When can we skip S-polynomial reduction?

(3 polynomials)

Hoon Hong Jack Perry

hong@ncsu.edu jeperry@ncsu.edu

8th September 2004

North Carolina State University

Partially supported by NSF 53344

Motivation

- Gröbner bases $\longrightarrow$ S-polynomial reductions to 0
- Reduction: computationally expensive
- So, we would like to skip whenever possible
- *WHEN?*

When can we skip S-polynomial reduction?

S-polynomials

Definition:

$$\mathbf{S}_{\succ}(f,g) = \frac{\mathbf{lcm}\left(\mathbf{lt}_{\succ}(f), \mathbf{lt}_{\succ}(g)\right)}{\mathbf{lm}_{\succ}(f)} \cdot f - \frac{\mathbf{lcm}\left(\mathbf{lt}_{\succ}(f), \mathbf{lt}_{\succ}(g)\right)}{\mathbf{lm}_{\succ}(g)} \cdot g$$

Reduction

“Get remainder”

Reduction

"Get remainder"

$$g = h{\color{blue}f} + r$$

$$\downarrow$$

$$g \longrightarrow_{\color{blue}f}^{*} r$$

Reduction

"Get remainder"

$$g = h_1 f_1 + h_2 f_2 + h_3 f_3 + r$$

$$\downarrow$$

$$g \longrightarrow_F^* r$$

where $F = (f_1, f_2, f_3)$

Question, restated

When can we skip S-polynomial reduction?

Previous Results

- Buchberger, 1965

$$\mathbf{gcd}\left(\widehat{f}_1, \widehat{f}_3\right) = 1 \quad \Rightarrow \quad \mathbf{S}_{13} \rightarrow_F^* 0 \qquad \text{(BC1)}$$

Previous Results

- Buchberger, 1965

  $$\mathbf{gcd}\left(\widehat{f_1}, \widehat{f_3}\right) = 1 \quad \Rightarrow \quad \mathbf{S}_{13} \rightarrow_F^* 0 \qquad \text{(BC1)}$$

- Buchberger, 1979

  $$\widehat{f_2} \mid \mathbf{lcm}\left(\widehat{f_1}, \widehat{f_3}\right)$$
  $$\Rightarrow \quad \left[\mathbf{S}_{12} \rightarrow_F^* 0 \wedge \mathbf{S}_{23} \rightarrow_F^* 0 \Rightarrow \mathbf{S}_{13} \rightarrow_F^* 0\right] \qquad \text{(BC2)}$$

Previous Results

- Buchberger, 1965

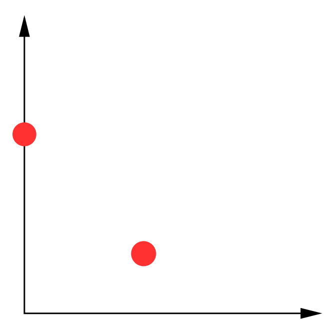
  $$\mathbf{gcd}\left(\widehat{f_1}, \widehat{f_3}\right) = 1 \quad \Rightarrow \quad \mathbf{S}_{13} \overset{*}{\underset{F}{\longrightarrow}} 0 \qquad \text{(BC1)}$$

- Buchberger, 1979

  $$\widehat{f_2} \mid \mathbf{lcm}\left(\widehat{f_1}, \widehat{f_3}\right)$$

  $$\Rightarrow \quad \left[\mathbf{S}_{12} \overset{*}{\underset{F}{\longrightarrow}} 0 \wedge \mathbf{S}_{23} \overset{*}{\underset{F}{\longrightarrow}} 0 \Rightarrow \mathbf{S}_{13} \overset{*}{\underset{F}{\longrightarrow}} 0\right] \qquad \text{(BC2)}$$

$$f_1 = x^2y + x^2 \qquad f_3 = y^3 + y^2$$



Previous Results

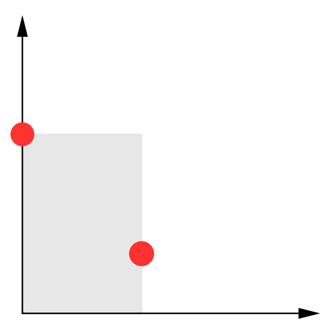
- Buchberger, 1965

  $$\mathbf{gcd}\left(\widehat{f_1}, \widehat{f_3}\right) = 1 \quad \Rightarrow \quad \mathbf{S}_{13} \xrightarrow{*}_{F} 0 \qquad \text{(BC1)}$$

- Buchberger, 1979

  $$\widehat{f_2} \mid \mathbf{lcm}\left(\widehat{f_1}, \widehat{f_3}\right) \qquad \text{(BC2)}$$
  $$\Rightarrow \quad \left[\mathbf{S}_{12} \xrightarrow{*}_{F} 0 \wedge \mathbf{S}_{23} \xrightarrow{*}_{F} 0 \Rightarrow \mathbf{S}_{13} \xrightarrow{*}_{F} 0\right]$$

$$f_1 = x^2y + x^2 \qquad f_3 = y^3 + y^2$$



Previous Results

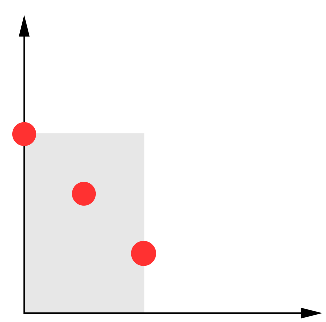
- Buchberger, 1965

  $$\mathbf{gcd}\left(\widehat{f_1}, \widehat{f_3}\right) = 1 \quad \Rightarrow \quad \mathbf{S}_{13} \to^{*}_{F} 0 \qquad \text{(BC1)}$$

