Polynomial Invariants for Affine Programs

Ehud Hrushovski, Joël Ouaknine, Amaury Pouly, James Worrell

Max Planck Institute for Software Systems &
Department of Computer Science, Oxford University &
Mathematical Institute, Oxford University &
Université de Paris, IRIF, CNRS
Does this program halt?

Affine program

\[
x := 2^{-10} \\
y := 1 \\
\text{while } y \geq x \text{ do} \\
\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}
\]
Does this program halt?

Affine program

\[
x := 2^{-10}
\]
\[
y := 1
\]
while \( y \geq x \) do
\[
\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ 7/4 & 1/4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}
\]

Certificate of non-termination:

\[x^2 y - x^3 = 1023\]

\(x^2 y - x^3 = 1073741824\) (1)

\[
y \quad x
\]

\[
\begin{bmatrix} y \\ x \end{bmatrix} \rightarrow (1)
\]

(1) is an invariant: it holds at every step

(1) implies the guard is true
Does this program halt?

**Affine program**

\[ x := 2^{-10} \]
\[ y := 1 \]

while \( y \geq x \) do

\[
\begin{bmatrix}
  x \\
  y
\end{bmatrix}
:=
\begin{bmatrix}
  2 & 0 \\
  \frac{7}{4} & \frac{1}{4}
\end{bmatrix}
\begin{bmatrix}
  x \\
  y
\end{bmatrix}
\]

\[ y^2 - x^3 = 1023 \]

\[ 1073741824 \]

\( y^2 \) is an invariant: it holds at every step.

\( y^2 \) implies the guard is true.
Does this program halt?

Affine program

\[
\begin{align*}
x &:= 2^{-10} \\
y &:= 1 \\
\text{while } y \geq x \text{ do} \\
\begin{bmatrix} x \\ y \end{bmatrix} &:= \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}
\end{align*}
\]

Certificate of non-termination:

\[
x^2 y - x^3 = 1023 - 1073741824 \quad (1)
\]

\(y\) is an invariant: it holds at every step.

\((1)\) implies the guard is true.
Does this program halt?

Affine program

\[ x := 2^{-10} \]
\[ y := 1 \]
while \( y \geq x \) do
\[
\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}
\]

Certificate of non-termination:
\[ x^2 y - x^3 = 1023 - 1073741824 \]
Does this program halt?

Affine program

\[
\begin{align*}
x &:= 2^{-10} \\
y &:= 1 \\
\text{while } y \geq x \text{ do} & \quad \begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}
\end{align*}
\]

\[
\begin{align*}
\text{Certificate of non-termination:} & \quad x^2y - x^3 = 1023 - 1073741824
\end{align*}
\]

\[\text{▶ (1) is an invariant: it holds at every step} \]

\[\text{▶ (1) implies the guard is true} \]

\[\frac{2}{38} \]
Does this program halt?

Affine program

\[
\begin{align*}
x &:= 2^{-10} \\
y &:= 1 \\
\text{while } y \geq x \text{ do} \\
\begin{bmatrix} x \\ y \end{bmatrix} &:= \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}
\end{align*}
\]

Certificate of non-termination:

\[
x^2 y - x^3 = \frac{1023}{1073741824}
\] (1)
Does this program halt?

Affine program

\[ x := 2^{-10} \]
\[ y := 1 \]
while \( y \geq x \) do
\[
\begin{bmatrix}
    x \\
    y
\end{bmatrix}
:=
\begin{bmatrix}
    2 & 0 \\
    7/4 & 1/4
\end{bmatrix}
\begin{bmatrix}
    x \\
    y
\end{bmatrix}
\]

Certificate of non-termination:

\[
x^2y - x^3 = \frac{1023}{1073741824} \tag{1}
\]

(1) is an invariant: it holds at every step
Does this program halt?

