Factoring a Multivariate Polynomial Represented by a Black Box – A Maple to C Implementation

Tian Chen and Michael Monagan

Department of Mathematics, Simon Fraser University,
British Columbia, Canada

The black box representation of a polynomial $f \in \mathbb{Z}[x_1, ..., x_n]$

Input: A prime p, $\boldsymbol{\alpha} \in \mathbb{Z}_p^n$
Output: $f(\boldsymbol{\alpha})$ mod p

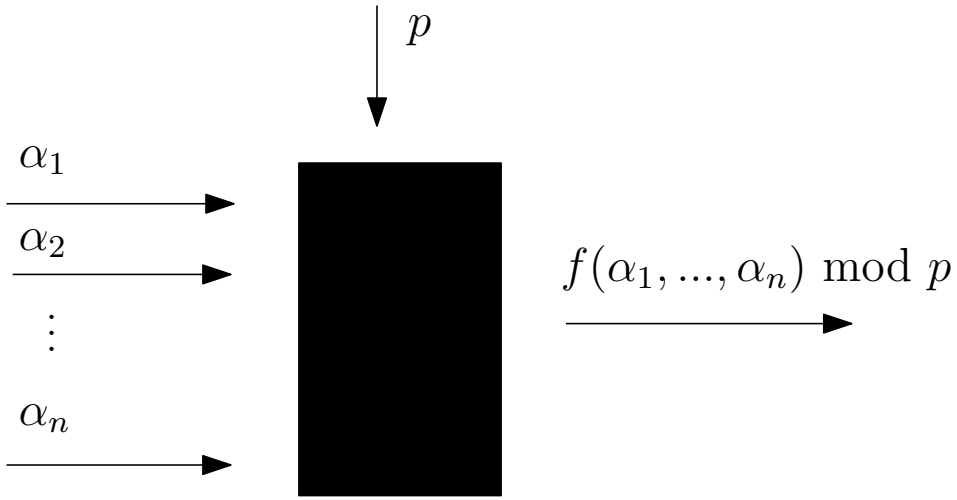
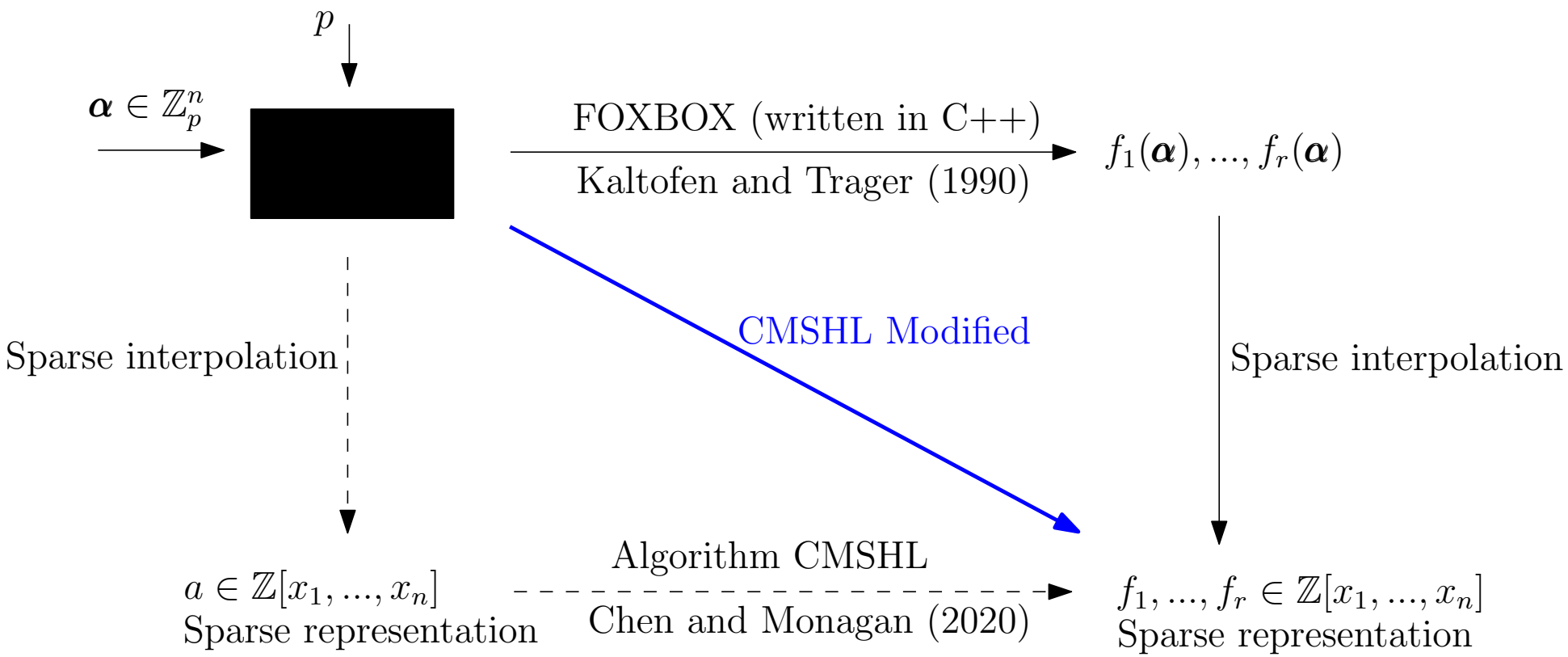


Figure: The black box representation of $f \in \mathbb{Z}[x_1, ..., x_n]$.

