Criteria on leading terms for S-polynomial representations

John Edward Perry

North Carolina Wesleyan College

Partially funded by NSF 0097976

Overview

- Question
- Answer
- Analysis of answer
- Future direction

Question

The question

Are Buchberger's criteria
for S-polynomial representations
the most general criteria *using leading terms alone?*

Background: representation

$$\boxed{\begin{array}{c}\mathbf{S}_{\succ}(f_i, f_j) \text{ has } \textbf{representation} \\ (h_1, \ldots, h_m) \\ \text{modulo } F = (f_1, \ldots, f_m)\end{array}}$$

$$\Updownarrow$$

$$\boxed{\begin{array}{c}\mathbf{S}_{\succ}(f_i, f_j) = h_1 f_1 + \cdots + h_m f_m \\ \text{and} \\ h_k \neq 0 \text{ implies } \mathbf{lt}_{\succ}(h_k f_k) \prec \mathbf{lcm}(\mathbf{lt}_{\succ}(f_i), \mathbf{lt}_{\succ}(f_j))\end{array}}$$

Notation: $\mathbf{Rep}(\mathbf{S}_{\succ}(f_1, f_2); F)$

Background: why representations?

Representations intimately tied to GB!

Theorem:

$$\boxed{F = (f_1, \ldots, f_m) \text{ a Gröbner basis}}$$

$$\Updownarrow$$

$$\boxed{\begin{array}{c} \mathbf{S}_{\succ}(f_i, f_j) \xrightarrow[F]{*} 0 \\ \forall i \neq j \in \{1, \ldots, m\} \end{array}}$$

$$\Updownarrow$$

$$\boxed{\begin{array}{c} \mathbf{S}_{\succ}(f_i, f_j) \text{ has representation} \\ \text{modulo } F \\ \forall i \neq j \in \{1, \ldots, m\} \end{array}}$$

Interesting fact

Sometimes,

$$? \quad \Longrightarrow \quad \exists i,j \ \mathbf{Rep}\left(\mathbf{S}_{\succ}\left(f_i,f_j\right);F\right)$$

$$\Longrightarrow \quad \exists i,j \text{ can skip } \mathbf{S}_{\succ}\left(f_i,f_j\right)$$

Previous work

1965 Buchberger, B. (BCG)

1979 Buchberger, B. (BCL)

1988 Gebauer, R. and Möller, H. (Efficient BC)

2002 Caboara, M.; Kreuzer, M.; Robbiano, L. (BC in syzygy module)

2003 Faugère, J.C. (criterion on other terms, coefficients)

Well-known: BC

BCG: t_1, t_3 rel. prime

$$t_k = \mathbf{lt}_\succ (f_k)$$

BCL: t_2 divides $\mathbf{lcm}\,(t_1, t_3)$

$$\begin{array}{c} \mathbf{BCG}(t_1, t_3) \\ \text{or} \\ \mathbf{BCL}(t_1, t_2, t_3) \end{array} \quad \Longrightarrow \quad \begin{array}{c} \text{Can skip} \\ \mathbf{S}_\succ (f_1, f_3) \end{array}$$

Why can we skip?

$$\textbf{BCG} \Longrightarrow \ \mathbf{Rep}\left(\mathbf{S}_{\succ}\left(f_1,f_3\right);F\right)$$

$$\textbf{BCL} \Longrightarrow \ \left.\begin{array}{l}\mathbf{Rep}\left(\mathbf{S}_{\succ}\left(f_1,f_2\right);F\right)\\ \mathbf{Rep}\left(\mathbf{S}_{\succ}\left(f_2,f_3\right);F\right)\end{array}\right\} \Rightarrow \mathbf{Rep}\left(\mathbf{S}_{\succ}\left(f_1,f_3\right);F\right)$$

$$\mathbf{S}_{\succ}\left(f_1,f_3\right)=\frac{\mathbf{lcm}\left(t_1,t_3\right)}{\mathbf{lcm}\left(t_1,t_2\right)}\cdot\mathbf{S}_{\succ}\left(f_1,f_2\right)+\frac{\mathbf{lcm}\left(t_1,t_3\right)}{\mathbf{lcm}\left(t_2,t_3\right)}\cdot\mathbf{S}_{\succ}\left(f_2,f_3\right)$$

Interesting question

BC: criterion $C(t_1, t_2, t_3)$ ***on terms***:

- for *every* $(f_1, \ldots, f_m)$ with $\mathbf{lt}_{\succ}(f_k) = t_k$
- can skip $\mathbf{S}_{\succ}(f_1, f_3)$

...Are there other criteria *on terms*?

The question (again)

Are Buchberger's criteria
for S-polynomial representations
the most general criteria *using leading terms alone?*

Answer:

“Almost... but not quite”

BCL: Chained representation

BCL: $t_2 \mid \mathbf{lcm}(t_1, t_3)$

$$\left.\begin{array}{l} \mathbf{Rep}\left(\mathbf{S}_{\succ}(f_1, f_2)\,;F\right) \\ \mathbf{Rep}\left(\mathbf{S}_{\succ}(f_2, f_3)\,;F\right) \end{array}\right\} \quad \Longrightarrow \quad \mathbf{Rep}\left(\mathbf{S}_{\succ}(f_1, f_3)\,;F\right)$$

