Equivariant Ideals of Polynomials

Arka Ghosh

Sławek Lasota

University of Warsaw

LICS'24

$X \longleftarrow$ set of variables

$\mathbb{Q}[X] \longleftarrow$ polynomials in X with rational coefficients

$I \subseteq \mathbb{Q}[X]$ is an **ideal** if

1. $I \neq \emptyset$
2. $f, g \in I \implies f + g \in I$
3. $f \in I,\ h \in \mathbb{Q}[X] \implies h \cdot f \in I$

$X \quad \longleftarrow \quad$ set of variables

$\mathbb{Q}[X] \quad \longleftarrow \quad$ polynomials in X with rational coefficients

$I \subseteq \mathbb{Q}[X]$ is an **ideal** if

1. $I \neq \varnothing$
2. $f, g \in I \implies f + g \in I$
3. $f \in I,\ h \in \mathbb{Q}[X] \implies h \cdot f \in I$

Example

$I =$ polynomials whose coefficients sum up to 0

$$x^2 - 3y + 2x$$

$\langle G \rangle$, ideal generated by $G \subseteq \mathbb{Q}[X]$

$$||$$

smallest ideal containing G

$\langle G \rangle$, ideal generated by $G \subseteq \mathbb{Q}[X]$

||

smallest ideal containing G

Example

$I =$ polynomials whose coefficients sum up to 0 $= \langle \{1 - x \mid x \in X\} \rangle$

$\langle G \rangle$, ideal generated by $G \subseteq \mathbb{Q}[X]$

$$||$$

smallest ideal containing G

Hilbert's basis theorem

X is finite $\quad \Longrightarrow \quad$ every ideal in $\mathbb{Q}[X]$ is finitely generated

Application:

1. Zeroness of polynomial automata.
2. Reachability in reversible Petri nets.

$X \longleftarrow$ an infinite set (of variables) with some structure

$X \longleftarrow$ an infinite set (of variables) with some structure

An ideal $I \subseteq \mathbb{Q}[X]$ is **equivariant** if it is invariant under renaming of variables using automorphisms of X.

$$x^2 - yz \quad \xrightarrow{\pi} \quad \pi(x)^2 - \pi(y)\pi(z)$$

$X \longleftarrow$ an infinite set (of variables) with some structure

An ideal $I \subseteq \mathbb{Q}[X]$ is **equivariant** if it is invariant under renaming of variables using automorphisms of X.

$$x^2 - yz \quad \xrightarrow{\pi} \quad \pi(x)^2 - \pi(y)\pi(z)$$

Example

$X =$ dense linear order

automorphisms = order preserving bijections

$I =$ polynomials whose coefficients sum up to 0

equivariant ideal $\langle G \rangle$ generated by $G \subseteq \mathbb{Q}[X]$

||

the smallest equivariant ideal containing G

equivariant ideal $\langle G \rangle$ generated by $G \subseteq \mathbb{Q}[X]$

||

the smallest equivariant ideal containing G

Example

X = dense linear order

I = polynomials whose coefficients sum up to 0 = $\langle 1 - x \rangle$

for any $x \in X$

$X \longleftarrow$ an infinite set (of variables) with some structure

An ideal $I \subseteq \mathbb{Q}[X]$ is **equivariant** if it is invariant under renaming of variables using automorphisms of X.

Hilbert's basis property

Every equivariant ideal in $\mathbb{Q}[X]$ is finitely generated

Which structures have Hilbert's basis property?

$\mathrm{Fin}(X)$ = Finite induced substructures of X labelled by $\mathbb{N}$
ordered by embeddings

Example:

$X =$ dense linear order

$\mathrm{Fin}(X) = \mathbb{N}^*$, subsequence ordering

Fin(X) = Finite induced substructures of X labelled by $\mathbb{N}$
ordered by embeddings

Example:

$X =$ dense linear order

Fin(X) = $\mathbb{N}^*$, subsequence ordering

Theorem: Fin(X) is WQO and X is totally ordered $\Longrightarrow$ X has Hilbert's basis property

$\Downarrow$

Fin(X) is WQO

$\Uparrow$? Pouzet's conjecture

Cohen (1967)

X	Finite induced substructures	Hilbert's basis property
Equality domain	Finite sets	✓
Dense linear order	Finite linear orders	✓
Random graph	Finite graphs	✗

Cohen (1967) → Equality domain

Preserved by lexicographic product → Hilbert's basis property

X	Finite induced substructures	Hilbert's basis property
Equality domain	Finite sets	✓
Dense linear order	Finite linear orders	✓
Random graph	Finite graphs	✗

Equivariant Ideal Membership Problem

Input : $f \in \mathbb{Q}[X]$ and finite $G \subseteq \mathbb{Q}[X]$.

