Discovering the roots: Uniform closure results for algebraic classes under factoring

To appear at STOC 2018

Pranjal Dutta (CMI) Nitin Saxena (IIT Kanpur) Amit Sinhababu (IIT Kanpur)

WACT'18, Université Paris Diderot

Table of contents

Introduction

- For given input $f \in \mathbb{F}[x_1, \ldots, x_n]$, goal is to relate "complexity" of its factors and possibly output it.

- For given input $f \in \mathbb{F}[x_1, \ldots, x_n]$, goal is to relate "complexity" of its factors and possibly output it.

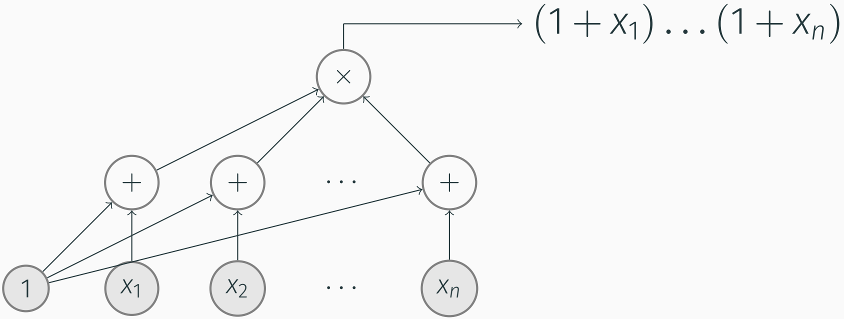
- How is the input given (model of computation)? What is the notion of "complexity" we are talking about?

- For given input $f \in \mathbb{F}[x_1, \ldots, x_n]$, goal is to relate "complexity" of its factors and possibly output it.

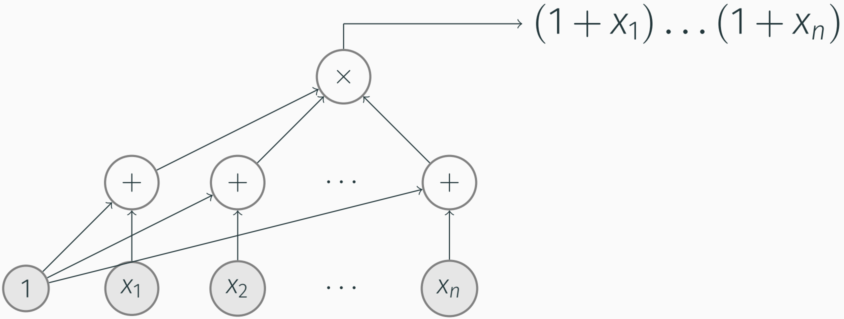
- How is the input given (model of computation)? What is the notion of "complexity" we are talking about?

- We will be talking about different algebraic models of computation throughout. One of the most important is the "circuit" model.

Arithmetic Circuits

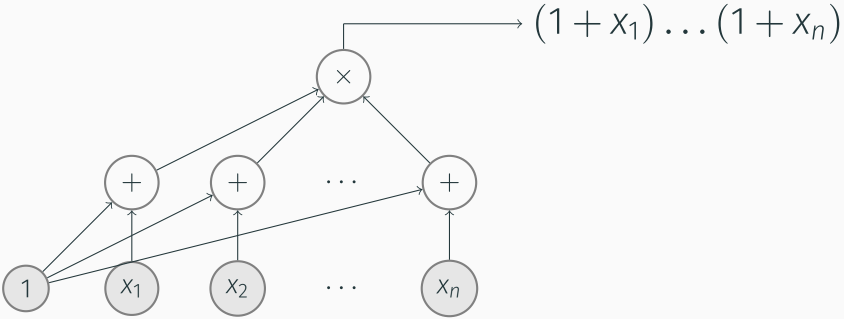


Arithmetic Circuits



- size= # of nodes + # of edges = $5n+2$

Arithmetic Circuits



- size= # of nodes + # of edges = $5n + 2$
- # of monomials = 2^n

Notation

- Notation : $\bar{x} = (x_1, \ldots, x_n)$, $[n] = \{1, \ldots, n\}$

Notation

- Notation : $\bar{x} = (x_1, \ldots, x_n)$, $[n] = \{1, \ldots, n\}$
- $\deg(f) :=$ total degree of f
  Example:
  $$f = x^2y + x^3y^2 + xy + 4$$
  Here $\deg(f) = 5$

Notation

- Notation : $\bar{x} = (x_1, \ldots, x_n)$, $[n] = \{1, \ldots, n\}$
- $\deg(f) :=$ total degree of f
  Example:
  $$f = x^2y + x^3y^2 + xy + 4$$
  Here $\deg(f) = 5$
- size(f) denotes the minimum size of circuit computing f

Notation

- Notation : $\bar{x} = (x_1, \ldots, x_n)$, $[n] = \{1, \ldots, n\}$
- $\deg(f) :=$ total degree of f
  Example:
  $$f = x^2y + x^3y^2 + xy + 4$$
  Here $\deg(f) = 5$
- $\mathrm{size}(f)$ denotes the minimum size of circuit computing f
- $f^{\leq d}$ denotes degree of f upto d i.e.
  $$f^{\leq d} = f \bmod \langle \bar{x} \rangle^{d+1}$$

Factorization in Circuit Models

Question: Given $f \in \mathbb{F}[\overline{x}]$ of $\text{size}(f) \leq s$, $\deg(f) = d$, what can we say about the size of its factors? 😫

Factorization in Circuit Models

Question: Given $f \in \mathbb{F}[\overline{x}]$ of size$(f) \leq s$, deg$(f) = d$, what can we say about the size of its factors? 😫

- (Kaltofen'87, Bürgisser'00, KSS'14, Oliveira'16) Any factor has poly(s, d)-size circuit

Factorization in Circuit Models

Question: Given $f \in \mathbb{F}[\overline{x}]$ of size$(f) \leq s$, deg$(f) = d$, what can we say about the size of its factors? 😫

- (Kaltofen'87, Bürgisser'00, KSS'14, Oliveira'16) Any factor has poly(s, d)-size circuit
- There is a randomized poly(s, d)-time algorithm that can output irreducible factor 😄

Factorization in Circuit Models

Question: Given $f \in \mathbb{F}[\overline{x}]$ of size$(f) \leq s$, deg$(f) = d$, what can we say about the size of its factors?

- (Kaltofen'87, Bürgisser'00, KSS'14, Oliveira'16) Any factor has poly(s, d)-size circuit
- There is a randomized poly(s, d)-time algorithm that can output irreducible factor

In other words, VP is *uniformly closed* under factoring!

Exponential degree circuit

- It is natural to ask whether we can allow degree to be $2^{O(s)}$ and claim whether the size of its factors are still poly(s).

Exponential degree circuit

- It is natural to ask whether we can allow degree to be $2^{O(s)}$ and claim whether the size of its factors are still poly(s).
- It is known that "all" factors of polynomial of size s can't have small circuit.

Exponential degree circuit

- It is natural to ask whether we can allow degree to be $2^{O(s)}$ and claim whether the size of its factors are still poly(s).
- It is known that "all" factors of polynomial of size s can't have small circuit.
- Consider

$$f_n = x^{2^n} - 1 = \prod_{j=1}^{2^n} (x - \zeta^j)$$

where ζ denotes 2^n-th root of unity.

Exponential degree circuit

- It is natural to ask whether we can allow degree to be $2^{O(s)}$ and claim whether the size of its factors are still poly(s).
- It is known that "all" factors of polynomial of size s can't have small circuit.
- Consider
$$f_n = x^{2^n} - 1 = \prod_{j=1}^{2^n} (x - \zeta^j)$$
where ζ denotes 2^n-th root of unity.
- (LS'78) f_n has $O(n)$ size circuit but there are factors which has size $\geq \Omega(\frac{2^{n/2}}{\sqrt{n}})$.

- The previous example is only about exponential degree factor

- The previous example is only about exponential degree factor

- Let $g = \prod_{i \in S} (x - \zeta^i)$ where $S \subset [2^n]$ with $|S| = n^{O(1)}$

- The previous example is only about exponential degree factor
- Let $g = \prod_{i \in S} (x - \zeta^i)$ where $S \subset [2^n]$ with $|S| = n^{O(1)}$
- Trivially g has poly(n) size circuit!

