# Course: Quantifier Elimination

**Thomas Sturm**

**http://www.mpi-inf.mpg.de/~sturm/**

**Winter Term 2011/2012**

# Contents I

# Contents II

# Direct Links to the Lectures by Date

▸ 2011-10-19 ▸ 2011-10-26 ▸ 2011-11-02 ▸ 2011-11-09 ▸ 2011-11-16 ▸ 2011-11-23 ▸ 2011-11-30

▸ 2011-12-14 ▸ 2011-12-21 ▸ 2012-01-11 ▸ 2012-01-18 ▸ 2012-01-25 ▸ 2012-02-01

# Solvability of Parametric Conditions – Examples

## Example (Real numbers)

Consider real parameters $a$, $b$, $c$.

(i) $ax + b = 0$ has a solution $x \in \mathbb{R}$ iff $a \neq 0 \vee b = 0$.

(ii) $ax^3 + bx + c = 0$ has a solution $x \in \mathbb{R}$ iff $a \neq 0 \vee b \neq 0 \vee c = 0$.

## Proof.

(i) "$\Leftarrow$:" For $b = 0$ set $x = 0$, and for $a \neq 0$ set $x = -b/a$.

"$\Rightarrow$:" Let $a = 0$ and $b \neq 0$. Then $ax + b = 0 \longleftrightarrow b = 0$.

(ii) "$\Leftarrow$:" For $a = 0$ we are in situation (i). Let $a \neq 0$, w.l.o.g. $a > 0$. Then $\lim_{x \to \infty} ax^3 + bx + c = \infty$, $\lim_{x \to -\infty} ax^3 + bx + c = -\infty$, and by the intermdiate value theorem there is a zero.

"$\Rightarrow$:" Analogously to (i). $\square$

### Example (Set theory)

Consider $P(M)$ for $M \neq \varnothing$ and parameters $A, B$ ranging over $P(M)$.
$\neg X \subseteq A \wedge X \cap B = \varnothing$ has a solution $X \in P(M)$ iff $A \cup B \neq M$.

### Proof.

Exercise. $\square$

### Example (Integers)

Consider integer parameters $a$, $b$, $c$.

$2x = a \wedge b < x \wedge x < c$ has a solution $x \in \mathbb{Z}$ iff $a$ is even and $2b < a < 2c$.

### Proof.

"$\Rightarrow$:" $2x = a \wedge b < x \wedge x < c \longleftrightarrow 2x = a \wedge 2b < 2x \wedge 2x = 2c$.

The only possible solution $x = a/2$ exists iff $a$ is even.

Equivalently replacing $2x$ with $a$ then yields our condition.

"$\Leftarrow$:" Set $x = a/2$, which is possible since $a$ is even. $2(a/2) = a$, and our condition implies $b < a/2$ and $a/2 < c$. □

**Example (Undirected graph)**

Consider $(V, E)$ with $V = \{1, 2, 3, 4\}$, $E = \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{3, 4\}, \{2, 4\}\}$, and let $a$, $b$ be parameters ranging over $V$.

$\{x, a\} \in E \land \{x, b\} \in E \land \neg\{a, b\} \in E$ has a solution $x \in V$ iff
$a = b \lor (a = 1 \land b = 3) \lor (a = 3 \land b = 1)$.

**Proof.**

Exercise. □

## Example (Linear equations in one indeterminate over $\mathbb{R}$)

Let $a_1, \ldots, a_m \in \mathbb{R}$ such that $a_1 \neq 0$. Consider real parameters $c_1, \ldots, c_m$. $\bigwedge_{i=1}^{m} a_i x + b_i = 0$ has a solution $x \in \mathbb{R}$ iff $\bigwedge_{i=2}^{m} a_i b_1 = a_1 b_i$.

## Proof.

Let $b_1, \ldots, b_m \in \mathbb{R}$.

"$\Rightarrow$:" Let $i \in \{2, \ldots, m\}$ such that $a_i b_1 \neq a_1 b_i$. If $a_i = 0$, then $b_i \neq 0$ , and it follows that in particular $a_i x + b_i = 0$ has no solution. If $a_i \neq 0$, then $x = -b_i/a_i$ is the only solution of $a_i x + b_i = 0$. Similarly $x = -b_1/a_1$ is the only solution of $a_1 x + b_1 = 0$. But our assumption $a_i b_1 \neq a_1 b_i$ is equivalent to $-b_1/a_1 \neq -b_i/a_i$.

"$\Leftarrow$:" Set $x = -b_1/a_1$, which obviously solves $a_1 x + b_1 = 0$. Consider now $a_i x + b_i = 0$ for $i \in \{2, \ldots, m\}$. We know $a_i b_1 = a_1 b_i$. If $a_i = 0$ then also $b_i = 0$, and our considered equation is trivial. Otherwise, we equivalently obtain $-b_i/a_i = -b_1/a_1 = x$, i.e., $x$ solves our considered equation. $\square$

### Example (Linear equations in two indeterminates over $\mathbb{R}$)

Let $a_1, \dots, a_m, b_1, \dots, b_m \in \mathbb{R}$, such that $a_1 \neq 0$ and $a_2b_1 - a_1b_2 \neq 0$.

Consider real parameters $c_1, \dots, c_m$.

$\bigwedge_{i=1}^{m} a_ix_1 + b_ix_2 + c_i = 0$ has a solution $(x_1, x_2) \in \mathbb{R}^2$ iff

$\bigwedge_{i=3}^{m} (a_ib_1 - a_1b_i)(a_2c_1 - a_1c_2) = (a_2b_1 - a_1b_2)(a_ic_1 - a_1c_i)$.

### Proof.

Exercise.

**Hint:** Temoporarily consider $x_2$ a parameter and use the previous result. $\square$

**Example (One linear constraint over $\mathbb{R}$)**

Consider real parameters $a$, $b$.

$ax + b \leqslant 0$ has a solution $x \in \mathbb{R}$ iff $a \neq 0 \vee b \leqslant 0$.

**Proof.**

Exercise. $\square$

# Syntax: Elementary Languages

A **language** is a triplet $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$ with $\mathcal{F} \cap \mathcal{R} = \varnothing$ und $\sigma : \mathcal{F} \cup \mathcal{R} \to \mathbb{N}$.

The elements $f \in \mathcal{F}$ are **function symbols**.

The elements $R \in \mathcal{R}$ are **relation symbols**.

For $z \in \mathcal{F} \cup \mathcal{R}$ we call $\sigma(z)$ the **arity** of $z$.

**Example**

The **language of ordered rings** is $\mathcal{L}_{OR} = (\{0, 1, +, -, \cdot\}, \{\leqslant\}, \sigma)$, where $\sigma(0) = \sigma(1) = 0$, $\sigma(-) = 1$, $\sigma(+) = \sigma(\cdot) = \sigma(\leqslant) = 2$.

A language is **finite** if $\mathcal{F} \cup \mathcal{R}$ is finite.

Finite languages can be written like $\mathcal{L}_{OR} = (0^{(0)}, 1^{(0)}, +^{(2)}, -^{(1)}, \cdot^{(2)}; \leqslant^{(2)})$.

$f \in \mathcal{F}$ with $\sigma(f) = 0$ is a **constant symbol**.

$\mathcal{L}$ is an **algebraic language** if $\mathcal{R} = \varnothing$.

$\mathcal{L}$ is a **relational language** if $\mathcal{F} = \varnothing$.

# Syntax: Extension Languages and Sublanguages

Consider languages $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$ and $\mathcal{L}' = (\mathcal{F}', \mathcal{R}', \sigma')$.
Then $\mathcal{L}'$ is an **extension** of $\mathcal{L}$, if

$$\mathcal{F} \subseteq \mathcal{F}', \quad \mathcal{R} \subseteq \mathcal{R}', \quad \sigma = \sigma'|_{\mathcal{F} \cup \mathcal{R}}.$$

Accordingly, $\mathcal{L}$ is a **sublanguage** of $\mathcal{L}'$.
We **write** $\mathcal{L} \subseteq \mathcal{L}'$.

**Example**

$$\mathcal{L}_R = (0, 1, +, -, \cdot) \subseteq (0, 1, +, -, \cdot; \leqslant) = \mathcal{L}_{OR}$$

The language of ordered rings is an extension of the language of rings.

The language of rings is an sublanguage of the language of ordered rings.

# Syntax: Special Symbols, Variables, and the Alphabet

We fix a set $\mathcal{X} = \{$**(**, **)**, **,**, **=**$\}$ of **special symbols**.

We fix an inifinite set $\mathcal{V}$ of **variables**.

The **alphabet** of a language $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$ is $\mathcal{Z}_\mathcal{L} = \mathcal{X} \cup \mathcal{V} \cup \mathcal{F} \cup \mathcal{R}$.

$\mathcal{Z}_\mathcal{L}^*$ is the set of all **finite words** über $\mathcal{Z}_\mathcal{L}$.

$\varepsilon \in \mathcal{Z}^*$ is the **empty word**.

The **length** $|w|$ of a word $w \in \mathcal{Z}_\mathcal{L}^*$ is the number of contained alphabet characters counting multiplicites.

## Convention

Our choices of $\mathcal{V}$, $\mathcal{F}$ and $\mathcal{R}$ are always such that:

(1) $\mathcal{X}$, $\mathcal{V}$, $\mathcal{F}$ and $\mathcal{R}$ are pairwsie disjoint.

(2) $w \in \mathcal{Z}_\mathcal{L}^*$ and $|w| \neq 1 \implies w \notin \mathcal{Z}_\mathcal{L}$

We shortly write $\mathcal{Z}$ and $\mathcal{Z}^*$ whenever $\mathcal{L}$ is obvious from the context.

# Syntax: Terms and Atomic Formulas

$\mathcal{L}$-**terms** are words $t \in \mathcal{Z}^*$ obtained by composition of variables and (possibly constant) function symbols according to their arity.

$\mathcal{T}_\mathcal{L} \subseteq \mathcal{Z}^*$ is the set of all $\mathcal{L}$-terms.

$\mathcal{V}(t) \subseteq \mathcal{V}$ is the (finite) set of variables contained in $t \in \mathcal{T}_\mathcal{L}$.

## Conventions

- Formally, all terms are in prefix notation.
- We use infix notation (with precedence rules) for our convenience.

**Atomic $\mathcal{L}$-formulas** are words $\varphi \in \mathcal{Z}^*$ that are

(a) **equations** $t_1 = t_2$, where $t_1, t_2 \in \mathcal{T}_\mathcal{L}$.

(b) **predicates** $R(t_1, \dots, t_n)$ where $R \in \mathcal{R}$ with $\sigma(R) = n$, and $t_1, \dots, t_n \in \mathcal{T}_\mathcal{L}$.

$\mathcal{A}_\mathcal{L} \subseteq \mathcal{Z}^*$ is the set of all atomic $\mathcal{L}$-formulas.

$\mathcal{V}(\varphi) \subset \mathcal{V}$ is the (finite) set of variables contained in $\varphi \in \mathcal{A}_\mathcal{L}$.

We shortly write $\mathcal{T}$ and $\mathcal{A}$ whenever $\mathcal{L}$ is obvious from the context.

# Semantics: Structures

Consider a language $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$.

An **$\mathcal{L}$-Structure** is a triplet $\mathbf{A} = (A, \iota_{\mathcal{F}}, \iota_{\mathcal{R}})$.

$A \neq \varnothing$ is the **universe** of **A**.

The **interpretation** $\iota_{\mathcal{F}}$ assigns to each $f \in \mathcal{F}$, $\sigma(f) = n$ a function $f^{\mathbf{A}} : A^n \to A$.

The functions $f^{\mathbf{A}}$ for $f \in \mathcal{F}$ are the **functions** of **A**.

For constant symbols $c \in \mathcal{F}$ with $\sigma(c) = 0$ we call $c^{\mathbf{A}} \in \mathbf{A}$ a **constant** of **A**.

The **interpretation** $\iota_{\mathcal{R}}$ assigns to $R \in \mathcal{R}$, $\sigma(R) = n$ a function $R^{\mathbf{A}} : A^n \to \{\bot, \top\}$.

The symbol $\bot$ means “false,” and the symbol $\top$ means “true.”

The functions $R^{\mathbf{A}}$ for $R \in \mathcal{R}$ are the **Relations** of **A**.

**You want it more formally?**

$\iota_{\mathcal{F}} : \mathcal{F} \to \bigcup_{n \in \mathbb{N}} A^{(A^n)}, \quad \iota_{\mathcal{R}} : \mathcal{R} \to \bigcup_{n \in \mathbb{N}} \{\bot, \top\}^{(A^n)}$.

max planck institut
informatik

# Semantics: Classification of $\mathcal{L}$-Structures and an Example

Consider a language $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$ and an $\mathcal{L}$-structure $\mathbf{A} = (A, \iota_{\mathcal{F}}, \iota_{\mathcal{R}})$.

If $\mathcal{L}$ is an algebraic language, then **A** is called an **algebra**.

If $\mathcal{L}$ is a relational language, then **A** called a **relational structure**.

**A** is called **finite** if its universe $A$ is finite.

### Example (The real numbers as an ordered ring)

Consider the language $\mathcal{L}_{\mathrm{OR}} = (0, 1, +, -, \cdot; \leqslant)$ of ordered rings.

One $\mathcal{L}_{OR}$-structure is $\mathbf{R} = (\mathbb{R}, \iota_{\mathcal{F}}, \iota_{\mathcal{R}})$:

- $\iota_{\mathcal{F}}(0) = 0^{\mathbf{R}} \in \mathbb{R}$ und $\iota_{\mathcal{F}}(1) = 1^{\mathbf{R}} \in \mathbb{R}$.
- $\iota_{\mathcal{F}}(+) = +^{\mathbf{R}}$, where $+^{\mathbf{R}} : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is the regular addition in $\mathbb{R}$.
- $\iota_{\mathcal{F}}(-) = -^{\mathbf{R}}$ and $\iota_{\mathcal{F}}(\cdot) = \cdot^{\mathbf{R}}$ analogously.
- $\iota_{\mathcal{R}}(\leqslant) = \leqslant^{\mathbf{R}}$, where $\leqslant^{\mathbf{R}} : \mathbb{R} \times \mathbb{R} \to \{\bot, \top\}$ with $\leqslant^{\mathbf{R}}(x, y) = \top \Leftrightarrow x \leqslant y$ in $\mathbb{R}$.

$\mathcal{L}_{OR}$ is finite but **R** is infinite.

# Structures Over Finite Languages

Consider a finite language $\mathcal{L} = (f_1^{(k_1)}, \ldots, f_m^{(k_m)}; R_1^{(l_1)}, \ldots, R_n^{(l_n)})$.
Then $\mathcal{L}$-structures can be specified like $\mathbf{A} = (A; \omega_1, \ldots, \omega_m; \varrho_1, \ldots, \varrho_n)$,
where $(\omega_i : A^{k_i} \to A) = \iota_{\mathcal{F}}(f_i)$ and $(\varrho_j : A^{l_j} \to \{\bot, \top\}) = \iota_{\mathcal{R}}(R_j)$.
The definitions of $\omega_i$ and $\varrho_j$ can often be derived from their names.

**Example (The real numbers as an ordered ring)**

$\mathcal{L} = (0, 1, +, -, \cdot; \leqslant)$, $\quad \mathbf{R} = (\mathbb{R}; 0, 1, +, -, \cdot; \leqslant)$

**Examples**

For $\mathcal{L} = (\circ^{(2)}, \varepsilon^{(0)})$ we have $\mathcal{L}$-structures $(\mathbb{Z}; +, 0)$, $(\mathbb{Q}; \cdot, 1)$, and $(\mathcal{Z}^*; \circ, \varepsilon)$.

**Note**

The notation $\mathbf{A} = (A; \omega_1, \ldots, \omega_m; \varrho_1, \ldots, \varrho_n)$ must **never** be abused for specifing the language.

Consider languages $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma) \subseteq (\mathcal{F}', \mathcal{R}', \sigma') = \mathcal{L}'$.

Let $\mathbf{A} = (A, \iota_{\mathcal{F}'}, \iota_{\mathcal{R}'})$ be an $\mathcal{L}'$-structure.

Constraining interpretations yields an $\mathcal{L}$-structure $\mathbf{A}|_{\mathcal{L}} = (A, \iota_{\mathcal{F}'}|_{\mathcal{F}}, \iota_{\mathcal{R}'}|_{\mathcal{R}})$.

$\mathbf{A}|_{\mathcal{L}}$ is the **$\mathcal{L}$-restriction** of $\mathbf{A}$.

$\mathbf{A}$ is an **$\mathcal{L}'$-expansion** of $\mathbf{A}|_{\mathcal{L}}$.

### Example

Consider $\mathcal{L}_R = (0, 1, +, -, \cdot) \subseteq (0, 1, +, -, \cdot; \leqslant) = \mathcal{L}_{OR}$.

$\mathbf{R} = (\mathbb{R}; 0, 1, +, -, \cdot; \leqslant)$ is an $\mathcal{L}_{OR}$-Structure, and $\mathbf{R}|_{\mathcal{L}_R} = (\mathbb{R}; 0, 1, +, -, \cdot)$.

The ring of real numbers is the $\mathcal{L}_R$-restriktion of the ordered ring.

The ordered ring of real numbers is an $\mathcal{L}_{OR}$-expansion the ring.

$(\mathbb{R}; 0, 1, +, -, \cdot; \geqslant)$ is another $\mathcal{L}_{OR}$-expansion of $(\mathbb{R}; 0, 1, +, -, \cdot)$.

# Motivation of Extended Terms

We are going to interprete funtion symbols as functions.

Terms are going to describe functions, too.

**Example (Polynomial functions)**

$$f : \mathbb{R}^3 \longrightarrow \mathbb{R} \quad \text{mit} \quad f(x, y, z) = x^4 + 2xy - 5y$$

- Using $\mathcal{L} = (0, 1, +, -, \cdot)$ we define $f$ using a term.
- $f$ is suffixed with a list of variables serving as formal parameters.
- The order of variables is relevant.
- All variables of the term must be listed.
- It is admissible to list further variables ($z$ in our example).

Proceed this way without having to name functions (in the formal theory):

$$(x^4 + 2xy - 5y)(x, y, z)$$

Generalize this idea to atomic formulas.

Consider a language $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$.

Let $t \in \mathcal{T}$, $x_1, \dots, x_n \in \mathcal{V}$ pairwise different such that $\mathcal{V}(t) \subseteq \{x_1, \dots, x_n\}$.

Then $(x_1, \dots, x_n)$ is an **extension** of $t$.

The ordered pair $(t, (x_1, \dots, x_n))$ is an **extended term**.

Convenient **notation** $t(x_1, \dots, x_n)$.

For $\mathcal{V}(t) = \emptyset$ we do not distinguish between $t()$ and $t$.

$\mathcal{T}(x_1, \dots, x_n) := \{ (t, (x_1, \dots, x_n)) \mid t \in \mathcal{T} \text{ und } \mathcal{V}(t) \subseteq \{x_1, \dots, x_n\} \}$

### Note

- Notation $t(x_1, \dots, x_n)$ contains implicit assertion about the variables of $t$.
- Similarly, $\mathcal{T}(x_1, \dots, x_n)$ constrains the possible choices for $t$.

Analogously: **extended atomic formulas** $\varphi(x_1, \dots, x_n)$, $\mathcal{A}(x_1, \dots, x_n)$.

# Semantics: Term Functions and Definable Relations

Consider a language $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$ and an $\mathcal{L}$-structure $\mathbf{A}$.

Let $t(x_1, \dots, x_n)$ be an extended term.

The **term function** $t^{\mathbf{A}} : A^n \to A$ is defined recursively wrt. $|t| \in \mathbb{N}$:

(i) $t = c \in \mathcal{F}$ with $\sigma(c) = 0 \Longrightarrow t^{\mathbf{A}}(a_1, \dots, a_n) = c^{\mathbf{A}}$.

(ii) $t = x_i \in \mathcal{V}$ for $i \in \{1, \dots, n\} \Longrightarrow t^{\mathbf{A}}(a_1, \dots, a_n) = a_i$.

(iii) $t = f(t_1, \dots, t_m)$ mit $f \in \mathcal{F}$, $\sigma(f) = m > 0$ and $t_1, \dots, t_m \in \mathcal{T} \Longrightarrow$
$t^{\mathbf{A}}(a_1, \dots, a_n) = f^{\mathbf{A}}(t_1^{\mathbf{A}}(a_1, \dots, a_n), \dots, t_m^{\mathbf{A}}(a_1, \dots, a_n))$
using extended terms $t_1(x_1, \dots, x_n), \dots, t_m(x_1, \dots, x_n)$.

Let $\varphi(x_1, \dots, x_n)$ be an extended atomic formula.

Define $\varphi^{\mathbf{A}} : A^n \to \{\bot, \top\}$ as follows:

(i) $\varphi = (t_1 = t_2) \Longrightarrow \varphi^{\mathbf{A}}(a_1, \dots, a_n) = \top \Leftrightarrow t_1^{\mathbf{A}}(a_1, \dots, a_n) = t_2^{\mathbf{A}}(a_1, \dots, a_n)$.

(ii) $\varphi = R(t_1, \dots, t_m)$ for $R \in \mathcal{R}$ with $\sigma(R) = m \Longrightarrow$
$\varphi^{\mathbf{A}}(a_1, \dots, a_n) = R^{\mathbf{A}}(t_1^{\mathbf{A}}(a_1, \dots, a_n), \dots, t_m^{\mathbf{A}}(a_1, \dots, a_n))$,
using extended terms $t_1(x_1, \dots, x_n), \dots, t_m(x_1, \dots, x_n)$.

# Semantics: Validity and Models

Consider a language $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$ and an $\mathcal{L}$-structure $\mathbf{A}$.

Let $\varphi(x_1, \ldots, x_n)$ be an extended atomic formula.

$\varphi(x_1, \ldots, x_n)$ is **valid in A at the point** $(a_1, \ldots, a_n) \in A^n$, if $\varphi^{\mathbf{A}}(a_1, \ldots, a_n) = \top$.

Notation: $\mathbf{A} \models \varphi(a_1, \ldots, a_n)$.

## Observation

$\mathbf{A} \models \varphi(a_1, \ldots, a_n)$ for all $(a_1, \ldots, a_n) \in A^n$ does not depend on the extension.

$\varphi$ is **valid in A**, if $\varphi^{\mathbf{A}}(a_1, \ldots, a_n) = \top$ for all $(a_1, \ldots, a_n) \in A^n$.

Alternatively, we say $\mathbf{A}$ is a **model** of $\varphi$. Notation: $\mathbf{A} \models \varphi$.

A set $\Phi$ of atomic formulas is **valid in A**, if $\mathbf{A} \models \varphi$ for all $\varphi \in \Phi$.

Alternatively, we say $\mathbf{A}$ is a **model** of $\Phi$. Notation: $\mathbf{A} \models \Phi$.

# Example: Trivial Models

Consider a language $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$.

Let $M = \{m\}$ for a set $m$. We are going to define an $\mathcal{L}$-structure **M** on $M$:

- For $f \in \mathcal{F}$ with $\sigma(f) = n$ set $f^{\mathbf{M}}(m, \ldots, m) := m$.
- For $R \in \mathcal{R}$ with $\sigma(R) = n$ set $R^{\mathbf{M}}(m, \ldots, m) := \top$.

**M** is the **trivial $\mathcal{L}$-structure** with universe $M$.

## Lemma

$\mathbf{M} \models \Phi$ *for all* $\Phi \subseteq A$. *In particular, each set of atomic formulas has a model.*

## Proof.

Let $\varphi \in \Phi$, and let $\varphi(x_1, \ldots, x_n)$ be an extended atomic formula.

**Case 1:** $\varphi = (t_1 = t_2)$. Then $t_1^{\mathbf{M}}(m, \ldots, m) = m = t_2^{\mathbf{M}}(m, \ldots, m)$ , thus $\varphi^{\mathbf{M}}(m, \ldots, m) = (t_1 = t_2)^{\mathbf{M}}(m, \ldots, m) = \top$.

**Case 2:** $\varphi = R(t_1, \ldots, t_k)$. Then $\varphi^{\mathbf{M}}(m, \ldots, m) = R(t_1, \ldots, t_k)^{\mathbf{M}}(m, \ldots, m) = R^{\mathbf{M}}(t_1^{\mathbf{M}}(m, \ldots, m), \ldots, t_k^{\mathbf{M}}(m, \ldots, m)) = R^{\mathbf{M}}(m, \ldots, m) = \top$. □

# Syntax: First-Order Formulas

Consider a language $\mathscr{L}$.

We fix a set $\mathscr{O} = \{\mathsf{false}, \mathsf{true}, \neg, \wedge, \vee, \longrightarrow, \longleftrightarrow\}$ of **logical operators**.

We **say** *false, true, not, and, or, if ... then, if and only if*.

We assume $\mathscr{Z} \cap \mathscr{O} = \emptyset$ and **define** $\mathscr{Z}' = \mathscr{Z} \cup \mathscr{O}$.

We fix a set $\{\forall, \exists\}$ of **quantifier symbols**.

We **say** *for all, there exists*.

We assume $\mathscr{Z}' \cap \{\forall, \exists\} = \emptyset$ and **define** $\mathscr{Z}'' = \mathscr{Z}' \cup \{\forall, \exists\}$.

The set $\mathscr{Q}^1$ of **first-order $\mathscr{L}$-formulas** is the smallest subset of $\mathscr{Z}''^*$ such that

(i) $\mathscr{A} \subseteq \mathscr{Q}^1$ und $\{\mathsf{false}, \mathsf{true}\} \subseteq \mathscr{Q}^1$.

(ii) $\varphi \in \mathscr{Q}^1 \Longrightarrow \neg(\varphi) \in \mathscr{Q}^1$

(iii) $\varphi, \psi \in \mathscr{Q}^1 \Longrightarrow (\varphi) \wedge (\psi),\ (\varphi) \vee (\psi),\ (\varphi) \longrightarrow (\psi),\ (\varphi) \longleftrightarrow (\psi) \in \mathscr{Q}^1$

(iv) $\varphi \in \mathscr{Q}^1$ und $x \in \mathscr{V} \Longrightarrow \forall x(\varphi),\ \exists x(\varphi) \in \mathscr{Q}^1$.

