# On the Universality of border width-2 ABPs over characteristic 2

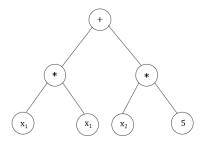
Joint work with Pranjal Dutta, Balagopal Komarath, Harshil Mittal, and Saraswati Nanoti.

Dhara Thakkar Indian Institute of Technology Gandhinagar, India.

31<sup>st</sup> March, 2023

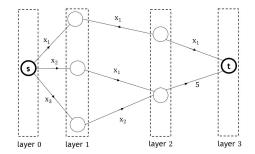
Workshop on Algebraic Complexity Theory 2023

- Basic definitions and terminologies
- Background
- Approximation and Allender-Wang polynomial
- ✤ Universality of ABPs of width-2 with approximation

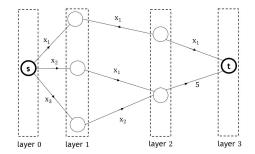


 $x_1^2 + 5x_2$ 

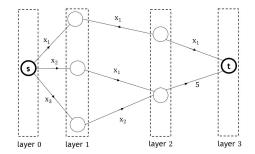
VF consists of families of polynomial with polynomially bounded formula size.



VBP consists of families of polynomial that have ABPs of polynomially bounded size.

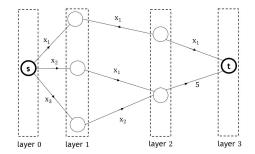


VBP consists of families of polynomial that have ABPs of polynomially bounded size. ABPs with restricted edge labels [BIZ, J. ACM, 2016]:



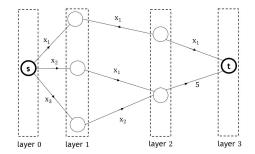
VBP consists of families of polynomial that have ABPs of polynomially bounded size. ABPs with restricted edge labels [BIZ, J. ACM, 2016]:

\* Weakest ABP: Edges are labeled by variables or constants.



VBP consists of families of polynomial that have ABPs of polynomially bounded size. ABPs with restricted edge labels [BIZ, J. ACM, 2016]:

- \* Weakest ABP: Edges are labeled by variables or constants.
- \* Weak ABP: Edges are labeled by simple affine linear forms  $\alpha x_i + \beta, \alpha, \beta \in \mathcal{F}$ .

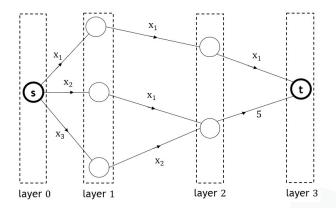


VBP consists of families of polynomial that have ABPs of polynomially bounded size. ABPs with restricted edge labels [BIZ, J. ACM, 2016]:

- \* Weakest ABP: Edges are labeled by variables or constants.
- \* Weak ABP: Edges are labeled by simple affine linear forms  $\alpha x_i + \beta, \alpha, \beta \in \mathcal{F}$ .
- We use Weakest ABP.



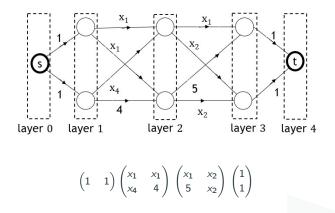
The width of an ABP is the maximum number of nodes in a layer.



Here, the width is 3.

# ABPs and Matrix Multiplication

#### **ABPs and Matrix Multiplication**



This computes the polynomial  $x_1^2 + 2x_1x_2 + x_2x_4 + x_1x_4 + 5x_1 + 4x_2 + 20$ .

# Background/Motivation



ABPs are 'at least as powerful' as formulas.
 Precisely, VF ⊆ VBP.

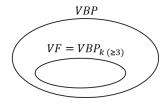


- ABPs are 'at least as powerful' as formulas.
   Precisely, VF ⊆ VBP.
- \* What if we restrict the width of ABPs to some fixed  $k \ge 3$ ?



- ABPs are 'at least as powerful' as formulas.
   Precisely, VF ⊆ VBP.
- ★ What if we restrict the width of ABPs to some fixed k ≥ 3? VBP<sub>k</sub> consists of families that have width-k ABPs of polynomially bounded size.

- ABPs are 'at least as powerful' as formulas.
   Precisely, VF ⊆ VBP.
- What if we restrict the width of ABPs to some fixed k ≥ 3?
   VBP<sub>k</sub> consists of families that have width-k ABPs of polynomially bounded size.
   VBP<sub>k</sub> = VF [Ben-Or and Cleve, SIAM J. Comp., 1992].





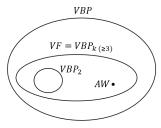
- ✤ VBP<sub>2</sub> <sup>?</sup> = VF.
- \* The polynomial AW =  $\sum_{i=1}^{8} x_{2i-1} x_{2i}$  cannot be computed by any width-2 ABP [Allender and Wang, CC, 2016].

- ★  $VBP_2 \stackrel{?}{=} VF.$
- \* The polynomial AW =  $\sum_{i=1}^{8} x_{2i-1} x_{2i}$  cannot be computed by any width-2 ABP [Allender and Wang, CC, 2016].
- ★  $VBP_2 \subsetneq VF$ .



- ✤ VBP<sub>2</sub> <sup>?</sup> = VF.
- \* The polynomial AW =  $\sum_{i=1}^{8} x_{2i-1} x_{2i}$  cannot be computed by any width-2 ABP [Allender and Wang, CC, 2016].
- ★  $VBP_2 \subsetneq VF$ .

