## 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<br>Indian Institute of Technology Gandhinagar, India.<br>31 ${ }^{\text {st }}$ March, 2023<br>Workshop on Algebraic Complexity Theory 2023

## Table of Contents

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


## Arithmetic Formula



$$
x_{1}^{2}+5 x_{2}
$$

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

## Algebraic Branching Programs (ABP)



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

## Algebraic Branching Programs (ABP)



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

## Algebraic Branching Programs (ABP)



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.


## Algebraic Branching Programs (ABP)



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 $\alpha x_{i}+\beta, \alpha, \beta \in \mathcal{F}$.


## Algebraic Branching Programs (ABP)



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.


## Width of an ABP

## Width of an 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 $x_{1}^{2}+2 x_{1} x_{2}+x_{2} x_{4}+x_{1} x_{4}+5 x_{1}+4 x_{2}+20$.

## Background/Motivation

* ABPs are 'at least as powerful' as formulas. Precisely, VF $\subseteq$ VBP.


## Background/Motivation

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


## Background/Motivation

* ABPs are 'at least as powerful' as formulas. Precisely, VF $\subseteq$ VBP.
* What if we restrict the width of ABPs to some fixed $k \geq 3$ ?
$V^{\prime} P_{k}$ consists of families that have width- $k$ ABPs of polynomially bounded size.


## Background/Motivation

* ABPs are 'at least as powerful' as formulas.

Precisely, VF $\subseteq$ VBP.

* What if we restrict the width of ABPs to some fixed $k \geq 3$ ? $V B P_{k}$ consists of families that have width- $k$ ABPs of polynomially bounded size. $V^{\prime} P_{k}=$ VF [Ben-Or and Cleve, SIAM J. Comp., 1992].



## Background/Motivation

* $\mathrm{VBP}_{2} \stackrel{?}{=} \mathrm{VF}$.


## Background/Motivation

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


## Background/Motivation

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


## Background/Motivation

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

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


## Background/Motivation

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

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

[^0]
## Background/Motivation

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

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

* What if we allow 'approximation'?

[^1]
## Background/Motivation

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

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 ${ }^{1}$.


[^2]
## Algebraic Approximation

## Algebraic Approximation

Definition: A polynomial $g \in \mathbb{F}(\epsilon)[X]$ approximates $f \in \mathbb{F}[X]$ with error degree $e$ if $g=f+\epsilon h_{1}+\epsilon^{2} h_{2}+\cdots+\epsilon^{e} h_{e}$ where each $h_{i} \in \mathbb{F}[X]$.

## Algebraic Approximation

Definition: A polynomial $g \in \mathbb{F}(\epsilon)[X]$ approximates $f \in \mathbb{F}[X]$ with error degree e if $g=f+\epsilon h_{1}+\epsilon^{2} h_{2}+\cdots+\epsilon^{e} h_{e}$ where each $h_{i} \in \mathbb{F}[X]$.

Definition: The approximation closure $\bar{C}(\mathbb{F})$ consists of families $\left(f_{n}\right)$ for which there exists a family $\left(g_{n}\right) \in C(\mathbb{F}(\epsilon))$ such that $g_{n}$ approximates $f_{n}$ for all $n$.

## Algebraic Approximation

Definition: A polynomial $g \in \mathbb{F}(\epsilon)[X]$ approximates $f \in \mathbb{F}[X]$ with error degree $e$ if $g=f+\epsilon h_{1}+\epsilon^{2} h_{2}+\cdots+\epsilon^{e} h_{e}$ where each $h_{i} \in \mathbb{F}[X]$.

Definition: The approximation closure $\bar{C}(\mathbb{F})$ consists of families $\left(f_{n}\right)$ for which there exists a family $\left(g_{n}\right) \in C(\mathbb{F}(\epsilon))$ such that $g_{n}$ approximates $f_{n}$ for all $n$.

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

## Algebraic Approximation

Definition: A polynomial $g \in \mathbb{F}(\epsilon)[X]$ approximates $f \in \mathbb{F}[X]$ with error degree $e$ if $g=f+\epsilon h_{1}+\epsilon^{2} h_{2}+\cdots+\epsilon^{e} h_{e}$ where each $h_{i} \in \mathbb{F}[X]$.

Definition: The approximation closure $\bar{C}(\mathbb{F})$ consists of families $\left(f_{n}\right)$ for which there exists a family $\left(g_{n}\right) \in C(\mathbb{F}(\epsilon))$ such that $g_{n}$ approximates $f_{n}$ for all $n$.

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

* $\mathrm{AW} \notin \mathrm{VBP}_{2} \subsetneq \mathrm{VF}$.


## Algebraic Approximation

Definition: A polynomial $g \in \mathbb{F}(\epsilon)[X]$ approximates $f \in \mathbb{F}[X]$ with error degree $e$ if $g=f+\epsilon h_{1}+\epsilon^{2} h_{2}+\cdots+\epsilon^{e} h_{e}$ where each $h_{i} \in \mathbb{F}[X]$.