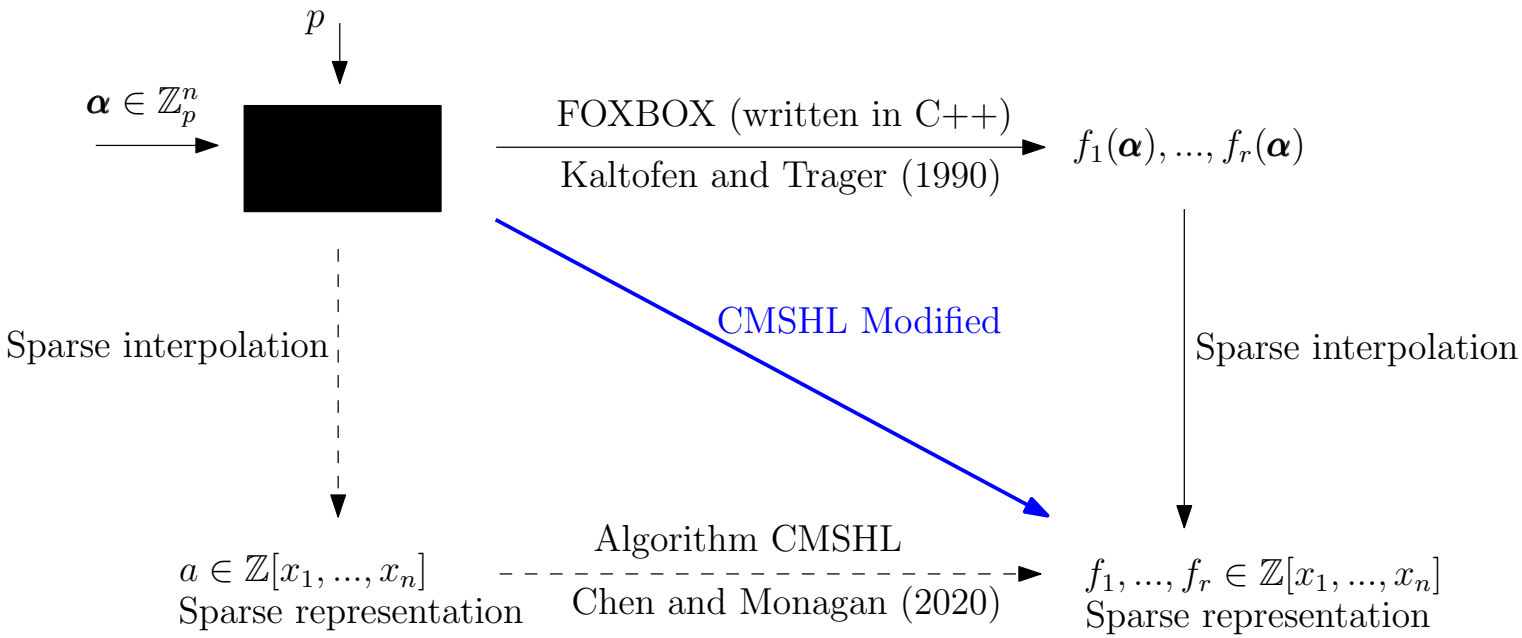
E.g. Let A be a matrix with multivariate polynomial entries.
We represent $\det(A)$ as a black box procedure $\mathbf{B}(\boldsymbol{\alpha}, p)$.

Black box representation is space efficient.

Factoring a multivariate polynomial $a \in \mathbb{Z}[x_1, ..., x_n]$



Factoring a multivariate polynomial $a \in \mathbb{Z}[x_1, ..., x_n]$



- Diaz and Kaltofen (1998): FOXBOX written in C++
- Lee (2001): PROTOBOX written entirely in Maple
- Our new approach:
  - Maple to C (subroutines in C to speed up the computation)
  - Computes directly from the black box to the factors in sparse representation
  - Extended algorithm CMSHL [Chen and Monagan (2020)] to multifactors

Outline

- Background/Motivation
- Analysis: How many probes to the blackbox?
- Implementation Details
- Code Demo
- Current and Future Work

How many probes to the black box for each approach?

- Method I: Obtain evaluations of the factors, and perform sparse interpolation [Kaltofen and Tragar (1990)].

  $O(nd_1 d_{\max} \# f_{\max})$ probes of $\mathbf{B}$ using Zippel's sparse interpolation, plus $O(nd_{\max} \# f_{\max})$ times the cost of univariate polynomial factorization.