# Syntax: Special Types of Formulas

Atomic formulas, negated atomic formulas, true, and false are **base formulas**.

**Note**

Base formulas correspond to literals in propositional logic.

Let $\varphi, \psi \in \mathcal{Q}^1$.

$(\varphi) \wedge (\psi) \in \mathcal{Q}^1$ is a **conjunction**.

$(\varphi) \vee (\psi) \in \mathcal{Q}^1$ is a **disjunction**.

$(\varphi) \longrightarrow (\psi) \in \mathcal{Q}^1$ is an **implication** with **antecedens** $\varphi$ und **succedens** $\psi$.

$(\varphi) \longleftrightarrow (\psi) \in \mathcal{Q}^1$ is a **biimplication**.

A word $\forall x \in \mathcal{Z}''^*$ with $x \in \mathcal{V}$ is a **universal quantifier**.
$\forall x(\varphi) \in \mathcal{Q}^1$ is a **universally quantified formula** with **matrix** $\varphi$.

A word $\exists x \in \mathcal{Z}''^*$ with $x \in \mathcal{V}$ is an **existential quantifier**.
$\exists x(\varphi) \in \mathcal{Q}^1$ is an **existentially quantified formula** with **matrix** $\varphi$.

# Precedence Conventions

For reducing the number of parentheses in informal notations we agree:

- $=$ and operators in $\mathcal{R}$ bind stronger than $\neg$.
- $\neg$ binds stronger than all other logical operators and quantifiers.
- $\wedge$ binds stronger than $\vee$.
- $\vee$ binds stronger than $\longrightarrow$.
- $\longrightarrow$ binds stronger than $\longleftrightarrow$.
- Parentheses around quantified subformulas may be omitted.
- Implication is right associative: $\varphi_1 \longrightarrow \varphi_2 \longrightarrow \varphi_3 = \varphi_1 \longrightarrow (\varphi_2 \longrightarrow \varphi_3)$.

**Example for $\mathcal{L} = (1, \cdot)$**

$$\big(\neg(p = 1)\big) \wedge \big(\forall a(\forall b(\exists q(\cdot(p,q) = \cdot(a,b)) \longrightarrow$$
$$(\exists q(\cdot(p,q) = a) \vee \exists q(\cdot(p,q) = b)))))\big) \in \mathcal{Q}^1$$

is written as $\neg p = 1 \wedge \forall a \forall b(\exists q(p \cdot q = a \cdot b) \longrightarrow \exists q(p \cdot q = a) \vee \exists q(p \cdot q = b))$.

We always make explicit the scope of quantifiers with parentheses.

# Syntax: Free vs. Bound Occurrences of Variables

An **occurrence** of $x \in \mathcal{V}$ in $\varphi \in \mathcal{Q}^1$ is an appearance inside a term.

An occurrence of $x$ within a subformula $\exists x(\dots)$ or $\forall x(\dots)$ is **bound**.

All other occurrences are **free**.

$\mathcal{V}_f(\varphi)$ is the set of all variables that occur freely in $\varphi$.

$\mathcal{V}_b(\varphi)$ is the set of all variables that occur boundly in $\varphi$.

$\mathcal{V}(\varphi) := \mathcal{V}_f(\varphi) \cup \mathcal{V}_b(\varphi)$ is the set of all variables **occurring** in $\varphi$.

### Example

$$\mathcal{L} = (f^{(1)}, g^{(2)}), \quad \varphi = \exists w \forall w \big(w = f(y)\big) \wedge \exists x \big(f(x) = y\big) \vee \forall z \big(g(w, y) = w\big)$$

- The variable $z$ does **not** occur in $\varphi$.
- $\mathcal{V}_f(\varphi) = \{w, y\}$, $\mathcal{V}_b(\varphi) = \{w, x\}$ and $\mathcal{V}(\varphi) = \{w, x, y\}$.
- $\mathcal{V}_f(\varphi) \cap \mathcal{V}_b(\varphi) \neq \varnothing$.

There are **no** “free variables” or “bound variables”!

# Syntax: Quantifier-Free Formulas and Sentences

(i) $\mathcal{A} \subseteq \mathcal{Q}^1$ und $\{\text{false}, \text{true}\} \subseteq \mathcal{Q}^1$.

(ii) $\varphi \in \mathcal{Q}^1 \Longrightarrow \neg(\varphi) \in \mathcal{Q}^1$

(iii) $\varphi, \psi \in \mathcal{Q}^1 \Longrightarrow (\varphi) \wedge (\psi),\ \ (\varphi) \vee (\psi),\ \ (\varphi) \longrightarrow (\psi),\ \ (\varphi) \longleftrightarrow (\psi) \in \mathcal{Q}^1$

(iv) $\varphi \in \mathcal{Q}^1$ und $x \in \mathcal{V} \Longrightarrow \forall x(\varphi),\ \ \exists x(\varphi) \in \mathcal{Q}^1$.

The set $\mathcal{Q}^0 \subseteq \mathcal{Q}^1$ of **quantifier-free formulas** is formed using only (i)–(iii).

From now on **formulas** are first-order formulas, and we write $\mathcal{Q} := \mathcal{Q}^1$.

A **sentence** is a formula $\varphi \in \mathcal{Q}$ with $\mathcal{V}_f(\varphi) = \varnothing$.
$\mathcal{Q}_\varnothing \subseteq \mathcal{Q}$ is the set of all sentences.

**Example for $\mathcal{L}_R = (0, 1, +, -, \cdot)$**

- $(a + b) \cdot c = a \cdot c + b \cdot c \in \mathcal{Q}^0$
- false $\vee\ \forall a \forall b \forall c\big((a + b) \cdot c = a \cdot c + b \cdot c\big) \vee 1 = 0 \in \mathcal{Q}_\varnothing$

# Extended Formulas and Closures

Let $\varphi \in \mathcal{Q}$, $x_1, \dots, x_n \in \mathcal{V}$ pairwise different such that $\mathcal{V}_f(\varphi) \subseteq \{x_1, \dots, x_n\}$.

The ordered pair $(\varphi, (x_1, \dots, x_n))$ is an **extended formula**.

Convenient **notation** as with atomic formulas: $\varphi(x_1, \dots, x_n)$.

Extended sentences $(\varphi, \emptyset)$ are written as $\varphi()$ and can be identified with $\varphi$.

Let $\varphi(x_1, \dots, x_n)$ be an extended atomic formula.

The sentence $\underline{\forall}\varphi := \forall x_1 \dots \forall x_n \varphi$ is a **universal closure** of $\varphi$.

The sentence $\underline{\exists}\varphi := \exists x_1 \dots \exists x_n \varphi$ is an **existential closure** of $\varphi$.

Alternative **notation** for the universal closure: $\bar{\varphi} := \underline{\forall}\varphi$.

For $\Phi \subseteq \mathcal{Q}$ we define $\bar{\Phi} := \{\, \bar{\varphi} \mid \varphi \in \Phi \,\}$.

# Semantics of First-Order Formulas

We agree that $\bot < \top$. Consider an $\mathcal{L}$-structure **A**, and an extended formula $\varphi(x_1, \ldots, x_n)$. We **define** $\varphi^{\mathbf{A}} : A^n \rightarrow \{\bot, \top\}$. Let $a_1, \ldots, a_n \in A$:

- For $\varphi \in \mathcal{A}$ we define $\varphi^{\mathbf{A}}(a_1, \ldots, a_n)$ as usual.
- $\text{false}^{\mathbf{A}}(a_1, \ldots, a_n) = \bot$ und $\text{true}^{\mathbf{A}}(a_1, \ldots, a_n) = \top$.
- $(\neg\psi)^{\mathbf{A}}(a_1, \ldots, a_n) = \top \iff \psi^{\mathbf{A}}(a_1, \ldots, a_n) = \bot$.
- $(\psi_1 \wedge \psi_2)^{\mathbf{A}}(a_1, \ldots, a_n) = \min\{\psi_1^{\mathbf{A}}(a_1, \ldots, a_n), \psi_2^{\mathbf{A}}(a_1, \ldots, a_n)\}$.
- $(\psi_1 \vee \psi_2)^{\mathbf{A}}(a_1, \ldots, a_n) = \max\{\psi_1^{\mathbf{A}}(a_1, \ldots, a_n), \psi_2^{\mathbf{A}}(a_1, \ldots, a_n)\}$.
- $(\psi_1 \longrightarrow \psi_2)^{\mathbf{A}}(a_1, \ldots, a_n) = \top \iff \psi_1^{\mathbf{A}}(a_1, \ldots, a_n) \leqslant \psi_2^{\mathbf{A}}(a_1, \ldots, a_n)$.
- $(\psi_1 \longleftrightarrow \psi_2)^{\mathbf{A}}(a_1, \ldots, a_n) = \top \iff \psi_1^{\mathbf{A}}(a_1, \ldots, a_n) = \psi_2^{\mathbf{A}}(a_1, \ldots, a_n)$.
- If $\varphi = \forall x(\psi)$, then $\psi(x_1, \ldots, x_n, x)$ is an extended formula;
$$\big(\forall x(\psi)\big)^{\mathbf{A}}(a_1, \ldots, a_n) = \min\Big\{ \psi^{\mathbf{A}}(a_1, \ldots, a_n, a) \in \{\bot, \top\} \;\Big|\; a \in A \Big\}$$
- If $\varphi = \exists x(\psi)$ then $\psi(x_1, \ldots, x_n, x)$ is an extended formulas;
$$\big(\exists x(\psi)\big)^{\mathbf{A}}(a_1, \ldots, a_n) = \max\Big\{ \psi^{\mathbf{A}}(a_1, \ldots, a_n, a) \in \{\bot, \top\} \;\Big|\; a \in A \Big\}$$

# Validity, Models, Model Classes, and Semantic Equivalence

Consider a language $\mathcal{L}$ and an $\mathcal{L}$-structure $\mathbf{A}$.

For $\varphi \in \mathcal{Q}$ with extension $(x_1, \ldots, x_n)$, $a_1, \ldots, a_n \in A$, and $\Phi \subseteq \mathcal{Q}$ define $\mathbf{A} \models \varphi(a_1, \ldots, a_n)$, $\mathbf{A} \models \varphi$, and $\mathbf{A} \models \Phi$ in analogy to atomic formulas.

## Note

$\mathbf{A} \models \varphi \iff \mathbf{A} \models \underline{\forall}\varphi$ and $\mathbf{A} \models \Phi \iff \mathbf{A} \models \bar{\Phi}$

Let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures.

$\varphi \in \mathcal{A}$ is **valid in** $\mathfrak{A}$, if $\mathbf{A} \models \varphi$ for all $\mathbf{A} \in \mathfrak{A}$. **Notation:** $\mathfrak{A} \models \varphi$.

$\Phi \subseteq \mathcal{A}$ is **valid in** $\mathfrak{A}$, if $\mathbf{A} \models \Phi$ for all $\mathbf{A} \in \mathfrak{A}$. **Notation:** $\mathfrak{A} \models \Phi$.

For fixed $\mathcal{L}$ the **model class** of $\Phi \subseteq \mathcal{Q}$ is $\mathrm{Mod}(\Phi) = \{\mathbf{A} \mid \mathbf{A} \models \Phi\}$.

$\varphi \in \mathcal{Q}$ is **generally valid**, if $\mathbf{A} \models \varphi$ for all $\mathcal{L}$-structures $\mathbf{A}$. **Notation:** $\models \varphi$

$\Phi \subseteq \mathcal{Q}$ is **generally valid**, if $\mathbf{A} \models \Phi$ for all $\mathcal{L}$-structures $\mathbf{A}$. **Notation:** $\models \Phi$

$\varphi, \psi \in \mathcal{Q}$ are **semantically equivalent**, if $\models \varphi \longleftrightarrow \psi$. **Notation:** $\varphi \approx \psi$.

# Some Axiomatizations

$$\mathcal{L}_M = (1, \circ), \quad \Xi_M = \left\{ (x \circ y) \circ z = x \circ (y \circ z), \;\; x \circ 1 = x, \;\; 1 \circ x = x \right\}.$$

**Example (Monoids)**

$\mathfrak{M} = \mathrm{Mod}(\Xi_M)$ is the class of all monoids as $\mathcal{L}_M$-structures.

**Example (Groups)**

Set $\Xi := \Xi_M \cup \{\forall x \exists y (x \circ y = 1)\}$.

Then $\mathfrak{G}_M = \mathrm{Mod}(\Xi)$ is the class of all groups as $\mathcal{L}_M$-structures.

**Exercise**

1. Axiomatize groups in the language $\mathcal{L}_S = (\circ) \subseteq \mathcal{L}_M$ of semigroups.
2. Axiomatize rings in the language $\mathcal{L}_R = (0, 1, +, -, \cdot)$.
3. Axiomatize integral domains in the language $\mathcal{L}_R$.

# Important Semantic Equivalences for Boolean Operators (1)

Consider a language $\mathcal{L}$, and let $\chi, \psi, \varphi \in \mathcal{Q}$:

- $\chi \wedge \psi \approx \psi \wedge \chi$
  $\chi \vee \psi \approx \psi \vee \chi$ (commutativity)
- $\chi \wedge (\psi \wedge \varphi) \approx (\chi \wedge \psi) \wedge \varphi$
  $\chi \vee (\psi \vee \varphi) \approx (\chi \vee \psi) \vee \varphi$ (associativity)
- $\chi \wedge \chi \approx \chi, \quad \chi \vee \chi \approx \chi$ (idempotence)
- $\chi \wedge (\chi \vee \psi) \approx \chi$
  $\chi \vee (\chi \wedge \psi) \approx \chi$ (absorption)
- $\chi \wedge (\psi \vee \varphi) \approx (\chi \wedge \psi) \vee (\chi \wedge \varphi)$
  $\chi \vee (\psi \wedge \varphi) \approx (\chi \vee \psi) \wedge (\chi \vee \varphi)$ (distributivity)
- $\neg(\chi \wedge \psi) \approx \neg\chi \vee \neg\psi$
  $\neg(\chi \vee \psi) \approx \neg\chi \wedge \neg\psi$ (de Morgan)
- $\neg\neg\chi \approx \chi$ (involution)

# Important Semantic Equivalences for Boolean Operators (2)

- $\chi \land \text{true} \approx \chi$
  $\chi \lor \text{false} \approx \chi$ (neutrality)
- $\neg\text{false} \approx \text{true}$
  $\neg\text{true} \approx \text{false}$
  $\chi \land \text{false} \approx \text{false}$
  $\chi \lor \text{true} \approx \text{true}$ (definiteness)
- $\chi \land \neg\chi \approx \text{false}$
  $\chi \lor \neg\chi \approx \text{true}$ (tertium non datur)
- $\chi \longleftrightarrow \psi \approx (\chi \longrightarrow \psi) \land (\psi \longrightarrow \chi)$
  $\chi \longrightarrow \psi \approx \neg\chi \lor \psi$ (reduction to $\land$, $\lor$, $\neg$)
- $\chi \longrightarrow \psi \approx \neg\psi \longrightarrow \neg\chi$ (contrapositive)
- $\chi \longleftrightarrow \psi \approx \neg\psi \longleftrightarrow \neg\chi$ (contrapositive)
- $\neg(\chi \longrightarrow \psi) \approx \chi \land \neg\psi$ (negation of implication)
- $\neg(\chi \longleftrightarrow \psi) \approx \chi \land \neg\psi \lor \psi \land \neg\chi$ (negation of biimplication)

# Important Semantic Equivalences with Quantifiers

- $\exists x(\varphi \lor \psi) \approx \exists x(\varphi) \lor \exists x(\psi)$
- $\exists x(\varphi \land \psi) \approx \exists x(\varphi) \land \psi$, if $x \notin \mathcal{V}_f(\psi)$
- $\forall x(\varphi \land \psi) \approx \forall x(\varphi) \land \forall x(\psi)$
- $\forall x(\varphi \lor \psi) \approx \forall x(\varphi) \lor \psi$, if $x \notin \mathcal{V}_f(\psi)$
- $\neg\exists x(\varphi) \approx \forall x(\neg\varphi)$
- $\neg\forall x(\varphi) \approx \exists x(\neg\varphi)$

## Exercise

Show the following:

- $\exists x(\varphi \land \psi) \not\approx \exists x(\varphi) \land \exists x(\psi)$
- $\forall x(\varphi \lor \psi) \not\approx \forall x(\varphi) \lor \forall x(\psi)$
- $\forall x \exists y(\varphi) \not\approx \exists x \forall y(\varphi)$

Consider a language $\mathcal{L}$.

Let $x_1, \ldots, x_n$ pairwise different, and let $t_1, \ldots, t_n \in \mathcal{T}$.

Let $t \in \mathcal{T}$.

$t[t_1/x_1, \ldots, t_n/x_n] \in \mathcal{T}$ is obtained by replacing in $t$ all occurrences of $x_i$ by $t_i$.

**Example for $\mathcal{L} = (f^{(3)}, g^{(1)})$**

$$f\big(x, g(y), g(g(z))\big)\big[f(y, x, z)/x, z/y, x/z\big] \equiv f\big(f(y, x, z), g(z), g(g(x))\big)$$

Let $\varphi \in \mathcal{Q}$.

$\varphi[t_1/x_1, \ldots, t_n/x_n] \in \mathcal{Q}$ is obtained by replacing in $\varphi$ all **free** occurrences of $x_i$ by $t_i$.

**Example for $\mathcal{L} = (f^{(3)}, g^{(1)})$**

$$x = g(y) \land \exists x(y = g(x))[f(x, y, z)/x, x/y] \equiv f(x, y, z) = g(x) \land \exists x(x = g(x))$$

## Lemma

*Consider a language $\mathcal{L}$.*

*Let $t_1(y_1, \ldots, y_m), \ldots, t_n(y_1, \ldots, y_m)$ be extended terms.*

*Let $\mathbf{A}$ be an $\mathcal{L}$-structure, and let $b_1, \ldots, b_m \in A$.*

(i) *Let $t(x_1, \ldots, x_n)$ be an extended Term.*
*Set $t' := t[t_1/x_1, \ldots, t_n/x_n]$. Then for $t'(y_1, \ldots, y_m)$ we have*

$$t'^{\mathbf{A}}(b_1, \ldots, b_m) = t^{\mathbf{A}}\left(t_1^{\mathbf{A}}(b_1, \ldots, b_m), \ldots, t_n^{\mathbf{A}}(b_1, \ldots, b_m)\right).$$

(ii) *Let $\varphi(x_1, \ldots, x_n)$ be an extended formula with $\mathcal{V}_b(\varphi) \cap \{y_1, \ldots, y_m\} = \varnothing$.*
*Set $\varphi' := \varphi[t_1/x_1, \ldots, t_n/x_n]$. Then for $\varphi'(y_1, \ldots, y_m)$ we have*

$$\varphi'^{\mathbf{A}}(b_1, \ldots, b_m) = \varphi^{\mathbf{A}}\left(t_1^{\mathbf{A}}(b_1, \ldots, b_m), \ldots, t_n^{\mathbf{A}}(b_1, \ldots, b_m)\right).$$

- The identical extensions $(y_1, \ldots, y_m)$ for $t_1, \ldots, t_n$ are not really a restriction.
- $\mathcal{V}(t_i) \subseteq \{y_1, \ldots, y_m\}$, thus $\mathcal{V}_b(\varphi) \cap \{y_1, \ldots, y_m\} = \varnothing \Longrightarrow \mathcal{V}_b(\varphi) \cap \bigcup_{i=1}^{n} \mathcal{V}(t_i) = \varnothing$.

# Exercises

1. Prove Part (i) of the Lemma.
2. Rephrase Part (ii) in terms of validity, i.e., using "$\models$."
3. Derive from Part (ii) a result for general validity, i.e. "$\models$" without reference to extended formulas or particular points.

max planck institut informatik

# Informal Notations Made Precise

In Mathematics, quantifier symbols are often used informally.

## Example

Consider the language $\mathcal{L} = (0, 1, +, -, \cdot; >)$.

- "‘$\exists\, \delta > 0 : \varphi$"’ stands for $\exists \delta (\delta > 0 \wedge \varphi)$.
- "‘$\forall\, \varepsilon > 0 : \varphi$"’ stands for $\forall \varepsilon (\varepsilon > 0 \longrightarrow \varphi)$.
- "‘$\exists! x : \varphi$"’ stands for $\exists x (\varphi \wedge \forall y (\varphi[y/x] \longrightarrow y = x))$.
- "‘$\exists^{>1} x : \varphi$"’ stands for $\exists x \exists y (x \neq y \wedge \varphi \wedge \varphi[y/x])$.

Notice that for “$\forall\, \varepsilon > 0 : \varphi$” and “$\exists\, \delta > 0 : \varphi$” in fact

$$\neg \forall \varepsilon (\varepsilon > 0 \longrightarrow \varphi) \approx \exists \varepsilon (\varepsilon > 0 \wedge \neg \varphi), \quad \neg \exists \delta (\delta > 0 \wedge \varphi) \approx \forall \delta (\delta > 0 \longrightarrow \neg \varphi).$$

max planck institut informatik

# Normal Forms for Terms in a Fixed $\mathcal{L}$-Structure

Consider a language $\mathcal{L}$ and a set $\mathcal{T}(x_1, \ldots, x_n)$ of extended terms.

Then every $\mathcal{L}$-structure $\mathbf{A}$ induces an equivalence relation $\sim_{\mathbf{A}}$ on $\mathcal{T}(x_1, \ldots, x_n)$:

$$t(x_1, \ldots, x_n) \sim_{\mathbf{A}} t'(x_1, \ldots, x_n) \quad :\Longleftrightarrow \quad t^{\mathbf{A}} = t'^{\mathbf{A}}.$$

$\mathcal{N} \subseteq \mathcal{T}(x_1, \ldots, x_n)$ is a set of **normal forms** for $\mathcal{T}(x_1, \ldots, x_n)$ in $\mathbf{A}$, if
for each $t(x_1, \ldots, x_n) \in \mathcal{T}(x_1, \ldots, x_n)$ there is $t'(x_1, \ldots, x_n) \in \mathcal{N}$ such that
$t'(x_1, \ldots, x_n) \sim_{\mathbf{A}} t(x_1, \ldots, x_n)$.

$\mathcal{N}$ if a set of **unique** (or **canonical**) normal forms in $\mathbf{A}$, if
there is exactly one such $t'(x_1, \ldots, x_n) \in \mathcal{N}$.

**Example for $L_R = (0, 1, +, -, \cdot)$, $\mathcal{T}(x)$, and $\mathbf{R} = (\mathbb{R}; 0, 1, +, -, \cdot)$**

$\mathbb{Z}[x]$ is a set of unique normal forms for $\mathcal{T}(x)$ in $\mathbf{R}$.

- The coefficients are formally Terms $0$, $1 + \cdots + 1$ oder $-(1 + \cdots + 1)$.
- The coefficient $0$ occurs only for the zero polynomial.

# Normal Forms for Formulas

Consider a language $\mathcal{L}$ and $\mathcal{Q}' \subseteq \mathcal{Q}$.

Then $\mathcal{N} \subseteq \mathcal{Q}'$ is a set of **normal forms** for $\mathcal{Q}'$, if for each $\varphi \in \mathcal{Q}'$ there is $\nu \in \mathcal{N}$ such that $\nu \approx \varphi$.

**Lemma (Negation Normal Forms)**

*The set $\mathcal{N}_{\text{NNF}} \subseteq \mathcal{Q}^0$ of $\wedge$-$\vee$-combinations of base formulas is a set of normal forms for quantifier-free formulas.*

**Proof.**

Rewrite "$\longleftrightarrow$" and "$\longrightarrow$" in terms of "$\neg$," "$\wedge$," "$\vee$."

Apply de Morgan to move inside all "$\neg$" to the atomic formulas.

Eliminate "$\neg\neg$" by involution. $\square$

We say that formulas in $\mathcal{N}_{\text{NNF}}$ are in **negation normal form (NNF)**.

# Conjunctive and Disjunctive Normal Forms

We generalize our notions of conjunctions and disjunctions:

For $n \in \mathbb{N}$ and $\varphi_1, \dots, \varphi_n \in \mathcal{Q}$ **conjunctions** and **disjunctions** are

$$\bigwedge_{i=1}^{n} \varphi_i = \begin{cases} \text{true}, & n = 0 \\ \varphi_1, & n = 1 \\ \varphi_1 \wedge \ldots \wedge \varphi_n, & n > 1 \end{cases} \quad \text{and} \quad \bigvee_{i=1}^{n} \varphi_i = \begin{cases} \text{false}, & n = 0 \\ \varphi_1, & n = 1 \\ \varphi_1 \vee \ldots \vee \varphi_n, & n > 1 \end{cases}$$

## Lemma (Disjunctive and Conjuncive Normal Forms)

*The set $\mathcal{N}_{\text{DNF}} \subseteq \mathcal{Q}^0$ of disjunctions of conjunctions of base formulas and the set $\mathcal{N}_{\text{CNF}} \subseteq \mathcal{Q}^0$ of conjunctions of disjunctions of base formulas are sets of normal forms for quantifier-free formulas.*

## Proof.

Compute an equivalent NNF and then apply the laws of distributivity. □

DNFs and CNFs are exponential in the size of the original formula in general!

# Prenex Normal Forms

A **prenex** formula is $Q_1 x_1 \dots Q_n x_n(\psi) \in \mathcal{Q}$ with $Q_i \in \{\exists, \forall\}$, $x_i \in \mathcal{V}$, and $\psi \in \mathcal{Q}^0$.