Factor Conjecture

Factor Conjecture

Factor Conjecture

If f has s size circuit and $g \mid f$ with $\deg(g) = d$, then g has $\mathrm{poly}(s, d)$ size circuit.

Factor Conjecture

If f has s size circuit and $g \mid f$ with $\deg(g) = d$, then g has $\text{poly}(s, d)$ size circuit.

- (Kaltofen'87) If $f = g^e$, $\text{size}(f) = s$, $\deg(g) = d$; then $\text{size}(g) \leq \text{poly}(s, d)$. This is true over character 0 or field of large characteristic.

Factor Conjecture

Factor Conjecture

If f has s size circuit and $g \mid f$ with $\deg(g) = d$, then g has $\text{poly}(s, d)$ size circuit.

- (Kaltofen'87) If $f = g^e$, $\text{size}(f) = s$, $\deg(g) = d$; then $\text{size}(g) \leq \text{poly}(s, d)$. This is true over character 0 or field of large characteristic.

- What can we say about factors of $f = g_1^{e_1} g_2^{e_2}$ where $\text{size}(f) = s$, $\deg(g_1), \deg(g_2) \leq d$? 😫

Relating Squarefree part to Complexity

Relating Squarefree part to Complexity

- For $f = \prod_i f_i^{e_i}$, define radical to be

$$\mathrm{rad}(f) = \prod_i f_i$$

Relating Squarefree part to Complexity

- For $f = \prod_i f_i^{e_i}$, define radical to be

$$\mathrm{rad}(f) = \prod_i f_i$$

- Assumption: $\mathbb{F}$ is algebraically closed and characteristic=0

Relating Squarefree part to Complexity

- For $f = \prod_i f_i^{e_i}$, define radical to be

$$\mathrm{rad}(f) = \prod_i f_i$$

- Assumption: $\mathbb{F}$ is algebraically closed and characteristic=0

Theorem 1

Any factor g of a polynomial f computed by a circuit of size s has size $\mathrm{poly}(s, \deg(\mathrm{rad}(f)))$.

Relating Squarefree part to Complexity

- For $f = \prod_i f_i^{e_i}$, define radical to be

$$\mathrm{rad}(f) = \prod_i f_i$$

- Assumption: $\mathbb{F}$ is algebraically closed and characteristic=0

Theorem 1

Any factor g of a polynomial f computed by a circuit of size s has size $\mathrm{poly}(s, \deg(\mathrm{rad}(f)))$.

- The degree of square-free part is polynomially bounded $\implies$ size "any" factor is!(and factor conjecture is true in this case!) 😄

Relating Squarefree part to Complexity

- For $f = \prod_i f_i^{e_i}$, define radical to be

$$\text{rad}(f) = \prod_i f_i$$

- Assumption: $\mathbb{F}$ is algebraically closed and characteristic=0

Theorem 1

Any factor g of a polynomial f computed by a circuit of size s has size $\text{poly}(s, \deg(\text{rad}(f)))$.

- The degree of square-free part is polynomially bounded $\implies$ size "any" factor is!(and factor conjecture is true in this case!) 😄
- This subsumes both the results of Kaltofen

Factoring Reduces to Root Approximation

Finding linear factor

- Suppose $f(\bar{x}, y) = (y - g(\bar{x})) \cdot u(\bar{x}, y)$ where $y - g \nmid u$. Can we find g?

Finding linear factor

- Suppose $f(\bar{x}, y) = (y - g(\bar{x})) \cdot u(\bar{x}, y)$ where $y - g \nmid u$. Can we find g? This is root finding as $f(\bar{x}, g) = 0$.

Finding linear factor

- Suppose $f(\bar{x}, y) = (y - g(\bar{x})) \cdot u(\bar{x}, y)$ where $y - g \nmid u$. Can we find g? This is root finding as $f(\bar{x}, g) = 0$.
- (Newton Iteration) Suppose we want to find “good enough“ approximation of x such that $f(x) = 0$. Assume $f'(x) \neq 0$. Idea is the following:

Finding linear factor

- Suppose $f(\bar{x}, y) = (y - g(\bar{x})) \cdot u(\bar{x}, y)$ where $y - g \nmid u$. Can we find g? This is root finding as $f(\bar{x}, g) = 0$.

- (Newton Iteration) Suppose we want to find “good enough“ approximation of x such that $f(x) = 0$. Assume $f'(x) \neq 0$. Idea is the following:
  1. guess a good `starting` point x_0

Finding linear factor

- Suppose $f(\bar{x}, y) = (y - g(\bar{x})) \cdot u(\bar{x}, y)$ where $y - g \nmid u$. Can we find g? This is root finding as $f(\bar{x}, g) = 0$.

- (Newton Iteration) Suppose we want to find "good enough" approximation of x such that $f(x) = 0$. Assume $f'(x) \neq 0$. Idea is the following:
  1. guess a good `starting` point x_0
  2. calculate $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$

Finding linear factor

- Suppose $f(\bar{x}, y) = (y - g(\bar{x})) \cdot u(\bar{x}, y)$ where $y - g \nmid u$. Can we find g? This is root finding as $f(\bar{x}, g) = 0$.
- (Newton Iteration) Suppose we want to find “good enough“ approximation of x such that $f(x) = 0$. Assume $f'(x) \neq 0$. Idea is the following:
    1. guess a good `starting` point x_0
    2. calculate $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$
- Can we do similar thing to find g? If yes, what is the notion of `approximation` ? What is the `starting point`? 😫

Finding linear factor Continued

- Initial starting point $y_0 = \mu$ where $\mu := g(\overline{0})$

Finding linear factor Continued

- Initial starting point $y_0 = \mu$ where $\mu := g(\overline{0})$
- Define $y_{t+1} = y_t - \frac{f(\overline{x}, y_t)}{f'(\overline{x}, y_t)}$. Can we say that y_t is an approximation of g?

Finding linear factor Continued

- Initial starting point $y_0 = \mu$ where $\mu := g(\overline{0})$
- Define $y_{t+1} = y_t - \frac{f(\overline{x}, y_t)}{f'(\overline{x}, y_t)}$. Can we say that y_t is an approximation of g?
- If $f'(\overline{x}, y_t)$ is invertible, then one can show that

$$y_t \equiv g \bmod \langle \overline{x} \rangle^{2^t} \implies y_{t+1} \equiv g \bmod \langle \overline{x} \rangle^{2^{t+1}}$$

Finding linear factor Continued

- Initial starting point $y_0 = \mu$ where $\mu := g(\overline{0})$
- Define $y_{t+1} = y_t - \frac{f(\overline{x}, y_t)}{f'(\overline{x}, y_t)}$. Can we say that y_t is an approximation of g?
- If $f'(\overline{x}, y_t)$ is invertible, then one can show that

$$y_t \equiv g \bmod \langle \overline{x} \rangle^{2^t} \implies y_{t+1} \equiv g \bmod \langle \overline{x} \rangle^{2^{t+1}}$$

- $f'(\overline{x}, y_t)$ is invertible $\iff f'(\overline{x}, y_t)\Big|_{\overline{x}=\overline{0}} \neq 0 \iff f'(\overline{0}, \mu) \neq 0$

Finding linear factor Continued

- Initial starting point $y_0 = \mu$ where $\mu := g(\overline{0})$
- Define $y_{t+1} = y_t - \frac{f(\overline{x}, y_t)}{f'(\overline{x}, y_t)}$. Can we say that y_t is an approximation of g?
- If $f'(\overline{x}, y_t)$ is invertible, then one can show that

$$y_t \equiv g \bmod \langle \overline{x} \rangle^{2^t} \implies y_{t+1} \equiv g \bmod \langle \overline{x} \rangle^{2^{t+1}}$$

- $f'(\overline{x}, y_t)$ is invertible $\iff f'(\overline{x}, y_t)\Big|_{\overline{x}=\overline{0}} \neq 0 \iff f'(\overline{0}, \mu) \neq 0$
- If $f(\overline{0}, \mu) = 0$ and $f'(\overline{0}, \mu) \neq 0$. Then, one can find g by calculating $y_{\log d+1}$ where $\deg(g) = d$.

- What if $f = (y - g_1)(y - g_2)$ but $g_1(\overline{0}) = g_2(\overline{0})$?