That is width-2 ABPs are 'strictly less powerful' than formulas.



•  $VBP_2 \stackrel{?}{=} VF.$ 

- \* The polynomial AW =  $\sum_{i=1}^{8} x_{2i-1} x_{2i}$  cannot be computed by any width-2 ABP [Allender and Wang, CC, 2016].
- ★  $VBP_2 \subsetneq VF$ .

That is width-2 ABPs are 'strictly less powerful' than formulas.

•  $VBP_2 \stackrel{?}{=} VF.$ 

- \* The polynomial AW =  $\sum_{i=1}^{8} x_{2i-1} x_{2i}$  cannot be computed by any width-2 ABP [Allender and Wang, CC, 2016].
- ★  $VBP_2 \subsetneq VF$ .

That is width-2 ABPs are 'strictly less powerful' than formulas.

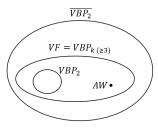
What if we allow 'approximation'?

✤ VBP<sub>2</sub> <sup>?</sup> = VF.

- \* The polynomial AW =  $\sum_{i=1}^{8} x_{2i-1} x_{2i}$  cannot be computed by any width-2 ABP [Allender and Wang, CC, 2016].
- ★  $VBP_2 \subsetneq VF$ .

That is width-2 ABPs are 'strictly less powerful' than formulas.

 What if we allow 'approximation'? Then, they become 'at least as powerful' as formulas<sup>1</sup>.



# Algebraic Approximation



**Definition:** The approximation closure  $\overline{C}(\mathbb{F})$  consists of families  $(f_n)$  for which there exists a family  $(g_n) \in C(\mathbb{F}(\epsilon))$  such that  $g_n$  approximates  $f_n$  for all n.

**Definition:** The approximation closure  $\overline{C}(\mathbb{F})$  consists of families  $(f_n)$  for which there exists a family  $(g_n) \in C(\mathbb{F}(\epsilon))$  such that  $g_n$  approximates  $f_n$  for all n.

In addition, if we restrict the error degree to be polynomially bounded in *n* then the class obtained is called *poly-approximation closure*, denoted as  $\overline{C}^{\text{poly}}(\mathbb{F})$ .

**Definition:** The approximation closure  $\overline{C}(\mathbb{F})$  consists of families  $(f_n)$  for which there exists a family  $(g_n) \in C(\mathbb{F}(\epsilon))$  such that  $g_n$  approximates  $f_n$  for all n.

In addition, if we restrict the error degree to be polynomially bounded in *n* then the class obtained is called *poly-approximation closure*, denoted as  $\overline{C}^{\text{poly}}(\mathbb{F})$ .

★ AW  $\notin$  VBP<sub>2</sub>  $\subsetneq$  VF.

**Definition:** The approximation closure  $\overline{C}(\mathbb{F})$  consists of families  $(f_n)$  for which there exists a family  $(g_n) \in C(\mathbb{F}(\epsilon))$  such that  $g_n$  approximates  $f_n$  for all n.

In addition, if we restrict the error degree to be polynomially bounded in *n* then the class obtained is called *poly-approximation closure*, denoted as  $\overline{C}^{\text{poly}}(\mathbb{F})$ .

- ★ AW  $\notin$  VBP<sub>2</sub>  $\subsetneq$  VF.
- ★ Is AW  $\in \overline{VBP_2}$ ?



Define F(x, y) :=

$$\begin{pmatrix} \frac{1}{\epsilon} - \frac{\epsilon x}{2} & -\frac{x}{2\epsilon} \\ \epsilon^3 & \epsilon \end{pmatrix} \begin{pmatrix} \frac{1}{2}(x-2y)\epsilon^2 + 1 & \frac{1}{2}(x-2y) \\ \epsilon^2 & 1 \end{pmatrix} \begin{pmatrix} \frac{x\epsilon^2}{2} + 1 & -\frac{x}{2} \\ -\epsilon^2 & 1 \end{pmatrix} \begin{pmatrix} \frac{x+2y}{2\epsilon} & \epsilon \\ \epsilon^{-1} & 0 \end{pmatrix}$$

Define F(x, y) :=

$$\begin{pmatrix} \frac{1}{\epsilon} - \frac{\epsilon x}{2} & -\frac{x}{2\epsilon} \\ \epsilon^3 & \epsilon \end{pmatrix} \begin{pmatrix} \frac{1}{2}(x-2y)\epsilon^2 + 1 & \frac{1}{2}(x-2y) \\ \epsilon^2 & 1 \end{pmatrix} \begin{pmatrix} \frac{x\epsilon^2}{2} + 1 & -\frac{x}{2} \\ -\epsilon^2 & 1 \end{pmatrix} \begin{pmatrix} \frac{x+2y}{2\epsilon} & \epsilon \\ \epsilon^{-1} & 0 \end{pmatrix}$$

$$F(x,y) = \begin{pmatrix} xy + \mathcal{O}(\epsilon) & 1 + \mathcal{O}(\epsilon) \\ 1 + \mathcal{O}(\epsilon) & 0 + \mathcal{O}(\epsilon) \end{pmatrix} = \begin{pmatrix} xy & 1 \\ 1 & 0 \end{pmatrix} + \mathcal{O}(\epsilon).$$