Generalization: chain condition

$\mathbf{Chain}\,(t_1,\ldots,t_\nu;m)$ iff

$$\forall \succ$$
$$\forall F=(f_1,\ldots,f_m) \text{ with } \mathbf{lt}_\succ f_1=t_1,\ \ldots,\ \mathbf{lt}_\succ f_\nu=t_\nu$$

$$\left.\begin{array}{c}\mathbf{Rep}\left(\mathbf{S}_\succ\left(f_1,f_2\right);F\right)\\ \text{and}\\ \mathbf{Rep}\left(\mathbf{S}_\succ\left(f_2,f_3\right);F\right)\\ \text{and}\\ \cdots\\ \text{and}\\ \mathbf{Rep}\left(\mathbf{S}_\succ\left(f_{\nu-1},f_\nu\right);F\right)\end{array}\right\}\Longrightarrow \mathbf{Rep}\left(\mathbf{S}_\succ\left(f_1,f_\nu\right);F\right)$$

$$(\nu\le m)$$

Chain condition: generality

$$\text{Generality} \quad \Longleftrightarrow \quad \text{Sufficiency } \textit{AND} \text{ Necessity}$$

Know

$$\left.\begin{array}{c} \text{BCG}\,(t_1, t_\nu) \\ \text{or} \\ \text{BCL}\,(t_1, t_i, t_\nu) \end{array}\right\} \quad \Longrightarrow \quad \mathbf{Chain}\,(t_1, \ldots, t_\nu; m)$$

$$(\exists i \; 1 < i < m)$$

Chain condition: generality

$$\text{Generality} \quad \Longleftrightarrow \quad \text{Sufficiency } \textit{AND} \text{ Necessity}$$

But

$$\left.\begin{array}{c} \text{BCG}\,(t_1, t_\nu) \\ \text{or} \\ \text{BCL}\,(t_1, t_i, t_3) \end{array}\right\} \quad \overset{?!?}{\Longleftarrow} \quad \textbf{Chain}\,(t_1, \ldots, t_\nu; m)$$

$$(\exists i \; 1 < i < m)$$

Almost... ($\nu < m$)

Theorem "Almost": For #lts $<$ #polys

Buchberger criteria are **necessary** for **Chain** $(t_1 \ldots t_\nu; m)$.

Almost... ($\nu < m$)

Theorem "Almost": For #lts $<$ #polys

Buchberger criteria are **necessary** for **Chain** $(t_1 \ldots t_\nu; m)$.

Sketch of proof:

- $F = (f_1, \ldots, f_m)$ where
  $f_1 = t_1 + 1$,
  $f_2 = t_2$, . . ., $f_\nu = t_\nu$,
  $f_{\nu+1} = \ldots = f_m = \mathbf{S}_\succ(f_1, f_2)$
- **Chain** $(t_1, \ldots, t_\nu; m) \quad \Longrightarrow \quad$ BCG or BCL!!!

Conclusion: BC most general criterion for #lts $<$ #polys

...but not quite! ($\nu = m$)

Theorem "But not quite": For #lts $=$ #polys,

Buchberger criteria are **not** necessary for
$\mathbf{Chain}\,(t_1, \ldots, t_m; m)$.

...but not quite! ($\nu = m$)

Theorem "But not quite": For #lts = #polys,

Buchberger criteria are **not** necessary for
$\mathbf{Chain}\,(t_1, \ldots, t_m; m)$.

New criteria:

$$\mathbf{Chain}\,(t_1, \ldots, t_m; m)$$
$$\Uparrow$$
$$t_1 = x_0 x_1 \quad t_2 = x_0 x_2 \quad \ldots \quad t_m = x_0 x_m$$

...but not quite! ($\nu = m$)

Theorem "But not quite": For #lts $=$ #polys,

Buchberger criteria are **not** necessary for
$\mathbf{Chain}\,(t_1, \ldots, t_m; m)$.

New criteria:

$$\mathbf{Chain}\,(t_1, \ldots, t_m; m)$$
$$\Uparrow$$
$$t_1 = x_0 x_1 \quad t_2 = x_0 x_2 \quad \ldots \quad t_m = x_0 x_m$$

$$t_1 = x_1^2 \quad t_2 = \cdots = t_{m-1} = x_1 x_2 \quad \ldots \quad t_m = x_1$$

Conclusion: *More general criteria* for #lts $<$ #polys

Proof: Structure

$t_k = x_0 x_k$:

$$\begin{array}{ccc}
\begin{array}{c}\mathbf{S}_{\succ}(f_i, f_{i+1}) \\ \text{have representation}\end{array} & & \begin{array}{c}\mathbf{S}_{\succ}(f_1, f_m) \\ \text{has representation}\end{array} \\
\Downarrow & & \Uparrow \\
\begin{array}{c}\mathbf{lt}_{\succ}(c_1), \ldots, \mathbf{lt}_{\succ}(c_m) \\ \text{pairwise rel. prime}\end{array} & \Rightarrow & \begin{array}{c}\mathbf{S}_{\succ}(c_1, c_m) \\ \text{has representation}\end{array}
\end{array}$$

c_k cofactor of $\mathbf{gcd}(f_1, f_m)$ in f_k:

$$f_1 = x^2 (y+1) \quad f_3 = z(y+1) \qquad \Rightarrow \qquad c_1 = x^2 \quad c_3 = z$$

Most general? $m = 3$

Theorem:

Can skip $\mathrm{S}_{\succ}(f_1, f_3)$ **modulo** $(\mathbf{f_1}, \mathbf{f_2}, \mathbf{f_3})$
$\forall f_1, f_2, f_3$ with leading terms t_1, t_2, t_3

Iff (EC-div) and (EC-var)

Most general? $m = 3$

Theorem:

Can skip $\mathbf{S}_{\succ}(f_1, f_3)$ **modulo** $(\mathbf{f_1}, \mathbf{f_2}, \mathbf{f_3})$
$\forall f_1, f_2, f_3$ with leading terms t_1, t_2, t_3

Iff (EC-div) and (EC-var)

(EC-div): $\mathbf{gcd}(t_1, t_3) \mid t_2$, *or*
$t_2 \mid \mathbf{lcm}(t_1, t_3)$

(EC-var): $\forall x$ $\deg_x t_1 = 0$, *or*
$\deg_x t_3 = 0$, *or*
$\deg_x t_2 \leq \deg_x \mathbf{lcm}(t_1, t_3)$

An example

$$t_1 = wx \quad t_2 = wy \quad t_3 = wz$$

- no pairs relatively prime $\Longrightarrow$ **not** BCG
- no link divides lcm $\Longrightarrow$ **not** BCL

$\therefore$ **BC** $\not\Longrightarrow$ Can skip $\mathbf{S}_{\succ}(f_i, f_j)$!

An example

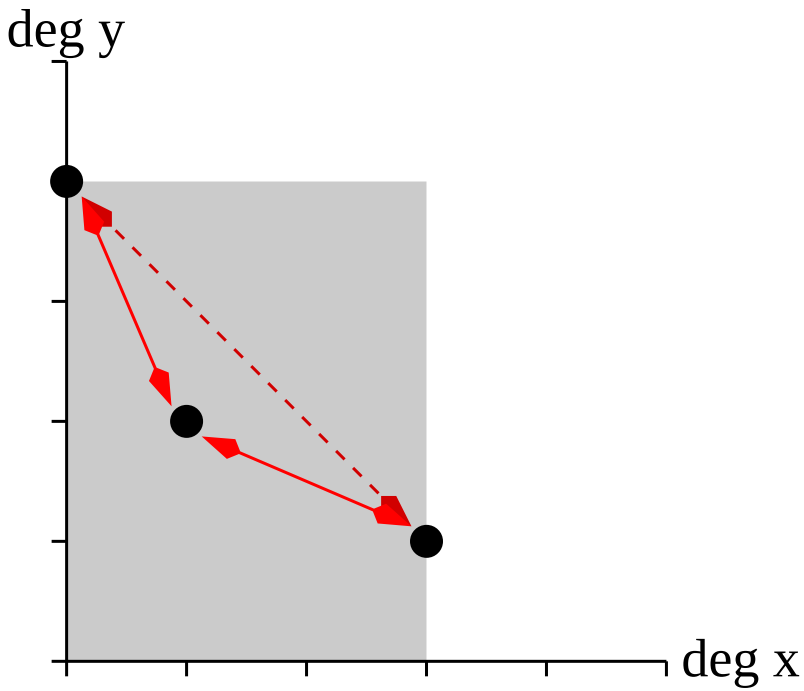
$$t_1 = wx \quad t_2 = wy \quad t_3 = wz$$

- $\mathbf{gcd}\,(t_1, t_3) \mid t_2 \implies$ EC-div (t_1, t_2, t_3)
- variable-wise:

$$\left.\begin{array}{l} \deg_w t_2 \le \deg_x \mathbf{lcm}\,(t_1, t_3) \\ \deg_x t_3 = 0 \\ \deg_y t_1 = 0 \\ \deg_z t_1 = 0 \end{array}\right\} \implies \text{EC-var}\,(t_1, t_2, t_3)$$

$\therefore$ We *can* skip $\mathbf{S}_{\succ}(f_1, f_3)$ for $F = (f_1, f_2, f_3)$!