Definition: The approximation closure $\bar{C}(\mathbb{F})$ consists of families $\left(f_{n}\right)$ for which there exists a family $\left(g_{n}\right) \in C(\mathbb{F}(\epsilon))$ such that $g_{n}$ approximates $f_{n}$ for all $n$.

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

* $\mathrm{AW} \notin \mathrm{VBP}_{2} \subsetneq \mathrm{VF}$.
* Is $\mathrm{AW} \in \overline{\mathrm{VBP}_{2}}$ ?


## Approximation Helps

The polynomial $\mathrm{AW}=\sum_{i=1}^{8} x_{2 i-1} x_{2 i}$ can be approximated by width-2 ABP when $\operatorname{char}(\mathbb{F}) \neq 2$ [BIZ, J.ACM 2018].

## Approximation Helps

The polynomial $\mathrm{AW}=\sum_{i=1}^{8} x_{2 i-1} x_{2 i}$ can be approximated by width-2 ABP when $\operatorname{char}(\mathbb{F}) \neq 2$ [BIZ, J.ACM 2018].

Define $F(x, y):=$

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

## Approximation Helps

The polynomial AW $=\sum_{i=1}^{8} x_{2 i-1} x_{2 i}$ can be approximated by width-2 ABP when $\operatorname{char}(\mathbb{F}) \neq 2$ [BIZ, J.ACM 2018].

Define $F(x, y):=$

$$
\begin{aligned}
& \left(\begin{array}{cc}
\frac{1}{\epsilon}-\frac{\epsilon x}{2} & -\frac{x}{2 \epsilon} \\
\epsilon^{3} & \epsilon
\end{array}\right)\left(\begin{array}{cc}
\frac{1}{2}(x-2 y) \epsilon^{2}+1 & \frac{1}{2}(x-2 y) \\
\epsilon^{2} & 1
\end{array}\right)\left(\begin{array}{cc}
\frac{x \epsilon^{2}}{2}+1 & -\frac{x}{2} \\
-\epsilon^{2} & 1
\end{array}\right)\left(\begin{array}{cc}
\frac{x+2 y}{2 \epsilon} & \epsilon \\
\epsilon^{-1} & 0
\end{array}\right) \\
& F(x, y)=\left(\begin{array}{cc}
x y+\mathcal{O}(\epsilon) & 1+\mathcal{O}(\epsilon) \\
1+\mathcal{O}(\epsilon) & 0+\mathcal{O}(\epsilon)
\end{array}\right)=\left(\begin{array}{cc}
x y & 1 \\
1 & 0
\end{array}\right)+\mathcal{O}(\epsilon) .
\end{aligned}
$$

## Approximation Helps

The polynomial AW $=\sum_{i=1}^{8} x_{2 i-1} x_{2 i}$ can be approximated by width-2 ABP when $\operatorname{char}(\mathbb{F}) \neq 2$ [BIZ, J.ACM 2018].

Define $F(x, y):=$

$$
\begin{aligned}
& \left(\begin{array}{cc}
\frac{1}{\epsilon}-\frac{\epsilon x}{2} & -\frac{x}{2 \epsilon} \\
\epsilon^{3} & \epsilon
\end{array}\right)\left(\begin{array}{cc}
\frac{1}{2}(x-2 y) \epsilon^{2}+1 & \frac{1}{2}(x-2 y) \\
\epsilon^{2} & 1
\end{array}\right)\left(\begin{array}{cc}
\frac{x \epsilon^{2}}{2}+1 & -\frac{x}{2} \\
-\epsilon^{2} & 1
\end{array}\right)\left(\begin{array}{cc}
\frac{x+2 y}{2 \epsilon} & \epsilon \\
\epsilon^{-1} & 0
\end{array}\right) \\
& F(x, y)=\left(\begin{array}{cc}
x y+\mathcal{O}(\epsilon) & 1+\mathcal{O}(\epsilon) \\
1+\mathcal{O}(\epsilon) & 0+\mathcal{O}(\epsilon)
\end{array}\right)=\left(\begin{array}{cc}
x y & 1 \\
1 & 0
\end{array}\right)+\mathcal{O}(\epsilon) .
\end{aligned}
$$

The following sequence approximately computes AW

$$
\left(\begin{array}{ll}
1 & 0
\end{array}\right) F\left(x_{1}, x_{2}\right)\left(\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right) \cdots\left(\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right) F\left(x_{15}, x_{16}\right)\binom{1}{0} .
$$

## Approximately computing AW when $\operatorname{char}(\mathbb{F})=2$

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

## Approximately computing AW when $\operatorname{char}(\mathbb{F})=2$

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

$$
\text { Define } F(x, y):=\left(\begin{array}{cc}
\frac{1}{\epsilon} & 0 \\
0 & 1
\end{array}\right)\left(\begin{array}{ll}
x & 1 \\
1 & 0
\end{array}\right)\left(\begin{array}{cc}
\epsilon & 1 \\
0 & 1
\end{array}\right)\left(\begin{array}{cc}
\frac{1}{\epsilon} & y \\
-1 & 1
\end{array}\right)\left(\begin{array}{cc}
x & 1 \\
1 & 0
\end{array}\right)\left(\begin{array}{cc}
1 & 0 \\
1 & -\epsilon
\end{array}\right) \text {. }
$$