## Lemma (Prenex Normal Form)

*The set $\mathcal{N}_{\text{PNF}} \subseteq \mathcal{Q}$ of prenex formulas is a set of normal forms for formulas.*

## Proof.

Let $\varphi \in \mathcal{Q}$. We show by induction on $|\varphi| \in \mathbb{N}$ that there is $\varphi \approx \varphi' \in \mathcal{N}_{\text{PNF}}$.
Rewrite "$\longleftrightarrow$" and "$\longrightarrow$" in terms of "$\neg$," "$\wedge$," "$\vee$."

Case 1: For $\varphi \in \mathcal{A}$ we observe $\mathcal{A} \subseteq \mathcal{N}_{\text{PNF}}$, so we can set $\varphi' := \varphi$.

Case 2: For $\varphi = Qx(\psi)$ we find $\psi \approx \psi' \in \mathcal{N}_{\text{PNF}}$, and we set $\varphi' := Qx(\psi')$.

Case 3: For $\varphi = \neg\psi$, we find $\psi \approx \psi' \in \mathcal{N}_{\text{PNF}}$, and we know how to equivalently move the negation inside the prenex quantifier block of $\psi'$.

Case 4: For $\varphi = \psi_1 \varrho \psi_2$ with $\varrho \in \{\wedge, \vee\}$ we find $\psi_1 \approx Q_1 x_1 \dots Q_n x_n(\psi_1')$ and $\psi_2 \approx \bar{Q}_1 \bar{x}_1 \dots \bar{Q}_m \bar{x}_m(\psi_2')$ with $\psi_1', \psi_2' \in \mathcal{Q}^0$. We may assume w.l.o.g. $\{x_1, \dots, x_n\} \cap \mathcal{V}(\psi_2') = \emptyset$ and $\{\bar{x}_1, \dots, \bar{x}_m\} \cap \mathcal{V}(\psi_1') = \emptyset$ (else rename bound variables). Set $\varphi' := Q_1 x_1 \dots Q_n x_n \bar{Q}_1 \bar{x}_1 \dots \bar{Q}_m \bar{x}_m(\psi_1' \varrho \psi_2')$. $\square$

# Normal Forms for Formulas in a Fixed $\mathcal{L}$-Structure

Consider a language $\mathcal{L}$, and $\mathcal{Q}' \subseteq \mathcal{Q}$.

Every $\mathcal{L}$-structure $\mathbf{A}$ induces an equivalence relation $\approx_{\mathbf{A}}$ on $\mathcal{Q}'$:

$$\varphi \approx_{\mathbf{A}} \varphi' \quad :\Longleftrightarrow \quad \mathbf{A} \models \varphi \longleftrightarrow \varphi'.$$

$\mathcal{N} \subseteq \mathcal{Q}'$ is a set of **(unique/canonical) normal forms** for $\mathcal{Q}'$ in $\mathbf{A}$, if for each $\varphi \in \mathcal{Q}'$ there is (exactly one) $\varphi' \in \mathcal{N}$ such that $\varphi' \sim_{\mathbf{A}} \varphi$.

A **positive** formula is an $\wedge$-$\vee$-combination of atomic formulas.

## Example (Positive Normal Forms over the Reals)

$\mathcal{L}'_{OR} = (0, 1, +, -, \cdot; \leqslant, \geqslant, <, >, \neq)$, $\mathbf{R} = (\mathbb{R}; 0, 1, +, -, \cdot; \leqslant, \geqslant, <, >, \neq)$:.

1. The set $\mathcal{N}_{\mathrm{POS}} \subseteq \mathcal{Q}^0$ of positive formulas is a set of normal forms for $\mathcal{Q}^0$ in $\mathbf{R}$.
2. Consider $\mathcal{A}_{\{x_1,\dots,x_n\}} = \{\, \varphi \in \mathcal{A} \mid \mathcal{V}(\varphi) \subseteq \{x_1, \dots, x_n\} \,\}$. Then

   $$\{\, f \varrho 0 \in \mathcal{A}_{\{x_1,\dots,x_n\}} \mid \varrho \in \{\leqslant, \geqslant, <, >, =, \neq\},\ f \in \mathbb{Z}[x_1, \dots, x_n] \,\}$$

   is a set of normal forms for $\mathcal{A}_{x_1,\dots,x_n}$ in $\mathbf{R}$. Much better but still not unique: primitive polynomials $f$ with positive head coefficients.

Consider a language $\mathcal{L}$, a class $\mathfrak{A}$ of $\mathcal{L}$-structures, and $\Phi \subseteq \mathcal{Q}$.

$\mathfrak{A}$ **admits quantifier elimination (QE) for** $\Phi$, if
for each $\varphi \in \Phi$ there is $\varphi' \in \mathcal{Q}^0$ such that $\mathfrak{A} \models \varphi' \longleftrightarrow \varphi$.

A **quantifier elimination procedure (QEP)** for $\Phi$ and $\mathfrak{A}$ is an algorithm that given $\varphi \in \Phi$ computes $\varphi' \in \mathcal{Q}^0$ such that $\mathfrak{A} \models \varphi' \longleftrightarrow \varphi$.

If $\mathfrak{A} = \{\mathbf{A}\}$, then we simply say **A** admits QE for $\Phi$ / QEP for **A** and $\Phi$.

If $\Phi = \mathcal{Q}$, then we need not explicitly refer to $\Phi$.

# Quantifier Elimination Without Introducing New Variables

## Lemma

*Consider a language $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$ and a class $\mathfrak{A}$ of $\mathcal{L}$-structures.*
*Let $\varphi \in \mathcal{Q}$, $\varphi' \in \mathcal{Q}^0$ such that $\mathfrak{A} \models \varphi' \longleftrightarrow \varphi$.*
*Assume that at least one of the following conditions holds:*

(i) $\mathcal{V}_f(\varphi) \neq \emptyset$

(ii) *There is $c \in \mathcal{F}$ with $\sigma(c) = 0$.*

*Then one can compute $\varphi'' \in \mathcal{Q}^0$ such that $\mathfrak{A} \models \varphi'' \longleftrightarrow \varphi$ and $\mathcal{V}(\varphi'') \subseteq \mathcal{V}_f(\varphi)$.*

## Proof.

The construction of $\varphi''$ depends on the condition that holds in the Lemma:

(i) Let $y \in \mathcal{V}_f(\varphi)$, $\mathcal{V}(\varphi') \setminus \mathcal{V}_f(\varphi) = \{z_1, \dots, z_n\}$. Set $\varphi'' := \varphi'[y/z_1, \dots, y/z_n]$.

(ii) Let $\mathcal{V}(\varphi') \setminus \mathcal{V}_f(\varphi) = \{z_1, \dots, z_n\}$. Set $\varphi'' := \varphi'[c/z_1, \dots, c/z_n]$. $\square$

# Quantifier Elimination and Addition of Constants

## Lemma

*Consider languages $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \sigma)$, $\mathcal{L}' = (\mathcal{F}', \mathcal{R}, \sigma') \supseteq \mathcal{L}$ such that $\sigma'(f) = 0$ for all $f \in \mathcal{F}' \setminus \mathcal{F}$. Let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures that admits QE. Let $\mathfrak{A}'$ be a class of $\mathcal{L}'$-structures such that $\mathbf{A}'|\mathcal{L} \in \mathfrak{A}$ for each $\mathbf{A}' \in \mathfrak{A}'$. Then $\mathfrak{A}'$ admits QE, and every QEP for $\mathfrak{A}$ induces a QEP for $\mathfrak{A}'$.*

## Proof.

Let $\varphi$ be an $\mathcal{L}'$-formula. Then there exist $c_1, \ldots, c_n \in \mathcal{F}'$ with $\sigma(c_i) = 0$, $y_1, \ldots, y_n \in \mathcal{V} \setminus \mathcal{V}(\varphi)$, and an $\mathcal{L}$-formula $\psi$ such that $\varphi = \psi[c_1/y_1, \ldots, c_n/y_n]$. Compute $\psi' \in \mathfrak{A}$ such that $\mathfrak{A} \models \psi' \longleftrightarrow \psi$. It follows that $\mathfrak{A}' \models \psi' \longleftrightarrow \psi$ and furthermore $\mathfrak{A}' \models \psi'[c_1/y_1, \ldots, c_n/y_n] \longleftrightarrow \psi[c_1/y_1, \ldots, c_n/y_n]$. $\square$

# Quantifier Elimination and Subclasses

Consider a language $\mathcal{L}$, $\Phi \subseteq \mathcal{Q}$.

## Obviously ...

Consider a class $\mathfrak{A}$ of $\mathcal{L}$-structures that admits *QE* for $\Phi$. Let $\mathfrak{A}' \subseteq \mathfrak{A}$.
Then $\mathfrak{A}'$ admits QE, and every QEP for $\mathfrak{A}$ and $\Phi$ is also a QEP for $\mathfrak{A}'$ and $\Phi$.
This holds in particular for $\mathfrak{A}' = \{\mathbf{A}\}$ for some $\mathcal{L}$-structure $\mathbf{A}$. □

Less obviously, the converse does **not** hold:

## Example

Consider $\mathcal{L} = ()$, $\mathbf{A} = (\{1\})$, $\mathbf{B} = (\{1, 2\})$. We are soon going to show that both $\mathbf{A}$ and $\mathbf{B}$ have a QEP. Here we show that $\mathfrak{A} = \{\mathbf{A}, \mathbf{B}\}$ does **not** admit QE:
Consider $\varphi = \exists x(\neg x = y)$. Assume for a contradiction that there is $\varphi' \in \mathcal{Q}^0$ with $\mathfrak{A} \models \varphi' \longleftrightarrow \varphi$. We may assume w.l.o.g that $\mathcal{V}(\varphi') \subseteq \mathcal{V}_f(\varphi) = \{y\} \neq \emptyset$.
The only atomic formula possibly occurring in $\varphi'$ is $y = y$, which is semantically equivalent to true. It follows that $\varphi' \approx$ true or $\varphi' \approx$ false, in particular $\mathfrak{A} \models \varphi' \longleftrightarrow$ true or $\mathfrak{A} \models \varphi' \longleftrightarrow$ false. But $\mathbf{A} \models \varphi \longleftrightarrow$ false and $\mathbf{B} \models \varphi \longleftrightarrow$ true. Hence $\mathfrak{A} \not\models \varphi' \longleftrightarrow \varphi$, a contradiction.

Denote by $\mathcal{B} \subseteq \mathcal{Q}^0$ the set of all base formulas.

A **1-primitive $\mathcal{L}$-formula** is of the form $\exists x \bigwedge_{i=1}^{n} \varphi_i$ for $x \in \mathcal{V}$, $n \in \mathbb{N}$, and $\varphi_i \in \mathcal{B}$.

Denote by $\mathcal{P} \subseteq \mathcal{Q}$ the set of all 1-primitive $\mathcal{L}$-formulas.

### Theorem

*If a class $\mathfrak{A}$ of $\mathcal{L}$-structures admits QE for $\mathcal{P}$, then $\mathfrak{A}$ admits QE (for $\mathcal{Q}$), and every QEP for $\mathcal{P}$ in $\mathfrak{A}$ induces a QEP for $\mathfrak{A}$ (and $\mathcal{Q}$).*

### Proof.

Let $\varphi \in \mathcal{Q}$. Induction on the number $k$ of quantifiers: If $k = 0$, then we are done. For $k > 0$ transform $\varphi$ into PNF yielding $\bar{\varphi} := Q_1 x_1 \dots Q_k x_k \psi$. We are going to eliminate $Q_k x_k$ from $Q_k x_k \psi$. By means of $\forall x_k \psi \approx \neg \exists x_k \neg \psi$ we may w.l.o.g. assume that $Q_k = \exists$. Transform $\psi$ into DNF yielding $\exists x_k \bigvee_i \bigwedge_j \psi_{ij}$. Now

$$\mathfrak{A} \models \exists x_k \bigvee_i \bigwedge_j \psi_{ij} \longleftrightarrow \bigvee_i \exists x_k \bigwedge_j \psi_{ij} \longleftrightarrow \bigvee_i \psi_i' \quad \text{with} \quad \psi_i' \in \mathcal{Q}^0,$$

and the remaining quantifiers can be eliminated by induction hypothesis. $\square$

# Some Remarks on QE for 1-Primitive Formulas

## Minimize Quantifier Scope in 1-Primitive Formulas

Recall that $\exists x(\varphi \wedge \psi) \approx \exists x(\varphi) \wedge \psi$, if $x \notin \mathcal{V}_f(\psi)$.
It thus suffices to consider 1-primitive formulas $\exists x \bigwedge_{i=1}^{n} \varphi_i$, where each $\varphi_i$ actually contains $x$.

Denote by $\mathcal{P}^+ \subseteq \mathcal{P}$ the set of all positive 1-primitive $\mathcal{L}$-formulas.

## Restriction to Positive 1-Primitive Formulas

Consider $\mathcal{L}$ and $\mathfrak{A}$ such that every negative base formula is equivalent to a positive quantifier-free formula.

(i) If $\mathfrak{A}$ admits QE for $\mathcal{P}^+$, then $\mathfrak{A}$ admits QE (for $\mathcal{Q}$).

(ii) If there is a QEP for $\mathfrak{A}$ and $\mathcal{P}^+$ and an algorithm computing positive quantifier-free equivalents for negative base formulas, then this induces a QEP for $\mathfrak{A}$ (and $\mathcal{Q}$). □

# A Remark on Complexity

Thinking about 1-primitive formulas is a good first approach when looking for quantifier elimination procedures.

Due to the iterated DNF computations in combination with logical negation for universal quantifiers, our procedure based on quantifier elimination for $\mathcal{P}$ is **not elementary recursive** in general.

In the end, one hopefully finds something better.

# Quantifier Elimination for Infinite Sets

Consider $\mathcal{L} = ()$, and denote by $\mathfrak{A}$ the class of all infinite sets as $\mathcal{L}$-structures.

Consider a 1-primitive Formula

$$\varphi := \exists x \left( \bigwedge_{i=1}^{m} x = y_i \wedge \bigwedge_{j=1}^{n} \neg x = z_j \right) \quad \text{with} \quad y_i,\ z_j \in \mathcal{V}.$$

Since $x = x \approx$ true and $\neg x = x \approx$ false, we assume w.l.o.g. that $x \notin \{y_1, \ldots, y_m, z_1, \ldots, z_n\}$.

Case 1: If $m > 0$, then $\mathfrak{A} \models \varphi \longleftrightarrow \exists x(x = y_1) \wedge \bigwedge_{i=2}^{m} y_1 = y_i \wedge \bigwedge_{j=1}^{n} \neg y_1 = z_j$, which is in turn equivalent to

$$\bigwedge_{i=2}^{m} y_1 = y_i \wedge \bigwedge_{j=1}^{n} \neg y_1 = z_j \in \mathcal{Q}^0.$$

Case 2: If $m = 0$, then $\mathfrak{A} \models \varphi \longleftrightarrow \text{true} \in \mathcal{Q}^0$.

# Quantifier Elimination for Two Particular Finite Sets

## Theorem

*Consider $\mathcal{L} = ()$.*

(i) *The $\mathcal{L}$-structure $\mathbf{A} = (\{1\})$ admits quantifier elimination.*

(ii) *The $\mathcal{L}$-structure $\mathbf{B} = (\{1, 2\})$ admits quantifier elimination.*

## Proof.

We proceed as for infinite sets:

$$\exists x \left( \bigwedge_{i=1}^{m} x = y_i \wedge \bigwedge_{j=1}^{n} \neg(x = z_j) \right) \quad \text{with} \quad y_i,\ z_j \in \mathcal{V}.$$

Only Case 2, $m = 0$, is different:

For $n = 0$ we trivially have true in both cases. Let $n \geqslant 1$. Then

(i) $\mathbf{A} \models \exists x \bigwedge_{j=1}^{n} \neg x = z_j \longleftrightarrow \text{false}$,

(ii) $\mathbf{B} \models \exists x \bigwedge_{j=1}^{n} \neg x = z_j \longleftrightarrow \bigwedge_{j=2}^{n} z_1 = z_j$. □

# Definable Sets

An extended $\mathcal{L}$-formula $\varphi(x_1, \ldots, x_n)$ **defines** a set in **A** as follows:

$$[\varphi]^{\mathbf{A}} := \{ (a_1, \ldots, a_n) \in \mathbf{A}^n \mid \mathbf{A} \models \varphi(a_1, \ldots, a_n) \}$$

$B \subseteq A^n$ is a **definable set** in **A** if there is $\varphi(x_1, \ldots, x_n)$ with $B = [\varphi]^{\mathbf{A}}$.

$B$ is a **quantifier-free definable set** in **A** if there is a suitable quantifier-free $\varphi$.

**Theorem**

**A** *admits QE iff in* **A** *every definable set is quantifier-free definable.*

**Proof.**

For extended formulas $\varphi(x_1, \ldots, x_n)$, $\varphi'(x_1, \ldots, x_n)$, we have
$\mathbf{A} \models \varphi \longleftrightarrow \varphi'$ iff $[\varphi]^{\mathbf{A}} = [\varphi']^{\mathbf{A}}$. □

# Definable Functions and Projections

For $f : A^n \to A^m$ define

$\mathrm{graph}(f) = \{ (a_1, \dots, a_n, b_1, \dots, b_m) \in A^{n+m} \mid (b_1, \dots, b_m) = f(a_1, \dots, a_n) \}$.

$f : A^n \to A^m$ is a **(quantifier-free) definable function** in $\mathbf{A}$, if the set $\mathrm{graph}(f)$ is (quantifier-free) definable.

For $B \subseteq A^{n+1}$ we define the **projection**

$\pi_{n+1}(B) := \{ (a_1, \dots, a_n) \in A^n \mid \text{exists } a_{n+1} \in A \text{ such that } (a_1, \dots, a_{n+1}) \in B \}$.

**Example**

Consider extended $\mathcal{L}$-terms $t_1(x_1, \dots, x_n), \dots, t_m(x_1, \dots, x_n)$.
Define $f : A^n \to A^m$ by $f(a_1, \dots, a_n) = (t_1^{\mathbf{A}}(a_1, \dots, a_n), \dots, t_m^{\mathbf{A}}(a_1, \dots, a_n))$.
Then we have

$$\mathrm{graph}(f) = \{ (a_1, \dots, a_n, b_1, \dots, b_m) \in A^{n+m} \mid \mathbf{A} \models \varphi(a_1, \dots, a_n, b_1, \dots, b_m) \},$$

where $\varphi(x_1, \dots, x_n, y_1, \dots, y_m)$ for $\varphi = \bigwedge_{j=1}^m y_j = t_j$.
Hence $f$ is quantifier-free definable.

### Theorem

*Consider an $\mathcal{L}$-structure* $\mathbf{A}$. *FAE:*

(i) $\mathbf{A}$ *admits QE.*

(ii) *For every quantifier-free definable set* $B \subseteq A^{n+1}$ *its projection* $\pi_{n+1}(B) \subseteq A^n$ *is quantifier-free definable, too.*

(iii) *For every definable function* $f : A^n \to A^m$ *and every quantifier-free definable set* $B \subseteq A^n$, *the range* $f(B)$ *is quantifier-free definable.*

### Proof

(i) $\Rightarrow$ (iii) Consider $\psi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ with $[\psi]^{\mathbf{A}} = \mathrm{graph}(f)$ and $\varphi(x_1, \ldots, x_n)$ with $[\varphi]^{\mathbf{A}} = B$. Then $f(B) = [\chi']^{\mathbf{A}}$ for $\chi'(y_1, \ldots, y_n)$, where $\chi' \in \mathcal{Q}^0$ with $\mathbf{A} \models \chi' \longleftrightarrow \exists x_1 \ldots \exists x_n(\varphi \wedge \psi)$.

(iii) $\Rightarrow$ (ii) By the previous example $\pi_{n+1}$ is a (quantifier-free) definable function.

### Theorem

*Consider an $\mathcal{L}$-structure $\mathbf{A}$. FAE:*

(i) $\mathbf{A}$ *admits QE.*

(ii) *For every quantifier-free definable set $B \subseteq A^{n+1}$ its projection $\pi_{n+1}(B) \subseteq A^n$ is quantifier-free definable, too.*

(iii) *For every definable function $f : A^n \longrightarrow A^m$ and every quantifier-free definable set $B \subseteq A^n$, the range $f(B)$ is quantifier-free definable.*

### Proof.

(ii) $\Rightarrow$ (i) Consider a 1-primitive formula $\exists x \psi$. Let $\psi(x_1, \ldots, x_n, x)$ be an extended formula. Set $B := [\psi]^{\mathbf{A}}$. By (ii) we have $\psi' \in \mathcal{Q}^0$ with $[\psi']^{\mathbf{A}} = \pi_{n+1}(B)$. By definition $\pi_{n+1}(B) = [\exists x \psi]^{\mathbf{A}}$. It follows that $[\psi']^{\mathbf{A}} = [\exists x \psi]^{\mathbf{A}}$ and hence $\mathbf{A} \models \psi' \longleftrightarrow \exists x \psi$. $\square$

# An Example from Real Algebraic Geometry

A **semialgebraic set** is a set described by a finite sequence of polynomial equations $f_i(x_1, \dots, x_n) = 0$ and polynomial inequalities $g_j(x_1, \dots, x_n) > 0$, or a union of such sets.

**Theorem**

The projection of semialgebraic set along a coordinate axis is again a semialgebraic set.

According to our previous result, this theorem is equivalent to the following fact: For $\mathcal{L} = (0, 1, +, \cdot; >)$ the real numbers $\mathbf{R} = (\mathbb{R}; 0, 1, +, \cdot; >)$ admit QE.

# Completeness and Decision Procedures

Consider a class $\mathfrak{A} \neq \varnothing$ of $\mathcal{L}$-structures and a set $\Phi \subseteq \mathcal{Q}$ of $\mathcal{L}$-sentences.

A **decision procedure (DP)** for $\mathfrak{A}$ and $\Phi$ is an algorithm that given $\varphi \in \Phi$ decides whether $\mathfrak{A} \models \varphi$ or not $\mathfrak{A} \models \varphi$.

$\mathfrak{A}$ is **decidable** for $\Phi$ is there exists a DP for $\mathfrak{A}$ and $\Phi$.

$\mathfrak{A}$ is **complete** for $\Phi$ if for every $\varphi \in \Phi$ either $\mathfrak{A} \models \varphi$ or $\mathfrak{A} \models \neg\varphi$.

**Example for $\mathcal{L}_R = (0, 1, +, -, \cdot)$ and $\mathfrak{A} = \{\mathbf{Z}/2, \mathbf{Z}/3\}$**

- $\mathfrak{A}$ is **not** complete for $\mathcal{Q}^0 \cap \mathcal{Q}_\varnothing$: neither $\mathfrak{A} \models 1 + 1 = 0$ nor $\mathfrak{A} \models \neg 1 + 1 = 0$.
- $\mathfrak{A}$ is decidable for $\mathcal{Q}^0 \cap \mathcal{Q}_\varnothing$: all Boolean combinations of (variable-free) equations can be evaluated to either true or false in both $\mathbf{Z}/2$ and $\mathbf{Z}/3$.

If $\mathfrak{A} = \{\mathbf{A}\}$, then we may simply say that $\mathbf{A}$ is decidable for $\Phi$.

Obviously, $\{\mathbf{A}\}$ is always complete for any $\Phi$.

If $\Phi = \mathcal{Q}$, then we need not explicitly refer to $\Phi$.

# QE and Completeness

## Theorem

*Consider a class $\mathfrak{A}$ of $\mathcal{L}$-structures, and assume that $\mathfrak{A}$ admits QE.*

(i) *If $\mathfrak{A}$ is complete for $A_{\{x\}} = \{\varphi \in A \mid \mathcal{V}(\varphi) \subseteq \{x\}\}$, then $\mathfrak{A}$ is complete.*

(ii) *If there is $c \in \mathcal{F}$ with $\sigma(c) = 0$ and $\mathfrak{A}$ is complete for $A_\emptyset = A \cap \mathcal{Q}_\emptyset$, then $\mathfrak{A}$ is complete.*

## Proof.

(i) Consider $\varphi \in \mathcal{Q}_\emptyset$. By QE there is $\varphi' \in \mathcal{Q}^0$ such that $\mathfrak{A} \models \varphi' \longleftrightarrow \varphi$. Denote $\{y_1, \ldots, y_n\} := \mathcal{V}(\varphi')$. Then for $\varphi'' = \varphi'[x/y_1, \ldots, x/y_n] \in \mathcal{Q}^0_{\{x\}}$ we have $\mathfrak{A} \models \varphi'' \longleftrightarrow \varphi' \longleftrightarrow \varphi$. Now for every atomic formula $\alpha$ in $\varphi''$ we have either $\mathfrak{A} \models \alpha$ or $\mathfrak{A} \models \neg\alpha$. It follows that either $\mathfrak{A} \models \varphi''$ or $\mathfrak{A} \models \neg\varphi''$.

(ii) Consider $\varphi \in \mathcal{Q}_\emptyset$. By QE and a previous result there is $\varphi'' \in \mathcal{Q}^0_\emptyset$ such that $\mathfrak{A} \models \varphi'' \longleftrightarrow \varphi$. Now argue as in (i). □

# QE and Decidability

## Theorem

*Consider a class $\mathfrak{A}$ of $\mathcal{L}$-structures, and assume that $\mathfrak{A}$ admits QE.*

(i) *If $\mathfrak{A}$ is decidable for $\mathcal{Q}^0_{\{x\}} = \{\varphi \in \mathcal{Q}^0 \mid \mathcal{V}(\varphi) \subseteq \{x\}\}$, then $\mathfrak{A}$ is decidable.*

(ii) *If there is $c \in \mathcal{F}$ with $\sigma(c) = 0$ and $\mathfrak{A}$ is decidable for $\mathcal{Q}_\varnothing$, then $\mathfrak{A}$ is decidable.*

(iii) *If $\mathfrak{A}$ is complete and decidable for $A_{\{x\}}$, then $\mathfrak{A}$ is complete and decidable.*

(iv) *If there is $c \in \mathcal{F}$ with $\sigma(c) = 0$ and $\mathfrak{A}$ is complete and decidable for $A_\varnothing$, then $\mathfrak{A}$ is complete and decidable.*

## Proof.

Exercise! □

# Some Applications of the Previous Theorem

**Example**

For $\mathcal{L} = ()$ the class $\mathfrak{A}$ of infinite sets is complete and decidable:

$\mathfrak{A}$ is complete and decidable for $A_{\{x\}} = \{x = x\}$ because $x = x \approx \text{true}$.
Now apply part (iii) of the previous theorem.