Illustration of BCL



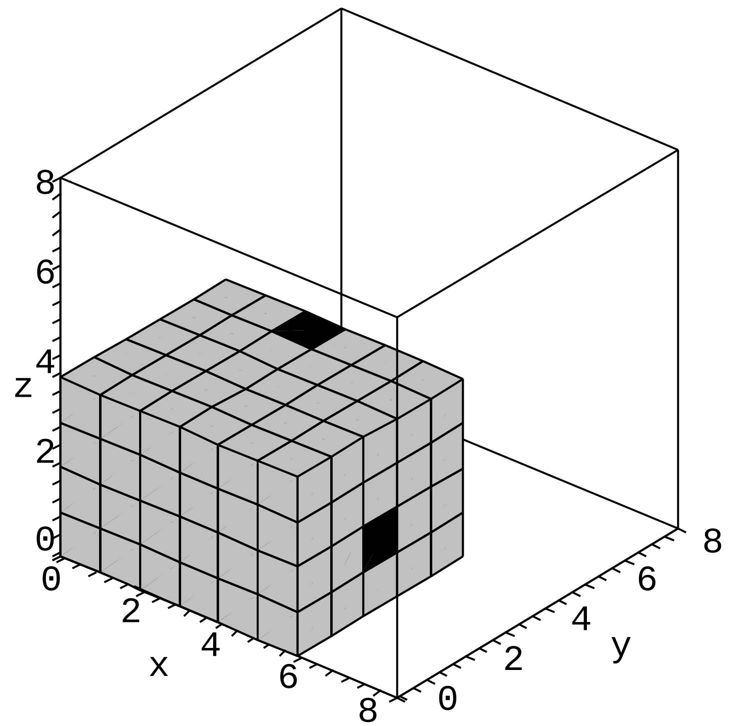
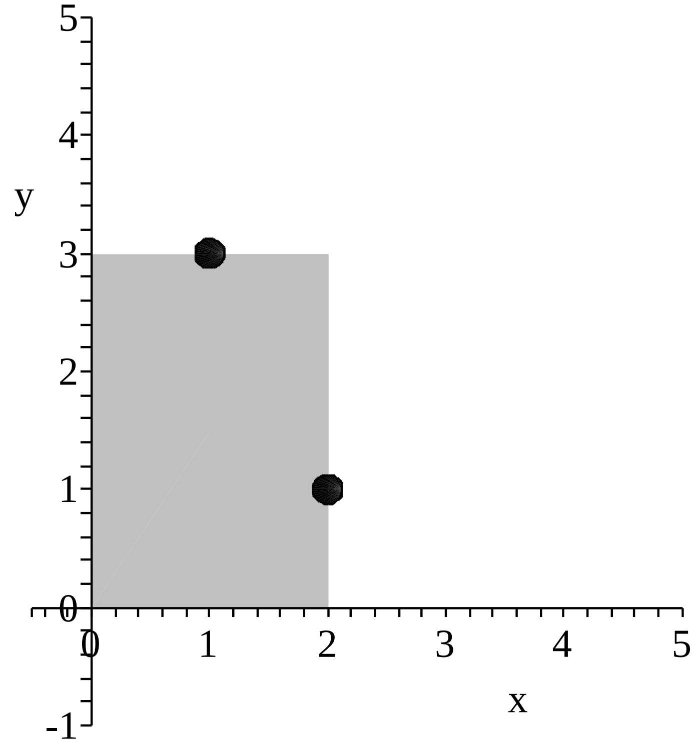
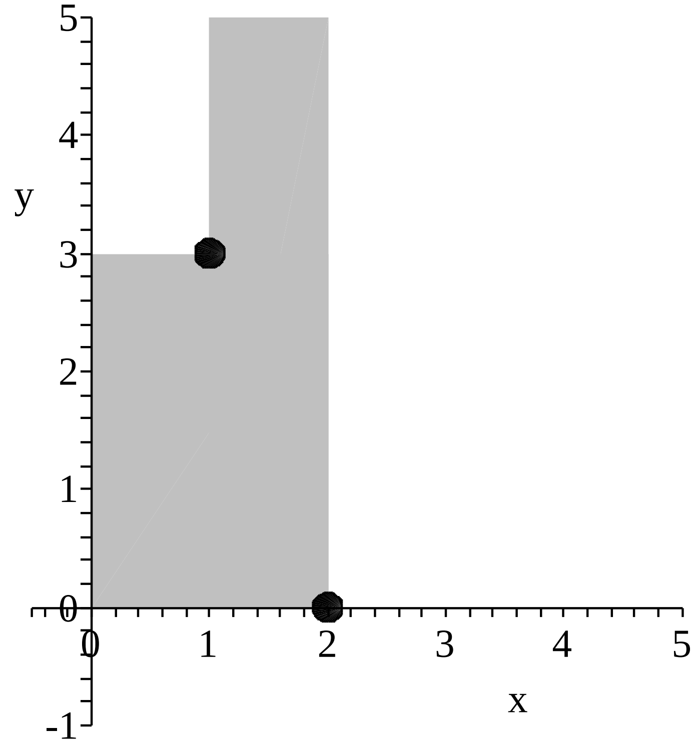


Illustration (2D)



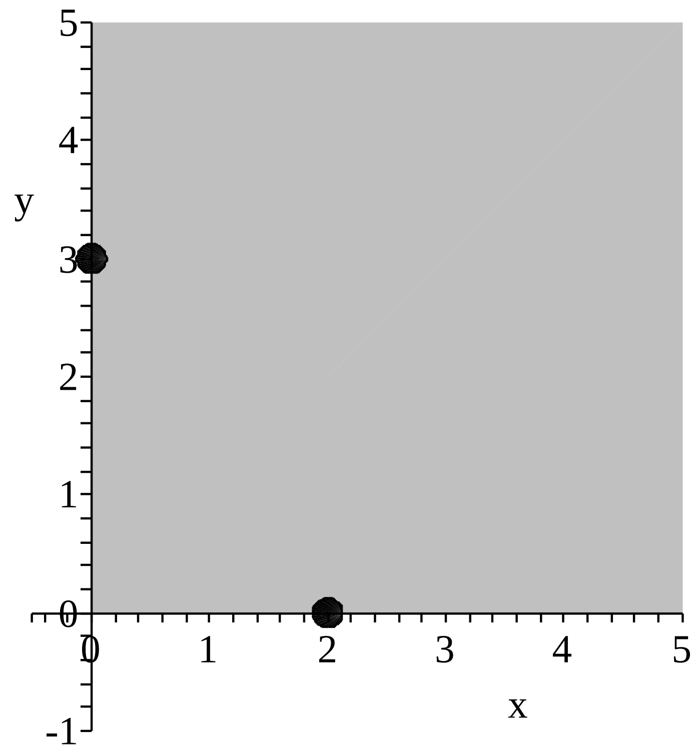
$$t_1 = x^2y \qquad t_3 = xy^3$$

Illustration (2D)



