Amortized bivariate multi-point evaluation

Joris van der Hoeven
CNRS, École polytechnique
Joint work with **Grégoire Lecerf**

July 21, 2021

Multi-point evaluation

Problem: multi-point evaluation

INPUT: $P \in \mathbb{K}[x_1, \ldots, x_D]$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^D)^n$

OUTPUT: $P(\boldsymbol{\alpha}) = (P(\alpha_1), \ldots, P(\alpha_n)) \in \mathbb{K}^n$

Multi-point evaluation

Problem: multi-point evaluation

INPUT: $P \in \mathbb{K}[x_1, \ldots, x_D]$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^D)^n$

OUTPUT: $P(\boldsymbol{\alpha}) = (P(\alpha_1), \ldots, P(\alpha_n)) \in \mathbb{K}^n$

Known complexity bounds when $\deg P \leqslant d, \quad d^D \approx n$?

Multi-point evaluation

Problem: multi-point evaluation

INPUT: $P \in \mathbb{K}[x_1, \ldots, x_D]$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^D)^n$

OUTPUT: $P(\boldsymbol{\alpha}) = (P(\alpha_1), \ldots, P(\alpha_n)) \in \mathbb{K}^n$

Known complexity bounds when $\deg P \leqslant d, \quad d^D \approx n$?

- $D = 1 \longrightarrow$ remainder trees $\longrightarrow O(\mathsf{M}(n) \log n) = \tilde{O}(n)$

Multi-point evaluation

Problem: multi-point evaluation

INPUT: $P \in \mathbb{K}[x_1, \ldots, x_D]$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^D)^n$

OUTPUT: $P(\boldsymbol{\alpha}) = (P(\alpha_1), \ldots, P(\alpha_n)) \in \mathbb{K}^n$

Known complexity bounds when $\deg P \leqslant d, \quad d^D \approx n$?

- $D = 1 \longrightarrow$ remainder trees $\longrightarrow O(\mathsf{M}(n) \log n) = \tilde{O}(n)$
- $D = 2 \longrightarrow$ Nüsken–Ziegler (2004) $\longrightarrow \tilde{O}\left(n^{\frac{\omega+1}{2}}\right) = \tilde{O}(n^{1.333})$

Multi-point evaluation

Problem: multi-point evaluation

INPUT: $P \in \mathbb{K}[x_1, \ldots, x_D]$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^D)^n$

OUTPUT: $P(\boldsymbol{\alpha}) = (P(\alpha_1), \ldots, P(\alpha_n)) \in \mathbb{K}^n$

Known complexity bounds when $\deg P \leqslant d, \quad d^D \approx n$?

- $D = 1 \longrightarrow$ remainder trees $\longrightarrow O(\mathsf{M}(n) \log n) = \tilde{O}(n)$
- $D = 2 \longrightarrow$ Nüsken–Ziegler (2004) $\longrightarrow \tilde{O}\left(n^{\frac{\omega+1}{2}}\right) = \tilde{O}(n^{1.333})$

Theorem (Kedlaya–Umans 2008, 2011)

If $\mathbb{K} = \mathbb{F}_q$, then the bit-complexity of multi-point evaluation is $O((n \log q)^{1+o(1)})$.

If $\mathbb{K} = \mathbb{Z}$ or $\mathbb{K} = \mathbb{Q}$, then nearly optimal bound in terms of bit-size (CRT).

Link with polynomial system solving

System of equations

$$(\Sigma)\quad \begin{cases} P_1(x_1,\ldots,x_D) = 0 & \deg P_1 \leqslant d \\ \quad\vdots & \\ P_D(x_1,\ldots,x_D) = 0 & \deg P_D \leqslant d \end{cases}$$

Link with polynomial system solving

System of equations

$$(\Sigma)\quad \begin{cases} P_1(x_1,\ldots,x_D) = 0 & \deg P_1 \leqslant d \\ \quad\vdots & \\ P_D(x_1,\ldots,x_D) = 0 & \deg P_D \leqslant d \end{cases}$$

System solving $\longrightarrow$ Multi-point evaluation

Tentative solution $\boldsymbol{\alpha} \in (\mathbb{K}^D)^{d^D} \longrightarrow$ Proof that $P_1(\boldsymbol{\alpha}) = \cdots = P_D(\boldsymbol{\alpha}) = 0$

Link with polynomial system solving

System of equations

$$(\Sigma) \quad \begin{cases} P_1(x_1,\ldots,x_D) &= 0 & \qquad \deg P_1 \leqslant d \\ & \vdots & \\ P_D(x_1,\ldots,x_D) &= 0 & \qquad \deg P_D \leqslant d \end{cases}$$

System solving $\longrightarrow$ Multi-point evaluation

Tentative solution $\boldsymbol{\alpha} \in (\mathbb{K}^D)^{d^D} \longrightarrow$ Proof that $P_1(\boldsymbol{\alpha}) = \cdots = P_D(\boldsymbol{\alpha}) = 0$

Theorem (vdH–Lecerf, 2018)

If $\mathbb{K} = \mathbb{F}_q$, *then the Las Vegas bit-complexity to solve* (Σ) *is bounded by*

$$\tilde{O}(d^{(2+o(1))D-1} \log q).$$

If $\mathbb{K} = \mathbb{Z}$ *or* $\mathbb{K} = \mathbb{Q}$, *then the complexity is nearly optimal in the generic output size.*

Amortized multi-point evaluation

Problem: amortized multi-point evaluation

FIXED: $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^D)^n$

INPUT: $P \in \mathbb{K}[x_1, \ldots, x_D]$

OUTPUT: $P(\boldsymbol{\alpha}) = (P(\alpha_1), \ldots, P(\alpha_n)) \in \mathbb{K}^n$

Amortized multi-point evaluation

Problem: amortized multi-point evaluation

FIXED: $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^D)^n$

INPUT: $P \in \mathbb{K}[x_1, \ldots, x_D]$

OUTPUT: $P(\boldsymbol{\alpha}) = (P(\alpha_1), \ldots, P(\alpha_n)) \in \mathbb{K}^n$

Example: multivariate discrete Fourier transforms

Amortized multi-point evaluation

Problem: amortized multi-point evaluation

FIXED: $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^D)^n$

INPUT: $P \in \mathbb{K}[x_1, \ldots, x_D]$

OUTPUT: $P(\boldsymbol{\alpha}) = (P(\alpha_1), \ldots, P(\alpha_n)) \in \mathbb{K}^n$

Example: multivariate discrete Fourier transforms

Theorem (vdH–Lecerf 2020, Neiger–Rosenkilde–Solomatov $D = 2$)

Assume that $\boldsymbol{\alpha}$ is in "general position".

For $n = d^D$ with $d = \deg P$ and fixed D, the complexity of amortized multi-point evaluation is bounded by $\tilde{O}(n)$.

Amortized multi-point evaluation

Problem: amortized multi-point evaluation

FIXED: $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^D)^n$

INPUT: $P \in \mathbb{K}[x_1, \ldots, x_D]$

OUTPUT: $P(\boldsymbol{\alpha}) = (P(\alpha_1), \ldots, P(\alpha_n)) \in \mathbb{K}^n$

Example: multivariate discrete Fourier transforms

Theorem (vdH–Lecerf 2020, Neiger–Rosenkilde–Solomatov $D = 2$)

Assume that $\boldsymbol{\alpha}$ is in "general position".

For $n = d^D$ with $d = \deg P$ and fixed D, the complexity of amortized multi-point evaluation is bounded by $\tilde{O}(n)$.

Theorem (this talk)

If $D = 2$ and $n = d^2$, then $\exists$ $\tilde{O}(n)$ algorithm for amortized multi-point evaluation.

k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1, 2, 3, \ldots\}$

$$\deg_k x^a y^b \;=\!=\; a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a + kb < u + kv & \text{or} \\ a + kb = u + kv \text{ and } b < v. \end{cases}$$

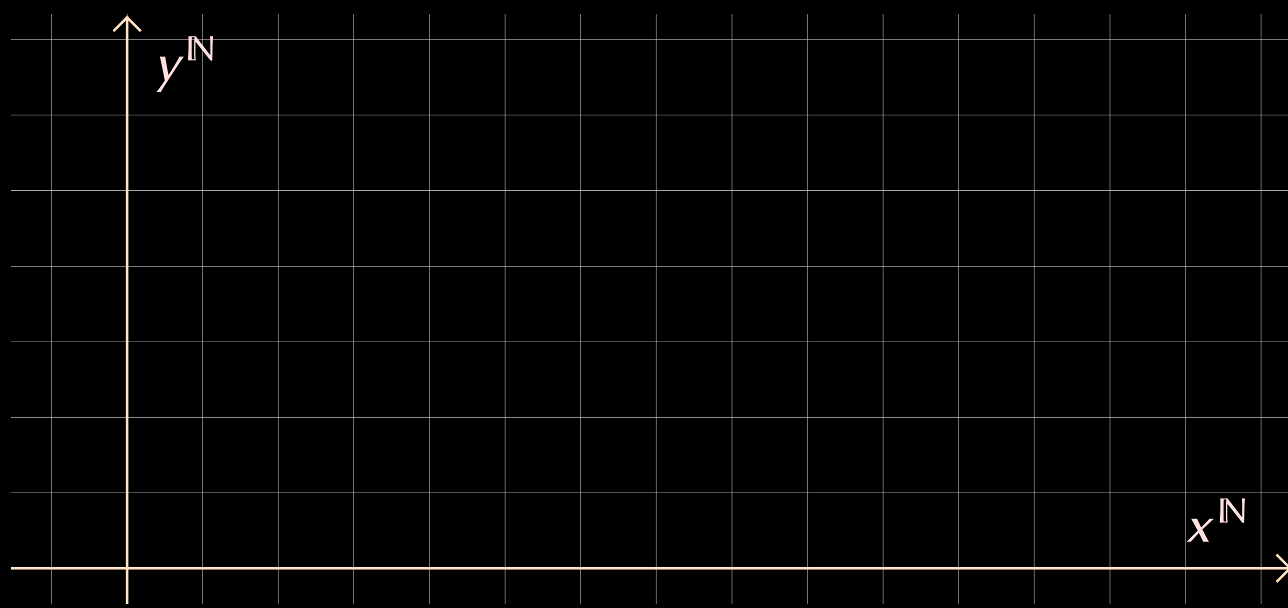
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1,2,3,\ldots\}$

$$\deg_k x^a y^b = a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a+kb < u+kv & \text{or} \\ a+kb = u+kv \text{ and } b < v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



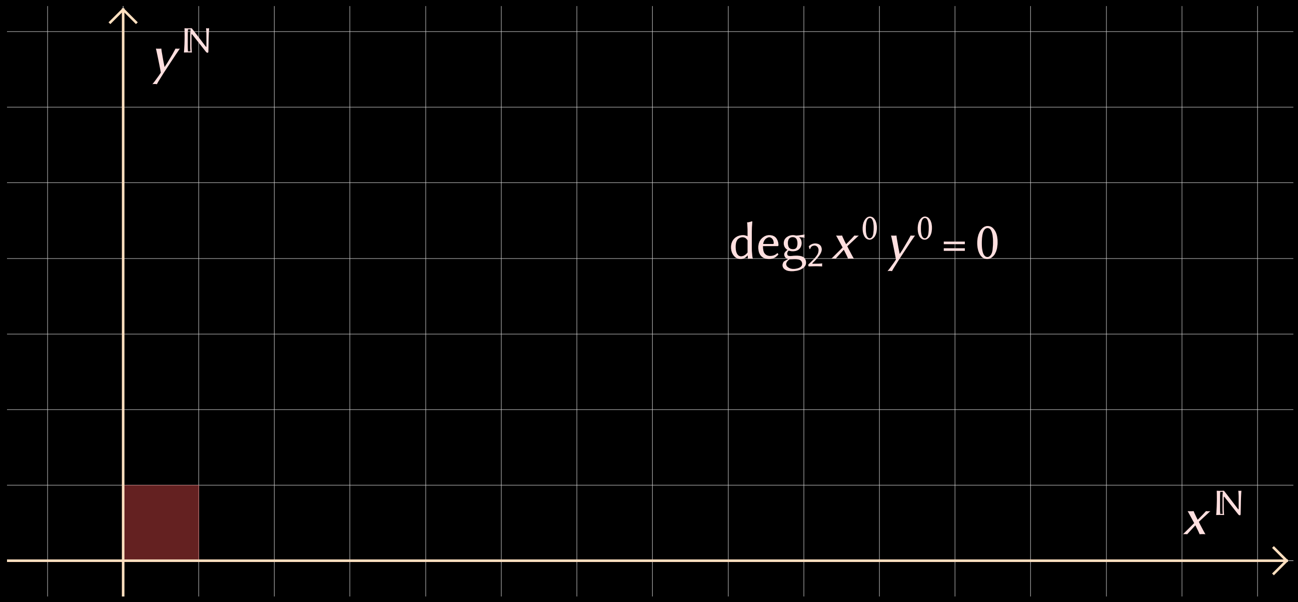
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1,2,3,\dots\}$

$$\deg_k x^a y^b \mathrel{=\!=} a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a+kb < u+kv & \text{or} \\ a+kb = u+kv \text{ and } b<v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



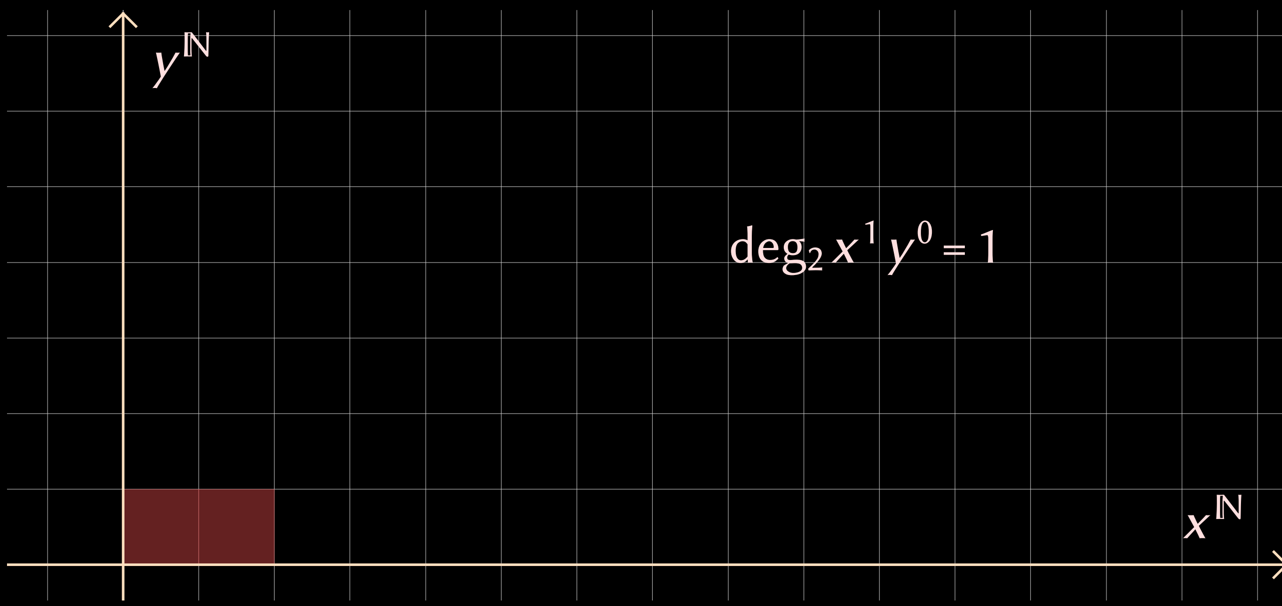
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1,2,3,\dots\}$

$$\deg_k x^a y^b \;=\!=\; a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a+kb < u+kv & \text{or} \\ a+kb = u+kv \text{ and } b<v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



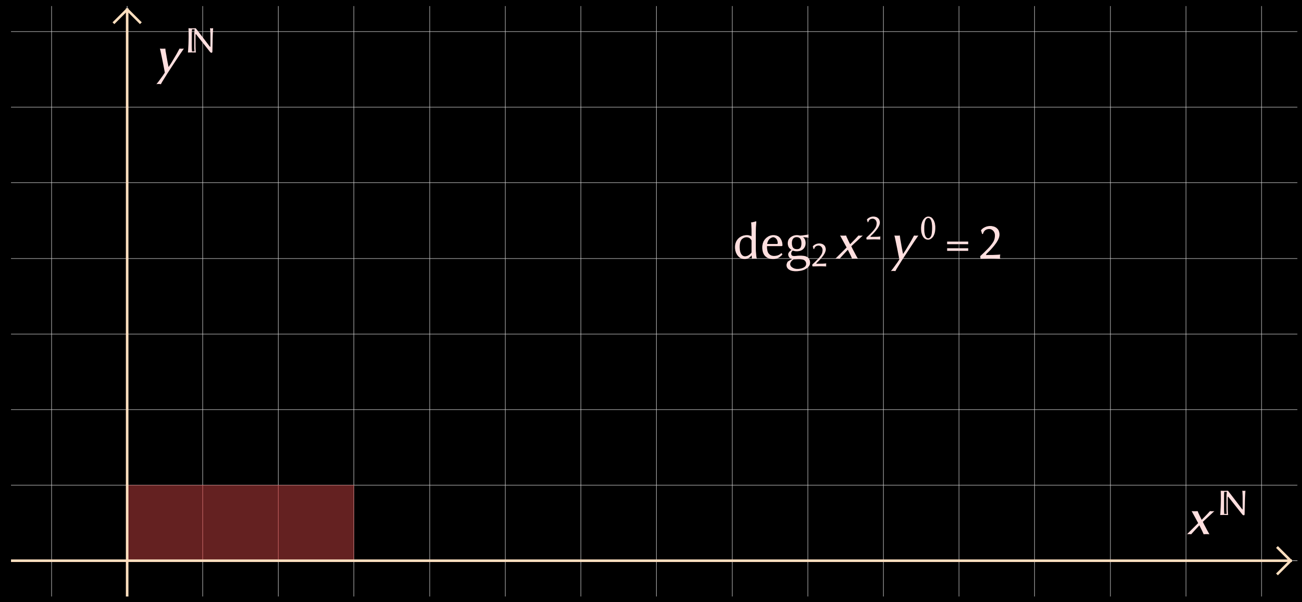
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1,2,3,\dots\}$

$$\deg_k x^a y^b \;=\!=\; a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a+kb < u+kv & \text{or} \\ a+kb = u+kv \text{ and } b<v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



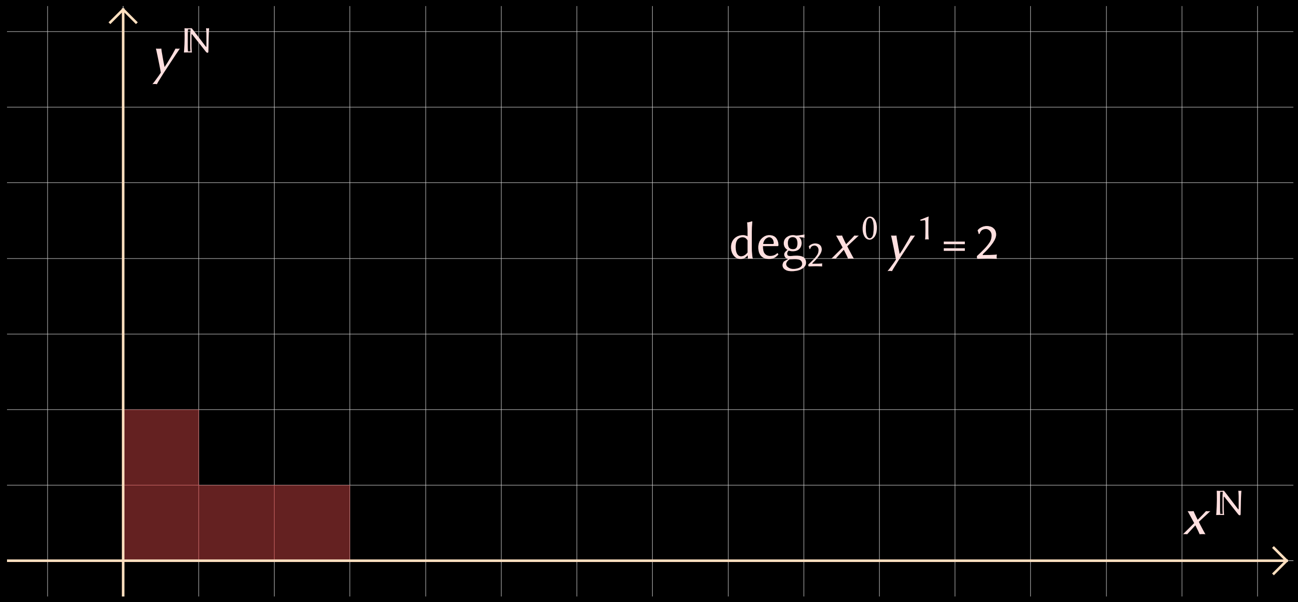
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1, 2, 3, \dots\}$

$$\deg_k x^a y^b \;=\!=\; a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a + kb < u + kv & \text{or} \\ a + kb = u + kv \text{ and } b < v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



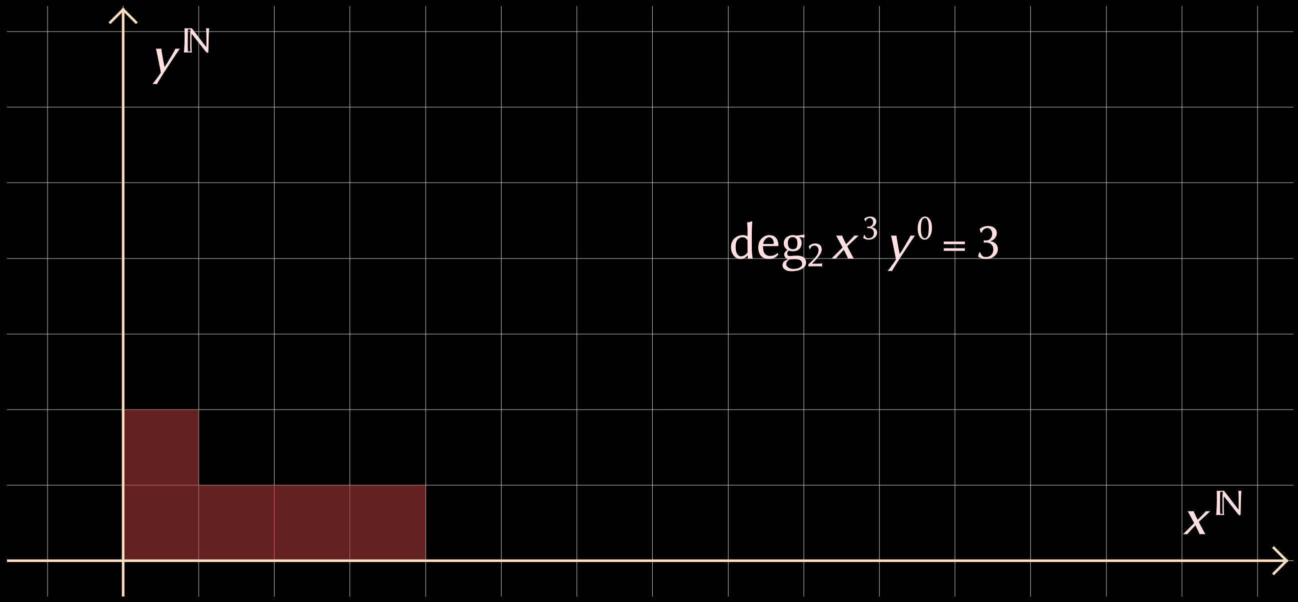
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1,2,3,\dots\}$

$$\deg_k x^a y^b \;=\!=\; a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a+kb < u+kv & \text{or} \\ a+kb = u+kv \text{ and } b < v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



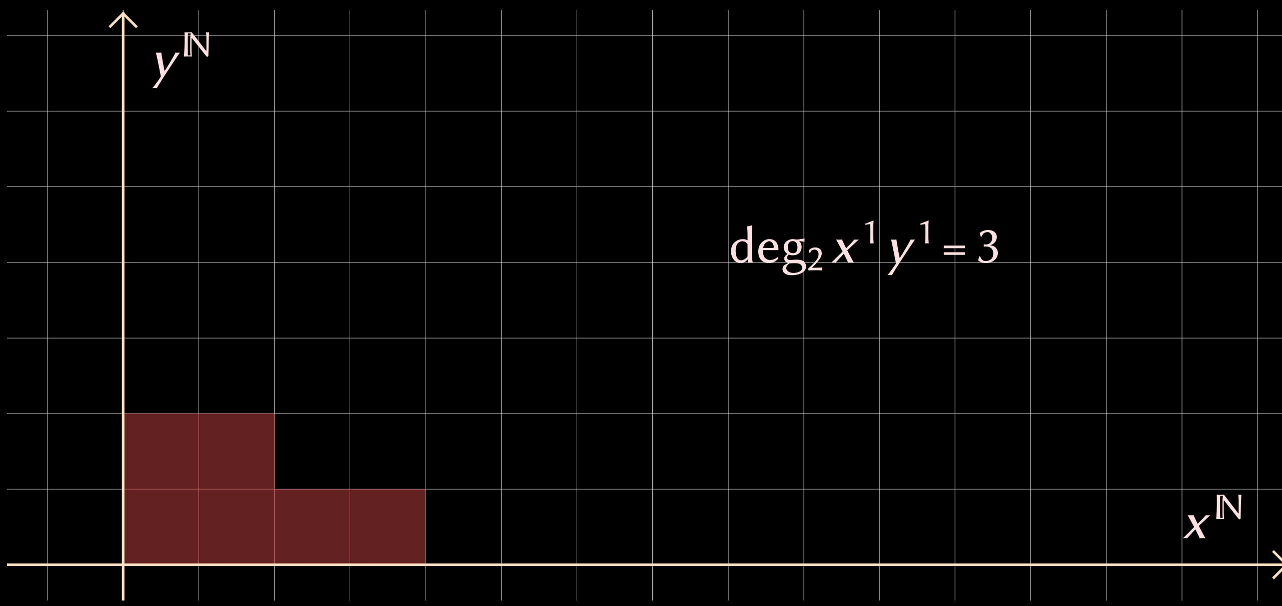
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1,2,3,\ldots\}$

$$\deg_k x^a y^b = a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a+kb < u+kv & \text{or} \\ a+kb = u+kv \text{ and } b < v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



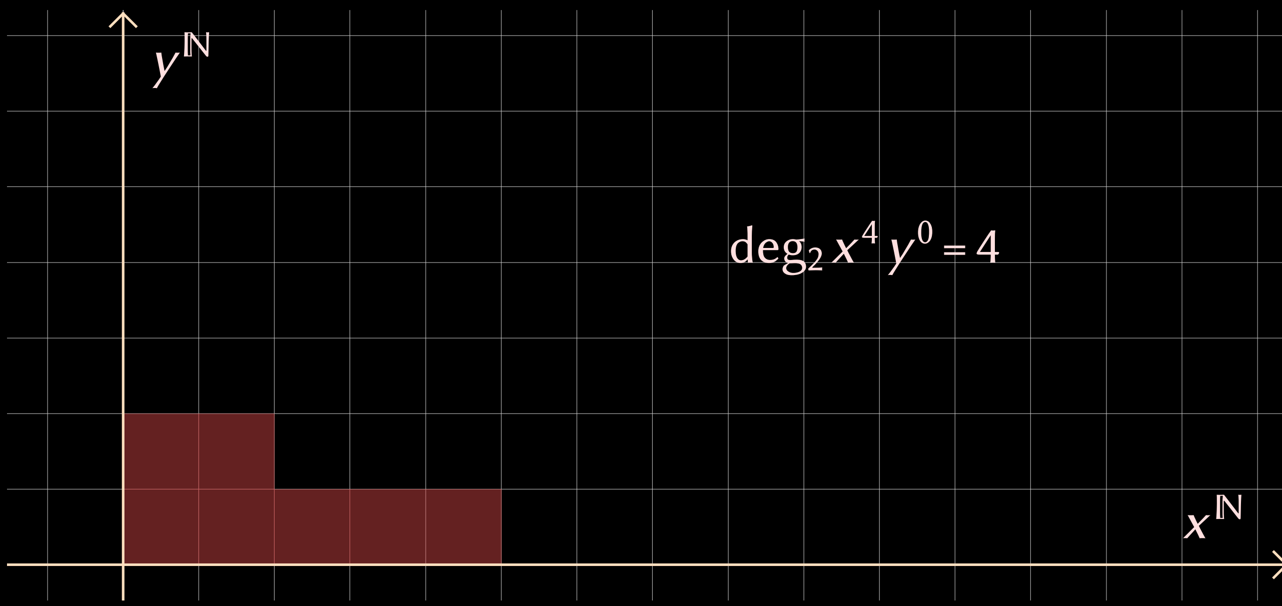
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1,2,3,\dots\}$

$$\deg_k x^a y^b = a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a+kb < u+kv & \text{or} \\ a+kb = u+kv \text{ and } b < v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1, 2, 3, \dots\}$

$$\deg_k x^a y^b \;=\!=\; a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a + kb < u + kv & \text{or} \\ a + kb = u + kv \text{ and } b < v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$

