LOWER BOUNDS FOR ALGEBRAIC CIRCUITS

SRIKANTH SRINIVASAN
(DEPT. OF MATH., IIT BOMBAY)

Polynomials

$$P(x_1,\dots,x_n) \in \mathbb{F}[x_1,\dots,x_n]$$

$$P(\bar{x}) = \sum_{\bar{e}=(e_1,\dots,e_n)} \alpha_{\bar{e}}\, x^{\bar{e}}$$

Polynomials

$P(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$

$$P(\bar{x}) = \sum_{\bar{e} = (e_1, \ldots, e_n)} \alpha_{\bar{e}} \, x^{\bar{e}}$$

Capture many interesting computational problems.

Eg: Determinant, Permanent, Matrix mult.

Polynomials

$P(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$

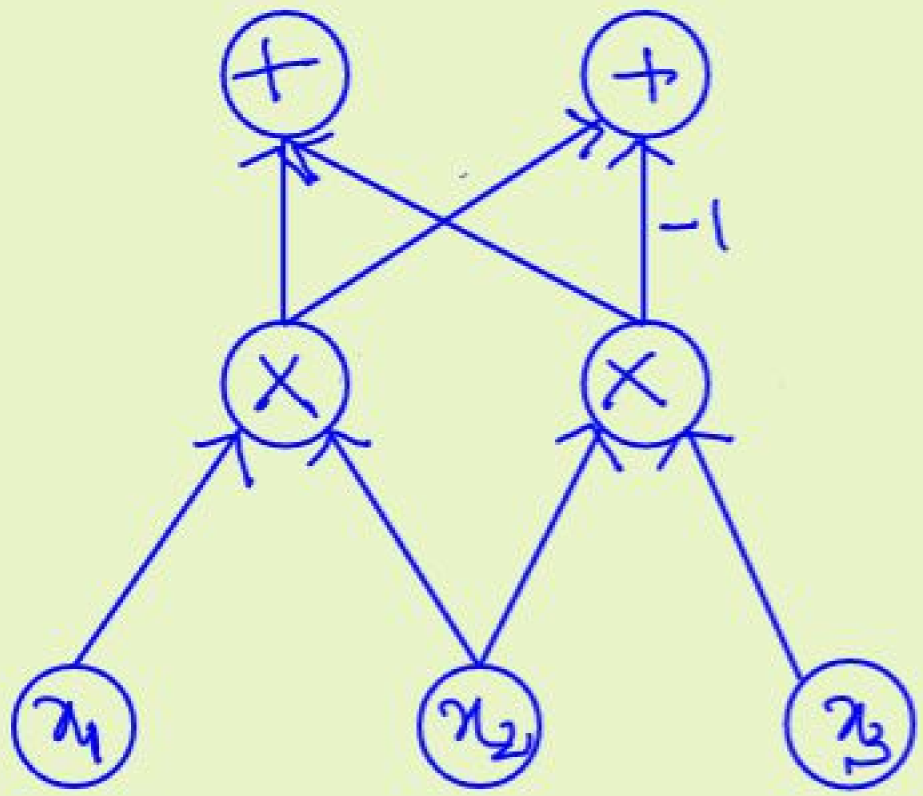
$$P(\bar{x}) = \sum_{\bar{e} = (e_1, \ldots, e_n)} \alpha_{\bar{e}} \, x^{\bar{e}}$$

Capture many interesting computational problems.

Eg: Deteminant, Permanent, Matrix mult.

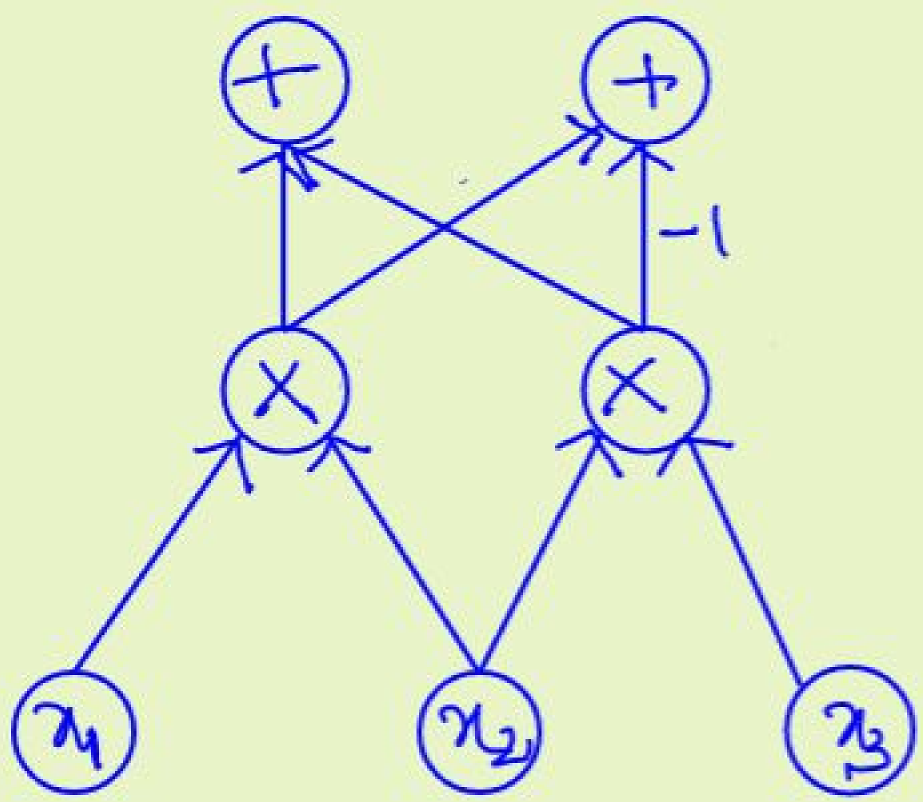
Typically, $\deg(P) = d \leq n^{O(1)}$

Algebraic circuits



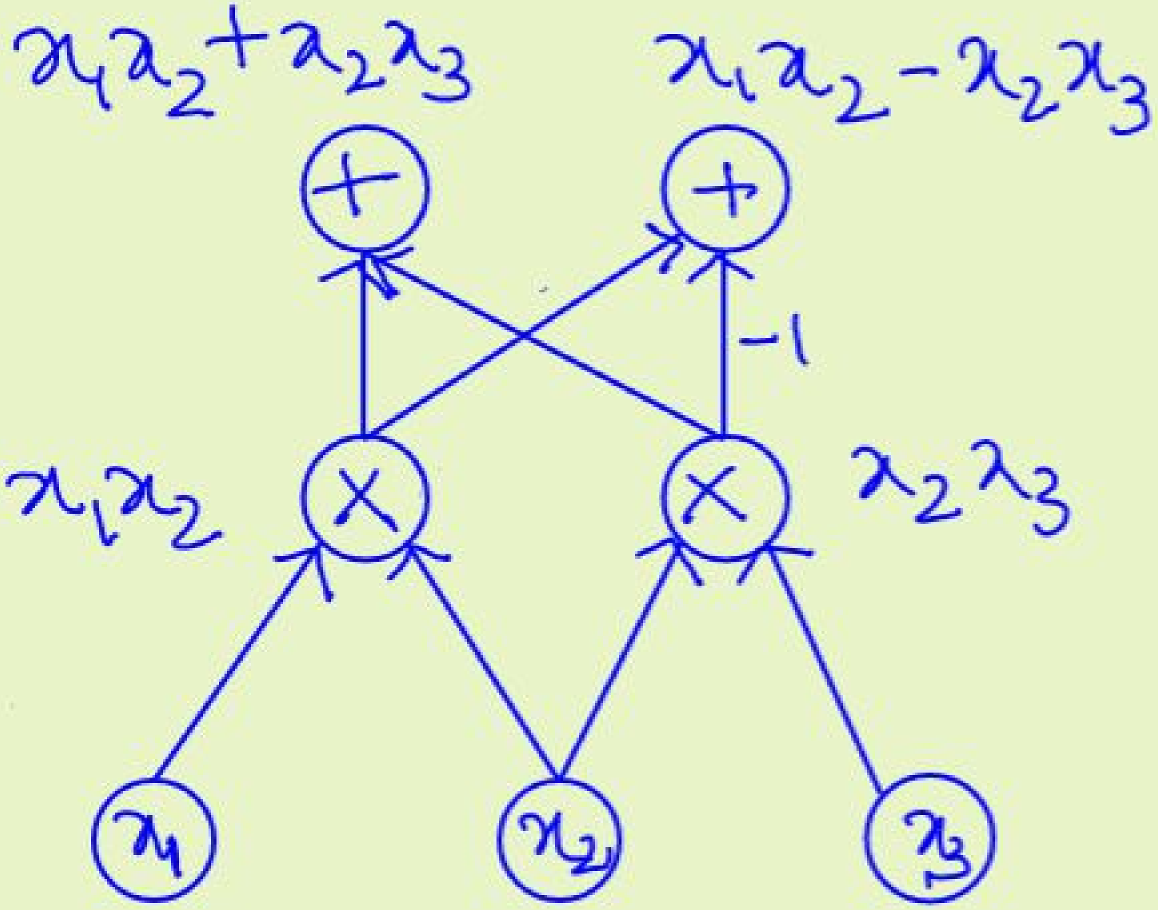
→ labelled DAG

Algebraic circuits



- → labelled DAG
- → Leaves ⟺ variables, constants
- → ×-gates for product
- → +-gates for sums (linear combinations)

Algebraic circuits



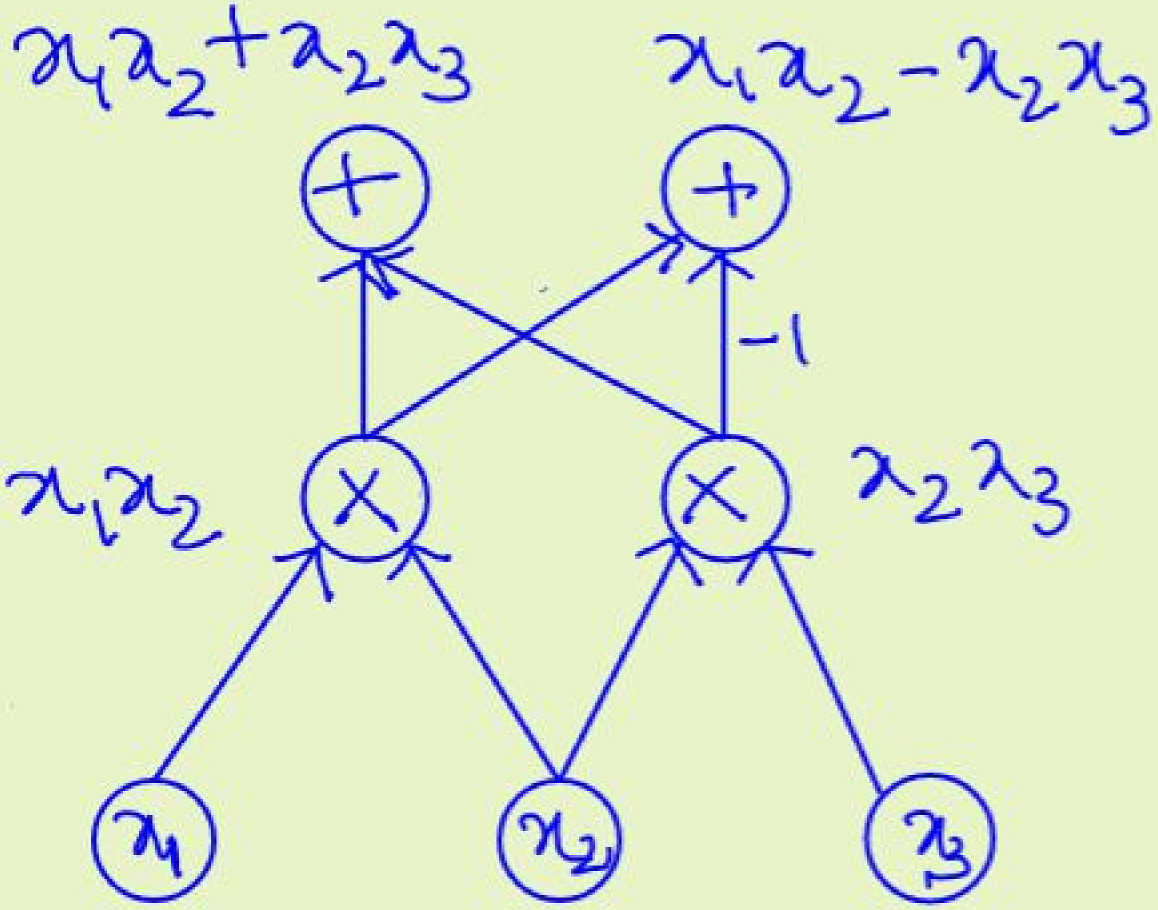
→ labelled DAG

→ Leaves ⟺ variables, constants

→ $\times$-gates for product

→ $+$-gates for sums (linear combinations)

Algebraic circuits



→ labelled DAG

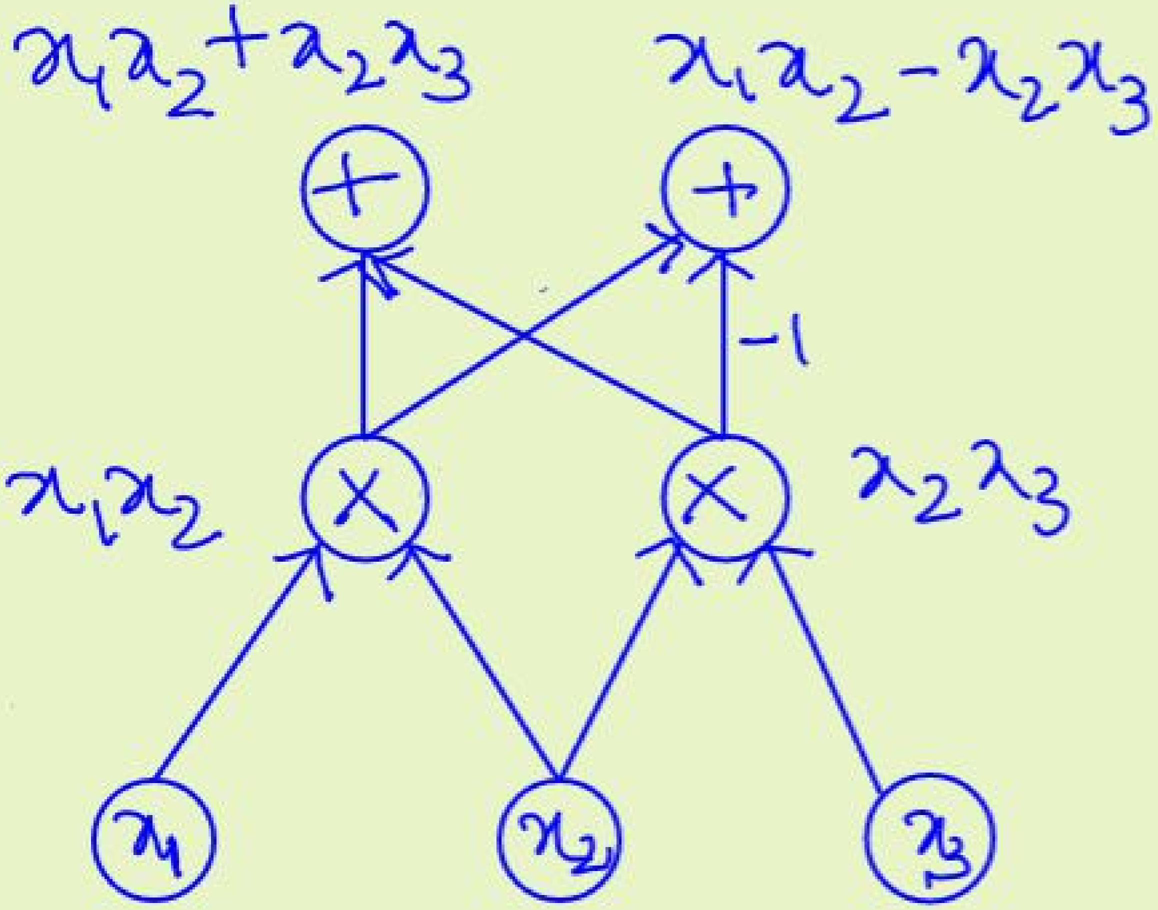
→ Leaves ⟺ variables, constants

→ $\times$-gates for product

→ $+$-gates for sums (linear combinations)

→ One or more output gates.