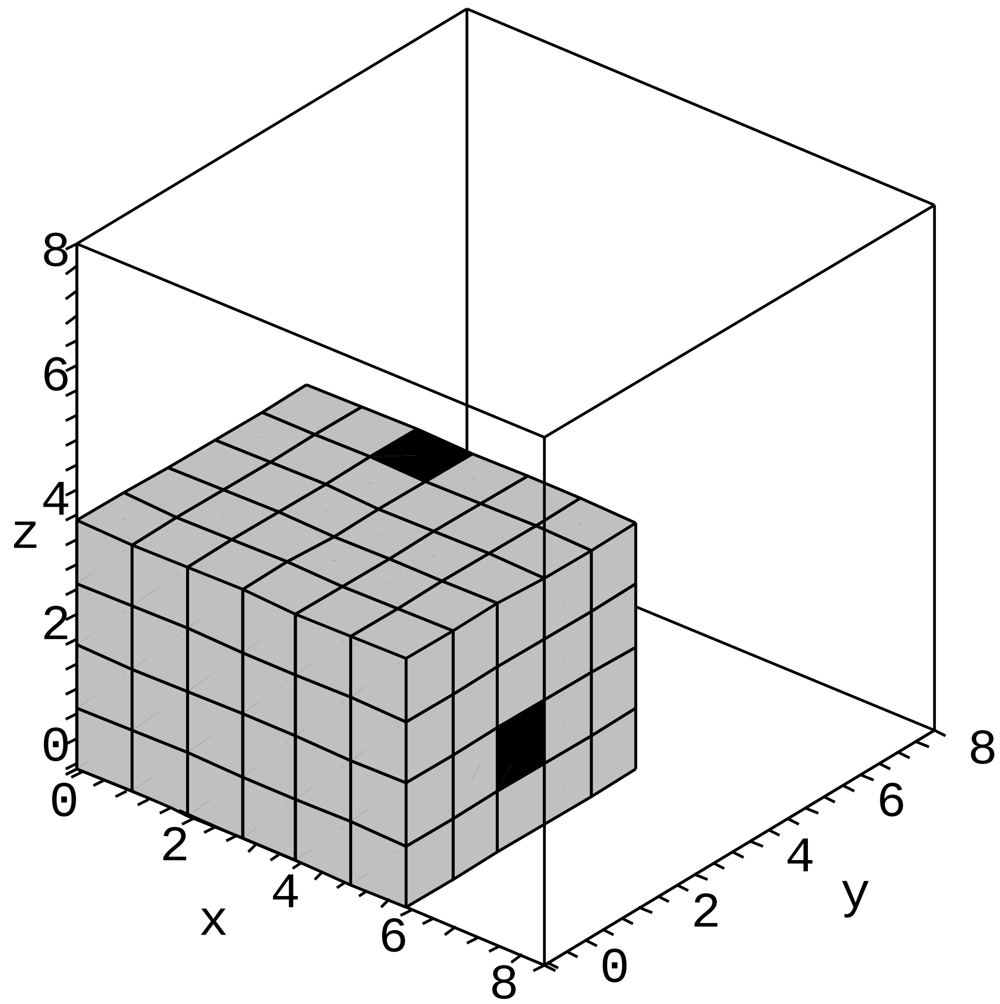
$$t_1 = x^2 \qquad t_3 = xy^3$$

Illustration (2D)



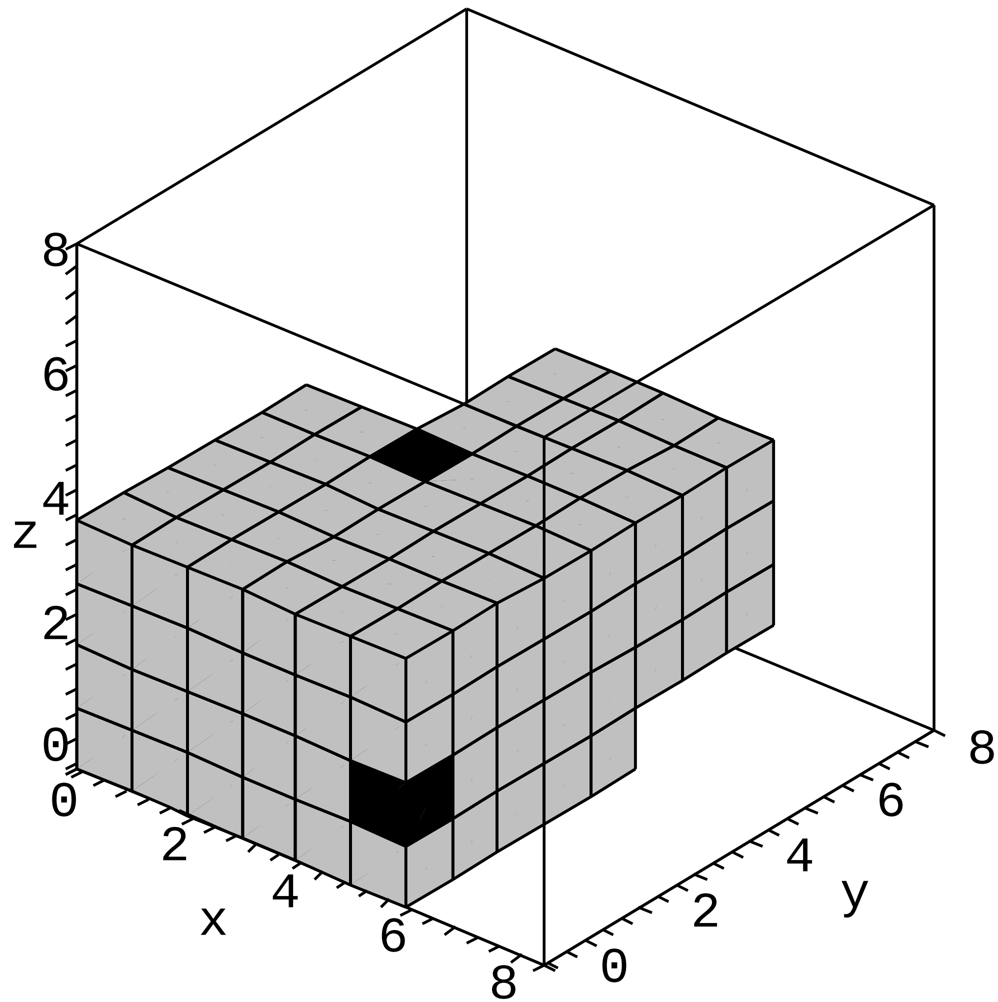
$$t_1 = x^2 \qquad\qquad t_3 = y^3$$

Illustration (3D, share all)