- Buchberger, 1979

  $$\widehat{f_2} \mid \mathbf{lcm}\left(\widehat{f_1}, \widehat{f_3}\right) \quad \Rightarrow \quad \left[\mathbf{S}_{12} \to^{*}_{F} 0 \wedge \mathbf{S}_{23} \to^{*}_{F} 0 \Rightarrow \mathbf{S}_{13} \to^{*}_{F} 0\right] \qquad \text{(BC2)}$$

$$f_1 = x^2 y + x^2 \qquad f_3 = y^3 + y^2$$



$$f_2 = xy^2 + xy$$

Question

Are there other cases *on leading terms?*

Question

Are there other cases *on leading terms?*

$$\boxed{\text{Can skip } \mathbf{S}_{13}}$$

$$\Updownarrow$$

$$\boxed{\forall F\ \forall i = 1,2,3\ \widehat{f_i} = t_i \Rightarrow \left[\mathbf{S}_{12} \rightarrow_F^* 0 \wedge \mathbf{S}_{23} \rightarrow_F^* 0 \Rightarrow \mathbf{S}_{13} \rightarrow_F^* 0\right]}$$

Question

Are there other cases *on leading terms?*

$$\boxed{\text{Can skip } \mathbf{S}_{13}}$$

$$\Updownarrow$$

$$\boxed{\forall F\ \forall i = 1,2,3\ \widehat{f_i} = t_i \Rightarrow \left[\mathbf{S}_{12} \xrightarrow{}{}_F^* 0 \wedge \mathbf{S}_{23} \xrightarrow{}{}_F^* 0 \Rightarrow \mathbf{S}_{13} \xrightarrow{}{}_F^* 0\right]}$$

Want $\boxed{\text{CC}(t_1, t_2, t_3)} \Leftrightarrow \boxed{\text{Can skip } \mathbf{S}_{13}}$

Question

Are there other cases *on leading terms?*

$$\boxed{\text{Can skip } \mathbf{S}_{13}}$$

$$\Updownarrow$$

$$\boxed{\forall F\ \forall i = 1,2,3\ \widehat{f_i} = t_i \Rightarrow [\mathbf{S}_{12} \xrightarrow[F]{*} 0 \wedge \mathbf{S}_{23} \xrightarrow[F]{*} 0 \Rightarrow \mathbf{S}_{13} \xrightarrow[F]{*} 0]}$$

Want $\boxed{\text{CC}(t_1, t_2, t_3)} \Leftrightarrow \boxed{\text{Can skip } \mathbf{S}_{13}}$

Note:

- (BC1) $\Rightarrow$ Can skip $\mathbf{S}_{13}$
- (BC2) $\Rightarrow$ Can skip $\mathbf{S}_{13}$

Theorem (2004)

$$\boxed{\text{Can skip } \mathrm{S}_{13}}$$

$$\Updownarrow$$

$$\boxed{\text{CC}(t_1, t_2, t_3) := \text{CC1}(t_1, t_2, t_3) \text{ and } \text{CC2}(t_1, t_2, t_3)}$$

Theorem (2004)

$$\boxed{\text{Can skip } \mathrm{S}_{13}}$$

$$\Updownarrow$$

$$\boxed{\mathrm{CC}(t_1, t_2, t_3) := \mathrm{CC1}(t_1, t_2, t_3) \text{ and } \mathrm{CC2}(t_1, t_2, t_3)}$$

where

$$\mathrm{CC1}(t_1, t_2, t_3) \quad \Leftrightarrow \quad \mathbf{gcd}\,(t_1, t_3) \mid t_2 \quad \text{or} \quad t_2 \mid \mathbf{lcm}\,(t_1, t_3)$$

Theorem (2004)

$$\boxed{\text{Can skip } S_{13}}$$

$$\Updownarrow$$

$$\boxed{\text{CC}(t_1, t_2, t_3) := \text{CC1}(t_1, t_2, t_3) \text{ and } \text{CC2}(t_1, t_2, t_3)}$$

where

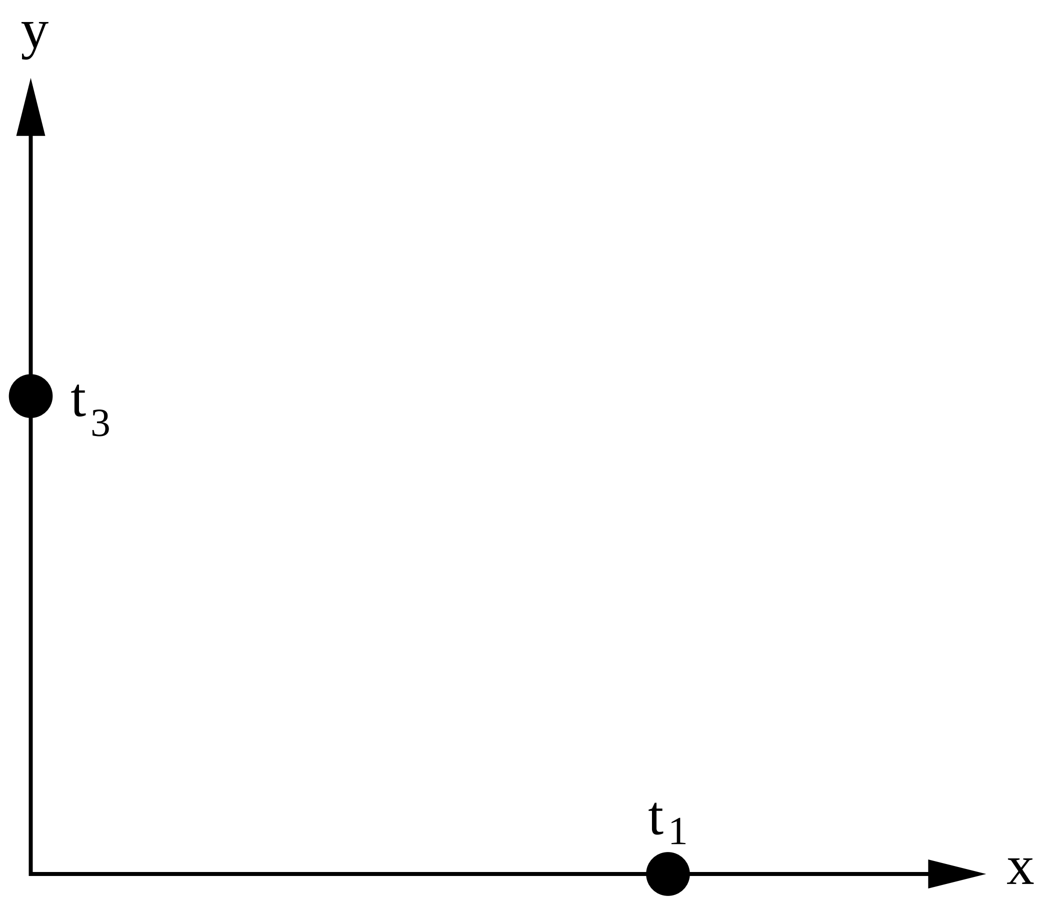
$$\text{CC1}(t_1, t_2, t_3) \quad \Leftrightarrow \quad \mathbf{gcd}\,(t_1, t_3) \mid t_2 \quad \text{or} \quad t_2 \mid \mathbf{lcm}\,(t_1, t_3)$$