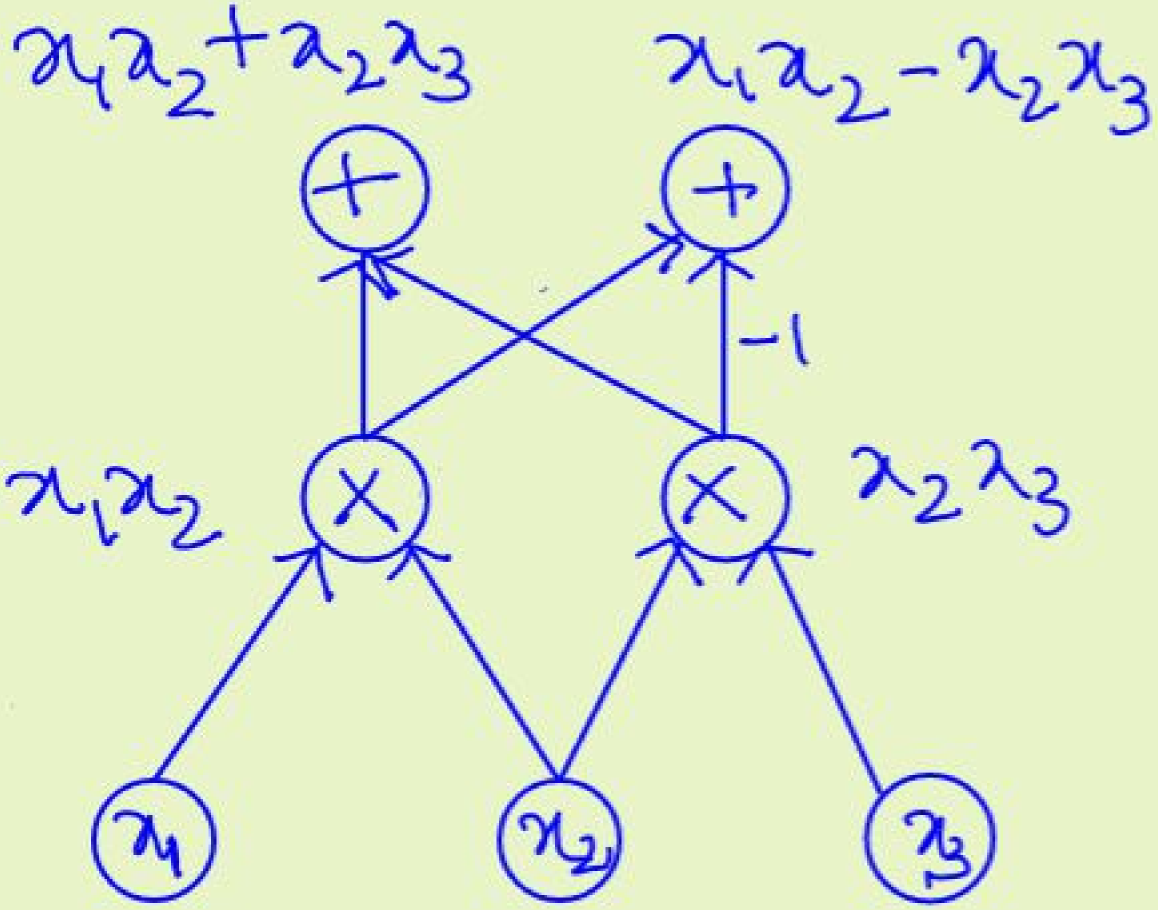
Algebraic circuits



Size $= 8$

Size $=$ # of edges/wires

Algebraic circuits



Size = 8

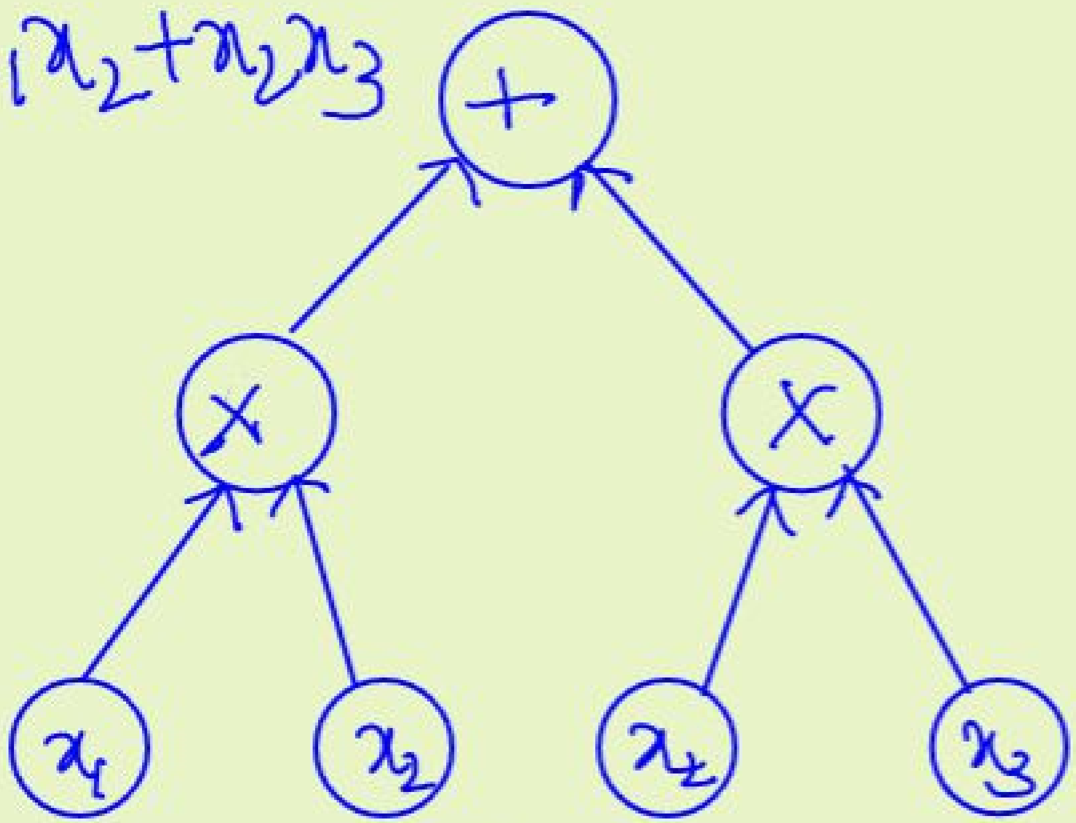
Depth = 2

Size = # of edges/wires

Depth = length of longest input-output path.

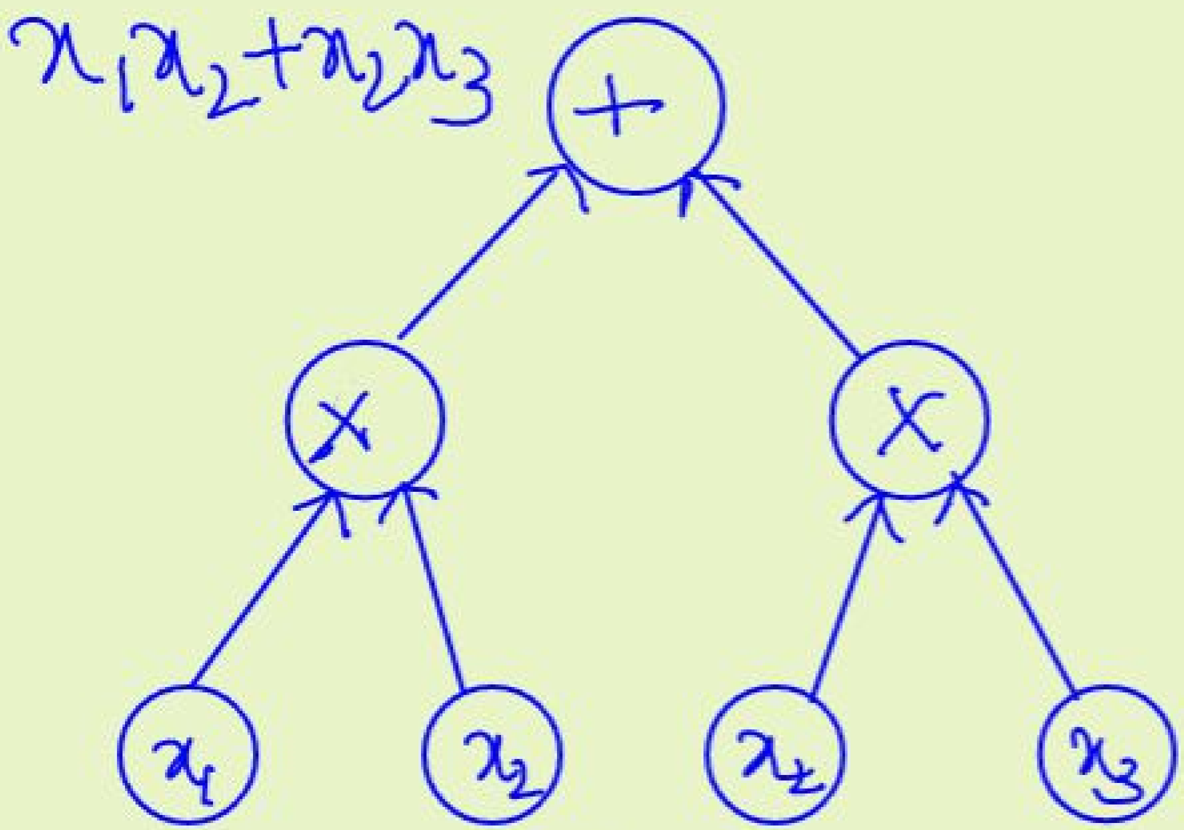
Algebraic formulas

$x_1x_2+x_2x_3$



→ Underlying graph is a tree

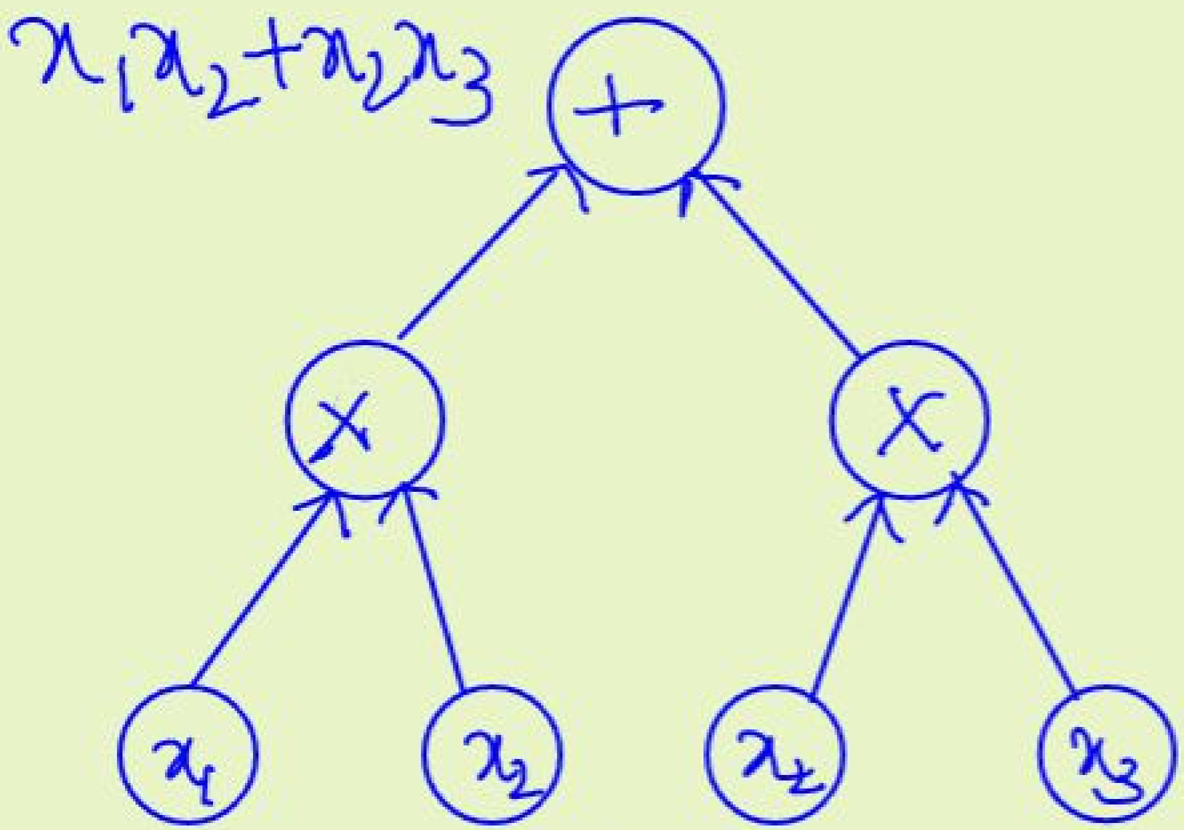
Algebraic formulas



→ Underlying graph is a tree

→ Formulas ⟷ algebraic expressions

Algebraic formulas



→ Underlying graph is a tree

→ Formulas <→ algebraic expressions

→ Size of formula ≈ Size of expression

Special kinds of small-depth formulas

Special kinds of small-depth formulas

→ $\Sigma\Pi$ formulas : Sum of monomials

Special kinds of small-depth formulas

→ $\Sigma\Pi$ formulas : Sum of monomials

→ $\Sigma\Pi\Sigma$ formulas: Sums of products of linear fns

Special kinds of small-depth formulas

→ $\Sigma\Pi$ formulas: Sum of monomials

→ $\Sigma\Pi\Sigma$ formulas: Sums of products of linear fns

→ $\Sigma\Pi\Sigma\Pi$ formulas, ...