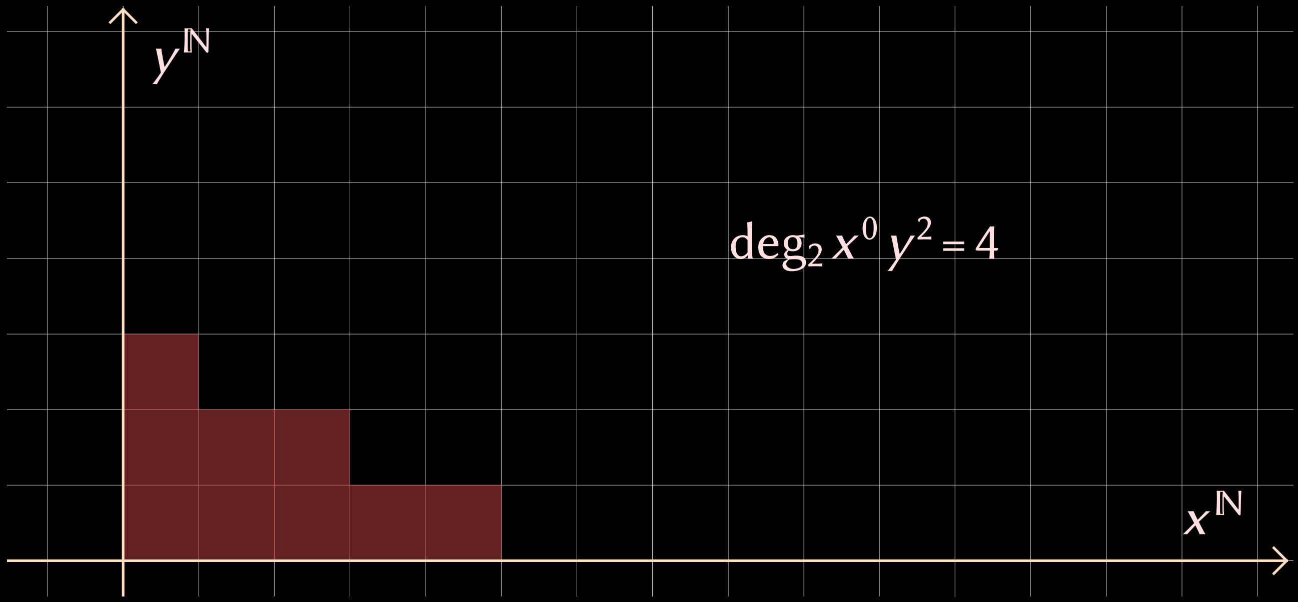
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1,2,3,\dots\}$

$$\deg_k x^a y^b \;=\!=\; a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a+kb < u+kv & \text{or} \\ a+kb = u+kv \text{ and } b<v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



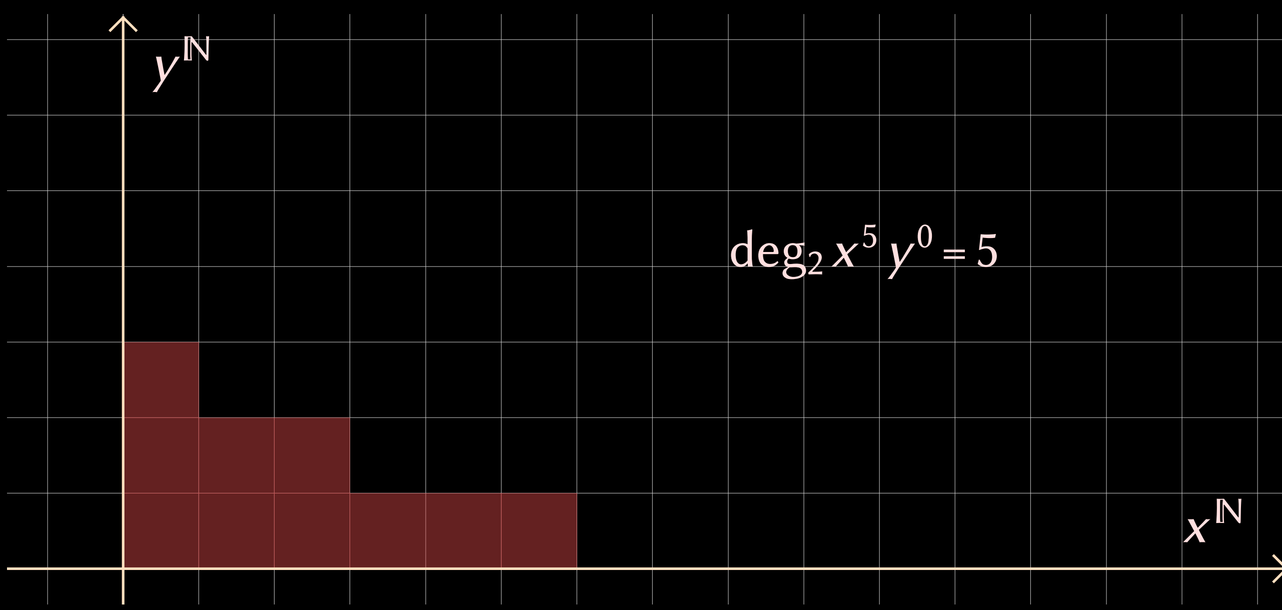
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1,2,3,\dots\}$

$$\deg_k x^a y^b \;=\!=\; a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a+kb < u+kv & \text{or} \\ a+kb = u+kv \text{ and } b < v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



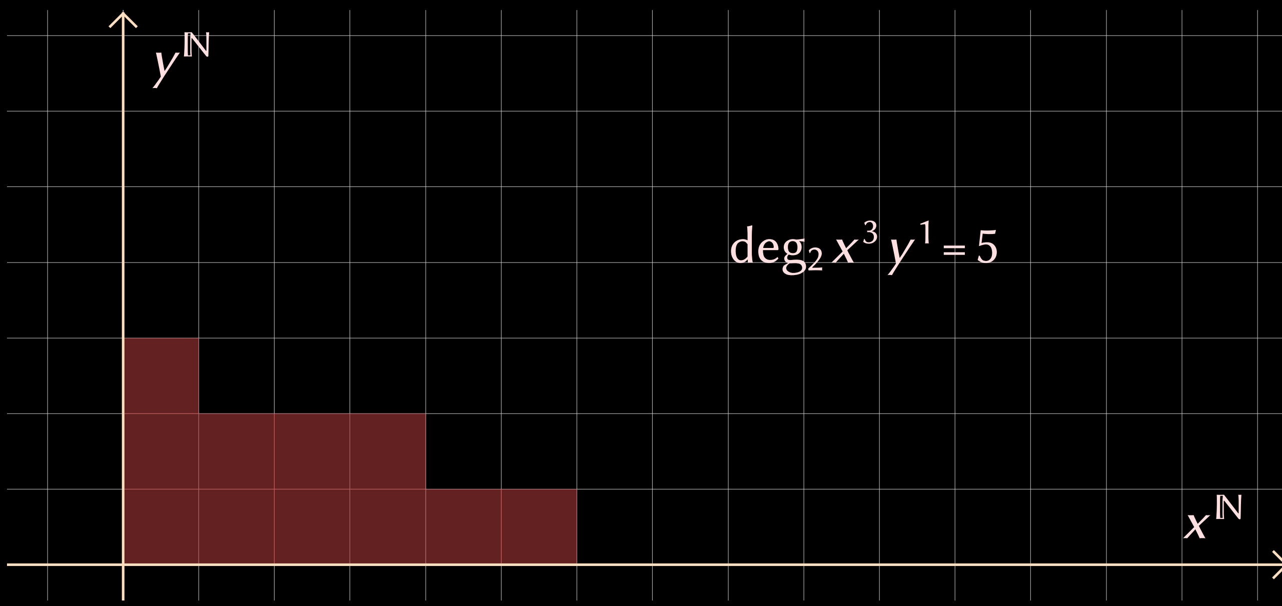
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1,2,3,\dots\}$

$$\deg_k x^a y^b \overset{\text{def}}{=\!=} a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a+kb < u+kv & \text{or} \\ a+kb = u+kv \text{ and } b < v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



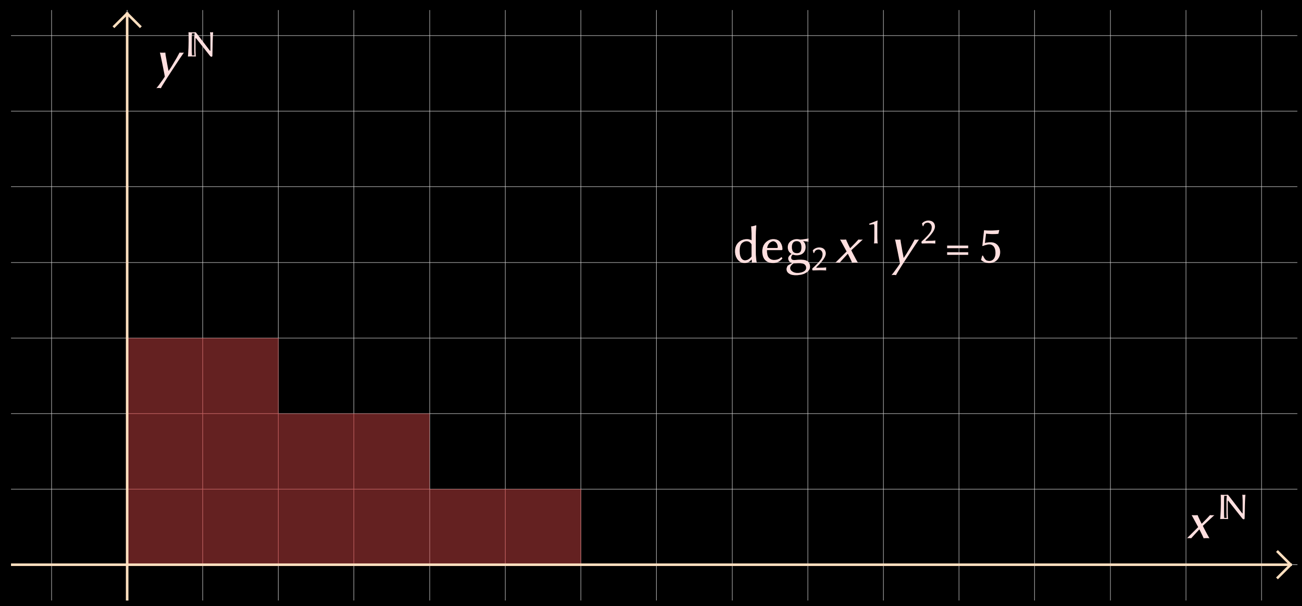
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1,2,3,\dots\}$

$$\deg_k x^a y^b \;=\!=\; a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a+kb < u+kv & \text{or} \\ a+kb = u+kv \text{ and } b < v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



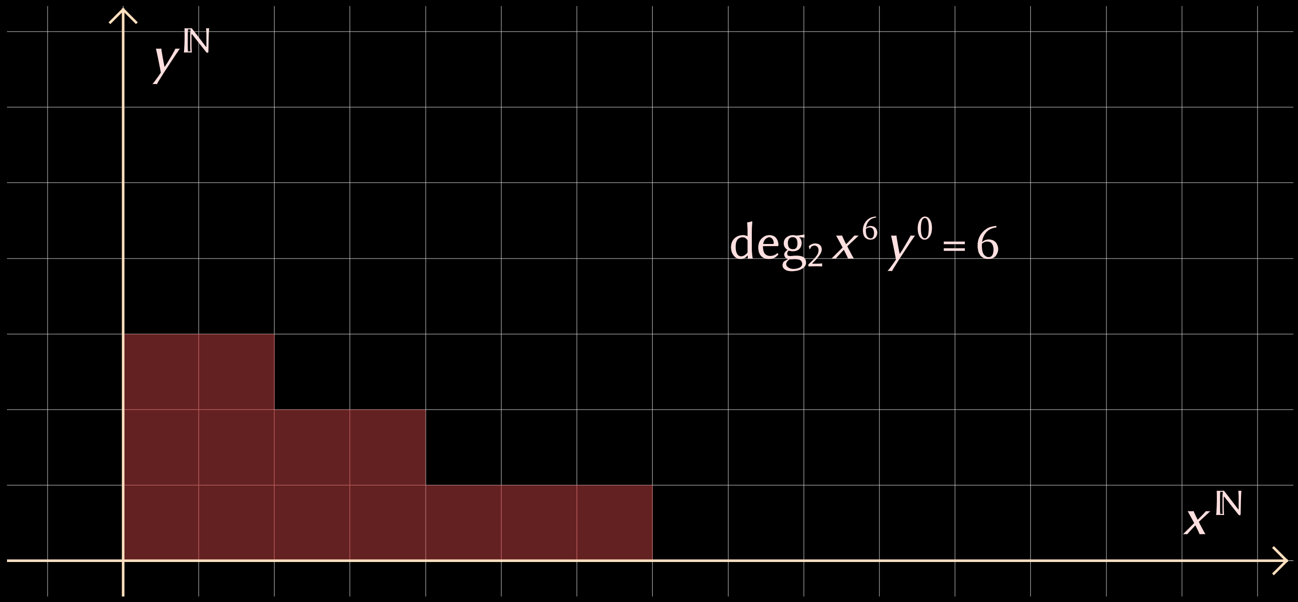
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1, 2, 3, \ldots\}$

$$\deg_k x^a y^b \;=\!=\; a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a + kb < u + kv & \text{or} \\ a + kb = u + kv \text{ and } b < v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



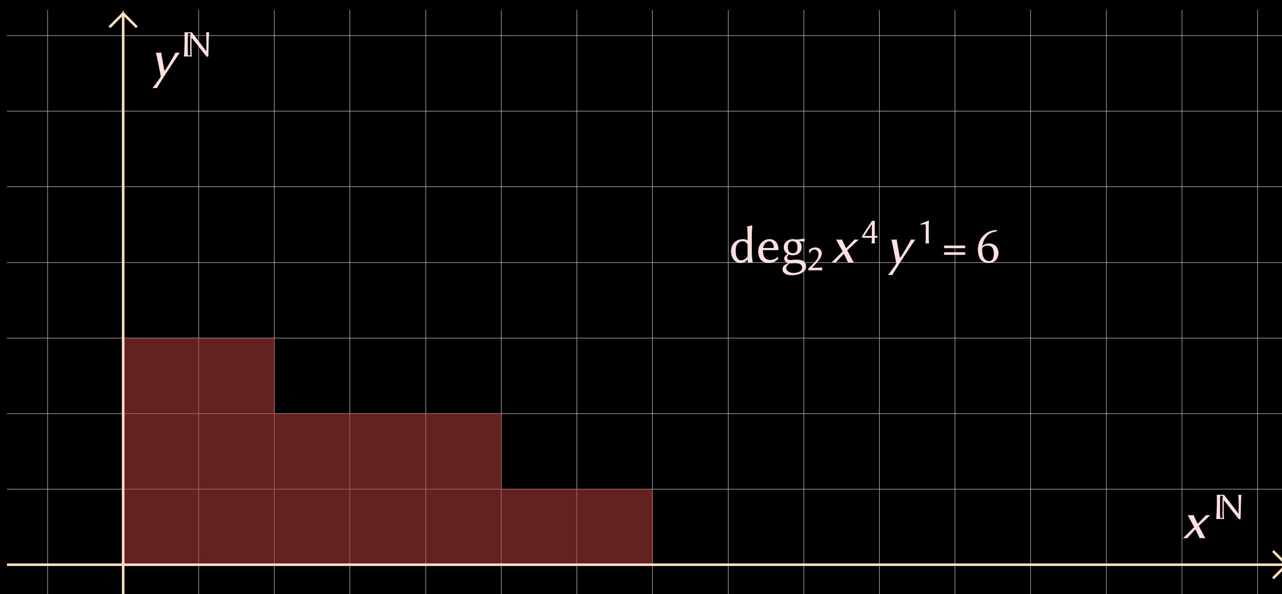
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1,2,3,\ldots\}$

$$\deg_k x^a y^b \;=\!=\; a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a+kb < u+kv & \text{or} \\ a+kb = u+kv \text{ and } b < v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



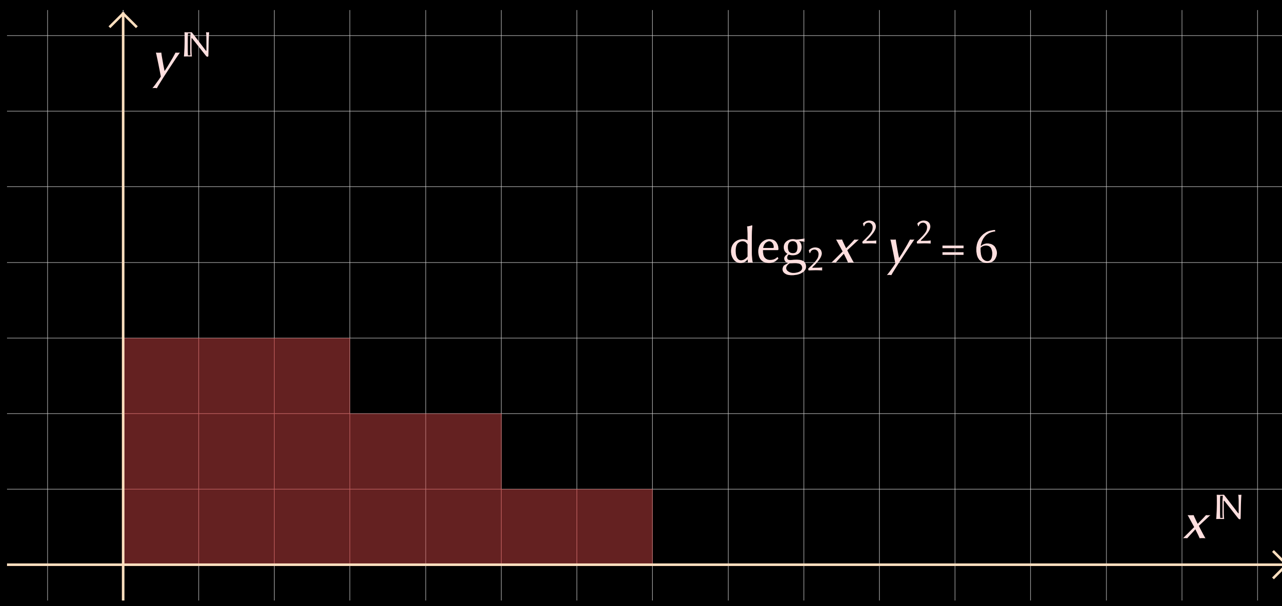
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1,2,3,\ldots\}$

$$\deg_k x^a y^b \;=\; a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a+kb < u+kv & \text{or} \\ a+kb = u+kv \text{ and } b < v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



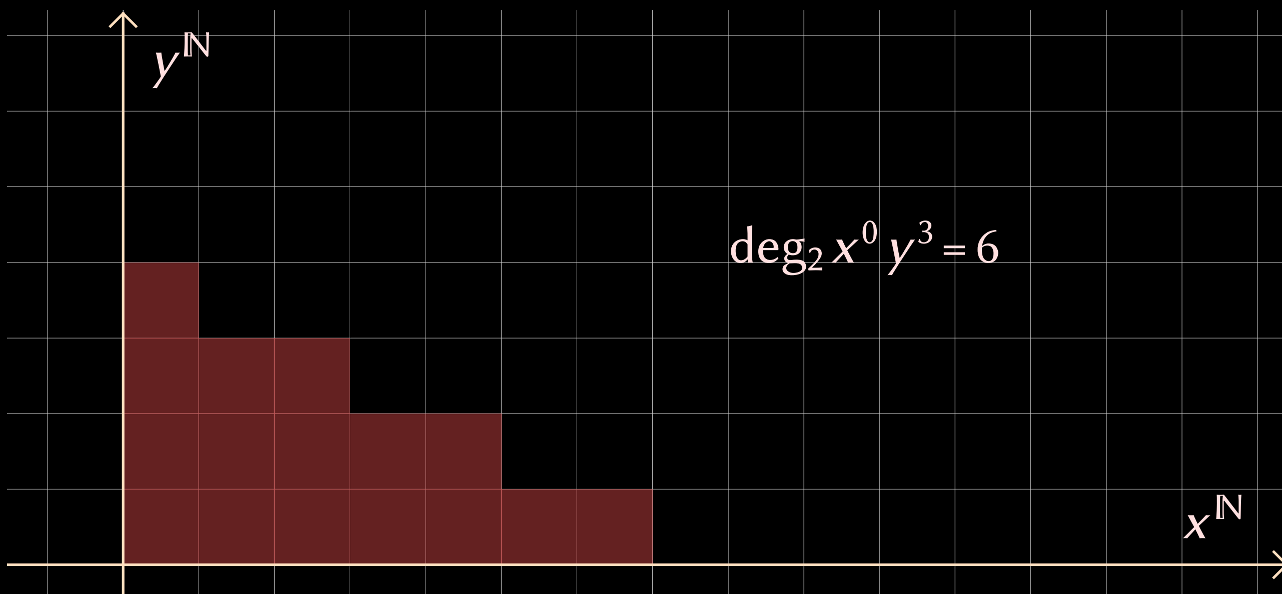
k-degree and the admissible ordering $\prec_k$

Definition: $\deg_k$ and $\prec_k$ for $k \in \{1,2,3,\ldots\}$

$$\deg_k x^a y^b \;=\!=\; a + kb$$

$$x^a y^b \prec_k x^u y^v \iff \begin{cases} a+kb < u+kv & \text{or} \\ a+kb = u+kv \text{ and } b<v. \end{cases}$$

Illustration: sorting the monomomials $x^a y^b$ by $\prec_2$



Gröbner basis of $I_{\boldsymbol{\alpha}}$ for $<_k$

$$\boldsymbol{\alpha} \;=\!=\!=\; (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$

$$I_{\boldsymbol{\alpha}} \;=\!=\!=\; \{P \in \mathbb{K}[x, y] : P(\boldsymbol{\alpha}) = 0\}$$

Gröbner basis of I_α for $\prec_k$

$$\boldsymbol{\alpha} \;=\!=\!=\; (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$

$$I_\alpha \;=\!=\!=\; \{P \in \mathbb{K}[x,y] : P(\boldsymbol{\alpha}) = 0\}$$

Gröbner basis for generic $\boldsymbol{\alpha}$

Gröbner basis of I_α for $<_k$

$$\boldsymbol{\alpha} \Longleftarrow (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$
$$I_\alpha \Longleftarrow \{P \in \mathbb{K}[x,y] : P(\boldsymbol{\alpha}) = 0\}$$

Gröbner basis for generic $\boldsymbol{\alpha}$

$$\boldsymbol{\alpha} \;=\!=\!=\; (\alpha_1, \ldots, \alpha_n) \;\in\; (\mathbb{K}^2)^n$$

$$I_{\boldsymbol{\alpha}} \;=\!=\!=\; \{P \in \mathbb{K}[x,y] : P(\boldsymbol{\alpha}) = 0\}$$

Gröbner basis for generic $\boldsymbol{\alpha}$

$$\boldsymbol{\alpha} \;=\!=\!=\; (\alpha_1, \ldots, \alpha_n) \;\in\; (\mathbb{K}^2)^n$$

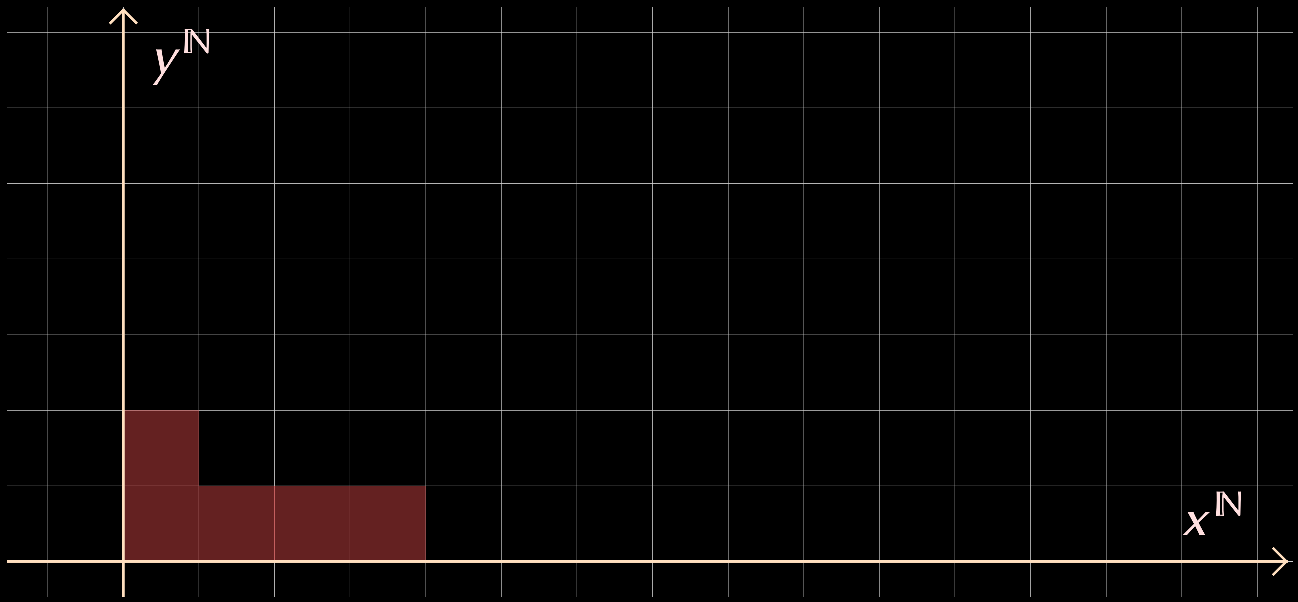
$$I_\alpha \;=\!=\!=\; \{P \in \mathbb{K}[x, y] : P(\boldsymbol{\alpha}) = 0\}$$

Gröbner basis for generic $\boldsymbol{\alpha}$

$$\boldsymbol{\alpha} == (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$

$$I_\alpha == \{P \in \mathbb{K}[x,y] : P(\boldsymbol{\alpha}) = 0\}$$

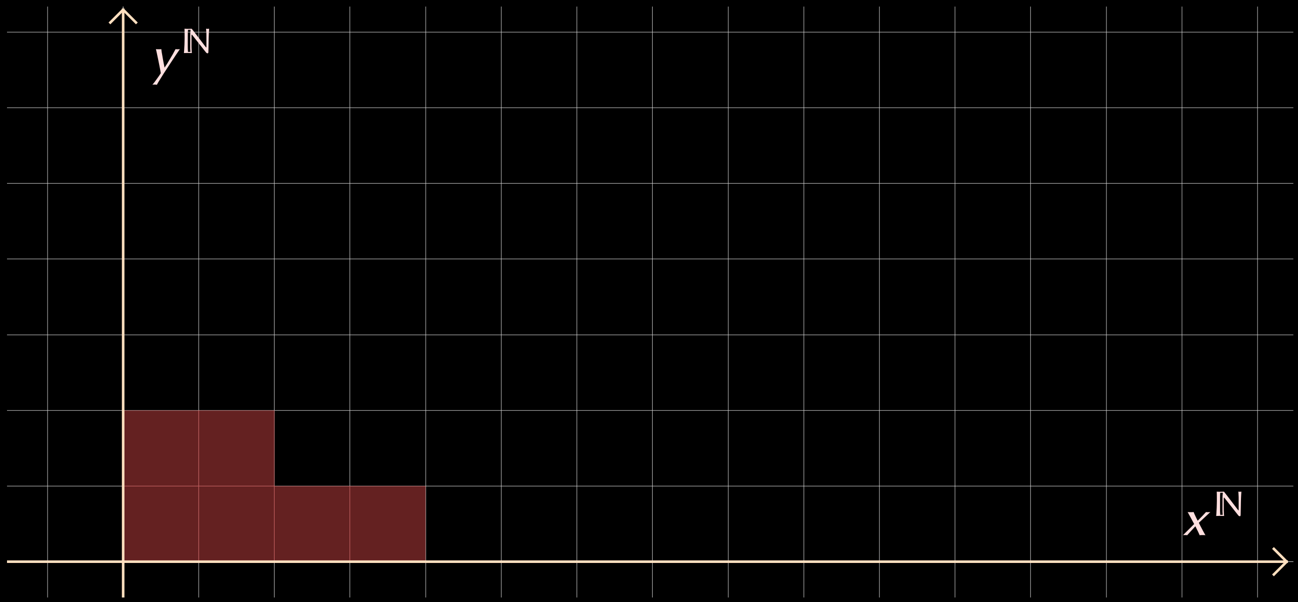
Gröbner basis for generic $\boldsymbol{\alpha}$



Gröbner basis of I_α for $\prec_k$

$$\boldsymbol{\alpha} \;=\!=\; (\alpha_1, \ldots, \alpha_n) \;\in\; (\mathbb{K}^2)^n$$
$$I_{\boldsymbol{\alpha}} \;=\!=\; \{P \in \mathbb{K}[x, y] : P(\boldsymbol{\alpha}) = 0\}$$