Define F(x, y) :=

$$\begin{pmatrix} \frac{1}{\epsilon} - \frac{\epsilon x}{2} & -\frac{x}{2\epsilon} \\ \epsilon^3 & \epsilon \end{pmatrix} \begin{pmatrix} \frac{1}{2}(x-2y)\epsilon^2 + 1 & \frac{1}{2}(x-2y) \\ \epsilon^2 & 1 \end{pmatrix} \begin{pmatrix} \frac{x\epsilon^2}{2} + 1 & -\frac{x}{2} \\ -\epsilon^2 & 1 \end{pmatrix} \begin{pmatrix} \frac{x+2y}{2\epsilon} & \epsilon \\ \epsilon^{-1} & 0 \end{pmatrix}$$

$$F(x,y) = \begin{pmatrix} xy + \mathcal{O}(\epsilon) & 1 + \mathcal{O}(\epsilon) \\ 1 + \mathcal{O}(\epsilon) & 0 + \mathcal{O}(\epsilon) \end{pmatrix} = \begin{pmatrix} xy & 1 \\ 1 & 0 \end{pmatrix} + \mathcal{O}(\epsilon).$$

The following sequence approximately computes AW

$$\begin{pmatrix} 1 & 0 \end{pmatrix} F(x_1, x_2) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} F(x_{15}, x_{16}) \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

# Question: Can AW be computed approximately even when $char(\mathbb{F}) = 2$ ? Yes!



# Question: Can AW be computed approximately even when $char(\mathbb{F}) = 2$ ? Yes!

Define 
$$F(x, y) := \begin{pmatrix} \frac{1}{\epsilon} & 0\\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 1\\ 1 & 0 \end{pmatrix} \begin{pmatrix} \epsilon & 1\\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\epsilon} & y\\ -1 & 1 \end{pmatrix} \begin{pmatrix} x & 1\\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0\\ 1 & -\epsilon \end{pmatrix}.$$

## Question: Can AW be computed approximately even when $char(\mathbb{F}) = 2$ ? Yes!

Define 
$$F(x, y) := \begin{pmatrix} \frac{1}{\epsilon} & 0\\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 1\\ 1 & 0 \end{pmatrix} \begin{pmatrix} \epsilon & 1\\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\epsilon} & y\\ -1 & 1 \end{pmatrix} \begin{pmatrix} x & 1\\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0\\ 1 & -\epsilon \end{pmatrix}.$$
  
 $F(x, y) \text{ computes } \begin{pmatrix} xy & 1\\ 1+\epsilon y & 0 \end{pmatrix}.$ 

Question: Can AW be computed approximately even when  $char(\mathbb{F}) = 2$ ? Yes!

Define 
$$F(x, y) := \begin{pmatrix} \frac{1}{\epsilon} & 0\\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 1\\ 1 & 0 \end{pmatrix} \begin{pmatrix} \epsilon & 1\\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\epsilon} & y\\ -1 & 1 \end{pmatrix} \begin{pmatrix} x & 1\\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0\\ 1 & -\epsilon \end{pmatrix}$$
.  
 $F(x, y) \text{ computes } \begin{pmatrix} xy & 1\\ 1+\epsilon y & 0 \end{pmatrix}$ .

The following sequence approximately computes AW

$$\begin{pmatrix} 1 & 0 \end{pmatrix} F(x_1, x_2) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} F(x_{15}, x_{16}) \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Question: Can AW be computed approximately even when  $char(\mathbb{F}) = 2$ ? Yes!

Define 
$$F(x, y) := \begin{pmatrix} \frac{1}{\epsilon} & 0\\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 1\\ 1 & 0 \end{pmatrix} \begin{pmatrix} \epsilon & 1\\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\epsilon} & y\\ -1 & 1 \end{pmatrix} \begin{pmatrix} x & 1\\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0\\ 1 & -\epsilon \end{pmatrix}$$
.  
 $F(x, y) \text{ computes } \begin{pmatrix} xy & 1\\ 1+\epsilon y & 0 \end{pmatrix}$ .

The following sequence approximately computes AW

$$\begin{pmatrix} 1 & 0 \end{pmatrix} F(x_1, x_2) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} F(x_{15}, x_{16}) \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Note: This is true for arbitrary field.





- \* AW  $\in \overline{VBP_2}$
- $\bullet \ \mathsf{VF} \stackrel{?}{\subseteq} \overline{\mathsf{VBP}_2}.$



- $\clubsuit \ \mathsf{AW} \in \overline{\mathsf{VBP}_2}$
- $\bullet VF \stackrel{?}{\subseteq} \overline{VBP_2}.$
- \* If we allow for approximation, it becomes 'at least as powerful' as formulas.

- $\clubsuit \ \mathsf{AW} \in \overline{\mathsf{VBP}_2}$
- $\clubsuit \ \mathsf{VF} \stackrel{?}{\subseteq} \overline{\mathsf{VBP}_2}.$
- \* If we allow for approximation, it becomes 'at least as powerful' as formulas. Precisely,  $VF \subseteq \overline{VBP_2}$  when  $char(\mathbb{F}) \neq 2$  [BIZ, J. ACM, 2016].

- ★ AW  $\in \overline{VBP_2}$
- VF  $\stackrel{?}{\subseteq} \overline{VBP_2}$ .
- \* If we allow for approximation, it becomes 'at least as powerful' as formulas. Precisely,  $VF \subseteq \overline{VBP_2}$  when  $char(\mathbb{F}) \neq 2$  [BIZ, J. ACM, 2016].
- \*  $\overline{VF} = \overline{VBP_2}$  when char( $\mathbb{F}$ )  $\neq 2$  [BIZ, J. ACM, 2016].