Special kinds of small-depth formulas

→ $\Sigma\Pi$ formulas: Sum of monomials

→ $\Sigma\Pi\Sigma$ formulas: Sums of products of linear fns

→ $\Sigma\Pi\Sigma\Pi$ formulas, ...

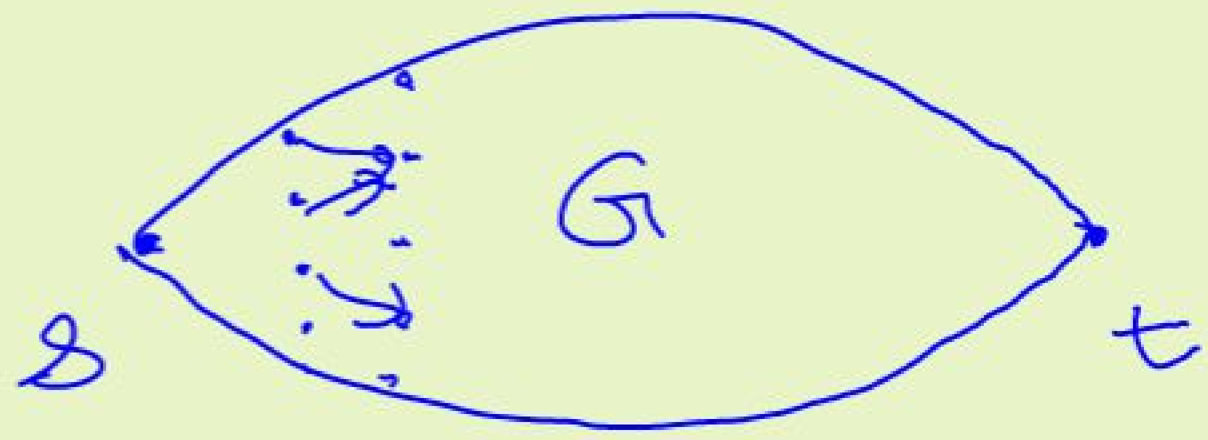
Any $p \in \mathbb{F}[x_1, \ldots, x_n]$ of deg d has a $\Sigma\Pi$ formula of size $\binom{n+d}{d}$ – "trivial" representation

Algebraic Branching Programs (ABPs)

→ Layered DAG

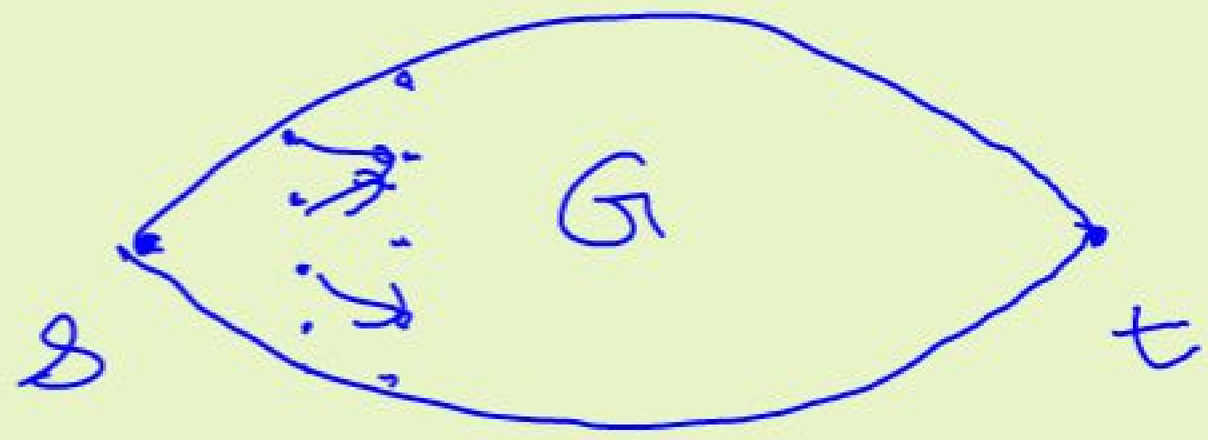
source s &

sink t



Algebraic Branching Programs (ABPs)

→ Layered DAG source s & sink t



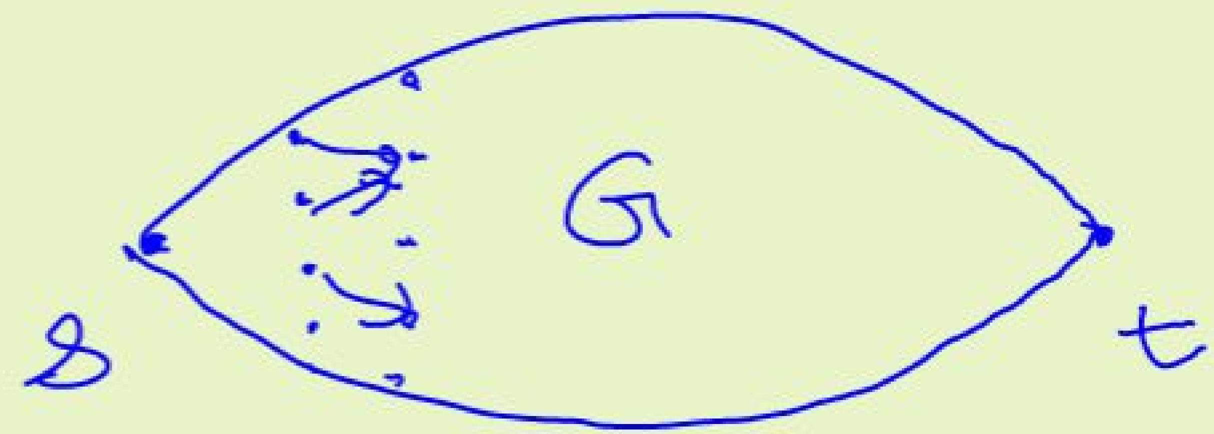
→ Edges labelled by linear polys

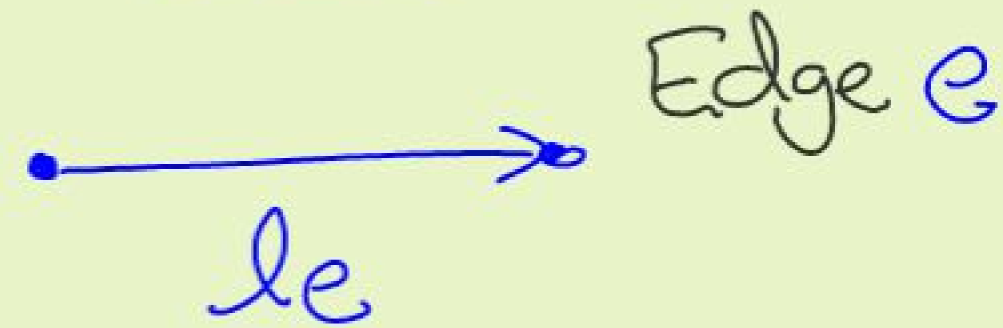
Edge e

Algebraic Branching Programs (ABPs)

→ Layered DAG
source s & sink t

→ Edges labelled by linear polys





$$P_G = \sum_{\substack{\rho : s \to t \\ \text{path}}} \prod_{e \text{ on } \rho} l_e$$

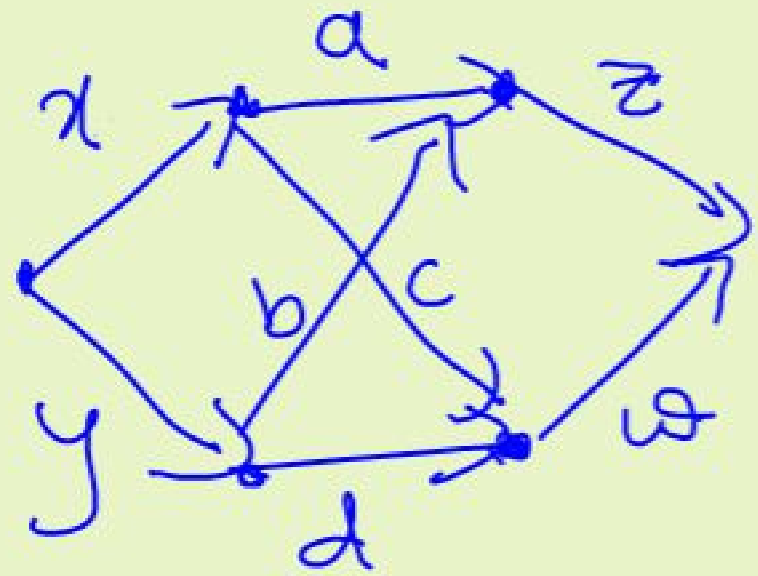
Examples of ABPs

$$G_1 = \bullet \xrightarrow{x_1} \bullet \xrightarrow{x_2} \bullet \xrightarrow{x_1+x_2+1} \bullet . \qquad P_{G_1} = x_1 x_2 (x_1 + x_2 + 1).$$

Examples of ABPs

$G_1 = \bullet \xrightarrow{x_1} \bullet \xrightarrow{x_2} \bullet \xrightarrow{x_1+x_2+1} \bullet.$ $\quad P_{G_1} = x_1 x_2 (x_1 + x_2 + 1).$

$G_2 =$

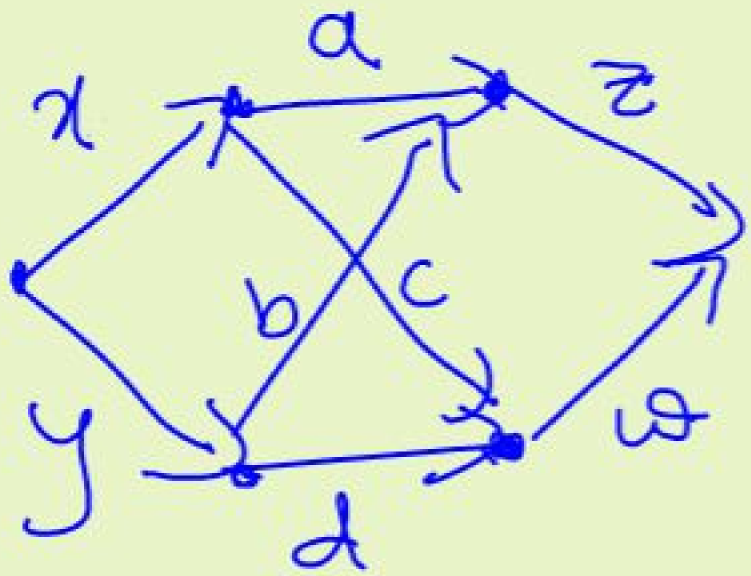


Examples of ABPs

$G_1 = \bullet \xrightarrow{x_1} \bullet \xrightarrow{x_2} \bullet \xrightarrow{x_1+x_2+1} \bullet .$

$P_{G_1} = x_1 x_2 (x_1 + x_2 + 1)$

$G_2 =$

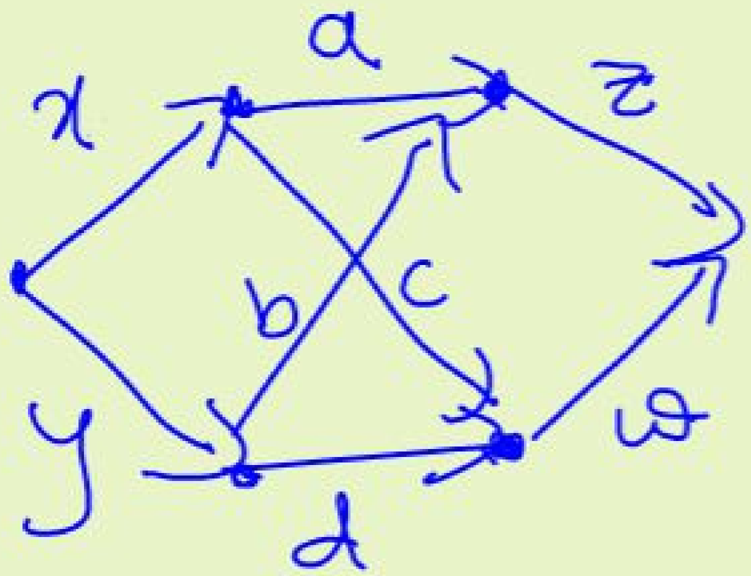


$P_{G_2} = xaz + xcw + ybz + ydw$

Examples of ABPs

$G_1 = \bullet \xrightarrow{x_1} \bullet \xrightarrow{x_2} \bullet \xrightarrow{x_1+x_2+1} \bullet$