**Affine program**

\[
x := 2^{-10} \\
y := 1 \\
\text{while } y \geq x \text{ do} \\
\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ 7/4 & 1/4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}
\]

**Certificate of non-termination:**

\[x^2y - x^3 = \frac{1023}{1073741824} \tag{1}\]

- (1) is an **invariant**: it holds at every step
- (1) implies the **guard** is true
invariant = \textit{overapproximation} of the \textit{reachable states}
Invariants

\[ \text{invariant} = \text{overapproximation of the reachable states} \]

\textbf{inductive} invariant = invariant preserved by the transition relation
Inductive invariants: example
Inductive invariants: example

$x, y, z$ range over $\mathbb{Q}$

$f_i : \mathbb{R}^3 \rightarrow \mathbb{R}^3$
Inductive invariants: example

\( x, y, z \) range over \( \mathbb{Q} \)

\[ f_i : \mathbb{R}^3 \rightarrow \mathbb{R}^3 \]
Inductive invariants: example

\(x, y, z\) range over \(\mathbb{Q}\)

\[f_i : \mathbb{R}^3 \rightarrow \mathbb{R}^3\]
Inductive invariants: example

\[ x, y, z \text{ range over } \mathbb{Q} \]

\[ f_i : \mathbb{R}^3 \rightarrow \mathbb{R}^3 \]
Inductive invariants: example

$x, y, z$ range over $\mathbb{Q}$

$f_i : \mathbb{R}^3 \to \mathbb{R}^3$
Inductive invariants: example

\[ x, y, z \text{ range over } \mathbb{Q} \]

\[ f_i : \mathbb{R}^3 \rightarrow \mathbb{R}^3 \]
Inductive invariants: example

\( x, y, z \) range over \( \mathbb{Q} \)

\( f_i : \mathbb{R}^3 \rightarrow \mathbb{R}^3 \)
Inductive invariants: example

$x, y, z$ range over $\mathbb{Q}$

$f_i : \mathbb{R}^3 \to \mathbb{R}^3$
Inductive invariants: example

$x, y, z$ range over $\mathbb{Q}$

$f_i : \mathbb{R}^3 \rightarrow \mathbb{R}^3$
Inductive invariants: example

\( x, y, z \) range over \( \mathbb{Q} \)

\[ f_i : \mathbb{R}^3 \rightarrow \mathbb{R}^3 \]
Inductive invariants: example

$x, y, z$ range over $\mathbb{Q}$

$f_i : \mathbb{R}^3 \rightarrow \mathbb{R}^3$
Inductive invariants: example

$x, y, z$ range over $\mathbb{Q}$

$f_i : \mathbb{R}^3 \rightarrow \mathbb{R}^3$
Inductive invariants: example

$x, y, z$ range over $\mathbb{Q}$

$f_i : \mathbb{R}^3 \rightarrow \mathbb{R}^3$

$S_1, S_2, S_3$ is an invariant
Inductive invariants: example

$x, y, z$ range over $\mathbb{Q}$

$S_1, S_2, S_3$ is an inductive invariant
Inductive invariants: example

$x, y, z$ range over $\mathbb{Q}$

$f_i : \mathbb{R}^3 \rightarrow \mathbb{R}^3$

$l_1, l_2, l_3$ is an invariant
Inductive invariants: example

\(x, y, z\) range over \(\mathbb{Q}\)

\(f_i : \mathbb{R}^3 \to \mathbb{R}^3\)

\(l_1, l_2, l_3\) is **NOT** an inductive invariant
Inductive invariants: example

$x, y, z$ range over $\mathbb{Q}$

$f_i : \mathbb{R}^3 \rightarrow \mathbb{R}^3$

$l_1, l_2, l_3$ is an inductive invariant
The classical approach to the verification of temporal safety properties of programs requires the construction of inductive invariants [...]. Automation of this construction is the main challenge in program verification.

D. Beyer, T. Henzinger, R. Majumdar, and A. Rybalchenko
Invariant Synthesis for Combined Theories, 2007
Which invariants?

Octagons
Polyhedrons
Affine/linear sets
Algebraic sets = polynomial equalities
Semialgebraic sets
Which invariants?

Intervals

Octagons

Polyhedrons

Affine/linear sets

Algebraic sets = polynomial equalities

Semialgebraic sets
Which invariants?

Octagons

\[ \lor \]

Intervals
Which invariants?

- Octagons
- Intervals
- Affine/linear sets

Algebraic sets = polynomial equalities

Semialgebraic sets
Which invariants?