$\text{CC2}(t_1, t_2, t_3) \quad \Leftrightarrow \quad$ variable-wise: BC1 or BC2

Geometrically speaking

Where t_2?

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

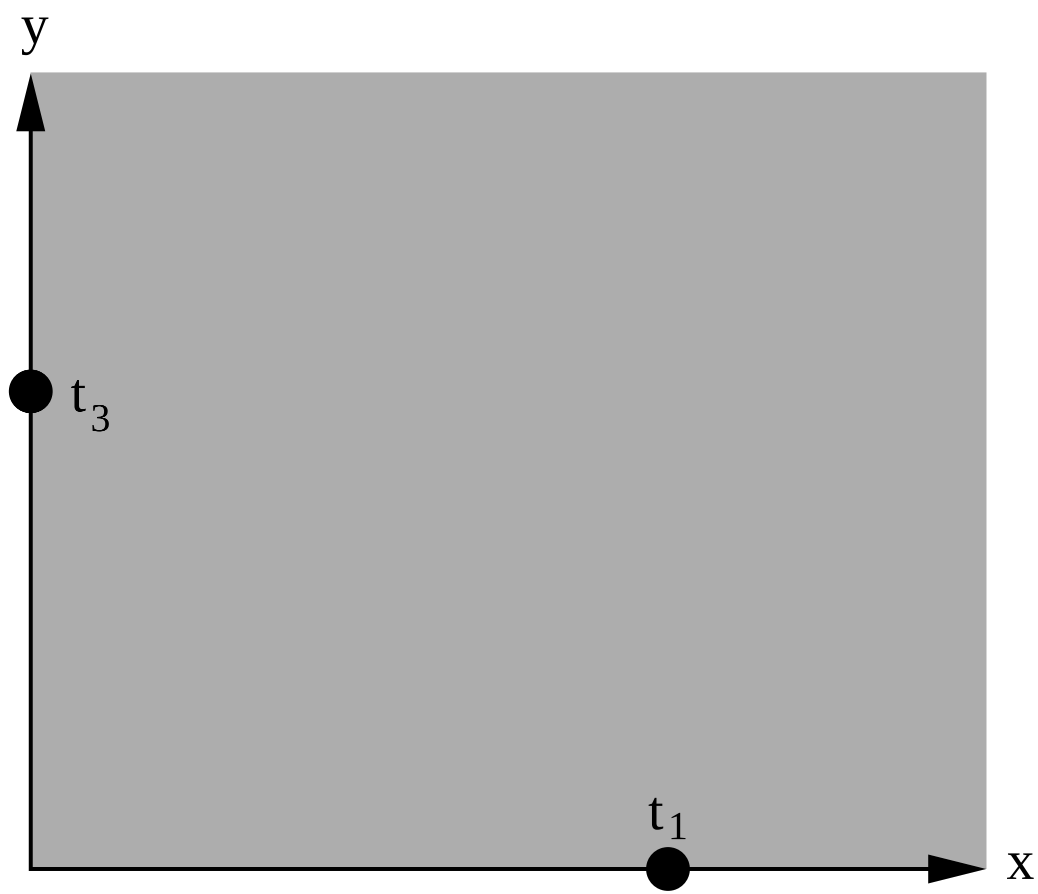


All variables relatively prime

Geometrically speaking

Where t_2?