Gröbner basis for generic $\boldsymbol{\alpha}$

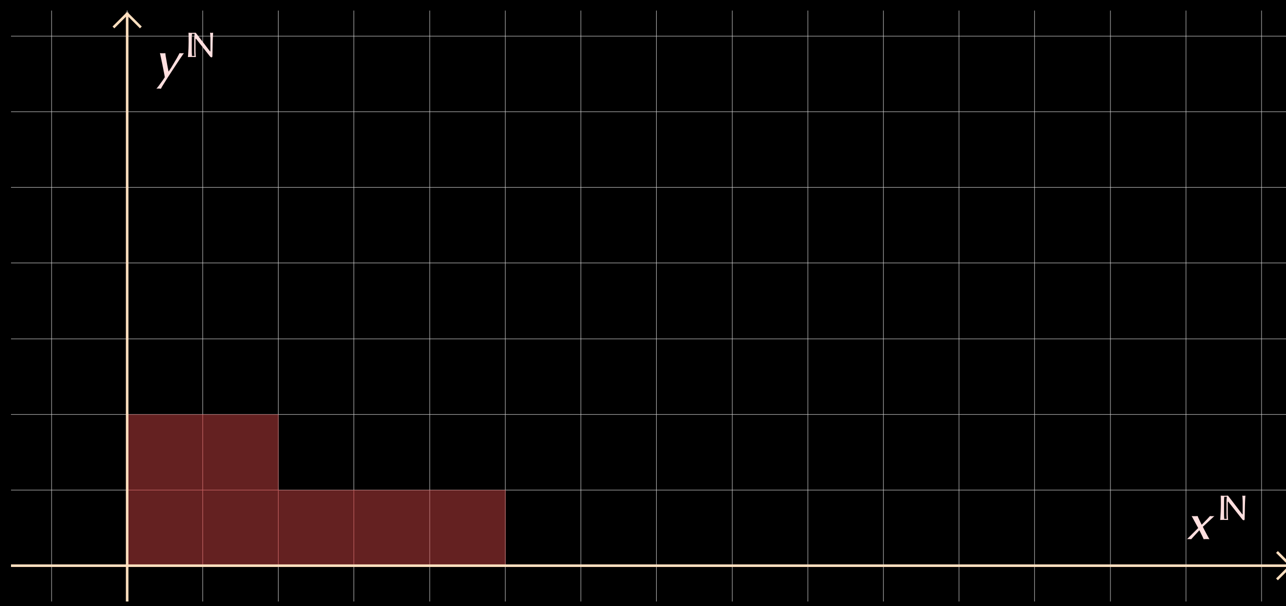


Gröbner basis of I_α for $\prec_k$

$$\boldsymbol{\alpha} \Longleftrightarrow (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$

$$I_\alpha \Longleftrightarrow \{P \in \mathbb{K}[x, y] : P(\boldsymbol{\alpha}) = 0\}$$

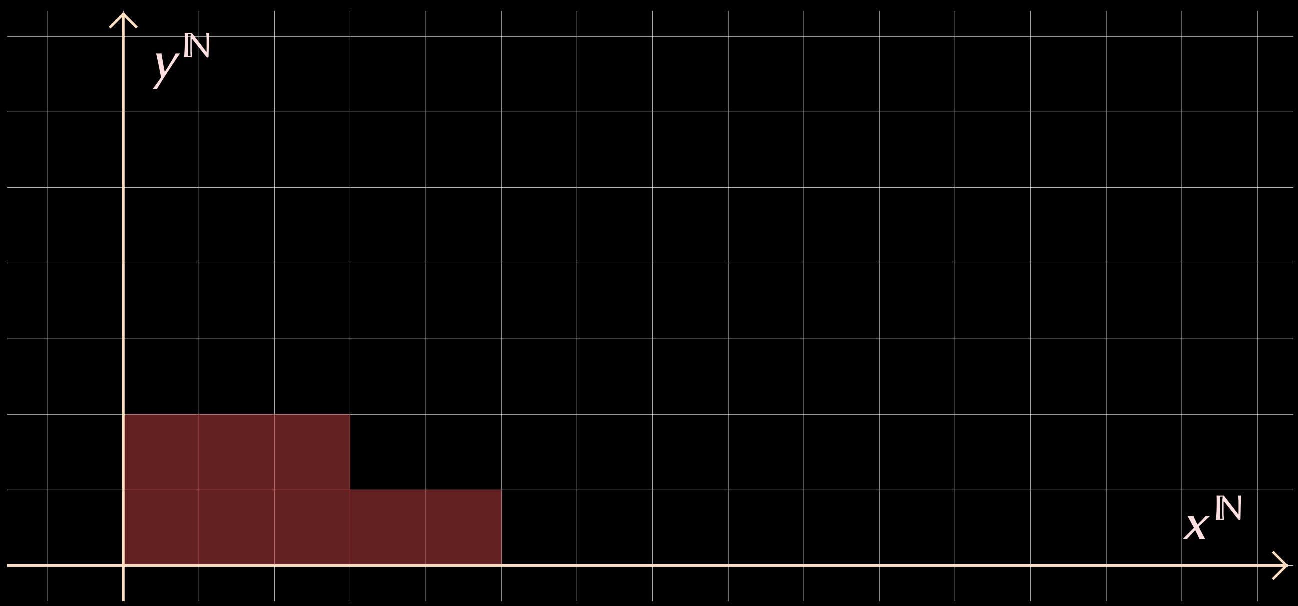
Gröbner basis for generic $\boldsymbol{\alpha}$



Gröbner basis of I_α for $\prec_k$

$$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$
$$I_{\boldsymbol{\alpha}} = \{P \in \mathbb{K}[x, y] : P(\boldsymbol{\alpha}) = 0\}$$

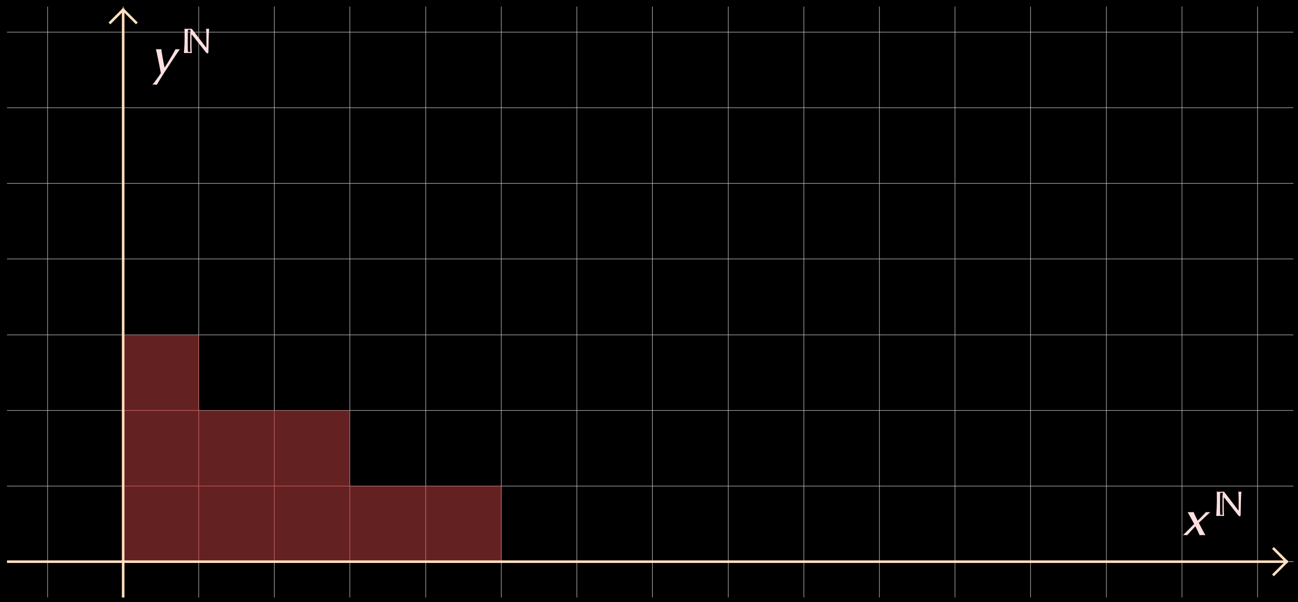
Gröbner basis for generic $\boldsymbol{\alpha}$



$$\boldsymbol{\alpha} == (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$

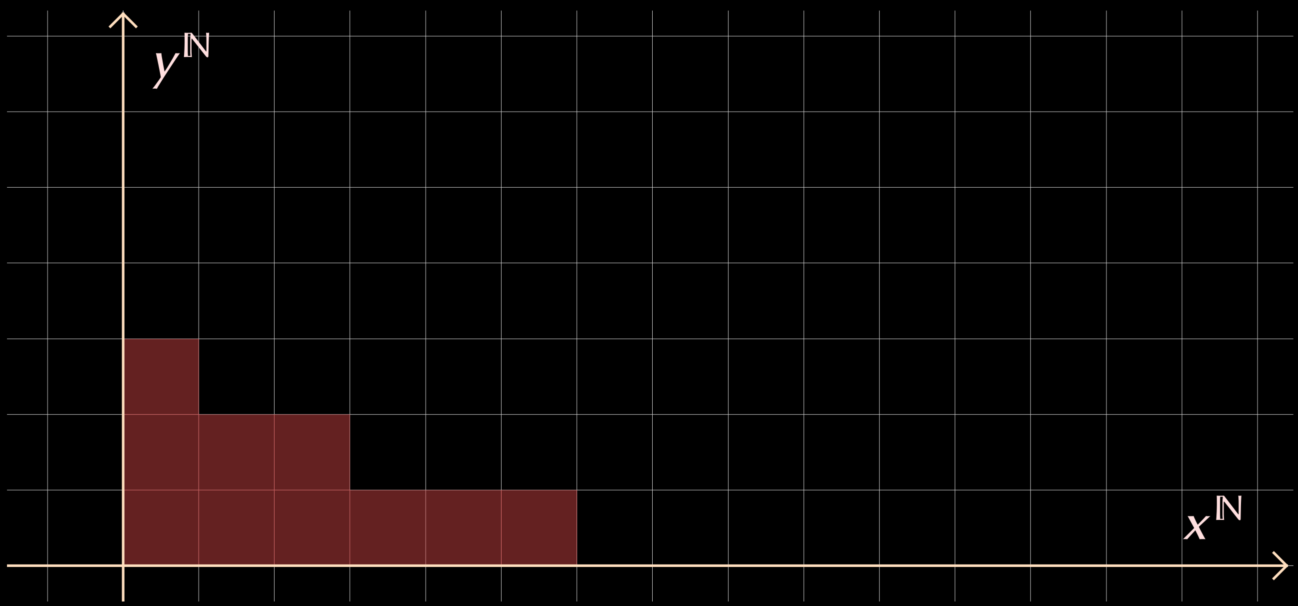
$$I_\alpha == \{P \in \mathbb{K}[x,y] : P(\boldsymbol{\alpha}) = 0\}$$

Gröbner basis for generic $\boldsymbol{\alpha}$



$$\boldsymbol{\alpha} \;=\!=\!= \; (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$
$$I_\alpha \;=\!=\!= \; \{P \in \mathbb{K}[x, y] : P(\boldsymbol{\alpha}) = 0\}$$

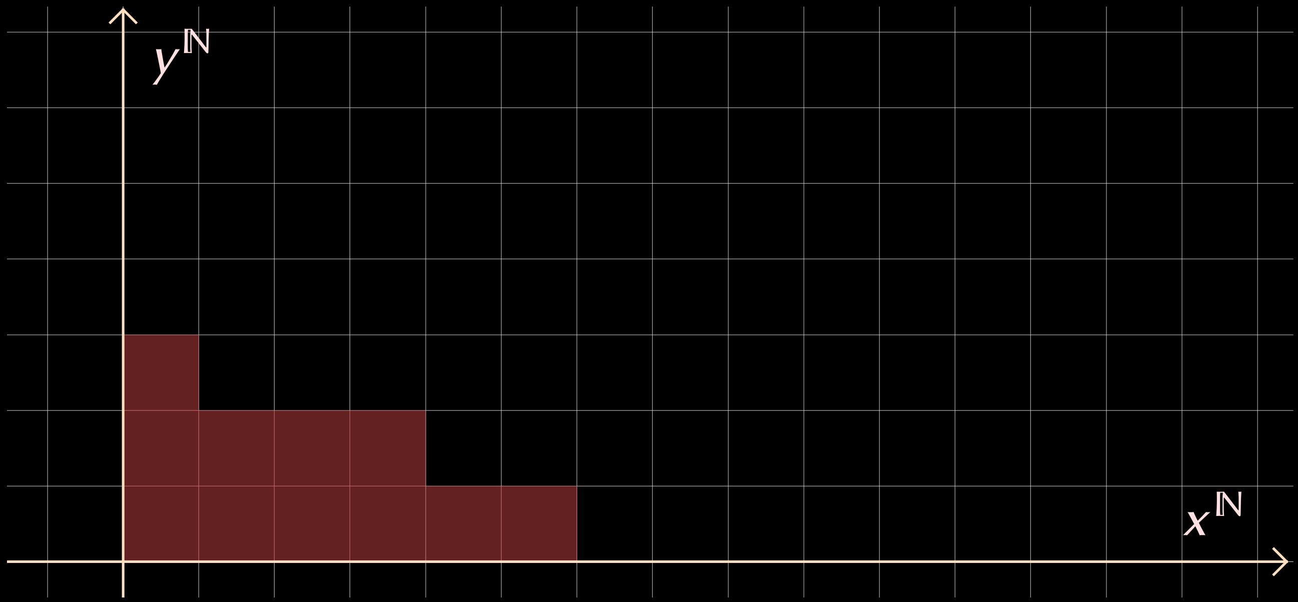
Gröbner basis for generic $\boldsymbol{\alpha}$



Gröbner basis of I_α for $\prec_k$

$$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$
$$I_{\boldsymbol{\alpha}} = \{P \in \mathbb{K}[x, y] : P(\boldsymbol{\alpha}) = 0\}$$

Gröbner basis for generic $\boldsymbol{\alpha}$

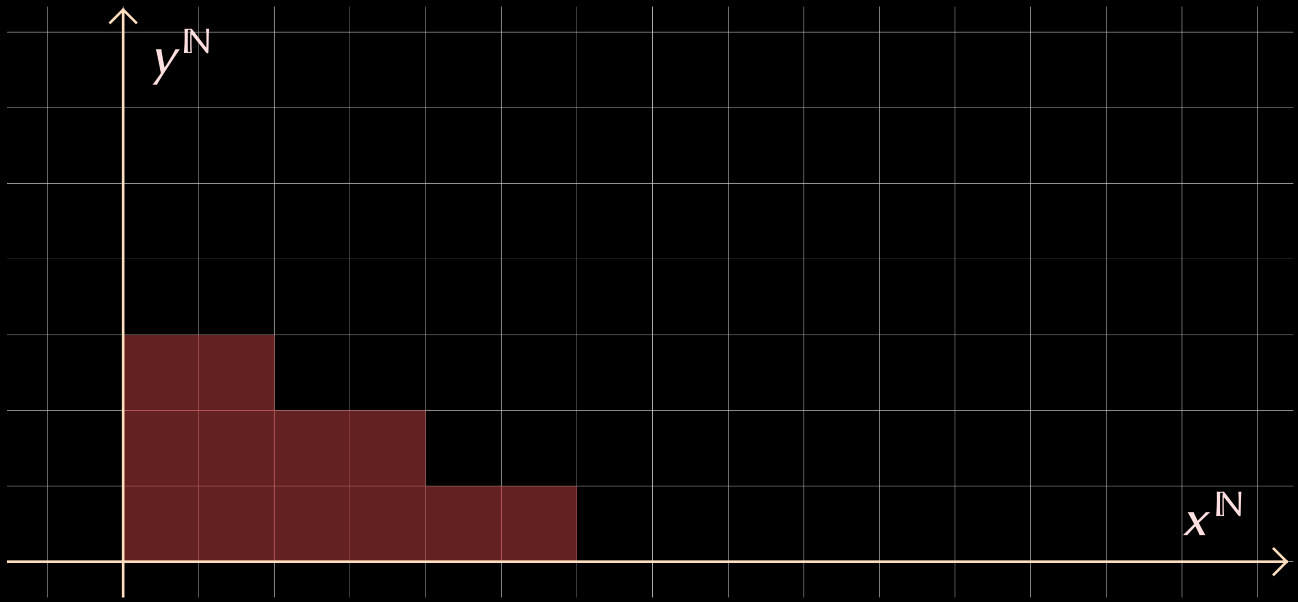


Gröbner basis of I_α for $<_k$

$$\boldsymbol{\alpha} \;==\; (\alpha_1, \ldots, \alpha_n) \;\in\; (\mathbb{K}^2)^n$$

$$I_\alpha \;==\; \{P \in \mathbb{K}[x,y] : P(\boldsymbol{\alpha}) = 0\}$$

Gröbner basis for generic $\boldsymbol{\alpha}$

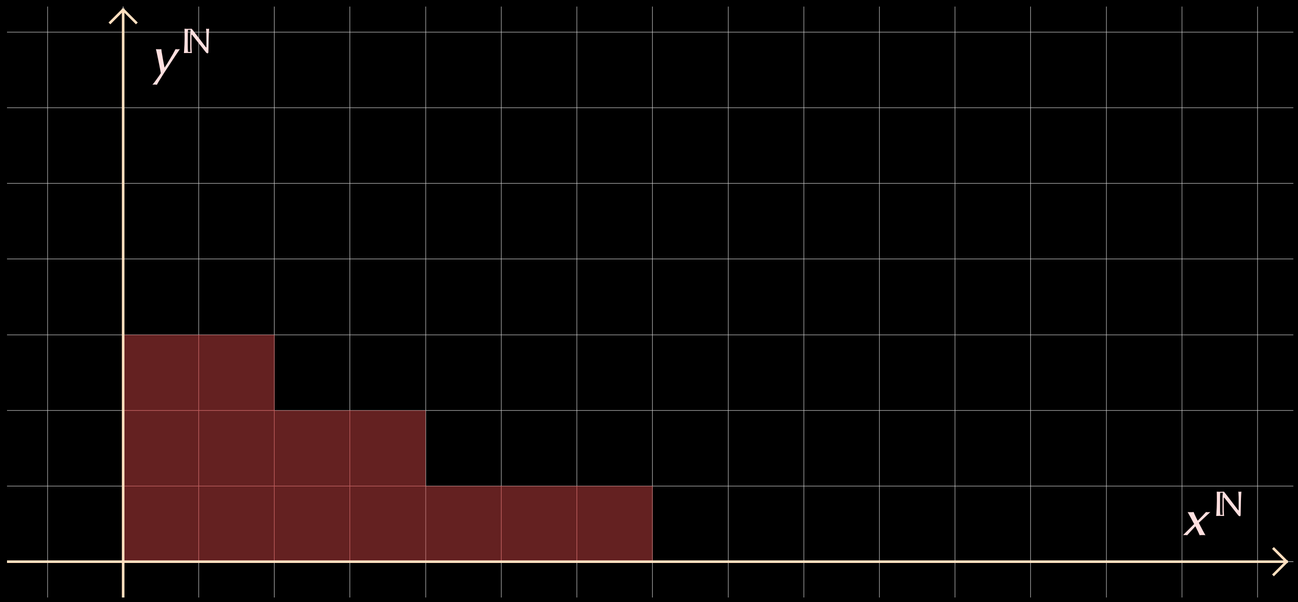


Gröbner basis of I_α for $\prec_k$

$$\boldsymbol{\alpha} \;=\!=\!=\; (\alpha_1, \ldots, \alpha_n) \;\in\; (\mathbb{K}^2)^n$$

$$I_\alpha \;=\!=\!=\; \{P \in \mathbb{K}[x, y] : P(\boldsymbol{\alpha}) = 0\}$$

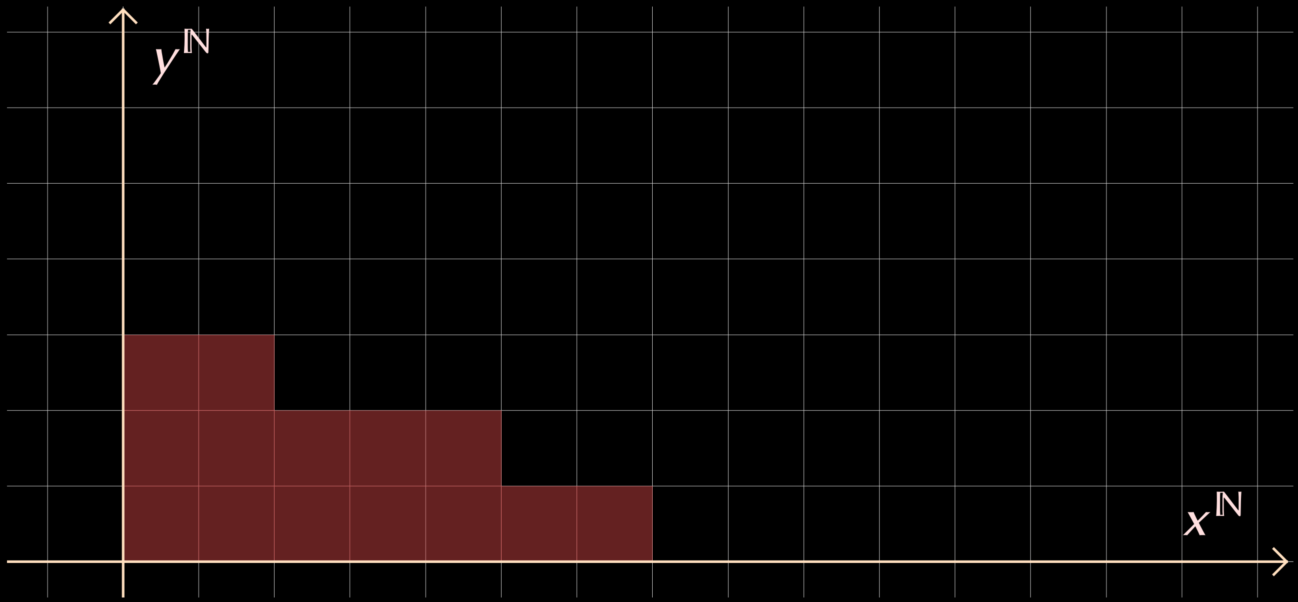
Gröbner basis for generic $\boldsymbol{\alpha}$



$$\boldsymbol{\alpha} \;=\!=\!=\; (\alpha_1, \ldots, \alpha_n) \;\in\; (\mathbb{K}^2)^n$$

$$I_\alpha \;=\!=\!=\; \{P \in \mathbb{K}[x,y] : P(\boldsymbol{\alpha}) = 0\}$$

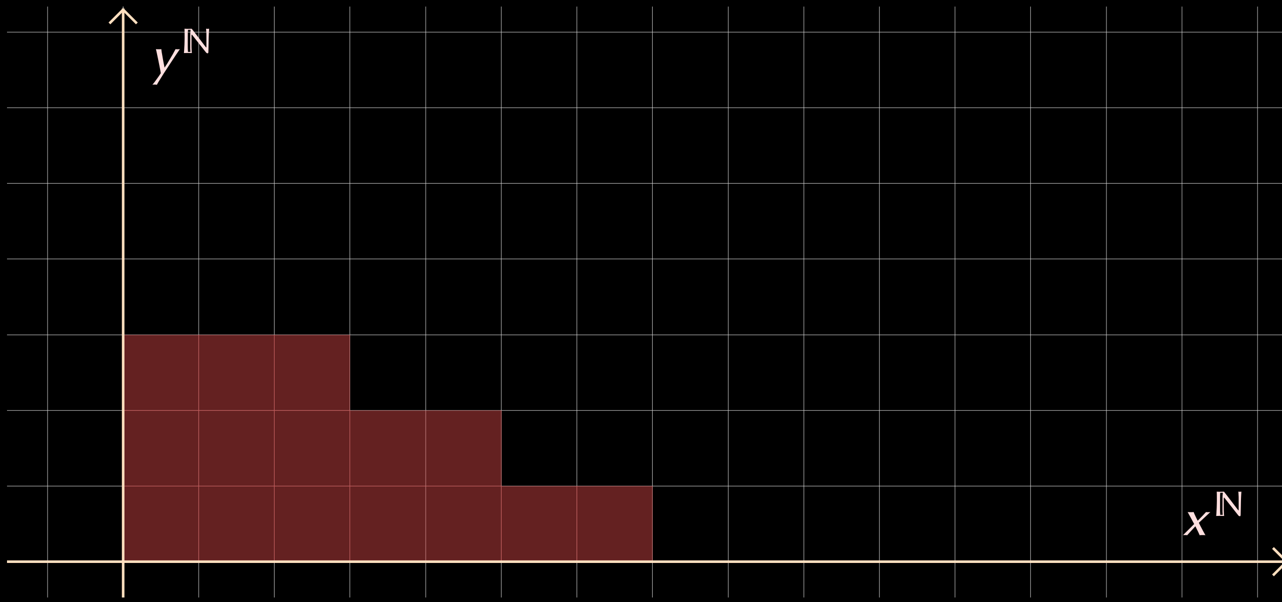
Gröbner basis for generic $\boldsymbol{\alpha}$



Gröbner basis of I_{α} for $<_k$

$$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$
$$I_{\boldsymbol{\alpha}} = \{P \in \mathbb{K}[x, y] : P(\boldsymbol{\alpha}) = 0\}$$

Gröbner basis for generic $\boldsymbol{\alpha}$

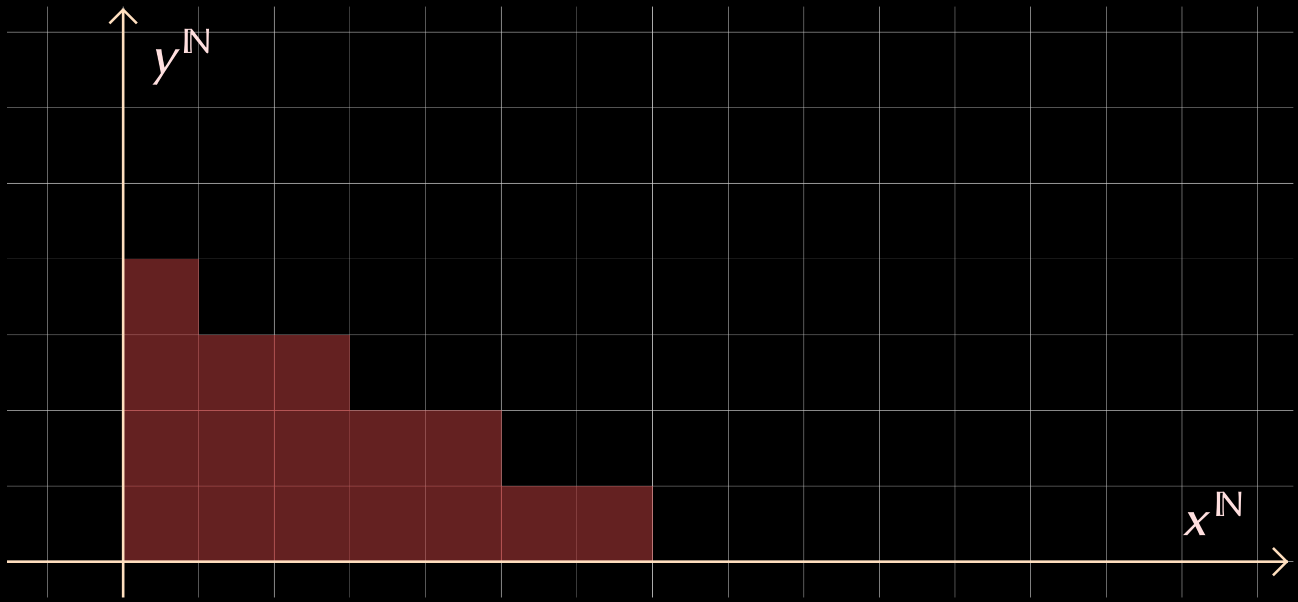


Gröbner basis of I_α for $<_k$

$$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$

$$I_\alpha = \{P \in \mathbb{K}[x, y] : P(\boldsymbol{\alpha}) = 0\}$$

Gröbner basis for generic $\boldsymbol{\alpha}$

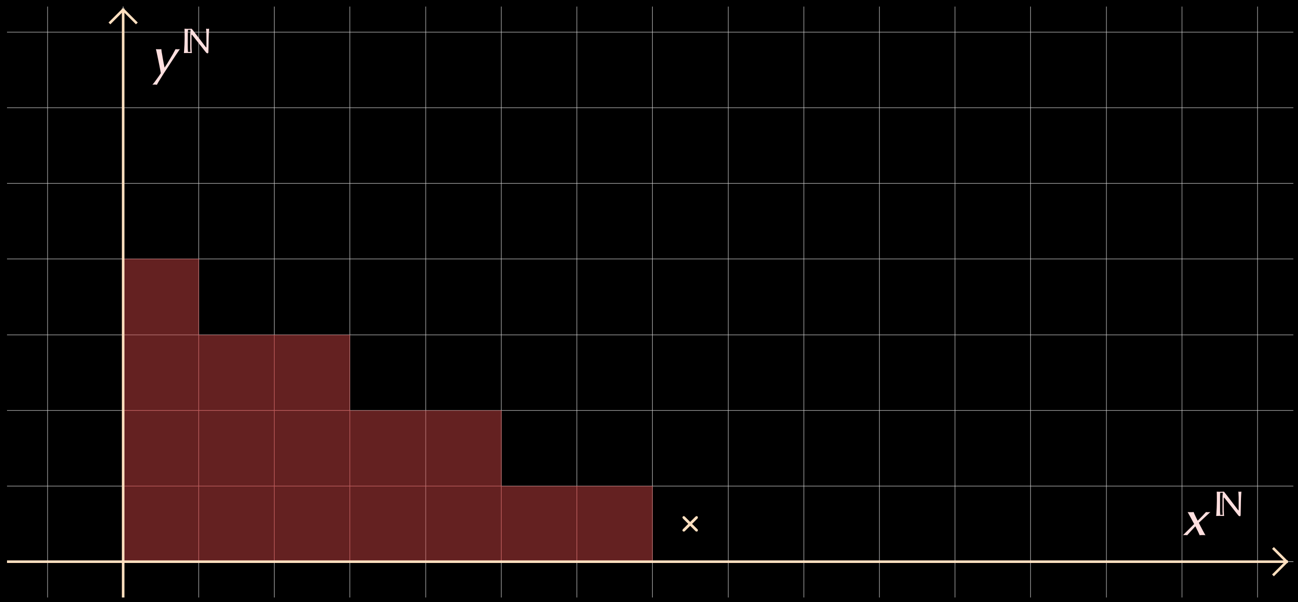


Gröbner basis of I_α for $<_k$

$$\boldsymbol{\alpha} \;=\!=\!=\; (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$