**Intervals**

**Octagons**

**Polyhedrons**

**Affine/linear sets**
Which invariants?

Intervals \subseteq Octagons \subseteq Polyhedrons

\subseteq

Intervals \subseteq Affine/linear sets \subseteq Algebraic sets = polynomial equalities
Which invariants?

- Octagons
- Polyhedrons
- Semialgebraic sets
- Intervals
- Affine/linear sets
- Algebraic sets = polynomial equalities
Affine programs

- Nondeterministic branching (no guards)
- All assignments are affine
- Allow nondeterministic assignments ($x := \ast$)
- Can overapproximate complex programs
- Covers existing formalisms: probabilistic, quantum, quantitative automata
Affine programs

- Nondeterministic branching (no guards)

![Diagram of an affine program with nodes 1, 2, and 3 connected by edges labeled with functions $f_1$, $f_2$, $f_3$, $f_4$, and $f_5$.]
Affine programs

- Nondeterministic branching (no guards)
- All assignments are affine

\[ x := 3x - 7y + 1 \]
Affine programs

- Nondeterministic branching (no guards)
- All assignments are affine
- Allow nondeterministic assignments ($x := *$)
Affine programs

- Nondeterministic branching (no guards)
- All assignments are affine
- Allow nondeterministic assignments ($x := \ast$)

- Can overapproximate complex programs

![Diagram](attachment:image.png)
Affine programs

- Nondeterministic branching (no guards)
- All assignments are affine
- Allow nondeterministic assignments ($x := \ast$)

\[
x := 3x - 7y + 1
\]

- Can overapproximate complex programs
- Covers existing formalisms: probabilistic, quantum, quantitative automata
There is an algorithm which computes, for any given affine program over $\mathbb{Q}$, its strongest affine inductive invariant.
Discovering Affine Equalities Using Random Interpretation

Sumit Gulwani George C. Necula
University of California, Berkeley
{gulwani,necula}@cs.berkeley.edu

ABSTRACT
We present a new polynomial-time randomized algorithm for discovering affine equalities involving variables in a program.

Keywords
Affine Relationships, Linear Equalities, Random Interpretation, Randomized Algorithm
A Note on Karr’s Algorithm

Markus Müller-Olm\textsuperscript{1,*} and Helmut Seidl\textsuperscript{2}

Abstract. We give a simple formulation of Karr’s algorithm for computing all affine relationships in affine programs. This simplified algorithm runs in time $O(nk^3)$ where $n$ is the program size and $k$ is the number of program variables assuming unit cost for arithmetic operations. This improves upon the original formulation by a factor of $k$. Moreover, our re-formulation avoids exponential growth of the lengths of intermediately occurring numbers (in binary representation) and uses less complicated elementary operations. We also describe a generalization that determines all polynomial relations up to degree $d$ in time $O(nk^{3d})$.

Theorem (ICALP 2004)

There is an algorithm which computes, for any given affine program over $\mathbb{Q}$, all its polynomial inductive invariants up to any fixed degree $d$. 
Computing polynomial program invariants

Markus Müller-Olm\textsuperscript{a,*},\textsuperscript{1}, Helmut Seidl\textsuperscript{b}

\textsuperscript{a} FernUniversität Hagen, LG Praktische Informatik 5, 58084 Hagen, Germany
\textsuperscript{b} TU München, Informatik, 12, 85748 München, Germany

Received 16 October 2003; received in revised form 20 April 2004
Available online 19 June 2004
Computing polynomial program invariants

Markus Müller-Olm\textsuperscript{a,\*},\textsuperscript{1,} Helmut Seidl\textsuperscript{b}

\textsuperscript{a} FernUniversität Hagen, LG Praktische Informatik 5, 58084 Hagen, Germany
\textsuperscript{b} TU München, Informatik, I2, 85748 München, Germany

Received 16 October 2003; received in revised form 20 April 2004
Available online 19 June 2004