**Theorem**

*Let $\mathcal{L}$ be finite, and let $\mathbf{A}$ be a finite $\mathcal{L}$-structure. Then $\mathbf{A}$ is decidable.*

**Proof.**

Let $A = \{a_1, \ldots, a_n\}$. We switch to $\mathcal{L}(A) \supseteq \mathcal{L}$ obtained by adding $a_1, \ldots, a_n$ as new constant symbols. The $\mathcal{L}(B)$-expansion $\mathbf{A}'$ of $\mathbf{A}$ admits QE: For a 1-primitive formula $\varphi = \exists x \psi$ we have $\mathbf{A}' \models \varphi \longleftrightarrow \bigvee_{i=1}^{n} \psi[a_i/x_j]$. $\mathbf{A}'$ is trivially complete. Atomic sentences in $\mathbf{A}'$ are decidable as all relations and functions in $\mathbf{A}'$ are finite sets. Now apply part (iv) of the previous theorem. $\square$

# More Decidability Results

**Theorem**

*Let $\mathfrak{A} = \{\mathbf{A}_1, \ldots, \mathbf{A}_n\}$ be a finite class of $\mathcal{L}$-structures. If every single one of the $\mathbf{A}_1, \ldots, \mathbf{A}_n$ is decidable for $\Phi \subseteq \mathcal{Q}_\varnothing$, then $\mathfrak{A}$ is decidable for $\Phi$.*

**Proof.**

Let $\varphi \in \Phi$. Then $\mathfrak{A} \models \varphi \iff \mathbf{A}_1 \models \varphi$ and $\ldots$ and $\mathbf{A}_n \models \varphi$, which can be checked independently in finite time. $\square$

**Theorem**

*Let $\mathfrak{A}$ be complete and decidable for $\Phi \subseteq \mathcal{Q}_\varnothing$. Then so is every $\mathbf{A} \in \mathfrak{A}$.*

**Proof.**

By completeness we have for $\varphi \in \Phi$ and for every single $\mathbf{A} \in \mathfrak{A}$ that $\mathfrak{A} \models \varphi \iff \mathbf{A} \models \varphi$. Thus every DP for $\mathfrak{A}$ and $\Phi$ is also a DP for $\mathbf{A}$ and $\Phi$. $\square$

## Theorem

*Let $\mathfrak{A}$ be complete and decidable for $\Phi \subseteq \mathcal{Q}_\varnothing$. Then so is every $\mathbf{A} \in \mathfrak{A}$.*

## Example

Consider $\mathcal{L} = (0^{(0)}, s^{(1)}; R^{(1)})$.

Let $M \subseteq \mathbb{N}$ be not recursive.

Set $\mathbf{A} := (\mathbb{N}; 0, s; M)$, $\mathbf{B} := (\mathbb{N}; 0, s; \mathbb{N} \setminus M)$ and $\mathfrak{A} := \{\mathbf{A}, \mathbf{B}\}$.

Consider $\Phi = \{ R(s^n(0)) \in \mathcal{A}_\varnothing \mid n \in \mathbb{N} \}$.

Then for every $R(s^n(0)) \in \Phi$ we have

$$\mathbf{A} \models R(s^n(0)) \iff n \in M \quad \text{and} \quad \mathbf{B} \models R(s^n(0)) \iff n \notin M.$$

It follows that **not** $\mathfrak{A} \models R(s^n(0))$, i.e., $\mathfrak{A}$ is decidable for $\Phi$.

But a DP for either **A** or **B** would render $M$ recursive.

# An Important Though Impractical Model Theoretical Result

**Theorem**

*Consider a countable language $\mathcal{L}$ and $\mathfrak{A} = \mathrm{Mod}(\Xi)$, where $\Xi$ is recursively enumerable. Let $\Phi \subseteq \mathcal{Q}_\varnothing$ be recursive.*
*If $\mathfrak{A}$ is complete for $\Phi$, then $\mathfrak{A}$ is decidable for $\Phi$.*

**Proof.**

Using Gödel's completeness theorem the set $\Phi' = \{\varphi \in \Phi \mid \mathfrak{A} \models \varphi\}$ is recursively enumerable, say, $\Phi' = \{\varphi_n \mid n \in \mathbb{N}\}$. Let $\varphi \in \Phi$. Due to the completeness of $\mathfrak{A}$ we have either $\varphi \in \Phi'$ or $\neg\varphi \in \Phi'$. So there is $n \in \mathbb{N}$ such that either $\varphi = \varphi_n$ or $\neg\varphi = \varphi_n$, and $\varphi_n$ will show up after $n$ steps of enumerating $\Phi'$. $\square$

# Homomorphisms and Isomorphy

Consider $\mathcal{L}$-structures $\mathbf{A}$ and $\mathbf{B}$ and a map $h : A \to B$.

For $a \in A$ we shortly write $ha$ instead of $h(a)$.

$h$ is a **homomorphism** from $\mathbf{A}$ to $\mathbf{B}$ (notation $h : \mathbf{A} \to \mathbf{B}$), if

(i) $hf^{\mathbf{A}}(a_1, \ldots, a_n) = f^{\mathbf{B}}(ha_1, \ldots, ha_n)$ for all $n \in \mathbb{N}$, $f \in \mathcal{F}$ with $\sigma(f) = n$.

(ii) $R^{\mathbf{A}}(a_1, \ldots, a_n) \leqslant R^{\mathbf{B}}(ha_1, \ldots, ha_n)$ for all $n \in \mathbb{N}$, $R \in \mathcal{R}$ with $\sigma(R) = n$.

$h$ is an **isomorphism** from $\mathbf{A}$ to $\mathbf{B}$, if

(i) $h$ is a bijective homomorphism from $\mathbf{A}$ to $\mathbf{B}$.

(ii) $R^{\mathbf{A}}(a_1, \ldots, a_n) = R^{\mathbf{B}}(ha_1, \ldots, ha_n)$ for all $n \in \mathbb{N}$, $R \in \mathcal{R}$ with $\sigma(R) = n$.

$\mathbf{A}$ and $\mathbf{B}$ are **isomorphic** (notation $\mathbf{A} \cong \mathbf{B}$), if
there exists an isomorphism from $\mathbf{A}$ to $\mathbf{B}$.

$\cong$ is reflexive, transitive, and symmetric.

# An Example for Homomorphisms and the “Isomorphielemma”

**Example for $\mathcal{L} = (0, +; \leqslant)$**

- $\mathrm{id}_{\mathbb{N}} : (\mathbb{N}; 0, +; <) \to (\mathbb{N}; 0, +; \leqslant)$ is a homomorphism but not an isomorphism.
- $\mathrm{id}_{\mathbb{N}}$ is **not** a homomorphism from $(\mathbb{N}; 0, +; \leqslant)$ to $(\mathbb{N}; 0, +; <)$.

**Theorem**

*Consider $\mathcal{L}$-structures $\mathbf{A}$, $\mathbf{B}$ such that there exists an isomorphism $h : \mathbf{A} \to \mathbf{B}$.*
*Let $\varphi(x_1, \ldots, x_n)$ be an extended formula, and let $a_1, \ldots, a_n \in A$.*
*Then $\mathbf{A} \models \varphi(a_1, \ldots, a_n) \iff \mathbf{B} \models \varphi(ha_1, \ldots, ha_n)$.*

**Proof.**

Exercise. $\square$

# Substructures

Consider $\mathcal{L}$-structures **A** and **B**.

**B** is a **substructure** of **A** (notation $\mathbf{B} \subseteq \mathbf{A}$), if

(i) $B \subseteq A$

(ii) $f^{\mathbf{B}} = f^{\mathbf{A}}|_{B^n}$ for $f \in \mathcal{F}$ with $\sigma(f) = n$.

(iii) $R^{\mathbf{B}} = R^{\mathbf{A}}|_{B^n}$ for $R \in \mathcal{R}$ with $\sigma(R) = n$.

Vice versa, **A** is an **extension structure** of **B**.

Do not confuse this with restriction and expansion!

$\subseteq$ is reflexive, transitive, and antisymmetric.

**Exercise**

(i) Consider $\mathcal{L}_R = (0, 1, +, -, \cdot)$. Is $\mathbf{Z} \subseteq \mathbf{Q}$? Is $\mathbf{Z}/4 \subseteq \mathbf{Z}$?

(ii) Consider an $\mathcal{L}$-structure **A** and $B \subseteq A$. There is $\mathbf{B} \subseteq \mathbf{A}$ with universe $B$, if and only if $B$ is closed under the functions $f^{\mathbf{A}}$ for $f \in \mathcal{F}$.
In the positive case **B** is uniquely determined by **A** and $B$.

# Elementary Equivalence and Elementary Substructures

Consider $\mathcal{L}$-structures $\mathbf{A}$ and $\mathbf{B}$.

$\mathbf{A}$ and $\mathbf{B}$ are **elementary equivalent** (notation $\mathbf{A} \equiv \mathbf{B}$), if
$\mathbf{A} \models \varphi \iff \mathbf{B} \models \varphi$ for all $\varphi \in \mathcal{Q}$.

$\mathbf{A}$ and $\mathbf{B}$ are **elementary equivalent over** $C \subseteq A \cap B$ (notation $\mathbf{A} \equiv_C \mathbf{B}$), if for all extended formulas $\varphi(x_1, \ldots, x_n)$ and all $c_1, \ldots, c_n \in C$ it holds that
$\mathbf{A} \models \varphi(c_1, \ldots, c_n) \iff \mathbf{B} \models \varphi(c_1, \ldots, c_n)$.

$\mathbf{A}$ is an **elementary substructure** of $\mathbf{B}$ (notation $\mathbf{A} \preceq \mathbf{B}$), if $\mathbf{A} \subseteq \mathbf{B}$ and $\mathbf{A} \equiv \mathbf{B}$.
Vice versa, $\mathbf{B}$ is called an **elementary extension** of $\mathbf{A}$.

## Exercise

(i) If $\mathbf{A} \equiv_C \mathbf{B}$ and $D \subseteq C$, then $\mathbf{A} \equiv_D \mathbf{B}$.

(ii) $\mathbf{A} \equiv \mathbf{B} \iff \mathbf{A} \equiv_\emptyset \mathbf{B}$

(iii) $\mathbf{A} \cong \mathbf{B} \implies \mathbf{A} \equiv \mathbf{B}$, but not vice versa.

(iv) Find an example for $\mathbf{A} \subseteq \mathbf{B}$ but not $\mathbf{A} \equiv_A \mathbf{B}$.

# Model Completeness and Substructure Completeness

Consider a class $\mathfrak{A}$ of $\mathcal{L}$-structures.

$\mathfrak{A}$ is **model complete**, if for all $\mathbf{A}, \mathbf{B} \in \mathfrak{A}$
it holds that $\mathbf{A} \subseteq \mathbf{B} \Longrightarrow \mathbf{A} \preceq \mathbf{B}$.

$\mathfrak{A}$ is **substructure complete**, if for all $\mathbf{A}, \mathbf{B} \in \mathfrak{A}$ and all $\mathcal{L}$-structures $\mathbf{C}$
it holds that $\mathbf{C} \subseteq \mathbf{A}$ and $\mathbf{C} \subseteq \mathbf{B} \Longrightarrow \mathbf{A} \equiv_C \mathbf{B}$.

**Exercise**

(i) $\mathfrak{A}$ is substructure complete $\Longrightarrow$ $\mathfrak{A}$ is model complete

(ii) $\mathfrak{A}$ is complete $\Longleftrightarrow$ $\mathbf{A} \equiv \mathbf{B}$ for all $\mathbf{A}, \mathbf{B} \in \mathfrak{A}$

# Substructure Completeness and Completeness

## Theorem

*Consider a substructure complete class $\mathfrak{A}$ of $\mathcal{L}$-structures. Assume that there is an $\mathcal{L}$-structure $\mathbf{C}$ such that for all $\mathbf{A} \in \mathfrak{A}$ there is $\mathbf{C}'$ such that $\mathbf{C} \cong \mathbf{C}' \subseteq \mathbf{A}$.*

*Then $\mathfrak{A}$ is complete.*

## Proof.

Let $\mathbf{A}, \mathbf{B} \in \mathfrak{A}$, and let $\mathbf{C} \cong \mathbf{C}_A \subseteq \mathbf{A}$ and $\mathbf{C} \cong \mathbf{C}_B \subseteq \mathbf{B}$.

Let $h_A : \mathbf{C_A} \to \mathbf{C}$ and $h_B : \mathbf{C_B} \to \mathbf{C}$ be corresponding isomorphisms.

Obtain $\mathbf{A}'$ from $\mathbf{A}$ by renaming all elements $c \in C_A \subseteq A$ to $h_{\mathbf{A}} c \in C$.

Obtain $\mathbf{B}'$ from $\mathbf{B}$ analogously.

Then $\mathbf{A}' \cong \mathbf{A}$, $\mathbf{B}' \cong \mathbf{B}$, $\mathbf{C} \subseteq \mathbf{A}'$, and $\mathbf{C} \subseteq \mathbf{B}'$.

It follows that $\mathbf{A} \cong \mathbf{A}' \equiv_C \mathbf{B}' \cong \mathbf{B}$, hence $\mathbf{A} \equiv \mathbf{B}$. $\square$

**Theorem**

*If a class $\mathfrak{A}$ of $\mathcal{L}$-structures admits QE, then $\mathfrak{A}$ is substructure complete.*

**Proof.**

Let $\mathbf{A}$, $\mathbf{B} \in \mathfrak{A}$, and let $\mathbf{C} \subseteq \mathbf{A}$ and $\mathbf{C} \subseteq \mathbf{B}$. Let $\varphi(x_1, \ldots, x_n)$ be an extended $\mathcal{L}$-formula. As $\mathfrak{A}$ admits QE, there is an extended quantifier-free $\mathcal{L}$-formula $\varphi'(x_1, \ldots, x_n)$ such that $\mathfrak{A} \models \varphi' \longleftrightarrow \varphi$. Let $c_1, \ldots, c_n \in C$. Then $\mathbf{A} \models \varphi(c_1, \ldots, c_n) \iff \mathbf{A} \models \varphi'(c_1, \ldots, c_n) \iff \mathbf{C} \models \varphi'(c_1, \ldots, c_n) \iff \mathbf{B} \models \varphi'(c_1, \ldots, c_n) \iff \mathbf{B} \models \varphi(c_1, \ldots, c_n)$. That is $\mathbf{A} \equiv_C \mathbf{B}$. $\square$

**Example**

The class of all infinite sets as ()-structures is substructure complete and thus also model complete.

Consider a class $\mathfrak{A}$ of $\mathcal{L}$-structures.

$\mathfrak{A}$ is **elementary**, if there is $\Xi \subseteq \mathcal{Q}_{\varnothing}$ such that $\mathfrak{A} = \mathrm{Mod}(\Xi)$.

**Theorem**

*If an elementary class $\mathfrak{A}$ of $\mathcal{L}$-structures is substructure complete, then $\mathfrak{A}$ admits QE.* □

The proof requires

- the compactness theorem for first-order logic, and
- Robinson's diagram method.

# A Concluding Remark on Model Completeness

An **existential** formula is of the form $\exists x_1 \dots \exists x_n \varphi$ for $\varphi \in \mathcal{Q}^0$.

A **universal** formula is of the form $\forall x_1 \dots \forall x_n \varphi$ for $\varphi \in \mathcal{Q}^0$.

## Theorem

*Let $\mathfrak{A}$ be an elementary class of $\mathcal{L}$-structures. FAE:*

(i) *$\mathfrak{A}$ is model complete.*

(ii) *For every $\varphi \in \mathcal{Q}$ there is an existential formula $\varphi'$ such that $\mathfrak{A} \models \varphi' \longleftrightarrow \varphi$.*

(iii) *For every $\varphi \in \mathcal{Q}$ there is a universal formula $\varphi'$ such that $\mathfrak{A} \models \varphi' \longleftrightarrow \varphi$.* □

## Exercise

Show "(ii) $\Rightarrow$ (iii)."

## We know already

For the empty language ():

- The class $\{\{1\},\{1,2\}\}$ does not admit QE.

  It follows that the class $\mathfrak{S}$ of all nonempty sets does not admit QE.
- The class of all infinite sets admits QE.

We consider now $\mathcal{L} = (\emptyset, \mathcal{R}, \sigma)$ with $\mathcal{R} = \{\, C_n^{(0)} \mid 2 \leqslant n \in \mathbb{N} \,\}$.

Define

$$\varphi_n := C_n \longleftrightarrow \exists x_1 \dots \exists x_n \bigwedge_{1 \leqslant i < j \leqslant n} \neg x_i = x_j.$$

Then $\mathfrak{S} := \mathrm{Mod}(\{\, \varphi_n \mid 2 \leqslant n \in \mathbb{N} \,\})$ is the class of all nonempty sets, where for $\mathbf{S} \in \mathfrak{S}$ we have $\mathbf{S} \models C_n$ if and only if $|\mathbf{S}| \geqslant n$.

## A Quantifier Elimination Procedure for $\mathfrak{S}$

**Theorem**

*There is a QEP for $\mathfrak{S}$.*

**Proof.**

Following our proof for the class of all infinite sets as ()-structures, the only case that remains to be considered is

$$\varphi := \exists x \bigwedge_{j=1}^{n} \neg x = z_j, \quad \text{where} \quad x \notin \{z_1, \ldots, z_n\} \subseteq \mathcal{V}.$$

For $k \in \{1, \ldots, n\}$ the following quantifier-free formula states that exactly $k$ of the $z_1, \ldots, z_k$ are pairwise different:

$$\psi_k := \bigvee_{j_1=1}^{n} \cdots \bigvee_{j_k=1}^{n} \left[ \bigwedge_{j=1}^{n} \bigvee_{i=1}^{k} z_j = z_{j_i} \wedge \bigwedge_{i=1}^{k} \bigwedge_{h=1}^{i-1} \neg z_{j_i} = z_{j_h} \right] \in \mathcal{Q}^0.$$

Now $\mathfrak{S} \models \varphi \longleftrightarrow \bigvee_{k=1}^{n} (C_{k+1} \wedge \psi_k)$. $\square$

# We Need a Lemma

## Lemma

(i) *Consider a disjunction* $\psi = \bigwedge_j \psi_j$ *of base formulas in at most one variable* $x \in \mathcal{V}$. *Then one can compute an interval* $M_\psi \subseteq \mathbb{N} \setminus \{0\}$ *such that*

(a) *For finite* $\mathbf{S} \in \mathfrak{S}$ *we have* $\mathbf{S} \models \psi \iff |\mathbf{S}| \in M_\psi$.

(b) *For infinite* $\mathbf{S} \in \mathfrak{S}$ *we have* $\mathbf{S} \models \psi$ *iff* $M_\psi$ *is unbounded from above.*

(ii) *For each* $\varphi \in \mathcal{Q}^0_{\{x\}}$ *one can compute a fininte disjunction of intervals* $M_\varphi \subseteq \mathbb{N} \setminus \{0\}$ *with corresponding properties (a) and (b) as in (i).*

## Proof.

(i) The atomic formulas of $\psi$ are $x = x \approx$ true or $C_n$ for $2 \leqslant n \in \mathbb{N}$. Since $\mathfrak{S} \models C_m \longrightarrow C_n$ for $n \leqslant m$, each $\psi$ is equivalent to one of true, false, $C_m$, $\neg C_m$, or $C_m \wedge \neg C_n$ for $2 \leqslant m < n \in \mathbb{N}$. This yields $M_\psi = \mathbb{N} \setminus \{0\}$, $M_\psi = \emptyset$, $M_\psi = [m, \infty)$, $M_\psi = [1, m-1]$, or $M_\psi = [m, n-1]$, respectively.

(ii) Compute a DNF $\varphi' = \bigvee_i \varphi_i$, where $\varphi_i = \bigwedge_j \psi_{ij}$, such that $\mathfrak{S} \models \varphi \longleftrightarrow \varphi'$. Apply (i) to all the $\varphi_i$ and then obtain $M_\varphi = M_{\varphi'} = \bigcup_i M_{\varphi_i}$. □

# Consequences of Our QEP

## Corollary

(i) *$\mathfrak{S}$ is substructure complete and model complete.*

(ii) *$\mathfrak{S}$ is not complete.*

(iii) *$\mathfrak{S}$ is decidable.*

(iv) *For each $n \in \mathbb{N}$ the subclass $\mathfrak{S}_n := \{\, \mathbf{S} \mid \mathbf{S} \in \mathfrak{S}$ and $|\mathbf{S}| = n \,\} \subseteq \mathfrak{S}$ is complete and decidable.*

## Proof.

(i) Follows from QE.

(ii) Consider $\mathbf{S}, \mathbf{T} \in \mathfrak{S}$ with $|\mathbf{S}| = 1$ and $|\mathbf{T}| = 2$. Then $\mathbf{S} \models \neg C_2$ and $\mathbf{T} \models C_2$. Hence neither $\mathfrak{S} \models C_2$ nor $\mathfrak{S} \models \neg C_2$.

(iii) It suffices to show that $\mathfrak{S}$ is decidable for $\mathcal{Q}^0_{\{x\}}$. Compute $M_\varphi$ according to our Lemma. It follows that $\mathfrak{S} \models \varphi \iff M_\varphi = \mathbb{N} \setminus \{0\}$.

(iv) Exercise. $\square$

Consider $\mathcal{L} = (<^{(2)})$ and $\mathbf{R} = (\mathbb{R}; <)$.

**Theorem**

*There is a QEP for* $\mathbf{R}$.

**Proof**

We have positive normal forms because $\mathbf{R} \models \neg x = y \longleftrightarrow x < y \vee y < x$ and $\mathbf{R} \models \neg x < y \longleftrightarrow y < x \vee y = x$. It thus suffices to consider a 1-primitive positive formula

$$\exists x \left[ \bigwedge_{i=1}^{m} x = y_i \wedge \bigwedge_{j=1}^{n} z_j < x \wedge \bigwedge_{k=1}^{p} x < u_k \right], \quad \text{where} \quad y_i, \quad z_j, \quad u_k \in \mathcal{V}.$$

Since $x = x \approx$ true and $\mathbf{R} \models x < x \longleftrightarrow$ false, we may assume that $x$ is not among the $y_i$, $z_j$, $u_k$. ...

$$\varphi = \exists x \left[ \bigwedge_{i=1}^{m} x = y_i \wedge \bigwedge_{j=1}^{n} z_j < x \wedge \bigwedge_{k=1}^{p} x < u_k \right]$$

**Proof.**

If $m > 0$, then

$$\mathbf{R} \models \varphi \longleftrightarrow \bigwedge_{i=2}^{m} y_1 = y_i \wedge \bigwedge_{j=1}^{n} z_j < y_1 \wedge \bigwedge_{k=1}^{p} y_1 < u_k.$$

If $m = 0$, then we distinguish 3 subcases:

If $n = 0$, then $\mathbf{R} \models \varphi \longleftrightarrow$ true, because $\mathbb{R}$ has no minimum.

If $p = 0$, then $\mathbf{R} \models \varphi \longleftrightarrow$ true, because $\mathbb{R}$ has no maximum.

If $n > 0$ and $p > 0$, then

$$\mathbf{R} \models \varphi \longleftrightarrow \bigwedge_{j=1}^{n} \bigwedge_{k=1}^{p} z_j < u_k.$$

"$\rightarrow$:" $<$ is transitive / "$\leftarrow$:" there exists $x \in \mathbb{R}$ with $\max_j z_j < x < \min_k u_k$. □

# Decidability of the Reals with Ordering

**Theorem**

**R** *is complete and decidable.*

**Proof.**

It suffices to show that **R** is complete and decidable for $\mathcal{A}_{\{x\}}$. The only atomic formulas to be considered are $x = x$ and $x < x$, where $x = x \approx$ true and **R** $\models x < x \longleftrightarrow$ false. $\square$

**Exercise**

In **R** decide the sentence $\forall x \exists y \forall z (x < y \land (x < z \longrightarrow (z = y \lor y < z)))$.

# Dense Orderings

## What have we actually used in our proofs?

- $<$ is a strict ordering.
- $\mathbb{R}$ has no minimum or maximum.
- For $a < b \in \mathbb{R}$ there is $x \in \mathbb{R}$ such that $a < x < b$.

$$\begin{aligned}\Xi_{DEO} \quad := \quad & \{\neg x < x, \quad x < y \vee x = y \vee y < x, \quad x < y \wedge y < z \longrightarrow x < z, \\ & \forall x \exists y (x < y), \quad \forall x \exists y (y < x), \quad \forall x \forall y \exists z (x < y \longrightarrow x < z \wedge z < y)\}\end{aligned}$$

$\mathfrak{O}_{DE} = \mathrm{Mod}(\Xi_{DEO})$ is the class of **dense orderings without endpoints**.

$\mathbf{R} \in \mathfrak{O}_{DE}$, and also $(\mathbb{Q}, <)$, $(\mathbb{R} \setminus \mathbb{Q}, <)$, $(\mathbb{N} \times \mathbb{R}, <_{\mathrm{lex}}) \in \mathfrak{O}_{DE}$.

## Theorem

*There is a QEP for $\mathfrak{O}_{DE}$. Thus $\mathfrak{O}_{DE}$ is substructure complete and model complete. Furthermore $\mathfrak{O}_{DE}$ is complete and decidable.* $\square$

# Let Us Now Consider Natural Numbers

Consider again $\mathcal{L} = (<)$ and now $(\mathbb{N}; <)$.

