Solving homogeneous linear equations over polynomial semrings

Ruiwen Dong

University of Oxford

March 2023

Acknowledgements to Markus Schweighofer and David Sawall from University of Konstanz.

Linear equations over integers and polynomial rings

Does the following equation have solutions $x_1, x_2, x_3 \in \mathbb{Z}$?

$$4x_1 + 12x_2 + 6x_3 = 7. \tag{1}$$

Linear equations over integers and polynomial rings

Does the following equation have solutions $x_1, x_2, x_3 \in \mathbb{Z}$?

$$4x_1 + 12x_2 + 6x_3 = 7. \tag{1}$$

No, $2 \mid LHS$ but $2 \nmid RHS$.

Linear equations over integers and polynomial rings

Does the following equation have solutions $x_1, x_2, x_3 \in \mathbb{Z}$?

$$4x_1 + 12x_2 + 6x_3 = 7. \tag{1}$$

No, $2 \mid LHS$ but $2 \nmid RHS$.

Does the following equation have solutions $x_1, x_2, x_3 \in \mathbb{N}^*$?

$$2x_1 + 3x_2 + 6x_3 = -4. \tag{2}$$

Linear equations over integers and polynomial rings

Does the following equation have solutions $x_1, x_2, x_3 \in \mathbb{Z}$?

$$4x_1 + 12x_2 + 6x_3 = 7. \tag{1}$$

No, $2 \mid LHS$ but $2 \nmid RHS$.

Does the following equation have solutions $x_1, x_2, x_3 \in \mathbb{N}^*$?

$$2x_1 + 3x_2 + 6x_3 = -4. \tag{2}$$

No, $LHS > 0$ but $RHS < 0$.

Linear equations over integers and polynomial rings

Does the following equation have solutions $x_1, x_2, x_3 \in \mathbb{Z}$?

$$4x_1 + 12x_2 + 6x_3 = 7. \tag{1}$$

No, $2 \mid LHS$ but $2 \nmid RHS$.

Does the following equation have solutions $x_1, x_2, x_3 \in \mathbb{N}^*$?

$$2x_1 + 3x_2 + 6x_3 = -4. \tag{2}$$

No, $LHS > 0$ but $RHS < 0$.

Does the following equation have solution $f_1, f_2, f_3 \in \mathbb{Z}[X]$?

$$(X - 1) \cdot f_1 + (X^2 - X) \cdot f_2 + (-X + 1) \cdot f_3 = X. \tag{3}$$

Linear equations over integers and polynomial rings

Does the following equation have solutions $x_1, x_2, x_3 \in \mathbb{Z}$?

$$4x_1 + 12x_2 + 6x_3 = 7. \tag{1}$$

No, $2 \mid LHS$ but $2 \nmid RHS$.

Does the following equation have solutions $x_1, x_2, x_3 \in \mathbb{N}^*$?

$$2x_1 + 3x_2 + 6x_3 = -4. \tag{2}$$

No, $LHS > 0$ but $RHS < 0$.

Does the following equation have solution $f_1, f_2, f_3 \in \mathbb{Z}[X]$?

$$(X-1) \cdot f_1 + (X^2 - X) \cdot f_2 + (-X+1) \cdot f_3 = X. \tag{3}$$

No, $X - 1 \mid LHS$ but $X - 1 \nmid RHS$.

Linear equations over polynomial semirings

Let ***Pos*** be the set of polynomials "positive everywhere".

$$\boldsymbol{Pos} := \{f \in \mathbb{Z}[X] \mid f(x) > 0 \text{ for all } x \in \mathbb{R}\}.$$

Does the following equation have solutions $f_1, f_2, f_3 \in \boldsymbol{Pos}$?

$$X^2 \cdot f_1 + (-X^2 - 2X) \cdot f_2 + (X+3) \cdot f_3 = 0. \tag{4}$$

Linear equations over polynomial semirings

Let ***Pos*** be the set of polynomials "positive everywhere".

$$\textbf{\textit{Pos}} := \{f \in \mathbb{Z}[X] \mid f(x) > 0 \text{ for all } x \in \mathbb{R}\}.$$

Does the following equation have solutions $f_1, f_2, f_3 \in \textbf{\textit{Pos}}$?

$$X^2 \cdot f_1 + (-X^2 - 2X) \cdot f_2 + (X + 3) \cdot f_3 = 0. \tag{4}$$

No, evaluate at $X = -1$, we have $LHS > 0$.