## Approximately computing AW when $\operatorname{char}(\mathbb{F})=2$

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

Define $F(x, y):=\left(\begin{array}{cc}\frac{1}{\epsilon} & 0 \\ 0 & 1\end{array}\right)\left(\begin{array}{ll}x & 1 \\ 1 & 0\end{array}\right)\left(\begin{array}{ll}\epsilon & 1 \\ 0 & 1\end{array}\right)\left(\begin{array}{cc}\frac{1}{\epsilon} & y \\ -1 & 1\end{array}\right)\left(\begin{array}{cc}x & 1 \\ 1 & 0\end{array}\right)\left(\begin{array}{cc}1 & 0 \\ 1 & -\epsilon\end{array}\right)$.
$F(x, y)$ computes $\left(\begin{array}{cc}x y & 1 \\ 1+\epsilon y & 0\end{array}\right)$.

## Approximately computing AW when $\operatorname{char}(\mathbb{F})=2$

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

Define $F(x, y):=\left(\begin{array}{cc}\frac{1}{\epsilon} & 0 \\ 0 & 1\end{array}\right)\left(\begin{array}{ll}x & 1 \\ 1 & 0\end{array}\right)\left(\begin{array}{ll}\epsilon & 1 \\ 0 & 1\end{array}\right)\left(\begin{array}{cc}\frac{1}{\epsilon} & y \\ -1 & 1\end{array}\right)\left(\begin{array}{cc}x & 1 \\ 1 & 0\end{array}\right)\left(\begin{array}{cc}1 & 0 \\ 1 & -\epsilon\end{array}\right)$.
$F(x, y)$ computes $\left(\begin{array}{cc}x y & 1 \\ 1+\epsilon y & 0\end{array}\right)$.
The following sequence approximately computes AW

$$
\left(\begin{array}{ll}
1 & 0
\end{array}\right) F\left(x_{1}, x_{2}\right)\left(\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right) \cdots\left(\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right) F\left(x_{15}, x_{16}\right)\binom{1}{0} .
$$

## Approximately computing AW when $\operatorname{char}(\mathbb{F})=2$

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

Define $F(x, y):=\left(\begin{array}{cc}\frac{1}{\epsilon} & 0 \\ 0 & 1\end{array}\right)\left(\begin{array}{ll}x & 1 \\ 1 & 0\end{array}\right)\left(\begin{array}{ll}\epsilon & 1 \\ 0 & 1\end{array}\right)\left(\begin{array}{cc}\frac{1}{\epsilon} & y \\ -1 & 1\end{array}\right)\left(\begin{array}{cc}x & 1 \\ 1 & 0\end{array}\right)\left(\begin{array}{cc}1 & 0 \\ 1 & -\epsilon\end{array}\right)$.
$F(x, y)$ computes $\left(\begin{array}{cc}x y & 1 \\ 1+\epsilon y & 0\end{array}\right)$.
The following sequence approximately computes AW

$$
\left(\begin{array}{ll}
1 & 0
\end{array}\right) F\left(x_{1}, x_{2}\right)\left(\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right) \cdots\left(\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right) F\left(x_{15}, x_{16}\right)\binom{1}{0} .
$$

Note: This is true for arbitrary field.

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

Theorem (BIZ, J. ACM, 2016)
$\mathrm{VF} \subset{\overline{\mathrm{VBP}}_{2}}^{\text {poly }}$ when $\operatorname{char}(\mathbb{F}) \neq 2$.

Theorem (BIZ, J. ACM, 2016)
$\mathrm{VF} \subset{\overline{\mathrm{VBP}}_{2}}^{\text {poly }}$ when $\operatorname{char}(\mathbb{F}) \neq 2$.

## Proof Idea:

Theorem (BIZ, J. ACM, 2016)
$\mathrm{VF} \subset \overline{\mathrm{VBP}}^{\text {poly }}$ when $\operatorname{char}(\mathbb{F}) \neq 2$.

## Proof Idea:

* Use induction on the depth to show

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

Theorem (BIZ, J. ACM, 2016)
$\mathrm{VF} \subset{\overline{\mathrm{VBP}}_{2}}^{\text {poly }}$ when $\operatorname{char}(\mathbb{F}) \neq 2$.

## Proof Idea:

* Use induction on the depth to show

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

* $Q(f):=\left(\begin{array}{ll}f & 1 \\ 1 & 0\end{array}\right)$.


## Theorem (BIZ, J. ACM, 2016)

$\mathrm{VF} \subset{\overline{\mathrm{VBP}}_{2}}^{\text {poly }}$ when $\operatorname{char}(\mathbb{F}) \neq 2$.

## Proof Idea:

* Use induction on the depth to show

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

## Theorem (BIZ, J. ACM, 2016)

$\mathrm{VF} \subset{\overline{\mathrm{VBP}}_{2}}^{\text {poly }}$ when $\operatorname{char}(\mathbb{F}) \neq 2$.