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

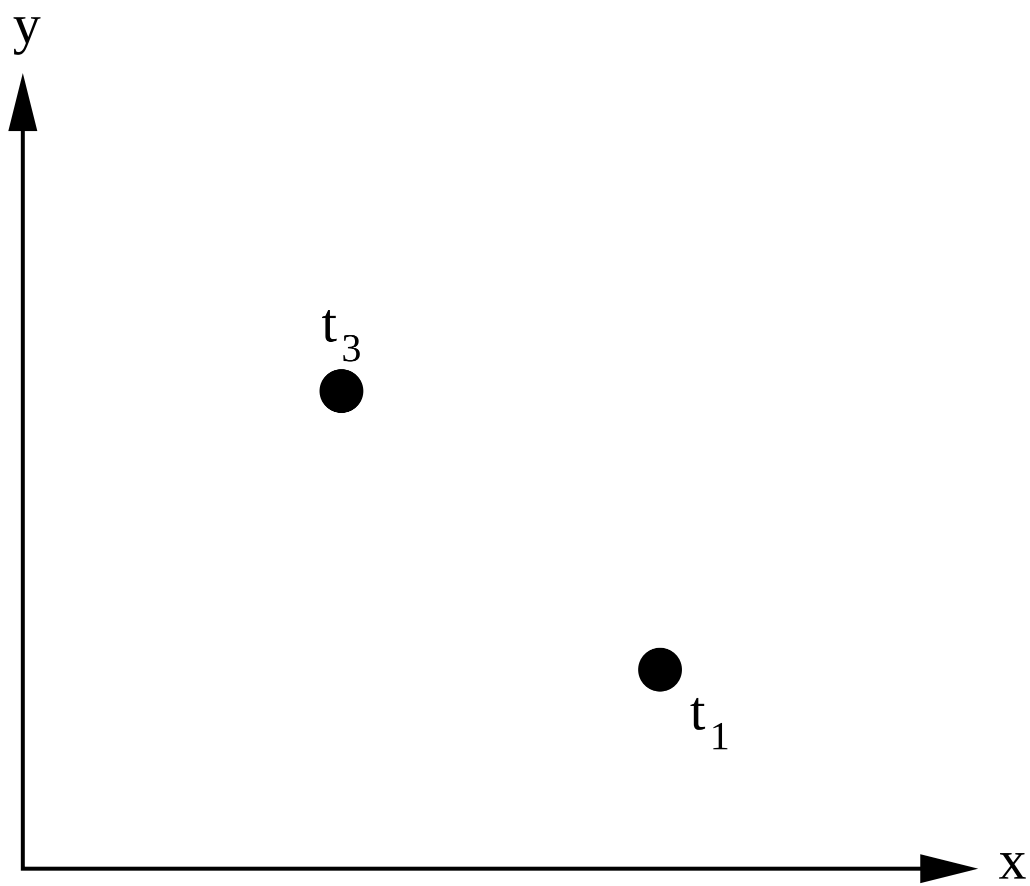


All variables relatively prime

Geometrically speaking

Where t_2?

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

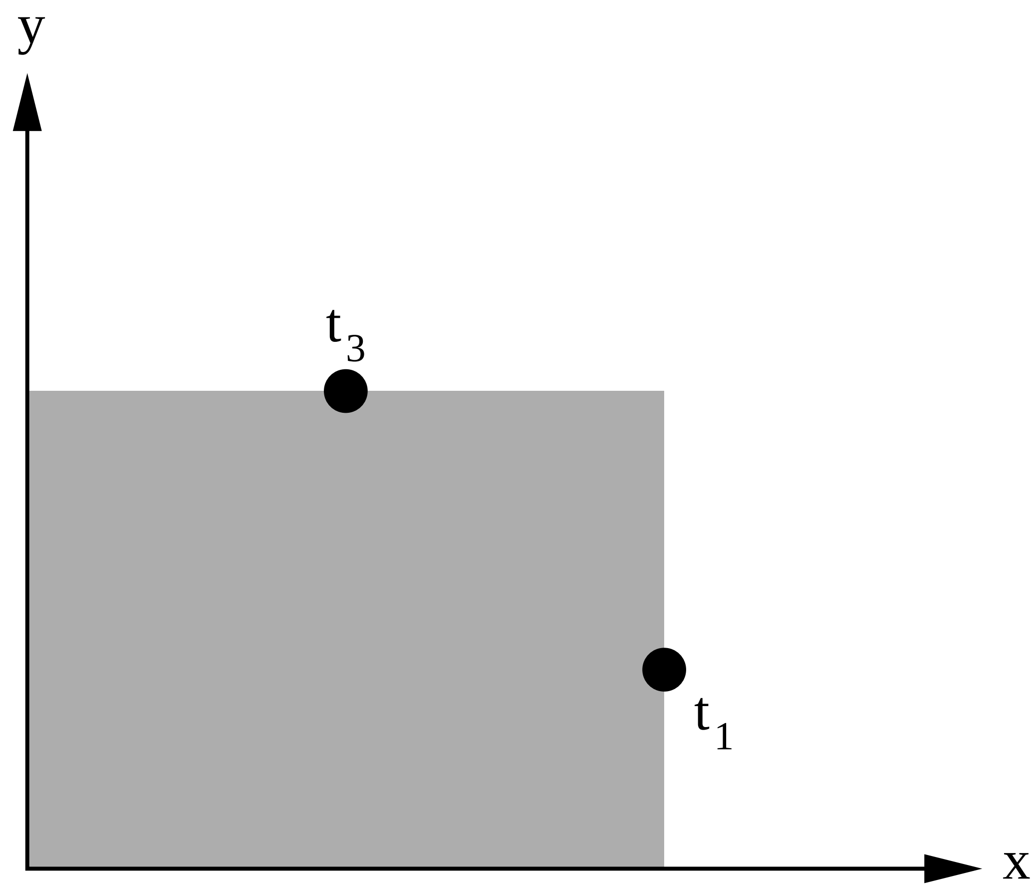


No variables relatively prime

Geometrically speaking

Where t_2?