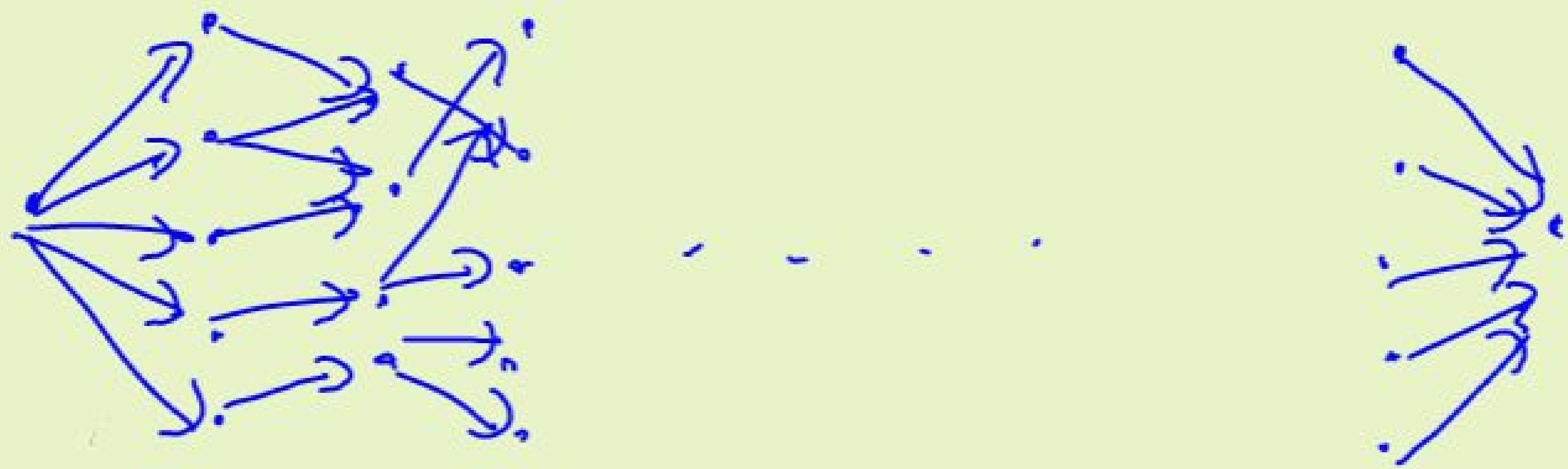
$P_{G_1} = x_1 x_2 (x_1 + x_2 + 1)$

$G_2 =$ 

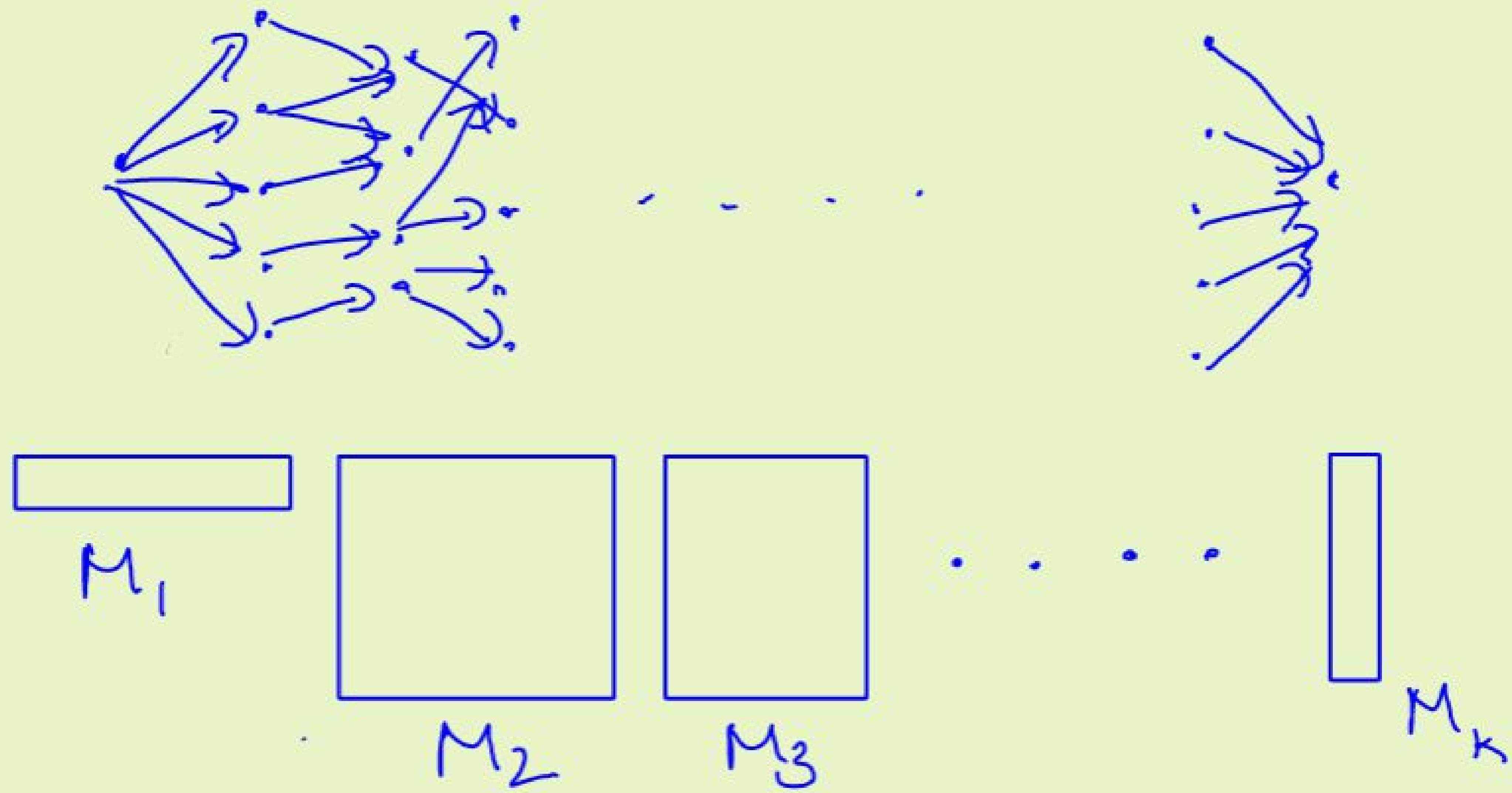
$P_{G_2} = xaz + xcw + ybz + ydw$

$$P_{G_2} = (x, y)\begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} z \\ w \end{pmatrix}$$

ABPs & Iterated Matrix Multiplication



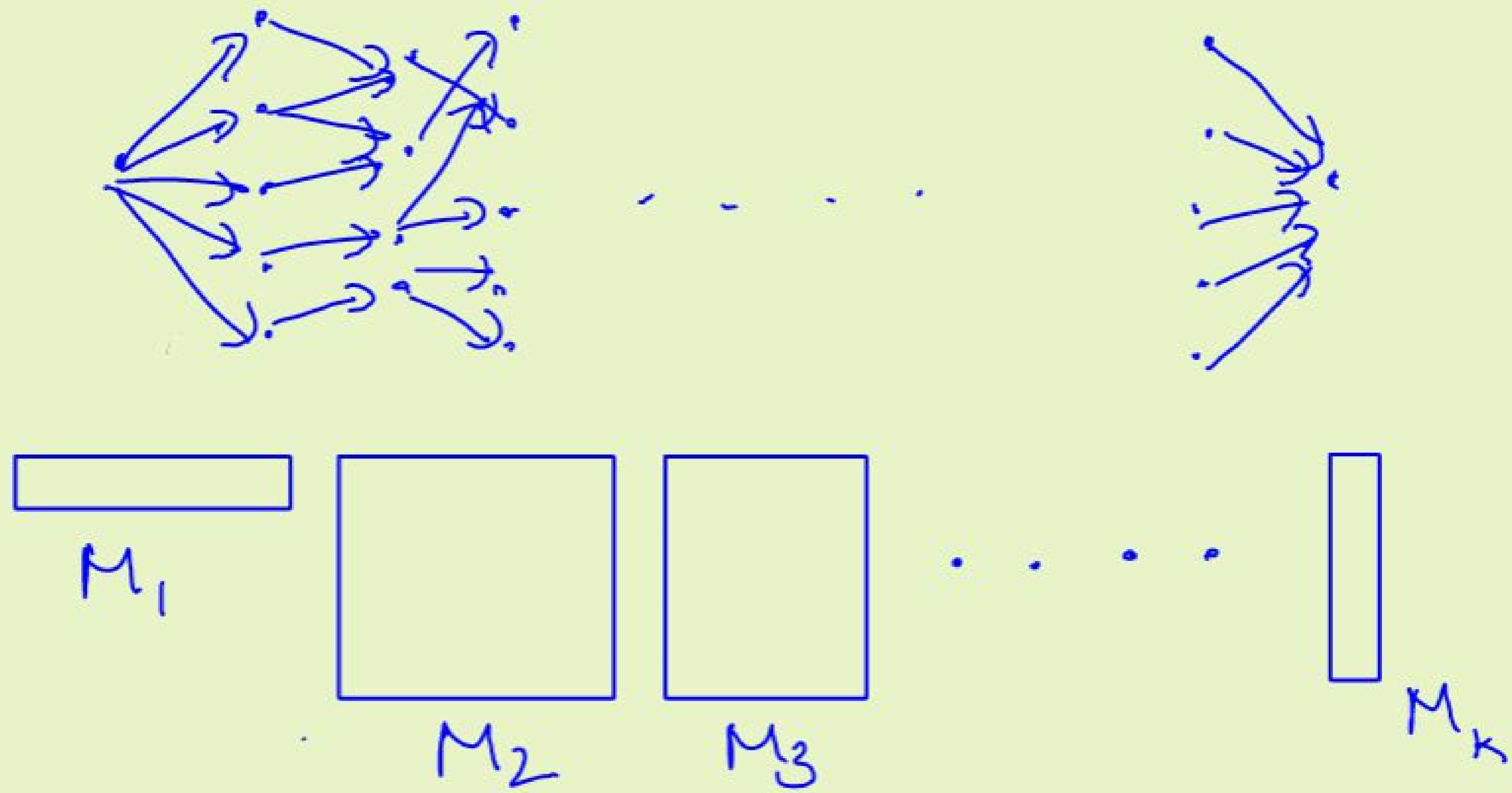
ABPs & Iterated Matrix Multiplication



ABPs & Iterated Matrix Multiplication

$$M_2(u,v) = \begin{cases} \ell_{(u,v)} & \text{if } (u,v) \in E \\ 0 & \text{o/w} \end{cases}$$

ABPs & Iterated Matrix Multiplication



Size of ABP = # vertices $\approx$ sum of matrix dimensions

Complexity classes

$(p_n(x_1, \ldots, x_n))_{n\geq 1}$ - a family of polys.

Complexity classes

$(p_n(x_1, \dots, x_n))_{n \geq 1}$ - a family of polys.

VF - polynomial families that have poly-sized formulas

Complexity classes

$(p_n(x_1, \ldots, x_n))_{n \geq 1}$ - a family of polys.

VF - polynomial families that have poly-sized formulas

VBP - poly-sized ABPs

VP - poly-sized circuits

Complexity classes

$(p_n(x_1, \ldots, x_n))_{n \geq 1}$ - a family of polys.

VF - polynomial families that have poly-sized formulas

VBP - poly-sized ABPs

VP - poly-sized circuits

$$VF \subseteq VBP \subseteq VP$$

Lower bounds question

Are there polynomials that do <u>not</u> have small formulas/ABPs/ckts?

Lower bounds question

Are there polynomials that do <u>not</u> have small formulas/ABPs/ckts?

YES. By "counting" arguments

Lower bounds question

Are there polynomials that do <u>not</u> have small formulas/ABPs/ckts?

YES. By "counting" arguments

Thm [H.Y]: For any n, d, $\exists p_n \in \mathbb{F}[x_1, \ldots, x_n]$

→ $\deg(p_n) \leq d$, → $\mathrm{Coeffs}(p) \in \{0,1\}$

Lower bounds question

Are there polynomials that do <u>not</u> have small formulas/ABPs/ckts?

YES. By "counting" arguments

Thm [H.Y]: For any n, d, $\exists p_n \in \mathbb{F}[x_1, \ldots, x_n]$

→ $\deg(p_n) \leq d$, → Coeffs$(p) \in \{0,1\}$

→ Any ckt. for p_n is "large."

[essentially trivial]

Lower bounds question

Are there explicit polynomials that do not have small formulas/ABPs/ckts?

Lower bounds question

Are there explicit polynomials that do <u>not</u> have small formulas/ABPs/ckts?

Explicit – VNP

Lower bounds question

Are there explicit polynomials that do <u>not</u> have small formulas/ABPs/ckts?

Explicit – VNP

Special case – $(p_n(x_1,\dots,x_n))_{n\geq 1}$ explicit if

$$\begin{array}{c} n \\ e_1,\dots,e_n \geq 0 \\ \sum_j e_j \leq d \end{array} \longrightarrow \boxed{\begin{array}{c}\text{Poly-time} \\ \text{algo}\end{array}}$$

Lower bounds question

Are there explicit polynomials that do not have small formulas/ABPs/ckts?

Explicit - VNP

Special case - $(p_n(x_1,\dots,x_n))_{n\geq 1}$ explicit if

$$\begin{array}{c} n \\ e_1,\dots,e_n \geq 0 \\ \sum_j e_j \leq d \end{array} \longrightarrow \boxed{\begin{array}{c}\text{Poly-time}\\ \text{algo}\end{array}} \longrightarrow \text{Coeff}(\bar{x}^{\bar{e}}) \text{ in } p_n$$

State-of-the-art

State-of-the-art

[B-S 83]: Explicit polys $p(x_1, \ldots, x_n)$ requiring circuit size $\Omega(n \log d)$.

State-of-the-art

[B-S 83]: Explicit polys $p(x_1, \ldots, x_n)$ requiring circuit size $\Omega(n \log d)$.

[Kalorkoti'85]: Formula lbds of $\Omega(n^2)$

State-of-the-art

[B-S 83]: Explicit polys $p(x_1, \ldots, x_n)$ requiring circuit size $\Omega(n \log d)$.

[Kalorkoti'85]: Formula lbds of $\Omega(n^2)$

More known for restricted models

Homogeneous, Monotone, Multilinear, Non-commutative, $\Sigma\Pi\Sigma$, $\Sigma\wedge\Sigma$, ...

Two-step approach to lower bounds

STEP 1:

STEP 2:

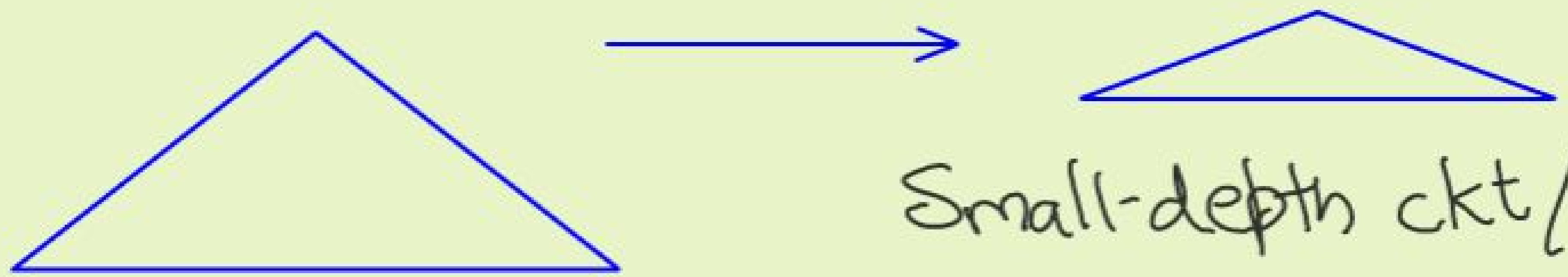
Two-step approach to lower bounds

STEP 1: Depth reduction

STEP 2:

Two-step approach to lower bounds

STEP 1: Depth reduction



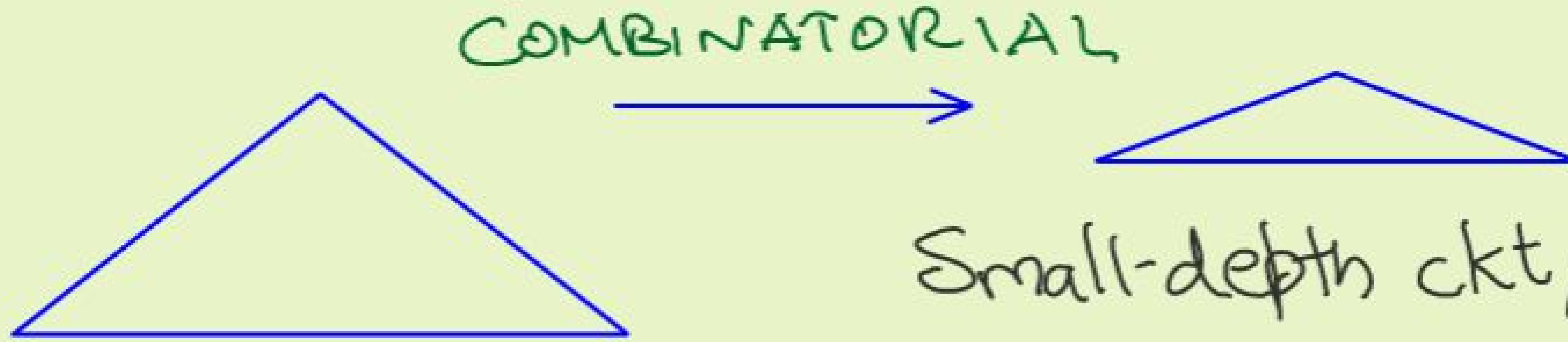
Small-depth ckt/formula

Ckt/formula/ABP

STEP 2:

Two-step approach to lower bounds

STEP 1: Depth reduction



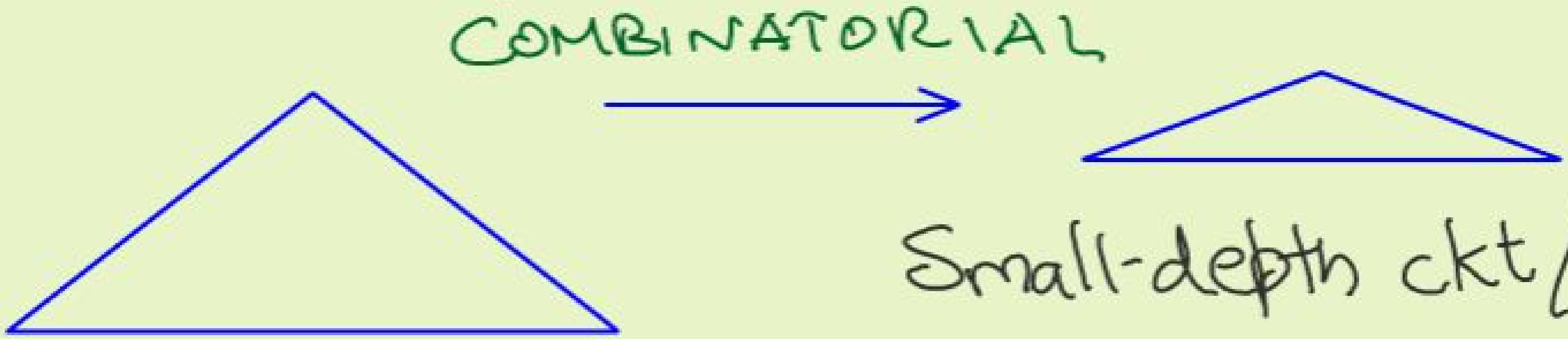
Small-depth ckt/formula

Ckt/formula/ABP

STEP 2:

Two-step approach to lower bounds

STEP 1: Depth reduction



Small-depth ckt/formula

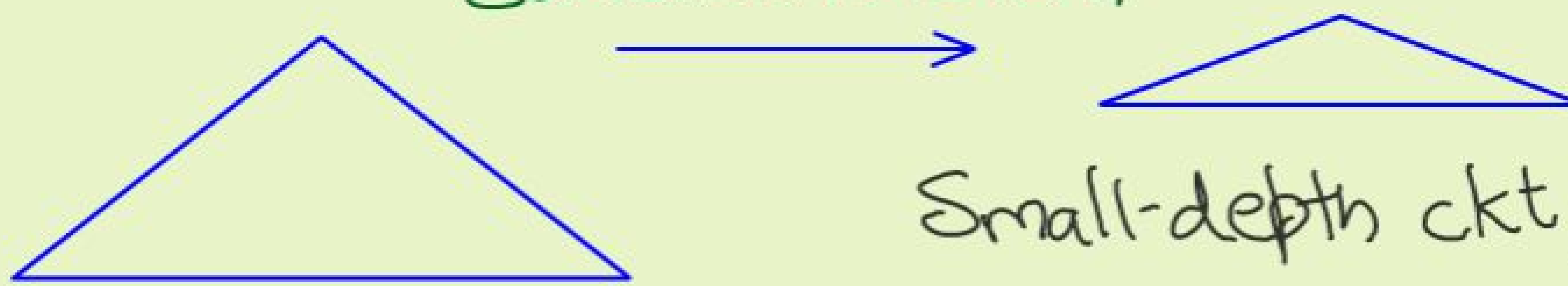
Ckt/formula/ABP

STEP 2: Lower bounds for small-depth

Two-step approach to lower bounds

STEP 1 : Depth reduction

COMBINATORIAL



Small-depth ckt/formula

Ckt/formula/ABP

STEP 2 : Lower bounds for small-depth

ALGEBRAIC

Depth reduction

Depth reduction

Thm :

template

Depth reduction

Thm : Any small circuit/ABP/ formula

<u>template</u>

can be written as a small-depth

ckt/formula

Depth reduction

Thm : Any $\underbrace{\text{small}}_{\text{poly}(n)}$ circuit/ABP/ formula

template

can be written as a $\underbrace{\text{small}}_{O(\log n)}$ -depth

ckt/formula

Depth reduction

Thm: Any $\underbrace{\text{small}}_{\text{poly}(n)}$ circuit/ABP/formula

template

can be written as a $\underbrace{\text{small}}_{O(\log n)}$-depth

ckt/formula that is $\left\{ \begin{array}{l} \text{moderately small} \\ \text{and/or} \\ \text{nice in some} \\ \text{structural way.} \end{array} \right.$

Depth reduction thms

Depth reduction thms

Thm [B'74]: Any size s formula F can be converted to an equivalent formula F' thas has size $s^{O(1)}$ and depth $O(\log s)$.

Depth reduction thms

Thm [B'74]: Any size s formula F can be converted to an equivalent formula F' thas has size $s^{O(1)}$ and depth $O(\log s)$.

Thm [VSBR'83]:

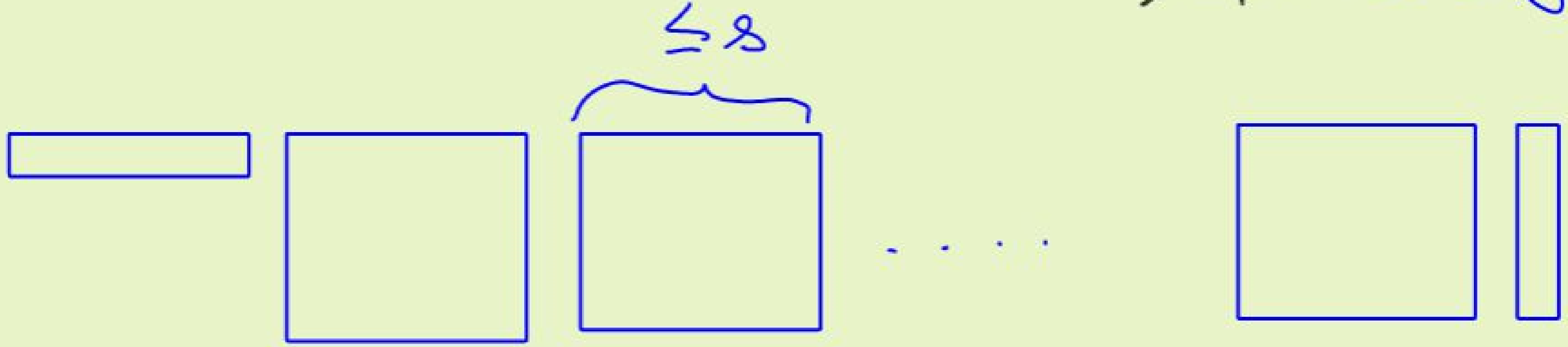
$$\begin{array}{ccc} \text{Size } s,\ \deg d & \longmapsto & \text{Size poly}(s,d) \\ \text{ckt. } C & & \text{ckt. } C' \\ & & \text{Depth } O(\log d) \end{array}$$

Depth reduction for ABPs

Thm : Size s, deg d ABP A $\longmapsto$ Size $\text{poly}(s,d)$ ckt. C' Depth $O(\log d)$

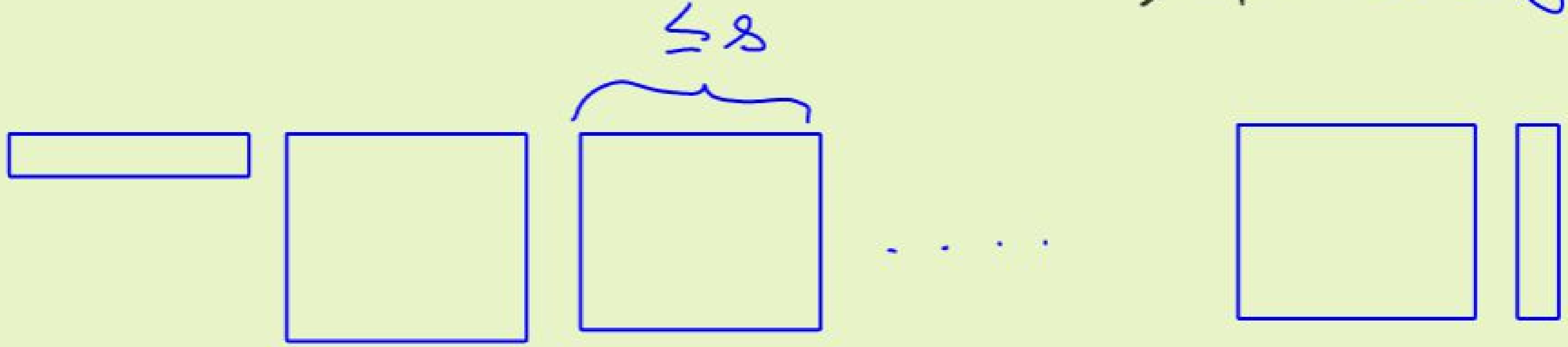
Depth reduction for ABPs

Thm : Size s, deg d ABP A $\longmapsto$ Size poly(s,d) ckt. C' Depth $O(\log d)$



Depth reduction for ABPs

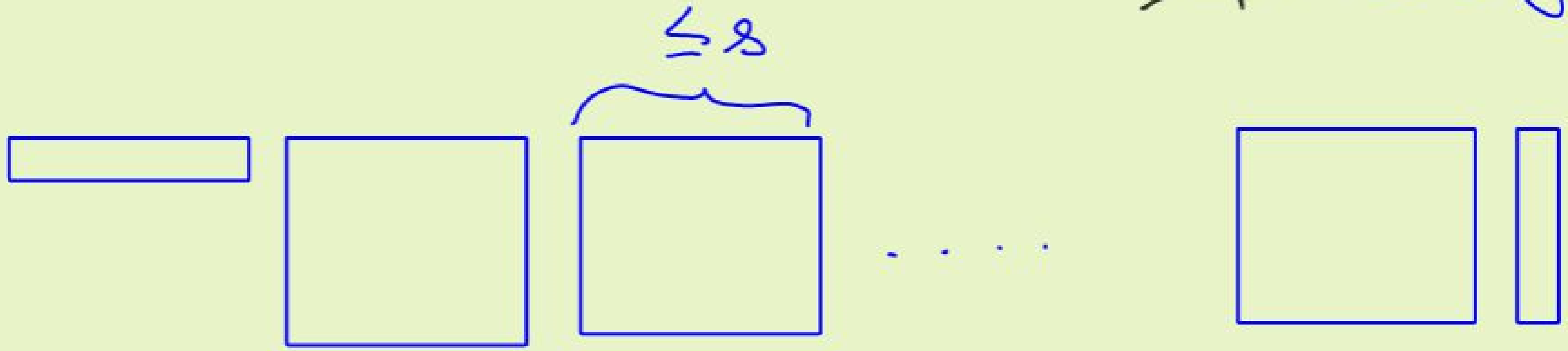
Thm: Size s, deg d ABP A $\longmapsto$ Size $\mathrm{poly}(s,d)$ ckt. C' Depth $O(\log d)$



Homogenization

Depth reduction for ABPs

Thm: Size s, deg d ABP A $\longmapsto$ Size $\mathrm{poly}(s,d)$ ckt. C' Depth $O(\log d)$

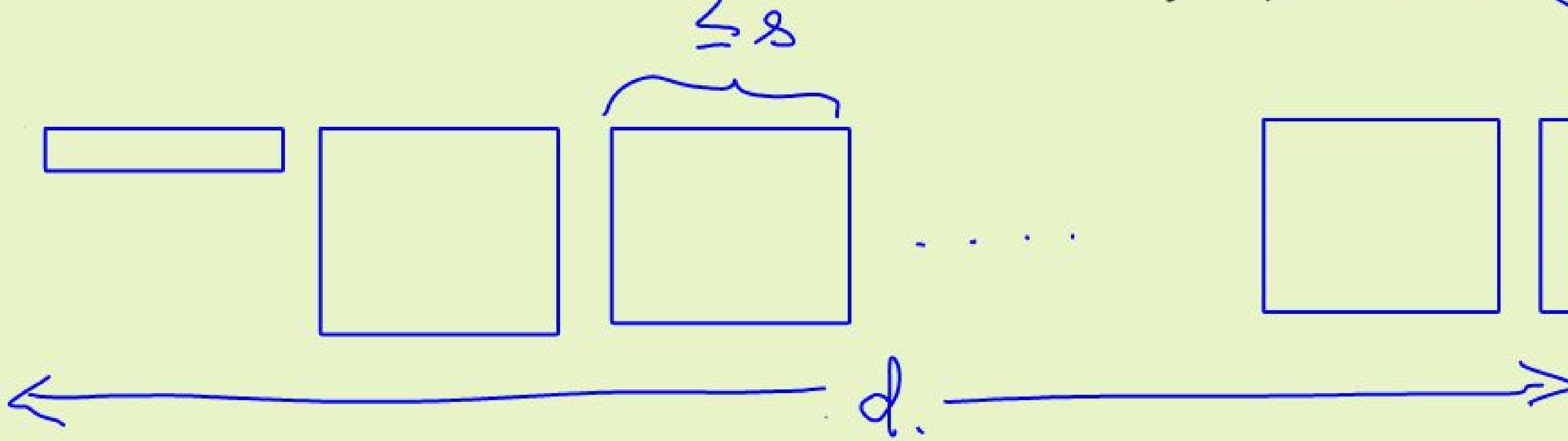


Homogenization: Reduce to d matrices

$$s \longmapsto s \cdot d$$

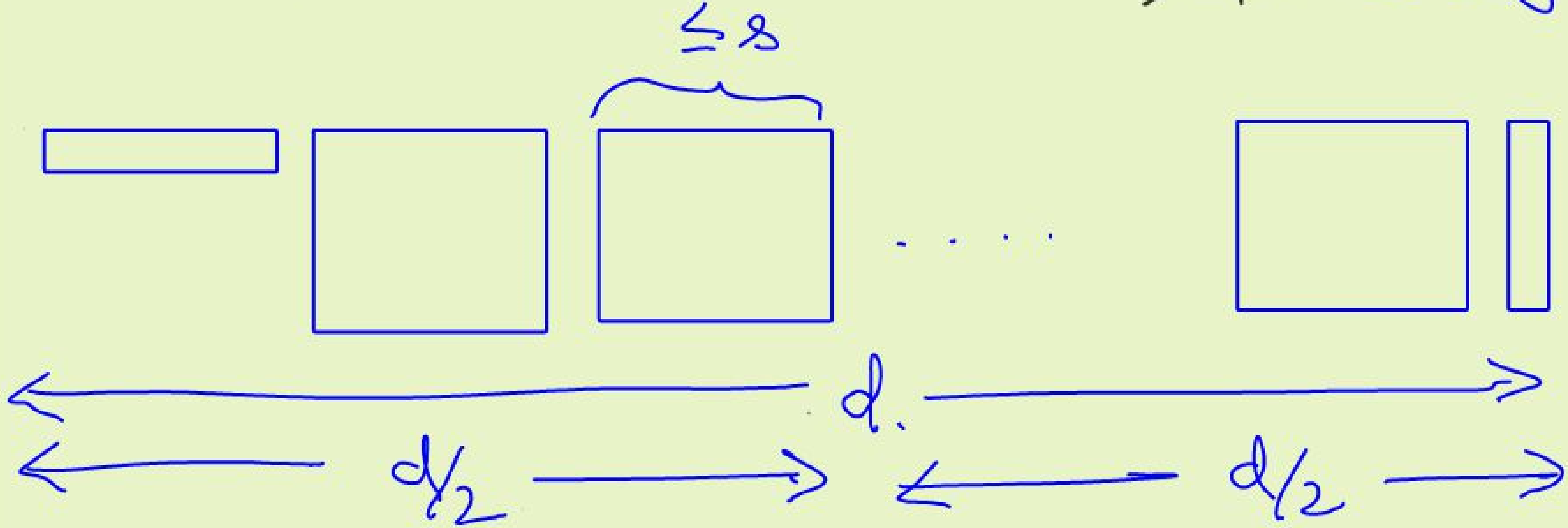
Depth reduction for ABPs

<u>Thm</u> : Size s, deg d ABP A $\longmapsto$ Size poly(s,d) ckt. C' Depth $O(\log d)$