## Proof Idea:

* Use induction on the depth to show

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

* $Q(f):=\left(\begin{array}{ll}f & 1 \\ 1 & 0\end{array}\right)$.
* $Q(f+g)=Q(f) Q(0) Q(g)$
* $Q(f \cdot g)$ ?

Theorem (BIZ, J. ACM, 2016)
$\mathrm{VF} \subset{\overline{\mathrm{VBP}}_{2}}^{\text {poly }}$ when $\operatorname{char}(\mathbb{F}) \neq 2$.

## Proof Idea:

* Use induction on the depth to show

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

* $Q(f):=\left(\begin{array}{ll}f & 1 \\ 1 & 0\end{array}\right)$.
* $Q(f+g)=Q(f) Q(0) Q(g)$
* $Q(f \cdot g)$ ?

$$
f \cdot g=(f / 2+g)^{2}+\left(-(f / 2)^{2}\right)+\left(-g^{2}\right)
$$

## Theorem (BIZ, J. ACM, 2016)

$\mathrm{VF} \subset{\overline{\mathrm{VBP}}_{2}}^{\text {poly }}$ when $\operatorname{char}(\mathbb{F}) \neq 2$.

## Proof Idea:

* Use induction on the depth to show

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

* $Q(f):=\left(\begin{array}{ll}f & 1 \\ 1 & 0\end{array}\right)$.
* $Q(f+g)=Q(f) Q(0) Q(g)$
* $Q(f \cdot g)$ ?

$$
f \cdot g=(f / 2+g)^{2}+\left(-(f / 2)^{2}\right)+\left(-g^{2}\right)
$$

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

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

## Theorem (BIZ, J. ACM, 2016)

$\mathrm{VF} \subset \overline{\mathrm{VBP}}^{\text {poly }}$ when $\operatorname{char}(\mathbb{F}) \neq 2$.

## Proof Idea:

* Use induction on the depth to show

$$
\begin{aligned}
& \text { depth } d \text { - formula } \Longrightarrow \text { sequence of } 2^{\mathcal{O}(d)} \text { matrices. } \\
& \text { * } Q(f):=\left(\begin{array}{ll}
f & 1 \\
1 & 0
\end{array}\right) \text {. } \\
& \text { * } Q(f+g)=Q(f) Q(0) Q(g) \text { ? }
\end{aligned}
$$

$$
f \cdot g=(f / 2+g)^{2}+\left(-(f / 2)^{2}\right)+\left(-g^{2}\right)
$$

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

Thus, $\overline{\mathrm{VF}}=\overline{\mathrm{VBP}_{2}}$ when $\operatorname{char}(\mathbb{F}) \neq 2$

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

We still do not know!

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

We still do not know!

* Is the Model universal? .... (i.e. can every polynomial be approximately computed using width- 2 ABP (or seq. of $2 \times 2$ matrices?)
* Is $\mathrm{VF} \subset \overline{\mathrm{VBP}_{2}}$ even when $\operatorname{char}(\mathbb{F})=2$ ?

We still do not know!

* Is the Model universal? .... (i.e. can every polynomial be approximately computed using width- 2 ABP (or seq. of $2 \times 2$ matrices?)
Yes!


## Showing Universality

## Lemma 1

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 $2 N+4$ matrices that approximately computes $Q(f x)$.

## Showing Universality

## Lemma 1

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 $2 N+4$ matrices that approximately computes $Q(f x)$.

## Proof Sketch:

$$
Q(f x)+\mathcal{O}(\epsilon)=\left.\left.\left(\begin{array}{cc}
\frac{1}{\epsilon} & 0 \\
0 & 1
\end{array}\right) \sigma\right|_{\epsilon \rightarrow \epsilon^{2}}\left(\begin{array}{cc}
\epsilon & 1 \\
0 & 1
\end{array}\right)\left(\begin{array}{cc}
\frac{1}{\epsilon} & x \\
-1 & 1
\end{array}\right) \sigma\right|_{\epsilon \rightarrow \epsilon^{2}}\left(\begin{array}{cc}
1 & 0 \\
1 & -\epsilon
\end{array}\right)
$$

## Showing Universality

## Lemma 1

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 $2 N+4$ matrices that approximately computes $Q(f x)$.

## Proof Sketch:

$Q(f x)+\mathcal{O}(\epsilon)=\left.\left.\left(\begin{array}{cc}\frac{1}{\epsilon} & 0 \\ 0 & 1\end{array}\right) \sigma\right|_{\epsilon \rightarrow \epsilon^{2}}\left(\begin{array}{ll}\epsilon & 1 \\ 0 & 1\end{array}\right)\left(\begin{array}{cc}\frac{1}{\epsilon} & x \\ -1 & 1\end{array}\right) \sigma\right|_{\epsilon \rightarrow \epsilon^{2}}\left(\begin{array}{cc}1 & 0 \\ 1 & -\epsilon\end{array}\right)$.

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


## Showing Universality

## Lemma 1

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 $2 N+4$ matrices that approximately computes $Q(f x)$.