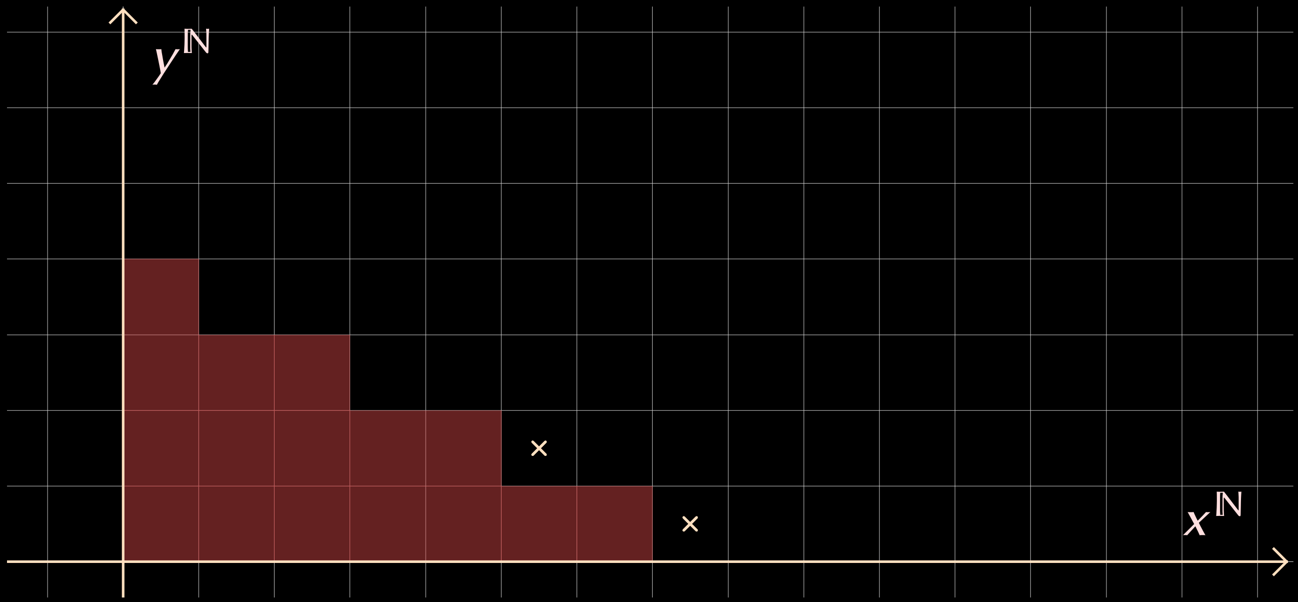
$$I_\alpha \;=\!=\!=\; \{P \in \mathbb{K}[x,y] : P(\boldsymbol{\alpha}) = 0\}$$

Gröbner basis for generic $\boldsymbol{\alpha}$



$$\boldsymbol{\alpha} \quad == \quad (\alpha_1, \ldots, \alpha_n) \ \in \ (\mathbb{K}^2)^n$$
$$I_\alpha \quad == \quad \{P \in \mathbb{K}[x,y] : P(\boldsymbol{\alpha}) = 0\}$$

Gröbner basis for generic $\boldsymbol{\alpha}$

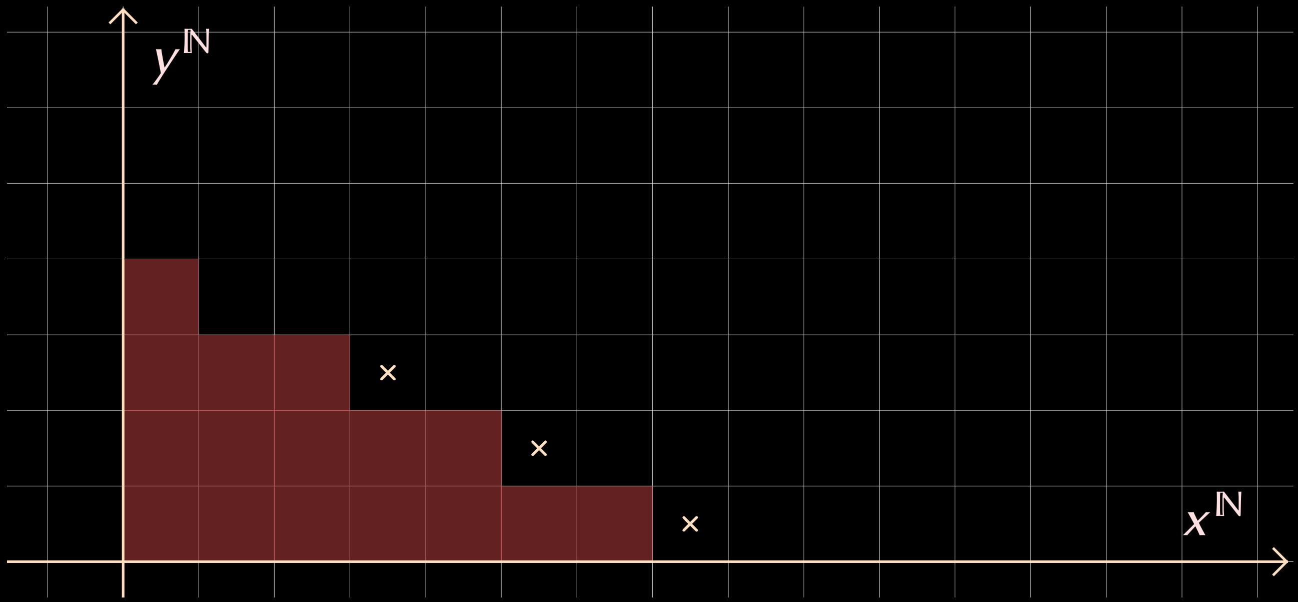


Gröbner basis of I_α for $<_k$

$$\boldsymbol{\alpha} \;=\!=\!=\; (\alpha_1, \ldots, \alpha_n) \;\in\; (\mathbb{K}^2)^n$$

$$I_\alpha \;=\!=\!=\; \{P \in \mathbb{K}[x, y] : P(\boldsymbol{\alpha}) = 0\}$$

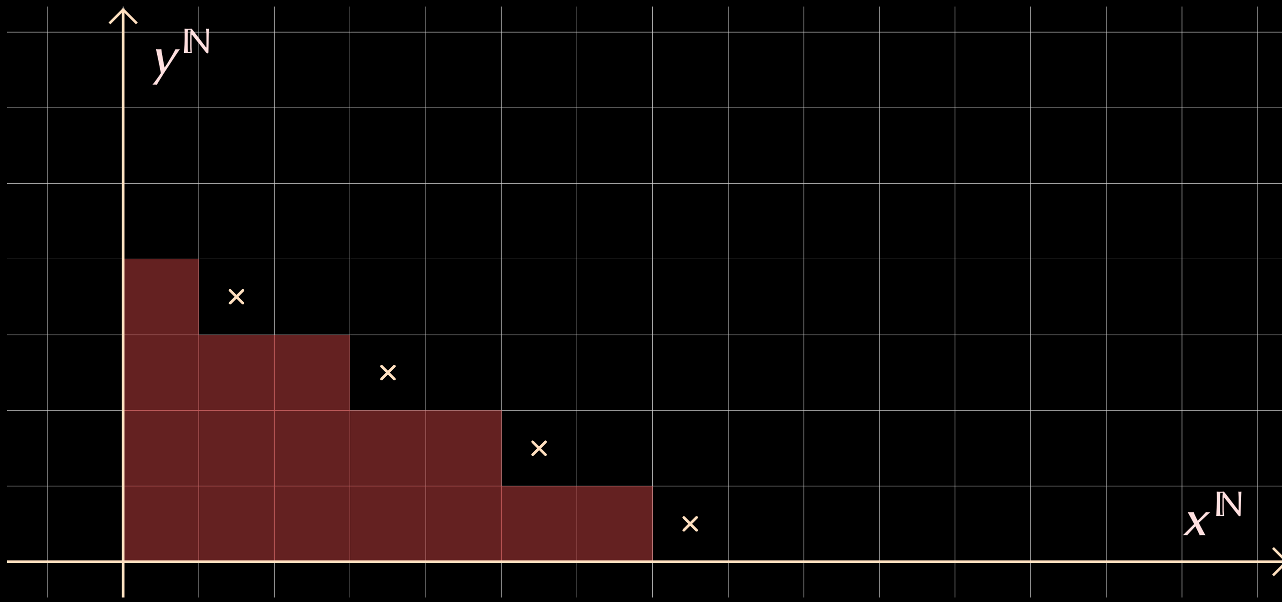
Gröbner basis for generic $\boldsymbol{\alpha}$



Gröbner basis of I_α for $<_k$

$$\boldsymbol{\alpha} \;=\!=\; (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$
$$I_\alpha \;=\!=\; \{P \in \mathbb{K}[x, y] : P(\boldsymbol{\alpha}) = 0\}$$

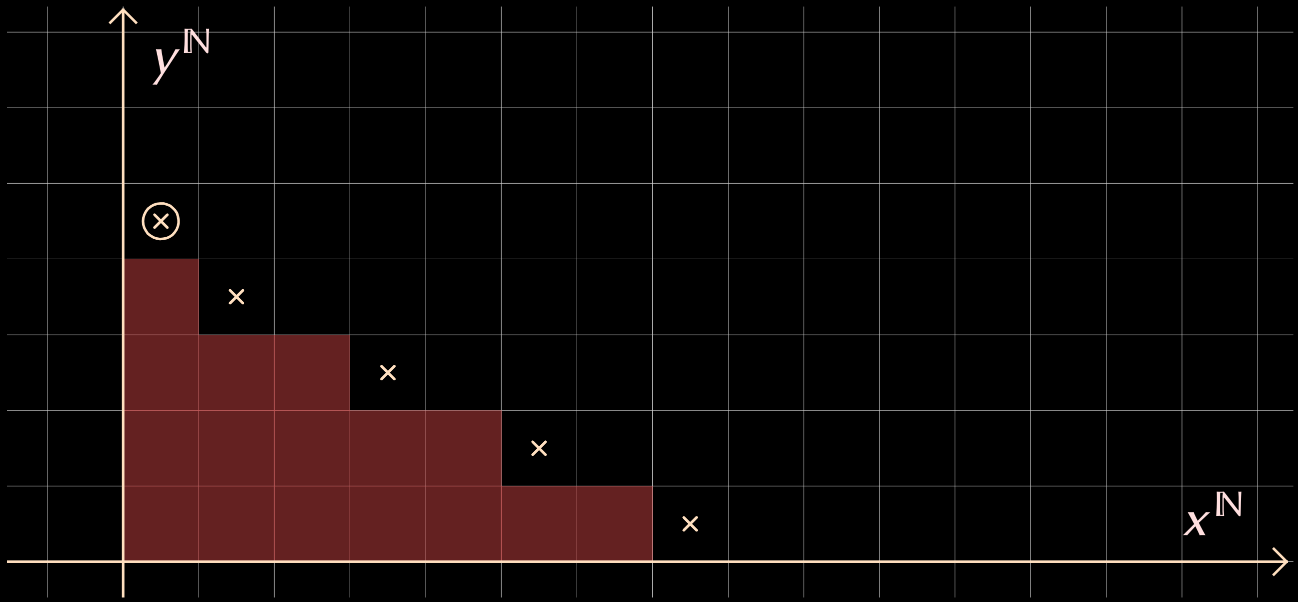
Gröbner basis for generic $\boldsymbol{\alpha}$



Gröbner basis of I_α for $<_k$

$$\boldsymbol{\alpha} \;==\; (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$
$$I_\alpha \;==\; \{P \in \mathbb{K}[x,y] : P(\boldsymbol{\alpha}) = 0\}$$

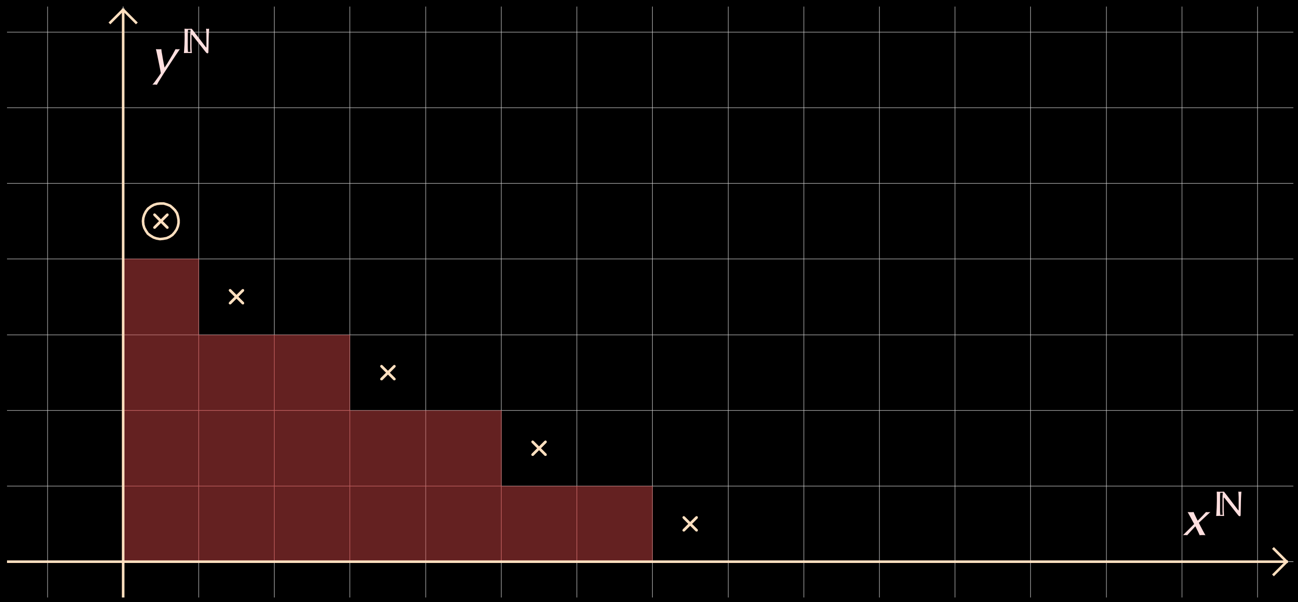
Gröbner basis for generic $\boldsymbol{\alpha}$



Gröbner basis of I_α for $<_k$

$$\boldsymbol{\alpha} \Longleftarrow (\alpha_1, \ldots, \alpha_n) \in (\mathbb{K}^2)^n$$
$$I_\alpha \Longleftarrow \{P \in \mathbb{K}[x, y] : P(\boldsymbol{\alpha}) = 0\}$$

Gröbner basis for generic $\boldsymbol{\alpha}$



$\exists B_k \in I_\alpha, \quad \mathrm{LM}(B_k) = y^b, \quad b \leqslant \sqrt{\frac{2n}{k}}$

Amortized multi-point evaluation, generic case

vdH–Larrieu 2018: dichotomic Gröbner walk w.r.t. $\prec_1, \prec_2, \prec_4, \prec_8, \ldots$

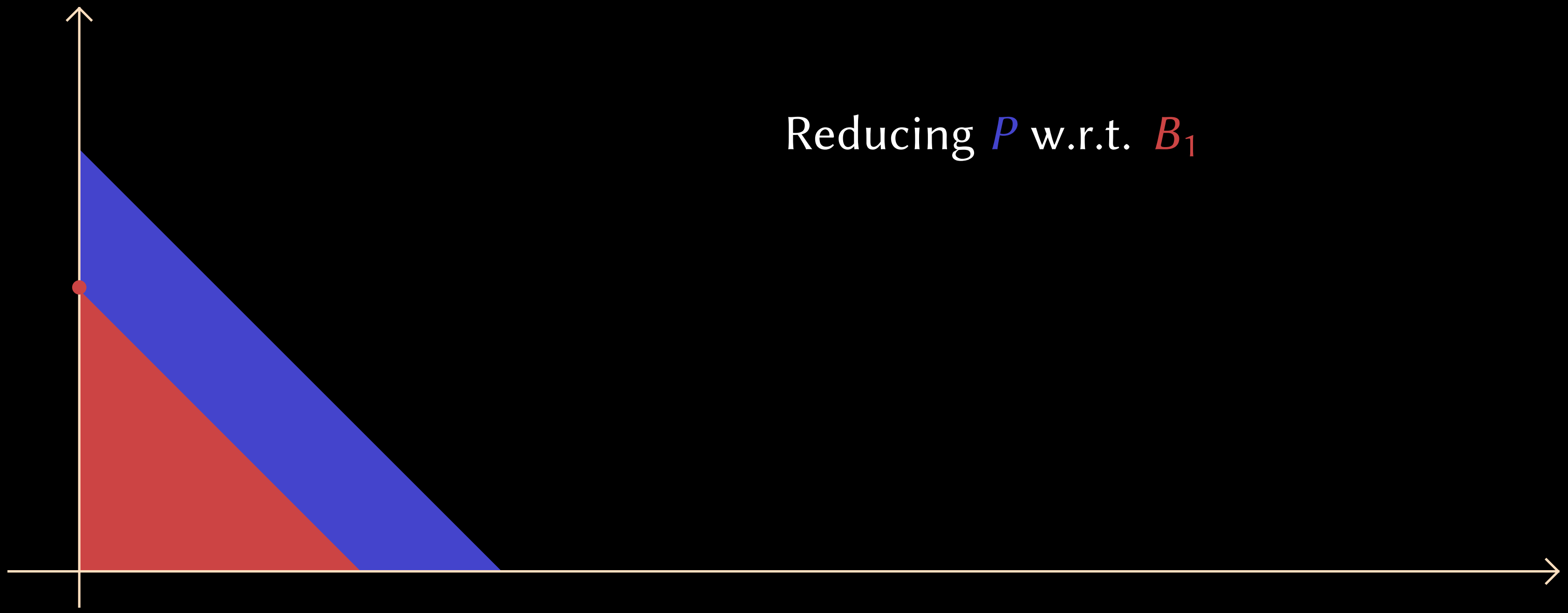
Amortized multi-point evaluation, generic case

vdH–Larrieu 2018: dichotomic Gröbner walk w.r.t. $\prec_1, \prec_2, \prec_4, \prec_8, \ldots$

Neiger–Rosenkilde–Solomatov: reduce w.r.t. $B_1, B_2, B_4, B_8, \ldots$

vdH–Larrieu 2018: dichotomic Gröbner walk w.r.t. $\prec_1, \prec_2, \prec_4, \prec_8, \ldots$

Neiger–Rosenkilde–Solomatov: reduce w.r.t. $B_1, B_2, B_4, B_8, \ldots$

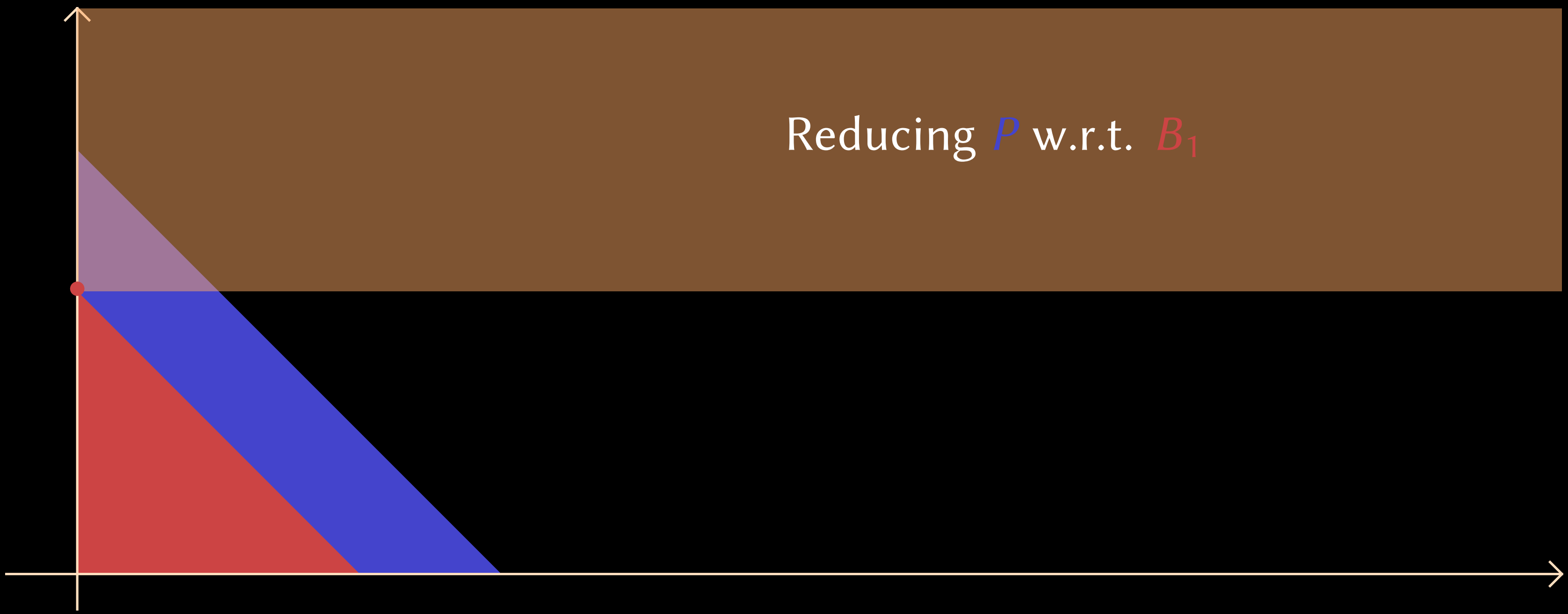


Reducing P w.r.t. B_1

Amortized multi-point evaluation, generic case

vdH–Larrieu 2018: dichotomic Gröbner walk w.r.t. $\prec_1, \prec_2, \prec_4, \prec_8, \ldots$

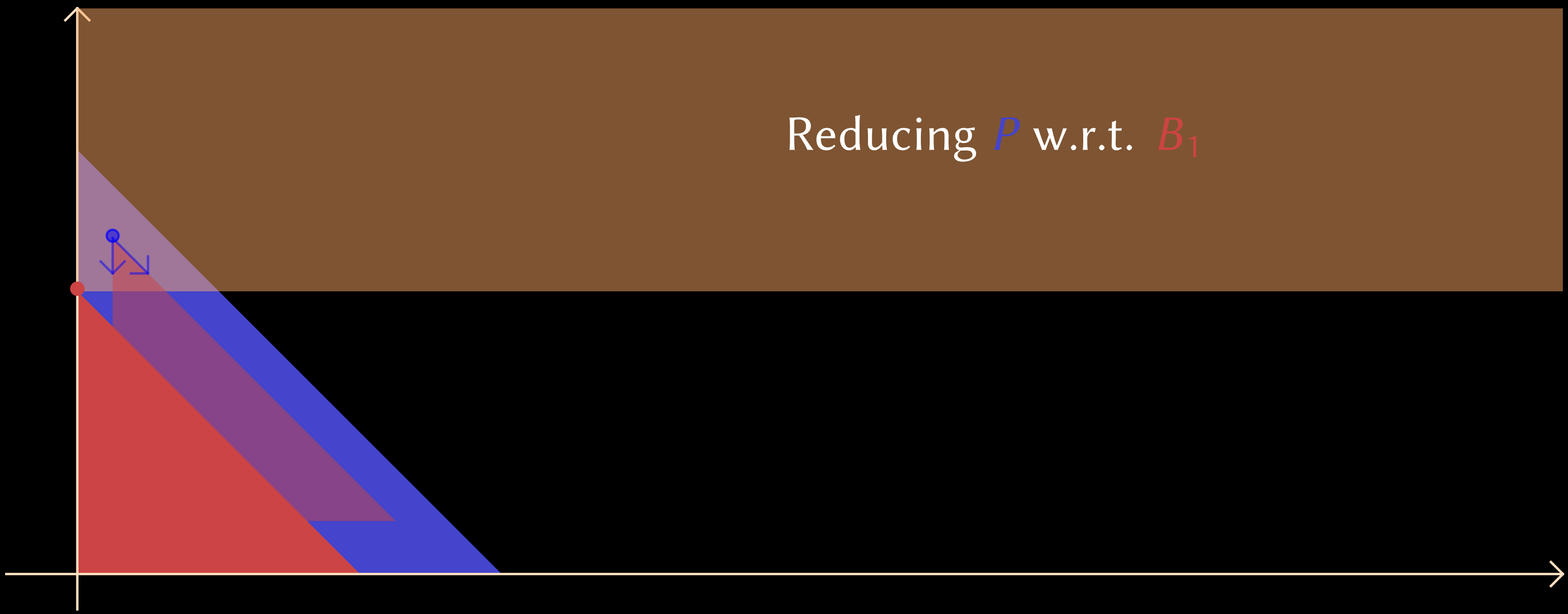
Neiger–Rosenkilde–Solomatov: reduce w.r.t. $B_1, B_2, B_4, B_8, \ldots$



Amortized multi-point evaluation, generic case

vdH–Larrieu 2018: dichotomic Gröbner walk w.r.t. $\prec_1, \prec_2, \prec_4, \prec_8, \ldots$

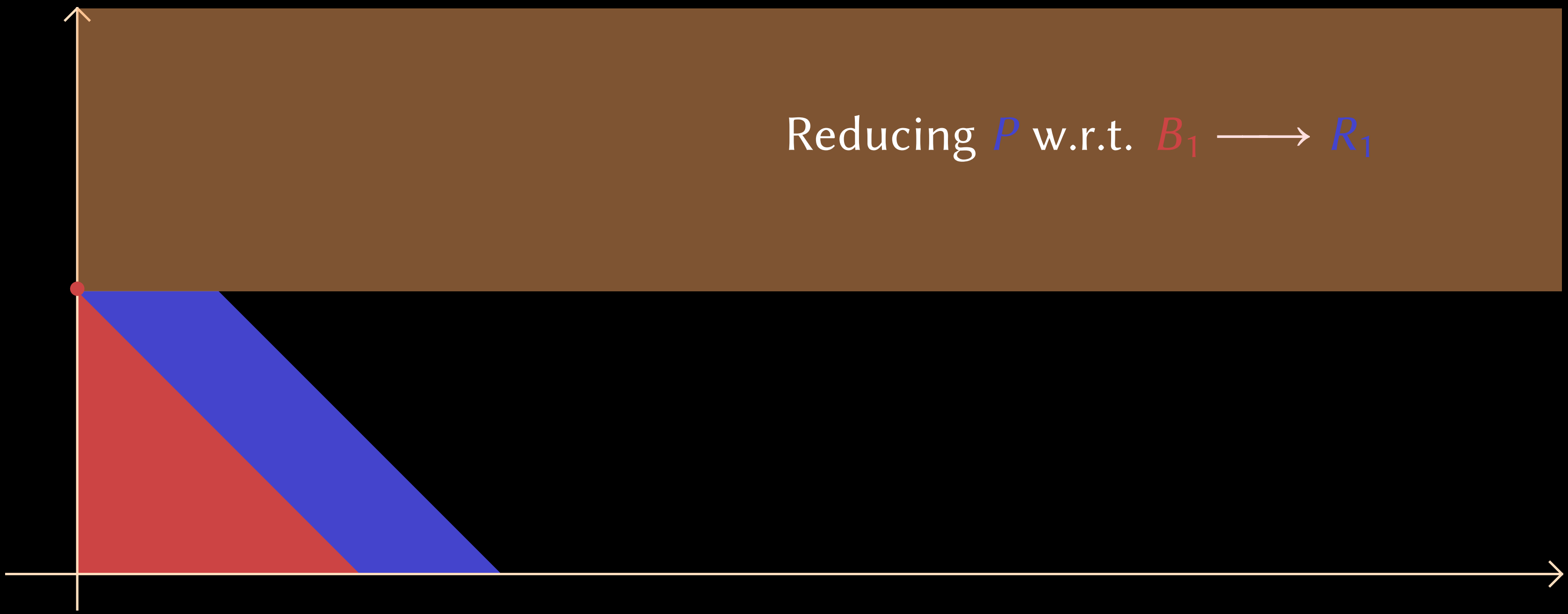
Neiger–Rosenkilde–Solomatov: reduce w.r.t. $B_1, B_2, B_4, B_8, \ldots$