Question : Is $f \in \langle G \rangle$?

Equivariant Ideal Membership Problem

Input : $f \in \mathbb{Q}[X]$ and finite $G \subseteq \mathbb{Q}[X]$.

Question : Is $f \in \langle G \rangle$?

Theorem: Fin(X) is WQO and X is totally ordered $\Longrightarrow$ X has Hilbert's basis property

X has Hilbert's basis property $\Longrightarrow$ Fin(X) is WQO

Fin(X) is WQO $\overset{?}{\Longrightarrow}$ Fin(X) is WQO and X is totally ordered (Pouzet's conjecture)

Equivariant Ideal Membership Problem

Input : $f \in \mathbb{Q}[X]$ and finite $G \subseteq \mathbb{Q}[X]$.

Question : Is $f \in \langle G \rangle$?

Theorem: Fin(X) is WQO and X is well ordered and computable $\Longrightarrow$ Decidable

Hillar, Sullivant (2012)

X	Finite induced substructures	Decidability of ideal membership
Equality domain	Finite sets	✓
Dense linear order	Finite linear orders	✓
Random graph	Finite graphs	✗

Hillar, Sullivant (2012)

Preserved by lexicographic product

X	Finite induced substructures	Decidability of ideal membership
Equality domain	Finite sets	✓
Dense linear order	Finite linear orders	✓
Random graph	Finite graphs	✗

Applications

1. Decidability of reachability of reversible data Petri nets for equality and ordered data.

2. Increasing chains of equivariant vector subspaces stabilise.
   Bojańczyk, Klin, Moerman (LICS'21)

   $\Downarrow$

3. Decidability of zeroness of weighted register automata.
   Bojańczyk, Klin, Moerman (LICS'21)

4. Solvability of orbit-finite systems of linear equations.
   G., Hofman, Lasota (LICS'22)

Fin(X) = Finite induced substructures of X labelled by $\mathbb{N}$
ordered by embeddings

Example :

$X =$ dense linear order

Fin(X) = $\mathbb{N}^*$, subsequence ordering

Fin(X) is WQO and
X is totally ordered $\Longrightarrow$ X has Hilbert's basis property

$\Swarrow$

Fin(X) is WQO

$\Uparrow$?

Pouzet's conjecture

Previous results

On the laws of a metabelian variety.
Daniel E Cohen (1967)

Closure relations, Buchberger's algorithm, and polynomials in infinitely many variables.
Daniel E Cohen (1987)

Finite generation of symmetric ideals.
Matthias Aschenbrenner, Christopher J. Hillar (2007)

An Algorithm for Finding Symmetric Gröbner Bases in Infinite Dimensional Rings.
Matthias Aschenbrenner, Christopher J. Hillar (2008)

Finite Gröbner bases in infinite dimensional polynomial rings and applications
Christopher J. Hillar, Seth Sullivant (2012)

Equivariant Gröbner bases
Christopher J. Hillar, Robert Kroner, Anton Leykin (2016)

known before

X	Finite induced substructures	Hilbert's basis property?
Equality domain	Finite sets	✓
Dense linear order	Finite linear orders	✓
Random graph	Finite graphs	✗
Infinite dimensional vector space on finite fields	Finite dimensional vector subspaces	✗
Dense tree	Finite trees/forests	✓

known before

Preserved by lexicographic product

X	Finite induced substructures	Hilbert's basis property?
Equality domain	Finite sets	✓
Dense linear order	Finite linear orders	✓
Random graph	Finite graphs	✗
Infinite dimensional vector space on finite fields	Finite dimensional vector subspaces	✗
Dense tree	Finite trees/forests	✓