- What if $f = (y - g_1)(y - g_2)$ but $g_1(\overline{0}) = g_2(\overline{0})$?
    1. Pick $\overline{\alpha} \in \mathbb{F}^n$ such that $g_1(\alpha) \neq g_2(\overline{\alpha})$

- What if $f = (y - g_1)(y - g_2)$ but $g_1(\overline{0}) = g_2(\overline{0})$?
    1. Pick $\overline{\alpha} \in \mathbb{F}^n$ such that $g_1(\alpha) \neq g_2(\overline{\alpha})$
    2. $f(\overline{x} + \overline{\alpha}, y) = (y - g_1(\overline{x} + \overline{\alpha}))\,(y - g_2(\overline{x} + \overline{\alpha}))$

- What if $f = (y - g_1)(y - g_2)$ but $g_1(\overline{0}) = g_2(\overline{0})$?
  1. Pick $\overline{\alpha} \in \mathbb{F}^n$ such that $g_1(\alpha) \neq g_2(\overline{\alpha})$
  2. $f(\overline{x} + \overline{\alpha}, y) = (y - g_1(\overline{x} + \overline{\alpha}))\,(y - g_2(\overline{x} + \overline{\alpha}))$
  3. when we put $\overline{x} = \overline{0}$ we will get $(y - g_1(\alpha))\,(y - g_2(\overline{\alpha}))$

- What if $f = (y - g_1)(y - g_2)$ but $g_1(\overline{0}) = g_2(\overline{0})$?
    1. Pick $\overline{\alpha} \in \mathbb{F}^n$ such that $g_1(\alpha) \neq g_2(\overline{\alpha})$
    2. $f(\overline{x} + \overline{\alpha}, y) = (y - g_1(\overline{x} + \overline{\alpha}))\,(y - g_2(\overline{x} + \overline{\alpha}))$
    3. when we put $\overline{x} = \overline{0}$ we will get $(y - g_1(\alpha))\,(y - g_2(\overline{\alpha}))$
    4. apply Newton Iteration (NI)

- What if $f = (y - g_1)(y - g_2)$ but $g_1(\overline{0}) = g_2(\overline{0})$?
    1. Pick $\overline{\alpha} \in \mathbb{F}^n$ such that $g_1(\alpha) \neq g_2(\overline{\alpha})$
    2. $f(\overline{x} + \overline{\alpha}, y) = (y - g_1(\overline{x} + \overline{\alpha}))\,(y - g_2(\overline{x} + \overline{\alpha}))$
    3. when we put $\overline{x} = \overline{0}$ we will get $(y - g_1(\alpha))\,(y - g_2(\overline{\alpha}))$
    4. apply Newton Iteration (NI)

- What if $f = (y - g)^e \cdot u$?

- What if $f = (y - g_1)(y - g_2)$ but $g_1(\overline{0}) = g_2(\overline{0})$?
    1. Pick $\overline{\alpha} \in \mathbb{F}^n$ such that $g_1(\alpha) \neq g_2(\overline{\alpha})$
    2. $f(\overline{x} + \overline{\alpha}, y) = (y - g_1(\overline{x} + \overline{\alpha}))\,(y - g_2(\overline{x} + \overline{\alpha}))$
    3. when we put $\overline{x} = \overline{0}$ we will get $(y - g_1(\alpha))\,(y - g_2(\overline{\alpha}))$
    4. apply Newton Iteration (NI)

- What if $f = (y - g)^e \cdot u$? We can differentiate $e - 1$ times and apply NI on $f^{(e-1)}$.

- What if $f = (y - g_1)(y - g_2)$ but $g_1(\overline{0}) = g_2(\overline{0})$?
    1. Pick $\overline{\alpha} \in \mathbb{F}^n$ such that $g_1(\alpha) \neq g_2(\overline{\alpha})$
    2. $f(\overline{x} + \overline{\alpha}, y) = (y - g_1(\overline{x} + \overline{\alpha}))\,(y - g_2(\overline{x} + \overline{\alpha}))$
    3. when we put $\overline{x} = \overline{0}$ we will get $(y - g_1(\alpha))\,(y - g_2(\overline{\alpha}))$
    4. apply Newton Iteration (NI)

- What if $f = (y - g)^e \cdot u$? We can differentiate $e - 1$ times and apply NI on $f^{(e-1)}$.

- What about $f(\overline{x}, y) = \left(y^k + c_{k-1}(\overline{x})y^{k-1} + \ldots + c_0(\overline{x})\right) \cdot u$ where $k > 1$? 😫

Non linear factor

We would like to relate non-linear factors to linear factors so that we can apply NI.

Non linear factor

We would like to relate non-linear factors to linear factors so that we can apply NI.

- Consider $f(x,z) = (z^2 - x^3) \cdot u(x,z) = (z - x^{3/2})(z + x^{3/2}) \cdot u$

Non linear factor

We would like to relate non-linear factors to linear factors so that we can apply NI.

- Consider $f(x,z) = (z^2 - x^3) \cdot u(x,z) = (z - x^{3/2})(z + x^{3/2}) \cdot u$
- One can assume that $z^2 - x^3 \nmid u$ as otherwise we can differentiate appropriately many times and work with the new polynomial

Non linear factor

We would like to relate non-linear factors to linear factors so that we can apply NI.

- Consider $f(x,z) = (z^2 - x^3) \cdot u(x,z) = (z - x^{3/2})(z + x^{3/2}) \cdot u$
- One can assume that $z^2 - x^3 \nmid u$ as otherwise we can differentiate appropriately many times and work with the new polynomial
- $f(x+1,z) = (z^2 - (x+1)^3) \cdot u(x+1,z) = \left(z - (x+1)^{3/2}\right)\left(z + (x+1)^{3/2}\right) \cdot u(x+1,z)$

Non linear factor

We would like to relate non-linear factors to linear factors so that we can apply NI.

- Consider $f(x,z) = (z^2 - x^3) \cdot u(x,z) = (z - x^{3/2})(z + x^{3/2}) \cdot u$
- One can assume that $z^2 - x^3 \nmid u$ as otherwise we can differentiate appropriately many times and work with the new polynomial
- $f(x+1,z) = (z^2 - (x+1)^3) \cdot u(x+1,z) = \left(z - (x+1)^{3/2}\right)\left(z + (x+1)^{3/2}\right) \cdot u(x+1,z)$
- $g := (x+1)^{3/2} = 1 + \frac{3}{2}x + \binom{\frac{3}{2}}{2}x^2 + \binom{\frac{3}{2}}{3}x^3 + \dots$

Non linear factor

We would like to relate non-linear factors to linear factors so that we can apply NI.

- Consider $f(x,z) = (z^2 - x^3)\cdot u(x,z) = (z - x^{3/2})(z + x^{3/2})\cdot u$
- One can assume that $z^2 - x^3 \nmid u$ as otherwise we can differentiate appropriately many times and work with the new polynomial
- $f(x+1,z) = (z^2 - (x+1)^3)\cdot u(x+1,z) = \left(z - (x+1)^{3/2}\right)\left(z + (x+1)^{3/2}\right)\cdot u(x+1,z)$
- $g := (x+1)^{3/2} = 1 + \frac{3}{2}x + \binom{\frac{3}{2}}{2}x^2 + \binom{\frac{3}{2}}{3}x^3 + \dots$
- So g is a root of $f(x+1,z) \in \mathbb{F}[[x]][z]$ as $f(x+1,g) = 0$

Non linear factor

We would like to relate non-linear factors to linear factors so that we can apply NI.