$$1 \cdot f_1(-1) + 1 \cdot f_2(-1) + 2 \cdot f_3(-1) = 0.$$

Linear equations over polynomial semirings

Let ***Pos*** be the set of polynomials "positive everywhere".

$$\boldsymbol{Pos} := \{f \in \mathbb{Z}[X] \mid f(x) > 0 \text{ for all } x \in \mathbb{R}\}.$$

Does the following equation have solutions $f_1, f_2, f_3 \in \boldsymbol{Pos}$?

$$X^2 \cdot f_1 + (-X^2 - 2X) \cdot f_2 + (X + 3) \cdot f_3 = 0. \tag{4}$$

No, evaluate at $X = -1$, we have $LHS > 0$.

$$1 \cdot f_1(-1) + 1 \cdot f_2(-1) + 2 \cdot f_3(-1) = 0.$$

Does the following equation have solutions $f_1, f_2, f_3 \in \mathbb{N}[X]^*$?

$$X \cdot f_1 + (X^2 - 1) \cdot f_2 + (-X^2 + 3X) \cdot f_3 = 0. \tag{5}$$

Linear equations over polynomial semirings

Let ***Pos*** be the set of polynomials “positive everywhere”.

$$\boldsymbol{Pos} := \{f \in \mathbb{Z}[X] \mid f(x) > 0 \text{ for all } x \in \mathbb{R}\}.$$

Does the following equation have solutions $f_1, f_2, f_3 \in \boldsymbol{Pos}$?

$$X^2 \cdot f_1 + (-X^2 - 2X) \cdot f_2 + (X + 3) \cdot f_3 = 0. \tag{4}$$

No, evaluate at $X = -1$, we have $LHS > 0$.

$$1 \cdot f_1(-1) + 1 \cdot f_2(-1) + 2 \cdot f_3(-1) = 0.$$

Does the following equation have solutions $f_1, f_2, f_3 \in \mathbb{N}[X]^*$?

$$X \cdot f_1 + (X^2 - 1) \cdot f_2 + (-X^2 + 3X) \cdot f_3 = 0. \tag{5}$$

No, evaluate at $X = 2$, we have $LHS > 0$.

Linear equations over polynomial semirings

Let ***Pos*** be the set of polynomials "positive everywhere".

$$\boldsymbol{Pos} := \{f \in \mathbb{Z}[X] \mid f(x) > 0 \text{ for all } x \in \mathbb{R}\}.$$

Does the following equation have solutions $f_1, f_2, f_3 \in \boldsymbol{Pos}$?

$$X^2 \cdot f_1 + (-X^2 - 2X) \cdot f_2 + (X + 3) \cdot f_3 = 0. \tag{4}$$

No, evaluate at $X = -1$, we have $LHS > 0$.

$$1 \cdot f_1(-1) + 1 \cdot f_2(-1) + 2 \cdot f_3(-1) = 0.$$

Does the following equation have solutions $f_1, f_2, f_3 \in \mathbb{N}[X]^*$?

$$X \cdot f_1 + (X^2 - 1) \cdot f_2 + (-X^2 + 3X) \cdot f_3 = 0. \tag{5}$$

No, evaluate at $X = 2$, we have $LHS > 0$.

If no solution, does a "certificate" always exist?

Linear equations over polynomial semirings

Let ***Pos*** be the set of polynomials "positive everywhere".

$$\textbf{\textit{Pos}} := \{f \in \mathbb{Z}[X] \mid f(x) > 0 \text{ for all } x \in \mathbb{R}\}.$$

Does the following equation have solutions $f_1, f_2, f_3 \in \textbf{\textit{Pos}}$?

$$X^2 \cdot f_1 + (-X^2 - 2X) \cdot f_2 + (X + 3) \cdot f_3 = 0. \quad (4)$$

No, evaluate at $X = -1$, we have $LHS > 0$.

$$1 \cdot f_1(-1) + 1 \cdot f_2(-1) + 2 \cdot f_3(-1) = 0.$$

Does the following equation have solutions $f_1, f_2, f_3 \in \mathbb{N}[X]^*$?

$$X \cdot f_1 + (X^2 - 1) \cdot f_2 + (-X^2 + 3X) \cdot f_3 = 0. \quad (5)$$

No, evaluate at $X = 2$, we have $LHS > 0$.

If no solution, does a "certificate" always exist? Decidability?