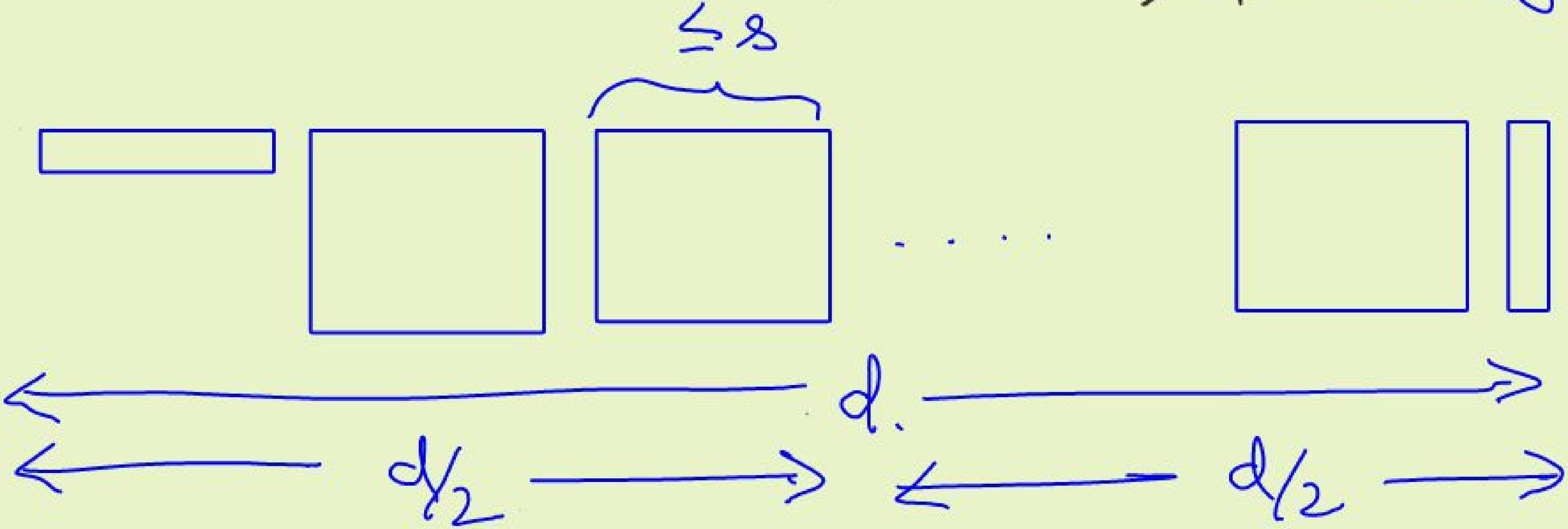
Depth reduction for ABPs

Thm : Size s, deg d ABP A $\longmapsto$ Size $\mathrm{poly}(s,d)$ ckt. C' Depth $O(\log d)$



Depth reduction for ABPs

Thm: Size s, deg d ABP A $\longmapsto$ Size poly(s,d) ckt. C' Depth $O(\log d)$



$\boxed{P_1\ P_2\ \cdots\ P_s}$ $\boxed{Q_1\ Q_2\ \cdots\ Q_s}^T$

Depth reduction for ABPs

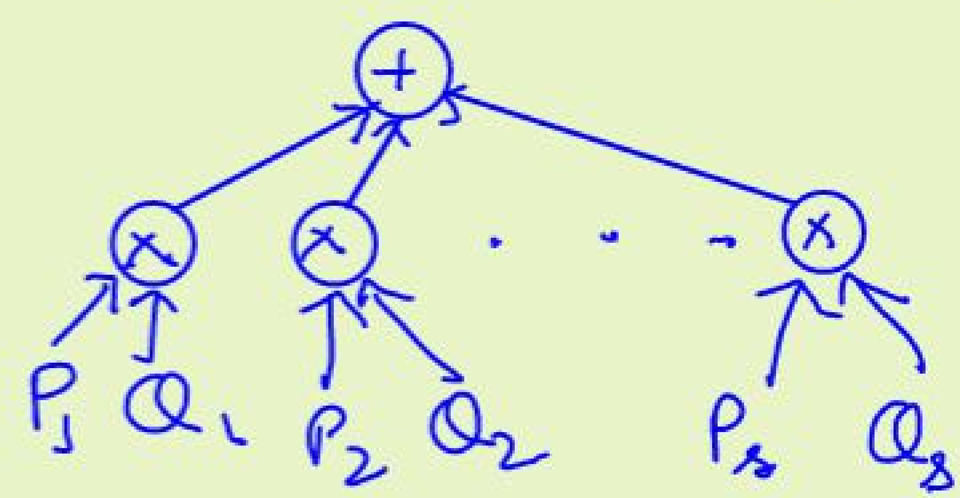
Thm: Size s, deg d ABP A $\longmapsto$ Size poly(s,d) ckt. C' Depth $O(\log d)$

$$A = \sum_{i=1}^{s} \underbrace{P_i}_{\deg d/2} \cdot \underbrace{Q_i}_{\deg d/2}$$

Depth reduction for ABPs

Thm: Size s, deg d ABP A $\longmapsto$ Size poly(s,d) ckt. C', Depth $O(\log d)$

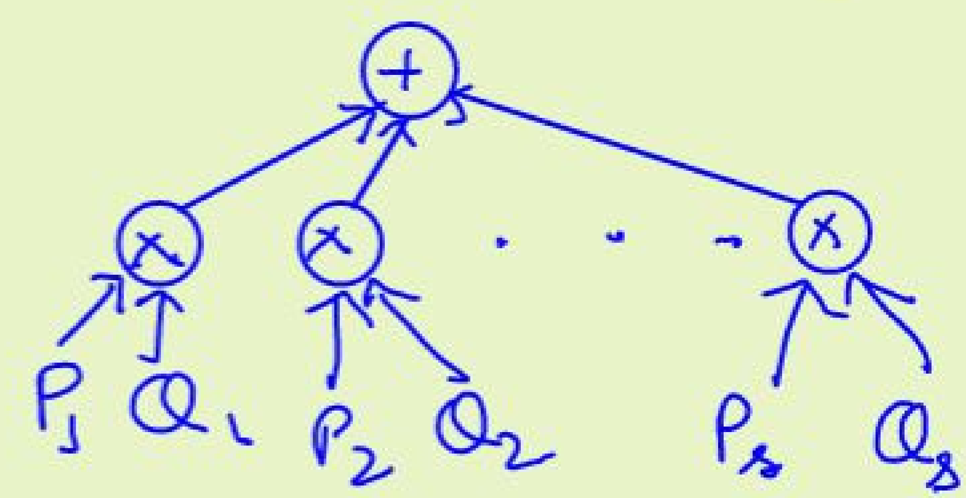
$$A = \sum_{i=1}^{s} \underbrace{P_i}_{\deg d/2} \cdot \underbrace{Q_i}_{\deg d/2}$$



Depth reduction for ABPs

Thm : Size s, deg d ABP A $\longmapsto$ Size poly(s,d) ckt. C' Depth $O(\log d)$

$$A = \sum_{i=1}^{s} \underbrace{P_i}_{\deg d/2} \cdot \underbrace{Q_i}_{\deg d/2}$$



Repeat for $P_1, \ldots, P_s, Q_1, \ldots, Q_s$ to get C'.

Reducing to depth 4

Reducing to depth 4

ABP A

size s, deg. d

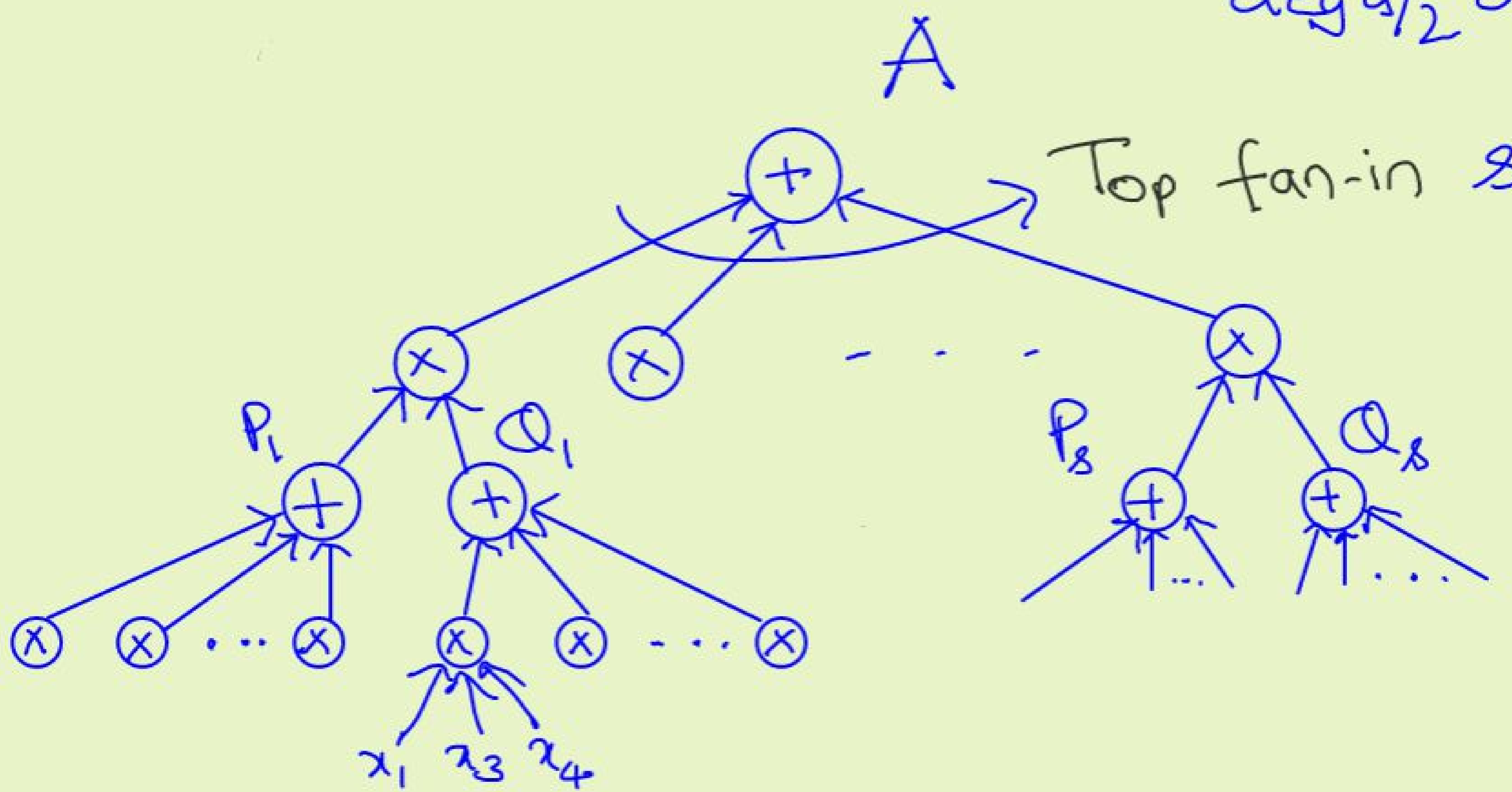
$$A = \sum_{i=1}^{s} \underbrace{P_i}_{\deg d/2} \underbrace{Q_i}_{\deg \frac{d}{2}}$$

Reducing to depth 4

ABP A

size s, deg. d

$$A = \sum_{i=1}^{s} \underbrace{P_i}_{\deg d/2} \underbrace{Q_i}_{\deg \frac{d}{2}}$$