 $VF \subset \overline{VBP_2}^{poly}$  when  $char(\mathbb{F}) \neq 2$ .



 $VF \subset \overline{VBP_2}^{poly}$  when  $char(\mathbb{F}) \neq 2$ .

Proof Idea:



 $VF \subset \overline{VBP_2}^{poly}$  when  $char(\mathbb{F}) \neq 2$ .

## Proof Idea:

✤ Use induction on the depth to show

depth *d*- formula  $\implies$  sequence of  $2^{\mathcal{O}(d)}$  matrices.



 $VF \subset \overline{VBP_2}^{poly}$  when  $char(\mathbb{F}) \neq 2$ .

## Proof Idea:

✤ Use induction on the depth to show

 $\begin{array}{rcl} & \mbox{depth $d$- formula} \implies \mbox{sequence of } 2^{\mathcal{O}(d)} \mbox{ matrices.} \\ & & \mbox{} \mathcal{Q}(f) := \begin{pmatrix} f & 1 \\ 1 & 0 \end{pmatrix}. \end{array}$ 



 $VF \subset \overline{VBP_2}^{poly}$  when  $char(\mathbb{F}) \neq 2$ .

#### Proof Idea:

✤ Use induction on the depth to show

depth *d*- formula  $\implies$  sequence of  $2^{\mathcal{O}(d)}$  matrices. \*  $Q(f) := \begin{pmatrix} f & 1 \\ 1 & 0 \end{pmatrix}$ . \* Q(f+g) = Q(f)Q(0)Q(g)



 $VF \subset \overline{VBP_2}^{poly}$  when  $char(\mathbb{F}) \neq 2$ .

#### Proof Idea:

Use induction on the depth to show

 $\begin{array}{rcl} \operatorname{depth} d\text{- formula} & \Longrightarrow & \operatorname{sequence} \text{ of } 2^{\mathcal{O}(d)} \text{ matrices.} \\ & & \mathcal{Q}(f) := \begin{pmatrix} f & 1 \\ 1 & 0 \end{pmatrix}. \\ & & \mathcal{Q}(f+g) = \mathcal{Q}(f)\mathcal{Q}(0)\mathcal{Q}(g) \end{array}$ 



 $VF \subset \overline{VBP_2}^{poly}$  when  $char(\mathbb{F}) \neq 2$ .

## Proof Idea:

Use induction on the depth to show

 $\begin{array}{rcl} \operatorname{depth} d\text{- formula} \implies \operatorname{sequence} \operatorname{of} 2^{\mathcal{O}(d)} \operatorname{matrices.} \\ & & Q(f) := \begin{pmatrix} f & 1 \\ 1 & 0 \end{pmatrix}. \\ & & Q(f+g) = Q(f)Q(0)Q(g) \\ & & Q(f \cdot g)? \end{array}$ 

$$f \cdot g = (f/2 + g)^2 + (-(f/2)^2) + (-g^2)$$

 $VF \subset \overline{VBP_2}^{poly}$  when  $char(\mathbb{F}) \neq 2$ .

### Proof Idea:

Use induction on the depth to show

depth *d*- formula  $\implies$  sequence of  $2^{\mathcal{O}(d)}$  matrices. \*  $Q(f) := \begin{pmatrix} f & 1 \\ 1 & 0 \end{pmatrix}$ . \* Q(f+g) = Q(f)Q(0)Q(g)

✤ Q(f · g)?

$$f \cdot g = (f/2 + g)^2 + (-(f/2)^2) + (-g^2)$$

$$Q(f^2 + \mathcal{O}(\epsilon)) = Q(-\epsilon^{-1}) \cdot Q(\epsilon) \cdot Q(-\epsilon^{-1}) \cdot (Q(f + \mathcal{O}(\epsilon^3))) \cdot Q(1) \cdot Q(-1) \cdot Q(1) \cdot Q(-\epsilon^2) \cdot (Q(f + \mathcal{O}(\epsilon^3))) \cdot Q(-\epsilon^{-1}) \cdot Q(\epsilon^{-1}) \cdot Q(1) \cdot Q(\epsilon^{-1} - 1)$$

 $VF \subset \overline{VBP_2}^{poly}$  when  $char(\mathbb{F}) \neq 2$ .

#### Proof Idea:

Use induction on the depth to show

depth *d*- formula  $\implies$  sequence of  $2^{\mathcal{O}(d)}$  matrices. \*  $Q(f) := \begin{pmatrix} f & 1 \\ 1 & 0 \end{pmatrix}$ . \* Q(f+g) = Q(f)Q(0)Q(g)

$$f \cdot g = (f/2 + g)^2 + (-(f/2)^2) + (-g^2)$$

$$Q(f^2 + \mathcal{O}(\epsilon)) = Q(-\epsilon^{-1}) \cdot Q(\epsilon) \cdot Q(-\epsilon^{-1}) \cdot (Q(f + \mathcal{O}(\epsilon^3))) \cdot Q(1) \cdot Q(-1) \cdot Q(1) \cdot Q(-\epsilon^2) \cdot (Q(f + \mathcal{O}(\epsilon^3))) \cdot Q(-\epsilon^{-1}) \cdot Q(\epsilon^{-1}) \cdot Q(1) \cdot Q(\epsilon^{-1} - 1)$$

Thus,  $\overline{VF} = \overline{VBP_2}$  when  $char(\mathbb{F}) \neq 2$ 



\* Is  $VF \subset \overline{VBP_2}$  even when  $\operatorname{char}(\mathbb{F}) = 2$ ?