Main result

Given $B \subseteq \mathbb{R}$, let $\boldsymbol{Pos}(B)$ be the set of polynomials "positive on B".

$$\boldsymbol{Pos}(B) := \{f \in \mathbb{Z}[X] \mid f(x) > 0 \text{ for all } x \in B\}.$$

Given $h_1, \ldots, h_n \in \mathbb{Z}[X]$, we want to solve the equation

$$h_1 f_1 + h_2 f_2 + \cdots + h_n f_n = 0 \tag{6}$$

over $\boldsymbol{Pos}(B)$.

Main result

Given $B \subseteq \mathbb{R}$, let $\boldsymbol{Pos}(B)$ be the set of polynomials "positive on B".

$$\boldsymbol{Pos}(B) := \{f \in \mathbb{Z}[X] \mid f(x) > 0 \text{ for all } x \in B\}.$$

Given $h_1, \ldots, h_n \in \mathbb{Z}[X]$, we want to solve the equation

$$h_1 f_1 + h_2 f_2 + \cdots + h_n f_n = 0 \tag{6}$$

over $\boldsymbol{Pos}(B)$.

Theorem

Equation (6) has no solution over $\boldsymbol{Pos}(B)$ if and only if:

- *there exists $t \in B$, such that $h_i(t) \geq 0$ for all i and $h_i(t) > 0$ for at least one i,*
- *or there exists $t \in B$, such that $h_i(t) \leq 0$ for all i and $h_i(t) < 0$ for at least one i.*

Main result

Given $B \subseteq \mathbb{R}$, let $\boldsymbol{Pos}(B)$ be the set of polynomials "positive on B".

$$\boldsymbol{Pos}(B) \coloneqq \{f \in \mathbb{Z}[X] \mid f(x) > 0 \text{ for all } x \in B\}.$$

Given $h_1, \ldots, h_n \in \mathbb{Z}[X]$, we want to solve the equation

$$h_1 f_1 + h_2 f_2 + \cdots + h_n f_n = 0 \tag{6}$$

over $\boldsymbol{Pos}(B)$.

Theorem

Equation (6) has no solution over $\boldsymbol{Pos}(B)$ if and only if:

- *there exists $t \in B$, such that $h_i(t) \geq 0$ for all i and $h_i(t) > 0$ for at least one i,*
- *or there exists $t \in B$, such that $h_i(t) \leq 0$ for all i and $h_i(t) < 0$ for at least one i.*

(Pólya's theorem) Connection with $\mathbb{N}[X]^*$: Equation (6) has solution over $\mathbb{N}[X]^*$ if and only if it has solution over $\boldsymbol{Pos}(\mathbb{R}_{\geq 0})$.

Field semiorderings (Prestel, 1970s)

Definition (Set linear ordering)

A linear ordering of a set S is a binary relation that satisfies

1. **Reflexivity:** $a \leq a$,
2. **Transitivity:** $a \leq b, b \leq c \implies a \leq c$,
3. **Antisymmetry:** $a \leq b, b \leq a \implies a = b$,
4. **Totality:** $a \leq b$ or $b \leq a$.

Examples: $(\mathbb{Z}, \leq)$, $(\mathbb{Z}^n, \leq_{lex})$.

Field semiorderings (Prestel, 1970s)

Definition (Set linear ordering)

A linear ordering of a set S is a binary relation that satisfies

1. **Reflexivity:** $a \leq a$,
2. **Transitivity:** $a \leq b, b \leq c \implies a \leq c$,
3. **Antisymmetry:** $a \leq b, b \leq a \implies a = b$,
4. **Totality:** $a \leq b$ or $b \leq a$.

Examples: $(\mathbb{Z}, \leq)$, $(\mathbb{Z}^n, \leq_{lex})$.

If the set S is a field F, we want $\leq$ to be compatible with $+$ and $(\cdot)^2$.

Field semiorderings (Prestel, 1970s)

Definition (Set linear ordering)

A linear ordering of a set S is a binary relation that satisfies

1. **Reflexivity:** $a \leq a$,
2. **Transitivity:** $a \leq b, b \leq c \implies a \leq c$,
3. **Antisymmetry:** $a \leq b, b \leq a \implies a = b$,
4. **Totality:** $a \leq b$ or $b \leq a$.

Examples: $(\mathbb{Z}, \leq)$, $(\mathbb{Z}^n, \leq_{lex})$.