- Consider $f(x,z) = (z^2 - x^3) \cdot u(x,z) = (z - x^{3/2})(z + x^{3/2}) \cdot u$
- One can assume that $z^2 - x^3 \nmid u$ as otherwise we can differentiate appropriately many times and work with the new polynomial
- $f(x+1,z) = (z^2 - (x+1)^3) \cdot u(x+1,z) = \left(z - (x+1)^{3/2}\right)\left(z + (x+1)^{3/2}\right) \cdot u(x+1,z)$
- $g := (x+1)^{3/2} = 1 + \frac{3}{2}x + \binom{\frac{3}{2}}{2}x^2 + \binom{\frac{3}{2}}{3}x^3 + \dots$
- So g is a root of $f(x+1,z) \in \mathbb{F}[[x]][z]$ as $f(x+1,g) = 0$
- Note that $z^2 - (x+1)^3 = (z - g^{\leq 3})(z + g^{\leq 3}) \bmod x^4$

Power Series Split Theorem

Power Series Split Theorem

Power Series Split Theorem (DSS'18)

$\tau : x_i \mapsto x_i + \alpha_i y + \beta_i$, where $\alpha_i, \beta_i \in_r \mathbb{F}$, $\deg(\mathrm{rad}(f)) = d_0$,

$$f(\tau\overline{x}) = k \cdot \prod_{i \in [d_0]} (y - g_i)^{\gamma_i}$$

where $k \in \mathbb{F}^{\times}$, $g_i \in \mathbb{F}[[\overline{x}]]$

Power Series Split Theorem

Power Series Split Theorem (DSS'18)

$\tau : x_i \mapsto x_i + \alpha_i y + \beta_i$, where $\alpha_i, \beta_i \in_r \mathbb{F}$, $\deg(\mathrm{rad}(f)) = d_0$,

$$f(\tau\overline{x}) = k \cdot \prod_{i \in [d_0]} (y - g_i)^{\gamma_i}$$

where $k \in \mathbb{F}^{\times}$, $g_i \in \mathbb{F}[[\overline{x}]]$ 😄

- $f(x_1 + \alpha_1 y, \ldots, x_n + \alpha_n y)$ makes f monic in y

Power Series Split Theorem

Power Series Split Theorem (DSS'18)

$\tau : x_i \mapsto x_i + \alpha_i y + \beta_i$, where $\alpha_i, \beta_i \in_r \mathbb{F}$, $\deg(\mathrm{rad}(f)) = d_0$,

$$f(\tau\overline{x}) = k \cdot \prod_{i \in [d_0]} (y - g_i)^{\gamma_i}$$

where $k \in \mathbb{F}^{\times}$, $g_i \in \mathbb{F}[[\overline{x}]]$

- $f(x_1 + \alpha_1 y, \ldots, x_n + \alpha_n y)$ makes f monic in y
- For irreducible h, one can show that

$$h(\tau\overline{x}) = c \cdot \prod_{i=1}^{\deg(h)} (y - g_i)$$

Factoring reduces to Root Approximation

Notation : $g^{\leq k} \equiv g \bmod \langle \overline{x} \rangle^{k+1}$.

Factoring reduces to Root Approximation

Notation : $g^{\leq k} \equiv g \bmod \langle \bar{x} \rangle^{k+1}$.

- Suppose $h \mid f$. Apply τ on f

Factoring reduces to Root Approximation

Notation : $g^{\leq k} \equiv g \bmod \langle \bar{x} \rangle^{k+1}$.

- Suppose $h \mid f$. Apply τ on f
- $f(\tau\bar{x}) = k \cdot \prod (y - g_i)^{e_i}$

Factoring reduces to Root Approximation

Notation : $g^{\leq k} \equiv g \bmod \langle \bar{x} \rangle^{k+1}$.

- Suppose $h \mid f$. Apply τ on f
- $f(\tau\bar{x}) = k \cdot \prod (y - g_i)^{e_i}$
- $\mathbb{F}[[\bar{x}]][y]$ is UFD $\implies h(\tau\bar{x}) = c \cdot \prod (y - g_i)^{b_i}$ for $b_i \leq e_i$

Factoring reduces to Root Approximation

Notation : $g^{\leq k} \equiv g \bmod \langle \bar{x} \rangle^{k+1}$.

- Suppose $h \mid f$. Apply τ on f
- $f(\tau\bar{x}) = k \cdot \prod (y - g_i)^{e_i}$
- $\mathbb{F}[[\bar{x}]][y]$ is UFD $\implies h(\tau\bar{x}) = c \cdot \prod (y - g_i)^{b_i}$ for $b_i \leq e_i$
- If $\deg(h) = d_h \implies \deg(h(\tau\bar{x})) = d_h$

Factoring reduces to Root Approximation

Notation : $g^{\leq k} \equiv g \bmod \langle \bar{x} \rangle^{k+1}$.

- Suppose $h \mid f$. Apply τ on f
- $f(\tau\bar{x}) = k \cdot \prod (y - g_i)^{e_i}$
- $\mathbb{F}[[\bar{x}]][y]$ is UFD $\implies h(\tau\bar{x}) = c \cdot \prod (y - g_i)^{b_i}$ for $b_i \leq e_i$
- If $\deg(h) = d_h \implies \deg(h(\tau\bar{x})) = d_h$
- Hence $h(\tau\bar{x}) = h(\tau\bar{x}) \bmod \langle \bar{x} \rangle^{d_h+1}$

Factoring reduces to Root Approximation

Notation : $g^{\leq k} \equiv g \bmod \langle \overline{x} \rangle^{k+1}$.

- Suppose $h \mid f$. Apply τ on f
- $f(\tau\overline{x}) = k \cdot \prod (y - g_i)^{e_i}$
- $\mathbb{F}[[\overline{x}]][y]$ is UFD $\implies h(\tau\overline{x}) = c \cdot \prod (y - g_i)^{b_i}$ for $b_i \leq e_i$
- If $\deg(h) = d_h \implies \deg(h(\tau\overline{x})) = d_h$
- Hence $h(\tau\overline{x}) = h(\tau\overline{x}) \bmod \langle \overline{x} \rangle^{d_h+1}$
- $h(\tau\overline{x}) = c \cdot \prod (y - g_i^{\leq d_h})^{b_i} \bmod \langle \overline{x} \rangle^{d_h+1}$

Factoring reduces to Root Approximation

Notation : $g^{\leq k} \equiv g \bmod \langle \bar{x} \rangle^{k+1}$.

- Suppose $h \mid f$. Apply τ on f
- $f(\tau\bar{x}) = k \cdot \prod (y - g_i)^{e_i}$
- $\mathbb{F}[[\bar{x}]][y]$ is UFD $\implies h(\tau\bar{x}) = c \cdot \prod (y - g_i)^{b_i}$ for $b_i \leq e_i$
- If $\deg(h) = d_h \implies \deg(h(\tau\bar{x})) = d_h$
- Hence $h(\tau\bar{x}) = h(\tau\bar{x}) \bmod \langle \bar{x} \rangle^{d_h+1}$
- $h(\tau\bar{x}) = c \cdot \prod (y - g_i^{\leq d_h})^{b_i} \bmod \langle \bar{x} \rangle^{d_h+1}$
- Apply τ^{-1} on $h(\tau\bar{x})$ to get back $h(\bar{x})$.

Simultaneous Root Approximation (allRootsNI)

Are we done?

- We know factoring reduces to root approximation.

Are we done?

- We know factoring reduces to root approximation.
- We know standard newton iteration would give us approximation.

Are we done?

- We know factoring reduces to root approximation.
- We know standard newton iteration would give us approximation.
- Are we done?

Are we done?

- We know factoring reduces to root approximation.
- We know standard newton iteration would give us approximation.
- Are we done?
- If $f = (y - g)^e \cdot u$, to find g, we have to differentiate $e - 1$-times (wrt y). What is the size of $f^{(e-1)}$?

Derivative Computation

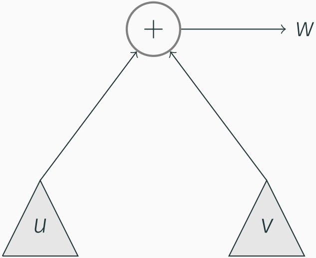
f computed by size s circuit $\implies \frac{\partial^k f}{\partial y^k}$ can be computed by $O(k^2 s)$ size circuit

Derivative Computation

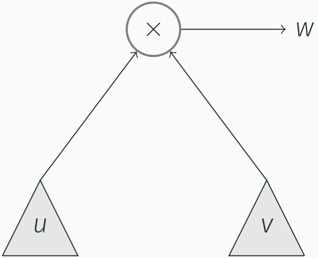
f computed by size s circuit $\implies \frac{\partial^k f}{\partial y^k}$ can be computed by $O(k^2 s)$ size circuit

Proof Idea.

Compute inductively from bottom to top calculating upto k-th derivative i.e. at some node calculating u in the actual circuit, we keep track of $(u, u^{(1)}, \ldots, u^{(k)})$ instead! $\square$



$$w^{(i)} = u^{(i)} + v^{(i)}$$



$$w^{(i)} = \sum_{\mu=0}^{i} \binom{i}{\mu} u^{(i-\mu)} v^{(\mu)}$$

Can we do better for derivative computing?

Observation: $\text{size}(f') = O(s)$ where $\text{size}(f) = s$

Can we do better for derivative computing?

Observation: $\text{size}(f') = O(s)$ where $\text{size}(f) = s$

- Can one show log dependency on k in the size of the derivative circuit?

Can we do better for derivative computing?