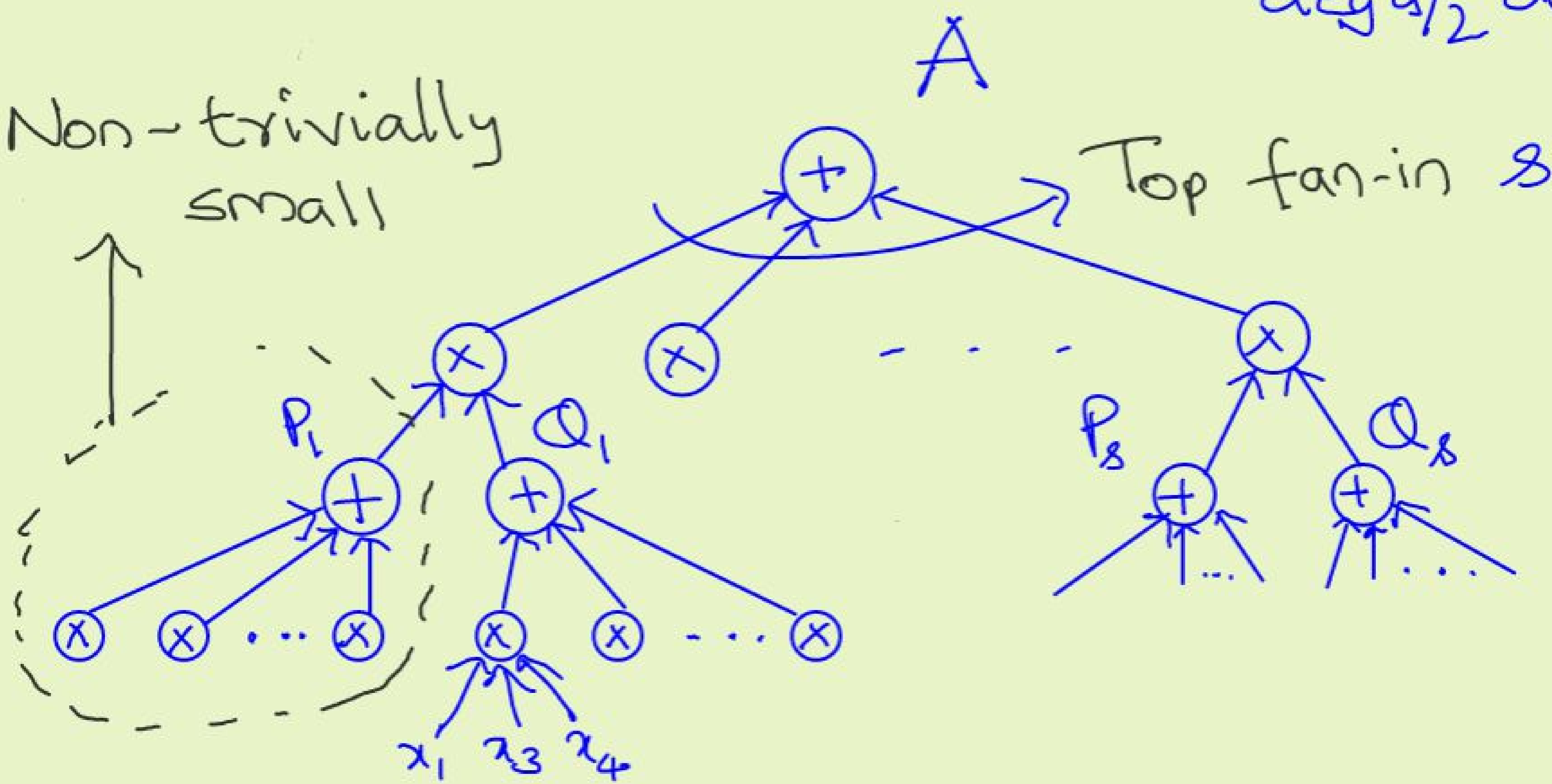


Reducing to depth 4

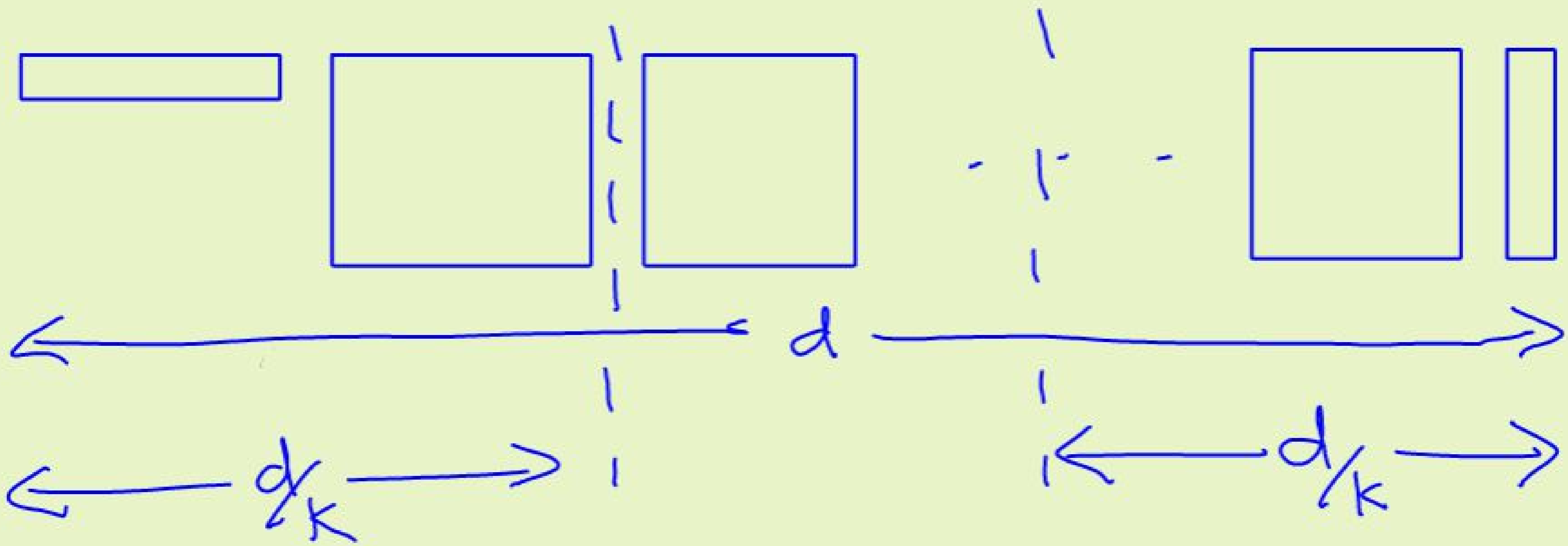
ABP A

size s, deg. d

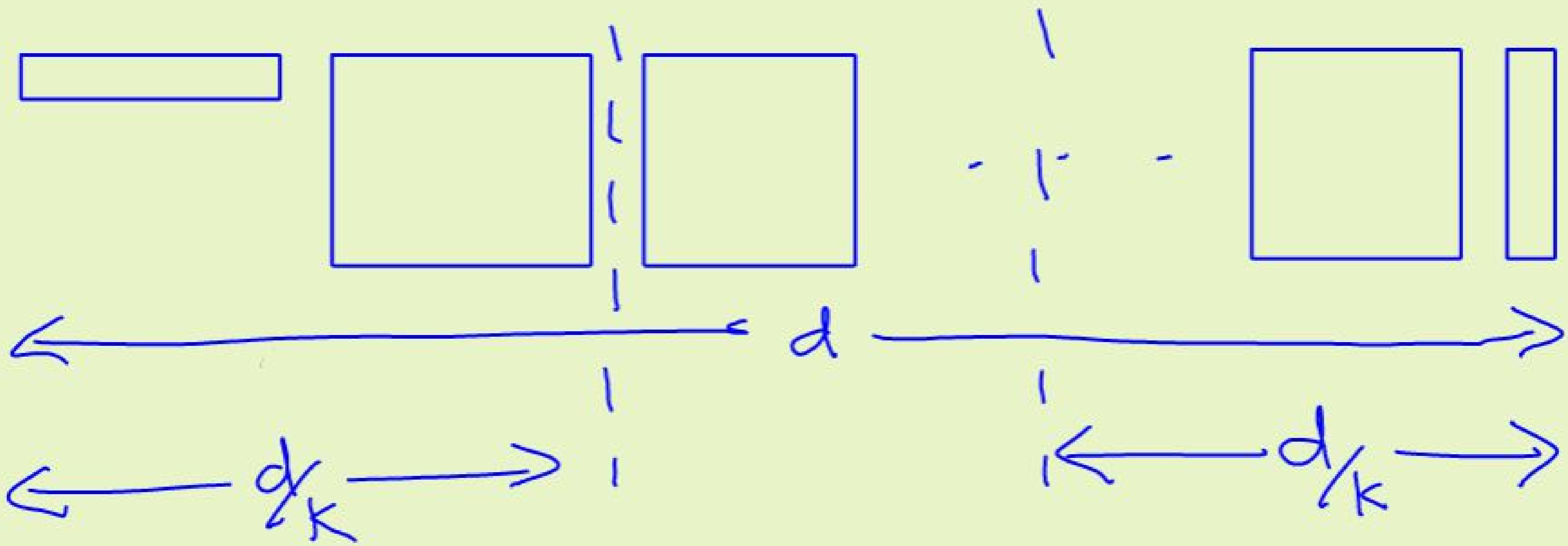
$$A = \sum_{i=1}^{s} \underbrace{P_i}_{\deg d/2} \underbrace{Q_i}_{\deg \frac{d}{2}}$$



Reduction to depth 4



Reduction to depth 4

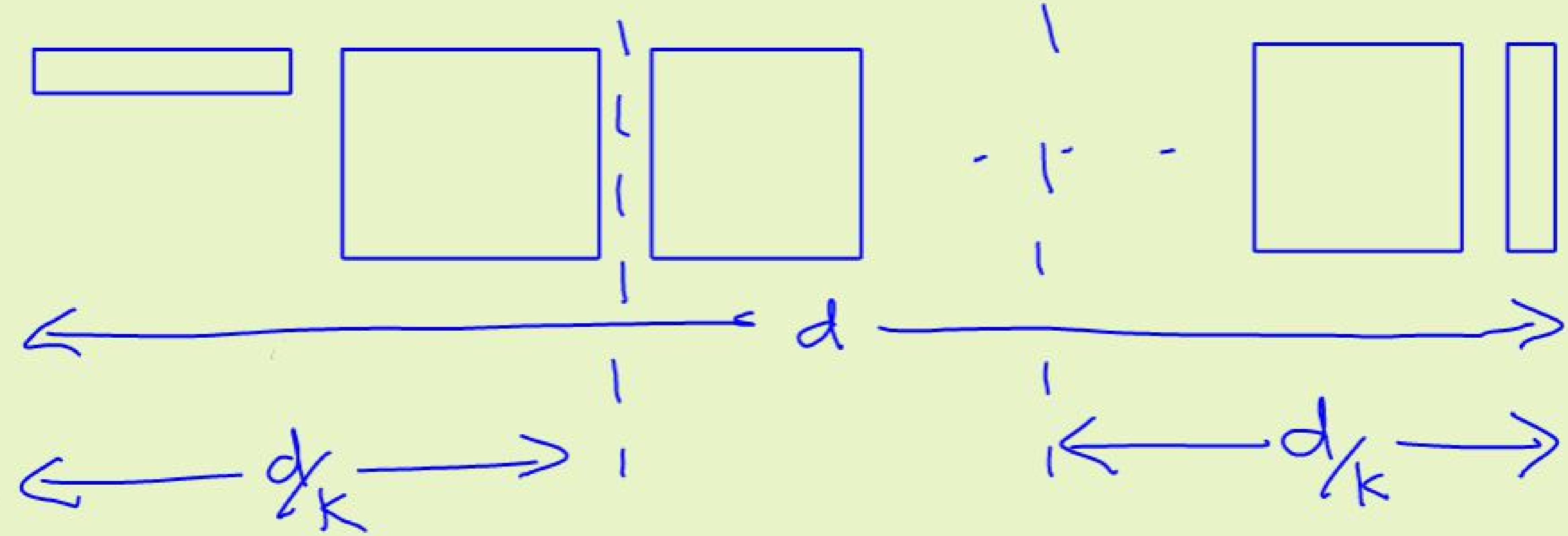


Thm: A ABP size s deg d

$$\Downarrow$$

$$A = \sum_{i=1}^{s^{O(\sqrt{d})}} P_{i,1} \cdots \overbrace{P_{i,\sqrt{d}}}^{\deg \sqrt{d}}$$

Reduction to depth 4



Thm: A ABP size s deg d

$$\Downarrow$$

$$A = \sum_{i=1}^{s^{O(\sqrt{d})}} \underbrace{P_{i,1} \cdots P_{i,\sqrt{d}}}_{\deg \sqrt{d}}$$

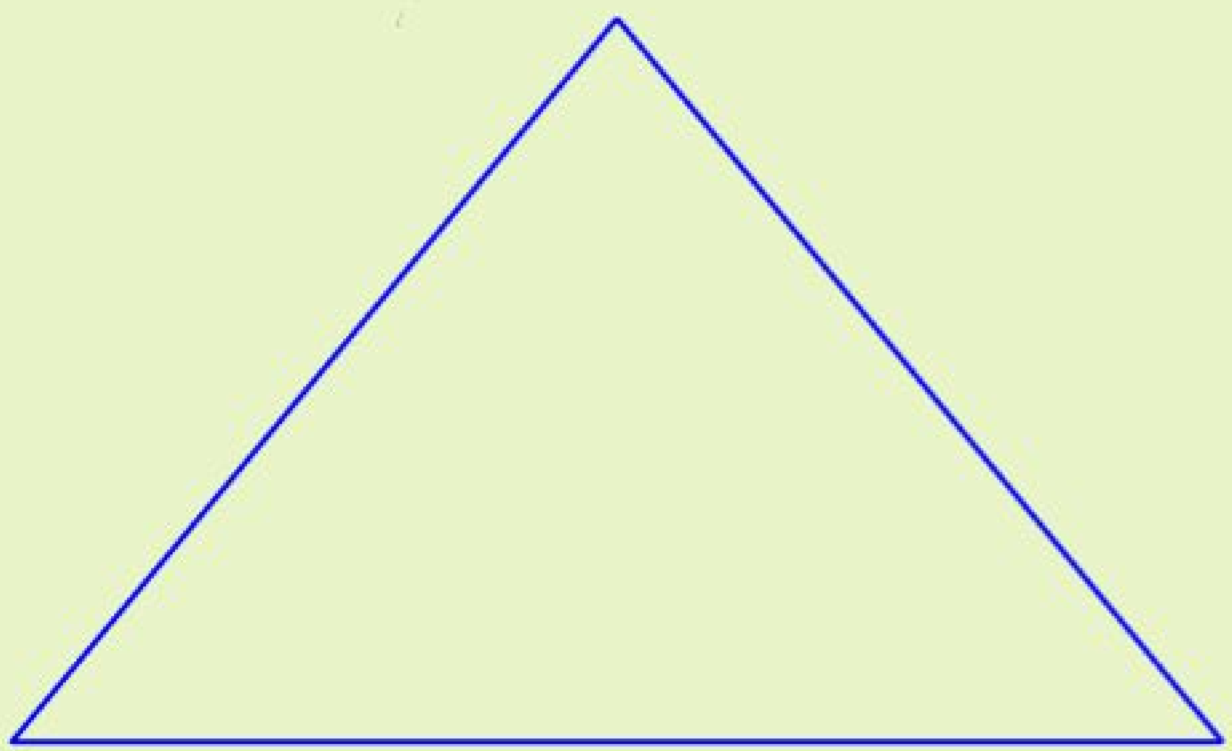
$\Sigma\Pi\Sigma\Pi$ formula of size $s^{O(\sqrt{d})}$.