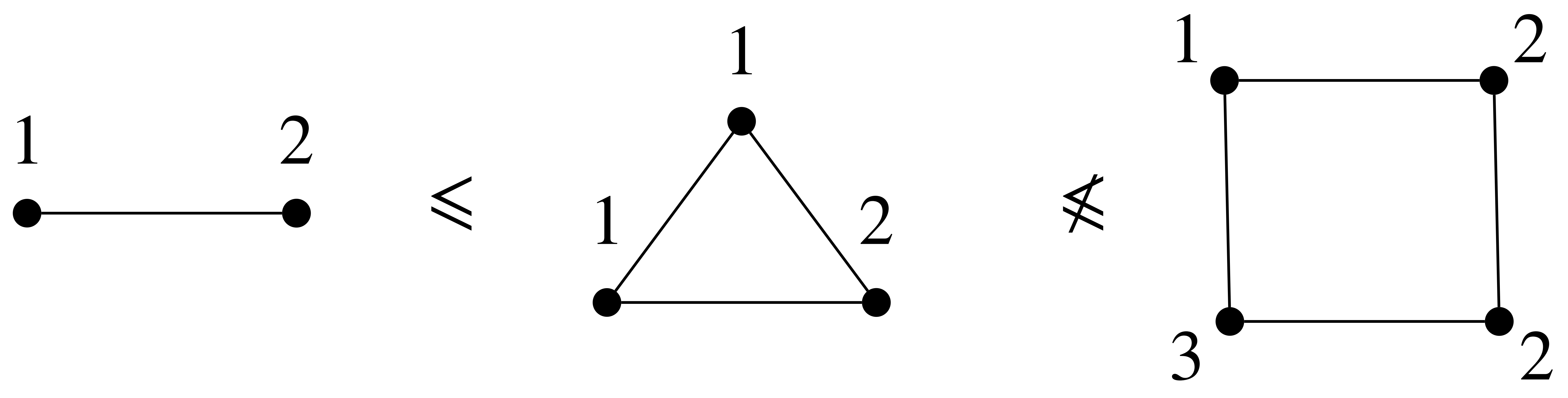
Known before

Preserved by lexicographic product

X	Finite induced substructures	Decidability of ideal membership
Equality domain	Finite sets	✓
Dense linear order	Finite linear orders	✓
Rado graph	Finite graphs	✗
Infinite dimensional vector space on finite fields	Finite dimensional vector subspaces	✗
Dense tree	Finite trees/forests	Ongoing work

$\mathrm{Fin}(X)$ = Finite induced substructures of X labelled by $\mathbb{N}$

Elements in $\mathrm{Fin}(X)$ are ordered by embeddings



$$X = \{x_1, x_2, \ldots\}$$

$$X = \{x_1, x_2, \ldots\}$$

$\langle x_1, x_2, \ldots \rangle$ is not a finitely generated ideal

$$X = \{x_1, x_2, \ldots\}$$

$\langle x_1, x_2, \ldots \rangle$ is not a finitely generated ideal

Proof by contradiction :

F, an arbitrary finite subset of $\langle x_1, x_2, \ldots \rangle$

$F' = \{x_i \mid x_i \text{ appears in some } f \in F\}$

$\langle F \rangle \subseteq \langle F' \rangle \subsetneq \langle x_1, x_2, \ldots \rangle$

$$X = \{x_1, x_2, \ldots\}$$

$\langle x_1, x_2, \ldots \rangle$ is not a finitely generated ideal

Proof by contradiction :

F, an arbitrary finite subset of $\langle x_1, x_2, \ldots \rangle$

$F' = \{x_i \mid x_i \text{ appears in some } f \in F\}$

$\langle F \rangle \subseteq \langle F' \rangle \subsetneq \langle x_1, x_2, \ldots \rangle$

We need to look at an appropiate class of ideals

X	edges of an infinite clique
$\mathrm{Emb}(X)$	injections of edges induced by injections of vertices

X

$$\left\langle \bigcup_{n\geq 3} C_n \right\rangle \text{ is not finitely generated}$$

$$C_n = \{e_1 \cdot \ldots \cdot e_n \mid e_1 \cdots e_n \text{ is a simple cycle } \}$$

X	edges of an infinite clique	X
$\mathrm{Emb}(X)$	injections of edges induced by injections of vertices	

Is this notion of ideals useful?

reachability of reversible Petri net

↓

polynomial ideal membership problem

data

reachability of reversible ^ Petri net

↓

equivariant polynomial ideal membership problem

Commutative Ring : $(R, + \,, \cdot\,)$

Commutative Ring : $(R, + , \cdot\ )$

Examples

1. Integers

2. $R[X] =$ Polynomials with variables X and coefficients from the ring R

Commutative Ring : $(R, +\ ,\ \cdot\ )$

$I \subseteq R$ is called an **ideal** if

1. $a + b \in I$ for all $a, b \in I$
2. $a \cdot c \in I$ for all $a \in I$ and $c \in R$