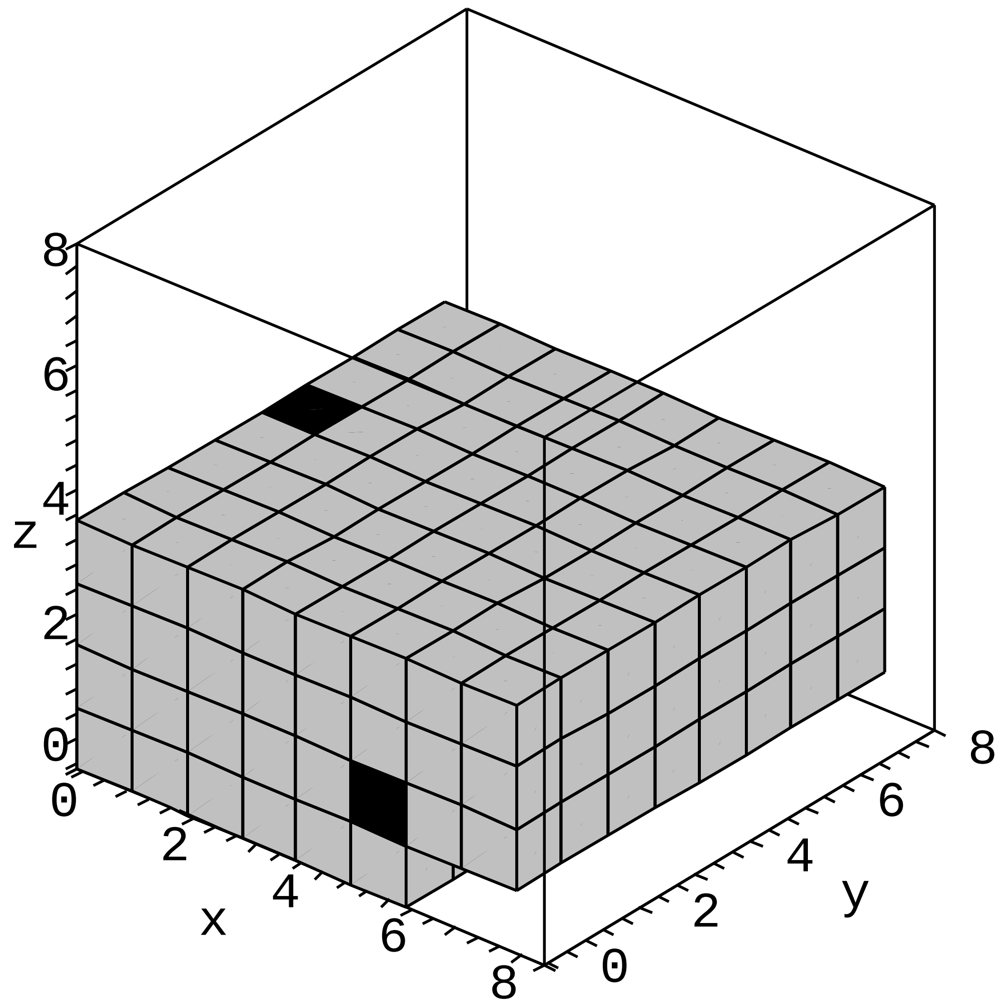
$$t_1 = x^5 y^2 z \qquad t_3 = x^2 y^4 z^3$$

Illustration (3D, share x, z)