Amortized multi-point evaluation, generic case

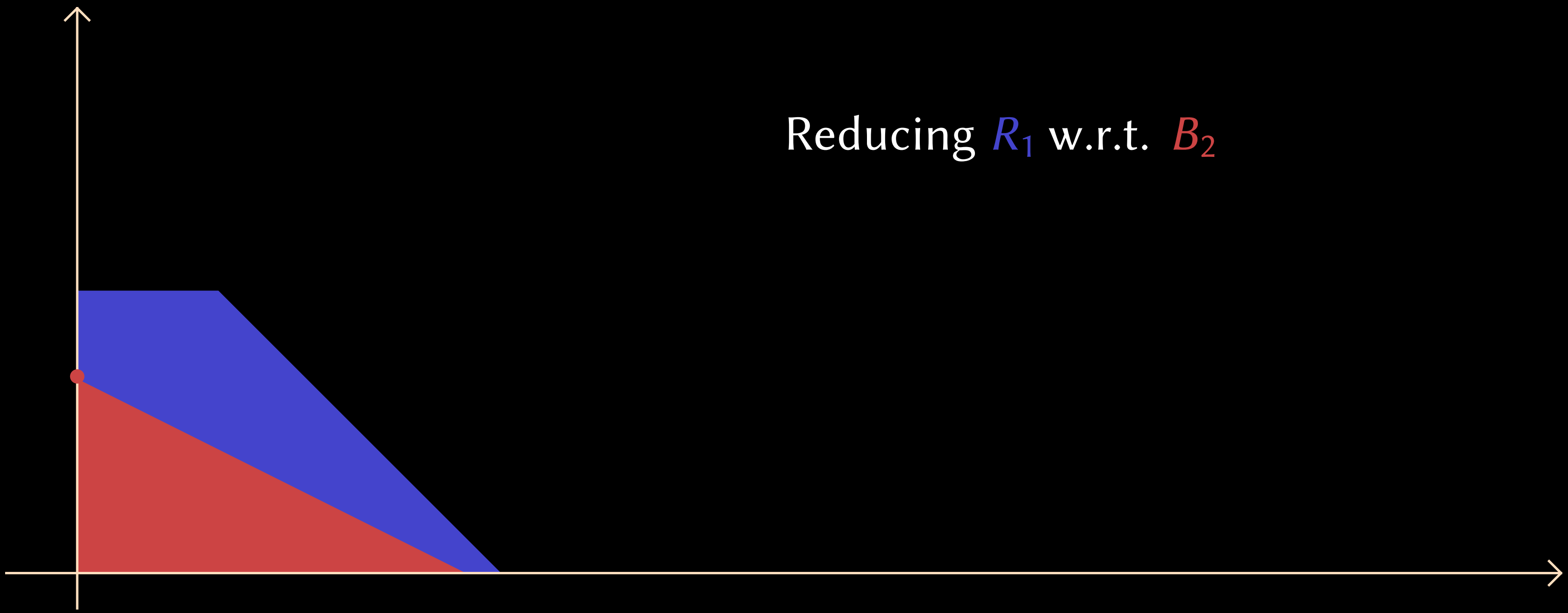
vdH–Larrieu 2018: dichotomic Gröbner walk w.r.t. $\prec_1, \prec_2, \prec_4, \prec_8, \ldots$

Neiger–Rosenkilde–Solomatov: reduce w.r.t. $B_1, B_2, B_4, B_8, \ldots$



vdH–Larrieu 2018: dichotomic Gröbner walk w.r.t. $\prec_1, \prec_2, \prec_4, \prec_8, \ldots$

Neiger–Rosenkilde–Solomatov: reduce w.r.t. $B_1, B_2, B_4, B_8, \ldots$

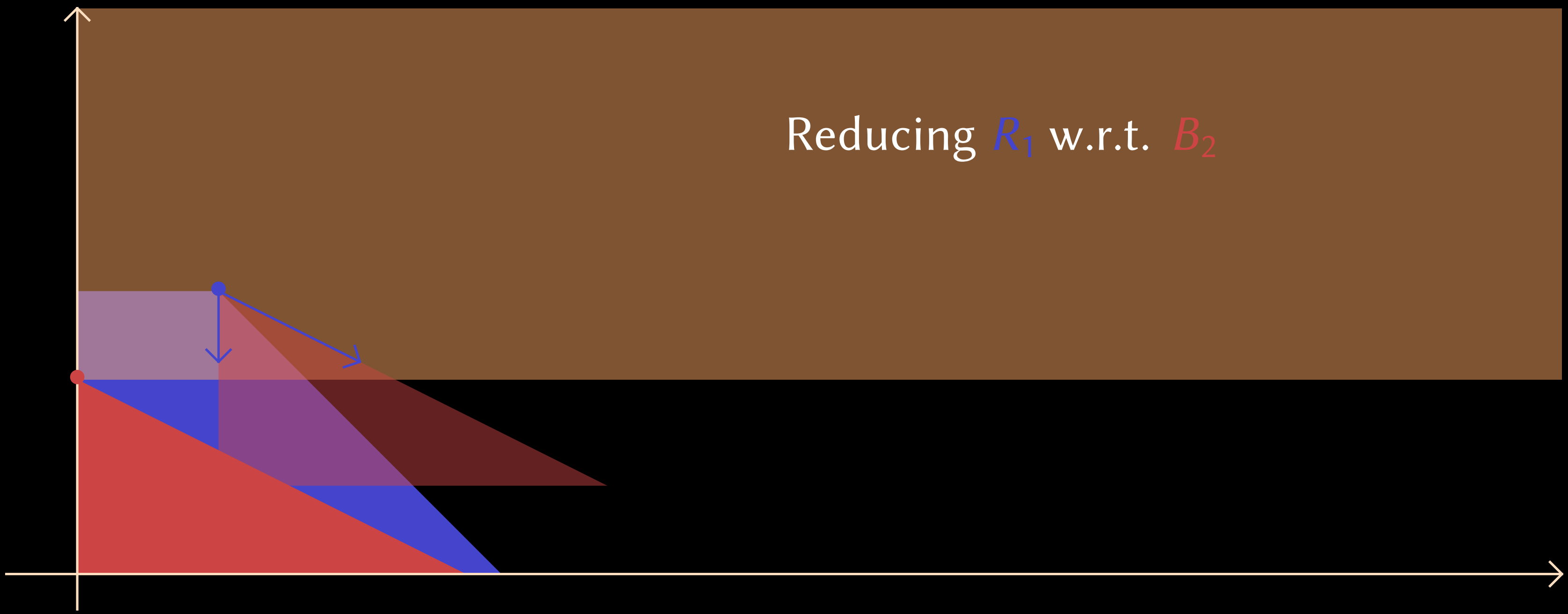


Reducing R_1 w.r.t. B_2

Amortized multi-point evaluation, generic case

vdH–Larrieu 2018: dichotomic Gröbner walk w.r.t. $\prec_1, \prec_2, \prec_4, \prec_8, \ldots$

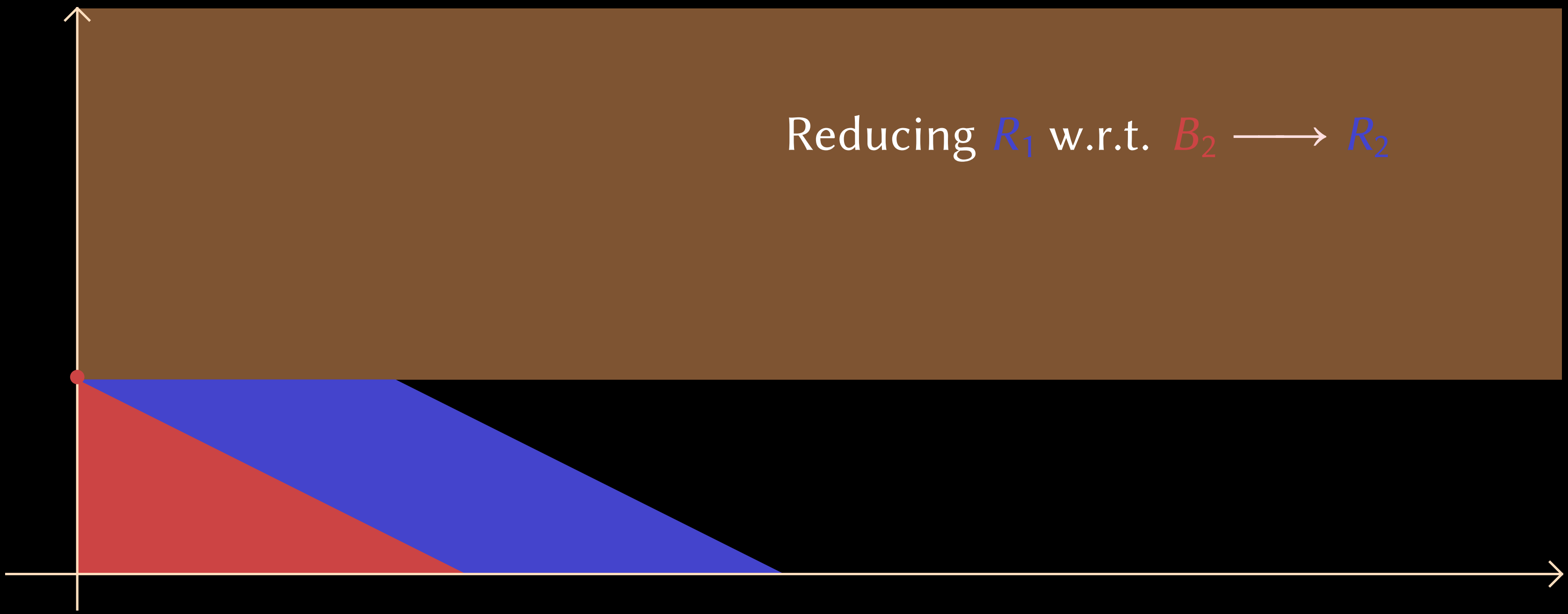
Neiger–Rosenkilde–Solomatov: reduce w.r.t. $B_1, B_2, B_4, B_8, \ldots$



Amortized multi-point evaluation, generic case

vdH–Larrieu 2018: dichotomic Gröbner walk w.r.t. $\prec_1, \prec_2, \prec_4, \prec_8, \ldots$

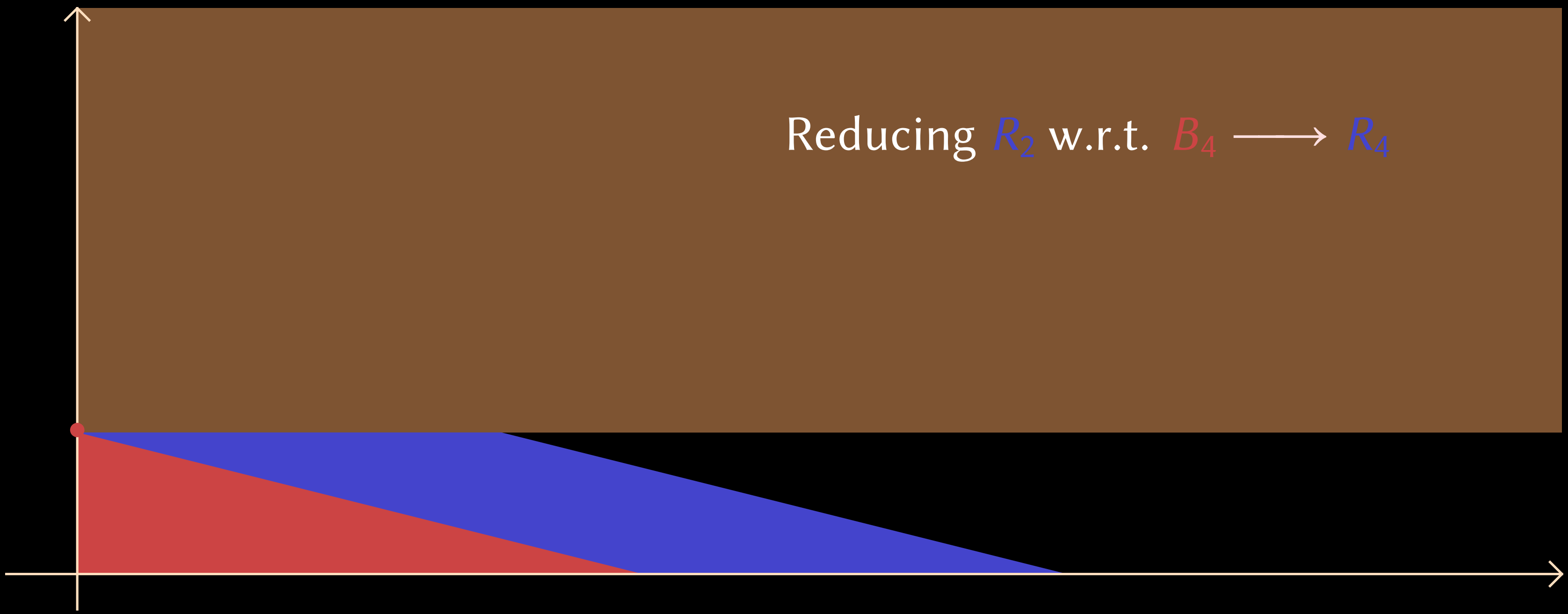
Neiger–Rosenkilde–Solomatov: reduce w.r.t. $B_1, B_2, B_4, B_8, \ldots$



Amortized multi-point evaluation, generic case

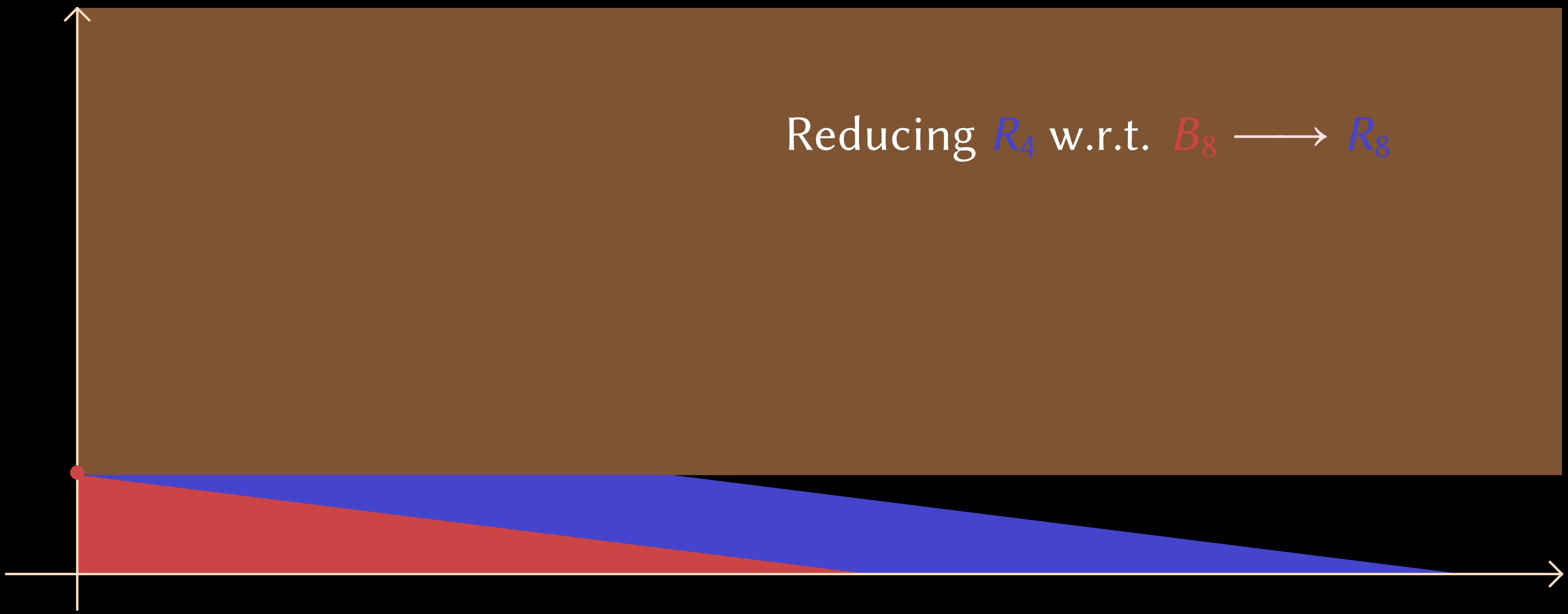
vdH–Larrieu 2018: dichotomic Gröbner walk w.r.t. $\prec_1, \prec_2, \prec_4, \prec_8, \ldots$

Neiger–Rosenkilde–Solomatov: reduce w.r.t. $B_1, B_2, B_4, B_8, \ldots$



vdH–Larrieu 2018: dichotomic Gröbner walk w.r.t. $\prec_1, \prec_2, \prec_4, \prec_8, \ldots$

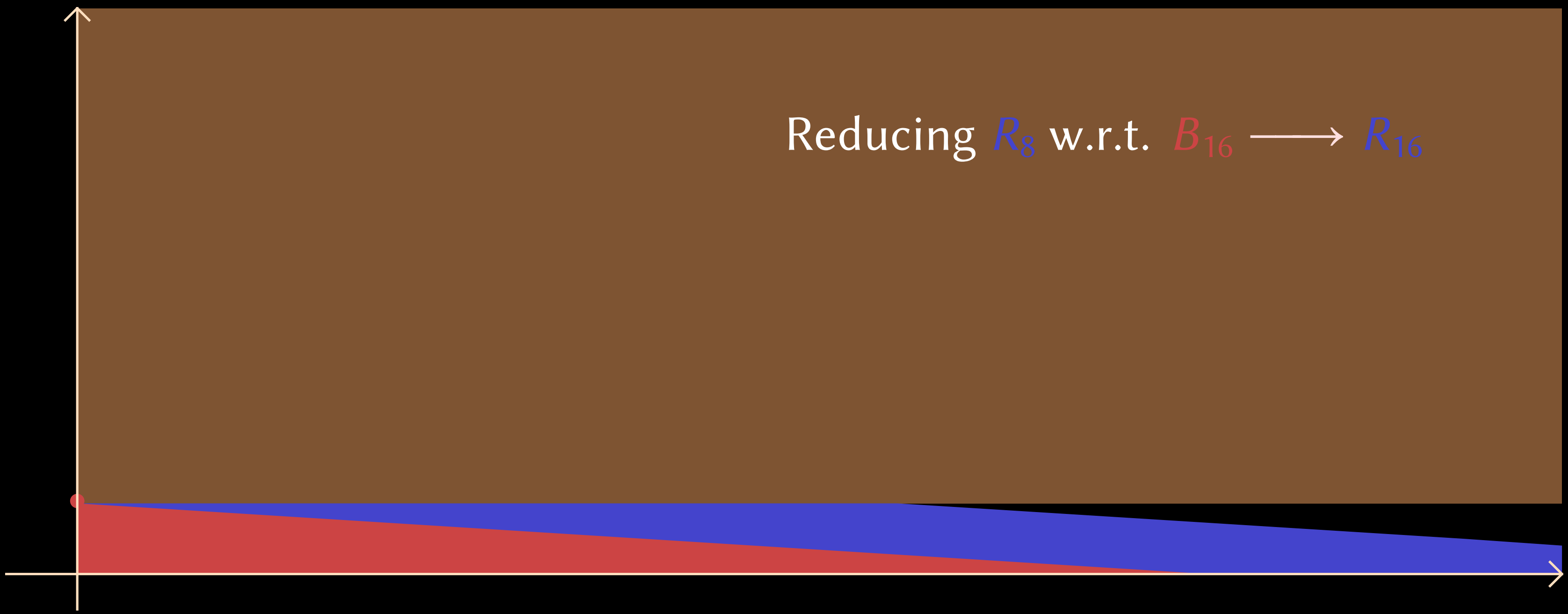
Neiger–Rosenkilde–Solomatov: reduce w.r.t. $B_1, B_2, B_4, B_8, \ldots$



Amortized multi-point evaluation, generic case

vdH–Larrieu 2018: dichotomic Gröbner walk w.r.t. $\prec_1, \prec_2, \prec_4, \prec_8, \ldots$

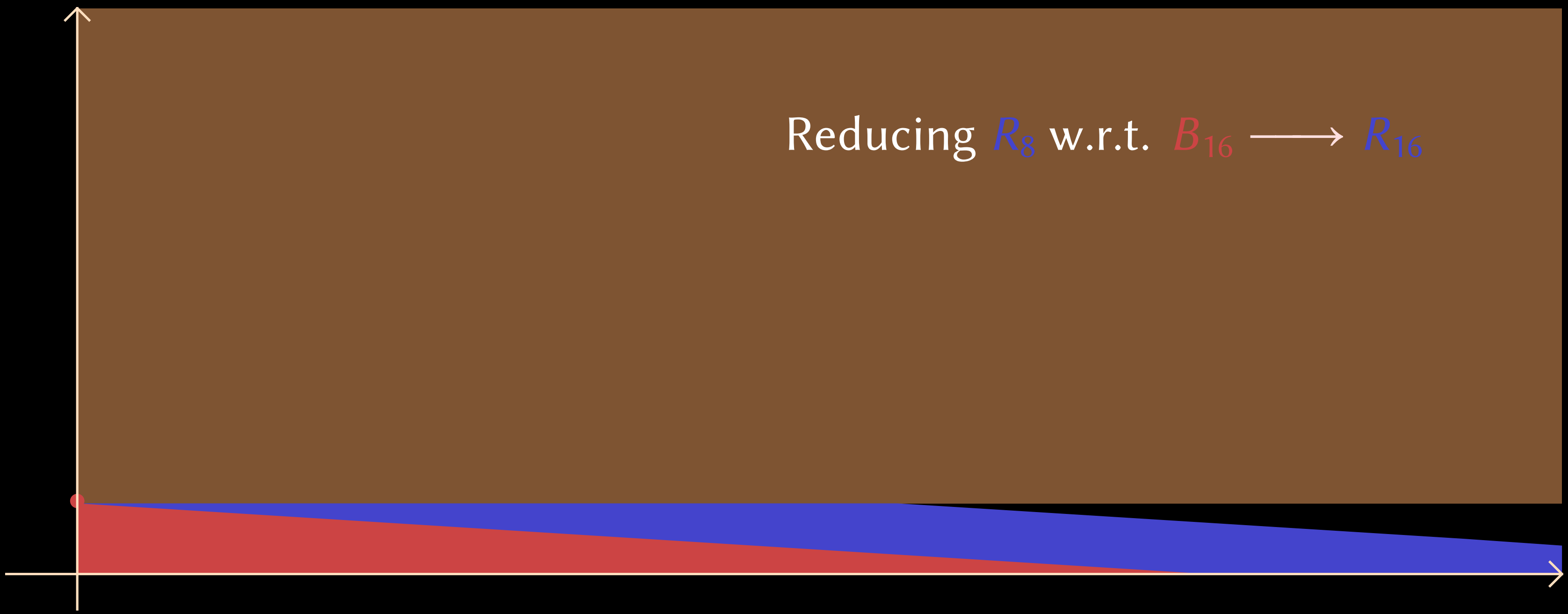
Neiger–Rosenkilde–Solomatov: reduce w.r.t. $B_1, B_2, B_4, B_8, \ldots$



Amortized multi-point evaluation, generic case

vdH–Larrieu 2018: dichotomic Gröbner walk w.r.t. $\prec_1, \prec_2, \prec_4, \prec_8, \ldots$

Neiger–Rosenkilde–Solomatov: reduce w.r.t. $B_1, B_2, B_4, B_8, \ldots$

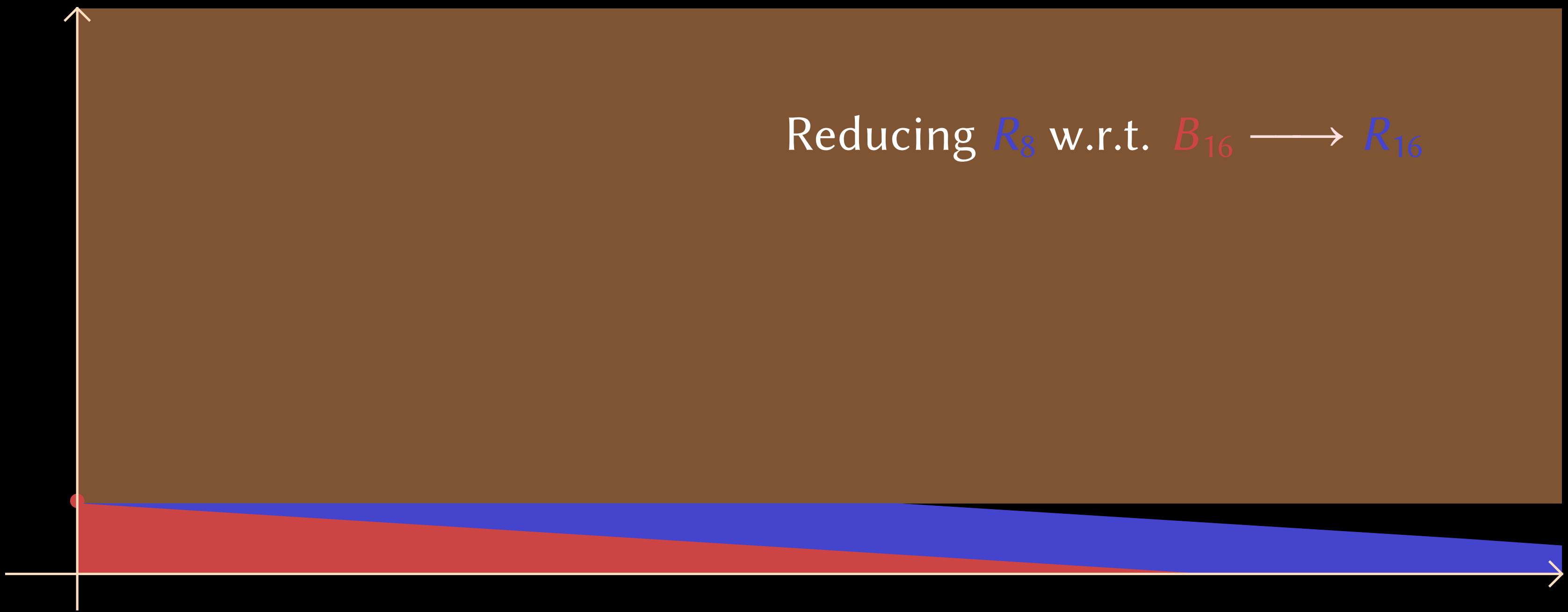


Result: $R = (((P \operatorname{rem} B_1) \operatorname{rem} B_2) \operatorname{rem} B_4) \operatorname{rem} \cdots \in \mathbb{K}[x]$ with $R - P \in I_\alpha$

Amortized multi-point evaluation, generic case

vdH–Larrieu 2018: dichotomic Gröbner walk w.r.t. $\prec_1, \prec_2, \prec_4, \prec_8, \ldots$

Neiger–Rosenkilde–Solomatov: reduce w.r.t. $B_1, B_2, B_4, B_8, \ldots$



Result: $R = (((P \operatorname{rem} B_1) \operatorname{rem} B_2) \operatorname{rem} B_4) \operatorname{rem} \cdots \in \mathbb{K}[x]$ with $R - P \in I_\alpha$