Observation: $\text{size}(f') = O(s)$ where $\text{size}(f) = s$

- Can one show log dependency on k in the size of the derivative circuit?
- If $\frac{\partial^k f}{\partial y^k}$ can be computed by $\text{poly}(\log k, s) \implies$ permanent can be computed by a polynomial size circuit 😢

Modified Newton Iteration : Does this help?

- Can we avoid exponential many derivatives?

Modified Newton Iteration : Does this help?

- Can we avoid exponential many derivatives?
- One can show that $f = (y - g)^e \cdot u$, then if we define

Modified Newton Iteration : Does this help?

- Can we avoid exponential many derivatives?
- One can show that $f = (y - g)^e \cdot u$, then if we define

$$y_{t+1} = y_t - e\frac{f(y_t)}{f'(y_t)} \text{ and } y_t \equiv g \bmod \langle \overline{x} \rangle^{2^t}$$

Modified Newton Iteration : Does this help?

- Can we avoid exponential many derivatives?
- One can show that $f = (y-g)^e \cdot u$, then if we define

$$y_{t+1} = y_t - e\frac{f(y_t)}{f'(y_t)} \text{ and } y_t \equiv g \bmod \langle \overline{x} \rangle^{2^t}$$

Then

$$y_{t+1} = g \bmod \langle \overline{x} \rangle^{2^{t+1}}$$

Modified Newton Iteration : Does this help?

- Can we avoid exponential many derivatives?
- One can show that $f = (y - g)^e \cdot u$, then if we define

$$y_{t+1} = y_t - e\frac{f(y_t)}{f'(y_t)} \text{ and } y_t \equiv g \bmod \langle \overline{x} \rangle^{2^t}$$

Then

$$y_{t+1} = g \bmod \langle \overline{x} \rangle^{2^{t+1}}$$

- Does this help?

Modified Newton Iteration : Does this help?

- Can we avoid exponential many derivatives?
- One can show that $f = (y - g)^e \cdot u$, then if we define

$$y_{t+1} = y_t - e\frac{f(y_t)}{f'(y_t)} \text{ and } y_t \equiv g \bmod \langle \overline{x} \rangle^{2^t}$$

Then

$$y_{t+1} = g \bmod \langle \overline{x} \rangle^{2^{t+1}}$$

- Does this help? No! 😰

- Recall to recover a factor, it is enough to calculate approximation upto its degree

- Recall to recover a factor, it is enough to calculate approximation upto its degree
- Suppose $h \mid f$ and $y - g \mid h(\tau\bar{x})$ for some $g \in \mathbb{F}[[\bar{x}]]$

- Recall to recover a factor, it is enough to calculate approximation upto its degree
- Suppose $h \mid f$ and $y - g \mid h(\tau\bar{x})$ for some $g \in \mathbb{F}[[\bar{x}]]$
- One has to calculate $g^{\leq d_h}$.

- Recall to recover a factor, it is enough to calculate approximation upto its degree
- Suppose $h \mid f$ and $y - g \mid h(\tau\bar{x})$ for some $g \in \mathbb{F}[[\bar{x}]]$
- One has to calculate $g^{\leq d_h}$. Calculate $y_{\log d_h + 1}$ by the modified iteration

$$y_{t+1} = y_t - e\frac{f(y_t)}{f'(y_t)}$$

- Recall to recover a factor, it is enough to calculate approximation upto its degree
- Suppose $h \mid f$ and $y - g \mid h(\tau\bar{x})$ for some $g \in \mathbb{F}[[\bar{x}]]$
- One has to calculate $g^{\leq d_h}$. Calculate $y_{\log d_h + 1}$ by the modified iteration

$$y_{t+1} = y_t - e\frac{f(y_t)}{f'(y_t)}$$

- Compute the whole thing as a circuit with "division" gate allowed

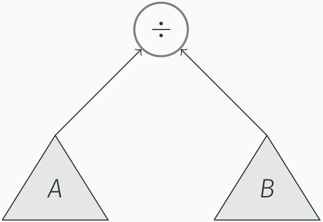
- Recall to recover a factor, it is enough to calculate approximation upto its degree
- Suppose $h \mid f$ and $y - g \mid h(\tau\bar{x})$ for some $g \in \mathbb{F}[[\bar{x}]]$
- One has to calculate $g^{\leq d_h}$. Calculate $y_{\log d_h + 1}$ by the modified iteration

$$y_{t+1} = y_t - e\frac{f(y_t)}{f'(y_t)}$$

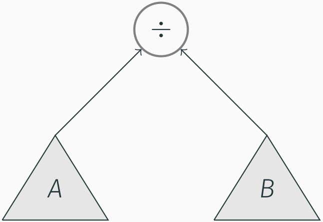
- Compute the whole thing as a circuit with "division" gate allowed
- Push the division gate and the top and try to remove division at the end

- How to eliminate only one division gate at the top?

- How to eliminate only one division gate at the top?

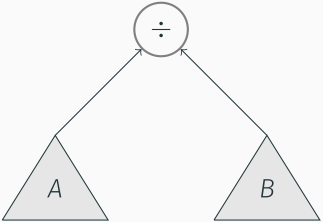


- How to eliminate only one division gate at the top?



- We will be spared with $\frac{A}{B}$ and we have to calculate $\frac{A}{B} \bmod \langle \overline{x} \rangle^{d_h+1}$ where B is not invertible.

- How to eliminate only one division gate at the top?



- We will be spared with $\frac{A}{B}$ and we have to calculate $\frac{A}{B} \bmod \langle \overline{x} \rangle^{d_h+1}$ where B is not invertible.

- We don't know how to calculate this! 

Strassen's Division Elimination

- Can we find $\frac{A}{B} \bmod \langle \overline{x} \rangle^{d+1}$ if B is invertible?
  where $\text{size}(A), \text{size}(B) \leq s$

Strassen's Division Elimination

- Can we find $\frac{A}{B} \bmod \langle \overline{x} \rangle^{d+1}$ if B is invertible?
  where $\text{size}(A), \text{size}(B) \leq s$
- $\frac{A}{B} \bmod \langle \overline{x} \rangle^{d+1}$ has size $O(sd^{O(1)})$

Bounding size of irreducible polynomials are enough

Bounding size of irreducible polynomials are enough

- Suppose we have size s circuit $f = \prod_i f_i^{a_i}$ and $d_0 = \deg(\mathrm{rad}(f))$

Bounding size of irreducible polynomials are enough

- Suppose we have size s circuit $f = \prod_i f_i^{a_i}$ and $d_0 = \deg(\text{rad}(f))$
- Theorem 1 says that any g of f has $\text{poly}(s, d_0)$ size circuit

Bounding size of irreducible polynomials are enough

- Suppose we have size s circuit $f = \prod_i f_i^{a_i}$ and $d_0 = \deg(\mathrm{rad}(f))$
- Theorem 1 says that any g of f has $\mathrm{poly}(s, d_0)$ size circuit
- it is enough to show that each f_i has $\mathrm{poly}(s, d_0)$ size circuit :

Bounding size of irreducible polynomials are enough

- Suppose we have size s circuit $f = \prod_i f_i^{a_i}$ and $d_0 = \deg(\mathrm{rad}(f))$
- Theorem 1 says that any g of f has $\mathrm{poly}(s, d_0)$ size circuit
- it is enough to show that each f_i has $\mathrm{poly}(s, d_0)$ size circuit :
    1. $a_i \leq \exp(s)$

Bounding size of irreducible polynomials are enough

- Suppose we have size s circuit $f = \prod_i f_i^{a_i}$ and $d_0 = \deg(\mathrm{rad}(f))$
- Theorem 1 says that any g of f has $\mathrm{poly}(s, d_0)$ size circuit
- it is enough to show that each f_i has $\mathrm{poly}(s, d_0)$ size circuit :
    1. $a_i \leq \exp(s)$
    2. $g \mid f \implies g = \prod f_i^{b_i}$

Bounding size of irreducible polynomials are enough

- Suppose we have size s circuit $f = \prod_i f_i^{a_i}$ and $d_0 = \deg(\mathrm{rad}(f))$
- Theorem 1 says that any g of f has $\mathrm{poly}(s, d_0)$ size circuit
- it is enough to show that each f_i has $\mathrm{poly}(s, d_0)$ size circuit :
    1. $a_i \leq \exp(s)$
    2. $g \mid f \implies g = \prod f_i^{b_i}$
    3. f_i has $\mathrm{poly}(s, d_0)$ size and $b_i \leq \exp(s)$, then by repeated squaring argument, each $f_i^{b_i}$ has $\mathrm{poly}(s, d_0)$ size circuit

Bounding size of irreducible polynomials are enough

- Suppose we have size s circuit $f = \prod_i f_i^{a_i}$ and $d_0 = \deg(\text{rad}(f))$
- Theorem 1 says that any g of f has poly(s, d_0) size circuit
- it is enough to show that each f_i has poly(s, d_0) size circuit :
    1. $a_i \leq \exp(s)$
    2. $g \mid f \implies g = \prod f_i^{b_i}$
    3. f_i has poly(s, d_0) size and $b_i \leq \exp(s)$, then by repeated squaring argument, each $f_i^{b_i}$ has poly(s, d_0) size circuit
    4. there can be at most d_0 many factors f_i's!