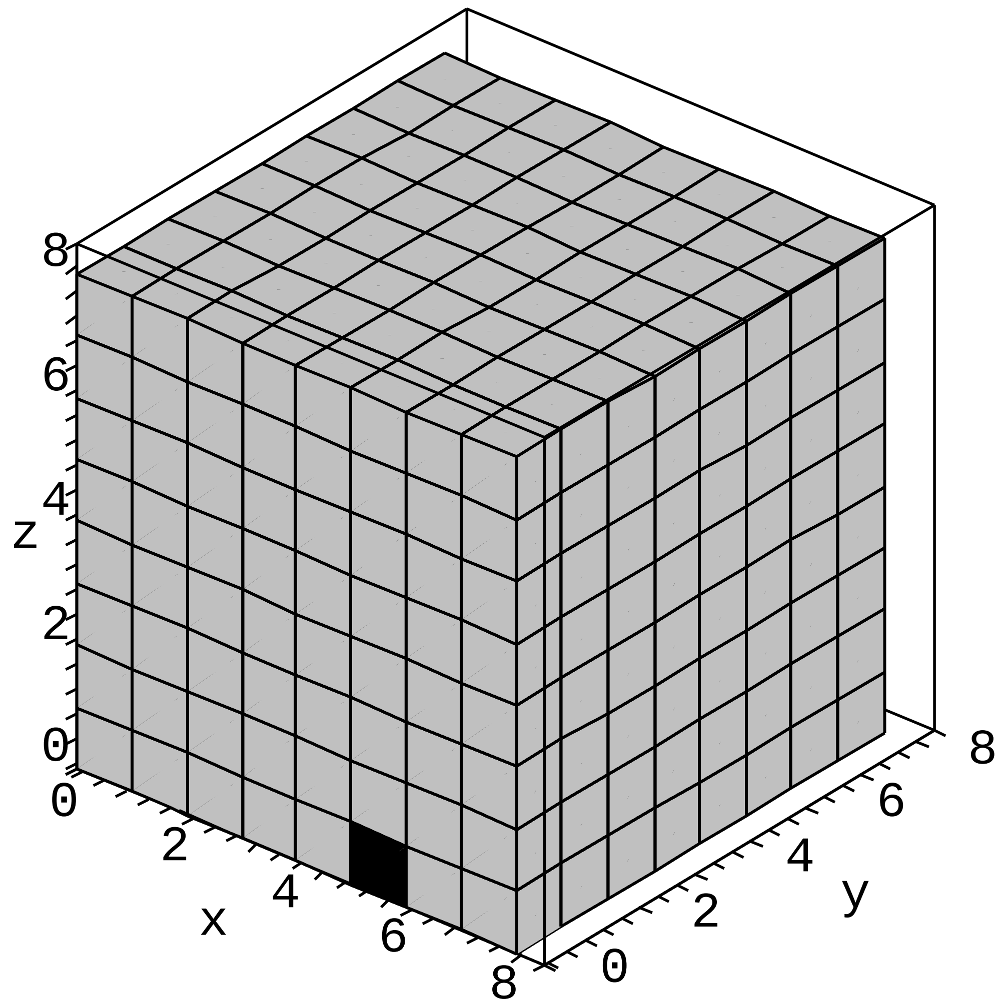
$t_1 = x^5 z \qquad t_3 = x^2 y^4 z^3$

Illustration (3D, share z)



$$t_1 = x^5 z \qquad t_3 = y^4 z^3$$

Illustration (3D, share none)



$$t_1 = x^5 \qquad t_3 = y^4 z^3$$

Quantifier alert!!!

Last theorem **does not apply**
to #lts $=$ 3, #polys $=$ 4 !!!
(#lts $<$ #polys)

Example:

$$f_1 = wx + y \quad f_2 = wy \quad f_3 = wz \quad f_4 = y^2$$

- $\mathbf{S}_{\succ}(f_1, f_2) = y^2 = f_4$
- $\mathbf{S}_{\succ}(f_2, f_3) = 0$
- BUT... $\mathbf{S}_{\succ}(f_1, f_3) = yz$

$\therefore$ We cannot skip $\mathbf{S}_{\succ}(f_1, f_3)$ for $F = (f_1, f_2, f_3, f_4)$!

Analysis of Answer

What benefit?

- 100,000 triplets (t_1, t_2, t_3)
- random exponents (uniform distribution)
- maximum degree of each indeterminate: 10
- Order critical pairs by ascending lcm
- Does third critical pair satisfy:
  - BC?
  - EC?

What benefit? lex

Chained Polynomial Skips

vars	BC	EC - BC	EC / BC
3	53294	7080	1.13
4	42542	6086	1.14
5	34633	4697	1.14
6	28310	3664	1.13

- 100,000 triplets (t_1, t_2, t_3)
- maximum degree of each indeterminate: 10
- ordered by ascending lcm, lex order

What benefit? tdeg

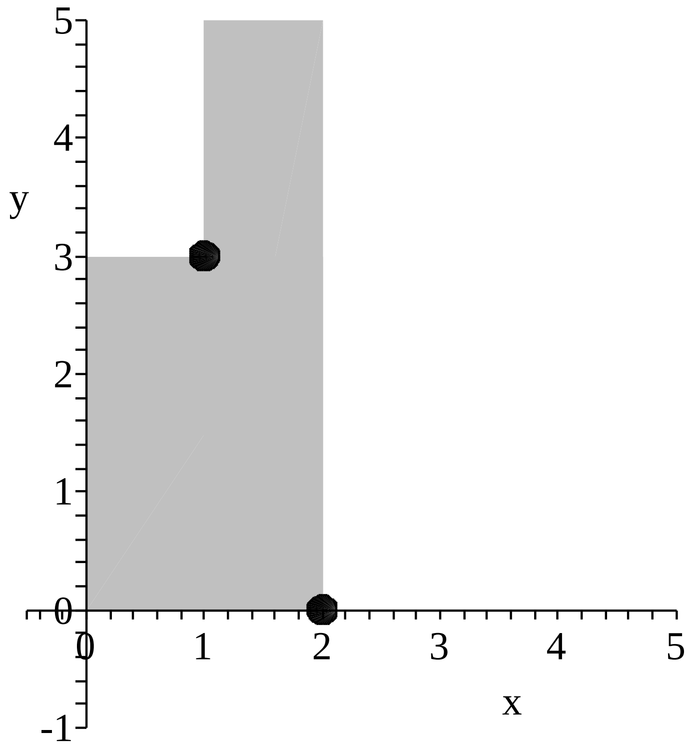
Chained Polynomial Skips

vars	BC	EC - BC	EC / BC
3	53319	6984	1.13
4	42478	5978	1.14
5	34452	4616	1.13
6	28216	3550	1.13

- 100,000 triplets (t_1, t_2, t_3)
- maximum degree of each indeterminate: 10
- ordered by ascending lcm, tdeg order (grevlex)

