Polynomial Factorization over Algebraic Function Fields

Seyed Mohammad Mahdi Javadi, Michael Monagan

sjavadi@cs.sfu.ca, mmonagan@cecm.sfu.ca

The Problem

The problem of factoring multivariate polynomials over a field is one of the most challenging problems in *computer algebra*. We are specially interested in factorization over algebraic number and function fields.

An **algebraic number** is a root of a univariate polynomial with integer coefficients.

E.g. $\alpha = \sqrt{2}$ is an algebraic number which is a root of $m_\alpha(z) = z^2 - 2$.

An **algebraic function** is a root of a univariate polynomial in $\mathbb{Z}(t_1, t_2, \ldots, t_k)[z]$.

E.g. $\alpha = \sqrt{t_1 + \sqrt{2}}$ is an algebraic function which is a root of $m_\alpha(z) = z^4 - (2t_1)z^2 + t_1^2 - 2$.

If $m_\alpha(z)$ is *monic* and irreducible, it is called the **minimal polynomial** for α.

Given algebraic functions $\alpha_1, \ldots, \alpha_r$ in parameters $t_1, \ldots, t_k$ we want to compute over the **algebraic function field** $L = \mathbb{Q}(t_1, \ldots, t_k)(\alpha_1, \ldots, \alpha_r)$. In this poster we want to factor a polynomial $f \in L[x_1, \ldots, x_v]$ into irreducible factors to obtain $f = l \times f_1 \times f_2 \times \cdots \times f_n$ where $l = \mathrm{lc}_{x_1,\ldots,x_v}(f)$ is the leading coefficient of f and each f_i is a monic irreducible polynomial.

Example 1. *For* $\alpha = \sqrt{1-t^2}$*, the algebraic function field is* $L = \mathbb{Q}(t)(\sqrt{1-t^2})$*. Factoring* $f = x^5 - \alpha x^2 y + x^2 + 3\alpha x^4 y - 3xy^2 + 3xy^2t^2 + 3\alpha xy - x^3 + \alpha y - 1$ *over* L *results in*

$$f = (x^2 + 3\alpha xy - 1) \times (x^3 - \alpha y + 1).$$

Trager's Algorithm

One way to factor $f \in L[x_1, \ldots, x_v]$ is to use **Trager's algorithm**:

$f \in L[x_1, \ldots, x_v]$

$\downarrow$

$h = \mathrm{norm}(f) \in \mathbb{Q}(t_1, \ldots, t_k)[x_1, \ldots, x_v]$

$\downarrow$

Factor $h = h_1 \times h_2 \times \cdots \times h_n$

$\uparrow$

$f_i = \gcd(f, h_i) \in L[x_1, \ldots, x_v]$

$\uparrow$

$f \sim f_1 \times f_2 \times \cdots \times f_n$

Motivation

The following problem was given to us by Jürgen Gerhard [2]:

$$f = \frac{19}{2}c_4^2 - \sqrt{11}\sqrt{5}\sqrt{2}c_5c_4 - 2\sqrt{5}c_1c_2 - 6\sqrt{2}c_3c_4 + \frac{3}{2}c_0^2 + \frac{23}{2}c_5^2 +$$
$$\frac{7}{2}c_1^2 - \sqrt{7}\sqrt{3}\sqrt{2}c_3c_2 + \frac{11}{2}c_2^2 - \sqrt{3}\sqrt{2}c_0c_1 + \frac{15}{2}c_3^2 - \frac{10681741}{1985}.$$

Here $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11})$ is a number field and $f \in L[c_0, \ldots, c_5]$. The norm of f is degree 64 in $c_0, c_1, c_2, c_3, c_4, c_5$ and has about 3 million terms and the integers in the rational coefficients have over 200 digits so it is not easy to compute $\mathrm{norm}(f)$ let alone factor it!!