\* Is  $VF \subset \overline{VBP_2}$  even when  $char(\mathbb{F}) = 2$ ? We still do not know!



- Is VF ⊂ VBP<sub>2</sub> even when char(F) = 2?
   We still do not know!
- Is the Model universal? .... (i.e. can every polynomial be approximately computed using width-2 ABP (or seq. of 2 × 2 matrices?)

- Is VF ⊂ VBP<sub>2</sub> even when char(F) = 2?
   We still do not know!
- Is the Model universal? .... (i.e. can every polynomial be approximately computed using width-2 ABP (or seq. of 2 × 2 matrices?) Yes!

Let f be a polynomial. Suppose that there is a sequence, say  $\sigma$ , of N matrices that approximately computes Q(f). Then, for any indeterminate x, there is a sequence of 2N + 4 matrices that approximately computes  $Q(f_X)$ .



Let f be a polynomial. Suppose that there is a sequence, say  $\sigma$ , of N matrices that approximately computes Q(f). Then, for any indeterminate x, there is a sequence of 2N + 4 matrices that approximately computes  $Q(f_X)$ .

## Proof Sketch:

$$Q(f_{\mathbf{X}}) + \mathcal{O}(\epsilon) = \begin{pmatrix} \frac{1}{\epsilon} & 0\\ 0 & 1 \end{pmatrix} \sigma \mid_{\epsilon \to \epsilon^{2}} \begin{pmatrix} \epsilon & 1\\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\epsilon} & x\\ -1 & 1 \end{pmatrix} \sigma \mid_{\epsilon \to \epsilon^{2}} \begin{pmatrix} 1 & 0\\ 1 & -\epsilon \end{pmatrix}$$

Let f be a polynomial. Suppose that there is a sequence, say  $\sigma$ , of N matrices that approximately computes Q(f). Then, for any indeterminate x, there is a sequence of 2N + 4 matrices that approximately computes  $Q(f_X)$ .

### Proof Sketch:

$$Q(f_{X}) + \mathcal{O}(\epsilon) = \begin{pmatrix} \frac{1}{\epsilon} & 0\\ 0 & 1 \end{pmatrix} \sigma \mid_{\epsilon \to \epsilon^{2}} \begin{pmatrix} \epsilon & 1\\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\epsilon} & x\\ -1 & 1 \end{pmatrix} \sigma \mid_{\epsilon \to \epsilon^{2}} \begin{pmatrix} 1 & 0\\ 1 & -\epsilon \end{pmatrix}.$$

 Although not as powerful as multiplying two arbitrary polynomials, this proves universality.

Let f be a polynomial. Suppose that there is a sequence, say  $\sigma$ , of N matrices that approximately computes Q(f). Then, for any indeterminate x, there is a sequence of 2N + 4 matrices that approximately computes  $Q(f_X)$ .

#### Proof Sketch:

$$Q(f_{X}) + \mathcal{O}(\epsilon) = \begin{pmatrix} \frac{1}{\epsilon} & 0\\ 0 & 1 \end{pmatrix} \sigma \mid_{\epsilon \to \epsilon^{2}} \begin{pmatrix} \epsilon & 1\\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\epsilon} & x\\ -1 & 1 \end{pmatrix} \sigma \mid_{\epsilon \to \epsilon^{2}} \begin{pmatrix} 1 & 0\\ 1 & -\epsilon \end{pmatrix}.$$

- Although not as powerful as multiplying two arbitrary polynomials, this proves universality.
- However, this is inefficient.

For example, consider  $x^n$ , we require  $\mathcal{O}(2^n)$  matrices to compute  $Q(x^n)$ .

Let f be a polynomial. Suppose that there is a sequence, say  $\sigma$ , of N matrices that approximately computes Q(f). Then, for any indeterminate x, there is a sequence of 2N + 4 matrices that approximately computes  $Q(f_X)$ .

## Proof Sketch:

$$Q(f_{X}) + \mathcal{O}(\epsilon) = \begin{pmatrix} \frac{1}{\epsilon} & 0\\ 0 & 1 \end{pmatrix} \sigma \mid_{\epsilon \to \epsilon^{2}} \begin{pmatrix} \epsilon & 1\\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\epsilon} & x\\ -1 & 1 \end{pmatrix} \sigma \mid_{\epsilon \to \epsilon^{2}} \begin{pmatrix} 1 & 0\\ 1 & -\epsilon \end{pmatrix}.$$

- Although not as powerful as multiplying two arbitrary polynomials, this proves universality.
- However, this is inefficient.

For example, consider  $x^n$ , we require  $\mathcal{O}(2^n)$  matrices to compute  $Q(x^n)$ .

\* We improve this to  $\mathcal{O}(n)$ .



Let f and g be polynomials. Suppose that there are sequences, say  $\sigma$  and  $\pi$ , of N and M matrices, that approximately compute Q(f) and Q(g) respectively. Then, there is a sequence of N + 2M + 4 matrices that approximately computes  $Q(fg^2)$ .



Let f and g be polynomials. Suppose that there are sequences, say  $\sigma$  and  $\pi$ , of N and M matrices, that approximately compute Q(f) and Q(g) respectively. Then, there is a sequence of N + 2M + 4 matrices that approximately computes  $Q(fg^2)$ .