**Theorem**

$\mathbf{N} = (\mathbb{N}, <)$ *does not admit QE.*

**Proof.**

For $\varphi = \forall x(x = y \vee y < x)$ consider the extended formula $\varphi(y)$. Then $[\varphi]^{\mathbf{N}} = \{0\}$. On the other hand, $\mathcal{A}_{\{y\}} = \{y = y, y < y\}$, where considering the extension $(y)$ it holds that $[y = y]^{\mathbf{N}} = \mathbb{N}$ and $[y < y]^{\mathbf{N}} = \varnothing$. Since $D = \{\varnothing, \ \mathbb{N}\}$ is closed under complement and union, the sets in $D$ are also the ones definable by $\varphi' \in \mathcal{Q}^0_{\{y\}}$. Hence for $\varphi' \in \mathcal{Q}^0_{\{y\}}$ and considering $\varphi'(y)$ we have $[\varphi']^{\mathbf{N}} \neq [\varphi]^{\mathbf{N}}$ and thus $\mathbf{N} \not\models \varphi' \longleftrightarrow \varphi$. $\square$

When adding the constant symbol 0 to $\mathcal{L}$, we have $x = 0$ as a possible quantifier-free equivalent for $\varphi$ in the proof.

# Next Attempt

Consider $\mathcal{L} = (0; <)$ and $(\mathbb{N}; 0; <)$.

## Theorem

$\mathbf{N} = (\mathbb{N}; 0; <)$ *does not admit QE.*

## Proof.

For $\varphi = 0 < y \wedge \forall x(0 < x \longrightarrow x = y \vee y < x)$ consider the extended formula $\varphi(y)$. Then $[\varphi]^{\mathbf{N}} = \{1\}$. On the other hand,

$$A_{\{y\}} = \{0 = 0,\ 0 < 0,\ 0 = y,\ y = 0,\ 0 < y,\ y < 0,\ y = y,\ y < y\},$$

where considering the extension $(y)$ it holds that

$$[0 = 0]^{\mathbf{N}} = [y = y] = \mathbb{N}, \qquad [0 < 0]^{\mathbf{N}} = [y < 0]^{\mathbf{N}} = [y < y]^{\mathbf{N}} = \emptyset,$$
$$[0 = y]^{\mathbf{N}} = [y = 0]^{\mathbf{N}} = \{0\}, \qquad [0 < y]^{\mathbf{N}} = \mathbb{N} \setminus \{0\}.$$

Since $D = \{\emptyset,\ \{0\},\ \mathbb{N} \setminus \{0\},\ \mathbb{N}\}$ is closed under complement and union, the sets in $D$ are also the ones definable by $\varphi' \in \mathcal{Q}^0_{\{y\}}$. $\square$

Consider $\mathcal{L} = (0, s^{(1)}; <)$ and $\mathbf{N} = (\mathbb{N}; 0, s; <)$, where $s(n) = n + 1$.

## Theorem

*There is a QEP for* $\mathbf{N} = (\mathbb{N}; 0, s; <)$.

## Proof.

In analogy to dense orderings we have positive normal forms. All terms are of one of the forms $s^k(0)$, $s^k(x)$ for $x \in \mathcal{V}$ and $k \in \mathbb{N}$, where in particular $s^0(0) = 0$ and $s^0(x) = x$. Consider a positive 1-primitive formula

$$\exists x \left[ \bigwedge_{i=1}^{m} s^{k_i}(x)\ \varrho_i\ a_i \wedge \bigwedge_{j=1}^{n} s^{l_j}(x)\ \varrho'_j\ s^{m_j}(x) \right], \quad \varrho_i \in \{<, =, >\}, \quad \varrho'_j \in \{<, =\},$$

where $a_i \in \mathcal{T}$ with $x \notin \mathcal{V}(a_i)$.Since $\mathbf{N} \models s^{l_j}(x)\ \varrho'_j\ s^{m_j}(x) \longleftrightarrow$ true if $l_j\ \varrho'_j\ m_j$ and $\mathbf{N} \models s^{l_j}(x)\ \varrho'_j\ s^{m_j}(x) \longleftrightarrow$ false else, it suffices to consider

$$\exists x \bigwedge_{i=1}^{m} s^{k_i}(x)\ \varrho_i\ a_i.$$

...

$$\varphi = \exists x \bigwedge_{i=1}^{m} s^{k_i}(x)\ \varrho_i\ a_i, \quad \varrho_i \in \{<, =, >\}, \quad a_i \in \mathcal{T}, \quad x \notin \mathcal{V}(a_i)$$

**Proof.**

$$\mathbf{N} \models \varphi \longleftrightarrow \underbrace{\exists x \bigwedge_{i=1}^{m} s^{k}(x)\ \varrho_i\ a'_i}_{\varphi'}, \quad \text{where} \quad k = \max_i k_i, \quad a'_i := s^{k-k_i}(a_i).$$

If there is at least one equation, say w.l.o.g. $\varrho_1$ is $=$, then

$$\begin{aligned}\mathbf{N} \models \varphi' &\longleftrightarrow \exists x(s^k(x) = a'_1) \land \bigwedge_{i=1}^{m} a'_1\ \varrho_i\ a'_i \\ &\longleftrightarrow (s^k(0) < a'_1 \lor s^k(0) = a'_1) \land \bigwedge_{i=1}^{m} a'_1\ \varrho_i\ a'_i\end{aligned}$$

Assume now that there is no equation, i.e., $\varrho_i \in \{<, >\}$. ...

$$\varphi' = \exists x \bigwedge_{i=1}^{m} s^k(x)\ \varrho_i\ a'_i, \quad \varrho_i \in \{<, >\}, \quad a'_i \in \mathcal{T}, \quad x \notin \mathcal{V}(a'_i)$$

## Proof.

- Case 1: $\varrho'_i$ is $<$ for all $i \in \{1, \dots, m\}$. Then $\mathbf{N} \models \varphi' \longleftrightarrow \bigwedge_{i=1}^{m} s^k(0) < a'_i$.
- Case 2: $\varrho'_i$ is $>$ for all $i \in \{1, \dots, m\}$. Then $\mathbf{N} \models \varphi' \longleftrightarrow$ true.
- Case 3: w.l.o.g. there is $p \in \{1, \dots, m\}$ such that

$$\varphi' = \exists x \left[\bigwedge_{i=1}^{p} s^k(x) > a'_i \wedge \bigwedge_{j=p+1}^{m} s^k(x) < a'_j\right]$$

Then $\mathbf{N} \models \varphi' \longleftrightarrow \bigwedge_{i=1}^{p} \bigwedge_{j=p+1}^{m} s(a'_i) < a'_j \wedge \bigwedge_{j=p+1}^{m} s^k(0) < a'_j$. □

# Discrete Orderings with Minimum

## What have we actually used in our proofs?

- $<$ is a strict ordering.
- $\mathbb{N}$ has a minimum.
- $s$ is the successor function.

Consider $\mathcal{L} = (0, s; <)$.

$$
\begin{aligned}
\Xi_{DIO} \quad := \quad & \{\neg x < x, \quad x < y \vee x = y \vee y < x, \quad x < y \wedge y < z \longrightarrow x < z, \\
& 0 < x \vee 0 = x, \quad x < s(x), \\
& x < y \longrightarrow s(x) < y \vee s(x) = y, \quad 0 < y \longrightarrow \exists x(s(x) = y)\}
\end{aligned}
$$

$\mathfrak{D}_{DI} = \mathrm{Mod}(\Xi_{DIO})$ is the class of **discrete orderings with minimum**.

It follows that $\mathfrak{D}_{DI} \models x < y \longleftrightarrow s(x) < s(y)$, in particular $s$ is injective.

$(\mathbb{N}; 0, s; <) \in \mathfrak{D}_{DE}$, and also $(\mathbb{R}^{\geqslant} \times \mathbb{N}; (0,0), s; <_{\mathrm{lex}}) \in \mathfrak{D}_{DE}$ with $s(x, n) = (x, n+1)$.

max planck institut informatik

# Results on Discrete Orderings with Minimum

## Theorem

(i) *There is a QEP for $\mathfrak{D}_{DI}$.*

(ii) *$\mathfrak{D}_{DE}$ is substructure complete and model complete.*

(iii) *$\mathfrak{D}_{DI}$ is complete and decidable.*

## Proof.

(i) Our proof for $(\mathbb{N}; 0, s; <)$ works with the axioms $\Xi_{DIO}$.

(ii) Follows from (i).

(iii) Since $\mathcal{L}$ contains a constant, it suffices to show that $\mathfrak{D}_{DI}$ is complete and decidable for $A_\varnothing = \left\{ s^k(0) \ \varrho \ s^l(0) \ \middle| \ k, l \in \mathbb{N}, \ \varrho \in \{<, =\} \right\}$. Each $s^k(0) \ \varrho \ s^l(0) \in A_\varnothing$ can be evaluated in $\mathfrak{D}_{DI}$ to either true or false by computing $k \ \varrho \ l$. $\square$

Consider $\mathcal{L} = (0, +, -)$ and $\mathbf{R} = (\mathbb{R}; 0, +, -)$.

There is a set of normal forms for $\mathcal{T}(x_1, \ldots, x_n)$ that can be described by linear combinations

$$\sum_{i=1}^{n} k_i x_i, \quad k_i \in \mathbb{Z}, \quad \text{where} \quad k_i x_i = \begin{cases} 0 & \text{if} \quad k = 0 \\ x_i + \cdots + x_i & \text{if} \quad k_i > 0 \\ (-x_i) + \cdots + (-x_i) & \text{if} \quad k_i < 0. \end{cases}$$

Since $-^{(1)}$ yields additive inverses in $\mathbb{R}$ there are normal forms for $\mathcal{A}(x_1, \ldots, x_n)$ of the form

$$\sum_{i=1}^{n} k_i x_i = 0, \quad k_i \in \mathbb{Z}.$$

Alternatively, there are normal forms for $\mathcal{A}(x_1, \ldots, x_n, x)$ of the form

$$kx = \sum_{i=1}^{n} k_i x_i, \quad k \in \mathbb{N}, \quad k_i \in \mathbb{Z}.$$

# Quantifier Elimination for the Additive Group of the Reals

**Theorem**

*There is a QEP for* **R**.

**Proof.**

We informally write $s \neq t$ for $\neg s = t$. Consider a 1-primitive formula

$$\varphi = \exists x \left[ \bigwedge_{i=1}^{m} k_i x = a_i \wedge \bigwedge_{j=1}^{n} l_j x \neq b_j \right],$$

where $k_i, l_j \in \mathbb{N} \setminus \{0\}$, $a_i$, $b_j \in \mathcal{T}$, $x \notin \mathcal{V}(a_i)$, $x \notin \mathcal{V}(b_j)$.

Set $k = \mathrm{lcm}(k_1, \dots, k_m, l_1, \dots, l_n) \in \mathbb{N}$. Then there are $k'_i$, $l'_j \in \mathbb{N}$ such that $k'_i k_i = k$ and $l'_j l_j = k$. Set $a'_i = k'_i a_i$ and $b'_j = l'_j b_j$. Then

$$\mathbf{R} \models \varphi \longleftrightarrow \exists x \left[ \bigwedge_{i=1}^{m} kx = a'_i \wedge \bigwedge_{j=1}^{n} kx \neq b'_j \right] \longleftrightarrow \exists y \left[ \bigwedge_{i=1}^{m} y = a'_i \wedge \bigwedge_{j=1}^{n} y \neq b'_j \right],$$

because for each $y \in \mathbb{R}$ there is $x = y/k \in \mathbb{R}$ with $kx = y$.

Now proceed as for infinite sets. $\square$

# Nontrivial Divisible Torsion-Free Abelian Groups

**What have we actually used for our proof?**

- **R** is an additive Abelian group:

  $$\{(x+y)+z = x+(y+z), \quad x+0 = x, \quad x+(-x) = 0, \quad x+y = y+x\}.$$
- **R** is divisible: $\{\forall x \exists y (ny = x)\}_{n \in \mathbb{N} \setminus \{0\}}$.
- **R** is torsion-free: $\{\forall x (nx = 0 \longrightarrow x = 0)\}_{n \in \mathbb{N} \setminus \{0\}}$.
- **R** is nontrivial: $\exists x (\neg x = 0)$.

Denote by $\Xi_{\mathrm{DAG}_0}$ the (infinite) set of these axioms.

$$\mathrm{DAG}_0 = \mathrm{Mod}(\Xi_{\mathrm{DAG}_0})$$

is the class of **nontrivial divisible torsion-free abelian groups**.

**R** $\in \mathrm{DAG}_0$, but also $(\mathbb{Q}^n, 0, 1, -)$, $(\mathbb{R}^n, 0, +, -) \in \mathrm{DAG}_0$ for $n \in \mathbb{N} \setminus \{0\}$.
More generally $(\mathbb{R}^S, 0, +, -) \in \mathrm{DAG}_0$ for $S \neq \varnothing$,
in particular $(\mathbb{R}^\mathbb{R}, 0, +, -)$ and the subgroups $(C^n(\mathbb{R}, \mathbb{R}), 0, +, -) \subseteq (\mathbb{R}^\mathbb{R}, 0, +, -)$
of $n \in \mathbb{N}$ times continuously differentiable functions.

# Results on Nontrivial Divisible Torsion-Free Abelian Groups

## Exercise

Every $\mathbf{G} \in \mathrm{DAG}_0$ is infinite.

## Theorem

(i) *There is a QEP for* $\mathrm{DAG}_0$*.*

(ii) $\mathrm{DAG}_0$ *is substructure complete and model complete.*

(iii) $\mathrm{DAG}_0$ *is complete and decidable. In particular,* $(\mathbb{R}, 0, +, -)$ *is decidable.*

## Proof.

(i) Our proof for $(\mathbb{R}, 0, +, -)$ works with the axioms $\Xi_{\mathrm{DAG}_0}$.

(ii) Follows from (i).

(iii) It suffices to observe that $\mathrm{DAG}_0$ is complete and decidable for $\mathcal{A}_\varnothing$, where we can restrict to $0 = 0$, which is the only variable-fee atomic formula in normal form. □

# The Additive Group of the Reals with Ordering

Consider $\mathcal{L} = (0, +, -; <)$ and $\mathbf{R} = (\mathbb{R}; 0, +, -; <)$.

We obviously have the same normal forms for terms as without ordering.

Furthermore, we have positive normal forms as discussed for dense orderings.

# Quantifier Elimination for the Additive Group of the Reals with Ordering

## Theorem

*There is a QEP for* **R**.

## Proof.

Consider a positive 1-primitive formula

$$\varphi = \exists x \left[ \bigwedge_{i=1}^{m} k_i x = a_i \wedge \bigwedge_{i=1}^{n} l_i x < b_i \wedge \bigwedge_{i=1}^{p} m_i x > c_i \right],$$

where $k_i, l_i, m_i \in \mathbb{N} \setminus \{0\}$, $a_i, b_i, c_i \in \mathcal{T}$, $x \notin \mathcal{V}(a_i)$, $x \notin \mathcal{V}(b_i)$, $x \notin \mathcal{V}(c_i)$.

In analogy to our proof without ordering we can transform

$$\begin{aligned} \mathbf{R} \models \varphi \quad &\longleftrightarrow \quad \exists x \left[ \bigwedge_{i=1}^{m} kx = a'_i \wedge \bigwedge_{i=1}^{n} kx < b'_i \wedge \bigwedge_{i=1}^{p} kx > c'_i \right] \\ &\longleftrightarrow \quad \exists y \left[ \bigwedge_{i=1}^{m} y = a'_i \wedge \bigwedge_{i=1}^{n} y < b'_i \wedge \bigwedge_{i=1}^{p} y > c'_i \right], \end{aligned}$$

and obtain a quantifier elimination problem for dense orderings. □

## Corollary

*The definable sets $M \subseteq \mathbb{R}$ in* **R** *are*

$$D = \{\mathbb{R}, \quad \varnothing, \quad \{0\}, \quad (-\infty, 0), \quad (0, \infty), \quad \mathbb{R} \setminus \{0\}, \quad [0, \infty), \quad (-\infty, 0]\}.$$

## Proof.

Since **R** admits QE, the definable sets are exactly the quantifier-free definable sets. Atomic formulas in $A_{\{x\}}$ in normal form are $0 = 0$, $0 < 0$, $x = 0$, $x < 0$, $0 < x$, which yield to the first five sets in $D$, respectively. Logical negation corresponding to set complement yields the remaining three sets. Then $D$ is closed under complement and union. □

# Application: Linear Programming

Our QEP for $(\mathbb{R}; 0, +, -; <)$ is essentially **Fourier–Motzkin Elimination.**

It has been found by Fourier in 1831 and rediscovered by Motzkin in 1936.

**Example**

Maximize the objective function $3x + 4y$ subject to the constraints

$3x + 2y \leqslant 500$, $0 \leqslant x \leqslant 100$, $0 \leqslant y \leqslant 200$.

We introduce a parameter $e$ which will be interpreted as 1 at the end, and we introduce a parameter $z$ to denote a lower bound on the objective function:

$$\exists x \exists y (3x + 2y \leqslant 500e \wedge 0 \leqslant x \wedge x \leqslant 100e \wedge 0 \leqslant y \wedge y \leqslant 200e \wedge z \leqslant 3x + 4y)$$

**Exercise**

Compute an optimal point and the optimal value by quantifier elimination.

# Nontrivial Divisible Ordered Abelean Groups

## What have we actually used for our proof?

- Axioms of nontrivial divisible Abelean groups.
- Axioms of strict orderings.
- Monotony: $x < y \longrightarrow x + z < y + z$

Denote by $\Xi_{\mathrm{DOAG}}$ the set of these axioms.

$$\mathrm{DOAG} = \mathrm{Mod}(\Xi_{\mathrm{DOAG}})$$

is the class of **nontrivial divisible ordered abelean groups**.

All $\mathbf{G} \in \mathrm{DOAG}$ are torsion-free, and $<^{\mathbf{G}}$ is dense without minimum or maximum.

$\mathbf{R} \in \mathrm{DOAG}$ and $(\mathbb{Q}^n, 0, +, -; <_{\mathrm{lex}}), (\mathbb{R}^n; 0, +, -; <_{\mathrm{lex}}) \in \mathrm{DOAG}$ for $1 \leqslant n \in \mathbb{N}$.

# Results on Nontrivial Divisible Ordered Abelian Groups

## Theorem

(i) *There is a QEP for* DOAG.

(ii) DOAG *is substructure complete and model complete.*

(iii) DOAG *is complete and decidable.*
*In particular,* $(\mathbb{R}, 0, +, -; <)$ *is decidable.*

## Proof.

(i) Our proof for $(\mathbb{R}, 0, +, -; <)$ works with the axioms $\Xi_{\mathrm{DOAG}}$.

(ii) Follows from (i).

(iii) It suffices to observe that DOAG is complete and decidable for $\mathcal{A}_{\varnothing}$, where we can restrict to $0 = 0$ and $0 < 0$, which are the only variable-fee atomic formulas in normal form. $\square$

# The Additive Group of the Integers with Ordering

Recall that already for the set $\mathbb{N}$ with ordering we needed $s^{(1)}$ in $\mathcal{L}$.

Since we have addition now, we can more naturally take $1^{(0)}$ instead.

Consider $\mathcal{L} = (0, 1, +, -; <)$ and $\mathbf{Z} = (\mathbb{Z}; 0, 1, +, -; <)$.

### Theorem

$\mathbf{Z} = (\mathbb{Z}; 0, 1, +, -; <)$ *does not admit QE.*

### Proof.

For $\varphi = \exists x(x + x = y)$ and the extended formula $\varphi(y)$, we have $[\varphi]^{\mathbf{Z}} = 2\mathbb{Z}$. Note that $2\mathbb{Z} \cap \mathbb{N}$ is neither finite nor co-finite in $\mathbb{N}$. On the other hand, all atomic formulas in $\mathcal{A}_{\{y\}}$ are equivalent in $\mathbf{Z}$ to one of the normal forms $z \cdot 1 = 0$, $z \cdot 1 < 0$, $ny = z$, $ny < z$, $z < ny$ for $n \in \mathbb{N}$, $z \in \mathbb{Z}$. These define the sets $D = \{\emptyset, \mathbb{Z}, \{z'\}, (-\infty, z'], [z', \infty) \mid z' \in \mathbb{Z}\}$. For all $I \in D$ we have $I \cap \mathbb{N}$ finite or co-finite in $\mathbb{N}$. It follows for $I$, $I' \in D$ that $(I \cup I') \cap \mathbb{N} = (I \cap \mathbb{N}) \cup (I' \cap \mathbb{N})$ and $(\mathbb{Z} \setminus I) \cap \mathbb{N} = (\mathbb{Z} \cap \mathbb{N}) \setminus (I \cap \mathbb{N}) = \mathbb{N} \setminus (I \cap \mathbb{N})$ are finite or co-finite in $\mathbb{N}$, too. $\square$

# Presburger Arithmetic

For $n \in \mathbb{N}$ and $z, z' \in \mathbb{Z}$ define $z \equiv_m z' \iff m \mid z - z'$ ("$m$ divides $z - z'$").

Consider $\mathcal{L}' = (0, 1, +, -; <, \{\equiv_m^{(2)}\}_{m \in \mathbb{N} \setminus \{0\}})$, $\mathbf{Z}' = (\mathbb{Z}; 0, 1, +, -; <, \{\equiv_m\}_{m \in \mathbb{N} \setminus \{0\}})$.

## Relevant Properties of the Congruences

(C1) $\mathbf{Z}' \models x + z \equiv_m y + z \longleftrightarrow x \equiv_m y \longleftrightarrow x - y \equiv_m 0$

(C2) $\mathbf{Z}' \models x \equiv_m y \longleftrightarrow nx \equiv_{nm} ny$ for $n \in \mathbb{N} \setminus \{0\}$

(C3) $\mathbf{Z}' \models \bigvee_{i=0}^{m-1} x \equiv_m y + i$

(C4) $\mathbf{Z}' \models x \equiv_{nm} y \longrightarrow x \equiv_m y$ for $n \in \mathbb{N} \setminus \{0\}$

## Positive Normal Forms

Using (C3), we obtain $\mathbf{Z}' \models \neg x \equiv_m y \longleftrightarrow \bigvee_{i=1}^{m-1} x \equiv_m y + i$. Furthermore, $\mathbf{Z} \models \neg x = y \longleftrightarrow x < y \vee y < x$. Finally, using $t \leqslant t'$ as an abbreviation for $t < t' + 1$ it holds that $\mathbf{Z}' \models \neg x < y \longleftrightarrow y \leqslant x$.

# Presburger Arithmetic Admits QE and is Decidable

## Theorem (Presburger, 1929)

(i) *There is a QEP for* $\mathbf{Z}' = (\mathbb{Z}; 0, 1, +, -; <, \{\equiv_m\}_{m \in \mathbb{N}})$.

(ii) $\mathbf{Z}' = (\mathbb{Z}; 0, 1, +, -; <, \{\equiv_m\}_{m \in \mathbb{N}})$ *is decidable.*

(iii) $\mathbf{Z} = (\mathbb{Z}; 0, 1, +, -; <)$ *is decidable.*

## Proof.

(i) On the next slides . . .

(ii) Atomic sentences are equivalent in $\mathbf{Z}'$ to of one of the normal forms $z = 0$, $z < 0$, $z \equiv_m 0$ for $z \in \mathbb{Z}$ and $m \in \mathbb{N}$. These can be evaluated to either true or false.

(iii) Follows immediately from (ii).