Conclusion: reduction to univariate multi-point evaluation of R

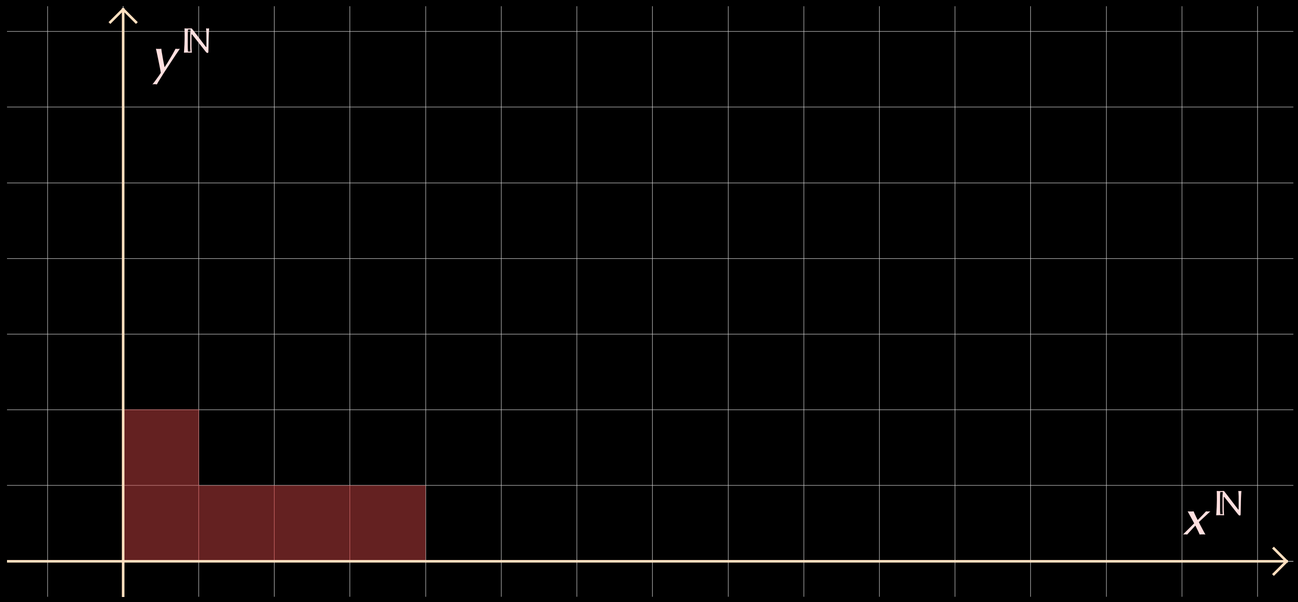
Gröbner basis, non-generic case

Gröbner basis, non-generic case

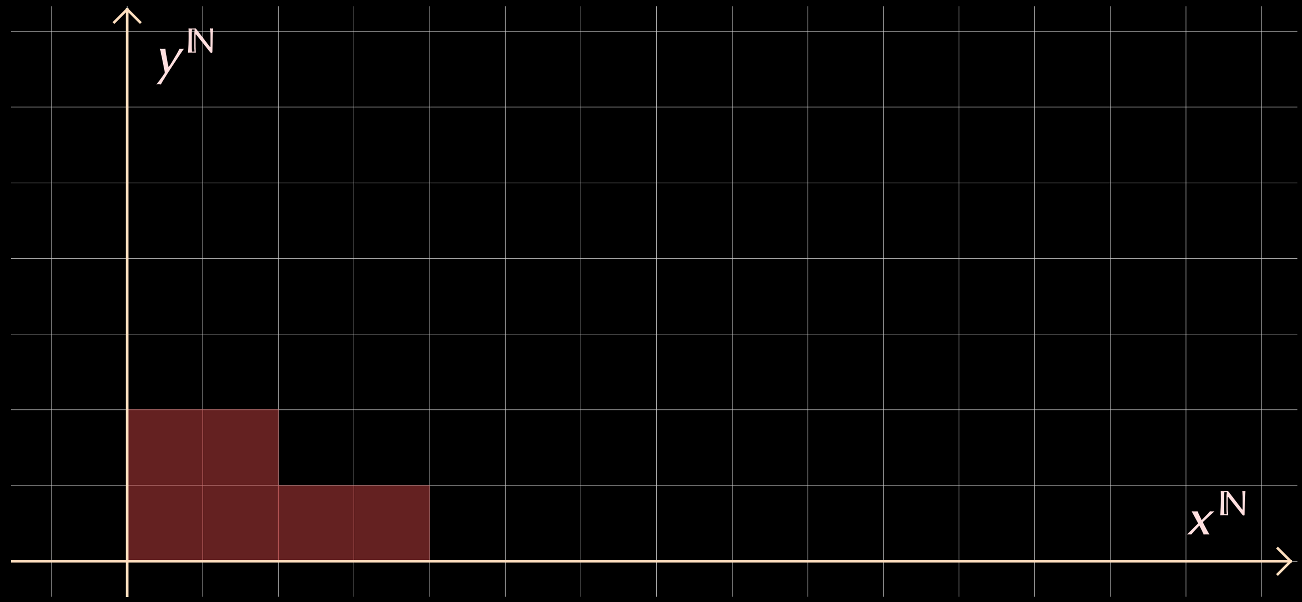
Gröbner basis, non-generic case

Gröbner basis, non-generic case

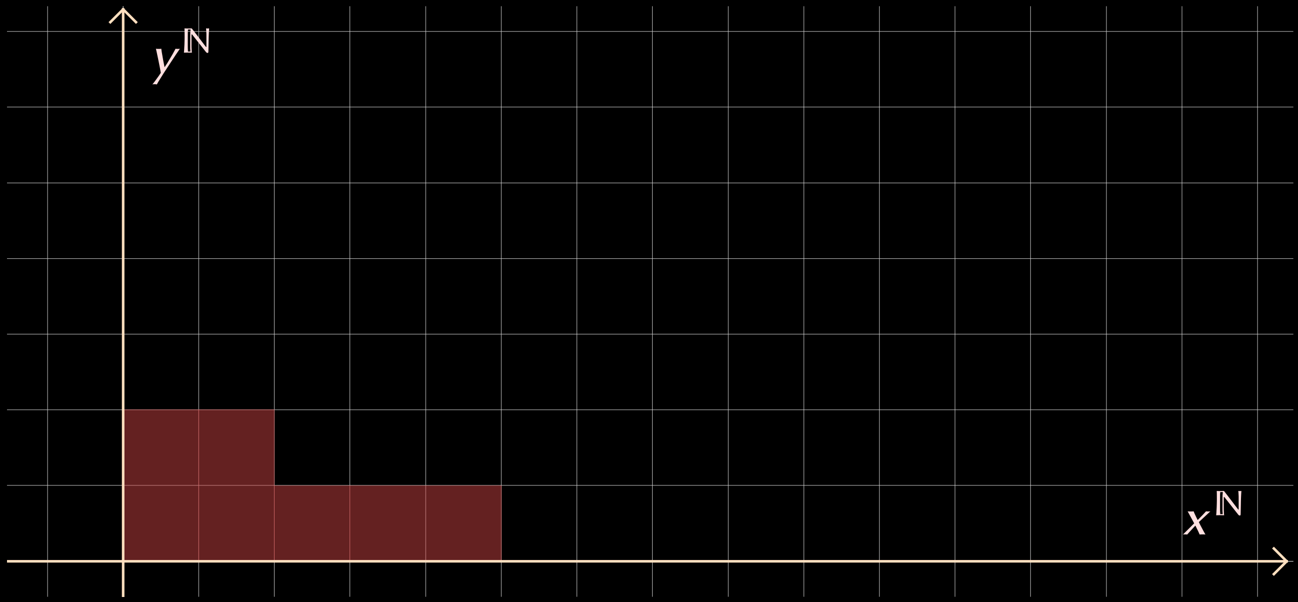
Gröbner basis, non-generic case



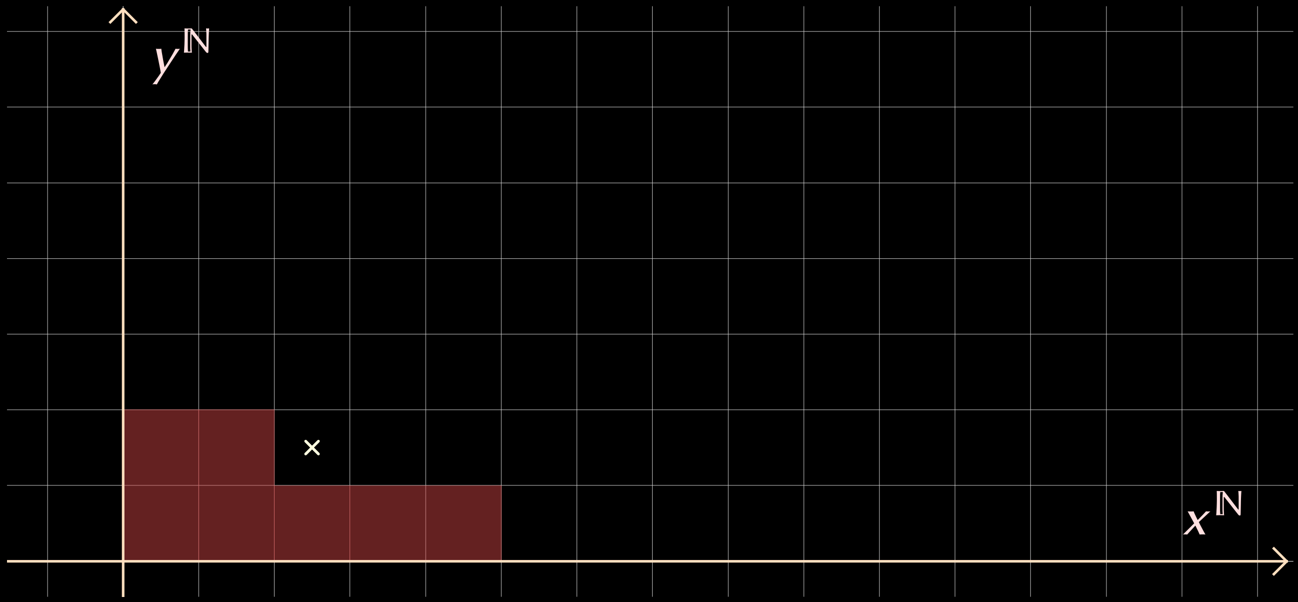
Gröbner basis, non-generic case



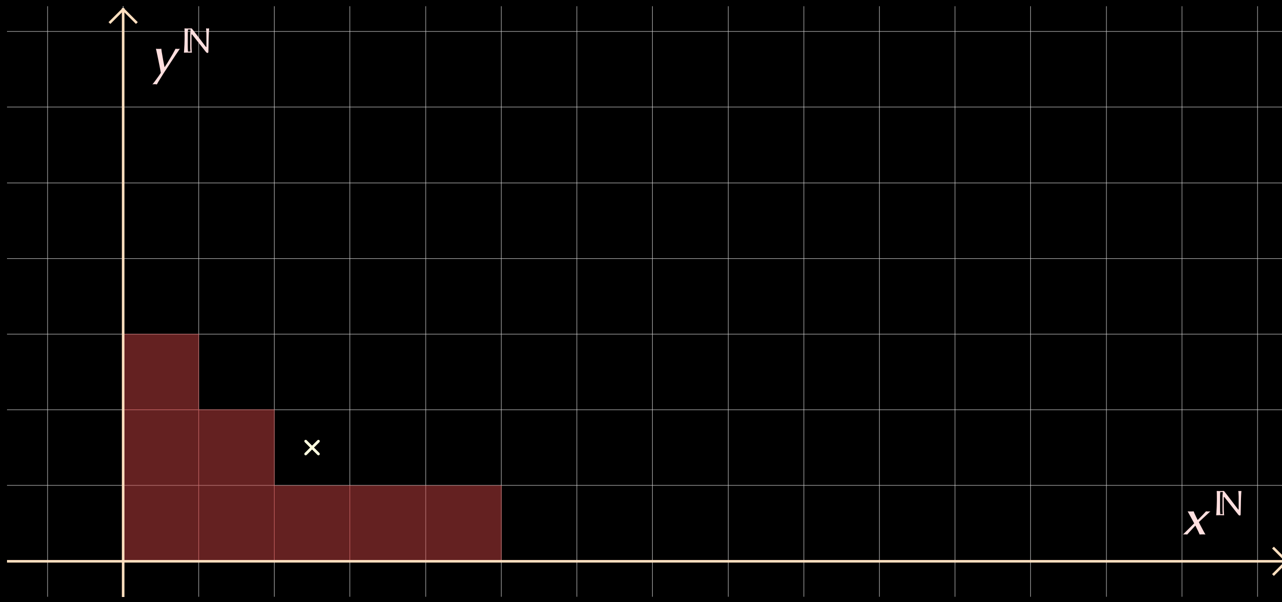
Gröbner basis, non-generic case



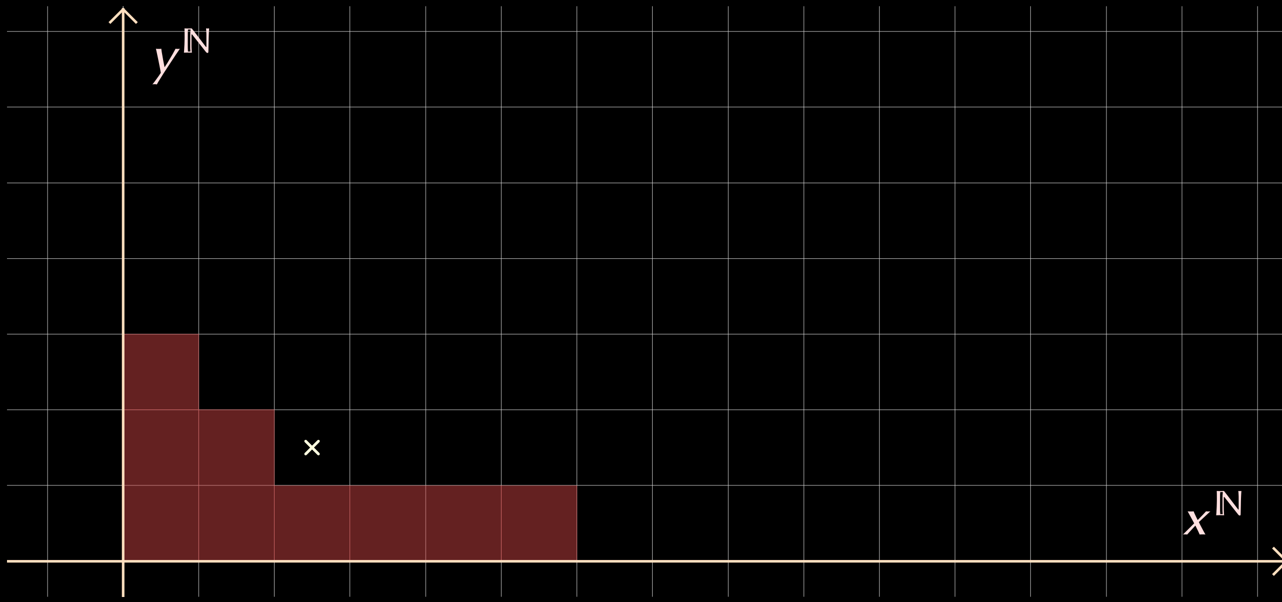
Gröbner basis, non-generic case



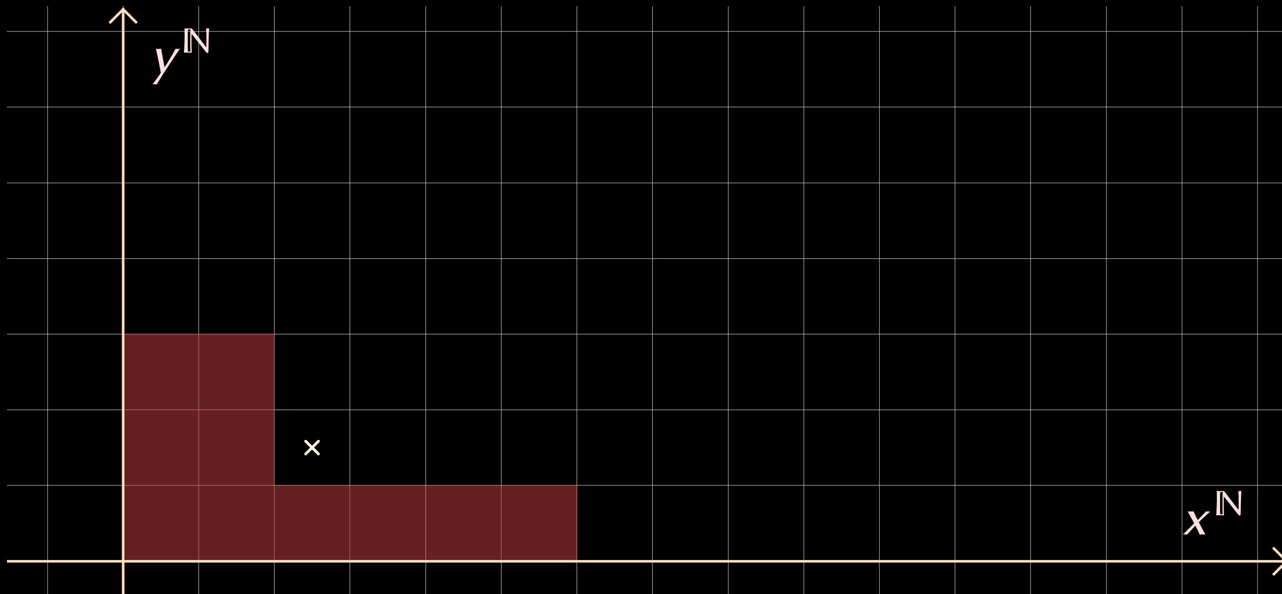
Gröbner basis, non-generic case



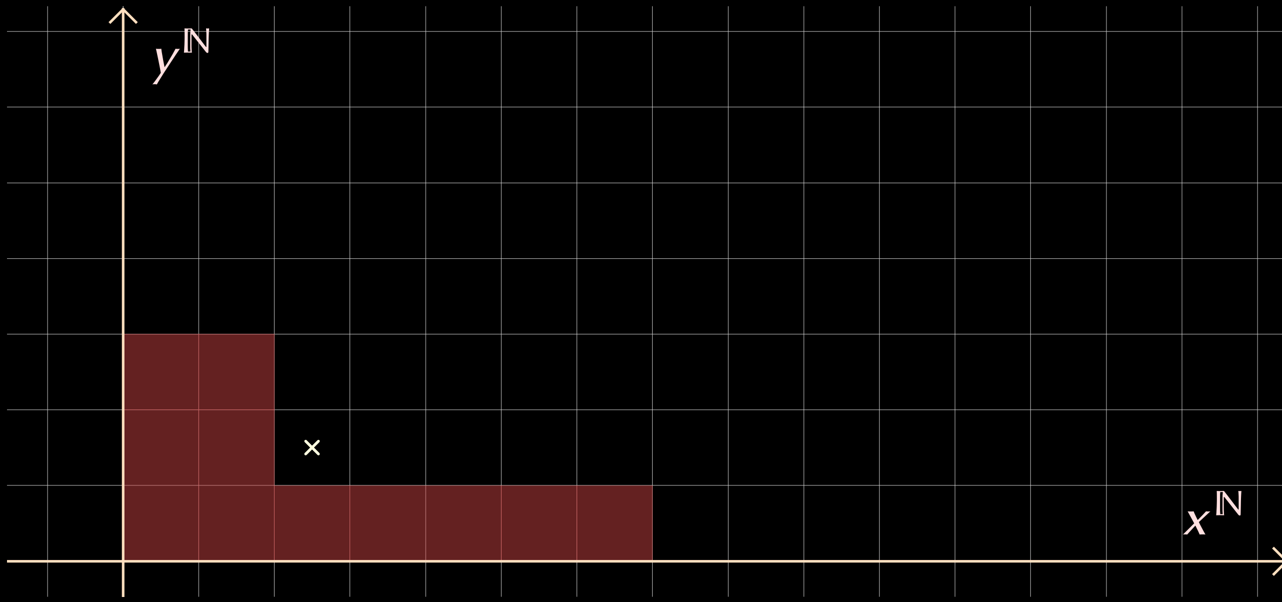
Gröbner basis, non-generic case



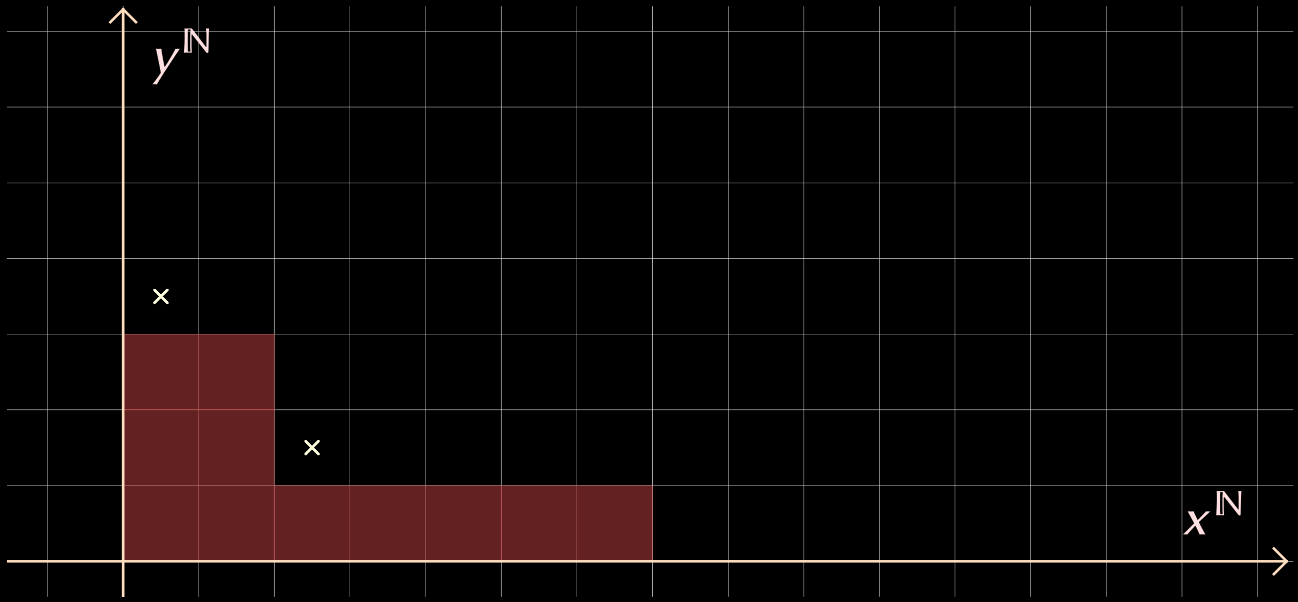
Gröbner basis, non-generic case



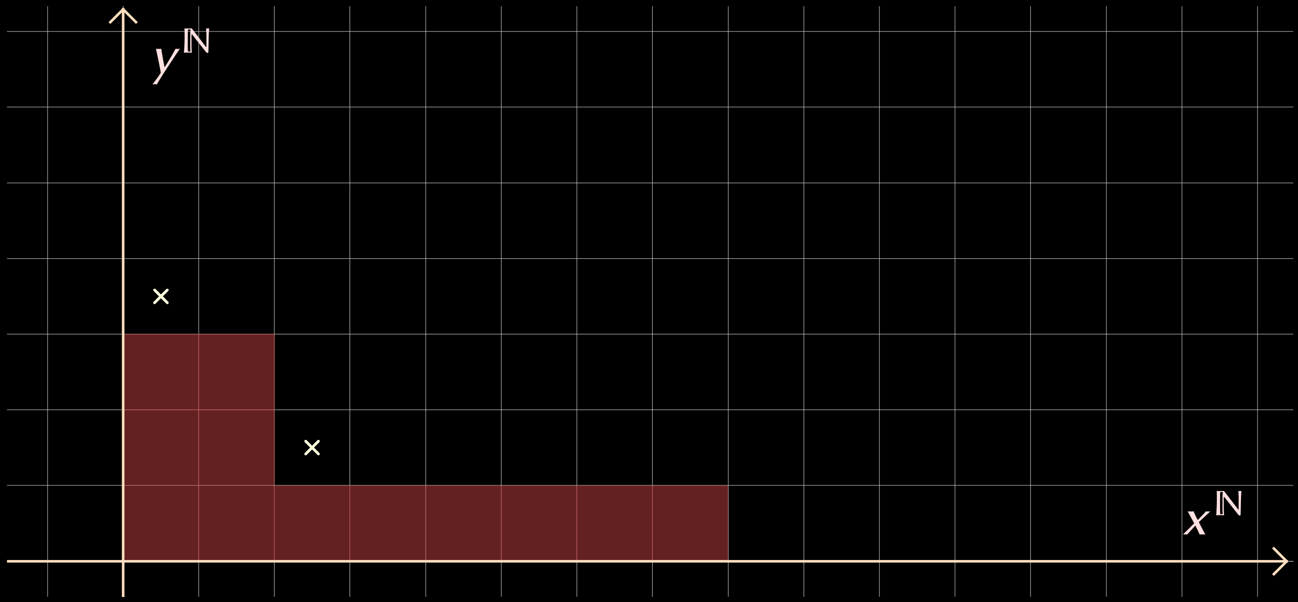
Gröbner basis, non-generic case



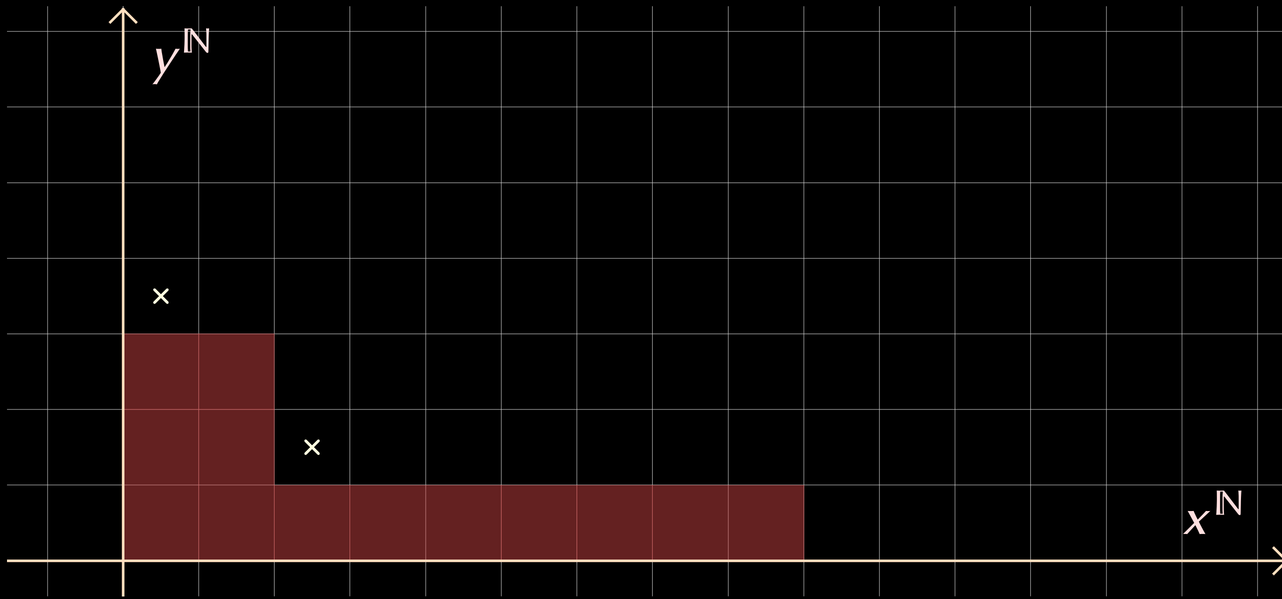
Gröbner basis, non-generic case