If the set S is a field F, we want $\leq$ to be compatible with $+$ and $(\cdot)^2$.

Definition (Field Semiordering)

A *semiordering* of a field F is a linear ordering $\leq$ that satisfies

1. **Compatibility with addition:** $a \leq b \implies a + c \leq b + c$,
2. **Compatibility with one:** $0 \leq 1$,
3. **Compatibility with squares:** $0 \leq a \implies 0 \leq ab^2$.

Example: $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$.

Why care about semiordering?

Observation (Positive set of a semiordering)

"$\leq$" is a semiordering of F if and only if $P := \{a > 0 \mid a \in F\}$ satisfies

1. **Compatibility with addition:** $P + P \subseteq P$,
2. **Compatibility with one:** $0 \notin P$,
3. **Compatibility with squares:** $P \cdot (F^2 \setminus \{0\}) \subseteq P$.
4. **Antisymmetry:** $P \cap -P = \emptyset$.
5. **Totality:** $P \cup -P = F \setminus \{0\}$.

Why care about semiordering?

Observation (Positive set of a semiordering)

"$\leq$" is a semiordering of F if and only if $P := \{a > 0 \mid a \in F\}$ satisfies

1. **Compatibility with addition:** $P + P \subseteq P$,
2. **Compatibility with one:** $0 \notin P$,
3. **Compatibility with squares:** $P \cdot (F^2 \setminus \{0\}) \subseteq P$.
4. **Antisymmetry:** $P \cap -P = \emptyset$.
5. **Totality:** $P \cup -P = F \setminus \{0\}$.

Main motivation:

If $h_1 f_1 + h_2 f_2 + \cdots + h_n f_n = 0$ has no solutions $f_i \in \boldsymbol{Pos}(B)$, then

$$P := \{h_1 f_1 + h_2 f_2 + \cdots + h_n f_n \mid f_i \in \boldsymbol{Pos}(B)\}$$

is "almost" the positive set of a semiordering of the field $\mathbb{R}(X)$.

Why care about semiordering? (continued)

Assume $(*) : h_1 f_1 + h_2 f_2 + \cdots + h_n f_n = 0$ has no solution over $\boldsymbol{Pos}(B)$.
Recall

$$P := \{h_1 f_1 + h_2 f_2 + \cdots + h_n f_n \mid f_i \in \boldsymbol{Pos}(B)\}.$$

Why care about semiordering? (continued)

Assume $(*) : h_1 f_1 + h_2 f_2 + \cdots + h_n f_n = 0$ has no solution over $\textbf{\textit{Pos}}(B)$. Recall

$$P := \{h_1 f_1 + h_2 f_2 + \cdots + h_n f_n \mid f_i \in \textbf{\textit{Pos}}(B)\}.$$

1. **Compatibility with addition:** $P + P \subseteq P$ (linearity of $\textbf{\textit{Pos}}(B)$)

Why care about semiordering? (continued)

Assume $(*): h_1 f_1 + h_2 f_2 + \cdots + h_n f_n = 0$ has no solution over $\textbf{\textit{Pos}}(B)$.
Recall

$$P := \{h_1 f_1 + h_2 f_2 + \cdots + h_n f_n \mid f_i \in \textbf{\textit{Pos}}(B)\}.$$

- (i) **Compatibility with addition:** $P + P \subseteq P$ (linearity of $\textbf{\textit{Pos}}(B)$)
- (ii) **Compatibility with one:** $0 \notin P$ ($(*)$ has no solution)

Why care about semiordering? (continued)

Assume $(*) : h_1 f_1 + h_2 f_2 + \cdots + h_n f_n = 0$ has no solution over $\textbf{\textit{Pos}}(B)$. Recall

$$P := \{h_1 f_1 + h_2 f_2 + \cdots + h_n f_n \mid f_i \in \textbf{\textit{Pos}}(B)\}.$$

1. **Compatibility with addition:** $P + P \subseteq P$ (linearity of $\textbf{\textit{Pos}}(B)$)
2. **Compatibility with one:** $0 \notin P$ ($(*)$ has no solution)
3. **Compatibility with squares:** $P \cdot (F^2 \setminus \{0\}) \subseteq P$ ("almost satisfied" by $\textbf{\textit{Pos}}(B)$)

Why care about semiordering? (continued)