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

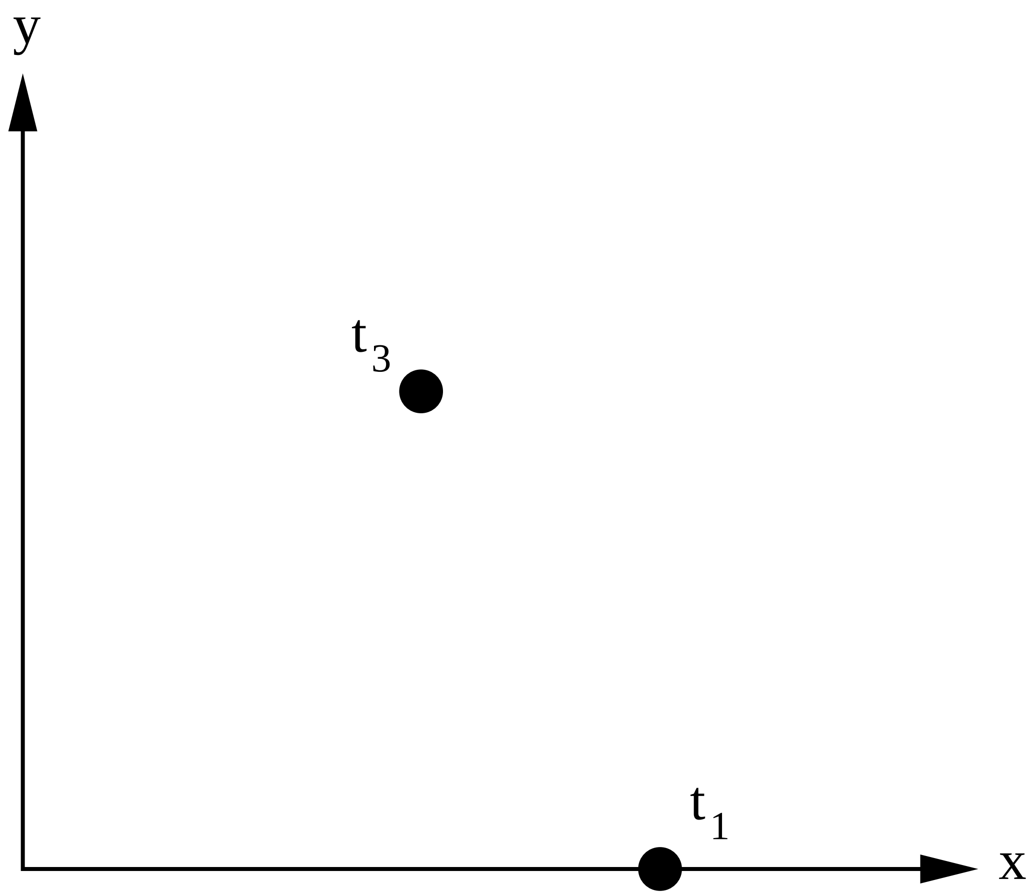


No variables relatively prime

Geometrically speaking

Where t_2?

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

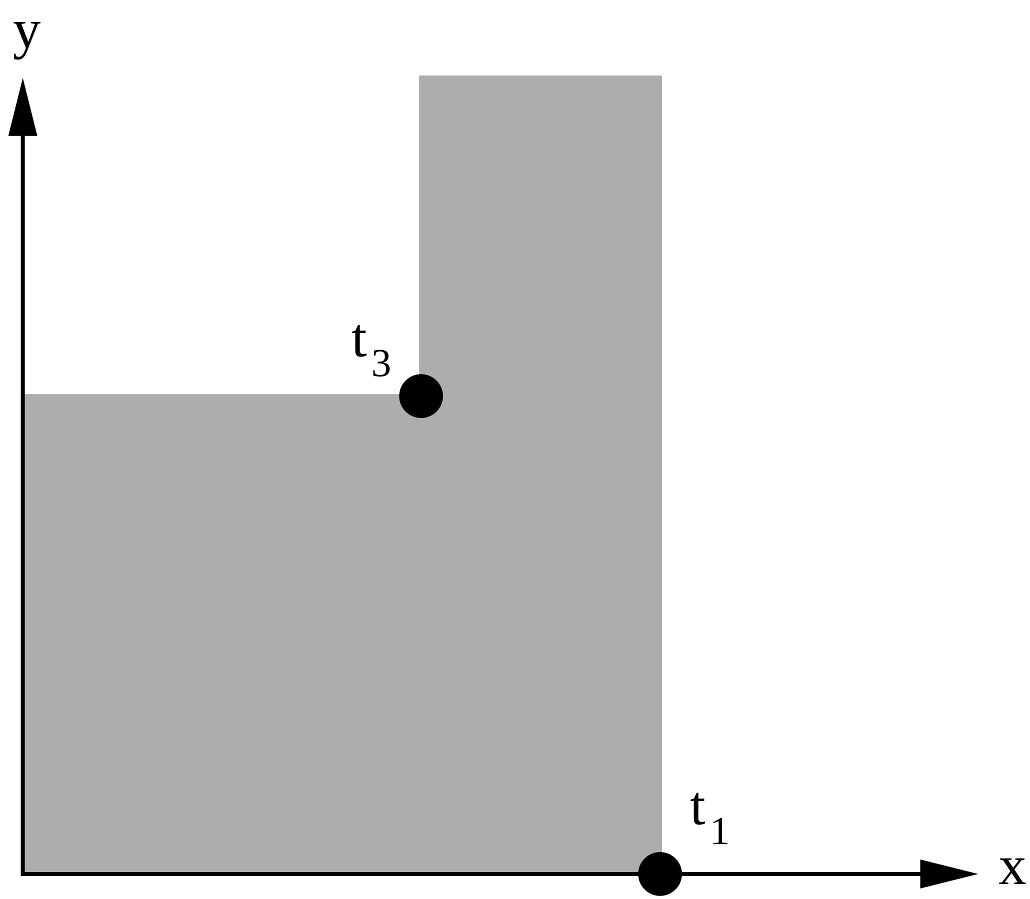


Relatively prime on y

Geometrically speaking

Where t_2?