Logarithmic Derivative

- From Split theorem, we have seen that each irreducible $f_i = \prod_j (y - g_j)$

Logarithmic Derivative

- From Split theorem, we have seen that each irreducible $f_i = \prod_j (y - g_j)$
- As $\deg(f_i) \leq d_0$, it is enough to bound size of $g_j^{\leq d_0}$

Logarithmic Derivative

- From Split theorem, we have seen that each irreducible $f_i = \prod_j (y - g_j)$
- As $\deg(f_i) \leq d_0$, it is enough to bound size of $g_j^{\leq d_0}$
- $g_j^{\leq d_0}$ has poly(s, d_0)-size circuit $\implies$

$$f_i \equiv \prod (y - g_j^{\leq d_0}) \bmod \langle \overline{x} \rangle^{d_0+1}$$

has poly(s, d_0)-size circuit as deg is bounded by d_0

- Apply τ on f. We will call this f from now on

- Apply τ on f. We will call this f from now on
- We have $f = c \cdot \prod_{i \in [d_0]} (y - g_i)^{e_i}$ with $g_i(\overline{0}) := \mu_i$

- Apply τ on f. We will call this f from now on
- We have $f = c \cdot \prod_{i \in [d_0]} (y - g_i)^{e_i}$ with $g_i(\overline{0}) := \mu_i$
- $\frac{f'}{f} = \sum_{i \in [d_0]} \frac{e_i}{y - g_i}$

- Apply τ on f. We will call this f from now on
- We have $f = c \cdot \prod_{i \in [d_0]} (y - g_i)^{e_i}$ with $g_i(\overline{0}) := \mu_i$
- $\frac{f'}{f} = \sum_{i \in [d_0]} \frac{e_i}{y - g_i}$
- $\frac{1}{y-g_i} \equiv \frac{1}{y-g_i^{\leq k-1}} + \frac{g_i^{=k}}{(y-\mu_i)^2} \bmod \langle \overline{x} \rangle^{k+1}$

- Apply τ on f. We will call this f from now on
- We have $f = c \cdot \prod_{i \in [d_0]} (y - g_i)^{e_i}$ with $g_i(\overline{0}) := \mu_i$
- $\frac{f'}{f} = \sum_{i \in [d_0]} \frac{e_i}{y - g_i}$
- $\frac{1}{y-g_i} \equiv \frac{1}{y-g_i^{\leq k-1}} + \frac{g_i^{=k}}{(y-\mu_i)^2} \mod \langle \overline{x} \rangle^{k+1}$
- Rearranging we have

$$\sum_{i \in [d_0]} \frac{e_i}{(y - \mu_i)^2} \cdot g_i^{=k} \equiv \frac{f'}{f} - \sum_{i \in [d_0]} \frac{e_i}{y - g_i^{\leq k-1}} \mod \langle \overline{x} \rangle^{k+1}$$

- Put different $y = c_1, \ldots, c_{d_0}$ and try to solve for $g_i^{=k}$

- Put different $y = c_1, \ldots, c_{d_0}$ and try to solve for $g_i^{=k}$
- Does this work?

- Put different $y = c_1, \ldots, c_{d_0}$ and try to solve for $g_i^{=k}$
- Does this work?

  Answer : No! 😫 😡

- Put different $y = c_1, \ldots, c_{d_0}$ and try to solve for $g_i^{=k}$
- Does this work?

  Answer : No! 😫 😡
- This is because we can not do mod at each step as this incurs multiplicative k-blow up at step k

- Put different $y = c_1, \ldots, c_{d_0}$ and try to solve for $g_i^{=k}$
- Does this work?

  Answer : No! 😫 😡
- This is because we can not do mod at each step as this incurs multiplicative k-blow up at step k
- Can we do without taking mod at each step?

- Put different $y = c_1, \ldots, c_{d_0}$ and try to solve for $g_i^{=k}$
- Does this work?

  Answer : No!
- This is because we can not do mod at each step as this incurs multiplicative k-blow up at step k
- Can we do without taking mod at each step?

  Answer : Yes! We can!

Self-correcting Behavior

Self-correcting Behavior

- Suppose we have $\tilde{g}_{i,k-1}$'s such that $\tilde{g}_{i,k-1} \equiv g_i^{\leq k-1} \bmod \langle \overline{x} \rangle^k$

Self-correcting Behavior

- Suppose we have $\tilde{g}_{i,k-1}$'s such that $\tilde{g}_{i,k-1} \equiv g_i^{\leq k-1} \bmod \langle \overline{x} \rangle^k$
- Try to solve for $\sum_{i \in [d_0]} \frac{e_i}{(y-\mu_i)^2} \cdot z_{i,k} \equiv \frac{f'}{f} - \sum_{i \in [d_0]} \frac{e_i}{y - \tilde{g}_{i,k-1}}$

Self-correcting Behavior

- Suppose we have $\tilde{g}_{i,k-1}$'s such that $\tilde{g}_{i,k-1} \equiv g_i^{\leq k-1} \mod \langle \overline{x} \rangle^k$
- Try to solve for $\sum_{i \in [d_0]} \frac{e_i}{(y - \mu_i)^2} \cdot z_{i,k} \equiv \frac{f'}{f} - \sum_{i \in [d_0]} \frac{e_i}{y - \tilde{g}_{i,k-1}}$
- Above equation when taken mod, $z_{i,k} = g_i^{=k}$ is a solution!

Self-correcting Behavior

- Suppose we have $\tilde{g}_{i,k-1}$'s such that $\tilde{g}_{i,k-1} \equiv g_i^{\leq k-1} \bmod \langle \overline{x} \rangle^k$
- Try to solve for $\sum_{i \in [d_0]} \frac{e_i}{(y-\mu_i)^2} \cdot z_{i,k} \equiv \frac{f'}{f} - \sum_{i \in [d_0]} \frac{e_i}{y - \tilde{g}_{i,k-1}}$
- Above equation when taken mod, $z_{i,k} = g_i^{=k}$ is a solution! Is there any relation between solution $z_{i,k}$ and $g_i^{=k}$?

Self-correcting Behavior

- Suppose we have $\tilde{g}_{i,k-1}$'s such that $\tilde{g}_{i,k-1} \equiv g_i^{\leq k-1} \mod \langle \overline{x} \rangle^k$
- Try to solve for $\sum_{i \in [d_0]} \frac{e_i}{(y-\mu_i)^2} \cdot z_{i,k} \equiv \frac{f'}{f} - \sum_{i \in [d_0]} \frac{e_i}{y - \tilde{g}_{i,k-1}}$
- Above equation when taken mod, $z_{i,k} = g_i^{=k}$ is a solution! Is there any relation between solution $z_{i,k}$ and $g_i^{=k}$?
- It can be shown that $\tilde{g}_{i,k-1} + z_{i,k} \equiv g_i^{\leq k} \mod \langle \overline{x} \rangle^{k+1}$

Self-correcting Behavior

- Suppose we have $\tilde{g}_{i,k-1}$'s such that $\tilde{g}_{i,k-1} \equiv g_i^{\leq k-1} \bmod \langle \overline{x} \rangle^k$
- Try to solve for $\sum_{i \in [d_0]} \frac{e_i}{(y-\mu_i)^2} \cdot z_{i,k} \equiv \frac{f'}{f} - \sum_{i \in [d_0]} \frac{e_i}{y - \tilde{g}_{i,k-1}}$
- Above equation when taken mod, $z_{i,k} = g_i^{=k}$ is a solution! Is there any relation between solution $z_{i,k}$ and $g_i^{=k}$?
- It can be shown that $\tilde{g}_{i,k-1} + z_{i,k} \equiv g_i^{\leq k} \bmod \langle \overline{x} \rangle^{k+1}$
- Define $\tilde{g}_{i,k-1} + z_{i,k} := \tilde{g}_{i,k}$