Consider a positive 1-primitive formula

$$\varphi = \exists x \left[ \bigwedge_{i=1}^{m} k_i x = a_i \wedge \bigwedge_{i=1}^{n} l_i x < b_i \wedge \bigwedge_{i=1}^{p} m_i x > c_i \wedge \bigwedge_{i=1}^{q} r_i x \equiv_{s_i} d_i \right],$$

where $k_i, l_i, m_i, r_i, s_i \in \mathbb{N} \setminus \{0\}$, $a_i, b_i, c_i, d_i \in \mathcal{T}$, $x \notin \mathcal{V}(a_i)$, $x \notin \mathcal{V}(b_i)$, $x \notin \mathcal{V}(c_i)$, $x \notin \mathcal{V}(d_i)$. For the normal form of the congruences, we have used (C1). In analogy to DOAG compute

$$k := \operatorname{lcm}(k_1, \dots k_m, l_1, \dots, l_n, m_1, \dots, m_p, r_1, \dots, r_q) \in \mathbb{N} \setminus \{0\}$$

and cofactors $k_i' = k/k_i$, $l_i' = k/l_i$, $m_i' = k/m_i$, $r_i' = k/r_i$. Set $a_i' = k_i' a_i$, $b_i' = l_i' b_i$, $c_i' = m_i' c_i$, $d_i' = r_i' d_i$, and $s_i' = r_i' s_i$ to obtain $\mathbf{Z}' \models \varphi \longleftrightarrow \varphi'$, where

$$\varphi' = \exists x \left[ \bigwedge_{i=1}^{m} kx = a_i' \wedge \bigwedge_{i=1}^{n} kx < b_i' \wedge \bigwedge_{i=1}^{p} kx > c_i' \wedge \bigwedge_{i=1}^{q} kx \equiv_{s_i'} d_i' \right]$$

For the choice of $s_i'$ we have used (C2).

$$\varphi' = \exists x \left[ \bigwedge_{i=1}^{m} kx = a_i' \wedge \bigwedge_{i=1}^{n} kx < b_i' \wedge \bigwedge_{i=1}^{p} kx > c_i' \wedge \bigwedge_{i=1}^{q} kx \equiv_{s_i'} d_i' \right]$$

For this $\varphi'$ we have in turn $\mathbf{Z}' \models \varphi' \longleftrightarrow \varphi''$, where

$$\varphi'' = \exists y \left[ \bigwedge_{i=1}^{m} y = a_i' \wedge \bigwedge_{i=1}^{n} y < b_i' \wedge \bigwedge_{i=1}^{p} y > c_i' \wedge \bigwedge_{i=1}^{q} y \equiv_{s_i'} d_i' \wedge y \equiv_k 0 \right].$$

If $m > 0$, then we obtain

$$\mathbf{Z}' \models \varphi'' \longleftrightarrow \bigwedge_{i=2}^{m} a_1' = a_i' \wedge \bigwedge_{i=1}^{n} a_1' < b_i' \wedge \bigwedge_{i=1}^{p} a_1' > c_i' \wedge \bigwedge_{i=1}^{q} a_1' \equiv_{s_i'} d_i' \wedge a_1' \equiv_k 0.$$

Consider now the case $m = 0$. Set $s = \operatorname{lcm}(s_1', \ldots, s_q', k) \in \mathbb{N} \setminus \{0\}$. Then using (C4) we obtain $\mathbf{Z}' \models \varphi'' \longleftrightarrow \varphi'''$, where

$$\varphi''' = \bigvee_{j=0}^{s-1} \left[ \exists y \left[ \bigwedge_{i=1}^{n} y < b_i' \wedge \bigwedge_{i=1}^{p} y > c_i' \wedge y \equiv_s j \right] \wedge \bigwedge_{i=1}^{q} j \equiv_{s_i'} d_i' \wedge j \equiv_k 0 \right].$$

$$\varphi''' = \exists y \left[ \bigwedge_{i=0}^{n} y < b_i' \wedge \bigwedge_{i=0}^{p} y > c_i' \wedge y \equiv_s j \right]$$

If $n = 0$ or $p = 0$, then one can choose $y = j \pm s \cdot t$ for sufficiently large $t \in \mathbb{N}$, hence

$$\mathbf{Z}' \models \varphi''' \longleftrightarrow \text{true}.$$

If, in contrast, $n > 0$ and $p > 0$, then

$$\mathbf{Z}' \models \varphi''' \longleftrightarrow \bigvee_{\max=1}^{p} \left[ \bigwedge_{i=1}^{p} c_i' \leqslant c_{\max}' \wedge \bigvee_{j'=1}^{s} \bigwedge_{i=1}^{n} (c_{\max}' + j' < b_i' \wedge c_{\max}' + j' \equiv_s j) \right].$$

That is, we trial substitute the smallest point that is larger than the largest lower bound $c_{\max}$ and satisfies the congruence. □

# Divisibility Instead of Congruences

Using (C1) we have for $x, y \in \mathbb{Z}$ and $m \in \mathbb{N} \setminus \{0\}$ that $x \equiv_m y$ iff $m \mid x - y$.

Instead of $\mathcal{L}'$ and $\mathbf{Z}'$ we could obviously use $\mathcal{L}'' = \left(0, 1, +, -; <, \{D_m^{(1)}\}_{m \in \mathbb{N} \setminus \{0\}}\right)$ and $\mathbf{Z}'' = \left(\mathbb{Z}; 0, 1, +, -; <, \{D_m\}_{m \in \mathbb{N} \setminus \{0\}}\right)$, where $\mathbf{Z}'' \models D_m(z) \iff m \mid z$.

## Exercise

Consider $\mathcal{L}''' = \left(0, 1, +, -; <, \{E_m^{(1)}\}_{m \in \mathbb{N} \setminus \{0\}}\right)$ and

$$\mathbf{Z}''' = \left(\mathbb{Z}; 0, 1, +, -, <, \{E_m\}_{m \in \mathbb{N} \setminus \{0\}}\right), \text{ where } \mathbf{Z}''' \models E_m(z) \iff z \mid m.$$

Then $\mathbf{Z}'''$ is decidable but does not admit QE.

Consider more generally $\mathcal{L}^* = (0, 1, +, -, \cdot; <, |^{(2)})$, $\mathbf{Z}^* = (\mathbb{Z}; 0, 1, +, -; <, |)$.

## Theorem

*$\mathbf{Z}^* = (\mathbb{Z}; 0, 1, +, -; <, |)$ is undecidable.*

Since $\mathbf{Z}^*$ is complete and decidable for $A_\varnothing$ it follows that $\mathbf{Z}^*$ does not admit QE.

By Gödel's incompleteness theorem $\mathbf{N} = (\mathbb{N} \setminus \{0\}, +, \cdot)$ is undecidable. Setting $\nu := 0 < x$ and considering $\nu(x)$ we have $[\nu]^{\mathbf{Z}^*} = \mathbb{N} \setminus \{0\}$. It now suffices to show that $\cdot^{\mathbf{N}}$ is definable in $\mathbf{Z}^*$. Consider $\mu_1(x, y, z)$ for

$$\begin{aligned} \mu_1 \quad = \quad & 0 < x \wedge 0 < y \wedge 0 < z \wedge x \mid z \wedge y \mid z \\ & \wedge \forall w (0 < w \wedge x \mid w \wedge y \mid w \longrightarrow z \mid w). \end{aligned}$$

Then $\mathbf{Z}^* \models \mu_1(a, b, c)$ iff $a, b, c \in \mathbb{N} \setminus \{0\}$ and $c = \operatorname{lcm}(a, b)$.
Next, consider $\mu_2(x, z)$ for

$$\mu_2 = \mu_1[x + 1/y].$$

Then $\mathbf{Z}^* \models \mu_2(a, c)$ iff $a, c \in \mathbb{N} \setminus \{0\}$ and

$$c = \operatorname{lcm}(a, a + 1) = a \cdot (a + 1) = a^2 + a.$$

Next, consider $\mu_3(x, z)$ for

$$\mu_3 = \mu_2[x + z/z].$$

Then $\mathbf{Z}^* \models \mu_3(a, c)$ iff $a, c \in \mathbb{N} \setminus \{0\}$ and $c = a^2$.

$$\mu_3(x,z), \quad \mathbf{Z}^* \models \mu_3(a,c) \text{ iff } a, c \in \mathbb{N} \setminus \{0\} \text{ and } c = a^2.$$

Finally, consider $\mu_4(x,y,z)$ for

$$\mu_4 = \exists u \exists v \exists w (\mu_3[u/z] \wedge \mu_3[y/x, v/z] \wedge \mu_3[x+y/x, w/z] \wedge w = u + 2z + v).$$

Then $\mathbf{Z}^* \models \mu_4(a,b,c)$ iff $a$, $b$, $c \in \mathbb{N} \setminus \{0\}$ and there are $n_u$, $n_v$, $n_w \in \mathbb{N} \setminus \{0\}$ such that

$$n_u = a^2, \quad n_v = b^2, \quad n_w = (a+b)^2, \quad \text{and} \quad n_w = n_u + 2c + n_v,$$

which is equivalent to $c = ab$. □

# Application: Integer Programming

## Exercise

Maximize the objective function $x + y$ subject to the constraints

$2x \geqslant 1$, $y \geqslant 0$, $y \leqslant 10 - 7x$

(a) over $\mathbb{R}$,

(b) over $\mathbb{Z}$.

Start with the elimination of $y$.

```
input  : a, b ∈ ℤ
output: c ∈ ℤ
begin
    if a < b then x := a; y := b; else y := a; x := b;
    while x < y do
        x := x + 1; y := y − 1;
    end
    if x = y then c := x; else c := y;
end
```

The program terminates with output $c \in \mathbb{Z}$ on input $a, b \in \mathbb{Z}$ iff $\mathbf{Z}' \models \varphi(a, b, c)$ for $\varphi(a, b, c)$, where

$$\begin{aligned}\varphi \quad = \quad & \exists x \exists y \exists x' \exists y' \exists z \big[((a < b \wedge x = a \wedge y = b) \vee (\neg a < b \wedge y = a \wedge x = b)) \\ & \wedge 0 \leqslant z \wedge y' \leqslant x' \wedge x' - 1 < y' + 1 \wedge x' = x + z \wedge y' = y - z \\ & \wedge ((x' = y' \wedge c = x') \vee (\neg x' = y' \wedge c = y'))\big].\end{aligned}$$

$$\begin{aligned}\varphi \quad = \quad & \exists x \exists y \exists x' \exists y' \exists z \big[((a < b \wedge x = a \wedge y = b) \vee (\neg a < b \wedge y = a \wedge x = b)) \\ & \wedge 0 \leqslant z \wedge y' \leqslant x' \wedge x' - 1 < y' + 1 \wedge x' = x + z \wedge y' = y - z \\ & \wedge ((x' = y' \wedge c = x') \vee (\neg x' = y' \wedge c = y'))\big]\end{aligned}$$

Our QEP yields $\mathbf{Z}' \models \varphi' \longleftrightarrow \varphi$ for

$$\varphi' = a + b = 2c \vee (2c \leqslant a + b \wedge a + b < 2c + 2 \wedge \neg a + b = 2c).$$

## Exercise

1. That is $c = \ldots$?
2. Perform the QE.

Consider $\mathcal{L}' = (0, 1, +, -, ; <, \equiv_m)$.

### What Have We Actually Used for Our Proof of Presburger QE?

1. $\mathbb{Z}$ is an ordered abelian Group with minimial a positive element 1.
2. The relations $\equiv_m$ for $1 < m \in \mathbb{N}$ are defined by $x \equiv_m y \longleftrightarrow \exists z(x + mz = y)$.
3. For all $1 < m \in \mathbb{N}$ it holds that $\bigvee_{i=0}^{m-1} x \equiv_m i \cdot 1$.

Denote by $\Xi_{\text{ZGROUPS}} \subseteq \mathcal{Q}$ the set of these axioms.

$$\text{ZGROUPS} = \text{Mod}(\Xi_{\text{ZGROUPS}})$$

is the class of $\mathbb{Z}$**-groups**.

$\mathbf{Z}' \in \text{ZGROUPS}$, and also

$(\mathbb{Q} \times \mathbb{Z}; 0, 1, +, -; <_{\text{lex}}, \equiv_m)$, $(\mathbb{R} \times \mathbb{Z}; 0, 1, +, -; <_{\text{lex}}, \equiv_m) \in \text{ZGROUPS}$.

# Results on $\mathbb{Z}$-Groups

## Theorem

(i) *There is a QEP for* ZGROUPS*.*

(ii) ZGROUPS *is substructure complete and model complete.*

(iii) ZGROUPS *is complete and decidable.*

## Proof.

(iii) Variable-free atomic formulas in normal form, i.e. $z = 0$, $z < 0$, $0 < z$, $z \equiv_m 0$ for $z \in \mathbb{Z}$, $1 < m \in \mathbb{N}$, are decidable. □

## Mojzesz Presburger

*Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt*

Dissertation, Warsaw 1929

Consider a set $M$. For $S \in P(M)$ define $\complement S = M \setminus S$.

Consider $\mathcal{L}_{BA} = (0^{(0)}, 1^{(0)}, \sqcap^{(2)}, \sqcup^{(2)}, \sim^{(1)}; \leqslant^{(2)})$, $\mathbf{A}_0 = (P(M); \varnothing, M, \cap, \cup, \complement; \subseteq)$.

## Theorem

$\mathbf{A}_0 = (P(M); \varnothing, M, \cap, \cup, \complement; \subseteq)$ *does not admit QE if* $|M| \geqslant 3$.

## Proof.

Consider $\varphi(y)$ for $\varphi = \exists x(\neg x = 0 \wedge \neg x = y \wedge x \leqslant y)$. Then $[\varphi]^{\mathbf{A}_0} = \{\, S \in P(M) \mid |S| \geqslant 2 \,\}$. In particular, $\varnothing \notin [\varphi]^{\mathbf{A}_0}$, and there are $m_1$, $m_2 \in M$ such that $\{m_1\} \notin [\varphi]^{\mathbf{A}_0}$, but $\{m_1, m_2\} \in [\varphi]^{\mathbf{A}_0}$ and $\{m_1, m_2\} \neq M$. All atomic formulas in $\mathcal{A}_{\{y\}}$ are equivalent to one of true, false, $y = 0$, $y = 1$, which define the sets $D = \{P(M), \varnothing, \{\varnothing\}, \{M\}\}$. Closing under complements and unions we see that the following sets are definable by formulas in $\mathcal{Q}^0_{\{y\}}$:
$D' = D \cup \{P(M) \setminus \{\varnothing\}, P(M) \setminus \{M\}, \{\varnothing, M\}, P(M) \setminus \{\varnothing, M\}\}$. However, $\varnothing \in P(M), \{\varnothing\}, P(M) \setminus \{M\}, \{\varnothing, M\}$, $\{m_1, m_2\} \notin \varnothing$, $\{M\}$, and $\{m_1\} \in P(M) \setminus \{\varnothing\}, P(M) \setminus \{\varnothing, M\}$. $\square$

# Once Again, We Have to Extend the Language

Consider $M \neq \varnothing$ and $A = P(M)$. For $n \in \mathbb{N}$ and $S$, $T \in A$ define

$$S \subset_n T \iff S \subseteq T \text{ and } |T \setminus S| \geqslant n.$$

In particular $S \subset_0 T \iff S \subseteq T$ and $\varnothing \subset_n T \iff n \leqslant |T|$.

Consider $\mathcal{L}'_{BA} = (0^{(0)}, 1^{(0)}, \sqcap^{(2)}, \sqcup^{(2)}, \sim^{(1)}; \{<_n\}_{n \in \mathbb{N}})$

and $\mathbf{A} = (P(M);\ \varnothing, M, \cap, \cup, \complement;\ \{\subset_n\}_{n \in \mathbb{N}})$.

**Lemma**

(i) $\mathbf{A} \models s <_0 t \longleftrightarrow 0 = s \sqcap {\sim} t$

$\mathbf{A} \models s = t \longleftrightarrow s <_0 t \wedge t <_0 s$

$\mathbf{A} \models s <_n t \longleftrightarrow s <_0 t \wedge 0 <_n t \sqcap {\sim} s$

(ii) $\mathbf{A} \models 0 <_n t \wedge 0 <_{n'} t \longleftrightarrow 0 <_{\max(n,n')} t$

$\mathbf{A} \models \neg 0 <_n t \wedge \neg 0 <_{n'} t \longleftrightarrow \neg 0 <_{\min(n,n')} t$

(iii) $\mathbf{A} \models \neg 0 = t \longleftrightarrow 0 <_1 t$ $\square$

So we can restrict our attention to atomic formulas $0 = t$ and $0 <_n t$.

In a conjunction, $0 <_n t$ need occur for at most one $n \in \mathbb{N}$,

and also $\neg 0 <_n t$ need occur for at most one $n \in \mathbb{N}$.

Logically negated equations can be made positive.

Consider $t \in \mathcal{T}$ with $\mathcal{V}(t) = \{x, y_1, \ldots, y_m\}$.

Transform $t$ into **full DNF** $t'$. That is, $\mathbf{A} \models t = t'$, where

$$t' = \bigsqcup_{i \in I} (x \sqcap a_i) \sqcup \bigsqcup_{i \in J} (\sim x \sqcap a_i), \quad a_i = \prod_{j=1}^{m} y_j^{(i)}, \quad y_j^{(i)} \in \{y_j, \sim y_j\}.$$

All the $a_i$ for $i \in I \cup J$ are pairwise different but $I \cap J \neq \varnothing$ in general.

For $i, i' \in I \cup J$ we have $\mathbf{A} \models (x \sqcap a_i) \sqcap (\sim x \sqcap a_{i'}) = 0$,

and if $i \neq i'$, then even $\mathbf{A} \models a_i \sqcap a_{i'} = 0$ and thus $\mathbf{A} \models (x \sqcap a_i) \sqcap (x \sqcap a_{i'}) = 0$.

It follows that all unions in $t'$ are disjoint unions for all choices of $x$, $y_1$, $\ldots$, $y_m \in P(M)$.

$$t' = \bigsqcup_{i \in I} (x \sqcap a_i) \sqcup \bigsqcup_{i \in J} (\sim x \sqcap a_i) \in \mathcal{T}$$

$$\mathbf{A} \models 0 = t' \longleftrightarrow \bigwedge_{i \in I} 0 = x \sqcap a_i \wedge \bigwedge_{i \in J} 0 = \sim x \sqcap a_i$$

$$\begin{aligned} \mathbf{A} \models 0 <_n t' &\longleftrightarrow \bigvee_{\substack{0 \leqslant n_1, n_2 \leqslant n \\ n_1 + n_2 = n}} \left[ 0 <_{n_1} \bigsqcup_{i \in I} x \sqcap a_i \wedge 0 <_{n_2} \bigsqcup_{i \in J} \sim x \sqcap a_i \right] \\ &\longleftrightarrow \bigvee_{\substack{0 \leqslant n_1, n_2 \leqslant n \\ n_1 + n_2 = n}} \bigvee_{\substack{\{0 \leqslant k_i \leqslant n_1\}_{i \in I} \\ \sum_{i \in I} k_i = n_1}} \bigvee_{\substack{\{0 \leqslant l_i \leqslant n_2\}_{i \in J} \\ \sum_{i \in J} l_i = n_2}} \left[ \bigwedge_{i \in I} 0 <_{k_i} x \sqcap a_i \wedge \bigwedge_{i \in j} 0 <_{l_i} \sim x \sqcap a_i \right] \end{aligned}$$

- We need only consider atomic formulas of the forms

$$0 = x \sqcap a_i, \quad 0 = \sim x \sqcap a_i, \quad 0 <_{k_i} x \sqcap a_i, \quad 0 <_{l_i} \sim x \sqcap a_i \quad \text{for} \quad i \in I \cup J.$$

- $\mathbf{A} \models a_i \sqcap a_{i'} = 0$ for $i \neq i'$.
- Equations occur only as positive base formulas (no "¬" in front of equations).

**Lemma (Elimination of complements)**

(i) $\mathbf{A} \models 0 = \sim x \sqcap a_i \longleftrightarrow a_i = x \sqcap a_i$

(ii) $\mathbf{A} \models 0 <_{l_i} \sim x \sqcap a_i \longleftrightarrow x \sqcap a_i <_{l_i} a_i$ $\square$

**Theorem**

*There is a QEP for* $\mathbf{A} = (P(M);\ \emptyset, M, \cap, \cup, \complement;\ \{\subset_n\}_{n \in \mathbb{N}})$.

It suffices to consider 1-primitive formulas of the form $\varphi = \exists x \bigwedge_{i \in I} \bigwedge \Phi_i$, where

$$\Phi_i \subseteq \{0 = x \sqcap a_i,\ a_i = x \sqcap a_i,$$
$$0 <_{k_i} x \sqcap a_i,\ \neg 0 <_{l_i} x \sqcap a_i,\ x \sqcap a_i <_{m_i} a_i,\ \neg x \sqcap a_i <_{n_i} a_i\},$$

and $\mathbf{A} \models a_i \sqcap a_{i'} = 0$ for $i, i' \in I$ with $i \neq i'$.Consider $\varphi' = \bigwedge_{i \in I} \exists x \bigwedge \Phi_i$.

Obviously $\mathbf{A} \models \varphi \longrightarrow \varphi'$. Vice versa, fix values for the $y_1, \ldots, y_m$ in $P(M)$, and for $i \in I$ let $s_i \in P(M)$ be a satisfying value for $x$ in $\bigwedge \Phi_i$. Set $s = \bigsqcup_{i \in I} s_i \sqcap a_i$. Then for $i \in I$ it holds that $s \sqcap a_i = s_i \sqcap a_i$. Hence $s$ is a satisfying value for $x$ in $\bigwedge_{i \in I} \bigwedge \Phi_i$. We have shown that also $\mathbf{A} \models \varphi' \longrightarrow \varphi$, altogether $\mathbf{A} \models \varphi \longleftrightarrow \varphi'$.

It thus suffices to independently consider 1-primitive formulas

$$\varphi_i'' = \exists x \bigwedge \Phi_i \quad \text{for} \quad i \in I.$$

$$\varphi'' = \exists x \bigwedge \Phi, \quad \Phi \quad \subseteq \quad \{0 = x \sqcap a, \ \ a = x \sqcap a,$$
$$0 <_k x \sqcap a, \ \ \neg 0 <_l x \sqcap a, \ \ x \sqcap a <_m a, \ \ \neg x \sqcap a <_n a\}$$

- If $0 = x \sqcap a \in \Phi$, then $x = 0$ is a solution of this equation, and we can equivalently replace $x \sqcap a$ with 0 in $\Phi$.
- If $a = x \sqcap a \in \Phi$, then $x = a$ is a solution of this equation, and we can equivalently replace $x \sqcap a$ with $a$ in $\Phi$.
- $\mathbf{A} \models \exists x(0 <_k x \sqcap a) \longleftrightarrow 0 <_k a$
- $\mathbf{A} \models \exists x(\neg 0 <_l x \sqcap a) \longleftrightarrow \begin{cases} \text{true} & \text{if} \quad l > 0 \\ \text{false} & \text{if} \quad l = 0 \end{cases}$
- $\mathbf{A} \models \exists x(x \sqcap a <_m a) \longleftrightarrow 0 <_m a$
- $\mathbf{A} \models \exists x(\neg x \sqcap a <_n a) \longleftrightarrow \begin{cases} \text{true} & \text{if} \quad n > 0 \\ \text{false} & \text{if} \quad n = 0 \end{cases}$

$$\varphi'' = \exists x \bigwedge \Phi$$
$$\Phi \subseteq \{0 <_k x \sqcap a,\ \neg 0 <_l x \sqcap a,\ x \sqcap a <_m a,\ \neg x \sqcap a <_n a\}, \quad |\Phi| \geqslant 2$$

- $\mathbf{A} \models \exists x(0 <_k x \sqcap a \land \neg 0 <_l x \sqcap a) \longleftrightarrow \begin{cases} 0 <_k a & \text{if} \quad k < l \\ \text{false} & \text{if} \quad l \leqslant k \end{cases}$
- $\mathbf{A} \models \exists x(0 <_k x \sqcap a \land x \sqcap a <_m a) \longleftrightarrow 0 <_{k+m} a$
- $\mathbf{A} \models \exists x(0 <_k x \sqcap a \land \neg x \sqcap a <_n a) \longleftrightarrow \begin{cases} 0 <_k a & \text{if} \quad n > 0 \\ \text{false} & \text{if} \quad n = 0 \end{cases}$
- $\mathbf{A} \models \exists x(\neg 0 <_l x \sqcap a \land x \sqcap a <_m a) \longleftrightarrow \begin{cases} 0 <_m a & \text{if} \quad l > 0 \\ \text{false} & \text{if} \quad l = 0 \end{cases}$
- $\mathbf{A} \models \exists x(\neg 0 <_l x \sqcap a \land \neg x \sqcap a <_n a) \longleftrightarrow \begin{cases} \neg 0 <_{l+n-1} a & \text{if} \quad l \cdot n > 0 \\ \text{false} & \text{if} \quad l \cdot n = 0 \end{cases}$
- $\mathbf{A} \models \exists x(x \sqcap a <_m a \land \neg x \sqcap a <_n a) \longleftrightarrow \begin{cases} \text{true} & \text{if} \quad m < n \\ \text{false} & \text{if} \quad n \leqslant m \end{cases}$

$$\begin{aligned} \varphi'' &= \exists x \bigwedge \Phi \\ \Phi &\subseteq \left\{ 0 <_k x \sqcap a,\ \ \neg 0 <_l x \sqcap a,\ \ x \sqcap a <_m a,\ \ \neg x \sqcap a <_n a \right\}, \quad |\Phi| \geqslant 3 \end{aligned}$$

## Exercise

- $\exists x(0 <_k x \sqcap a \wedge \neg 0 <_l x \sqcap a \wedge x \sqcap a <_m a) \longleftrightarrow \dots$
- $\exists x(0 <_k x \sqcap a \wedge \neg 0 <_l x \sqcap a \wedge \neg x \sqcap a <_n a) \longleftrightarrow \dots$
- $\exists x(0 <_k x \sqcap a \wedge x \sqcap a <_m a \wedge \neg x \sqcap a <_n a) \longleftrightarrow \dots$
- $\exists x(\neg 0 <_l x \sqcap a \wedge x \sqcap a <_m a \wedge \neg x \sqcap a <_n a) \longleftrightarrow \dots$

$$\varphi'' \quad = \quad \exists x(0 <_k x \sqcap a \wedge \neg 0 <_l x \sqcap a \wedge x \sqcap a <_m a \wedge \neg x \sqcap a <_n a)$$

$$\varphi'' \longleftrightarrow \begin{cases} \neg 0 <_{l+n-1} a & \text{if} \quad k < l \text{ and } m < n \\ \text{false} & \text{if} \quad l \leqslant k \text{ or } n \leqslant m \end{cases}$$

□

## Corollary

(i) $\mathbf{A} = (P(M);\ \varnothing, M, \cap, \cup, \complement;\ \{\subset_n\}_{n\in\mathbb{N}})$ *is decidable in* $\mathcal{L}'_{BA}$.

(ii) $\mathbf{A}_0 = (P(M);\ \varnothing, M, \cap, \cup, \complement;\ \subseteq)$ *is decidable in* $\mathcal{L}_{BA}$.

## Proof.

(i) We need only decide atomic sentences of the forms $0 = 0$, $0 = 1$, $0 <_n 0$, $0 <_n 1$ for $n \in \mathbb{N}$: We have $\mathbf{A} \models 0 = 0 \longleftrightarrow \text{true}$,

$$\begin{aligned}
\mathbf{A} &\models 0 = 1 \longleftrightarrow \begin{cases} \text{true} & \text{iff} \quad |A| = 1 \quad \text{iff} \quad M = \varnothing \\ \text{false} & \text{iff} \quad |A| > 1 \quad \text{iff} \quad M \neq \varnothing, \end{cases} \\
\mathbf{A} &\models 0 <_n 0 \longleftrightarrow \begin{cases} \text{true} & \text{iff} \quad n = 0 \\ \text{false} & \text{iff} \quad n > 0, \end{cases} \\
\mathbf{A} &\models 0 <_n 1 \longleftrightarrow \begin{cases} \text{true} & \text{iff} \quad |A| \geqslant 2^n \quad \text{iff} \quad |M| \geqslant n \\ \text{false} & \text{iff} \quad |A| < 2^n \quad \text{iff} \quad |M| < n, \end{cases}
\end{aligned}$$

(ii) For $\varphi \in \mathbf{A}_0$ rewrite $\subseteq$ as $\subset_0$, and decide $\varphi$ in $\mathbf{A}$. □

# Atomic Boolean Algebras

Let $B$ be a Boolean Algebra.