## Proof Sketch:

$Q(f x)+\mathcal{O}(\epsilon)=\left.\left.\left(\begin{array}{cc}\frac{1}{\epsilon} & 0 \\ 0 & 1\end{array}\right) \sigma\right|_{\epsilon \rightarrow \epsilon^{2}}\left(\begin{array}{ll}\epsilon & 1 \\ 0 & 1\end{array}\right)\left(\begin{array}{cc}\frac{1}{\epsilon} & x \\ -1 & 1\end{array}\right) \sigma\right|_{\epsilon \rightarrow \epsilon^{2}}\left(\begin{array}{cc}1 & 0 \\ 1 & -\epsilon\end{array}\right)$.

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

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

## Showing Universality

## Lemma 1

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 $2 N+4$ matrices that approximately computes $Q(f x)$.

## Proof Sketch:

$Q(f x)+\mathcal{O}(\epsilon)=\left.\left.\left(\begin{array}{cc}\frac{1}{\epsilon} & 0 \\ 0 & 1\end{array}\right) \sigma\right|_{\epsilon \rightarrow \epsilon^{2}}\left(\begin{array}{ll}\epsilon & 1 \\ 0 & 1\end{array}\right)\left(\begin{array}{cc}\frac{1}{\epsilon} & x \\ -1 & 1\end{array}\right) \sigma\right|_{\epsilon \rightarrow \epsilon^{2}}\left(\begin{array}{cc}1 & 0 \\ 1 & -\epsilon\end{array}\right)$.

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

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

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


## Improving efficiency

## Improving efficiency

## Lemma 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 $N+2 M+4$ matrices that approximately computes $Q\left(f g^{2}\right)$.

## Improving efficiency

## Lemma 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 $N+2 M+4$ matrices that approximately computes $Q\left(f g^{2}\right)$.

## Proof Sketch:

$$
Q\left(f g^{2}\right)+\mathcal{O}(\epsilon)=\left.\left.\left.\left(\begin{array}{cc}
-1 & 0 \\
0 & \epsilon
\end{array}\right) \pi\right|_{\epsilon \rightarrow \epsilon^{2}}\left(\begin{array}{cc}
1 & 0 \\
0 & \frac{1}{\epsilon}
\end{array}\right) \sigma\right|_{\epsilon \rightarrow \epsilon^{3}}\left(\begin{array}{cc}
-1 & 0 \\
0 & \frac{1}{\epsilon}
\end{array}\right) \pi\right|_{\epsilon \rightarrow \epsilon^{2}}\left(\begin{array}{cc}
1 & 0 \\
0 & \epsilon
\end{array}\right)
$$

## Improving efficiency

## Lemma 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 $N+2 M+4$ matrices that approximately computes $Q\left(f g^{2}\right)$.
Proof Sketch:

$$
Q\left(f g^{2}\right)+\mathcal{O}(\epsilon)=\left.\left.\left.\left(\begin{array}{cc}
-1 & 0 \\
0 & \epsilon
\end{array}\right) \pi\right|_{\epsilon \rightarrow \epsilon^{2}}\left(\begin{array}{cc}
1 & 0 \\
0 & \frac{1}{\epsilon}
\end{array}\right) \sigma\right|_{\epsilon \rightarrow \epsilon^{3}}\left(\begin{array}{cc}
-1 & 0 \\
0 & \frac{1}{\epsilon}
\end{array}\right) \pi\right|_{\epsilon \rightarrow \epsilon^{2}}\left(\begin{array}{cc}
1 & 0 \\
0 & \epsilon
\end{array}\right)
$$

## 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 $\mathcal{O}\left(\ell \cdot\left(2^{t}+\operatorname{degree}(p)\right)\right)$ matrices.

## Improving efficiency

## Lemma 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 $N+2 M+4$ matrices that approximately computes $Q\left(f g^{2}\right)$.
Proof Sketch:

$$
Q\left(f g^{2}\right)+\mathcal{O}(\epsilon)=\left.\left.\left.\left(\begin{array}{cc}
-1 & 0 \\
0 & \epsilon
\end{array}\right) \pi\right|_{\epsilon \rightarrow \epsilon^{2}}\left(\begin{array}{cc}
1 & 0 \\
0 & \frac{1}{\epsilon}
\end{array}\right) \sigma\right|_{\epsilon \rightarrow \epsilon^{3}}\left(\begin{array}{cc}
-1 & 0 \\
0 & \frac{1}{\epsilon}
\end{array}\right) \pi\right|_{\epsilon \rightarrow \epsilon^{2}}\left(\begin{array}{cc}
1 & 0 \\
0 & \epsilon
\end{array}\right)
$$

## 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 $\mathcal{O}\left(\ell \cdot\left(2^{t}+\operatorname{degree}(p)\right)\right)$ matrices.