Examples

1. Integers
2. $R[X] =$ Polynomials with variables X and coefficients from the ring R

Commutative Ring : $(R, +, \cdot)$

$I \subseteq R$ is called an **ideal** if

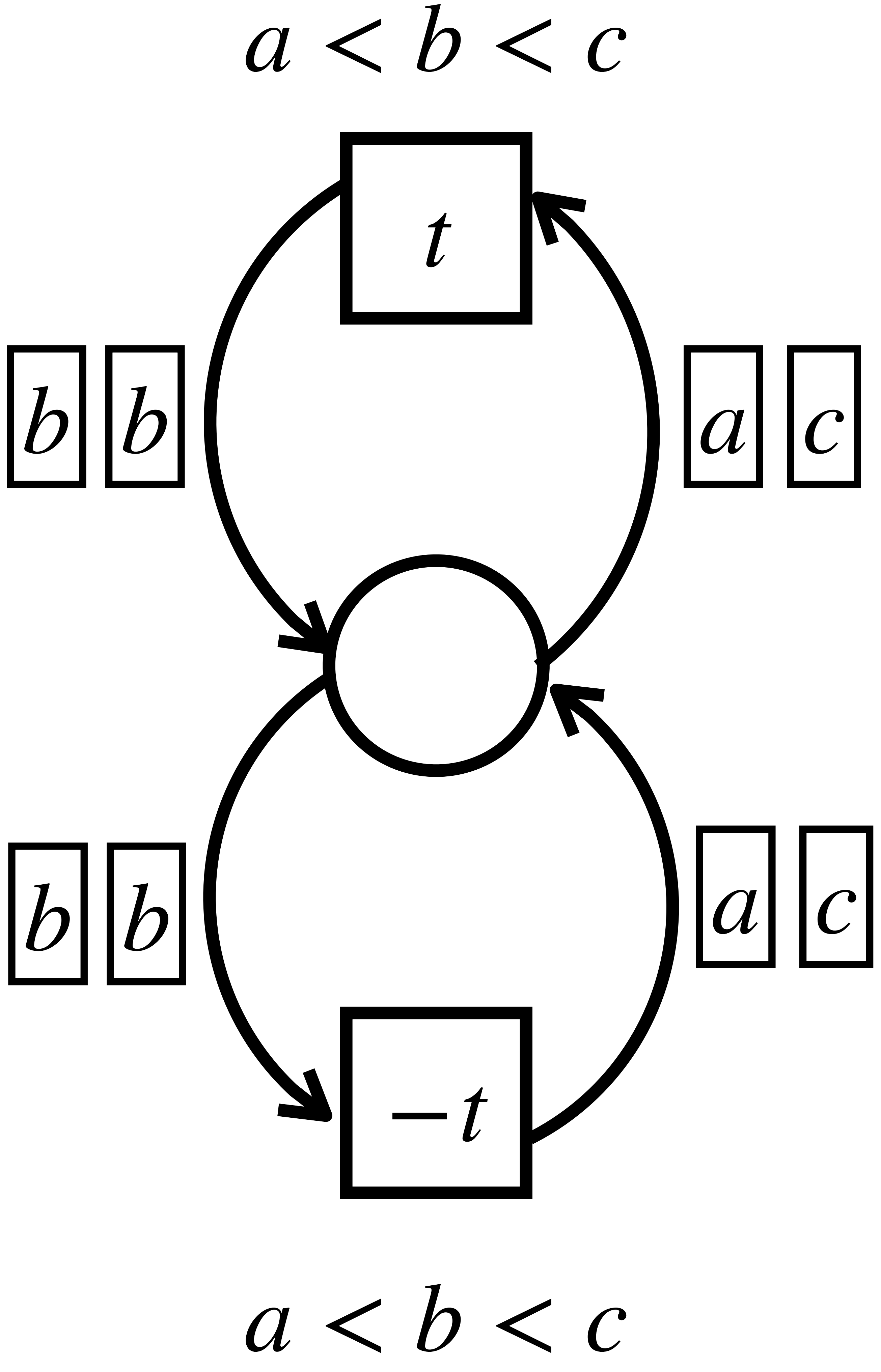
1. $a + b \in I$ for all $a, b \in I$
2. $a \cdot c \in I$ for all $a \in I$ and $c \in R$

