DETERMINISTIC FACTORIZATION OF CONSTANT DEPTH CIRCUITS

Somnath Bhattacharjee, Mrinal Kumar, Varun Ramanathan, Ramprasad Saptharishi, Shubhangi Saraf

Introduction

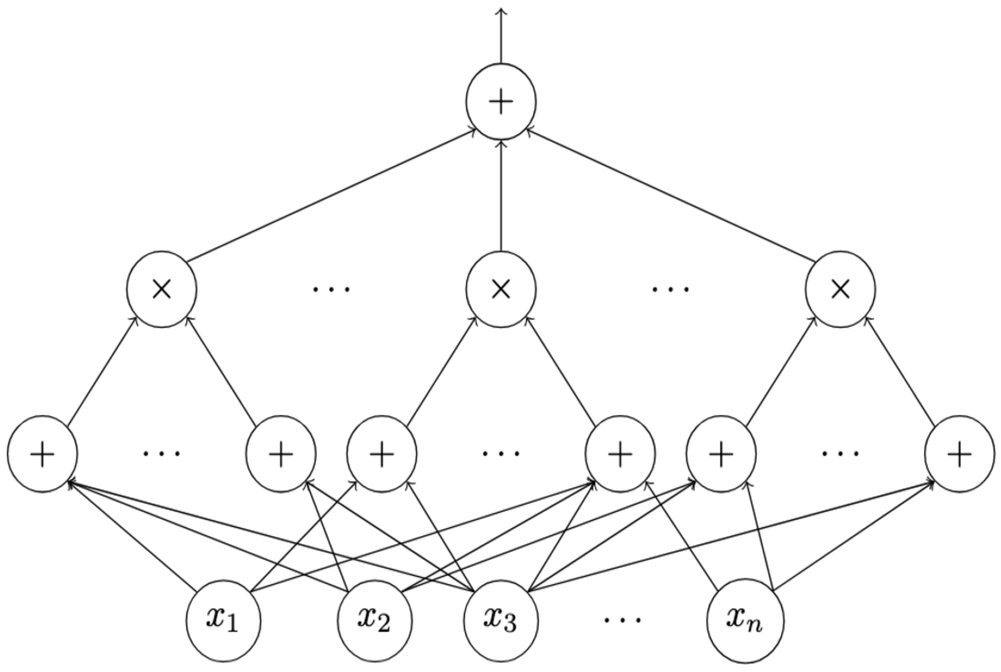
Polynomial Factorization Problem:
- **Input**: Algebraic circuit over field $\mathbb{Q}$
- **Output**: All the irreducible factors

- [Kal 80] proved that algebraic circuits are closed under factorization (given the degree is polynomially bounded) and gave a deterministic poly-time algorithm with oracle access to *Polynomial Identity Testing (PIT).*

- PIT problem is testing whether *a given algebraic circuit is zero or not*. Well-known to be in **RP**

- Hence, we have randomized algorithm for the polynomial factorization problem.

- Polynomial factorization has applications in Coding Theory, Cryptography, Graph Algorithms etc.



Algebraic circuits

size: #gates **depth**: length of the shortest path from root to leaf

[LST 21] gave a *Sub-Exponential* deterministic Algorithm for **Constant Depth** algebraic circuits.

This raise a possibility of sub-exponential factorization algorithm for constant depth circuits.

[KRS 23], [DST24], [KRSV 24] made progress towards this problem. Finally, we answered the question.

Main Result: *Given $\varepsilon > 0$, and n-variate d-degree constant depth circuit of size s, we can output algebraic circuits for all the irreducible factors of C with multiplicities in time $\mathcal{O}((sd)^{n^{\varepsilon}})$*

Overview

Constant-Depth PIT idea:
Combining the result of [LST 21] with the construction based on [KI 04], we can construct a polynomial map/generator on small number of variables:

$$KI : \mathbb{Q}[x_1, \dots, x_n] \to \mathbb{Q}[w_1, \dots, w_m]$$

Where $m = n^{\varepsilon}$.

If *C* is a constant-depth circuit, then

$$C \neq 0 \leftrightarrow C \circ KI \neq 0$$

We proved a stronger property of the generator:

Main Technical Theorem: *Let the irreducible factorization of a constant depth circuit C be $C = f_1^{e_1} \dots f_k^{e_k}$, then the irreducible factorization of $C \circ KI$ will be*

$$C \circ KI = (f_1 \circ KI)^{e_1} \dots (f_k \circ KI)^{e\_k}$$

Main Algorithm (Informal):

- Compute the *KI*- Generator on variables n^{ε}
- Construct the circuit $C' = C \circ KI$
- Factorize C' via brute force on variables
- Use **Newton Iteration** to get back the original factors

This process requires some preprocessing which can be done due to the recent work by [AW 24]

High-Level proof idea:

- We considered all the PIT instances throughout the standard factorization algorithm. Though the circuits in those instances are NOT constant depth, but they are closely related with constant depth circuits.
- Generalizing [CKS 19] we proved ***low degree roots*** *of all those polynomials has small constant depth circuits.*
- We used the well-studied KI generator and LST-Hardness to exploit the above property and get a derandomized algorithm

Discussion

- Our algorithm is efficient in terms of bit-complexity
- **Field dependency:** Our algorithm works on every field of characteristics 0 or $\omega(d)$ and where univariate factorization is known

Open questions:
- Are constant depth circuits closed under factorization
- Can we generalize our approach for other randomized algorithms for constant depth circuits?

CONTACT: {somnath,shubhangi}@cs.toronto.edu, {mrinal, varun.ramanathan,r ramprasad}@tifr.re.in