Observation: If we evaluate f at $(c_1 = 1, c_2 = 2, c_3 = 3, c_4 = 4, c_5 = 5)$ the resulting polynomial can be proven irreducible using Trager's algorithm. In general we have:

Theorem 1. *Let* $f \in L[x_1, \ldots, x_v]$ *and* $\beta \in \mathbb{Z}^{k+v-1}$ *be an evaluation point for all the parameters and variables except* x_1*. If* $\mathrm{lc}_{x_1}(f)(\beta) \neq 0$ *then*

$$f(x_1, \beta) \in L(\beta)[x_1] \text{ is irreducible} \Rightarrow f \text{ is irreducible.}$$

Efactor: Our New Algorithm

Our idea is to use polynomial evaluation and interpolation using **Hensel lifting**. To factor a univariate polynomial we will use Trager's algorithm. Things to be done:

- In order to use Hensel lifting we need to determine the true leading coefficient of each factor f_i.
- How to avoid the fractions in $\mathbb{Q}$ and fractions in the parameters $t_1, \ldots, t_k$ when doing Hensel lifting? Because doing arithmetic with fractions is expensive.

To find the leading coefficient of each factor we will use a trick similar to Wang's idea [3] to factoring polynomials over $\mathbb{Q}$.

Example 2. *Let* $\alpha = \sqrt{t}$ *and*

$$f = \left(-ty^2\alpha + 2y^3 + 3t^2 - t\alpha - 6y\alpha + 2y\right)x^3 + (4y - 2t\alpha)x^2 + \left(y^2 - 3\alpha + 1\right)x + 2.$$

For evaluation point $\beta = (t = 5, y = 7)$ *using Trager's algorithm we get:*

$$f(\beta) = (775 - 292\alpha)\left(x^2 + \frac{14}{71} + \frac{5}{71}\alpha\right)\left(x + \frac{20}{491} + \frac{6}{2455}\alpha\right)$$

The denominators are $d_1 = 71$ *and* $d_2 = 491$*. We factor* $lc_x(f)$ *recursively:*

$$lc_x(f) = l_1 \times l_2 = (y^2 - 3\alpha + 1)(2y - t\alpha)$$

We compute

$$\frac{1}{l_1(\beta)} = \frac{10}{491} + \frac{3}{2455}\alpha \quad \text{and} \quad \frac{1}{l_2(\beta)} = \frac{14}{71} + \frac{5}{71}\alpha.$$

We can see that l_1 *must be the leading coefficient of* f_2 *and* l_2 *must be the leading coefficient of* f_1*.*

To avoid fractions in $\mathbb{Q}$, we will do Hensel lifting modulo a machine prime. To lift the integer coefficients of each factor, we use a new algorithm called **Sparse p-adic Lifting**:

$f \equiv f_1 \times f_2 \bmod p$ and $e = f - f_1 \times f_2$

$\Downarrow$

Find σ_1, σ_2: $f \equiv (f_1 + \sigma_1 p) \times (f_2 + \sigma_2 p) \bmod p \Rightarrow \frac{e}{p} \equiv f_1\sigma_2 + f_2\sigma_1$

$\Downarrow$

σ_1 and σ_2 have the same terms as f_1 and f_2 respectively w.h.p.

$\Downarrow$

Solve the linear system obtained from $\frac{e}{p} \equiv f_1\sigma_2 + f_2\sigma_1$ with unknown coefficients for σ_1 and σ_2

$\Downarrow$

Update $f_1 := f_1 + \sigma_1 p$ and $f_2 := f_2 + \sigma_2 p \Rightarrow f \equiv f_1 \times f_2 \bmod p$

Algorithm Efactor:

1 Factor the leading coefficient of the input polynomial f recursively.

2 Find a random evaluation point β for every parameter and variable except the main variable x_1.

3 Factor $f(\beta)$ (univariate) using Trager's algorithm.

4 Find the true leading coefficient of each univariate factor.

5 Use Hensel Lifting modulo a machine prime p.

6 Use sparse p-adic lifting to lift the integer coefficients.

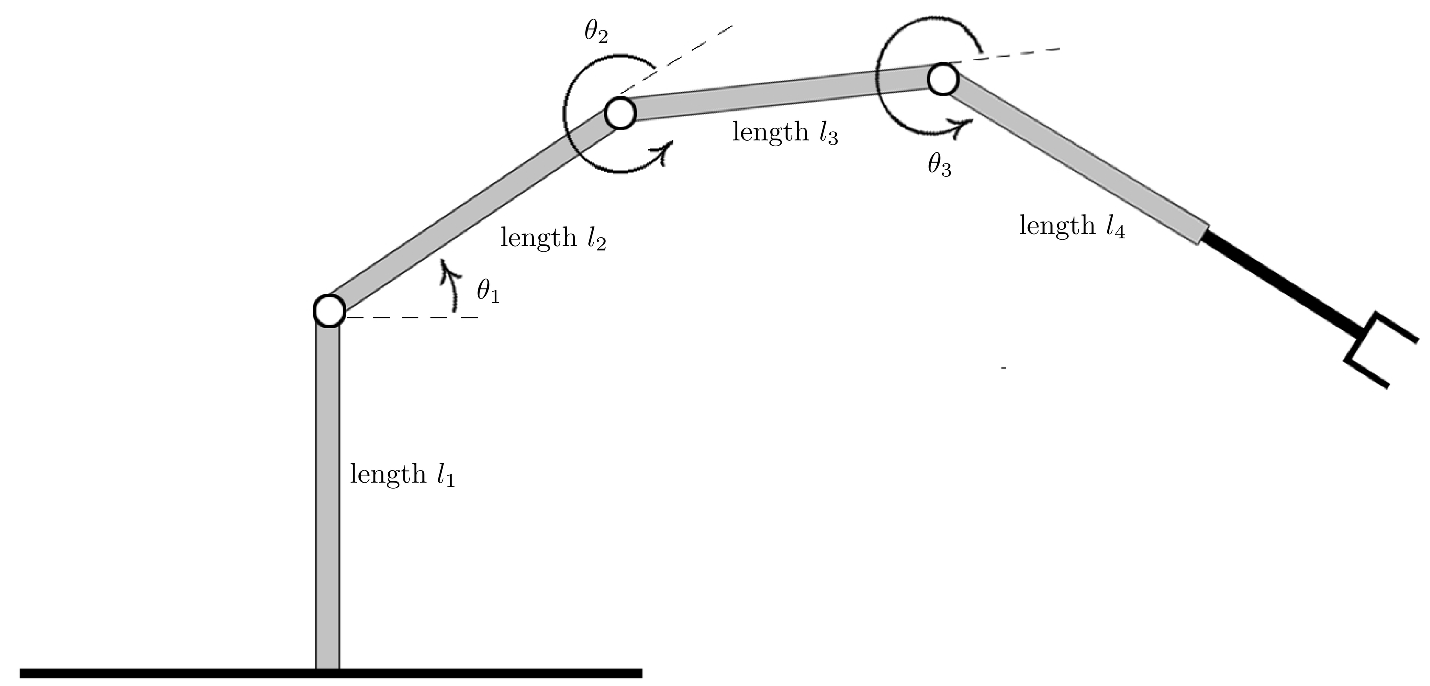
Benchmarks

#	n	r	k	d	$\#f$	Trager	Efactor	GCD
1	2	2	1	17	6408	5500	259.91	47.47
2	2	2	1	22	12008	37800	296.74	56.90
3	2	2	2	10	34	120	0.22	0.16
4	2	2	2	12	34	571	0.31	0.19
5	3	2	2	10	69	5953	0.27	0.29
6	6	5	0	4	46	> 50000	88.43	1.93
7	5	2	1	10	17052	> 50000	58.41	57.75
8	1	1	2	102	928	16427	72.10	7.71

Table 1: Timings (in CPU seconds)

Applications

Polynomial factorization has many applications. It is especially used for solving systems of polynomial equations. Another application of factorization is in coding theory for developing error-correcting codes. Here is an example from robotics:



This picture is taken from [1]. Here l_1, l_2, l_3 and l_4 are variables, $c_1 = \cos(\theta_1), c_2 = \cos(\theta_2)$ and $c_3 = \cos(\theta_3)$ are parameters and $s_1 = \sqrt{1-c_1^2}, s_2 = \sqrt{1-c_2^2}$ and $s_3 = \sqrt{1-c_3^2}$ are the field extensions. The algebraic function field is $L = \mathbb{Q}(c_1, c_2, c_3)(s_1, s_2, s_3)$.

References

[1] D. A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[2] Jürgen Gerhard and Ilias S. Kotsireas. Private communication.

[3] Paul S. Wang. An improved multivariate polynomial factorization algorithm. *Math. Comp.*, 32(144):1215–1231, 1978.