Assume $(*) : h_1 f_1 + h_2 f_2 + \cdots + h_n f_n = 0$ has no solution over $\textbf{\textit{Pos}}(B)$. Recall

$$P := \{h_1 f_1 + h_2 f_2 + \cdots + h_n f_n \mid f_i \in \textbf{\textit{Pos}}(B)\}.$$

(i) **Compatibility with addition:** $P + P \subseteq P$ (linearity of $\textbf{\textit{Pos}}(B)$)

(ii) **Compatibility with one:** $0 \notin P$ ($(*)$ has no solution)

(iii) **Compatibility with squares:** $P \cdot (F^2 \setminus \{0\}) \subseteq P$ ("almost satisfied" by $\textbf{\textit{Pos}}(B)$)

(iv) **Antisymmetry:** $P \cap -P = \emptyset$ ($(*)$ has no solution)

Why care about semiordering? (continued)

Assume $(*) : h_1 f_1 + h_2 f_2 + \cdots + h_n f_n = 0$ has no solution over $\boldsymbol{Pos}(B)$.
Recall

$$P := \{h_1 f_1 + h_2 f_2 + \cdots + h_n f_n \mid f_i \in \boldsymbol{Pos}(B)\}.$$

1. **Compatibility with addition:** $P + P \subseteq P$ (linearity of $\boldsymbol{Pos}(B)$)
2. **Compatibility with one:** $0 \notin P$ ($(*)$ has no solution)
3. **Compatibility with squares:** $P \cdot (F^2 \setminus \{0\}) \subseteq P$ ("almost satisfied" by $\boldsymbol{Pos}(B)$)
4. **Antisymmetry:** $P \cap -P = \emptyset$ ($(*)$ has no solution)
5. **Totality:** $P \cup -P = \mathbb{R}(X) \setminus \{0\}$ (Not satisfied!!)

Why care about semiordering? (continued)

Assume $(*) : h_1 f_1 + h_2 f_2 + \cdots + h_n f_n = 0$ has no solution over $\textbf{\textit{Pos}}(B)$. Recall

$$P := \{h_1 f_1 + h_2 f_2 + \cdots + h_n f_n \mid f_i \in \textbf{\textit{Pos}}(B)\}.$$

1. **Compatibility with addition:** $P + P \subseteq P$ (linearity of $\textbf{\textit{Pos}}(B)$)
2. **Compatibility with one:** $0 \notin P$ ($(*)$ has no solution)
3. **Compatibility with squares:** $P \cdot (F^2 \setminus \{0\}) \subseteq P$ ("almost satisfied" by $\textbf{\textit{Pos}}(B)$)
4. **Antisymmetry:** $P \cap -P = \emptyset$ ($(*)$ has no solution)
5. **Totality:** $P \cup -P = \mathbb{R}(X) \setminus \{0\}$ (Not satisfied!!)

Fixing Compatibility with squares: slightly extend P. (Quite technical!)

Fixing Totality: "complete" P into semiordering using Zorn's Lemma.

Proposition

Suppose $(*)$ has no solution over $\textbf{\textit{Pos}}(B)$. There exists a semiordering $>_P$ of $\mathbb{R}(X)$ such that $h_1 f_1 + h_2 f_2 + \cdots + h_n f_n >_P 0$ for all $f_i \in \textbf{\textit{Pos}}(B)$.

What are the semiorderings of $\mathbb{R}(X)$?

Example of a semiordering of $\mathbb{R}(X)$:

What are the semiorderings of $\mathbb{R}(X)$?

Example of a semiordering of $\mathbb{R}(X)$:

Let $t \in \mathbb{R}$, define $>_{t+}$ the following way. Given $f \in \mathbb{R}(X)$:

- In case $f(t)$ is well-defined: $f >_{t+} 0$ if $f(t) > 0$.

What are the semiorderings of $\mathbb{R}(X)$?

Example of a semiordering of $\mathbb{R}(X)$:

Let $t \in \mathbb{R}$, define $>_{t+}$ the following way. Given $f \in \mathbb{R}(X)$:

- In case $f(t)$ is well-defined: $f >_{t+} 0$ if $f(t) > 0$.
- In case $f(t)$ is not well-defined or $f(t) = 0$: then $f >_{t+} 0$ if $f(t + \varepsilon) > 0$ for all small enough $\varepsilon > 0$.

What are the semiorderings of $\mathbb{R}(X)$?