Examples

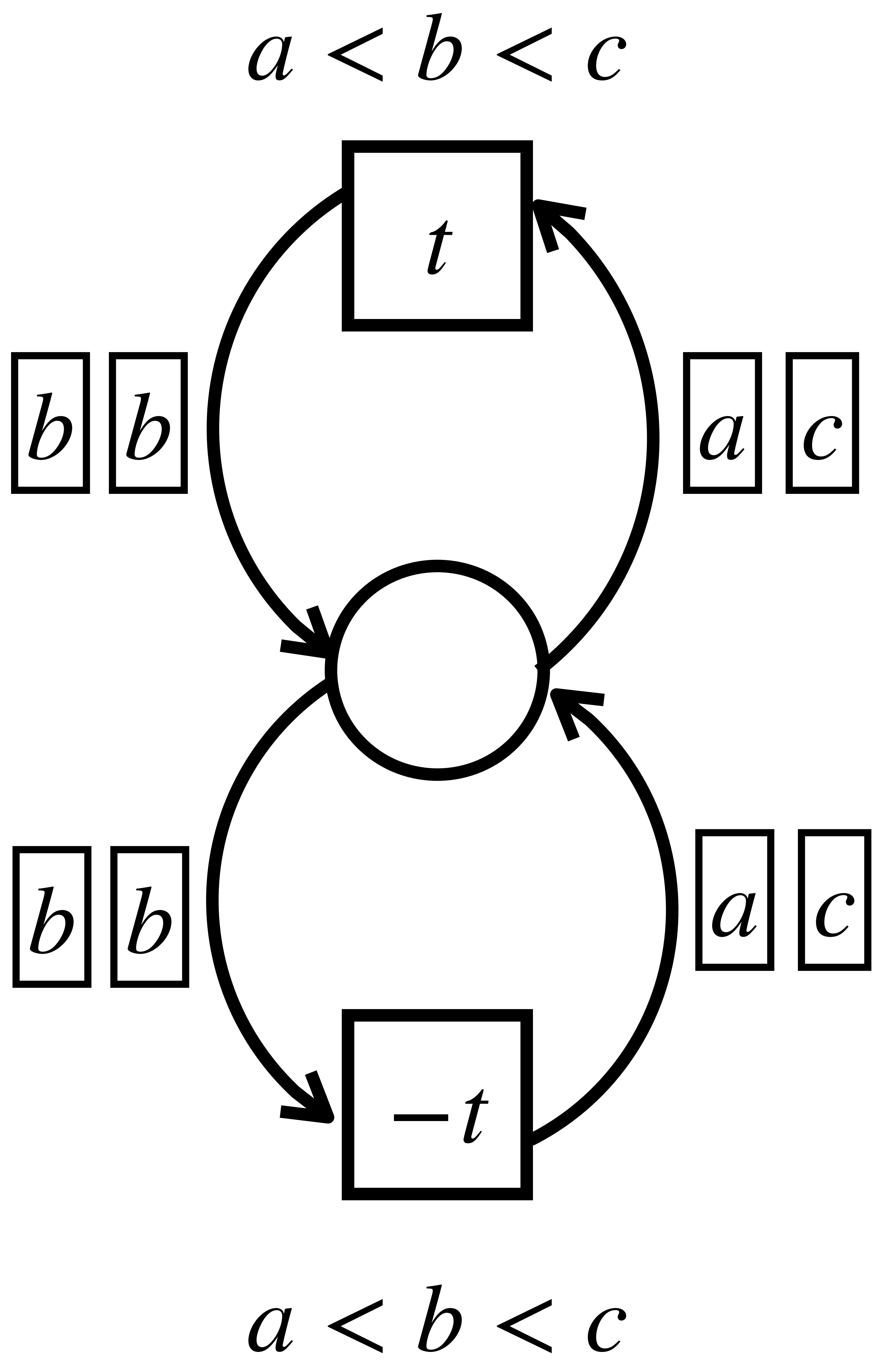
1. Integers
2. $R[X] =$ Polynomials with variables X and coefficients from the ring R

Examples

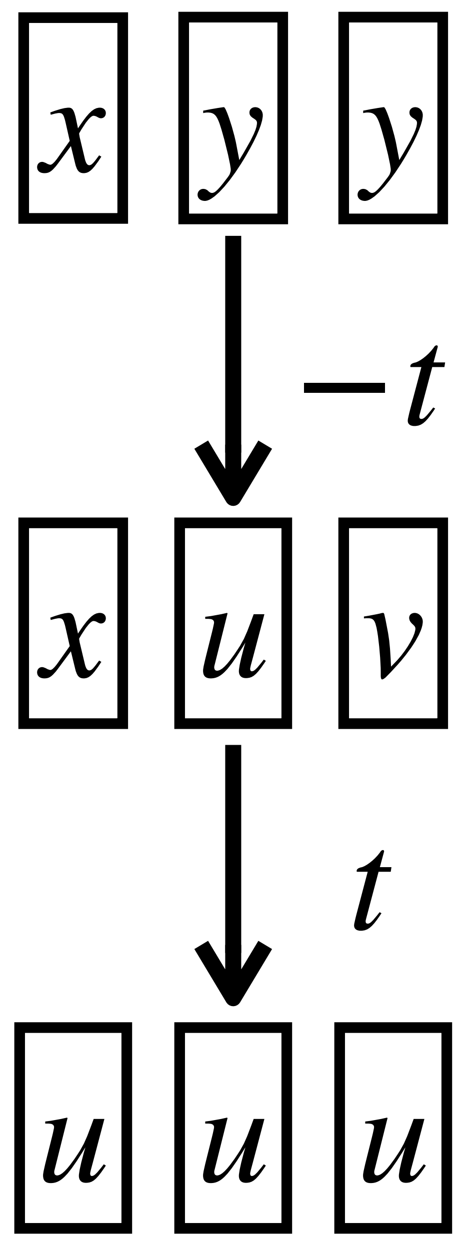
1. Even integers
2. Polynomials which vanish at $x = 0,\ y = 1$