#### Proof Sketch:

$$Q(fg^2) + \mathcal{O}(\epsilon) = \begin{pmatrix} -1 & 0 \\ 0 & \epsilon \end{pmatrix} \pi \mid_{\epsilon \to \epsilon^2} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\epsilon} \end{pmatrix} \sigma \mid_{\epsilon \to \epsilon^3} \begin{pmatrix} -1 & 0 \\ 0 & \frac{1}{\epsilon} \end{pmatrix} \pi \mid_{\epsilon \to \epsilon^2} \begin{pmatrix} 1 & 0 \\ 0 & \epsilon \end{pmatrix}.$$

Let f and g be polynomials. Suppose that there are sequences, say  $\sigma$  and  $\pi$ , of N and M matrices, that approximately compute Q(f) and Q(g) respectively. Then, there is a sequence of N + 2M + 4 matrices that approximately computes  $Q(fg^2)$ .

#### **Proof Sketch:**

$$Q(fg^2) + \mathcal{O}(\epsilon) = \begin{pmatrix} -1 & 0 \\ 0 & \epsilon \end{pmatrix} \pi \mid_{\epsilon \to \epsilon^2} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\epsilon} \end{pmatrix} \sigma \mid_{\epsilon \to \epsilon^3} \begin{pmatrix} -1 & 0 \\ 0 & \frac{1}{\epsilon} \end{pmatrix} \pi \mid_{\epsilon \to \epsilon^2} \begin{pmatrix} 1 & 0 \\ 0 & \epsilon \end{pmatrix}.$$

#### Theorem

Let p be a polynomial with  $\ell$  monomials, each containing at most t indeterminates. Then, Q(p) can be approximately computed using a sequence of at most  $O(\ell \cdot (2^t + degree(p)))$  matrices.

Let f and g be polynomials. Suppose that there are sequences, say  $\sigma$  and  $\pi$ , of N and M matrices, that approximately compute Q(f) and Q(g) respectively. Then, there is a sequence of N + 2M + 4 matrices that approximately computes  $Q(fg^2)$ .

#### **Proof Sketch:**

$$Q(fg^2) + \mathcal{O}(\epsilon) = \begin{pmatrix} -1 & 0 \\ 0 & \epsilon \end{pmatrix} \pi \mid_{\epsilon \to \epsilon^2} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\epsilon} \end{pmatrix} \sigma \mid_{\epsilon \to \epsilon^3} \begin{pmatrix} -1 & 0 \\ 0 & \frac{1}{\epsilon} \end{pmatrix} \pi \mid_{\epsilon \to \epsilon^2} \begin{pmatrix} 1 & 0 \\ 0 & \epsilon \end{pmatrix}.$$

#### Theorem

Let p be a polynomial with  $\ell$  monomials, each containing at most t indeterminates. Then, Q(p) can be approximately computed using a sequence of at most  $O(\ell \cdot (2^t + degree(p)))$  matrices.

Observe that  $x^n$  needs only O(n) matrices.

# Improving efficiency cont.

## Improving efficiency cont.

#### Theorem:

Sequence of  $\mathcal{O}(\ell \cdot (2^t + degree(p)))$  matrices that approximately computes Q(p) where,

 $\ell = no.$  of monomials in p

 $t = \max$  no. of indeterminates per monomial



#### Theorem:

Sequence of  $O(\ell \cdot (2^t + degree(p)))$  matrices that approximately computes Q(p) where,  $\ell = \text{no. of monomials in } p$  $t = \max \text{ no. of indeterminates per monomial}$ 

## Proof Idea:

\* Goal: Compute each monomial using at most  $\mathcal{O}(2^t + degree(p))$  matrices.

#### Theorem:

Sequence of  $O(\ell \cdot (2^t + degree(p)))$  matrices that approximately computes Q(p) where,  $\ell = \text{no. of monomials in } p$  $t = \max \text{ no. of indeterminates per monomial}$ 

## Proof Idea:

\* Goal: Compute each monomial using at most  $\mathcal{O}(2^t + degree(p))$  matrices.

\* Let 
$$\underbrace{X_1^{r_1} \cdots X_k^{r_k}}_{\text{odd } r'_i \text{s}} \underbrace{X_{k+1}^{r_{k+1}} \cdots X_m^{r_m}}_{\text{even } r'_i \text{s}}$$

#### Theorem:

Sequence of  $O(\ell \cdot (2^t + degree(p)))$  matrices that approximately computes Q(p) where,  $\ell = \text{no. of monomials in } p$  $t = \max \text{ no. of indeterminates per monomial}$ 

### Proof Idea:

\* Goal: Compute each monomial using at most  $\mathcal{O}(2^t + degree(p))$  matrices.

\* Let 
$$\underbrace{X_1^{r_1}\cdots X_k^{r_k}}_{\text{odd }r_i^{\prime}s}\underbrace{X_{k+1}^{r_{k+1}}\cdots X_m^{r_m}}_{\text{even }r_i^{\prime}s} = (X_1\cdots X_k)\cdot (X_1^{r_1-1}\cdots X_k^{r_k-1}X_{k+1}^{r_{k+1}}\cdots X_m^{r_m})$$

#### Theorem:

Sequence of  $O(\ell \cdot (2^t + degree(p)))$  matrices that approximately computes Q(p) where,  $\ell = \text{no. of monomials in } p$  $t = \max \text{ no. of indeterminates per monomial}$ 

### Proof Idea:

\* Goal: Compute each monomial using at most  $O(2^t + degree(p))$  matrices.

$$Let \underbrace{X_1^{r_1} \cdots X_k^{r_k}}_{\text{odd } r_i^{\prime} s} \underbrace{X_{k+1}^{r_{k+1}} \cdots X_m^{r_m}}_{\text{even } r_i^{\prime} s} = (X_1 \cdots X_k) \cdot (X_1^{r_1-1} \cdots X_k^{r_k-1} X_{k+1}^{r_{k+1}} \cdots X_m^{r_m})$$

**Corollary:** Let p be a univariate polynomial of degree d. Then Q(p) can be approximately computed using a sequence of at most  $O(d^2)$  matrices.