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

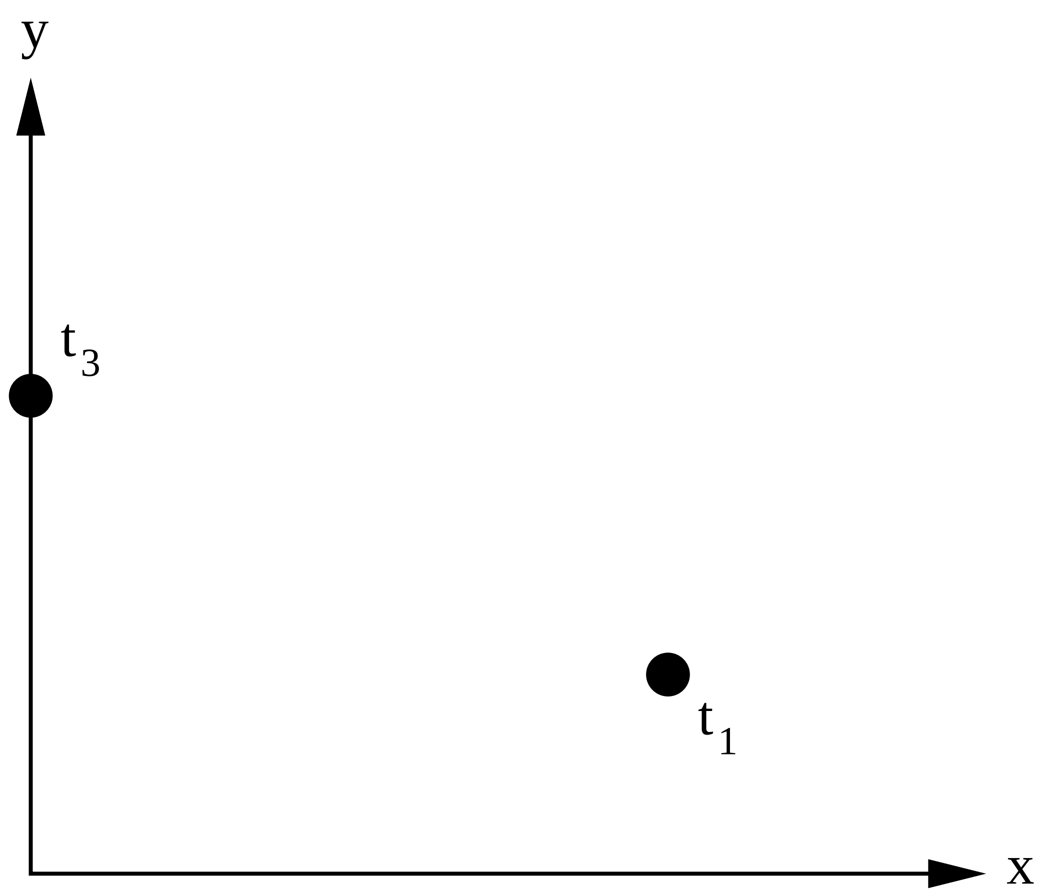


Relatively prime on y

Geometrically speaking

Where t_2?

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

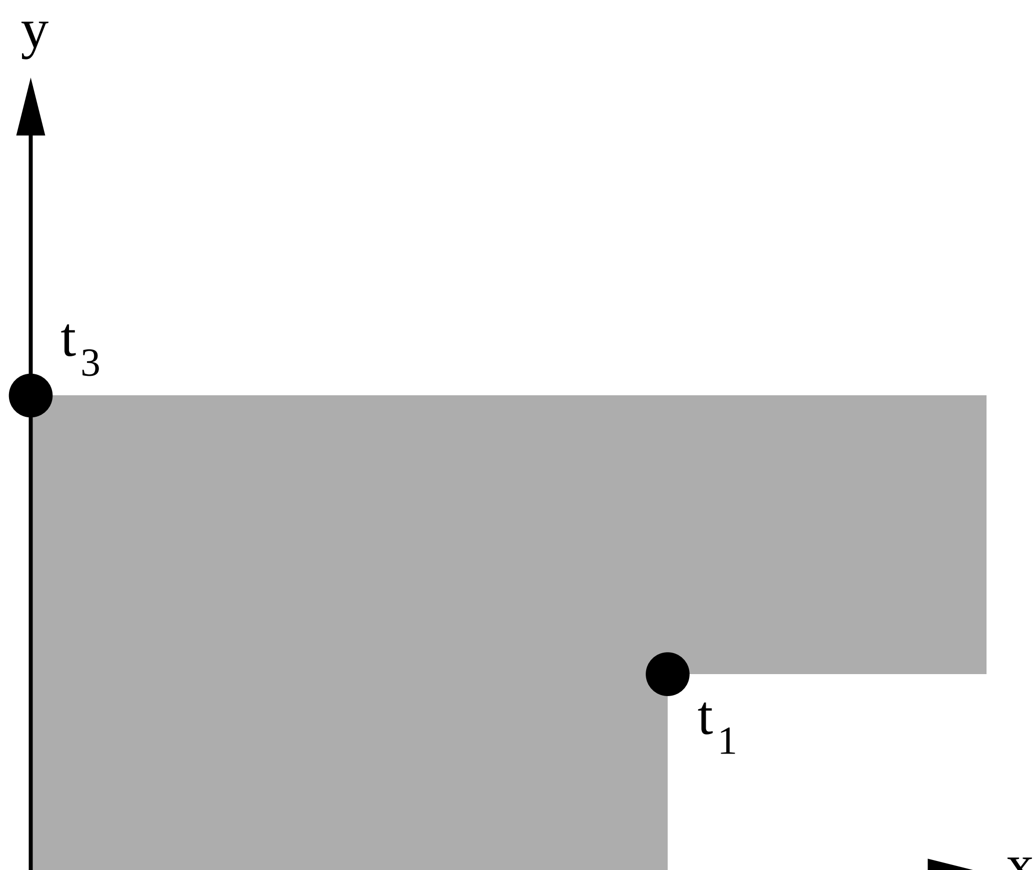


Relatively prime on x

Geometrically speaking

Where t_2?

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



Relatively prime on x

Observations

- (BC1) or (BC2) $\not\Leftarrow$ Can skip S_{13}

Observations

- (BC1) or (BC2) $\not\Leftarrow$ Can skip $\mathbf{S}_{13}$
- Gebauer and Möller (1988) and Caboara, Kreuzer and Robbiano (2002) apply (BC1), (BC2) repeatedly to obtain minimal generating set for syzygy

Observations

- (BC1) or (BC2) $\not\Leftarrow$ Can skip $\mathbf{S}_{13}$
- Gebauer and Möller (1988) and Caboara, Kreuzer and Robbiano (2002) apply (BC1), (BC2) repeatedly to obtain minimal generating set for syzygy
- Finding minimal generating set for syzygy is *not* good enough

$$\widehat{f_1} = x^2y \qquad \widehat{f_2} = xy^2 \qquad \widehat{f_3} = xz$$

$$\mathbf{S}_{12} \leftrightarrow \begin{pmatrix} y \\ -\ x^2 \\ 0 \end{pmatrix} \qquad \mathbf{S}_{23} \leftrightarrow \begin{pmatrix} 0 \\ z \\ -y^2 \end{pmatrix} \qquad \mathbf{S}_{13} \leftrightarrow \begin{pmatrix} z \\ 0 \\ xy \end{pmatrix}$$