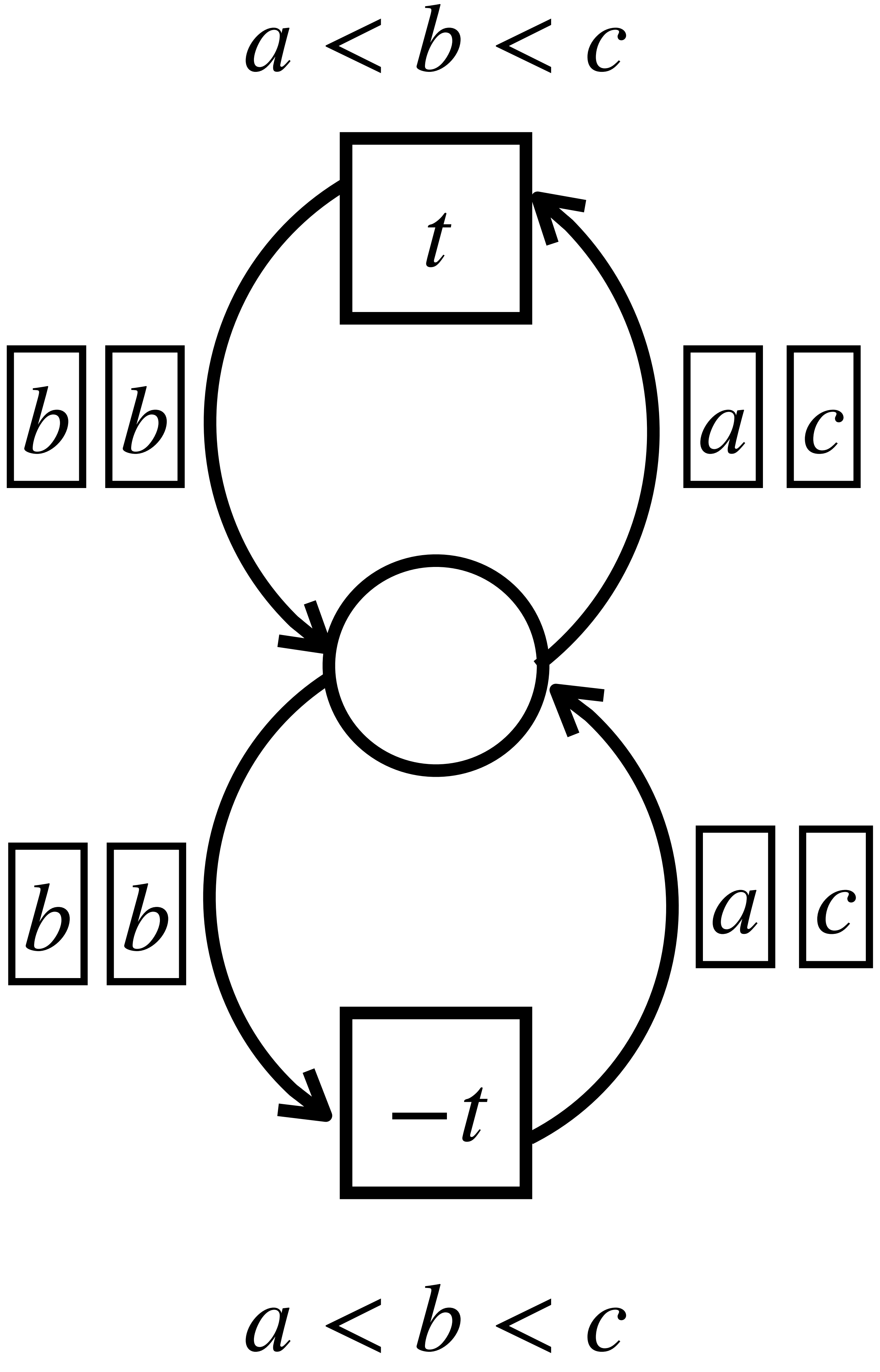
$a < b < c$
t
b b
a c
b b
a c
$-t$
$a < b < c$