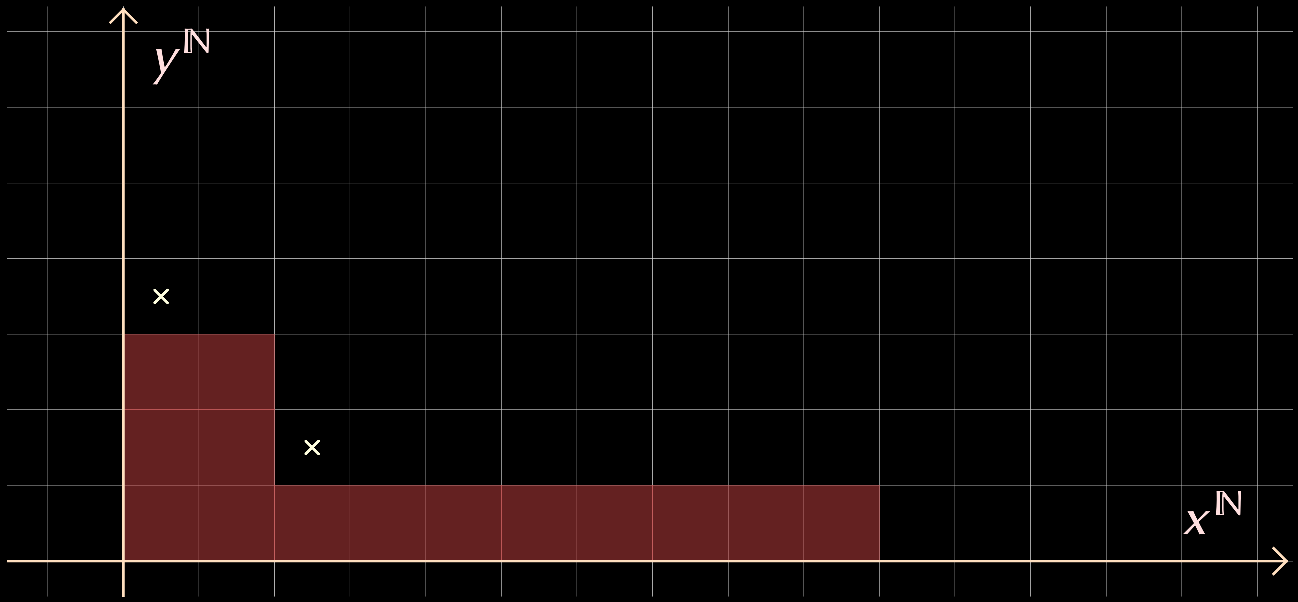
Gröbner basis, non-generic case



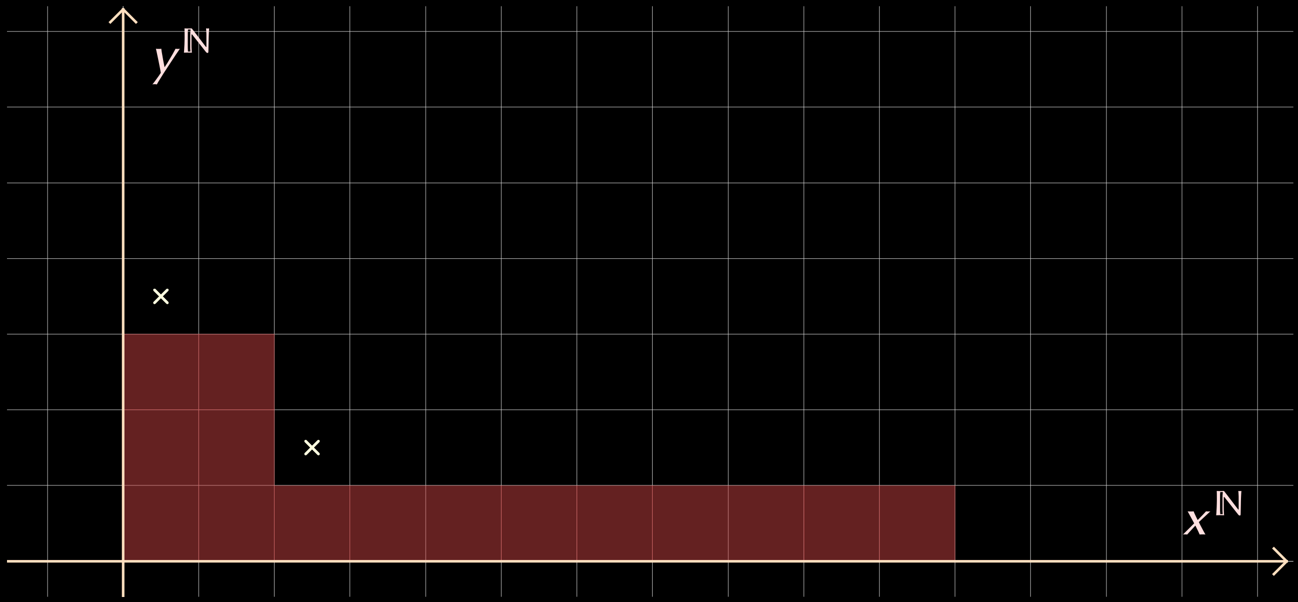
Gröbner basis, non-generic case



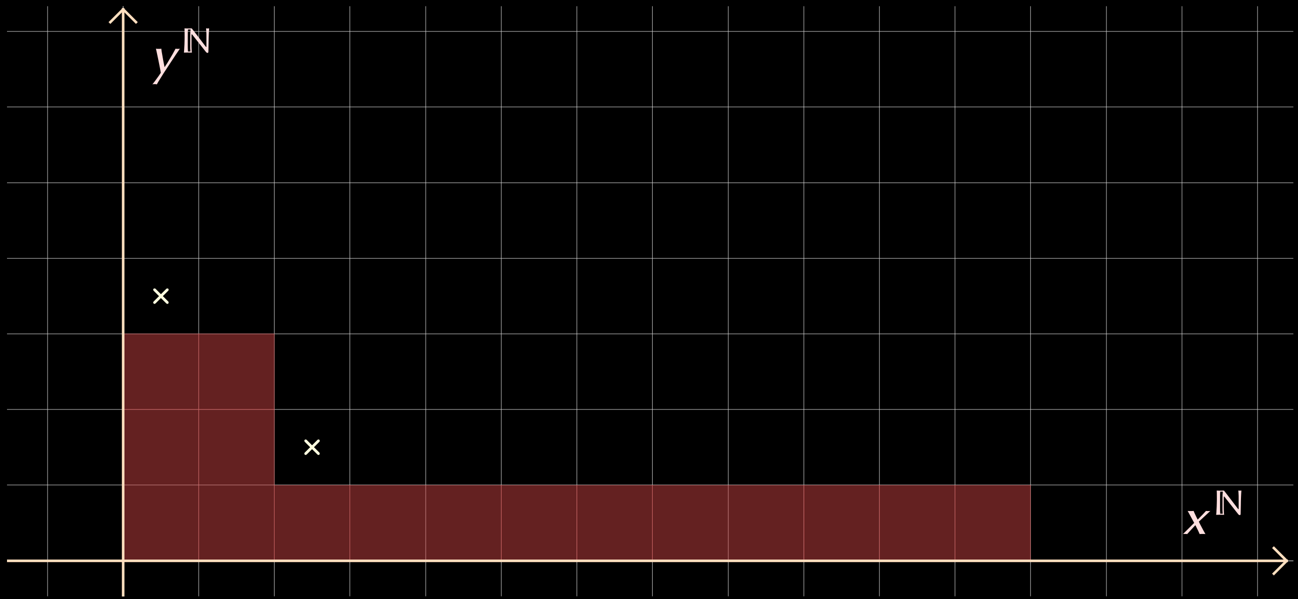
Gröbner basis, non-generic case



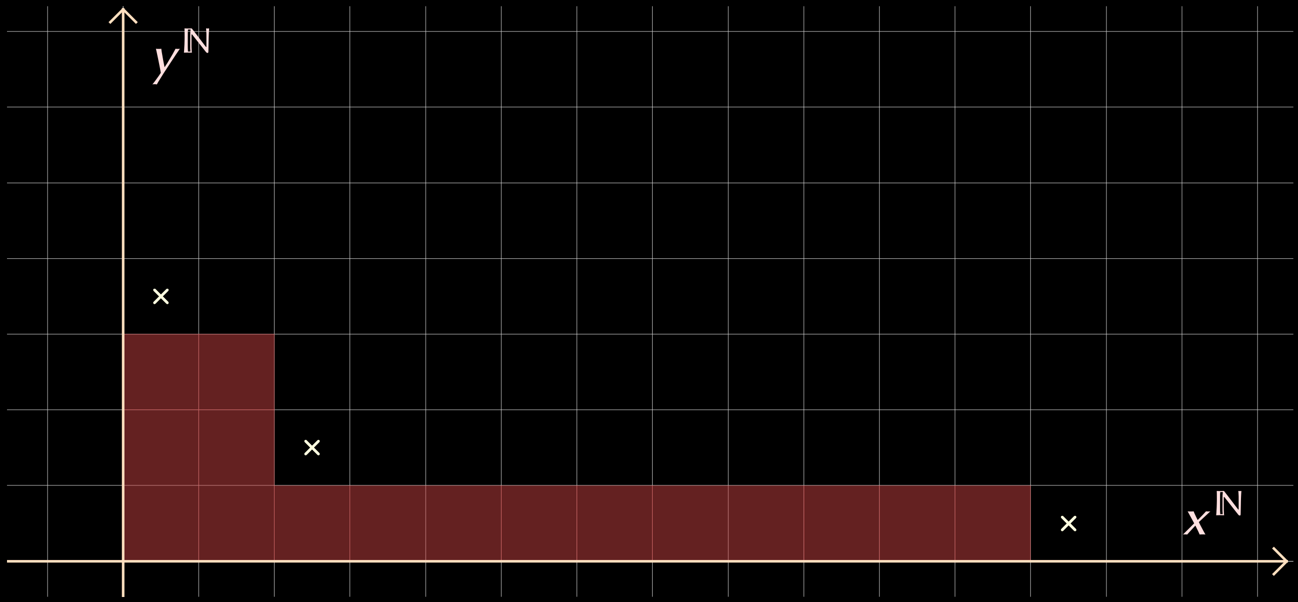
Gröbner basis, non-generic case



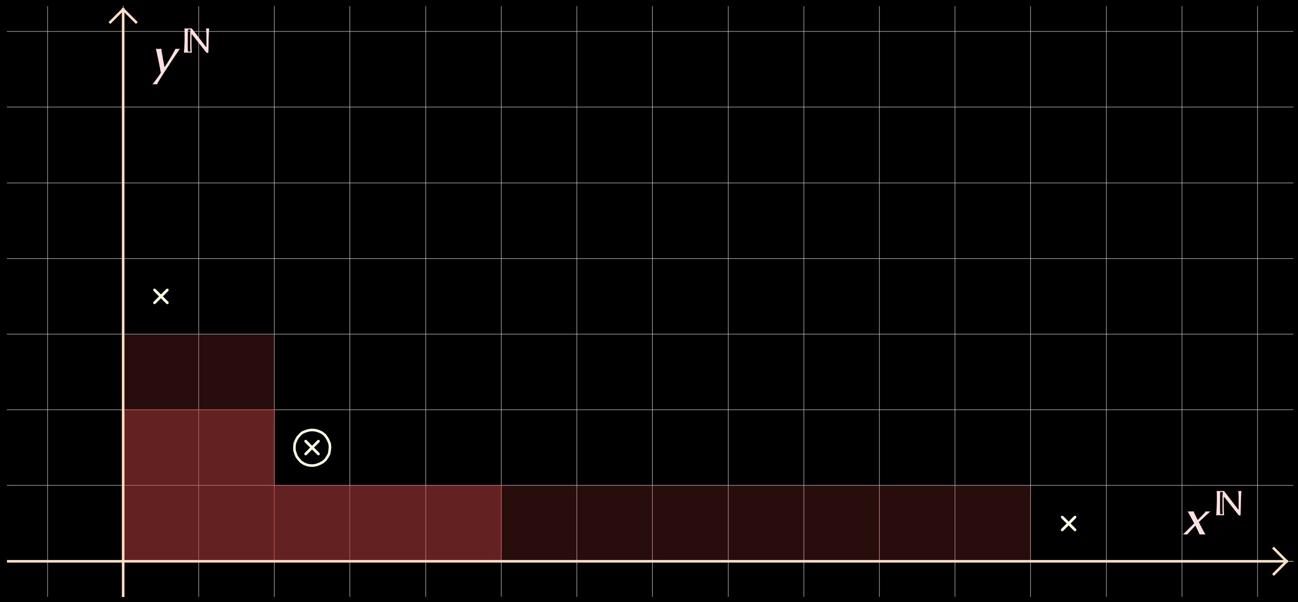
Gröbner basis, non-generic case



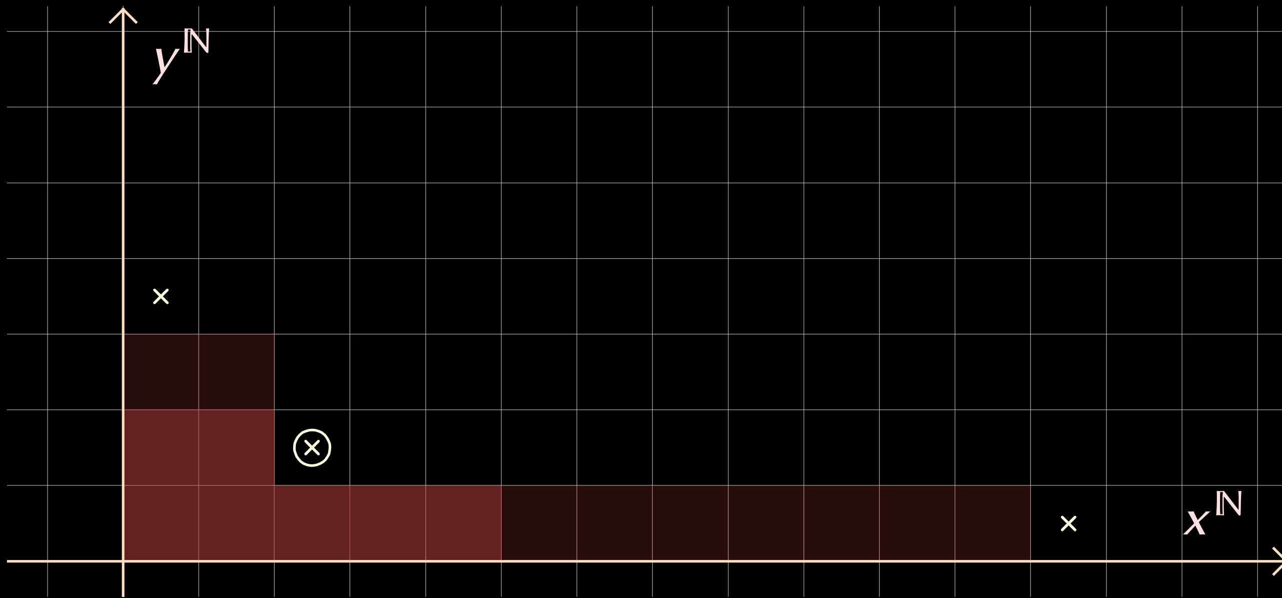
Gröbner basis, non-generic case



Gröbner basis, non-generic case

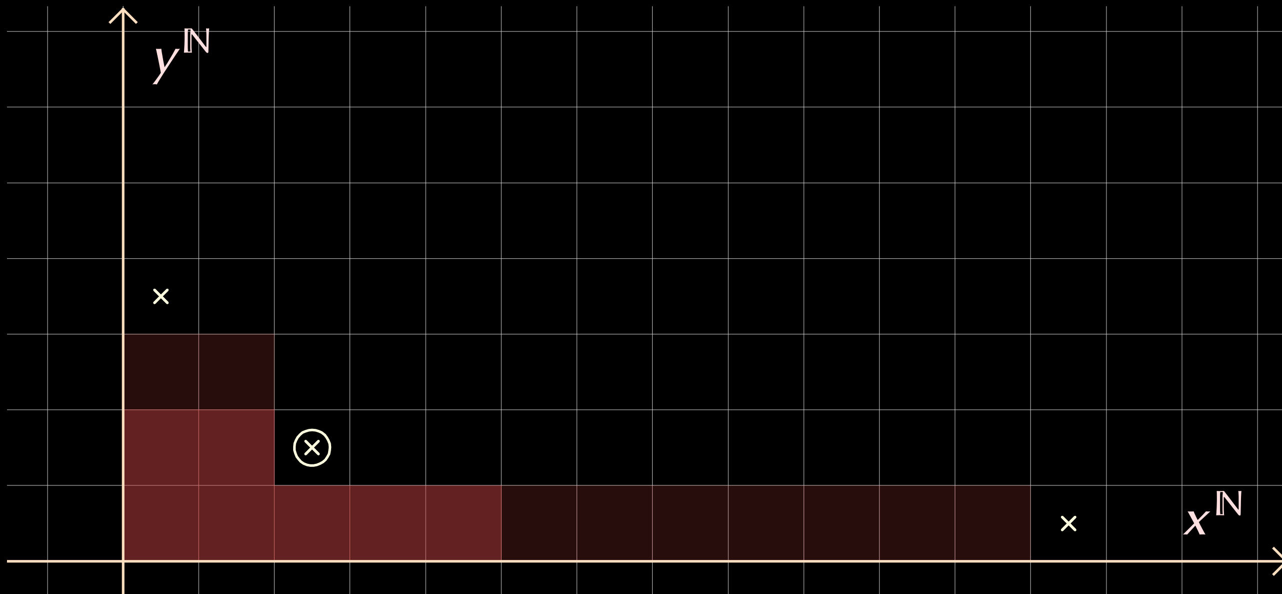


Gröbner basis, non-generic case



This time: $\exists B_k \in I_\alpha, \quad b \leq \sqrt{\frac{2n}{k}}$

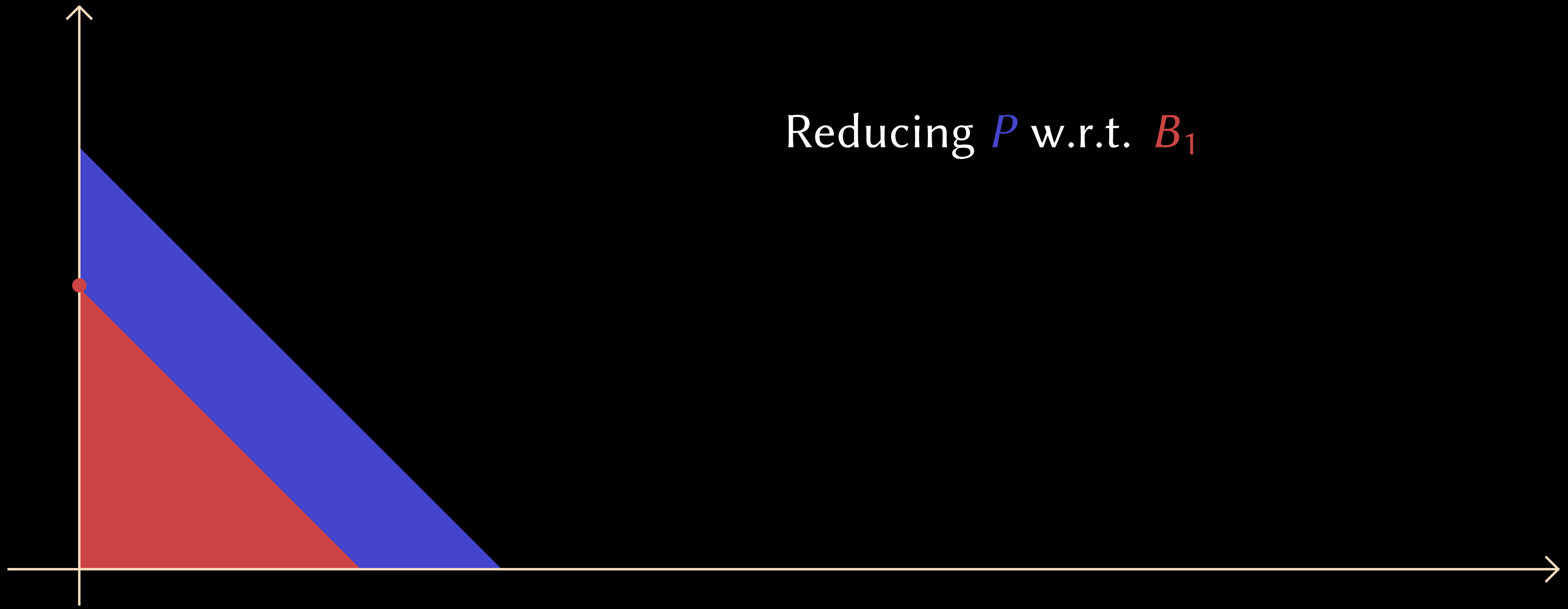
Gröbner basis, non-generic case



This time: $\exists B_k \in I_\alpha, \quad b \leqslant \sqrt{\frac{2n}{k}}$

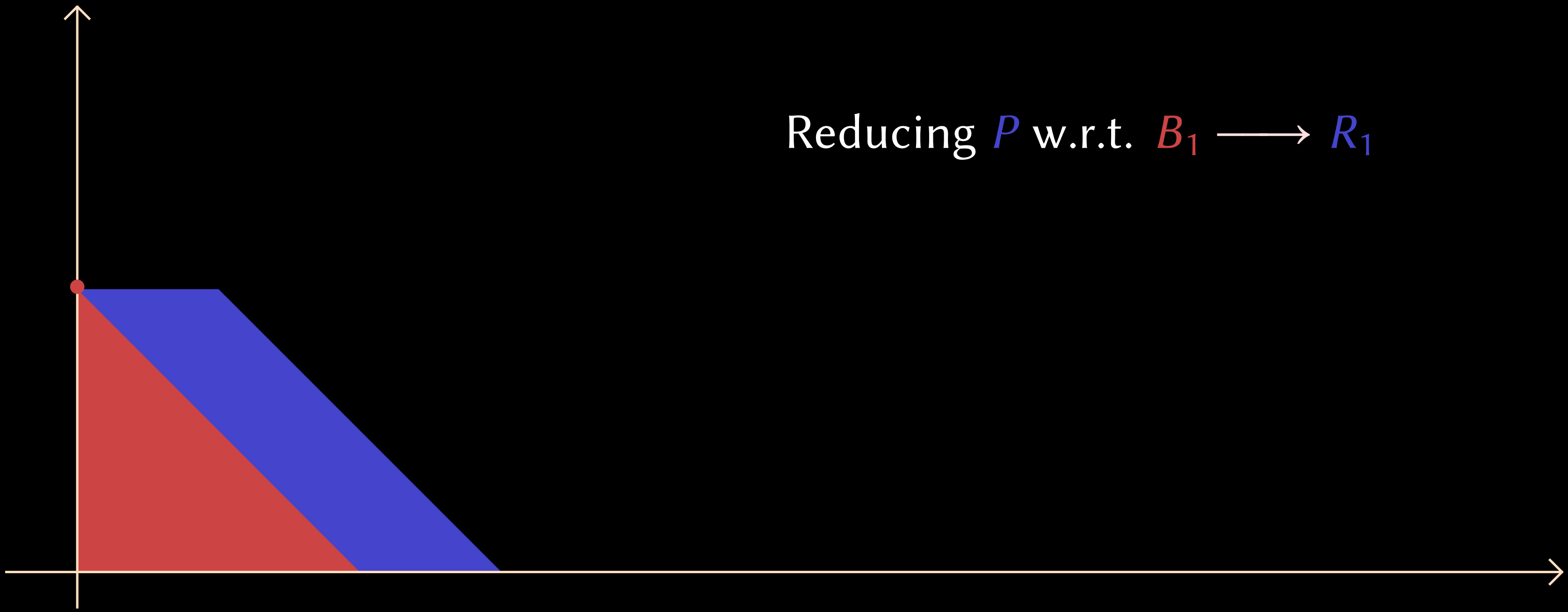
Also: modulo $x \longrightarrow \tilde{x} + \lambda y$, we may assume that $\mathrm{LM}(B_1) = y^b$