#### Theorem:

Sequence of  $O(\ell \cdot (2^t + degree(p)))$  matrices that approximately computes Q(p) where,  $\ell = \text{no. of monomials in } p$  $t = \max \text{ no. of indeterminates per monomial}$ 

### Proof Idea:

\* Goal: Compute each monomial using at most  $\mathcal{O}(2^t + degree(p))$  matrices.

$$Let \underbrace{X_1^{r_1} \cdots X_k^{r_k}}_{\text{odd } r_i^{\prime} s} \underbrace{X_{k+1}^{r_{k+1}} \cdots X_m^{r_m}}_{\text{even } r_i^{\prime} s} = (X_1 \cdots X_k) \cdot (X_1^{r_1-1} \cdots X_k^{r_k-1} X_{k+1}^{r_{k+1}} \cdots X_m^{r_m})$$

**Corollary:** Let p be a univariate polynomial of degree d. Then Q(p) can be approximately computed using a sequence of at most  $O(d^2)$  matrices.

Note: However, we can do better!

#### Theorem

Consider a degree-d univariate polynomial in x, say  $p = a_d x^d + a_{d-1} x^{d-1} + \dots + a_2 x^2 + a_1 x + a_0$ . Then, Q(p) can be approximately computed using a sequence of at most O(d) matrices.



### Theorem

Consider a degree-d univariate polynomial in x, say  $p = a_d x^d + a_{d-1} x^{d-1} + \dots + a_2 x^2 + a_1 x + a_0$ . Then, Q(p) can be approximately computed using a sequence of at most O(d) matrices.

Idea: Use Horner's rule



### Theorem

Consider a degree-d univariate polynomial in x, say  $p = a_d x^d + a_{d-1} x^{d-1} + \dots + a_2 x^2 + a_1 x + a_0$ . Then, Q(p) can be approximately computed using a sequence of at most O(d) matrices.

Idea: Use Horner's rule

$$a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = (a_4x^2 + a_3x + a_2)x^2 + a_1x + a_0$$

### Theorem

Consider a degree-d univariate polynomial in x, say  $p = a_d x^d + a_{d-1} x^{d-1} + \dots + a_2 x^2 + a_1 x + a_0$ . Then, Q(p) can be approximately computed using a sequence of at most O(d) matrices.

Idea: Use Horner's rule

$$a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = (a_4x^2 + a_3x + a_2)x^2 + a_1x + a_0$$
  
 $Q(a_4) \xrightarrow{\text{Lemma 2}} Q(a_4x^2)$ 

### Theorem

Consider a degree-d univariate polynomial in x, say  $p = a_d x^d + a_{d-1} x^{d-1} + \dots + a_2 x^2 + a_1 x + a_0$ . Then, Q(p) can be approximately computed using a sequence of at most O(d) matrices.

Idea: Use Horner's rule

$$a_{4}x^{4} + a_{3}x^{3} + a_{2}x^{2} + a_{1}x + a_{0} = (a_{4}x^{2} + a_{3}x + a_{2})x^{2} + a_{1}x + a_{0}.$$

$$Q(a_{4}) \xrightarrow{\text{Lemma 2}} Q(a_{4}x^{2})$$

$$\downarrow \text{append } Q(0) \begin{pmatrix} a_{3} & a_{2} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & \frac{1}{a_{3}} \\ 1 & 0 \end{pmatrix}$$

$$Q(a_{4}x^{2} + a_{3}x + a_{2})$$

#### Theorem

Consider a degree-d univariate polynomial in x, say  $p = a_d x^d + a_{d-1} x^{d-1} + \dots + a_2 x^2 + a_1 x + a_0$ . Then, Q(p) can be approximately computed using a sequence of at most O(d) matrices.

Idea: Use Horner's rule

$$a_{4}x^{4} + a_{3}x^{3} + a_{2}x^{2} + a_{1}x + a_{0} = (a_{4}x^{2} + a_{3}x + a_{2})x^{2} + a_{1}x + a_{0}.$$

$$Q(a_{4}) \xrightarrow{\text{Lemma 2}} Q(a_{4}x^{2})$$

$$\downarrow \text{append } Q(0) \begin{pmatrix} a_{3} & a_{2} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & \frac{1}{a_{3}} \\ 1 & 0 \end{pmatrix}$$

$$Q(a_{4}x^{2} + a_{3}x + a_{2}) \xrightarrow{\text{Lemma 2}} Q((a_{4}x^{2} + a_{3}x + a_{2})x^{2})$$

### Theorem

Consider a degree-d univariate polynomial in x, say  $p = a_d x^d + a_{d-1} x^{d-1} + \dots + a_2 x^2 + a_1 x + a_0$ . Then, Q(p) can be approximately computed using a sequence of at most O(d) matrices.