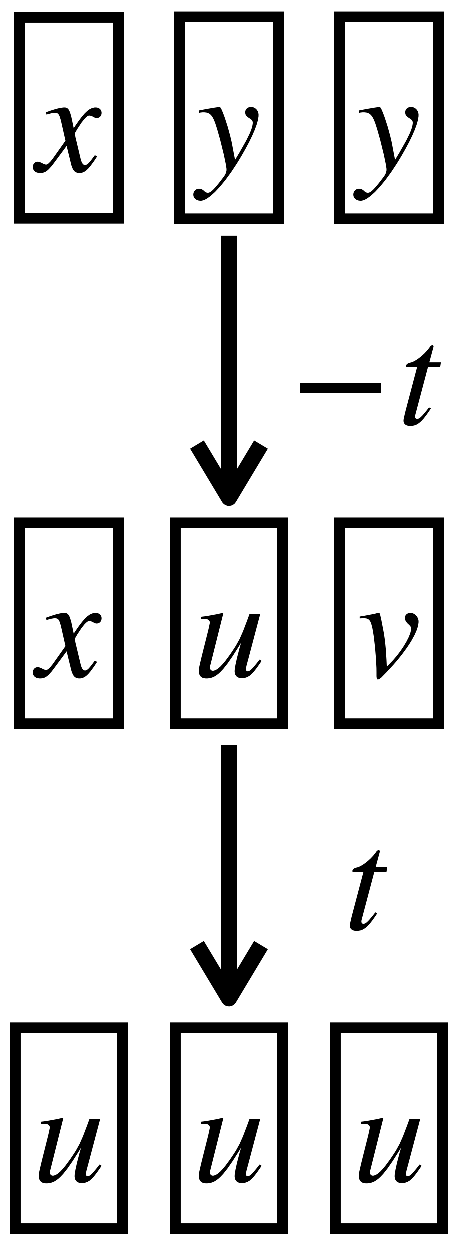


a < b < c
t
b b
a c
b b
a c
−t
a < b < c

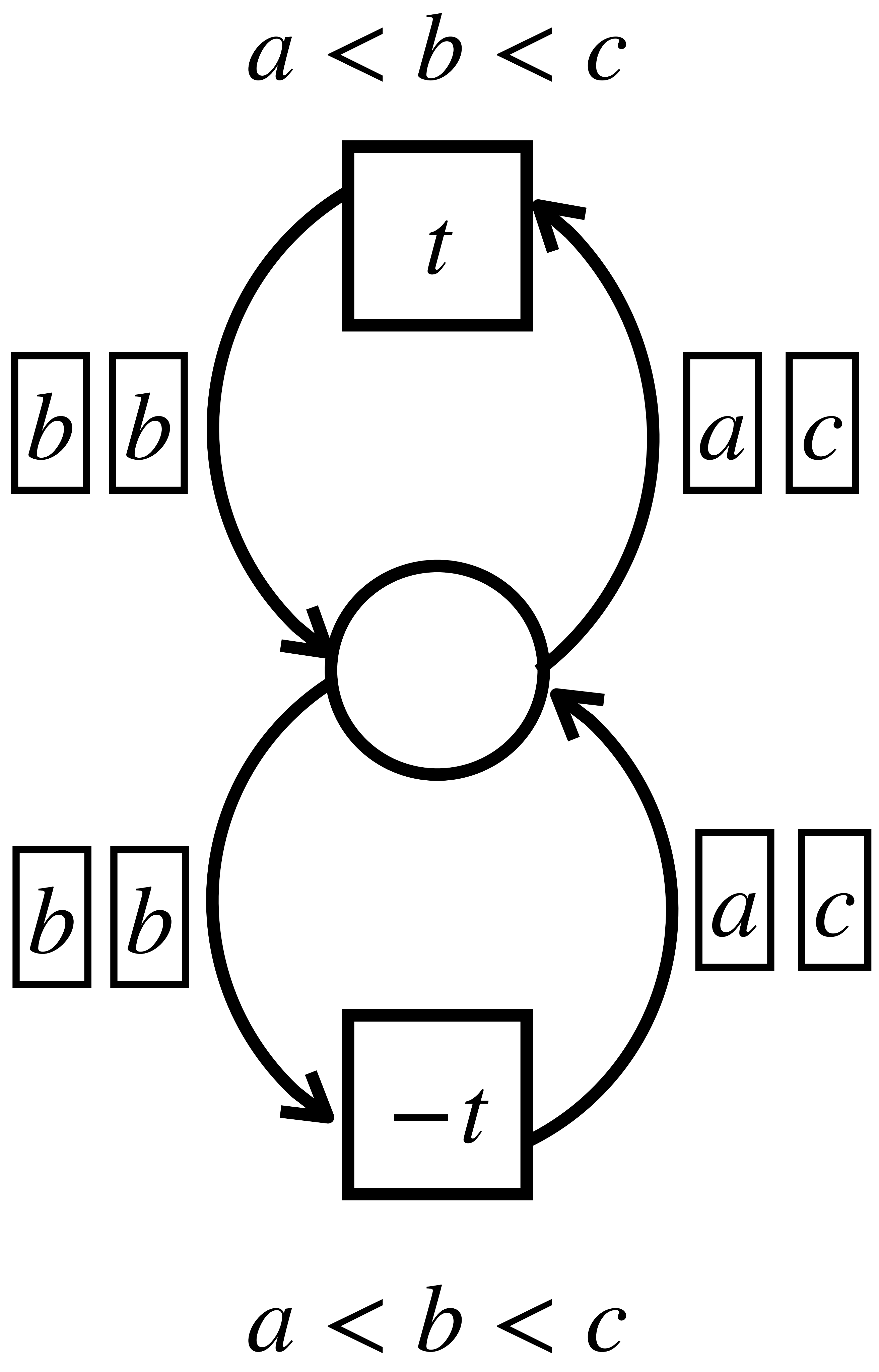


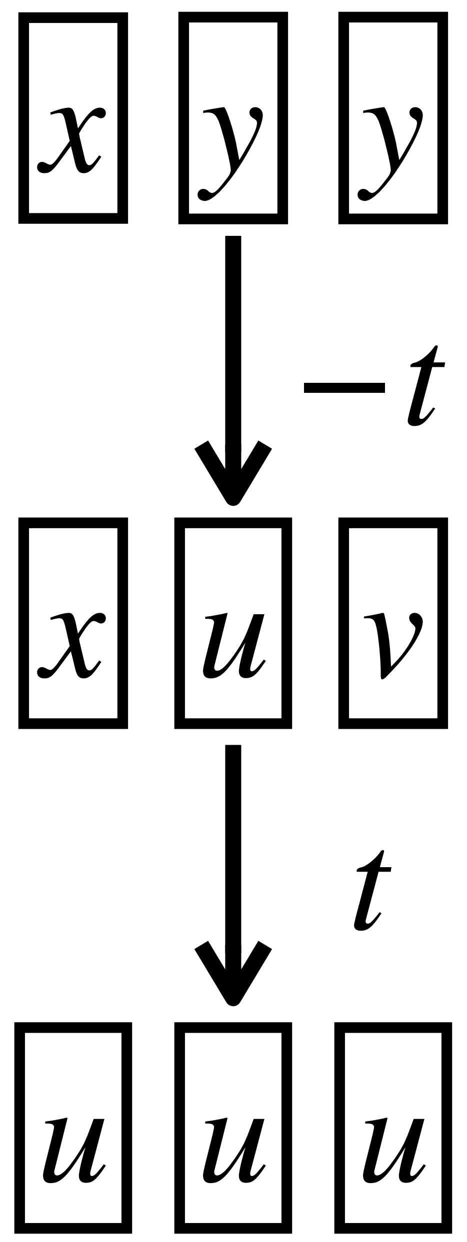
x y y
−t
x u v
t
u u u





$$
\begin{aligned}
& xy^2 \\
+ \quad & x \cdot (y^2 - uv) \\
= \quad & xuv \\
+ \quad & u \cdot (xv - u^2) \\
= \quad & u^3
\end{aligned}
$$





$$
\begin{aligned}
& xy^2 \\
+ \quad & x \cdot (y^2 - uv) \\
= \quad & xuv \\
+ \quad & u \cdot (xv - u^2) \\
= \quad & u^3
\end{aligned}
$$

Configuration $\mathbf{f}$ is reachable from configuration $\mathbf{i}$

iff

$(m_{\mathbf{f}} - m_{\mathbf{i}})$ is in the ideal generated by binomials of the form

$(ac - b^2)$ for $a < b < c$

Ideal with non-equivariant solutions

$$x^2 + y^2 - 2$$