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

## Improving efficiency cont.

## Improving efficiency cont.

```
Theorem:
Sequence of }\mathcal{O}(\ell\cdot(\mp@subsup{2}{}{t}+\operatorname{degree}(p)))\mathrm{ matrices that approxi-
mately computes Q(p) where,
\ell= no. of monomials in p
t=max no. of indeterminates per monomial
```


## Improving efficiency cont.

```
Theorem:
Sequence of \mathcal{O}(\ell\cdot(\mp@subsup{2}{}{t}+\operatorname{degree}(p)))\mathrm{ matrices that approxi-}
mately computes Q(p) where,
\ell = \text { no. of monomials in p}
t=max no. of indeterminates per monomial
```


## Proof Idea:

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


## Improving efficiency cont.

## Theorem:

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

## Proof Idea:

* Goal: Compute each monomial using at most $\mathcal{O}\left(2^{t}+\operatorname{degree}(p)\right)$ matrices.
* Let $\underbrace{X_{1}^{r_{1}} \cdots X_{k}^{r_{k}}}_{\text {odd } r_{i}^{\prime} \mathrm{s}} \underbrace{X_{k+1}^{r_{k+1}} \cdots X_{m}^{r_{m}}}_{\text {even } r_{i}^{\prime} \mathrm{s}}$


## Improving efficiency cont.

## Theorem:

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

## Proof Idea:

* Goal: Compute each monomial using at most $\mathcal{O}\left(2^{t}+\operatorname{degree}(p)\right)$ matrices.
* Let $\underbrace{X_{1}^{r_{1}} \cdots X_{k}^{r_{k}}}_{\text {odd } r_{i}^{\prime} \mathrm{s}} \underbrace{X_{k+1}^{r_{k+1}} \cdots X_{m}^{r_{m}}}_{\text {even } r_{i}^{\prime} \mathrm{s}}=\left(X_{1} \cdots X_{k}\right) \cdot\left(X_{1}^{r_{1}-1} \cdots X_{k}^{r_{k}-1} X_{k+1}^{r_{k+1}} \cdots X_{m}^{r_{m}}\right)$


## Improving efficiency cont.

## Theorem:

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

## Proof Idea:

* Goal: Compute each monomial using at most $\mathcal{O}\left(2^{t}+\operatorname{degree}(p)\right)$ matrices.
* Let $\underbrace{X_{1}^{r_{1}} \cdots X_{k}^{r_{k}}}_{\text {odd } r_{i}^{\prime} \mathrm{s}} \underbrace{X_{k+1}^{r_{k+1}} \cdots X_{m}^{r_{m}}}_{\text {even } r_{i}^{\prime} \mathrm{s}}=\left(X_{1} \cdots X_{k}\right) \cdot\left(X_{1}^{r_{1}-1} \cdots X_{k}^{r_{k}-1} X_{k+1}^{r_{k+1}} \cdots X_{m}^{r_{m}}\right)$

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

## Improving efficiency cont.

## Theorem:

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

## Proof Idea:

* Goal: Compute each monomial using at most $\mathcal{O}\left(2^{t}+\operatorname{degree}(p)\right)$ matrices.
* Let $\underbrace{X_{1}^{r_{1}} \cdots X_{k}^{r_{k}}}_{\text {odd } r_{i}^{\prime} \mathrm{s}} \underbrace{X_{k+1}^{r_{k+1}} \cdots X_{m}^{r_{m}}}_{\text {even } r_{i}^{\prime} \mathrm{s}}=\left(X_{1} \cdots X_{k}\right) \cdot\left(X_{1}^{r_{1}-1} \cdots X_{k}^{r_{k}-1} X_{k+1}^{r_{k+1}} \cdots X_{m}^{r_{m}}\right)$

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

Note: However, we can do better!

Improving efficiency Further for univariate polynomial

## Improving efficiency Further for univariate polynomial

## Theorem

Consider a degree-d univariate polynomial in $x$, say
$p=a_{d} x^{d}+a_{d-1} x^{d-1}+\ldots \ldots+a_{2} x^{2}+a_{1} x+a_{0}$. Then, $Q(p)$ can be approximately computed using a sequence of at most $\mathcal{O}(d)$ matrices.

## Improving efficiency Further for univariate polynomial

## Theorem

Consider a degree-d univariate polynomial in $x$, say
$p=a_{d} x^{d}+a_{d-1} x^{d-1}+\ldots . .+a_{2} x^{2}+a_{1} x+a_{0}$. Then, $Q(p)$ can be approximately computed using a sequence of at most $\mathcal{O}(d)$ matrices.

Idea: Use Horner's rule

## Improving efficiency Further for univariate polynomial

## Theorem

Consider a degree-d univariate polynomial in $x$, say
$p=a_{d} x^{d}+a_{d-1} x^{d-1}+\ldots . .+a_{2} x^{2}+a_{1} x+a_{0}$. Then, $Q(p)$ can be approximately computed using a sequence of at most $\mathcal{O}(d)$ matrices.

Idea: Use Horner's rule
Illustration: Consider a polynomial
$a_{4} x^{4}+a_{3} x^{3}+a_{2} x^{2}+a_{1} x+a_{0}=\left(a_{4} x^{2}+a_{3} x+a_{2}\right) x^{2}+a_{1} x+a_{0}$.

## Improving efficiency Further for univariate polynomial

## Theorem

Consider a degree-d univariate polynomial in $x$, say
$p=a_{d} x^{d}+a_{d-1} x^{d-1}+\ldots . .+a_{2} x^{2}+a_{1} x+a_{0}$. Then, $Q(p)$ can be approximately computed using a sequence of at most $\mathcal{O}(d)$ matrices.