Circuit depth-reduction

Circuit depth-reduction

C size s $\xrightarrow{\text{VSBR'83}}$ C' size $\mathrm{poly}(s,d)$

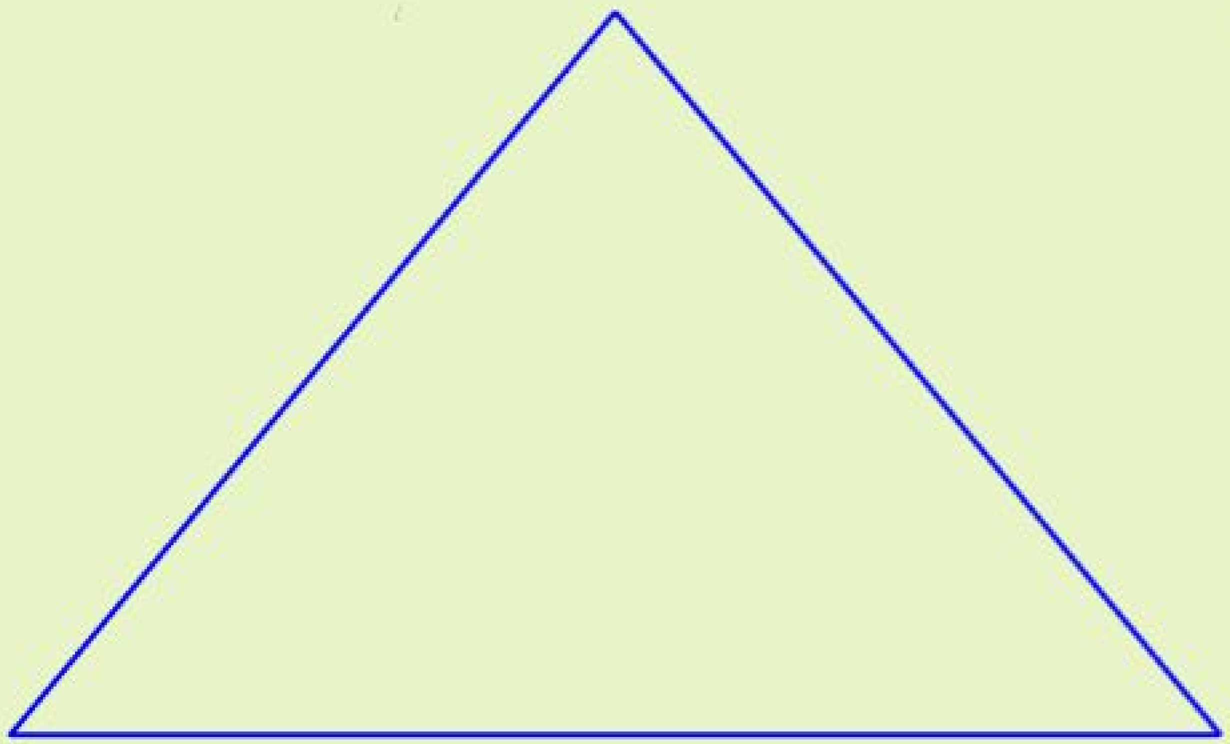
deg d depth $O(\log d)$



Circuit depth-reduction

C size s $\xrightarrow{\text{VSBR'83}}$ C' size $\text{poly}(s,d)$

deg d depth $O(\log d)$

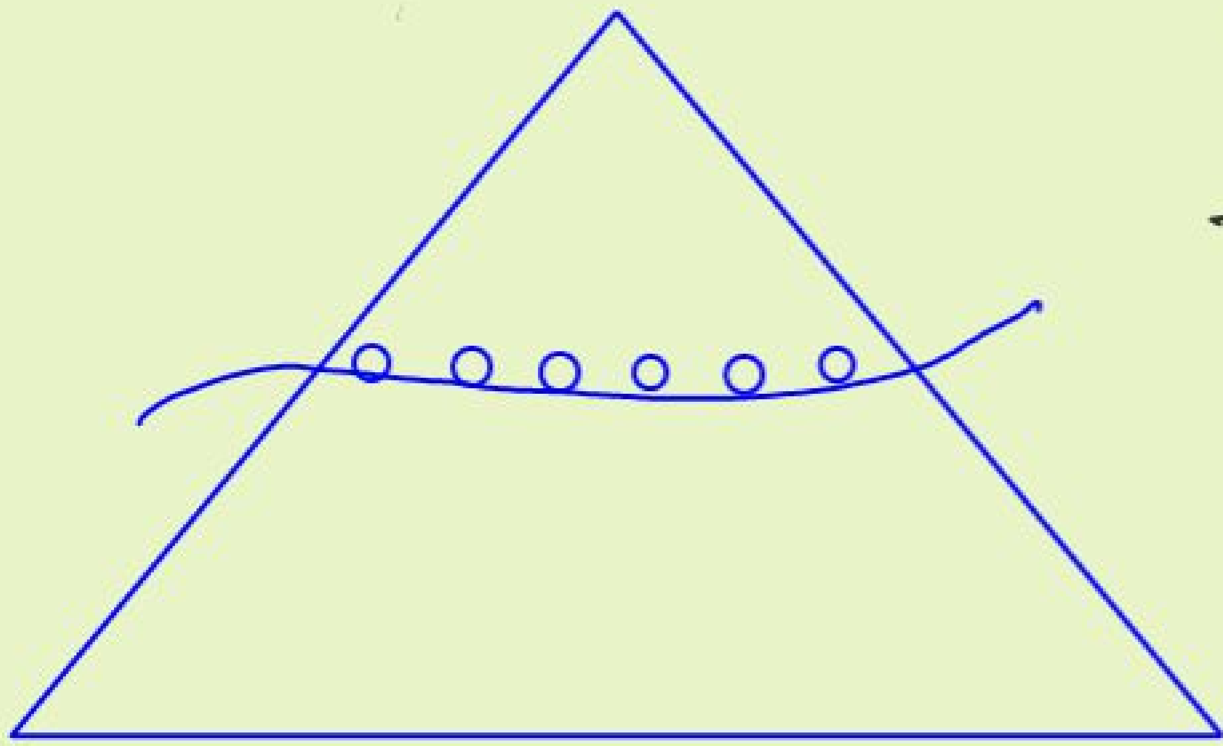


$\rightarrow$ Homogenization

Circuit depth-reduction

C size s $\xrightarrow{\text{VSBR'83}}$ C' size $\text{poly}(s,d)$

deg d depth $O(\log d)$



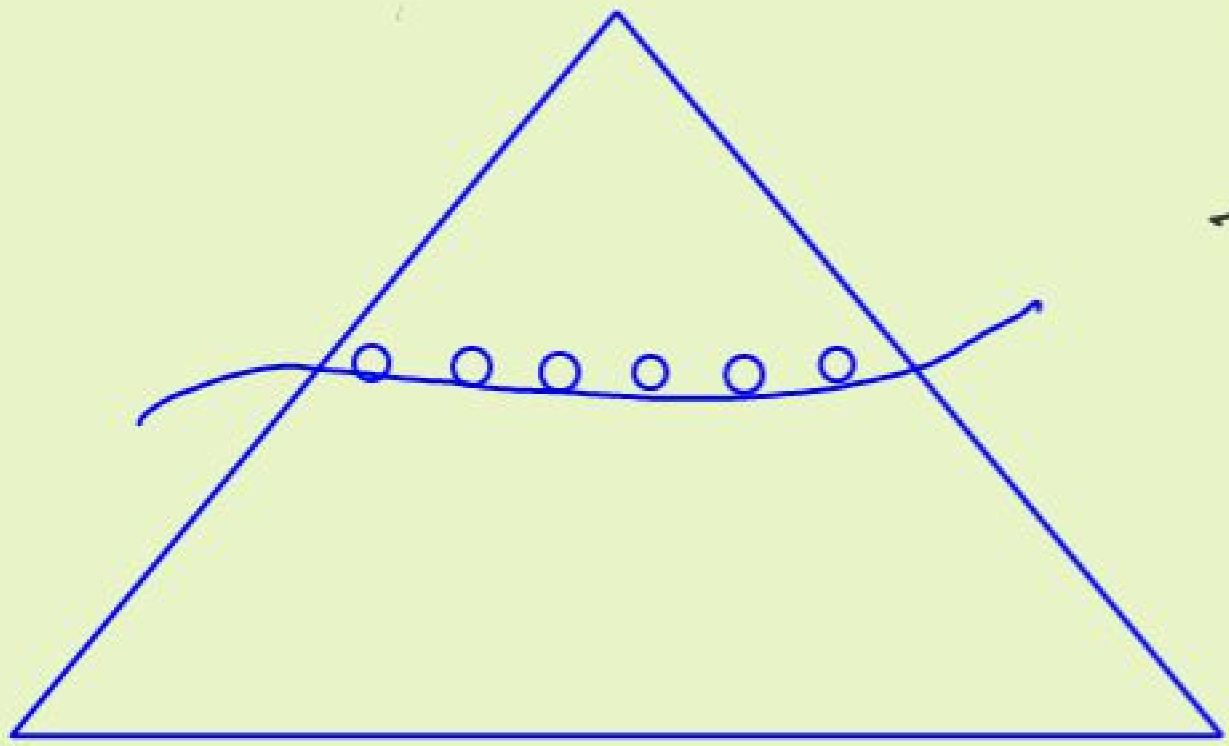
→ Homogenization

→ Find gates $g_1, \ldots, g_s$ of deg. $\approx d/2$

Circuit depth-reduction

C size s $\xrightarrow{\text{VSBR'83}}$ C' size $\mathrm{poly}(s,d)$

deg d depth $O(\log d)$



→ Homogenization

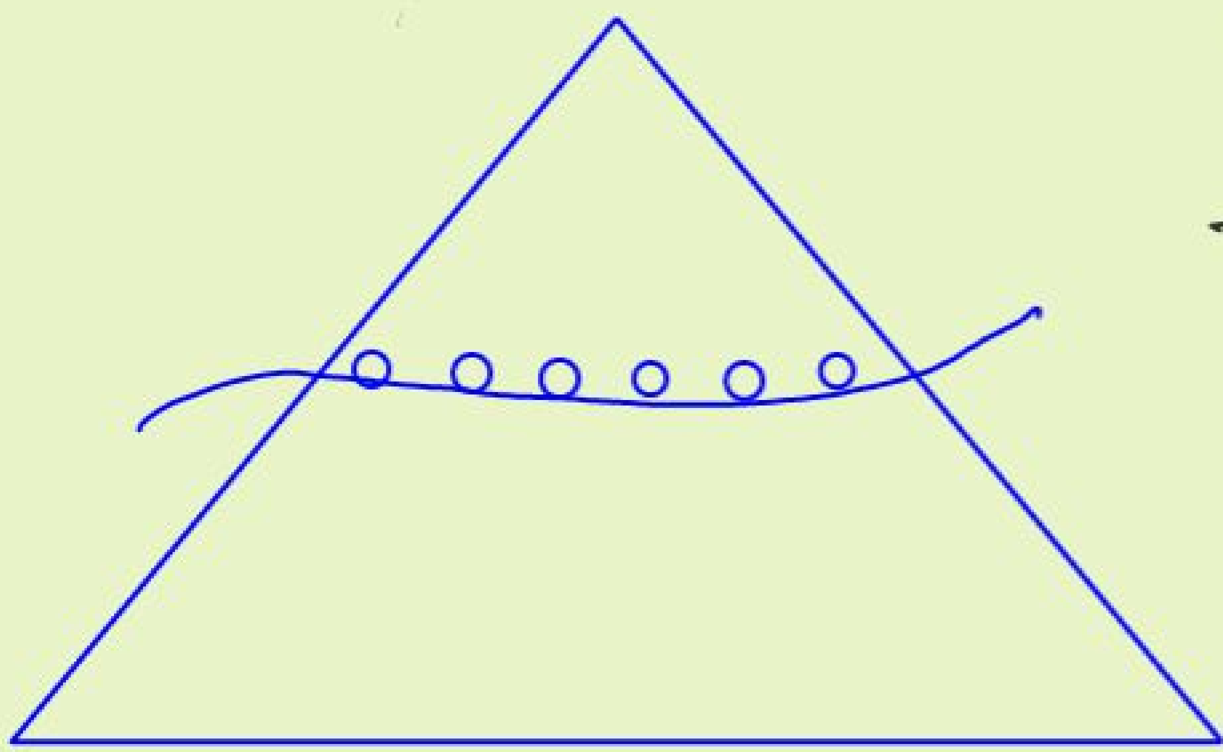
→ Find gates $g_1, \ldots, g_s$ of deg. $\approx d/2$

→ $C = \sum_{i=1}^{s} g_i \cdot \frac{\partial C}{\partial g_i}$

Circuit depth-reduction

C size s $\xrightarrow{\text{VSBR'83}}$ C' size $\mathrm{poly}(s,d)$

deg d depth $O(\log d)$



→ Homogenization

→ Find gates $g_1, \ldots, g_s$ of deg. $\approx d/2$

→ $C = \sum_{i=1}^{s} g_i \cdot \frac{\partial C}{\partial g_i}$

→ Recurse

Circuit depth-reduction

C size s $\xrightarrow{\text{VSBR'83}}$ C' size poly(s,d)

deg d depth $O(\log d)$

$$C = \sum_{i=1}^{s} \underbrace{g_i}_{} \cdot \underbrace{h_i}_{}$$

$\deg \in [d/3, 2d/3]$

Circuit depth-reduction

C size s, deg d $\xrightarrow{\text{VSBR'83}}$ C' size poly(s,d), depth $O(\log d)$

C size s, deg d $\xrightarrow{\text{AV'08, Tav'13}}$ $\Sigma\Pi\Sigma\Pi$ formula of size $s^{O(\sqrt{d})}$

Circuit depth-reduction

C size s $\xrightarrow{\text{VSBR'83}}$ C' size $\mathrm{poly}(s,d)$

deg d depth $O(\log d)$

$\xrightarrow{\text{AV'08, Tav'13}}$ $\Sigma\Pi\Sigma\Pi$ formula of size $s^{O(\sqrt{d})}$

$\mathrm{Per} \in \mathrm{VP} \implies \mathrm{Per}_n$ has $\Sigma\Pi\Sigma\Pi$ formula of size $n^{O(\sqrt{n})}$.

Circuit depth-reduction

C size s, deg d $\xrightarrow{\text{VSBR'83}}$ C' size $\mathrm{poly}(s,d)$, depth $O(\log d)$

$\xrightarrow{\text{AV'08, Tav'13}}$ $\Sigma\Pi\Sigma\Pi$ formula of size $s^{O(\sqrt{d})}$

$\xrightarrow{\text{GKKS'13}}$ $\Sigma\Pi\Sigma$ formula of size $s^{O(\sqrt{d})}$ (*)

Circuit depth-reduction

C size s, deg d $\xrightarrow{\text{VSBR'83}}$ C' size $\mathrm{poly}(s,d)$, depth $O(\log d)$

$\xrightarrow{\text{AV'08, Tav'13}}$ $\Sigma\Pi\Sigma\Pi$ formula of size $s^{O(\sqrt{d})}$

$\xrightarrow{\text{GKKS'13}}$ $\Sigma\Pi\Sigma$ formula of size $s^{O(\sqrt{d})}$ (*)

(*) - $\mathbb{F} = \mathbb{Q}$

Can we prove lower bds for small-depth formulas/circuits?