Reduction, non-generic case



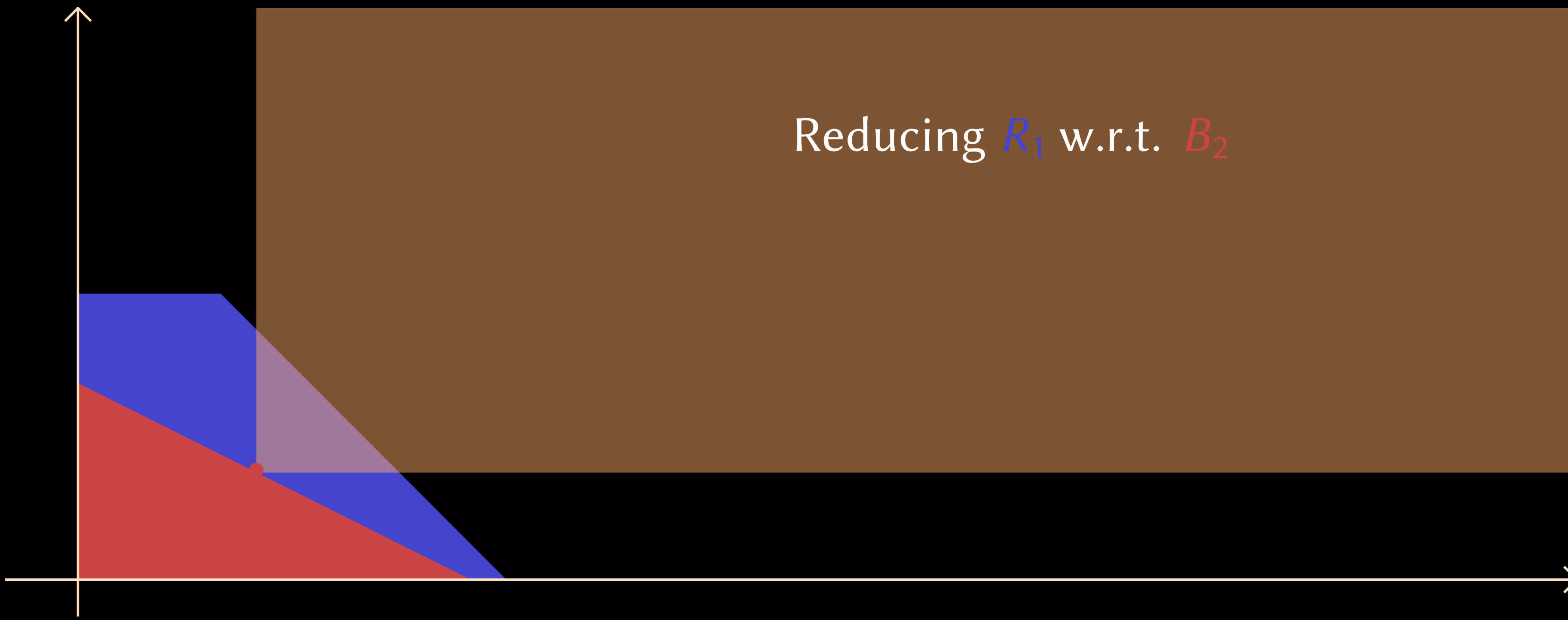
Reducing P w.r.t. B_1

Reduction, non-generic case

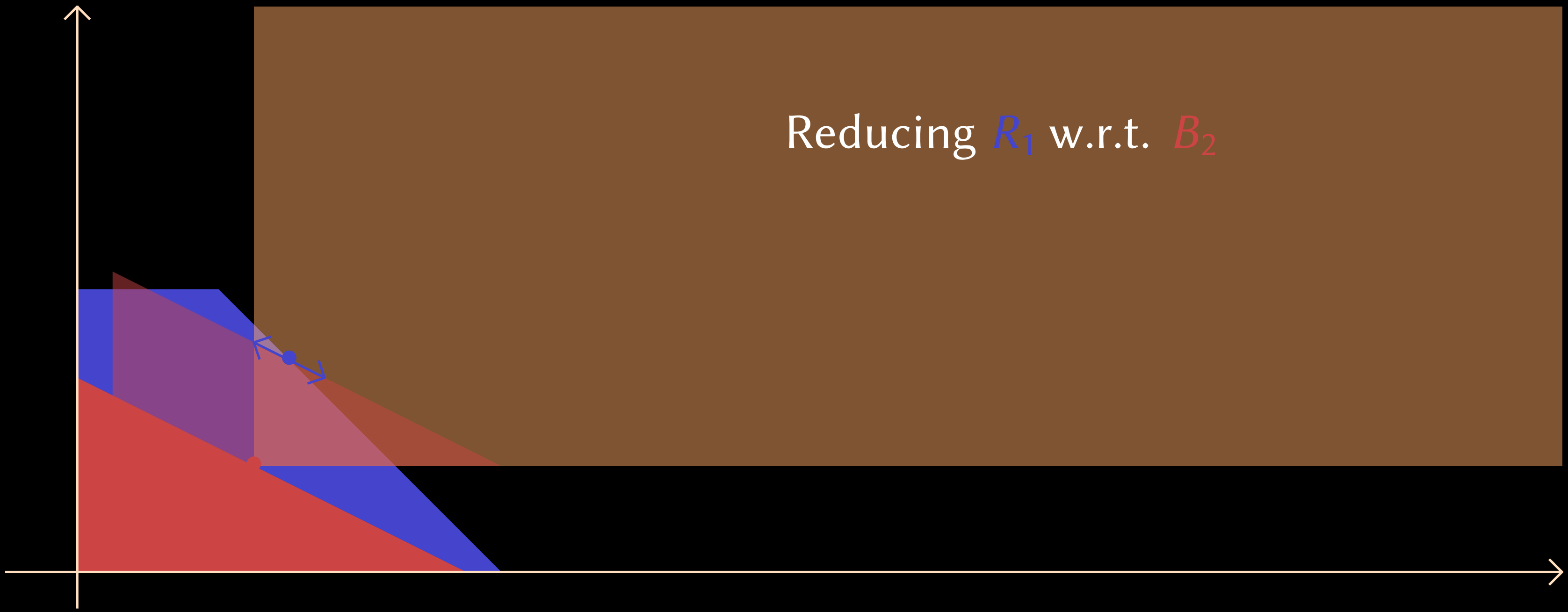


Reducing P w.r.t. $B_1 \longrightarrow R_1$

Reduction, non-generic case

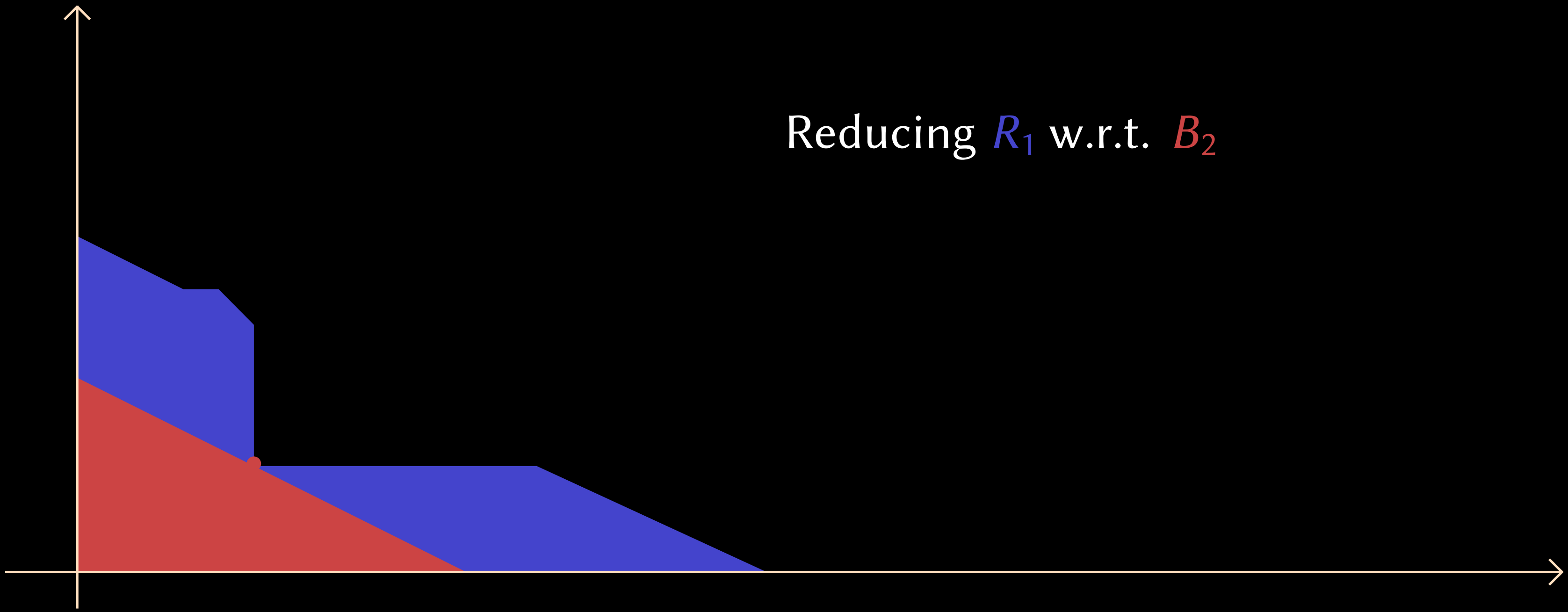


Reduction, non-generic case



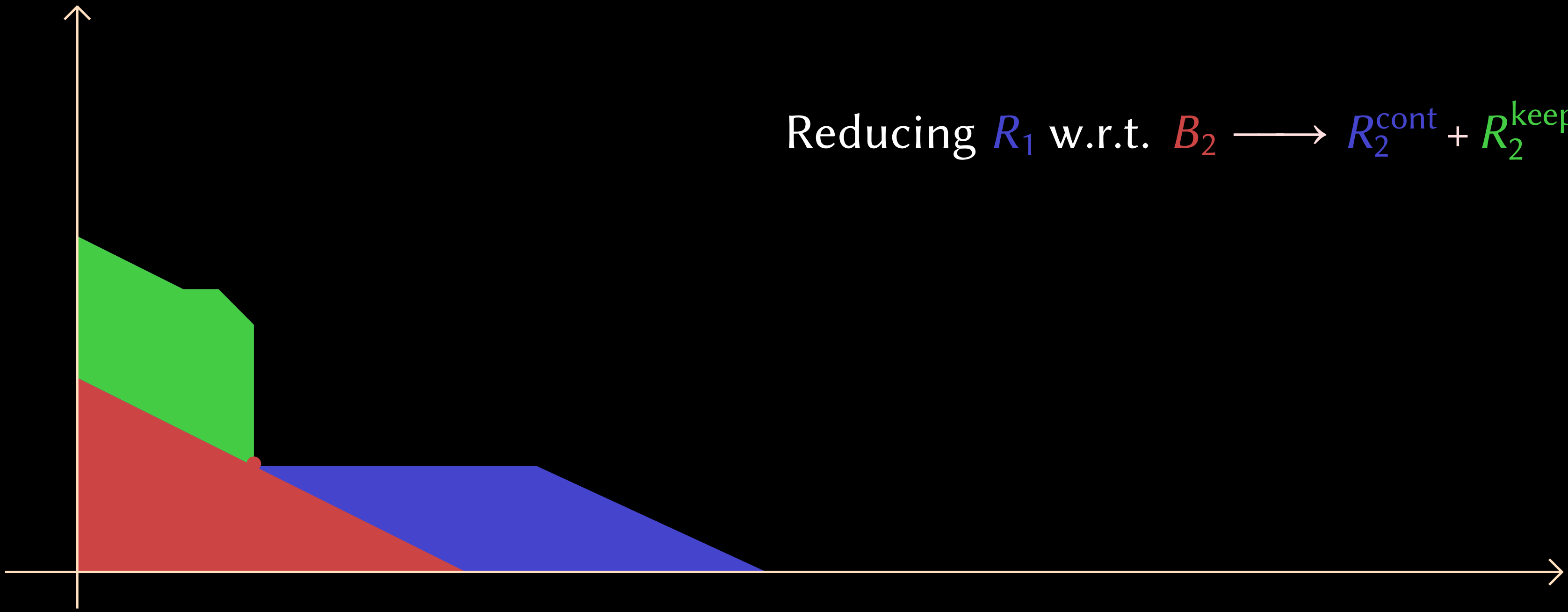
Reducing R_1 w.r.t. B_2

Reduction, non-generic case



Reducing R_1 w.r.t. B_2

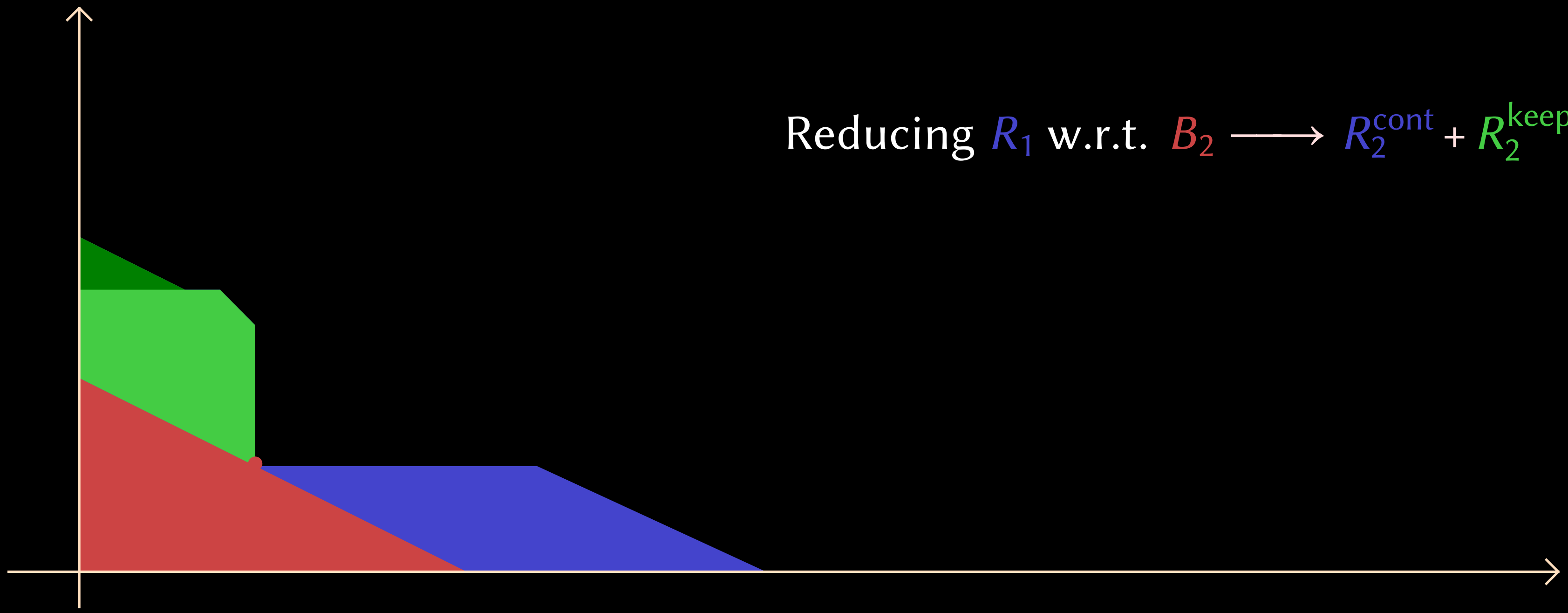
Reduction, non-generic case



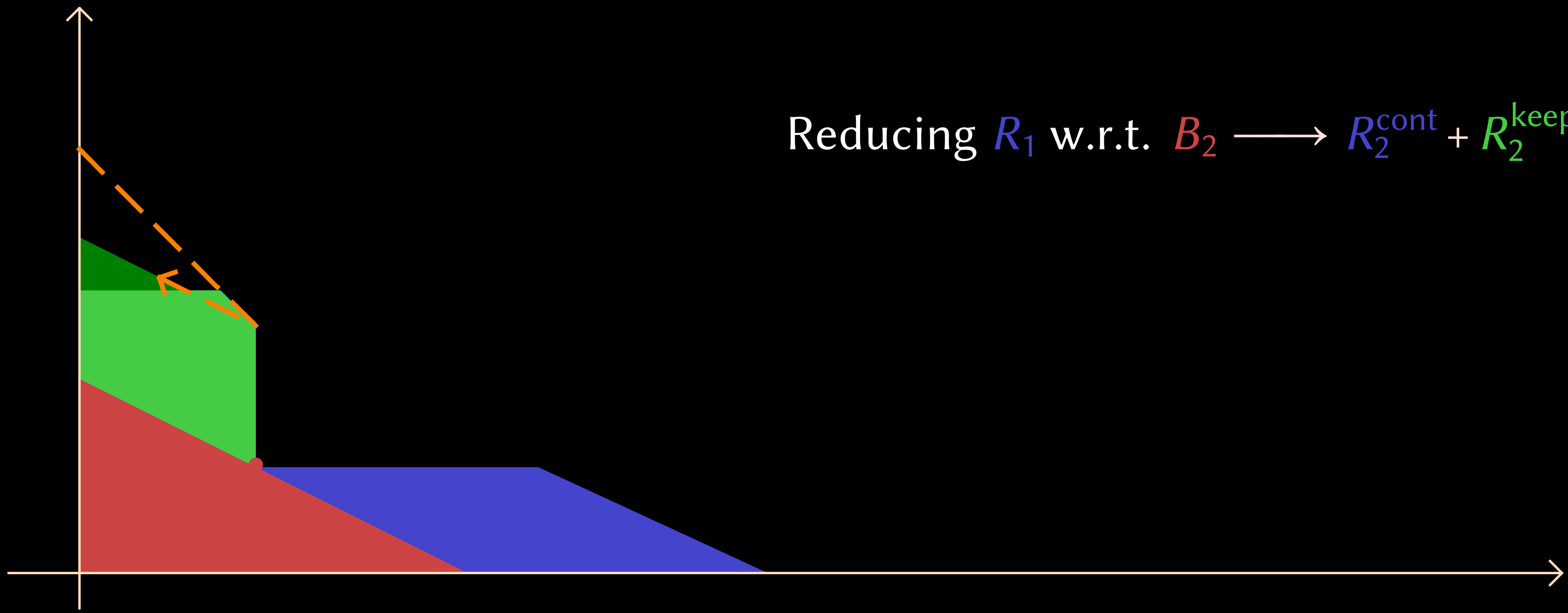
Reducing R_1 w.r.t. $B_2 \longrightarrow R_2^{\text{cont}} + R_2^{\text{keep}}$

Reduction, non-generic case

Reducing R_1 w.r.t. $B_2 \longrightarrow R_2^{\text{cont}} + R_2^{\text{keep}}$

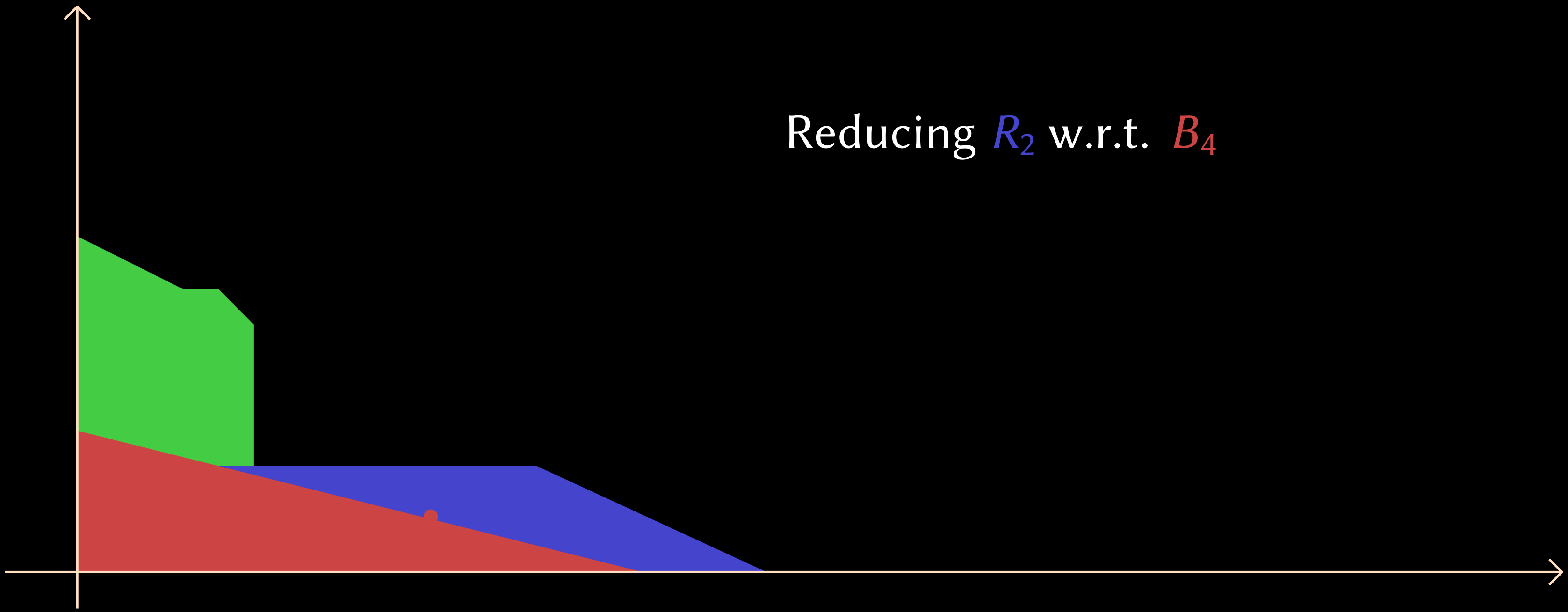


Reduction, non-generic case



Reducing R_1 w.r.t. B_2 $\longrightarrow$ $R_2^{\text{cont}} + R_2^{\text{keep}}$

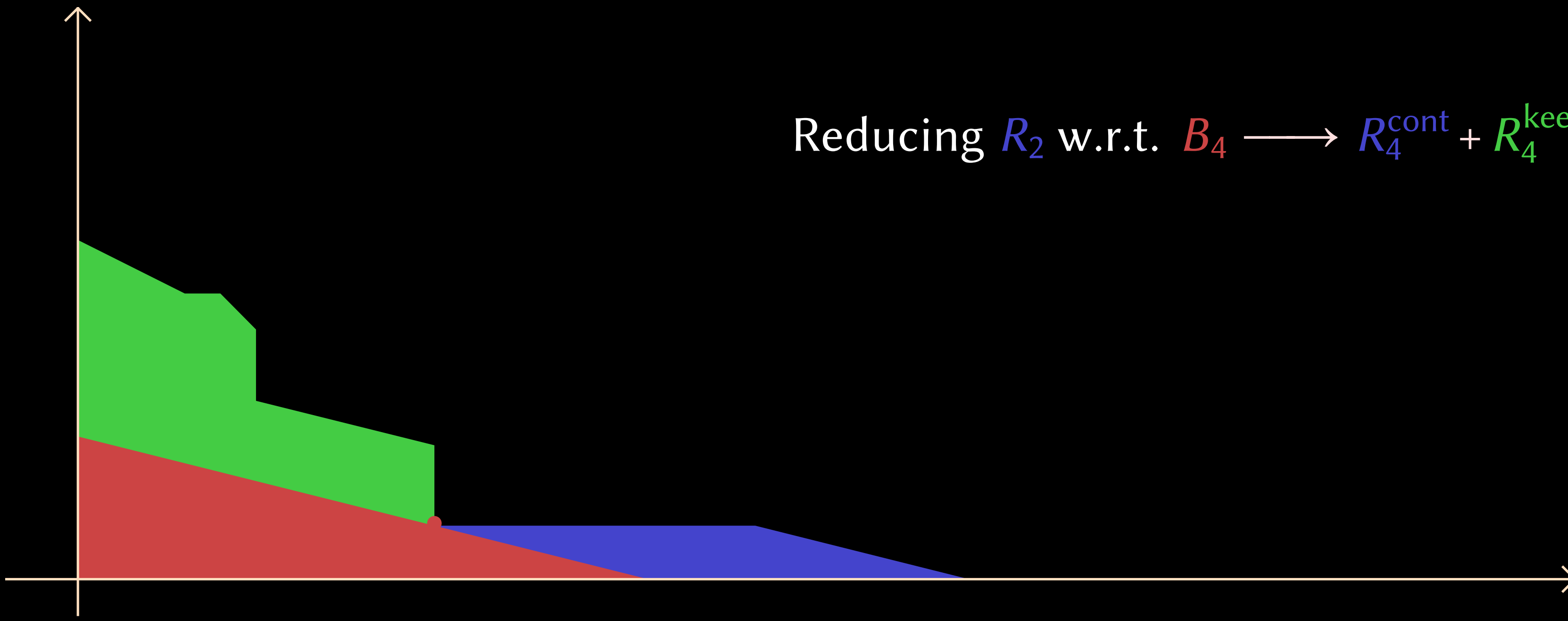
Reduction, non-generic case



Reducing R_2 w.r.t. B_4

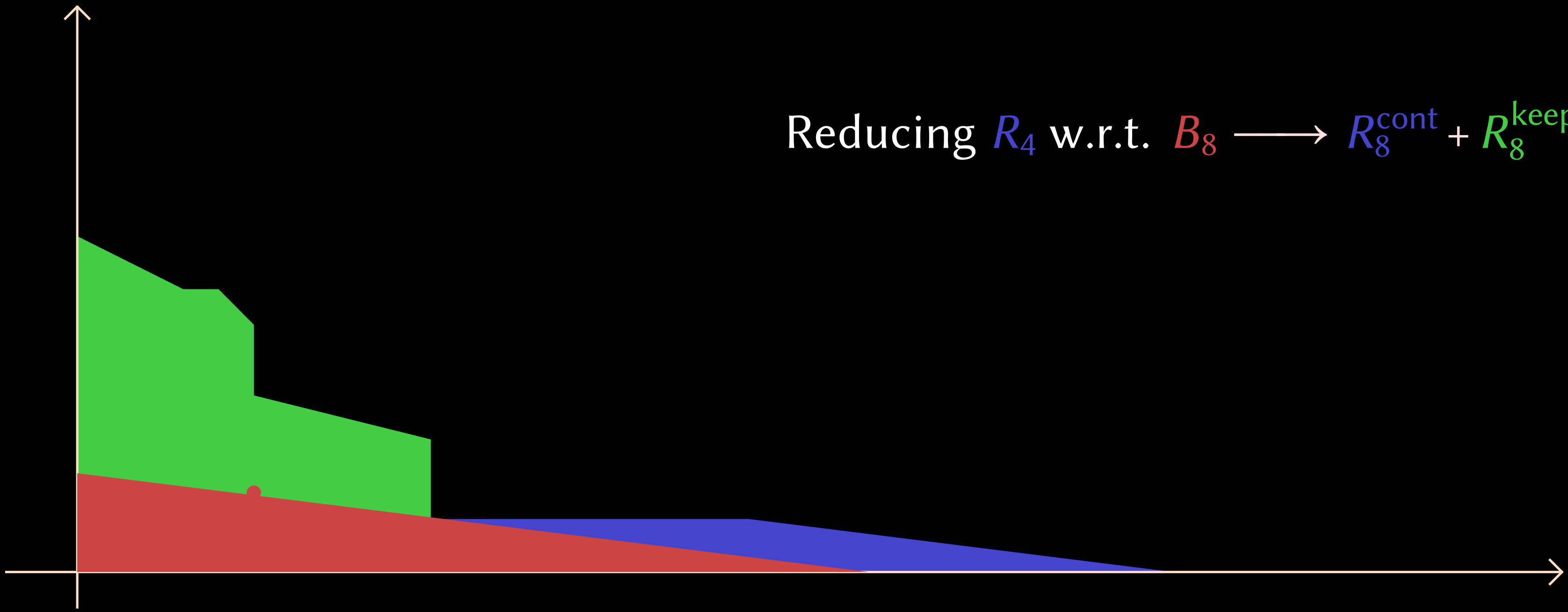
Reduction, non-generic case

Reducing R_2 w.r.t. $B_4 \longrightarrow R_4^{\text{cont}} + R_4^{\text{keep}}$



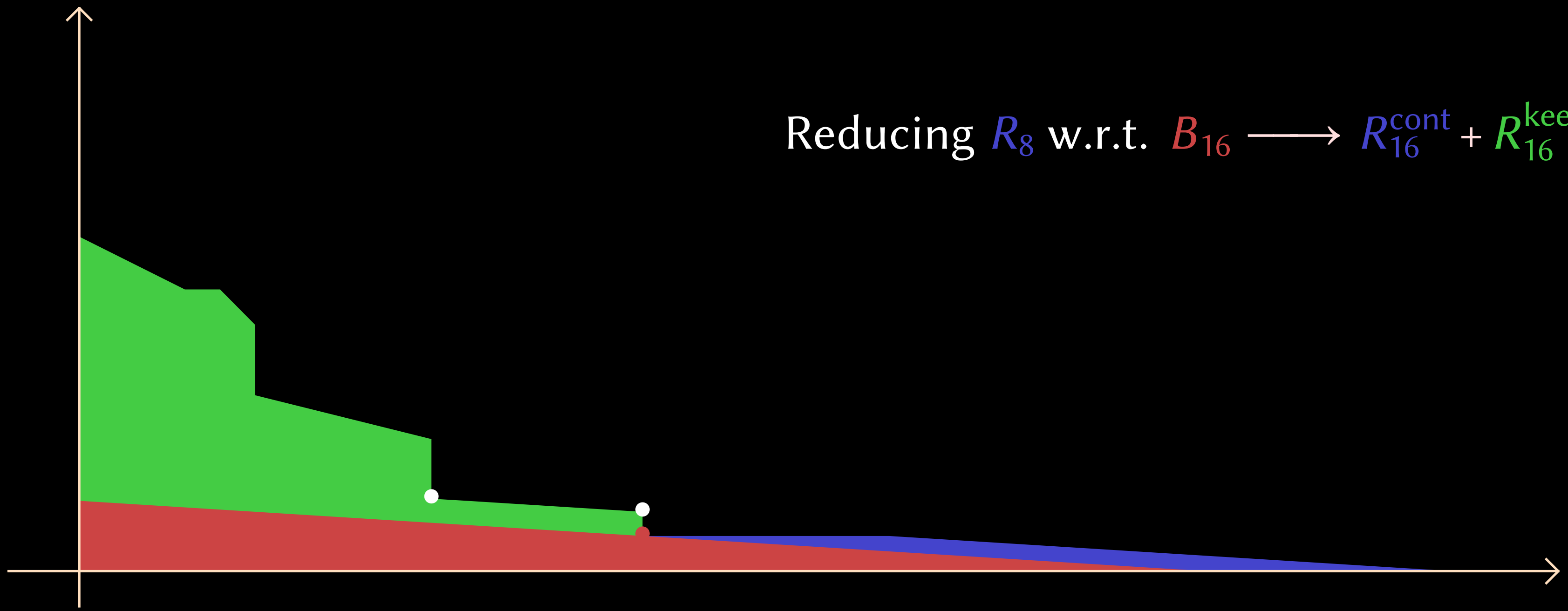
Reduction, non-generic case

Reducing R_4 w.r.t. $B_8 \longrightarrow R_8^{\text{cont}} + R_8^{\text{keep}}$

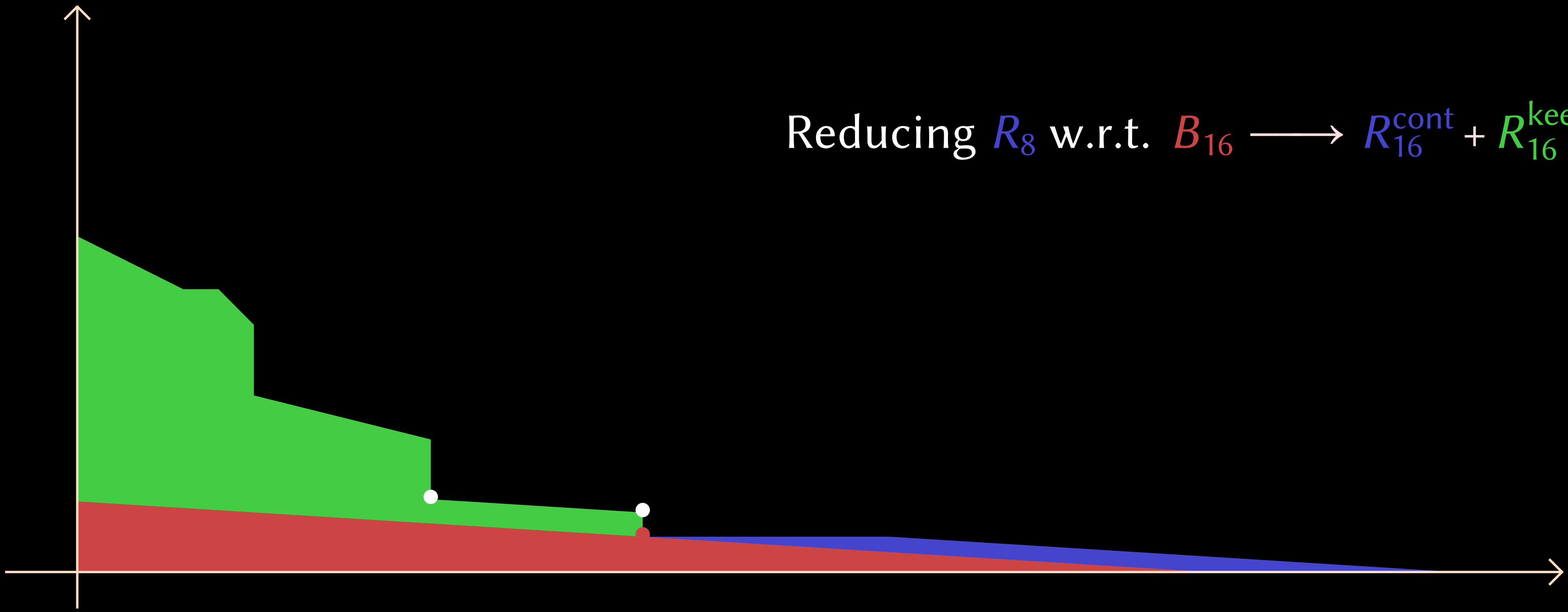


Reduction, non-generic case

Reducing R_8 w.r.t. B_{16} $\longrightarrow$ $R_{16}^{\text{cont}} + R_{16}^{\text{keep}}$



Reduction, non-generic case



Reducing R_8 w.r.t. B_{16} $\longrightarrow$ $R_{16}^{\text{cont}} + R_{16}^{\text{keep}}$

In general:

- $P = P_1 + P_2 + P_4 + \cdots \longrightarrow R = R_1 + R_2 + R_4 + \cdots, \qquad R - P \in I_\alpha$
- Controlled decrease of $\deg_k P_k$ during this reduction

Remainder trees for ideals

$$\boldsymbol{\alpha}_{\text{lo}} := (\alpha_1, \ldots, \alpha_{\lfloor n/2 \rfloor})$$
$$\boldsymbol{\alpha}_{\text{hi}} := (\alpha_{\lfloor n/2 \rfloor + 1}, \ldots, \alpha_n)$$

$$P$$

Remainder trees for ideals

$$\boldsymbol{\alpha}_{\mathrm{lo}} := (\alpha_1, \ldots, \alpha_{\lfloor n/2 \rfloor})$$
$$\boldsymbol{\alpha}_{\mathrm{hi}} := (\alpha_{\lfloor n/2 \rfloor + 1}, \ldots, \alpha_n)$$

$$P \operatorname{rem} I_{\boldsymbol{\alpha}}$$

Remainder trees for ideals

$$\boldsymbol{\alpha}_{\mathrm{lo}} := (\alpha_1, \ldots, \alpha_{\lfloor n/2 \rfloor})$$
$$\boldsymbol{\alpha}_{\mathrm{hi}} := (\alpha_{\lfloor n/2 \rfloor + 1}, \ldots, \alpha_n)$$

$$P \operatorname{rem} I_{\boldsymbol{\alpha}}$$

$$(P \operatorname{rem} I_{\boldsymbol{\alpha}}) \operatorname{rem} I_{\boldsymbol{\alpha}_{\mathrm{lo}}} \qquad (P \operatorname{rem} I_{\boldsymbol{\alpha}}) \operatorname{rem} I_{\boldsymbol{\alpha}_{\mathrm{hi}}}$$

Remainder trees for ideals

$$\boldsymbol{\alpha}_{\mathrm{lo}} := (\alpha_1, \ldots, \alpha_{\lfloor n/2 \rfloor})$$

$$\boldsymbol{\alpha}_{\mathrm{hi}} := (\alpha_{\lfloor n/2 \rfloor + 1}, \ldots, \alpha_n)$$

$$P \operatorname{rem} I_{\boldsymbol{\alpha}}$$

$$P \operatorname{rem} I_{\boldsymbol{\alpha}_{\mathrm{lo}}} \qquad P \operatorname{rem} I_{\boldsymbol{\alpha}_{\mathrm{hi}}}$$

Remainder trees for ideals

$$\boldsymbol{\alpha}_{\mathrm{lo}} := (\alpha_1, \ldots, \alpha_{\lfloor n/2 \rfloor})$$

$$\boldsymbol{\alpha}_{\mathrm{hi}} := (\alpha_{\lfloor n/2 \rfloor + 1}, \ldots, \alpha_n)$$

$$P \operatorname{rem} I_{\boldsymbol{\alpha}}$$

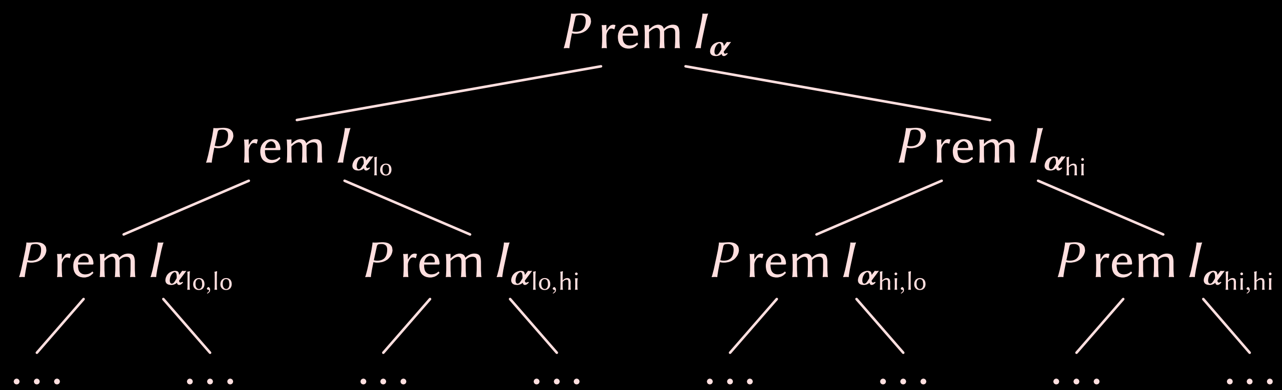
$$P \operatorname{rem} I_{\boldsymbol{\alpha}_{\mathrm{lo}}} \qquad P \operatorname{rem} I_{\boldsymbol{\alpha}_{\mathrm{hi}}}$$

$$P \operatorname{rem} I_{\boldsymbol{\alpha}_{\mathrm{lo,lo}}} \qquad P \operatorname{rem} I_{\boldsymbol{\alpha}_{\mathrm{lo,hi}}} \qquad P \operatorname{rem} I_{\boldsymbol{\alpha}_{\mathrm{hi,lo}}} \qquad P \operatorname{rem} I_{\boldsymbol{\alpha}_{\mathrm{hi,hi}}}$$

Remainder trees for ideals

$$\boldsymbol{\alpha}_{\mathrm{lo}} := (\alpha_1, \ldots, \alpha_{\lfloor n/2 \rfloor})$$

$$\boldsymbol{\alpha}_{\mathrm{hi}} := (\alpha_{\lfloor n/2 \rfloor + 1}, \ldots, \alpha_n)$$



Thank you !

http://www.texmacs.org