Idea: Use Horner's rule
Illustration: Consider a polynomial
$a_{4} x^{4}+a_{3} x^{3}+a_{2} x^{2}+a_{1} x+a_{0}=\left(a_{4} x^{2}+a_{3} x+a_{2}\right) x^{2}+a_{1} x+a_{0}$.
$Q\left(a_{4}\right) \xrightarrow{\text { Lemma } 2} Q\left(a_{4} x^{2}\right)$

## Improving efficiency Further for univariate polynomial

## Theorem

Consider a degree-d univariate polynomial in $x$, say
$p=a_{d} x^{d}+a_{d-1} x^{d-1}+\ldots \ldots+a_{2} x^{2}+a_{1} x+a_{0}$. Then, $Q(p)$ can be approximately computed using a sequence of at most $\mathcal{O}(d)$ matrices.

Idea: Use Horner's rule
Illustration: Consider a polynomial
$a_{4} x^{4}+a_{3} x^{3}+a_{2} x^{2}+a_{1} x+a_{0}=\left(a_{4} x^{2}+a_{3} x+a_{2}\right) x^{2}+a_{1} x+a_{0}$.
$Q\left(a_{4}\right) \xrightarrow{\text { Lemma } 2} Q\left(a_{4} x^{2}\right)$

$$
\begin{aligned}
& \quad \downarrow \text { append } Q(0)\left(\begin{array}{cc}
a_{3} & a_{2} \\
0 & 1
\end{array}\right)\left(\begin{array}{cc}
x & \frac{1}{a_{3}} \\
1 & 0
\end{array}\right) \\
& Q\left(a_{4} x^{2}+a_{3} x+a_{2}\right)
\end{aligned}
$$

## Improving efficiency Further for univariate polynomial

## Theorem

Consider a degree-d univariate polynomial in $x$, say
$p=a_{d} x^{d}+a_{d-1} x^{d-1}+\ldots \ldots+a_{2} x^{2}+a_{1} x+a_{0}$. Then, $Q(p)$ can be approximately computed using a sequence of at most $\mathcal{O}(d)$ matrices.

Idea: Use Horner's rule
Illustration: Consider a polynomial

$$
a_{4} x^{4}+a_{3} x^{3}+a_{2} x^{2}+a_{1} x+a_{0}=\left(a_{4} x^{2}+a_{3} x+a_{2}\right) x^{2}+a_{1} x+a_{0}
$$

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

$$
\begin{aligned}
& \quad \downarrow \text { append } Q(0)\left(\begin{array}{cc}
a_{3} & a_{2} \\
0 & 1
\end{array}\right)\left(\begin{array}{cc}
x & \frac{1}{a_{3}} \\
1 & 0
\end{array}\right) \\
& Q\left(a_{4} x^{2}+a_{3} x+a_{2}\right) \xrightarrow{\text { Lemma 2 }} Q\left(\left(a_{4} x^{2}+a_{3} x+a_{2}\right) x^{2}\right)
\end{aligned}
$$

## Improving efficiency Further for univariate polynomial

## Theorem

Consider a degree-d univariate polynomial in $x$, say
$p=a_{d} x^{d}+a_{d-1} x^{d-1}+\ldots . .+a_{2} x^{2}+a_{1} x+a_{0}$. Then, $Q(p)$ can be approximately computed using a sequence of at most $\mathcal{O}(d)$ matrices.

Idea: Use Horner's rule
Illustration: Consider a polynomial
$a_{4} x^{4}+a_{3} x^{3}+a_{2} x^{2}+a_{1} x+a_{0}=\left(a_{4} x^{2}+a_{3} x+a_{2}\right) x^{2}+a_{1} x+a_{0}$.
$Q\left(a_{4}\right) \xrightarrow{\text { Lemma } 2} Q\left(a_{4} x^{2}\right)$

$$
\begin{aligned}
& \quad \downarrow \text { append } Q(0)\left(\begin{array}{cc}
a_{3} & a_{2} \\
0 & 1
\end{array}\right)\left(\begin{array}{cc}
x & \frac{1}{a_{3}} \\
1 & 0
\end{array}\right) \\
& Q\left(a_{4} x^{2}+a_{3} x+a_{2}\right) \xrightarrow{\text { Lemma } 2} Q\left(\left(a_{4} x^{2}+a_{3} x+a_{2}\right) x^{2}\right) \\
& \quad \downarrow \text { append } Q(0)\left(\begin{array}{cc}
a_{1} & a_{0} \\
0 & 1
\end{array}\right)\left(\begin{array}{cc}
x & \frac{1}{a_{1}} \\
1 & 0
\end{array}\right) \\
& Q\left(\left(a_{4} x^{2}+a_{3} x+a_{2}\right) x^{2}+a_{1} x+a_{0}\right) .
\end{aligned}
$$