Self-correcting Behavior

- Suppose we have $\tilde{g}_{i,k-1}$'s such that $\tilde{g}_{i,k-1} \equiv g_i^{\leq k-1} \bmod \langle \overline{x} \rangle^k$
- Try to solve for $\sum_{i \in [d_0]} \frac{e_i}{(y-\mu_i)^2} \cdot z_{i,k} \equiv \frac{f'}{f} - \sum_{i \in [d_0]} \frac{e_i}{y - \tilde{g}_{i,k-1}}$
- Above equation when taken mod, $z_{i,k} = g_i^{=k}$ is a solution! Is there any relation between solution $z_{i,k}$ and $g_i^{=k}$?
- It can be shown that $\tilde{g}_{i,k-1} + z_{i,k} \equiv g_i^{\leq k} \bmod \langle \overline{x} \rangle^{k+1}$
- Define $\tilde{g}_{i,k-1} + z_{i,k} := \tilde{g}_{i,k}$
- So the idea is solve each step without the mod and take the cumulative sum

Size Bound

- We choose $y = c_1, \ldots, c_{d_0}$ and solve $z_{i,k}$'s. How does a solution look like in terms of $\tilde{g}_{i,k-1}$?

Size Bound

- We choose $y = c_1, \ldots, c_{d_0}$ and solve $z_{i,k}$'s. How does a solution look like in terms of $\tilde{g}_{i,k-1}$?
- $z_{1,k}$ looks like

$$z_{1,k} = \sum_{j \in [d_0]} \beta_j \left(\frac{f'}{f} - \sum_{i \in [d_0]} \frac{e_i}{y - \tilde{g}_{i,k-1}} \right) \Big|_{y=c_j}$$

Size Bound

- We choose $y = c_1, \ldots, c_{d_0}$ and solve $z_{i,k}$'s. How does a solution look like in terms of $\tilde{g}_{i,k-1}$?
- $z_{1,k}$ looks like

$$z_{1,k} = \sum_{j \in [d_0]} \beta_j \left(\frac{f'}{f} - \sum_{i \in [d_0]} \frac{e_i}{y - \tilde{g}_{i,k-1}} \right) \Big|_{y=c_j}$$

- Like the previous one, compute $z_{i,k}$'s and hence $\tilde{g}_{i,k}$'s as circuit with division gates allowed

Size Bound

- We choose $y = c_1, \ldots, c_{d_0}$ and solve $z_{i,k}$'s. How does a solution look like in terms of $\tilde{g}_{i,k-1}$?
- $z_{1,k}$ looks like

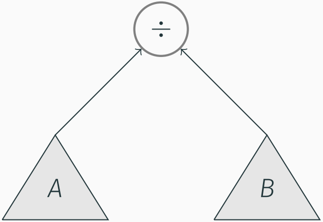
$$z_{1,k} = \sum_{j \in [d_0]} \beta_j \left(\frac{f'}{f} - \sum_{i \in [d_0]} \frac{e_i}{y - \tilde{g}_{i,k-1}} \right) \Big|_{y=c_j}$$

- Like the previous one, compute $z_{i,k}$'s and hence $\tilde{g}_{i,k}$'s as circuit with division gates allowed
- One can show that it has $\text{poly}(s, d_0)$ size circuit with division

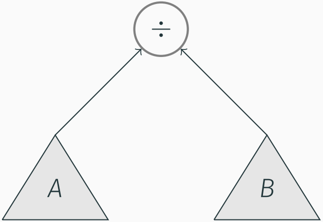
- Push the division gate at the top

- Push the division gate at the top

- In this case, we can show that after d_0 steps, the resulting division circuit has invertible denominator.



- Push the division gate at the top
- In this case, we can show that after d_0 steps, the resulting division circuit has invertible denominator.



- This is because f evaluated at c_j's are invertible

- In contrast, in the previous case we had $f(y_t)$ as denominator which would be non-invertible

- In contrast, in the previous case we had $f(y_t)$ as denominator which would be non-invertible
- So one can eliminate division. Ultimately each g_i upto approximation d_0. So, elimination at the end only blows up the size by multiplicative d_0^2. Altogether, each $g_i^{\leq d_0}$ has poly(s, d_0) circuit

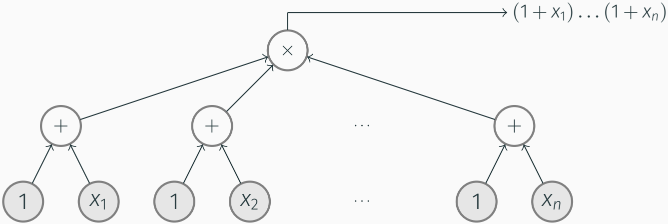
- In contrast, in the previous case we had $f(y_t)$ as denominator which would be non-invertible

- So one can eliminate division. Ultimately each g_i upto approximation d_0. So, elimination at the end only blows up the size by multiplicative d_0^2. Altogether, each $g_i^{\leq d_0}$ has $\text{poly}(s, d_0)$ circuit

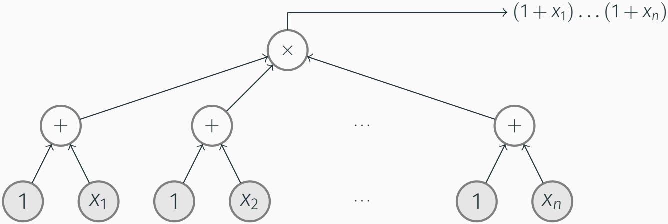
- Hence any irreducible factor (hence any factor) has $\text{poly}(s, d_0)$-size circuit 😄 😄

Some closure results

Arithmetic Formula



Arithmetic Formula



- Tree
- Leaves containing variables or constants

Factoring in other models

- Does a polynomial f of degree d which can be computed by a formula of size s have factors of poly(s, d)-formula size?

Factoring in other models

- Does a polynomial f of degree d which can be computed by a formula of size s have factors of poly(s, d)-formula size?

- Yet not known! In particular, VF is *not known* to be closed under factoring! 

Factoring in other models

- Does a polynomial f of degree d which can be computed by a formula of size s have factors of poly(s, d)-formula size?
- Yet not known! In particular, VF is *not known* to be closed under factoring! 😢
- VF contains family of polynomials of n-variate polynomials computed by $n^{O(1)}$-sized formulas (similarly for VBP, the corresponding class for ABP's)

Factoring in other models

- Does a polynomial f of degree d which can be computed by a formula of size s have factors of poly(s, d)-formula size?

- Yet not known! In particular, VF is *not known* to be closed under factoring! 😰

- VF contains family of polynomials of n-variate polynomials computed by $n^{O(1)}$-sized formulas (similarly for VBP, the corresponding class for ABP's)

- (Oliveira'15) Constant degree $f(\bar{x})$ of size s computed by a formula or circuit resp. has factors of size poly(s) in the respective model

Factoring in other models

- Does a polynomial f of degree d which can be computed by a formula of size s have factors of poly(s, d)-formula size?

- Yet not known! In particular, VF is *not known* to be closed under factoring! 😢

- VF contains family of polynomials of n-variate polynomials computed by $n^{O(1)}$-sized formulas (similarly for VBP, the corresponding class for ABP's)

- (Oliveira'15) Constant degree $f(\bar{x})$ of size s computed by a formula or circuit resp. has factors of size poly(s) in the respective model

Closure Results

Quasi-poly sized algebraic classes

$\{f_n\}_n \in \mathsf{VF}(n^{\log n})$ (resp. $\mathsf{VBP}(n^{\log n})$) such that n-variate f_n can be computed by an algebraic formula (resp. ABP) of size $n^{O(\log n)}$ and has degree poly(n).

Closure Results

Quasi-poly sized algebraic classes

$\{f_n\}_n \in \mathrm{VF}(n^{\log n})$ (resp. $\mathrm{VBP}(n^{\log n})$) such that n-variate f_n can be computed by an algebraic formula (resp. ABP) of size $n^{O(\log n)}$ and has degree poly(n).

Theorem 2

$\mathrm{VF}(n^{\log n})$ (resp. $\mathrm{VBP}(n^{\log n})$) is *closed* under factoring.