$a \in B$ is an **atom** if $a \neq 0$, and there is **no** $b \in B$ with $0 < b < a$.

$B$ is **atomic** if for all $\emptyset \neq b \in B$ there is an atom $a \in B$ such that $a \leqslant b$.

## What have we actually used in our proofs

1. Axioms of Boolean Algebras in $\mathcal{L}'_{BA}$.
2. Definition of $<_n$ for $n \in \mathbb{N}$:

   $$x <_0 y \longleftrightarrow x \sqcap y = x,$$

   $$x <_1 y \longleftrightarrow x <_0 y \wedge \neg x = y,$$

   $$\{x <_n y \longleftrightarrow \exists x_1 \ldots \exists x_{n-1}(x <_1 x_1 \wedge x_1 <_1 x_2 \wedge \ldots \wedge x_{n-1} <_1 y)\}_{n>1}$$
3. Atomicity:

   $$\forall x(0 <_1 x \longrightarrow \exists y(0 <_1 y \wedge \neg 0 <_2 y \wedge y <_0 x))$$

Denote by $\Xi_{\mathrm{BA}} \subseteq \mathcal{Q}$ the set of these axioms.

$\mathrm{BA} = \mathrm{Mod}(\Xi_{\mathrm{BA}})$ is the class of **atomic Boolean Algebras**.

# Quantifier Eliminability and Decidability of BA

## Corollary

BA *has a QEP, is substructure complete and model complete but not complete.* □

## Corollary

BA *is decidable.*

## Proof.

Consider $\varphi \in \mathcal{Q}_{\varnothing}$. By QE compute $\varphi' \in \mathcal{Q}^0$ such that $\mathrm{BA} \models \varphi' \longleftrightarrow \varphi$. Recall that in $\varphi'$ we need only decide atomic sentences of the forms $0 = 0$, $0 = 1$, $0 <_n 0$, $0 <_n 1$ for $n \in \mathbb{N}$. Using our observations from the decision procedure for $\mathbf{A}$ above, we can compute a finite union $M_\varphi$ of intervals in $\mathbb{N}$ such that for $\mathbf{B} \in \mathrm{BA}$ it holds that $\mathbf{B} \models \varphi'$ iff there is $n \in M_\varphi$ such that $|B| = 2^n$. Accordingly, $\mathrm{BA} \models \varphi$ iff $M_\varphi = \mathbb{N}$. □

# Polynomials

Consider $\mathcal{L}_R = (0, 1, +, -, \cdot)$.

Let $\Xi_{\mathsf{FIELDS}} \subseteq \mathcal{Q}$ be a (finite) set of first-order axioms for fields.

Then $\mathsf{FIELDS} = \mathrm{Mod}(\Xi_{\mathsf{FIELDS}})$ is the class of all fields.

Recall that $0 \neq z \in \mathbb{Z}$ is a short notation for $\pm(1 + \cdots + 1)$ in $\mathcal{L}_R$.

The **distributive representation** of $t' \in \mathbb{Z}[x_1, \ldots, x_n]$ is $t' = \sum_{m \in M} a_m m$, where $M$ is finite, $0 \neq a_m \in \mathbb{Z}$, and $m = x_1^{e_1} \ldots x_n^{e_n}$ is a **power product** of variables.

The **semidistributive representation** wrt. $x_1$ of $t' \in \mathbb{Z}[x_1, \ldots, x_n]$ is $\sum_{i=1}^{d} p_i x_1^i$, where $p_i \in \mathbb{Z}[x_2, \ldots, x_n]$ are polynomials in distributive representation.

We call $\deg_{x_1}(t') = d$ the $x_1$**-degree**, $\mathrm{lc}_{x_1}(t') = p_d$ the **leading** $x_1$**-coefficient**, and $t'$ an $x_1$**-polynomial**.

## Lemma

*For each extended $\mathcal{L}_R$-term $t(x_1, \ldots, x_n)$ there is $t' \in \mathbb{Z}[x_1, \ldots, x_n]$ in semi-distributive representation wrt. $x_1$ such that* $\mathsf{FIELDS} \models t = t'$. □

# Pseudo-Reduction

Consider $x$-polynomials $0 \neq f = \sum_{i=1}^{m} a_i x^i$ and $g = \sum_{i=1}^{n} b_i x^i$ with $m \geqslant n$.

Define $h := b_n f - a_m x^{m-n} g = \sum_{i=0}^{m-1} (b_n a_i - a_m b_{i-(m-n)}) x^i$.

Notice that either $h = 0$ or $\deg_x(h) < m$.

We write $f \underset{g}{\longrightarrow} h$ and say that $h$ is obtained from $f$ via $x$**-reduction** modulo $g$.

Iterated $x$-reduction $f \underset{g}{\longrightarrow} f_1 \underset{g}{\longrightarrow} \dots \underset{g}{\longrightarrow} f_r$ is written as $f \overset{*}{\underset{g}{\longrightarrow}} f_r$.

If $f = 0$ or $\deg_x(f) < \deg_x(g)$, then there is no $x$-reduction modulo $g$ possible.

We then call $f$ in $x$**-normal form** modulo $g$.

# Pseudo-Division

For $x$-polynomials $f, g$ there is a unique $x$-reduction chain $f \xrightarrow[g]{} f_1 \xrightarrow[g]{} \dots \xrightarrow[g]{} f_r$ such that $f_r$ is in normal form modulo $g$.

There is then an $x$-polynomial $q$ with $\deg_x(q) = \deg_x(f) - \deg_x(g)$ such that

$$f_r = \mathrm{lc}_x(g)^r f - qg.$$

Equivalently, $\mathrm{lc}_x(g)^r f = qg + f_r$.

We call $\mathrm{quot}_x(f, g) := q$ the **quotient** of the $x$-division of $f$ by $g$.

We call $\mathrm{rem}_x(f, g) := f_r$ the **remainder** of the $x$-division of $f$ by $g$.

# Zeros of Remainders

## Lemma

*Let $f(x, y_1, \dots, y_s)$, $g(x, y_1, \dots, y_s)$ be nonzero $x$-polynomials. Let $\mathbf{F} \in$ FIELDS, and let $a, b_1, \dots, b_s \in F$ such that $\mathbf{F} \models \mathrm{lc}_x(g)(b_1, \dots, b_s) \neq 0$ and $\mathbf{F} \models g(a, b_1, \dots, b_s) = 0$.*

*If $f \xrightarrow[g]{*} f_r$, then $\mathbf{F} \models f(a, b_1, \dots, b_s) = 0 \longleftrightarrow f_r(a, b_1, \dots, b_s) = 0$.*
*In particular, $\mathbf{F} \models f(a, b_1, \dots, b_s) = 0 \longleftrightarrow \mathrm{rem}_x(f, g) = 0$.*

## Proof.

We have $f \xrightarrow[g]{*} f_r = \mathrm{lc}_x(g)f - qg$ for an $x$-polynomial $q$. Thus

$$\mathbf{F} \models f_r(a, \mathbf{b}) = \mathrm{lc}_x(g)(\mathbf{b})f(a, \mathbf{b}) - q(a, \mathbf{b})g(a, \mathbf{b}). \qquad \square$$

# Reducta

Consider an $x$-polynomial $f = \sum_{i=0}^{n} a_i x^i$ with $a_n \neq 0$.

We call $\mathrm{red}_x\, f = \sum_{i=0}^{n-1} a_i x^i$ the $x$-**reductum** of $f$.

**Lemma**

*For* $\mathbf{F} \in \mathrm{FIELDS}$ *and* $a, b_1, \dots, b_s \in F$ *with* $\mathbf{F} \models \mathrm{lc}_x(f)(\boldsymbol{b}) = 0$ *we have*

$$\mathbf{F} \models f(a, \boldsymbol{b}) = 0 \longleftrightarrow \mathrm{red}_x(f)(a, \boldsymbol{b}) = 0. \quad \square$$

## Theorem (Tarski, 1935)

*There is a QEP for* $\mathbf{C} = (\mathbb{C}; 0, 1, +, -, \cdot) \in$ FIELDS.

## Proof.

Consider a 1-primitive formula

$$\varphi = \exists x \left[ \bigwedge_{i=1}^{m} f_i = 0 \wedge \bigwedge_{i=1}^{m'} g_i \neq 0 \right],$$

where $\mathcal{V}(\varphi) \subseteq \{x, y_1, \dots, y_s\}$.

Set $g = \prod_{i=1}^{m'} g_i$, and recall that $g = 1$ for $m' = 0$.

Then $\mathbf{C} \models \varphi \longleftrightarrow \varphi'$, where $\varphi' = \exists x \left[ \bigwedge_{i=1}^{m} f_i = 0 \wedge g \neq 0 \right]$.

We are ging to distinguish three cases: $m = 0$, $m = 1$, $m > 1$. ...

# Case 1: $m = 0$

$\varphi' = \exists x\,(g \neq 0)$

Let $g = \sum_{j=0}^{n} b_j x^j$, and consider $\varphi'' = \bigvee_{j=0}^{n} b_j \neq 0$.

We are going to show that $\mathbf{C} \models \varphi' \longleftrightarrow \varphi''$:

Consider $(g \neq 0)(x, y_1, \dots, y_s)$, $\varphi''(y_1, \dots, y_s)$, and let $c_1, \dots, c_s \in \mathbb{C}$.

There is $d \in \mathbb{C}$ such that $g^{\mathbf{C}}(d, c_1, \dots, c_s) \neq 0^{\mathbf{C}}$ iff the univariate polynomial

$$g(x, c_1, \dots, c_s) := \sum_{j=0}^{n} b_j^{\mathbf{C}}(c_1, \dots, c_s) x^j$$

is not the zero polynomial iff $\varphi''^{\mathbf{C}}(c_1, \dots, c_s) = \top$. ...

$\varphi' = \exists x\, (f_1 = 0 \wedge g \neq 0)$

Let $f_1 = \sum_{j=0}^{n} a_j x^j$. Induction wrt. $\deg_x(f_1) = n$.

If $n = 0$, then $\mathbf{C} \models \varphi' \longleftrightarrow a_0 = 0 \wedge \exists x(g \neq 0)$, and we are in Case 1.

If $n > 0$, then $\mathbf{C} \models \varphi' \longleftrightarrow \varphi'' \vee \tilde{\varphi}''$, where

$$\varphi'' = a_n \neq 0 \wedge \varphi', \quad \tilde{\varphi}'' = a_n = 0 \wedge \exists x(\mathrm{red}_x(f_1) = 0 \wedge g \neq 0).$$

The quantifier in $\tilde{\varphi}''$ can be eliminated by the induction hypothesis.

Let $h = \mathrm{rem}_x(g^n, f_1)$, say, $h = \sum_{j=0}^{k} c_j x^j = a_n^r g^n - q f_1$.
Recall that $h = 0$ or $\deg_x(h) < \deg_x(f_1)$.
We are going to show that $\mathbf{C} \models \varphi'' \longleftrightarrow \varphi'''$, where $\varphi''' = a_n \neq 0 \wedge \bigvee_{j=0}^{k} c_j \neq 0$:
Let $b_1, \dots, b_s \in \mathbb{C}$ such that $a_n^{\mathbf{C}}(\mathbf{b}) \neq 0^{\mathbf{C}}$.

Let $a \in \mathbb{C}$ such that $f_1^{\mathbf{C}}(a, \mathbf{b}) = 0^{\mathbf{C}}$ and $g^{\mathbf{C}}(a, \mathbf{b}) \neq 0^{\mathbf{C}}$. It follows that $h^{\mathbf{C}}(a, \mathbf{b}) = {a_n^r}^{\mathbf{C}}(\mathbf{b}) {g^n}^{\mathbf{C}}(a, \mathbf{b}) \neq 0^{\mathbf{C}}$. Thus the univariate polynomial $\sum_{j=0}^{k} c_j^{\mathbf{C}}(\mathbf{b}) x^k$ is not the zero polynomial, and hence ${\varphi'''}^{\mathbf{C}}(\mathbf{b}) = \top$. ...

$\varphi'' = a_n \neq 0 \wedge \exists x\,(f_1 = 0 \wedge g \neq 0), \quad f_1 = \sum_{j=0}^{n} a_j x^j,$
$h = \sum_{j=0}^{k} c_j x^j = \mathrm{rem}_x(g^n, f_1) = a_n^r g^n - q f_1; \quad h = 0$ or $\deg_x h < \deg_x f_1$.
To show: $\mathbf{C} \models \varphi'' \longleftrightarrow \varphi'''$, where $\varphi''' = a_n \neq 0 \wedge \bigvee_{j=0}^{k} c_j \neq 0$.
Let $b_1, \dots, b_s \in \mathbb{C}$ such that $a_n^{\mathbf{C}}(\mathbf{b}) \neq 0^{\mathbf{C}}$.

Assume, vice versa, that $\varphi'''^{\mathbf{C}}(\mathbf{b}) = \top$. Let $g = \sum_{j=0}^{l} b_j x^j$. From $f_1$ and $g$ obtain univariate polynomials $f_1(x, \mathbf{b})$ and $g(x, \mathbf{b})$ by plugging in $\mathbf{b}$, and factorize:

$$f_1(x, \mathbf{b}) = a_n^{\mathbf{C}}(\mathbf{b}) \prod_{j=1}^{N} (x - \alpha_j)^{\mu_j}, \quad g(x, \mathbf{b}) = b_l^{\mathbf{C}}(\mathbf{b}) \prod_{j=1}^{L} (x - \beta_j)^{\nu_j},$$

where $\alpha_j$ pairwise different, $\beta_j$ pairwise different, $\sum_{j=1}^{N} \mu_j = n$, and $\sum_{j=1}^{L} \nu_j = l$. Assume for a contradiction that $\{\alpha_1, \dots, \alpha_N\} \subseteq \{\beta_1, \dots, \beta_L\}$. It follows that $g^n(x, \mathbf{b}) = b_l^{n\,\mathbf{C}}(\mathbf{b}) \prod_{j=1}^{L} (x - \beta_j)^{\nu_j n}$ with $\nu_j n \geqslant \nu_j$, and for a suitable $q'(x) \in \mathbb{C}[x]$ we obtain $f_1(x, \mathbf{b}) q'(x) = a_n^{r\,\mathbf{C}}(\mathbf{b}) g^n(x, \mathbf{b}) = h(x, \mathbf{b}) + q(x, \mathbf{b}) f_1(x, \mathbf{b})$. Thus $h(x, \mathbf{b}) = (q'(x) - q(x, \mathbf{b})) f_1(x, \mathbf{b})$. Now $\varphi'''^{\mathbf{C}}(\mathbf{b})$ states that $h(x, \mathbf{b}) \neq 0$ and thus $h \neq 0$. However, $\deg_x(f_1) = \deg_x(f_1(x, \mathbf{b})) \leqslant \deg_x(h(x, \mathbf{b})) \leqslant \deg_x(h)$, a contradiction. So $\varphi''^{\mathbf{C}}(\mathbf{b}) = \top$ with $x$ from $\{\alpha_1, \dots, \alpha_N\} \setminus \{\beta_1, \dots, \beta_L\} \neq \emptyset$. $\dots$

# Case 3: $m > 1$

$$\varphi' = \exists x \left[ \bigwedge_{i=1}^{m} f_i = 0 \wedge g \neq 0 \right]$$

Induction on $D = \sum_{i=1}^{m} \deg_x(f_i)$. If $D = 0$, then $\deg_x(f_i) = 0$ for all $i$, thus $\mathbf{C} \models \varphi' \longleftrightarrow \bigwedge_{i=1}^{m} f_i = 0 \wedge \exists x\,(g \neq 0)$, and we are in the Case 1. Consider now $D > 0$. If there is only one $i$ with $\deg f_i > 0$, then we are in Case 2. Assume w.l.o.g. that $\deg_x(f_1) \geqslant \deg_x(f_2) > 0$. Using our Lemma above, we obtain $\mathbf{C} \models \varphi' \longleftrightarrow \varphi'' \vee \varphi'''$, where

$$\begin{aligned} \varphi'' &= \exists x \left[ \mathrm{lc}_x(f_2) \neq 0 \wedge \mathrm{rem}_x(f_1, f_2) = 0 \wedge f_2 = 0 \wedge \bigwedge_{i=3}^{m} f_i = 0 \wedge g \neq 0 \right] \\ \varphi''' &= \exists x \left[ \mathrm{lc}_x(f_2) = 0 \wedge f_1 = 0 \wedge \mathrm{red}_x(f_2) = 0 \wedge \bigwedge_{i=3}^{m} f_i = 0 \wedge g \neq 0 \right]. \end{aligned}$$

On both $\varphi''$ and $\varphi'''$ we can perform QE by induction hypothesis. $\square$

# Decidability of the Field of Complex Numbers

**Theorem**

**C** *is decidable.*

**Proof.**

It suffices to decide atomic sentences of the form $z = 0$ for $z \in \mathbb{Z}$. We have

$$\mathbf{C} \models z = 0 \longleftrightarrow \begin{cases} \text{true} & \text{if} \quad z = 0 \\ \text{false} & \text{if} \quad z \neq 0. \end{cases} \qquad \square$$

# Algebraically Closed Fields

## What have we actually used in our proofs?

1. Axioms of fields in $\mathcal{L}_R$.
2. Every nonconstant univariate polynomial has a zero:

$$\left\{\forall a_0 \ldots \forall a_n \exists x \left[a_n \neq 0 \longrightarrow \sum_{i=0}^{n} a_i x^i = 0\right]\right\}_{n>0}$$

## Exercise

It follows that every nonconstant univariate polynomial factors into linear factors. Furthermore, universes of algebraically closed fields are infinite, because $x^n - 1$ has got $n$ different linear factors/zeros.

Denote by $\Xi_{\mathrm{ACF}}$ the set of these axioms.

$$\mathrm{ACF} = \mathrm{Mod}(\Xi_{\mathrm{ACF}}) \subset \mathrm{FIELDS}$$

is the class of **algebraically closed fields**.

# The Characteristic of a Field

Consider $\mathbf{F} \in$ FIELDS. There a two possible cases:

(a) There is $p \in \mathbb{N} \setminus \{0\}$ such that $\mathbf{F} \models p = 0$ and $\mathbf{F} \models \neg n = 0$ for all $n < p$.

(b) $\mathbf{F} \models \neg z = 0$ for all $z \in \mathbb{Z}$.

In Case (a) we say $\mathbf{F}$ has **characteristic** $p$, and we write $\operatorname{char}(\mathbf{F}) = p$.

In Case (b) we say $\mathbf{F}$ has **characteristic** 0, and we write $\operatorname{char}(\mathbf{F}) = 0$.

Denote by PRIMES $\subset \mathbb{N}$ the set of prime numbers.

## Examples

- $\operatorname{char}(\mathbb{C}) = \operatorname{char}(\mathbb{R}) = \operatorname{char}(\mathbb{Q}) = 0$
- for $p \in$ PRIMES we have $\mathbf{Z}/p \in$ FIELDS and $\operatorname{char}(\mathbf{Z}/p) = p$.

## Exercise

For $\mathbf{F} \in$ FIELDS we have $\operatorname{char}(\mathbf{F}) \in \text{PRIMES} \cup \{0\}$.

# QE and Completeness Results for ACF

## Some facts from algebra

- The characteristic is invariant under field extensions.
- Every field has got an algebraically closed extension field.

It follows that ACF contains fields of arbitrary (prime or zero) characteristic.

## Theorem

*There is a QEP for* ACF*. It follows that* ACF *is substructure complete and model complete.* ACF *is, however, not complete.*

## Proof.

We have constructed ACF in such a way that our QEP for $\mathbf{C}$ works there. Consider $\overline{\mathbf{Z}/2}, \mathbf{C} \in$ ACF, where $\overline{\mathbf{Z}/2}$ is an algebraically closed extension field of $\mathbf{Z}/2$. Then $\overline{\mathbf{Z}/2} \models 1 + 1 = 0$ but $\mathbf{C} \models \neg 1 + 1 = 0$. $\square$

# The Key to Decidability and Limited Completeness

## Theorem

*Consider $\mathcal{L}_R$ and $\varphi \in \mathcal{Q}_\varnothing$. One can compute a set $P_\varphi \subseteq \mathrm{PRIMES}$ with the following properties:*

(i) *$P_\varphi$ is either finite or co-finite.*

(ii) *For all $\mathbf{F} \in \mathrm{ACF}$ with $\mathrm{char}(\mathbf{F}) \neq 0$ we have $\mathbf{F} \models \varphi$ iff $\mathrm{char}(\mathbf{F}) \in P_\varphi$.*

(iii) *$\mathbf{F} \models \varphi$ for all $\mathbf{F}$ with $\mathrm{char}(\mathbf{F}) = 0$ iff $P_\varphi$ is co-finite.*

## Proof.

Compute a quantifier-free equivalent $\varphi'$ of $\varphi$. It suffices to construct $P_{\varphi'}$. Induction on $|\varphi'|$: If $\varphi'$ is atomic, then $\varphi'$ is equivalent to $z = 0$ for $z \in \mathbb{N}$. In case $z = 0$ we choose $P_{\varphi'}$ to be the set of all primes. In case $z \neq 0$ we choose $P_{\varphi'}$ to be the set of all prime factors of $z$. If $\varphi' = \neg\psi$, set $P_{\varphi'} = \mathrm{PRIMES} \setminus P_\psi$. If $\varphi' = \psi_1 \vee \psi_2$, set $P_{\varphi'} = P_{\psi_1} \cup P_{\psi_2}$. □

max planck institut informatik

# Decidability of ACF and Complete Subclasses

For $p \in \text{PRIMES} \cup \{0\}$ set $\text{ACF}_p = \{\, \mathbf{F} \mid \mathbf{F} \in \text{ACF and char}(\mathbf{F}) = p \,\}$.

**Theorem**

$\text{ACF}_p$ *is complete and decidable.*

**Proof.**

If $p \in \text{PRIMES}$, then $\text{ACF}_p \models \varphi$ iff $p \in P_\varphi$.

If $p = 0$ then $\text{ACF}_p \models \varphi$ iff $P_\varphi$ is co-finite. □

**Theorem**

ACF *is decidable.*

**Proof.**

$\text{ACF} \models \varphi$ iff $P_\varphi = \text{PRIMES}$. □

# The Lefschetz Principle

**Corollary**

*Let $\varphi \in \mathcal{Q}_{\varnothing}$. Assume that $\mathbf{C} \models \varphi$. Then $\mathrm{ACF}_0 \models \varphi$, and one can compute $p_\varphi \in \mathrm{PRIMES}$ such that $\mathrm{ACF}_p \models \varphi$ for all $p \geqslant p_\varphi$.*

**Proof.**

$\mathrm{ACF}_0 \models \varphi$ follows from the completeness of $\mathrm{ACF}_0$.
Compute a quantifier-free equivalent $\varphi'$ of $\varphi$. The set of atomic formulas in $\varphi'$ is essentially $\{ z = 0 \mid z \in N \}$ for some finite $N \subset \mathbb{N}$. For $p \in P = \{ p \in \mathrm{PRIMES} \mid p > \max N \}$ it holds that $\mathrm{ACF}_p \models \varphi'$ iff $\mathbf{C} \models \varphi'$. Hence we can choose $p_\varphi = \min P$. □

The $p_\varphi$ constructed in the proof is not necessarily the minimal possible choice.

# Signs of Univariate Real Polynomials



Consider $0 \neq f \in \mathbb{R}[x]$ with $\deg(f) = d$. Denote by $V_{\mathbb{R}}(f) = \{\, c \in \mathbb{R} \mid f(c) = 0 \,\}$

Assume that $V_{\mathbb{R}}(f) = \{c_1, \dots, c_r\}$ with $c_1 < \cdots < c_r$. Obviously $r \leqslant d$.

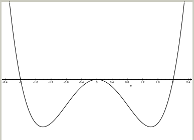
Then $f$ is sign invariant over each of the $2r + 1$ intervals

$$(-\infty, c_1), \quad c_1, \quad (c_1, c_2), \quad \dots, \quad c_r, \quad (c_r, \infty).$$

Define $\varepsilon = (\varepsilon_1, \dots, \varepsilon_{2r+1}) \in \{0, 1, -1\}^{2r+1}$:

$$\begin{aligned} \varepsilon_1 &= \operatorname{sgn} f(c_1 - 1), & \varepsilon_{2r+1} &= \operatorname{sgn} f(c_r + 1), \\ \varepsilon_{2j} &= \operatorname{sgn} f(c_j) = 0, & \varepsilon_{2j+1} &= \operatorname{sgn} f\left(\tfrac{c_{2j} + c_{2j+1}}{2}\right) \qquad (1 \leqslant j < r). \end{aligned}$$

## Example



$$f = x^4 - 4x^2$$

$$r = 3, \quad c_1 = -2, \quad c_2 = 0, \quad c_3 = 2$$

$$\varepsilon = (1, 0, -1, 0, -1, 0, 1)$$

# Combined Signs of Univariate Polynomials

Consider $0 \neq f_1, \ldots, f_n \in \mathbb{R}[x]$. Then $\bigcup_{i=1}^n V_{\mathbb{R}}(f_i) = V_{\mathbb{R}}\left(\prod_{i=1}^n f_i\right)$.

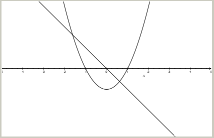
Let $V_{\mathbb{R}}(f_1 \cdot \cdots \cdot f_n) = \{c_1, \ldots, c_r\}$ with $c_1 < \cdots < c_r$, where $r \leqslant \sum_{i=1}^n \deg f_i$.

