A new black box algorithm for factoring multivariate polynomials in Maple

Tian Chen and Michael Monagan
tca71@sfu.ca, mmonagan@sfu.ca
Department of Mathematics, Simon Fraser University, Canada

Abstract

We have designed and implemented a new algorithm for factoring a multivariate polynomial $f \in \mathbb{Z}[x_1, \cdots, x_n]$ represented by a black box [1, 2]. The black box representation allows one to represent much larger polynomials than can be represented in the standard (expanded) representation. It was first introduced in Computer Algebra by Kaltofen and Trager [4] in 1990.

A black box for a polynomial $f(x_1, \cdots, x_n)$ is a computer program that takes as input an evaluation point $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n$ for the variables $x_1, \cdots, x_n$ and outputs $f(\boldsymbol{\alpha})$. In Maple, we represent a black box as a Maple procedure.

Our new algorithm outperforms the previous best black box factorization algorithm of Rubinfeld and Zippel [3] because it requires fewer probes to the black box than Rubinfeld and Zippel's algorithm and it uses a modular black box to avoid multiprecision arithmetic.

We have implemented our algorithm in Maple with several major subroutines in C. With the help of Dr. Juergen Gerhard of Maplesoft, our software is being integrated into Maple's `factor` command and is expected to be released in Maple 2026. One application of our algorithm is to factor the determinant of a matrix A which has multivariate polynomial entries. A new option is expected to appear in the `LinearAlgebra` package to use our algorithm when computing $\det(A)$.

For the talk we shall present a description of our algorithm, a timing benchmark, and give a code demo and show how the user can create a black box as an input and call the `factor` command.

References

[1] T. Chen and M. Monagan. A new black box factorization algorithm - the non-monic case. In Proceedings of ISSAC 2023. ACM (2023)

[2] T. Chen. Sparse Hensel lifting algorithms for multivariate polynomial factorization. PhD Thesis (2024)

[3] R. Rubinfeld and R. E. Zippel. A new modular interpolation algorithm for factoring multivariate polynomials. In Proceedings of Algorithmic Number Theory, First International Symposium, ANTS-I (1994)

[4] Kaltofen E., Trager, B.M.: Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators. *J. Symb. Cmpt.* **9**(3), 301–320. Elsevier (1990)