How many probes to the black box for each approach?

- Method I: Obtain evaluations of the factors, and perform sparse interpolation [Kaltofen and Tragar (1990)].

  $O(nd_1 d_{\max} \# f_{\max})$ probes of $\mathbf{B}$ using Zippel's sparse interpolation, plus $O(nd_{\max} \# f_{\max})$ times the cost of univariate polynomial factorization.

- Method II: Modified CMSHL [Chen and Monagan (2020)].

  $O(nd_1 d_{\max} s)$ probes of $\mathbf{B}$, to get bi-variate images of a.
  Total cost is:
  $O\left((n-2)\left(s_{\max} d_{\max}\left(\sum_{i=1}^{r} \# f_i + d_1^2 + d_1 d_{\max}\right) + s_{\max} d_1 d_{\max} C(\text{probe } \mathbf{B})\right)\right)$.

How many probes to the black box for each approach?

- Method I: Obtain evaluations of the factors, and perform sparse interpolation [Kaltofen and Tragar (1990)].

  $O(nd_1 d_{\max} \# f_{\max})$ probes of $\mathbf{B}$ using Zippel's sparse interpolation, plus $O(nd_{\max} \# f_{\max})$ times the cost of univariate polynomial factorization.

- Method II: Modified CMSHL [Chen and Monagan (2020)].

  $O(nd_1 d_{\max} s)$ probes of $\mathbf{B}$, to get bi-variate images of a.
  Total cost is:
  $O\left((n-2)\left(s_{\max} d_{\max}\left(\sum_{i=1}^{r} \# f_i + d_1^2 + d_1 d_{\max}\right) + s_{\max} d_1 d_{\max} C(\text{probe } \mathbf{B})\right)\right)$.

How many probes to the black box for each approach?

- Method I: Obtain evaluations of the factors, and perform sparse interpolation [Kaltofen and Tragar (1990)].

  $O(nd_1 d_{\max} \# f_{\max})$ probes of $\mathbf{B}$ using Zippel's sparse interpolation, plus $O(nd_{\max} \# f_{\max})$ times the cost of univariate polynomial factorization.

- Method II: Modified CMSHL [Chen and Monagan (2020)].

  $O(nd_1 d_{\max} s)$ probes of $\mathbf{B}$, to get bi-variate images of a.
  Total cost is:
  $O\left((n-2)\left(s_{\max} d_{\max}\left(\sum_{i=1}^{r} \# f_i + d_1^2 + d_1 d_{\max}\right) + s_{\max} d_1 d_{\max} C(\text{probe } \mathbf{B})\right)\right)$.

From experiments, we observed that $s \ll \# f_i$, $i = 1..r$, where s is the number of bi-variate images to be interpolated.

Implementation Details

Already implemented Method II in Maple for monic polynomials.

Subroutines for black box

- BB := proc(X::list, alpha::list, p::prime)
  (contains a subroutine to compute determinant in $\mathbb{Z}_p$ in C)
- degBB := proc(X::list, p::prime, j::posint)

Subroutines for CMSHL (Method II)

- Evaluation (done with black box)
  denseinterp := proc(X::list, beta::list, index::integer, p::prime)
- Multifactor BHL (in the middle of integrating it)
- Vandermonde Solve (to be implemented in C)

Current and Future Work

- To integrate more components in C, i.e. BHL (multifactor) and Vandermonde Solve.
- Investigate the efficiency of black box procedure.
- Compare both method I and II.

In the future, may include the non-monic case for completeness.

Current and Future Work

- To integrate more components in C, i.e. BHL (multifactor) and Vandermonde Solve.
- Investigate the efficiency of black box procedure.
- Compare both method I and II.

In the future, may include the non-monic case for completeness.

Thank you for attending!

References

- Chen, T., Monagan, M.: The complexity and parallel implementation of two sparse multivariate Hensel lifting algorithms for polynomial factorization. In Proceedings of CASC 2020, LNCS **12291**, pp. 150–169. Springer (2020)
- Diaz A., Kaltofen E.: FOXBOX: A system for manipulating symbolic objects in black box representation. In Proceedings of ISSAC '98, pp. 30–37. ACM (1998)
- 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)
- Lee, W.S.: Early termination strategies in sparse interpolation algorithms. Ph.D. Thesis (2001)
- Monagan, M., Tuncer, B.: Factoring multivariate polynomials with many factors and huge coefficients. In Proceedings of CASC 2018, LNCS **11077**, pp. 319–334. Springer (2018)
- Monagan, M., Tuncer, B.: Polynomial factorization in Maple 2019. In Maple in Mathematics Education and Research. *Communications in Computer and Information Science* **1125**, pp. 341–345. Springer (2020)
- Paluck, G.: A new bivariate Hensel lifting algorithm for n factors. MSc. Thesis (2019)
- Zippel, R.E.: Interpolating polynomials from their values. *J. Symb. Cmpt.* **9**(3), 375–403. Elsevier (1990)