Observations

- (BC1) or (BC2) $\not\Leftarrow$ Can skip $\mathbf{S}_{13}$
- Gebauer and Möller (1988) and Caboara, Kreuzer and Robbiano (2002) apply (BC1), (BC2) repeatedly to obtain minimal generating set for syzygy
- Finding minimal generating set for syzygy is *not* good enough

$$\widehat{f}_1 = x^2 y \qquad \widehat{f}_2 = xy^2 \qquad \widehat{f}_3 = xz$$

$$\mathbf{S}_{12} \leftrightarrow \begin{pmatrix} y \\ -\;x^2 \\ 0 \end{pmatrix} \qquad \mathbf{S}_{23} \leftrightarrow \begin{pmatrix} 0 \\ z \\ -y^2 \end{pmatrix} \qquad \mathbf{S}_{13} \leftrightarrow \begin{pmatrix} z \\ 0 \\ xy \end{pmatrix}$$

- We truly found *new* cases

Can skip $S_{13} \Rightarrow$ CC

Contrapositive: $\neg$CC $\Rightarrow$ $\neg$Can skip $\mathbf{S}_{13}$

Can skip $S_{13} \Rightarrow$ CC

Contrapositive: $\neg$CC $\Rightarrow$ $\neg$Can skip S_{13}

Assume $\neg$CC: $\neg$CC1 or $\neg$CC2

Can skip $S_{13} \Rightarrow$ CC

Contrapositive: $\neg$CC $\Rightarrow$ $\neg$Can skip S_{13}

Assume $\neg$CC: $\neg$CC1 or $\neg$CC2

$\neg$CC1:

$$f_1 = t_1 + \mathbf{gcd}\,(t_1, t_2) \quad f_2 = t_2 \quad f_3 = t_3$$

Can skip $S_{13} \Rightarrow$ CC

Contrapositive: $\neg$CC $\Rightarrow$ $\neg$Can skip $\mathbf{S}_{13}$

Assume $\neg$CC: $\neg$CC1 or $\neg$CC2

$\neg$CC2:

$$f_1 = t_1 + u \quad f_2 = t_2 \quad f_3 = t_3$$

where

$$\forall x \quad \deg_x u = \begin{cases} \deg_x t_3 & x \neq y \\ \max\left(0, \deg_x \frac{t_1 t_3}{t_2}\right) & x = y \end{cases}$$

where $\deg_y t_2 > \deg_y \mathbf{lcm}\,(t_1, t_3)$

CC $\Rightarrow$ Can skip S_{13}

$$\boxed{\begin{array}{c}\mathbf{S}_{\succ}(f_1, f_2) \longrightarrow^*_F 0 \\ \text{and} \\ \mathbf{S}_{\succ}(f_2, f_3) \longrightarrow^*_F 0\end{array}}$$

$$\boxed{\mathbf{S}_{\succ}(f_1, f_3) \longrightarrow^*_F 0}$$

CC $\Rightarrow$ Can skip S_{13}

$$\boxed{\begin{array}{c}\mathbf{S}_{\succ}(f_1, f_2) \longrightarrow^*_F 0 \\ \text{and} \\ \mathbf{S}_{\succ}(f_2, f_3) \longrightarrow^*_F 0\end{array}}$$

$$\boxed{\mathbf{S}_{\succ}(f_1, f_3) \longrightarrow^*_F 0}$$

$$\Downarrow$$

CC $\Rightarrow$ Can skip S_{13}

$$\boxed{\begin{array}{c}\mathbf{S}_{\succ}(f_1, f_2) \longrightarrow^*_F 0 \\ \text{and} \\ \mathbf{S}_{\succ}(f_2, f_3) \longrightarrow^*_F 0\end{array}}$$

$$\boxed{\mathbf{S}_{\succ}(f_1, f_3) \longrightarrow^*_F 0}$$

$$\Downarrow$$

$$\boxed{\begin{array}{c}\mathbf{S}_{\succ}(c_1, c_2) \longrightarrow^*_C 0 \\ \text{and} \\ \mathbf{S}_{\succ}(c_2, c_3) \longrightarrow^*_C 0\end{array}}$$

... where $C = (c_1, c_2, c_3)$ are cofactors of $\mathbf{gcd}(f_1, f_2, f_3)$

CC $\Rightarrow$ Can skip S_{13}

$$\boxed{\begin{array}{c}\mathbf{S}_{\succ}(f_1, f_2) \longrightarrow^*_F 0 \\ \text{and} \\ \mathbf{S}_{\succ}(f_2, f_3) \longrightarrow^*_F 0\end{array}} \qquad \boxed{\mathbf{S}_{\succ}(f_1, f_3) \longrightarrow^*_F 0}$$

$$\Downarrow$$

$$\boxed{\begin{array}{c}\mathbf{S}_{\succ}(c_1, c_2) \longrightarrow^*_C 0 \\ \text{and} \\ \mathbf{S}_{\succ}(c_2, c_3) \longrightarrow^*_C 0\end{array}} \quad \overset{\text{CC}}{\Longrightarrow} \quad \boxed{\mathbf{S}_{\succ}(c_1, c_3) \longrightarrow^*_C 0}$$

... where $C = (c_1, c_2, c_3)$ are cofactors of $\mathbf{gcd}(f_1, f_2, f_3)$

CC $\Rightarrow$ Can skip S_{13}

$$\boxed{\begin{array}{c}\mathbf{S}_{\succ}\left(f_1, f_2\right) \longrightarrow_F^* 0 \\ \text{and} \\ \mathbf{S}_{\succ}\left(f_2, f_3\right) \longrightarrow_F^* 0\end{array}} \qquad \boxed{\mathbf{S}_{\succ}\left(f_1, f_3\right) \longrightarrow_F^* 0}$$

$$\Downarrow \qquad\qquad\qquad\qquad \Uparrow$$

$$\boxed{\begin{array}{c}\mathbf{S}_{\succ}\left(c_1, c_2\right) \longrightarrow_C^* 0 \\ \text{and} \\ \mathbf{S}_{\succ}\left(c_2, c_3\right) \longrightarrow_C^* 0\end{array}} \quad \overset{\text{CC}}{\Longrightarrow} \quad \boxed{\mathbf{S}_{\succ}\left(c_1, c_3\right) \longrightarrow_C^* 0}$$

... where $C = \left(c_1, c_2, c_3\right)$ are cofactors of $\mathbf{gcd}\left(f_1, f_2, f_3\right)$