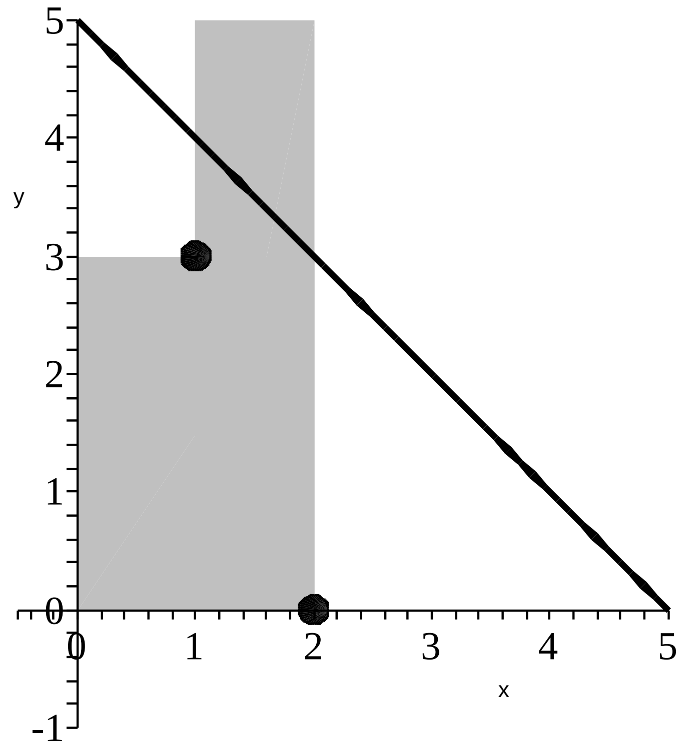
Why new rare?

Idea 1:
Appropriate t_1, t_3 rare (one lacks other's indeterminate).



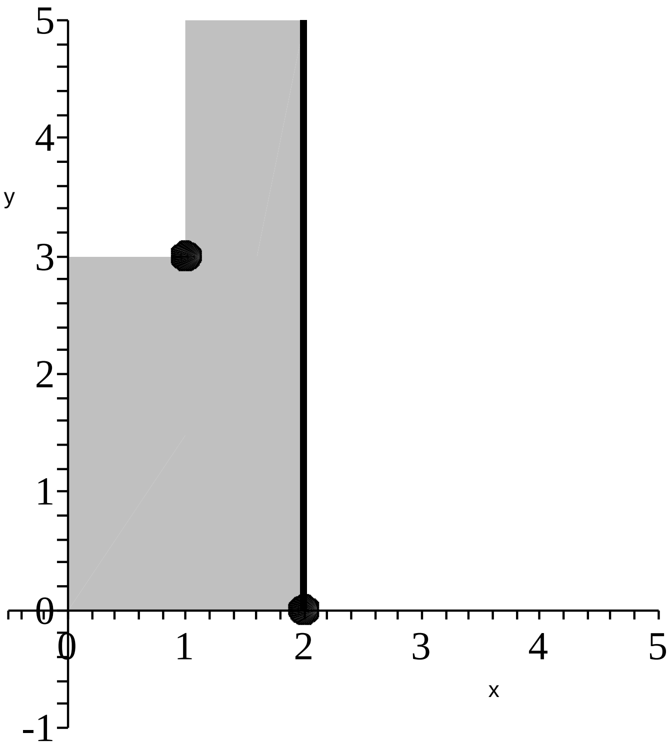
Why new so rare?

Idea 2:
Appropriate t_2 rare (order cp's by ascending lcm).



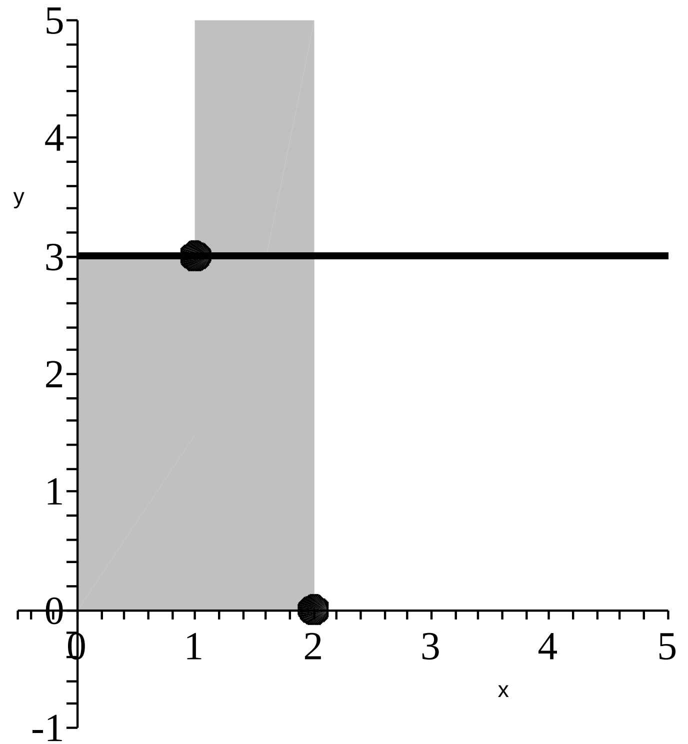
Why new so rare?

Idea 2:
Appropriate t_2 rare (order cp's by ascending lcm).



Why new so rare?

Idea 2:
Appropriate t_2 rare (order cp's by ascending lcm).



Future direction

Generalization of criteria:

- #leading terms = # polynomials > 3
- What leading terms exploit gcd fully?
- Generalized criteria $\equiv$ GB decision?

The end

Thank you!