynomials. *Journal of Complexity*, 26(6):608–628, 2010.

[5] W. Wu, J. Chen, and Y. Feng. Sparse bivariate polynomial factorization, 2011. Availabel at `https://sites.google.com/site/jingweichen84/publications`

[6] R. Zippel. *Probabilistic Algorithms for Sparse Polynomials*. PhD thesis, Massachusetts Institute of Technology, 1979.