Example of a semiordering of $\mathbb{R}(X)$:

Let $t \in \mathbb{R}$, define $>_{t+}$ the following way. Given $f \in \mathbb{R}(X)$:

- In case $f(t)$ is well-defined: $f >_{t+} 0$ if $f(t) > 0$.
- In case $f(t)$ is not well-defined or $f(t) = 0$: then $f >_{t+} 0$ if $f(t + \varepsilon) > 0$ for all small enough $\varepsilon > 0$.

Then $>_{t+}$ is a semiordering of $\mathbb{R}(X)$.

What are the semiorderings of $\mathbb{R}(X)$?

Example of a semiordering of $\mathbb{R}(X)$:

Let $t \in \mathbb{R}$, define $>_{t+}$ the following way. Given $f \in \mathbb{R}(X)$:

- In case $f(t)$ is well-defined: $f >_{t+} 0$ if $f(t) > 0$.
- In case $f(t)$ is not well-defined or $f(t) = 0$: then $f >_{t+} 0$ if $f(t+\varepsilon) > 0$ for all small enough $\varepsilon > 0$.

Then $>_{t+}$ is a semiordering of $\mathbb{R}(X)$.

Similarly, we can define $>_{t-}$ by changing $t+\varepsilon$ to $t-\varepsilon$ in the second conditions.

What are the semiorderings of $\mathbb{R}(X)$?

Example of a semiordering of $\mathbb{R}(X)$:

Let $t \in \mathbb{R}$, define $>_{t+}$ the following way. Given $f \in \mathbb{R}(X)$:

- In case $f(t)$ is well-defined: $f >_{t+} 0$ if $f(t) > 0$.
- In case $f(t)$ is not well-defined or $f(t) = 0$: then $f >_{t+} 0$ if $f(t + \varepsilon) > 0$ for all small enough $\varepsilon > 0$.

Then $>_{t+}$ is a semiordering of $\mathbb{R}(X)$.

Similarly, we can define $>_{t-}$ by changing $t + \varepsilon$ to $t - \varepsilon$ in the second conditions.

We can also define $>_{\infty}$: Define $f >_{\infty} 0$ if and only if $f(N) > 0$ for all large enough $N > 0$.

What are the semiorderings of $\mathbb{R}(X)$?

Example of a semiordering of $\mathbb{R}(X)$:

Let $t \in \mathbb{R}$, define $>_{t+}$ the following way. Given $f \in \mathbb{R}(X)$:

- In case $f(t)$ is well-defined: $f >_{t+} 0$ if $f(t) > 0$.
- In case $f(t)$ is not well-defined or $f(t) = 0$: then $f >_{t+} 0$ if $f(t+\varepsilon) > 0$ for all small enough $\varepsilon > 0$.

Then $>_{t+}$ is a semiordering of $\mathbb{R}(X)$.

Similarly, we can define $>_{t-}$ by changing $t+\varepsilon$ to $t-\varepsilon$ in the second conditions.

We can also define $>_{\infty}$: Define $f >_{\infty} 0$ if and only if $f(N) > 0$ for all large enough $N > 0$.

We can also define $>_{-\infty}$ similarly.

What are the semiorderings of $\mathbb{R}(X)$?

Example of a semiordering of $\mathbb{R}(X)$:

Let $t \in \mathbb{R}$, define $>_{t+}$ the following way. Given $f \in \mathbb{R}(X)$:

- In case $f(t)$ is well-defined: $f >_{t+} 0$ if $f(t) > 0$.
- In case $f(t)$ is not well-defined or $f(t) = 0$: then $f >_{t+} 0$ if $f(t + \varepsilon) > 0$ for all small enough $\varepsilon > 0$.

Then $>_{t+}$ is a semiordering of $\mathbb{R}(X)$.

Similarly, we can define $>_{t-}$ by changing $t + \varepsilon$ to $t - \varepsilon$ in the second conditions.

We can also define $>_{\infty}$: Define $f >_{\infty} 0$ if and only if $f(N) > 0$ for all large enough $N > 0$.

We can also define $>_{-\infty}$ similarly.

Theorem (Prestel et al.)

The set of all semiorderings of $\mathbb{R}(X)$ is

$$\{>_{-\infty}\} \cup \{>_{t+}, >_{t-} \mid t \in \mathbb{R}\} \cup \{>_{\infty}\}.$$

Putting it together

Assume $(*) : h_1 f_1 + h_2 f_2 + \cdots + h_n f_n = 0$ has no solution over $\textbf{\textit{Pos}}(B)$.

