WISST! The Lefschetz principle

or: What is... quantifier elimination?

Given polynomials $f_1, \ldots, f_r$ and $g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_n]$ study the solvability of the system

$$\begin{aligned} f_i &= 0,\ i \in [r], \\ g_j &\neq 0,\ j \in [s], \end{aligned} \tag{$\exists$}$$

over varying fields $\mathbb{K}$.

WISST! The Lefschetz principle

or: What is... quantifier elimination?

Given polynomials $f_1, \ldots, f_r$ and $g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_n]$ study the solvability of the system

$$\begin{aligned} f_i = 0,\ i \in [r], \\ g_j \neq 0,\ j \in [s], \end{aligned} \tag{$\exists$}$$

over varying algebraically closed fields $\mathbb{K}$.

WISST! The Lefschetz principle

or: What is... quantifier elimination?

Given polynomials $f_1, \dots, f_r$ and $g_1, \dots, g_s \in \mathbb{Z}[x_1, \dots, x_n]$ study the solvability of the system

$$\begin{aligned} f_i &= 0,\ i \in [r], \\ g_j &\neq 0,\ j \in [s], \end{aligned} \tag{$\exists$}$$

over varying algebraically closed fields $\mathbb{K}$.

Note: the $\mathbb{Z}$ coefficients make sense in every field $\mathbb{K}$ by interpreting $k \in \mathbb{Z}$ as $\underbrace{1 + 1 + \cdots + 1}_{k \text{ times}} \in \mathbb{K}$.

The Lefschetz principle

1. The answer to $(\exists)$ depends only on the characteristic of the field. If a solution exists over $\mathbb{K}$, then also over $\overline{\mathbb{K}'}$ (i.e. $\overline{\mathbb{Q}}$ or $\overline{\mathbb{F}_p}$).

The Lefschetz principle

1. The answer to $(\exists)$ depends only on the characteristic of the field. If a solution exists over $\mathbb{K}$, then also over $\overline{\mathbb{K}'}$ (i.e. $\overline{\mathbb{Q}}$ or $\overline{\mathbb{F}_p}$).

2. If $(\exists)$ has a solution in characteristic 0, then it has a solution over characteristic $p > 0$ for all but finitely many primes p.

The Lefschetz principle

1. The answer to $(\exists)$ depends only on the characteristic of the field. If a solution exists over $\mathbb{K}$, then also over $\overline{\mathbb{K}'}$ (i.e. $\overline{\mathbb{Q}}$ or $\overline{\mathbb{F}_p}$).

2. If $(\exists)$ has a solution in characteristic 0, then it has a solution over characteristic $p > 0$ for all but finitely many primes p.

3. In particular if $(\exists)$ has a solution over $\mathbb{C}$, it has a solution in finite fields $\mathbb{F}_{p^m}$ for all but finitely many primes p.

The Lefschetz principle

1. The answer to $(\exists)$ depends only on the characteristic of the field. If a solution exists over $\mathbb{K}$, then also over $\overline{\mathbb{K}'}$ (i.e. $\overline{\mathbb{Q}}$ or $\overline{\mathbb{F}_p}$).

2. If $(\exists)$ has a solution in characteristic 0, then it has a solution over characteristic $p > 0$ for all but finitely many primes p.

3. In particular if $(\exists)$ has a solution over $\mathbb{C}$, it has a solution in finite fields $\mathbb{F}_{p^m}$ for all but finitely many primes p.

4. The set of characteristics over which $(\exists)$ has a solution can be effectively computed from the defining polynomials f_i and g_j.

Polynomial systems and Model theory

Model theory studies "models": mathematical objects interpreting symbols of a formal language and satisfying axioms written in that language

Polynomial systems and Model theory

Model theory studies "models": mathematical objects interpreting symbols of a formal language and satisfying axioms written in that language as well as the theory of a given model, i.e. all formulas in the language which are true in this model.

Polynomial systems and Model theory

Model theory studies "models": mathematical objects interpreting symbols of a formal language and satisfying axioms written in that language as well as the theory of a given model, i.e. all formulas in the language which are true in this model.

(First-order) language of rings:

- constants 0 and 1
- functions $+$, $-$, $\cdot$
- relations $=$

Polynomial systems and Model theory

Model theory studies "models": mathematical objects interpreting symbols of a formal language and satisfying axioms written in that language as well as the theory of a given model, i.e. all formulas in the language which are true in this model.

(First-order) language of rings:

- constants 0 and 1
- functions $+$, $-$, $\cdot$
- relations $=$
- Boolean logic connectives $\wedge$, $\vee$, $\neg$ ($\Rightarrow$, $\Leftrightarrow$, $\dots$)
- $\exists$ and $\forall$ quantifiers
- variables $x_1, x_2, \dots$.

Formulas, axioms and definability

The definition of a ring can be written in the language of rings:

- $\forall a : a - a = 0$
- $\forall a, b, c : (a + b) + c = a + (b + c)$
- $\forall a, b : a + b = b + a$
- $\dots$

Formulas, axioms and definability

The definition of a ring can be written in the language of rings:

- $\forall a : a - a = 0$
- $\forall a, b, c : (a + b) + c = a + (b + c)$
- $\forall a, b : a + b = b + a$
- $\ldots$

A field is a commutative ring with inverses:

- $\forall a \exists b : \neg(a = 0) \Rightarrow ab = 1$

Formulas, axioms and definability

The definition of a ring can be written in the language of rings:

- $\forall a : a - a = 0$
- $\forall a, b, c : (a + b) + c = a + (b + c)$
- $\forall a, b : a + b = b + a$
- ...

A field is a commutative ring with inverses:

- $\forall a \exists b : \neg(a = 0) \Rightarrow ab = 1$

($\exists$) is expressible as a sentence in this language:

$$\exists x_1, \ldots, x_n : \bigwedge_{i=1}^{r} f_i(x_1, \ldots, x_n) = 0 \wedge \bigwedge_{j=1}^{s} \neg(g_j(x_1, \ldots, x_n) = 0)$$

Quantifier elimination

The theory of *algebraically closed* fields admits quantifier elimination in the language of rings.

Quantifier elimination

The theory of *algebraically closed* fields admits quantifier elimination in the language of rings. That is, for each formula φ there exists an equivalent formula ψ without $\exists$ or $\forall$ quantifiers, such that for every algebraically closed field $\mathbb{K}$:

$$\mathbb{K} \models \varphi \iff \mathbb{K} \models \psi.$$

Quantifier elimination

The theory of *algebraically closed* fields admits quantifier elimination in the language of rings. That is, for each formula φ there exists an equivalent formula ψ without $\exists$ or $\forall$ quantifiers, such that for every algebraically closed field $\mathbb{K}$:

$$\mathbb{K} \models \varphi \quad \Leftrightarrow \quad \mathbb{K} \models \psi.$$

Eliminating quantifiers (and hence all variables) from ($\exists$) results in a Boolean combination of (in)equations $n = m$ for some $n, m \in \mathbb{Z}$.

Quantifier elimination

The theory of *algebraically closed* fields admits quantifier elimination in the language of rings. That is, for each formula φ there exists an equivalent formula ψ without $\exists$ or $\forall$ quantifiers, such that for every algebraically closed field $\mathbb{K}$:

$$\mathbb{K} \models \varphi \quad \Leftrightarrow \quad \mathbb{K} \models \psi.$$

Eliminating quantifiers (and hence all variables) from ($\exists$) results in a Boolean combination of (in)equations $n = m$ for some $n, m \in \mathbb{Z}$.

These inequalities point out exactly which characteristics are required and which are ruled out for having a solution to ($\exists$).