CC $\Rightarrow$ Can skip S_{13}

$$
\begin{tikzcd}
\boxed{\begin{array}{c} \mathbf{S}_{\succ}(f_1, f_2) \longrightarrow^*_F 0 \\ \text{and} \\ \mathbf{S}_{\succ}(f_2, f_3) \longrightarrow^*_F 0 \end{array}} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \boxed{\mathbf{S}_{\succ}(f_1, f_3) \longrightarrow^*_F 0} \\
\boxed{\begin{array}{c} \mathbf{S}_{\succ}(c_1, c_2) \longrightarrow^*_C 0 \\ \text{and} \\ \mathbf{S}_{\succ}(c_2, c_3) \longrightarrow^*_C 0 \end{array}} \arrow[r, Rightarrow, "\text{CC}"] & \boxed{\mathbf{S}_{\succ}(c_1, c_3) \longrightarrow^*_C 0} \arrow[u, Rightarrow]
\end{tikzcd}
$$

... where $C = (c_1, c_2, c_3)$ are cofactors of $\mathbf{gcd}\,(f_1, f_2, f_3)$

Another view

Recall: $\boxed{\text{Can skip } \mathbf{S}_{13}} \Leftrightarrow \boxed{\forall F \ \ldots\ \mathbf{S}_{13} \rightarrow_F^* 0}$

Another view

Recall: $\boxed{\text{Can skip } \mathrm{S}_{13}} \Leftrightarrow \boxed{\forall F \ \ldots\ \mathrm{S}_{13} \longrightarrow^{*}_{F} 0}$

Main Theorem: $\boxed{\text{Can skip } \mathrm{S}_{13}} \Leftrightarrow \boxed{\text{CC}}$

Another view

Recall: $\boxed{\text{Can skip } \mathbf{S}_{13}} \Leftrightarrow \boxed{\forall F \ \ldots\ \mathbf{S}_{13} \to_F^* 0}$

Main Theorem: $\boxed{\text{Can skip } \mathbf{S}_{13}} \Leftrightarrow \boxed{\text{CC}}$

Recall counterexamples: $\boxed{\text{CC}}$

$$\Leftrightarrow \boxed{F = (t_1 + u, t_2, t_3) \Rightarrow \ldots \mathbf{S}_{13} \to_F^* 0}$$

Another view

Recall: $\boxed{\text{Can skip } \mathbf{S}_{13}} \Leftrightarrow \boxed{\forall F \ \ldots\ \mathbf{S}_{13} \to^*_F 0}$

Main Theorem: $\boxed{\text{Can skip } \mathbf{S}_{13}} \Leftrightarrow \boxed{\text{CC}}$

Recall counterexamples: $\boxed{\text{CC}}$

$\Leftrightarrow \boxed{F = (t_1 + u, t_2, t_3) \Rightarrow \ \ldots\ \mathbf{S}_{13} \to^*_F 0}$

Thus: $\boxed{\forall F \ \ldots\ \mathbf{S}_{13} \to^*_F 0} \Leftrightarrow \boxed{F = (t_1 + u, t_2, t_3) \Rightarrow \ \ldots\ \mathbf{S}_{13} \to^*_F 0}$

Another view

Recall: $\boxed{\text{Can skip } \mathbf{S}_{13}} \Leftrightarrow \boxed{\forall F \ \ldots\ \mathbf{S}_{13} \rightarrow_F^* 0}$

Main Theorem: $\boxed{\text{Can skip } \mathbf{S}_{13}} \Leftrightarrow \boxed{\text{CC}}$

Recall counterexamples: $\boxed{\text{CC}}$

$$\Leftrightarrow \boxed{F = (t_1 + u, t_2, t_3) \Rightarrow \ldots \mathbf{S}_{13} \rightarrow_F^* 0}$$

Thus: $\boxed{\forall F \ \ldots\ \mathbf{S}_{13} \rightarrow_F^* 0} \Leftrightarrow \boxed{F = (t_1 + u, t_2, t_3) \Rightarrow \ldots \mathbf{S}_{13} \rightarrow_F^* 0}$

We have eliminated $\forall$!

Summary

"When can we skip S-polynomial reduction?"

- Complete answer for three polynomials
- Four polynomials: ...?

Thank you!

Examples

Example 1:

$$\widehat{f_1} = x^2 y \qquad \widehat{f_2} = y^2 \qquad \widehat{f_3} = xz$$

Can we skip S_{13}?

Examples

Example 1:

$$\widehat{f_1} = x^2y \qquad \widehat{f_2} = y^2 \qquad \widehat{f_3} = xz$$

Can we skip $\mathbf{S}_{13}$?

No!

$$\mathbf{gcd}\left(\widehat{f_1}, \widehat{f_3}\right) \nmid \widehat{f_2} \text{ and } f_2 \nmid \mathbf{lcm}\left(\widehat{f_1}, \widehat{f_3}\right)$$

Examples

Example 1:

$$\widehat{f_1} = x^2 y \qquad \widehat{f_2} = y^2 \qquad \widehat{f_3} = xz$$

Can we skip S_{13}?

No!

$$\mathbf{gcd}\left(\widehat{f_1}, \widehat{f_3}\right) \nmid \widehat{f_2} \text{ and } f_2 \nmid \mathbf{lcm}\left(\widehat{f_1}, \widehat{f_3}\right)$$

Example 2:

$$\widehat{f_1} = x^2 y \qquad \widehat{f_2} = xy^2 \qquad \widehat{f_3} = xz$$

Can we skip S_{13}?

Examples

Example 1:

$$\widehat{f_1} = x^2y \qquad \widehat{f_2} = y^2 \qquad \widehat{f_3} = xz$$

Can we skip S_{13}?

No!

$$\mathbf{gcd}\left(\widehat{f_1}, \widehat{f_3}\right) \nmid \widehat{f_2} \text{ and } f_2 \nmid \mathbf{lcm}\left(\widehat{f_1}, \widehat{f_3}\right)$$

Example 2:

$$\widehat{f_1} = x^2y \qquad \widehat{f_2} = xy^2 \qquad \widehat{f_3} = xz$$

Can we skip S_{13}?

Yes!