Closure Results

Quasi-poly sized algebraic classes

$\{f_n\}_n \in \mathrm{VF}(n^{\log n})$ (resp. $\mathrm{VBP}(n^{\log n})$) such that n-variate f_n can be computed by an algebraic formula (resp. ABP) of size $n^{O(\log n)}$ and has degree poly(n).

Theorem 2

$\mathrm{VF}(n^{\log n})$ (resp. $\mathrm{VBP}(n^{\log n})$) is *closed* under factoring.
Moreover,there exists a `randomized` poly($n^{\log n}$)-time algorithm that: for a given $n^{O(\log n)}$ sized formula (resp. ABP) f of poly(n)-degree, outputs $n^{O(\log n)}$ sized formula (resp. ABP) of a nontrivial factor of f (if one exists).

Bounding size of factor of formula

Goal: Given f of formula size $n^{\log n}$ and degree $n^{O(1)}$, show upper bound on size of its factors

Bounding size of factor of formula

Goal: Given f of formula size $n^{\log n}$ and degree $n^{O(1)}$, show upper bound on size of its factors

- Suppose $(y - g)^e \mid\mid f(\tau\overline{x})$

Bounding size of factor of formula

Goal: Given f of formula size $n^{\log n}$ and degree $n^{O(1)}$, show upper bound on size of its factors

- Suppose $(y - g)^e \mid\mid f(\tau\bar{x})$
- One can show that if f of degree d has s size formula, then $\frac{\partial^k f}{\partial y^k}$ has poly(s, d) size formula

Bounding size of factor of formula

Goal: Given f of formula size $n^{\log n}$ and degree $n^{O(1)}$, show upper bound on size of its factors

- Suppose $(y-g)^e \mid\mid f(\tau\overline{x})$
- One can show that if f of degree d has s size formula, then $\frac{\partial^k f}{\partial y^k}$ has $\mathrm{poly}(s,d)$ size formula
- differentiate $e-1$ times and use NI

Bounding size of factor of formula

Goal: Given f of formula size $n^{\log n}$ and degree $n^{O(1)}$, show upper bound on size of its factors

- Suppose $(y-g)^e \mid\mid f(\tau\bar{x})$
- One can show that if f of degree d has s size formula, then $\frac{\partial^k f}{\partial y^k}$ has $\mathrm{poly}(s,d)$ size formula
- differentiate $e-1$ times and use NI
- $g^{\leq d}$ will have size $n^{O(\log n)}$ formula

Bounding size of factor of formula

Goal: Given f of formula size $n^{\log n}$ and degree $n^{O(1)}$, show upper bound on size of its factors

- Suppose $(y-g)^e \,||\, f(\tau\bar{x})$
- One can show that if f of degree d has s size formula, then $\frac{\partial^k f}{\partial y^k}$ has poly(s, d) size formula
- differentiate $e-1$ times and use NI
- $g^{\leq d}$ will have size $n^{O(\log n)}$ formula
- Algorithm is non-trivial, uses idea by kaltofen

Closure of VNP

Definition of VNP

A family $\{f_n\}_n$ is in VNP if there exist polynomials $s(n), t(n)$ and a family $\{g_n\}_n$ in VP such that for every n,
$f_n(\bar{x}) = \sum_{w \in \{0,1\}^{t(n)}} g_n(\bar{x}, w_1, \ldots, w_{t(n)})$ where $\mathrm{size}(g_n) \leq s(n)$.

Closure of VNP

Definition of VNP

A family $\{f_n\}_n$ is in VNP if there exist polynomials $s(n), t(n)$ and a family $\{g_n\}_n$ in VP such that for every n,
$f_n(\bar{x}) = \sum_{w \in \{0,1\}^{t(n)}} g_n(\bar{x}, w_1, \ldots, w_{t(n)})$ where $\text{size}(g_n) \leq s(n)$.

What about closure property of VNP under factoring?

Closure of VNP

Definition of VNP

A family $\{f_n\}_n$ is in VNP if there exist polynomials $s(n), t(n)$ and a family $\{g_n\}_n$ in VP such that for every n, $f_n(\bar{x}) = \sum_{w \in \{0,1\}^{t(n)}} g_n(\bar{x}, w_1, \ldots, w_{t(n)})$ where $\text{size}(g_n) \leq s(n)$.

What about closure property of VNP under factoring?We define VNP($n^{\log n}$) if we allow $s(n)$ and $t(n)$ to be $n^{O(\log n)}$. We showed that:

Closure of VNP

Definition of VNP

A family $\{f_n\}_n$ is in VNP if there exist polynomials $s(n), t(n)$ and a family $\{g_n\}_n$ in VP such that for every n,
$f_n(\bar{x}) = \sum_{w \in \{0,1\}^{t(n)}} g_n(\bar{x}, w_1, \ldots, w_{t(n)})$ where $\text{size}(g_n) \leq s(n)$.

What about closure property of VNP under factoring?We define VNP($n^{\log n}$) if we allow $s(n)$ and $t(n)$ to be $n^{O(\log n)}$. We showed that:

Theorem 2 continued

VNP($n^{\log n}$) is closed under factoring

Closure of VNP

Definition of VNP

A family $\{f_n\}_n$ is in VNP if there exist polynomials $s(n), t(n)$ and a family $\{g_n\}_n$ in VP such that for every n,
$f_n(\bar{x}) = \sum_{w \in \{0,1\}^{t(n)}} g_n(\bar{x}, w_1, \ldots, w_{t(n)})$ where $\text{size}(g_n) \leq s(n)$.

What about closure property of VNP under factoring?We define VNP($n^{\log n}$) if we allow $s(n)$ and $t(n)$ to be $n^{O(\log n)}$. We showed that:

Theorem 2 continued

VNP($n^{\log n}$) is closed under factoring

It `was` conjectured that VNP is closed under factoring (Bürgisser).

Closure of VNP

Definition of VNP

A family $\{f_n\}_n$ is in VNP if there exist polynomials $s(n), t(n)$ and a family $\{g_n\}_n$ in VP such that for every n,
$f_n(\bar{x}) = \sum_{w \in \{0,1\}^{t(n)}} g_n(\bar{x}, w_1, \ldots, w_{t(n)})$ where $\text{size}(g_n) \leq s(n)$.

What about closure property of VNP under factoring?We define VNP($n^{\log n}$) if we allow $s(n)$ and $t(n)$ to be $n^{O(\log n)}$. We showed that:

Theorem 2 continued

VNP($n^{\log n}$) is closed under factoring

It `was` conjectured that VNP is closed under factoring (Bürgisser). This has been very recently shown to be true by Chou, Kumar and Solomon.

Closure of VNP

Definition of VNP

A family $\{f_n\}_n$ is in VNP if there exist polynomials $s(n), t(n)$ and a family $\{g_n\}_n$ in VP such that for every n,
$f_n(\bar{x}) = \sum_{w \in \{0,1\}^{t(n)}} g_n(\bar{x}, w_1, \ldots, w_{t(n)})$ where $\text{size}(g_n) \leq s(n)$.

What about closure property of VNP under factoring?We define $\text{VNP}(n^{\log n})$ if we allow $s(n)$ and $t(n)$ to be $n^{O(\log n)}$. We showed that:

Theorem 2 continued

$\text{VNP}(n^{\log n})$ is closed under factoring

It `was` conjectured that VNP is closed under factoring (Bürgisser). This has been very recently shown to be true by Chou, Kumar and Solomon. NI technique can also be used to derive the result as well!

Open Problems

Open Problems

- Prove/Disprove Factor Conjecture

Open Problems

- Prove/Disprove Factor Conjecture
- Can we eliminate division for $\frac{A}{B}$ mod $\langle \overline{x} \rangle^d$ when B is non-invertible? (one can show that this implies Factor Conjecture (DSS'18))

Open Problems

- Prove/Disprove Factor Conjecture
- Can we eliminate division for $\frac{A}{B} \bmod \langle \overline{x} \rangle^d$ when B is non-invertible? (one can show that this implies Factor Conjecture (DSS'18))
- Prove or disprove that VF (resp. VBP) is closed under factoring

Open Problems

- Prove/Disprove Factor Conjecture
- Can we eliminate division for $\frac{A}{B}$ mod $\langle \overline{x} \rangle^d$ when B is non-invertible? (one can show that this implies Factor Conjecture (DSS'18))
- Prove or disprove that VF (resp. VBP) is closed under factoring

THANK YOU! 😄