## Powering Efficiently

## Powering Efficiently

Seq. of $N$ matrices that $\stackrel{?}{\Rightarrow}$ Seq. of $\mathcal{O}(r N)$ matrices that approximately computes $Q(f) \Longrightarrow$ approximately computes $Q\left(f^{r}\right)$

## Powering Efficiently

Seq. of $N$ matrices that $\stackrel{?}{\Rightarrow}$ Seq. of $\mathcal{O}(r N)$ matrices that approximately computes $Q(f) \Rightarrow$ approximately computes $Q\left(f^{r}\right)$
$Q(1) \xrightarrow[2 N+4]{\text { Lemma 2 }} Q\left(f^{2}\right) \xrightarrow[2 N+4]{\text { Lemma 2 }} \cdots \xrightarrow[2 N+4]{\text { Lemma 2 }} Q\left(f^{r-2}\right) \xrightarrow[2 N+4]{\text { Lemma 2 }} Q\left(f^{r}\right)$

## Powering Efficiently

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

$$
\begin{aligned}
& Q(1) \xrightarrow[2 N+4]{\text { Lemma 2 }} Q\left(f^{2}\right) \xrightarrow[2 N+4]{\text { Lemma 2 }} \cdots \xrightarrow[2 N+4]{\text { Lemma 2 }} Q\left(f^{r-2}\right) \xrightarrow[2 N+4]{\text { Lemma 2 }} Q\left(f^{r}\right) \\
& Q(f) \xrightarrow[2 N+4]{\text { Lemma 2 }} Q\left(f^{3}\right) \xrightarrow[2 N+4]{\text { Lemma 2 }} \cdots \xrightarrow[2 N+4]{\text { Lemma 2 }} Q\left(f^{r-2}\right) \xrightarrow[2 N+4]{\text { Lemma 2 }} Q\left(f^{r}\right)
\end{aligned}
$$

Note that

* $Q(f), Q(g) \Longrightarrow Q(f+g)$ ?


## Easy!

Note that

* $Q(f), Q(g) \Longrightarrow Q(f+g)$ ?

Easy!

* $Q(f) \Longrightarrow Q\left(f^{n}\right)$ ?

Easy!

Note that

* $Q(f), Q(g) \Longrightarrow Q(f+g)$ ?

Easy!

* $Q(f) \Longrightarrow Q\left(f^{n}\right)$ ?

Easy!

* Why is powering interesting?

Can this compute non-sparse polynomials?

Note that

* $Q(f), Q(g) \Longrightarrow Q(f+g)$ ?

Easy!

* $Q(f) \Longrightarrow Q\left(f^{n}\right)$ ?

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 $\operatorname{char}(\mathbb{F})=2$.

# Conclusion and Open Problem 

## Conclusion and Open Problem

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


## Conclusion and Open Problem

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

Open Problems

## Conclusion and Open Problem

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


## Open Problems

H Is $Q\left(x_{1} x_{2} \cdots x_{n}\right)$ computable efficiently?

## Conclusion and Open Problem

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


## Open Problems

* Is $Q\left(x_{1} x_{2} \cdots x_{n}\right)$ computable efficiently?
* Can we compute $Q(f x)$ using a single $Q(f)$ ?


## Conclusion and Open Problem

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


## Open Problems

* Is $Q\left(x_{1} x_{2} \cdots x_{n}\right)$ computable efficiently?
* Can we compute $Q(f x)$ using a single $Q(f)$ ?

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

## Conclusion and Open Problem

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


## Open Problems

* Is $Q\left(x_{1} x_{2} \cdots x_{n}\right)$ computable efficiently?
* Can we compute $Q(f x)$ using a single $Q(f)$ ?

Can we compute $Q(f g)$ using constant many $Q(f)$ 's and $Q(g)$ 's?
Can we show some lower bound for $Q(f \cdot g)$ ?

## Conclusion and Open Problem

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


## Open Problems

* Is $Q\left(x_{1} x_{2} \cdots x_{n}\right)$ computable efficiently?
* Can we compute $Q(f x)$ using a single $Q(f)$ ?

Can we compute $Q(f g)$ 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?


## Conclusion and Open Problem

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


## Open Problems

* Is $Q\left(x_{1} x_{2} \cdots x_{n}\right)$ computable efficiently?
* Can we compute $Q(f x)$ using a single $Q(f)$ ?

Can we compute $Q(f g)$ 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 $\mathrm{VF} \subset \overline{\mathrm{VBP}_{2}}$ when $\operatorname{char}(\mathbb{F})=2$ ?


## Conclusion and Open Problem

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


## Open Problems

* Is $Q\left(x_{1} x_{2} \cdots x_{n}\right)$ computable efficiently?
* Can we compute $Q(f x)$ using a single $Q(f)$ ?

Can we compute $Q(f g)$ 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 $\mathrm{VF} \subset \overline{\mathrm{VBP}_{2}}$ when $\operatorname{char}(\mathbb{F})=2$ ?


[^0]:    ${ }^{1}$ when $\operatorname{char}(F) \neq 2$.

[^1]:    ${ }^{1}$ when $\operatorname{char}(F) \neq 2$.

[^2]:    ${ }^{1}$ when $\operatorname{char}(F) \neq 2$.