Define $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_{2r+1}) \in \{0, 1, -1\}^{n \times (2r+1)}$:

$$\varepsilon_{i,1} = \operatorname{sgn} f_i(c_1 - 1), \qquad \varepsilon_{i,2r+1} = \operatorname{sgn} f_i(c_r + 1),$$
$$\varepsilon_{i,2j} = \operatorname{sgn} f_i(c_j), \qquad \varepsilon_{i,2j+1} = \operatorname{sgn} f_i\left(\tfrac{c_{2j} + c_{2j+1}}{2}\right) \qquad (1 \leqslant j < r).$$

The **combined sign matrix** $\operatorname{CSM}(f_1, \ldots, f_n) := \varepsilon$ of $(f_1, \ldots, f_n)$ is uniquely determined by $(f_1, \ldots, f_n)$.

## Example



$f_1 = x^2 - 1$, $f_2 = -x$, $r = 3$, $c_1 = -1$, $c_2 = 0$, $c_3 = 1$

$$\operatorname{CSM}(f_1, f_2) = \begin{bmatrix} 1 & 0 & -1 & -1 & -1 & 0 & 1 \\ 1 & 1 & 1 & 0 & -1 & -1 & -1 \end{bmatrix}$$

Even columns contain at least one 0, odd columns never contain 0.

## Combined Signs: Zero Polynomials and Condensing

To obtain a non-empty matirx at least one of the $f_i$ must be non-constant.

We admit also zero polynomials in $\mathrm{CSM}(f_1, \ldots, f_n)$, which create a zero line.

Given $\mathrm{CSM}(f_1, \ldots, f_n)$, we can compute $\mathrm{CSM}(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_n)$ as follows:

1. Obtain $C \in \{0, 1, -1\}^{n-1 \times 2r+1}$ by deleting the $i$-th line of $\mathrm{CSM}(f_1, \ldots, f_n)$.
2. In $C$ substitute subsequent identical columns by one such column.

**Exercise**

1. Compute $\mathrm{CSM}(x, 2x + 1, 0, x^2 - 1)$.
2. From $\mathrm{CSM}(x, 2x + 1, 0, x^2 - 1)$ derive $\mathrm{CSM}(x, 2x + 1)$.

Our examples and exercises were based on guessing zeros of the $f_j$.

We now want to algorithmically obtain $\mathrm{CSM}(f_1, \ldots, f_n)$.

# Computation of Combined Sign Matrices

Consider $n > 0$, $f_1, \ldots, f_n \in \mathbb{R}[x]$ with $\prod_{j=1}^{n} f_j \neq 0$.

We proceed by recursion on $(d, k)$ wrt. $\leqslant_{\text{lex}}$,
where $d = \max\{\deg f_1, \ldots, \deg f_n\}$ and $k = |\{ j \in \{1, \ldots, n\} \mid \deg f_j = k \}|$.

If $d = 0$, then $f_1, \ldots, f_n \in \mathbb{R}$, and $\mathrm{CSM}(f_1, \ldots, f_n) = [\operatorname{sgn} f_1, \ldots, \operatorname{sgn} f_n]^t$.

**Theorem**

*Let $0 \neq f, g_1, \ldots, g_n \in \mathbb{R}[x]$ with $\deg f \geqslant \deg g_j \geqslant 1$ for $j \in \{1, \ldots, n\}$. Let $f'$ denote the formal derivative of $f$. Set $f_0 := \mathrm{rem}(f, f')$ and $f_j := \mathrm{rem}(f, g_j)$ for $j \in \{1, \ldots, n\}$. Assume that we know $\mathrm{CSM}(g_1, \ldots, g_n, f', f_0, \ldots, f_n)$.*

*Then we can compute $\mathrm{CSM}(f, g_1, \ldots, g_n, f', f_0, \ldots, f_n)$ and hence $\mathrm{CSM}(f, g_1, \ldots, g_n)$.*

Lines for constant polynomials $f_j$ can be tenporarily removed for recursion.

Let $(d', k')$ be the recursion parameter for $\mathrm{CSM}(g_1, \ldots, g_n, f', f_0, \ldots, f_n)$.
If $\deg f = \deg g_j$ for some $j$, then $d' = d$ but $k' < k$, else $d' = d - 1 < d$.

We are given $C' = \mathrm{CSM}(g_1, \dots, g_n, f', f_0, \dots, f_n)$.
From this we compute $C^* = \mathrm{CSM}(g_1, \dots, g_n, f') \in \{0, 1, -1\}^{(n+1)\times(2r+1)}$.
For obtaining $C = \mathrm{CSM}(f, g_1, \dots, g_n, f') \in \{0, 1, -1\}^{(n+2)\times(2s+1)}$ for $s \geqslant r$ we are going to proceed in two steps:

1. Compute the sign of $f$ for the even columns of $C^*$:
   Let $j \in \{1, \dots, r-1\}$. Column $2j$ of $C^*$ corresponds to a root $c_j$ of one of the polynomials $g_1, \dots, g_n, f'$. If $f'(c_j) = 0$, then
   $$f(c_j) = \mathrm{quot}(f, f')(c_j) \cdot f'(c_j) + \mathrm{rem}(f, f')(c_j) = \mathrm{rem}(f, f')(c_j) = f_0(c_j).$$
   Thus $\operatorname{sgn} f(c_j) = \operatorname{sgn} f_0(c_j)$. Similarly, if $g_i(c_j) = 0$, then $\operatorname{sgn} f(c_j) = \operatorname{sgn} f_i(c_j)$.
2. Compute entries for $f$ for the odd columns of $C^*$, which possibly requires replacing such columns by several ones ...

# Proof 

Let $j \in \{1, \ldots, r-1\}$ and consider sgn $f$ at column $2j+1$ of $C^*$:

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| sgn $f$ at $2j$ | 0 | 1 | $-1$ | $-1$ | $-1$ | 0 | 1 | 1 | 1 | $-1$ |
| sgn $f'$ at $2j+1$ | 1 | 1 | 1 | 1 | 1 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| sgn $f$ at $2j+2$ | | | 0 | 1 | $-1$ | | 0 | 1 | $-1$ | |
| sgn $f$ at $2j+1$ | 1 | 1 | $-1$ | $[-1, 0, 1]$ | $-1$ | $-1$ | 1 | 1 | $[1, 0, -1]$ | $-1$ |

## Exercise

Complete the proof by considering sgn $f$ at the columns 1 and $2r+1$ of $C^*$.

$\square$

# The Field of the Reals

**Theorem**

*Consider $\mathcal{L}_R = (0, 1, +, -, \cdot)$ and $\mathbf{R} = (\mathbb{R}; 0, 1, +, -, \cdot)$.*
*Then $\mathbf{R}$ does not admit QE.*

**Proof.**

Consider $\varphi(y)$ for $\varphi = \exists x (y = x \cdot x)$. We have $[\varphi]^{\mathbf{R}} = \mathbb{R}^{\geqslant} \subset \mathbb{R}$, which is neither finite nor cofinite in $\mathbb{R}$. Essentially $\mathcal{A}_{\{y\}} = \{\, f = 0 \mid f \in \mathbb{Z}[y] \,\}$. These define for $f = 0$ the cofinite set $\mathbb{R}$ and for left hand side polynomials $f \neq 0$ the finite sets $V_{\mathbb{R}}(f)$. It follows that quantifier-free formulas in $y$ define only finite and cofinite sets. □

We are now going to consider $\mathcal{L}_{OR} = (0, 1, +, -, ; \leqslant)$.
Our aim is to show that $\mathbf{R} = (\mathbb{R}; 0, 1, +, -, \cdot; \leqslant)$ admits QE.

# A Parametric Generalization of Combined Sign Matrices

## Theorem

*For $n > 0$ consider $x$-polynomials $f_1, \dots, f_n \in \mathbb{R}[x, y_1, \dots, y_m]$. Let $d = \max\{\deg_x f_1, \dots, \deg_x f_n\}$. Let $E \in \{0, 1, -1\}^{n \times (2r+1)}$ for $r \leqslant nd$. Then one can compute an extended quantifier-free $\mathcal{L}_{OR}$-formula $\psi_{E,n,d,f_1,\dots,f_n}(y_1, \dots, y_m)$ such that for $b_1, \dots, b_m \in \mathbb{R}$ it holds that $\mathbf{R} \models \psi_{E,n,d,f_1,\dots,f_n}(\boldsymbol{b}) \iff \mathrm{CSM}(f_1(x, \boldsymbol{b}), \dots, f_n(x, \boldsymbol{b})) = E$.*

## Proof.

We define $\square_0 :=$ " $=$ ", $\square_1 :=$ " $>$ ", $\square_{-1} :=$ " $<$ ". For $d = 0$ and $E = [\varepsilon_1, \dots, \varepsilon_n]^t \in \{0, 1, -1\}^{n \times 1}$ we have $f_1, \dots, f_n \in \mathbb{R}[y_1, \dots, y_m]$, and we can set $\psi = \bigwedge_{i=1}^{n} f_i \, \square_{\varepsilon_i} \, 0$. ...

# Proof.

For $d > 0$ we proceed recursively as for the computation of CSM with the following modifications:

- We use $x$-pseudodivision. When multiplying with a suitable power of the leading coefficient of the divisor, we must use even powers to preserve signs.
- We have to introduce case distinctions on the vanishing of the leading coefficient, and in the case, where it vanishes, use the reductum (with further case distinctions).
- Instead of computing signs of $f$, we conjunctuively collect the corresponding conditions $f \,\square_\sigma\, 0$ taking $\sigma$ from $E$. $\square$

# The Ordered Field of the Reals

**Theorem (Tarksi 1948 with a different proof)**

*There is a QEP for* $\mathbf{R} = (\mathbb{R}; 0, 1, +, -, \cdot; \leqslant)$ *in* $\mathcal{L}_{OR}$.

**Proof.**

It suffices to consider a positive 1-primitive formula $\varphi = \exists x \bigwedge_{i=1}^{n} f_i \, \varrho_i \, 0$ with $\varrho \in \{=, <\}$. Let $d = \max\{\deg_x f_1, \dots, \deg_x f_n\}$. The set $M = \bigcup_{r \leqslant nd} \{0, 1, -1\}^{n \times (2r+1)}$ is finite. Let $M_\varphi$ be the finite set of all $E \in M$ that contain a column $[\varepsilon_1, \dots, \varepsilon_n]^t$ such that $\varepsilon_i = \square_{\varrho_i}$. Then $\mathbf{R} \models \varphi \longleftrightarrow \bigvee_{E \in M_\varphi} \psi_{E,n,d,f_1,\dots,f_n}$. $\square$

# Real Closed Fields

## What have we used in our proofs?

1. Axioms of ordered fields:
   (a) Axioms of fields.
   (b) Monotonicity: $x \leqslant y \longrightarrow x + z \leqslant y + z$ and $x \leqslant y \wedge 0 \leqslant z \longrightarrow xz \leqslant yz$.
   This implies characteristic 0.
2. Every nonnegative number has square root: $0 \leqslant x \longrightarrow \exists y(y^2 = x)$.
3. Every nonconstant univariate polynomial of odd degree has a zero:

$$\left\{\forall a_0 \dots \forall a_{2n+1} \exists x \left[a_{2n+1} \neq 0 \longrightarrow \sum_{i=0}^{2n+1} a_i x^i = 0\right]\right\}_{n \geqslant 0}.$$

Denote by $\Xi_{\mathrm{RCF}}$ the set of these axioms.

$\mathrm{RCF} = \mathrm{Mod}(\Xi_{\mathrm{RCF}}) \subset \mathrm{FIELDS}$ is the class of **real closed fields**.

We have $\mathbf{R} \in \mathrm{RCF}$ but $\mathbf{Q} = (\mathbb{Q}; 0, 1, +, -, \cdot; \leqslant) \notin \mathrm{RCF}$.

# QE, Completeness, and Decidability for RCF

**Theorem**

RCF *admits QE. It follows that* RCF *is substructure complete and thus model complete. Furthermore,* RCF *is complete and decidable.*

**Proof.**

It suffices to show that RCF is complete and decidable for atomic sentences, which are equivalent to either $z = 0$ or $z \leqslant 0$ for $z \in \mathbb{Z}$. Monotonicity implies that 0, $\pm(1 + \cdots + 1)$ are ordered as in $\mathbb{Z}$. □

# Completeness and Decidability for RCF Without Ordering

## Corollary

*The class* $\mathrm{RCF}' = \{\, \mathbf{F}|_{\mathcal{L}_R} \mid \mathbf{F} \in \mathrm{RCF}\,\}$ *of real closed fields in a the language of rings without ordering does not admit QE. Hence* $\mathrm{RCF}'$ *is not substructure complete.* $\mathrm{RCF}'$ *is, however, model complete, complete, and decidable.*

## Proof.

For model completeness we have to show that every $\mathcal{L}_R$-formula $\varphi$ is equivalent to an existential $\mathcal{L}_R$-formula. Consider an $\mathcal{L}_R$-formula $\varphi$. Then $\varphi$ is also an $\mathcal{L}_{OR}$-formula. By QE compute a positive quantifier-free $\mathcal{L}_{OR}$-formula $\varphi'$ such that $\mathrm{RCF} \models \varphi \longleftrightarrow \varphi'$. From $\varphi'$ we obtain $\varphi''$ by equivalently replacing all atomic formulas $0 \leqslant f$ with $\exists r_f(r_f^2 = f)$ and making prenex. Then we have $\mathrm{RCF} \models \varphi \longleftrightarrow \varphi' \longleftrightarrow \varphi''$, and since $\varphi''$ is an $\mathcal{L}_R$-formula it follows that $\mathrm{RCF}' \models \varphi \longleftrightarrow \varphi''$. □

Recall that quantifier elimination procedures based on considering 1-primitive formulas are not elementary recursive in general.

**Theorem (Collins, 1975)**

*The time complexity procedure of real quantifier elimination is bounded from above by* $2^{2^{O(n^k)}}$*, where* $k \in \mathbb{N} \setminus \{0\}$ *is fixed and n is the word length of the input formula.* $\square$

**Theorem (Davenport–Heintz and independently Weispenning, 1988)**

*The time complexity of real quantifier elimination bounded from below by* $2^{2^{\Omega(n)}}$*, where n is the word length of the input formula.* $\square$

# Software

Collins proof was constructive:

- He described **cylindrical algebraic decomposition** (CAD) as a QE method.
- A first implementation QEPCAD was finished in 1983.
- Considerable heuristic improvemend by Hong lead to **partial CAD** in 1995.
- QEPCAD B is now maintained by Brown and freely available at `http://www.usna.edu/cs/~qepcad/B/QEPCAD.html`.

**Exercise**

Download, compile, and try.

# Focus on Formulas with Low Degrees in the Quantified Variables

Let $f$ be in distributive representation $f = \sum_{m \in M} a_m x_1^{e_{m,1}} \cdots x_n^{e_{m,n}}$.
For $I \subseteq \{1, \dots, n\}$ the **total degree** in $V = \{\, x_i \mid i \in I \,\}$ of $f$ is $\max_{m \in M} \sum_{i \in I} e_{m,i}$.

**Example**

The total degree of $2a^7 x^2 yz + y^3 - x + 1$ in $\{x, y, z\}$ is 4.

The total degree in $V$ of an atomic $\mathcal{L}_{OR}$-formula $f \varrho 0$, $\varrho \in \{=, \leqslant\}$ is that of $f$.

The total degree in $V$ of a quantifier-free formula is the maximum of the total degrees of the contained atomic formulas.

The total degree of a prenex formula $\varphi = Q_1 x_1 \dots Q_n x_n \psi$ is the total degree in $\{x_1, \dots, x_n\}$ of $\psi$.

In particular, $\varphi$ is **linear** if its total degree is 1, **quadratic** if its total degree is 2, and **cubic** if its total degree is 3.

**Exercise**

Give some examples for linear and quadratic formulas.

# Weispfenning Has Shown Much More

- The lower bound $2^{2^{O(n)}}$ holds even when restricting to linear formulas. This is called the **linear real quantifier elimination problem**.
- Looking at finer complexity parameters, linear QE looks nicer.

**Theorem (Weispfenning 1988)**

*Consider the subset of prenex linear formulas $\Phi_{c,q,a}$ with at most $c$ changes between $\exists$ and $\forall$ in the quantifier block, at most $q$ quantifiers, and at most $a$ different atomic formulas. Then the real quantifier elimination problem for $\Phi_{c,n,a}$ is bounded from above by $2^{2^{O(c)}}$, $2^{O(q)}$, and $O(a^k)$ for some $k \in \mathbb{N} \setminus \{0\}$ not depending on $\Phi_{c,q,a}$.* $\square$

- Note that the number of unquantified variables does not significantly contribute to the complexity.
- Partial CAD, in contrast, is doubly exponential in the number of **all** variables.

Consider a linear formula $\varphi = Q_1 x_1 \dots Q_n x_n \psi$.

By induction on $n$ it suffices to eliminate the innermost quantifier $Q_n x_n$.

If $Q_n = \forall$, then we transform $\mathbf{R} \models \forall x_n \psi \longleftrightarrow \neg\exists x_n \neg\psi$.

It thus suffices to eliminate $\exists x_n \psi$, and we may assume w.l.o.g. that $\psi$ is positive.

Note that we have not computed any Boolean normal form.

$\psi$ is an arbitrary $\wedge$-$\vee$-combination of atomic formulas $ax_n < b$, $ax_n \leqslant b$, $b < 0$, $b \leqslant 0$, where $a \in \mathcal{T} \setminus \{0\}$, $b \in \mathcal{T}$ with $x_n \notin \mathcal{V}(a) \cup \mathcal{V}(b)$.

Fix real values for all variables in $\mathcal{V}(\psi) \setminus \{x_n\}$.

Then atomic formulas describe intervals $(-\infty, \frac{b}{a})$, $(\frac{b}{a}, \infty)$, $(-\infty, \frac{b}{a}]$, $[\frac{b}{a}, \infty)$, $\emptyset$, $\mathbb{R}$.

$\psi$ describes $\emptyset$, $\mathbb{R}$, or a finite union of intervals

$$(-\infty, \tfrac{b}{a}), \quad (\tfrac{b}{a}, \infty), \quad (-\infty, \tfrac{b}{a}], \quad [\tfrac{b}{a}, \infty), \quad (\tfrac{b}{a}, \tfrac{b'}{a'}), \quad [\tfrac{b}{a}, \tfrac{b'}{a'}), \quad (\tfrac{b}{a}, \tfrac{b'}{a'}], \quad [\tfrac{b}{a}, \tfrac{b'}{a'}],$$

which contains one of the points $\frac{b}{a} \pm 1$, $\frac{b/a + b'/a'}{2}$.

Consider $\varphi = \exists x_n \psi$. Let $\{\, a_i x_n \ \varrho_i \ b_i \mid i \in I \,\}$, where $\varrho_i \in \{<, \leqslant\}$, be the finite set of atomic formulas in $\psi$ containing $x$. Then

$$E = \left\{\, (\mathrm{true}, 0),\ \left(a_i \neq 0 \land a_j \neq 0, \tfrac{b_i/a_i + b_j/a_j}{2}\right),\ \left(a_i \neq 0, \tfrac{b_i}{a_i} \pm 1\right) \;\middle|\; i,\ j \in I \,\right\}$$

is an **elimination set** for $\varphi$ with the property

$$\mathbf{R} \models \varphi \longleftrightarrow \bigvee_{(\gamma, t) \in E} \left(\gamma \land \psi[t//x_n]\right).$$

Notice that the **test terms** $t$ contain division with even parametric divisors.

The **guards** $\gamma$ guarantee that the $t$ are at least semantically meaningful.

For all bounded intervals we substitute the midpoint.

For the unbounded intervals we substitute the endpoints $\pm 1$.

We substitute 0 for the case that all other guards are false.

Recall that for regular substitution we have $[t/x_n] : \mathcal{T} \to \mathcal{T}$.

We define a **virtual substitution** $[t//x_n] : \mathcal{A} \to \mathcal{Q}^0$:

$$(a_i x_n \ \varrho_i \ b_i)\left[\tfrac{p}{q}//x_n\right] := a_i p q \ \varrho_i \ b_i q^2.$$

This substitution result is linear in $\{x_1, \dots, x_{n-1}\}$, which is important.

# Examples for Advanced Virtual Substitution

Instead of the $\left(a_i \neq 0, \frac{b_i}{a_i} + 1\right)$ for all $i \in I$ for the unbounded interval $\left(\frac{b_i}{a_i}, \infty\right)$ we can use $(\text{true}, \infty)$, where

$$\begin{aligned} (a_i x_n < b_i)[\infty // x_n] \quad &:= \quad a_i < 0 \\ (a_i x_n \leqslant b_i)[\infty // x_n] \quad &:= \quad a_i < 0 \lor (a_i = 0 \land 0 \leqslant b_i). \end{aligned}$$

Consider $\left(a_i \neq 0 \land a_j \neq 0, \frac{b_i/a_i + b_j/a_j}{2}\right)$ used for an interval with endpoints $\frac{b_i}{a_i}$, $\frac{b_j}{a_j}$.

If both $\frac{b_i}{a_i}$ and $\frac{b_j}{a_j}$ origin from strict constraints $a_i x_n < b_i$, $a_j x_n < b_j$, then it suffices to subsitute $\left(a_i \neq 0, \frac{b_i}{a_i} - \varepsilon\right)$, $\left(a_j \neq 0, \frac{b_j}{a_j} - \varepsilon\right)$, where

$$\begin{aligned} (a_i x_n < b_i)\left[\tfrac{p}{q} - \varepsilon // x_n\right] \quad &:= \quad a_i pq < b_i q^2 \lor (a_i pq = b_i q^2 \land 0 < a_i) \\ (a_i x_n \leqslant b_i)\left[\tfrac{p}{q} - \varepsilon // x_n\right] \quad &:= \quad (a_i x_n < b_i)\left[\tfrac{p}{q} - \varepsilon // x_n\right] \lor (a_i = 0 \land b_i = 0). \end{aligned}$$

If w.l.o.g. $\frac{b_i}{a_i}$ origins from a **weak constraint** $a_i x_n \leqslant b_i$, then we use $\left(a_i \neq 0, \frac{b_i}{a_i}\right)$.

This reduces $|E|$ from $O(|I|^2)$ to $O(|I|)$.

# Understanding the Complexity Results

Consider $\varphi = Q_{n-1}x_{n-1}\exists x_n\psi$.

We obtain $E$ and compute $\mathbf{R} \models \varphi \longleftrightarrow \varphi'$, where

$$\varphi' = Q_{n-1}x_{n-1} \bigvee_{(\gamma,t)\in E} \big(\gamma \wedge \psi[t//x_n]\big).$$

In the case that $Q_{n-1} = \exists$, we can transform

$$\mathbf{R} \models \varphi' \longleftrightarrow \bigvee_{(\gamma,t)\in E} \exists x_{n-1}\big(\gamma \wedge \psi[t//x_n]\big).$$

This yields for the next step $|E|$ many **independent** QE problems $\varphi''_1, \dots, \varphi''_{|E|}$.

Test terms produced for some $\varphi''_i$ need not be substituted into $\varphi''_j$ for $j \neq i$.

Therefore, the complexity is only exponential in the quantifiers
but doubly exponential in the quantifier changes.

# Quadratic Formulas

Consider a quadratic formula $\varphi = Q_1 x_1 \dots \exists x_n \psi$.

$\psi$ is an arbitrary $\wedge$-$\vee$-combination of linear atomic formulas and, in addition, $a x_n^2 + b x_n + c \mathrel{\varrho} 0$ for $a \in \mathcal{T} \setminus \{0\}$, $b, c \in \mathcal{T}$ with $x \notin \mathcal{V}(a) \cup \mathcal{V}(b) \cup \mathcal{V}(c)$.

Fix real values for all variables in $\mathcal{V}(\psi) \setminus \{x\}$.

Then all atomic formulas describe finite unions of intervals, where $a x_n^2 + b x_n + c$ contributes interval boundaries $\pm\infty$ and $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

We have to explain how to perform virtual substitutions $(f \mathrel{\varrho} 0)\left[\frac{p_1 \pm \sqrt{p_2}}{q} // x\right]$.

## Exercise

Let $f \in [x_1, \dots, x_n]$. There are $P_1$, $P_2$, $Q$ such that $f\left[\frac{p_1 + p_2\sqrt{p_3}}{q} / x_n\right] = \frac{P_1 + P_2\sqrt{p_3}}{Q}$.

Using this we have, e.g.,

$$(f = 0)\left[\frac{p_1 + p_2\sqrt{p_3}}{q} // x_n\right] = (x_n = 0)\left[\frac{P_1 + P_2\sqrt{p_3}}{Q} // x_n\right] := P_1 P_2 \leqslant 0 \wedge P_1^2 - P_2^2 p_3 = 0.$$

The substitution result is **not** quadratic in $\{x_1, \dots, x_{n-1}\}$ in general.

# Beyond the Quadratic Case

We have just seen that eliminating an innermost quantifier from a quadratic formula, the result is not necessarily quadratic anymore.

It is not clear in advance if the elimination of several quantifiers from a quadratic formula using our quadratic method will succeed.

With linear formulas this problem does not exist.

Weispfenning (1997) has shown that virtual substitution is flexible enough to generalize to arbitrary total degrees.

In particular, the fact that roots of polynomials beyond degree 4 cannot be expressed with root expressions is **no obstacle**.

The (incomplete) method for the quadratic case is successfully used in practice.

In case of **degree violations** one switches to partial CAD.

Implementations of virtual substitution for the cubic case appear promising.

# Software

The virtual substitution methods, partial CAD, and many other QE procedures are implemented in the package Redlog of the open-source computer algebra system Reduce.

Reduce/Redlog is freely available at Sourceforge `http://sourceforge.net/apps/mediawiki/reduce-algebra/index.php?title=Installation`.

**Exercise**

SVN checkout, compile, and try.

Comprehensive information on Redlog can be found at `http://www.redlog.eu`.

The online database Remis there, contains many application examples for QE.