Idea: Use Horner's rule



Seq. of N matrices that ?	Seq. of $\mathcal{O}(rN)$ matrices that
approximately computes $Q(f)$	approximately computes $Q(f^r)$

Seq. of *N* matrices that 
$$\xrightarrow{?}$$
 Seq. of  $\mathcal{O}(rN)$  matrices that approximately computes  $Q(f)$ 

$$Q(1) \xrightarrow{\text{Lemma 2}} Q(f^2) \xrightarrow{\text{Lemma 2}} \cdots \xrightarrow{\text{Lemma 2}} Q(f^{r-2}) \xrightarrow{\text{Lemma 2}} Q(f^{r-2})$$

Seq. of N matrices that 
$$\stackrel{?}{\Longrightarrow}$$
 Seq. of  $\mathcal{O}(rN)$  matrices that approximately computes  $Q(f)$ 

~

.

$$Q(1) \xrightarrow{\text{Lemma 2}}{2N+4} Q(f^2) \xrightarrow{\text{Lemma 2}}{2N+4} \cdots \xrightarrow{\text{Lemma 2}}{2N+4} Q(f^{r-2}) \xrightarrow{\text{Lemma 2}}{2N+4} Q(f^r)$$
$$Q(f) \xrightarrow{\text{Lemma 2}}{2N+4} Q(f^3) \xrightarrow{\text{Lemma 2}}{2N+4} \cdots \xrightarrow{\text{Lemma 2}}{2N+4} Q(f^{r-2}) \xrightarrow{\text{Lemma 2}}{2N+4} Q(f^r)$$

~



\* 
$$Q(f), Q(g) \implies Q(f+g)?$$
  
Easy!



- \*  $Q(f), Q(g) \implies Q(f+g)?$ Easy!
- \*  $Q(f) \implies Q(f^n)?$ Easy!



- \*  $Q(f), Q(g) \implies Q(f+g)?$ Easy!
- $Q(f) \implies Q(f^n)?$ Easy!
- Why is powering interesting?
   Can this compute non-sparse polynomials?



- \*  $Q(f), Q(g) \implies Q(f+g)?$ Easy!
- \*  $Q(f) \implies Q(f^n)?$ Easy!
- Why is powering interesting?
   Can this compute non-sparse polynomials?
   Yes!

**Observation:** There is an *n*-variate polynomial over  $\mathbb{F}$  with  $2^{\Omega(n)}$  monomials that can be approximately computed using a sequence of  $n^{\mathcal{O}(1)}$  matrices, when  $\operatorname{char}(\mathbb{F}) = 2$ .

\* The model (i.e. width-2 ABPs with approximation) is Universal.



\* The model (i.e. width-2 ABPs with approximation) is Universal.

**Open Problems** 



\* The model (i.e. width-2 ABPs with approximation) is Universal.

### **Open Problems**

\* Is  $Q(x_1x_2\cdots x_n)$  computable efficiently?

\* The model (i.e. width-2 ABPs with approximation) is Universal.

### **Open Problems**

- \* Is  $Q(x_1x_2\cdots x_n)$  computable efficiently?
- \* Can we compute  $Q(f_X)$  using a single Q(f)?



\* The model (i.e. width-2 ABPs with approximation) is Universal.

### **Open Problems**

- \* Is  $Q(x_1x_2\cdots x_n)$  computable efficiently?
- \* Can we compute  $Q(f_X)$  using a single Q(f)?

Can we compute Q(fg) using constant many Q(f)'s and Q(g)'s?

\* The model (i.e. width-2 ABPs with approximation) is Universal.

### **Open Problems**

- \* Is  $Q(x_1x_2\cdots x_n)$  computable efficiently?
- \* Can we compute  $Q(f_X)$  using a single Q(f)?

Can we compute Q(fg) using constant many Q(f)'s and Q(g)'s?

Can we show some lower bound for  $Q(f \cdot g)$ ?

\* The model (i.e. width-2 ABPs with approximation) is Universal.

### **Open Problems**

- \* Is  $Q(x_1x_2\cdots x_n)$  computable efficiently?
- \* Can we compute  $Q(f_X)$  using a single Q(f)?

Can we compute Q(fg) using constant many Q(f)'s and Q(g)'s?

Can we show some lower bound for  $Q(f \cdot g)$ ?

\* Can we construct small size width-two ABPs for sparse polynomials?

\* The model (i.e. width-2 ABPs with approximation) is Universal.

#### **Open Problems**

- \* Is  $Q(x_1x_2\cdots x_n)$  computable efficiently?
- \* Can we compute  $Q(f_X)$  using a single Q(f)?

Can we compute Q(fg) using constant many Q(f)'s and Q(g)'s?

Can we show some lower bound for  $Q(f \cdot g)$ ?

- \* Can we construct small size width-two ABPs for sparse polynomials?
- \* Is VF  $\subset \overline{VBP_2}$  when  $char(\mathbb{F}) = 2$ ?

\* The model (i.e. width-2 ABPs with approximation) is Universal.

#### **Open Problems**

- \* Is  $Q(x_1x_2\cdots x_n)$  computable efficiently?
- \* Can we compute  $Q(f_X)$  using a single Q(f)?

Can we compute Q(fg) using constant many Q(f)'s and Q(g)'s?

Can we show some lower bound for  $Q(f \cdot g)$ ?

- \* Can we construct small size width-two ABPs for sparse polynomials?
- \* Is VF  $\subset \overline{VBP_2}$  when  $char(\mathbb{F}) = 2$ ?