Proposition

Suppose $(*)$ has no solution over $\textbf{\textit{Pos}}(B)$. There exists a semiordering $>_P$ of $\mathbb{R}(X)$ such that $h_1 f_1 + h_2 f_2 + \cdots + h_n f_n >_P 0$ for all $f_i \in \textbf{\textit{Pos}}(B)$.

Theorem (Prestel et al.)

The set of all semiorderings of $\mathbb{R}(X)$ is

$$\{>_{-\infty}\} \cup \{>_{t+}, >_{t-} \mid t \in \mathbb{R}\} \cup \{>_{\infty}\}.$$

Putting it together

Assume $(*) : h_1 f_1 + h_2 f_2 + \cdots + h_n f_n = 0$ has no solution over $\textbf{\textit{Pos}}(B)$.

Proposition

Suppose $(*)$ has no solution over $\textbf{\textit{Pos}}(B)$. There exists a semiordering $>_P$ of $\mathbb{R}(X)$ such that $h_1 f_1 + h_2 f_2 + \cdots + h_n f_n >_P 0$ for all $f_i \in \textbf{\textit{Pos}}(B)$.

Theorem (Prestel et al.)

The set of all semiorderings of $\mathbb{R}(X)$ is

$$\{>_{-\infty}\} \cup \{>_{t+}, >_{t-} \mid t \in \mathbb{R}\} \cup \{>_{\infty}\}.$$

- If $>_P$ is $>_{t+}$ for some $t \in \mathbb{R}$: we have $h_1(t+\varepsilon) \geq 0, h_2(t+\varepsilon) \geq 0, \ldots, h_n(t+\varepsilon) \geq 0$ for some $\varepsilon > 0$. **We have found the certificate $t + \varepsilon$!** (Easy to prove $t + \varepsilon \in B$).

Putting it together

Assume $(*) : h_1 f_1 + h_2 f_2 + \cdots + h_n f_n = 0$ has no solution over $\boldsymbol{Pos}(B)$.

Proposition

Suppose $(*)$ has no solution over $\boldsymbol{Pos}(B)$. There exists a semiordering $>_P$ of $\mathbb{R}(X)$ such that $h_1 f_1 + h_2 f_2 + \cdots + h_n f_n >_P 0$ for all $f_i \in \boldsymbol{Pos}(B)$.

Theorem (Prestel et al.)

The set of all semiorderings of $\mathbb{R}(X)$ is

$$\{>_{-\infty}\} \cup \{>_{t+}, >_{t-} \mid t \in \mathbb{R}\} \cup \{>_{\infty}\}.$$

- If $>_P$ is $>_{t+}$ for some $t \in \mathbb{R}$: we have $h_1(t+\varepsilon) \geq 0, h_2(t+\varepsilon) \geq 0, \ldots, h_n(t+\varepsilon) \geq 0$ for some $\varepsilon > 0$. **We have found the certificate $t + \varepsilon$!** (Easy to prove $t + \varepsilon \in B$).
- If $>_P$ is $>_{\infty}$, $>_{t-}$ or $>_{-\infty}$: proof is similar.

Applications and possible extensions

Example of application: can be used to decide whether certain sub-semigroups of $\mathbb{Z} \wr \mathbb{Z}$ are actually groups.

$$\mathbb{Z} \wr \mathbb{Z} \cong \left\{ \begin{pmatrix} X^b & y \\ 0 & 1 \end{pmatrix} \;\middle|\; y \in \mathbb{Z}[X^{\pm}], b \in \mathbb{Z} \right\}.$$

This lays the foundation to solving semigroup algorithmic problems in *metabelian* groups.

Applications and possible extensions

Example of application: can be used to decide whether certain sub-semigroups of $\mathbb{Z} \wr \mathbb{Z}$ are actually groups.

$$\mathbb{Z} \wr \mathbb{Z} \cong \left\{ \begin{pmatrix} X^b & y \\ 0 & 1 \end{pmatrix} \middle| \; y \in \mathbb{Z}[X^{\pm}], b \in \mathbb{Z} \right\}.$$

This lays the foundation to solving semigroup algorithmic problems in *metabelian* groups.

Possible extensions and open problems:

- Multivariate polynomial rings? (Semiorderings of $\mathbb{R}(X, Y)$ can be highly pathological!)
- Non-homogeneous equations? (Apply the theory of *pure states*.)
- Develop a local-global theory of semi*groups* instead of semirings?