It is a challenging open problem whether or not the set of all valid polynomial relations can be computed not just the ones of some given form. It is not
Why fixed degree is not enough

\[
\begin{align*}
\text{Paraboloid} \quad & z = x^2 + y^2 \\
\text{Union of 3 hyperplanes} \quad & (x - y)(10y + x)(y + 10x) = 0
\end{align*}
\]
Why fixed degree is not enough

- Paraboloid

\[ z = x^2 + y^2 \]
Why fixed degree is not enough

- Paraboloid

\[ z = x^2 + y^2 \]
Why fixed degree is not enough

- Paraboloid
- Union of 3 hyperplanes

\[ z = x^2 + y^2 \]

\[ (x - y)(10y + x)(y + 10x) = 0 \]
Why fixed degree is not enough

- Paraboloid
- Union of 3 hyperplanes

\[ z = x^2 + y^2 \]

\[ (x - y)(10y + x)(y + 10x) = 0 \]
Why fixed degree is not enough

- Paraboloid
  \[ z = x^2 + y^2 \]
- Union of 3 hyperplanes
  \[ (x - y)(10y + x)(y + 10x) = 0 \]
Main result

**Theorem**

*There is an algorithm which computes, for any given affine program over $\mathbb{Q}$, its strongest polynomial inductive invariant.*
Main result

Theorem

There is an algorithm which computes, for any given affine program over \( \mathbb{Q} \), its strongest polynomial inductive invariant.

- strongest polynomial invariant \( \iff \) smallest algebraic set
Main result

Theorem

There is an algorithm which computes, for any given affine program over $\mathbb{Q}$, its strongest polynomial inductive invariant.

- strongest polynomial invariant $\iff$ smallest algebraic set
- algebraic sets = finite $\bigcup$ and $\bigcap$ of polynomial equalities
Main result

**Theorem**

There is an algorithm which computes, for any given affine program over $\mathbb{Q}$, its strongest polynomial inductive invariant.

- strongest polynomial invariant $\iff$ smallest algebraic set
  - algebraic sets $=$ finite $\bigcup$ and $\bigcap$ of polynomial equalities
- Thus our algorithm computes all polynomial relations that always hold among program variables at each program location, in all possible executions of the program
Main result

Theorem

There is an algorithm which computes, for any given affine program over $\mathbb{Q}$, its strongest polynomial inductive invariant.

- strongest polynomial invariant $\iff$ smallest algebraic set
  - algebraic sets $=$ finite $\bigcup$ and $\bigcap$ of polynomial equalities
- Thus our algorithm computes all polynomial relations that always hold among program variables at each program location, in all possible executions of the program
- We can represent this (usually infinite) set of relations using a finite basis of polynomial equalities
At the edge of decidability

Theorem (Markov 1947*)
There is a fixed set of $6 \times 6$ integer matrices $M_1, \ldots, M_k$ such that the reachability problem "$y$ is reachable from $x_0$?" is undecidable.

Theorem (Paterson 1970*)
The mortality problem "$0$ is reachable from $x_0$ with $M_1, \ldots, M_k$?" is undecidable for $3 \times 3$ matrices.

*Original theorems about semigroups, reformulated with affine programs.
At the edge of decidability

Theorem (Markov 1947*)

There is a **fixed set** of $6 \times 6$ integer matrices $M_1, \ldots, M_k$ such that the reachability problem “$y$ is reachable from $x_0$?” is **undecidable**.

*Original theorems about semigroups, reformulated with affine programs.
Theorem (Markov 1947*)

There is a fixed set of $6 \times 6$ integer matrices $M_1, \ldots, M_k$ such that the reachability problem “$y$ is reachable from $x_0$?” is undecidable.

Theorem (Paterson 1970*)

The mortality problem “$0$ is reachable from $x_0$ with $M_1, \ldots, M_k$?” is undecidable for $3 \times 3$ matrices.

*Original theorems about semigroups, reformulated with affine programs.
Theorem (Derksen, Jeandel and Koiran, 2004)
There is an algorithm which computes, for any given affine program over $\mathbb{Q}$ using only invertible transformations, its strongest polynomial inductive invariant.
Theorem (Derksen, Jeandel and Koiran, 2004)

There is an algorithm which computes, for any given affine program over \( \mathbb{Q} \) using only invertible transformations, its strongest polynomial inductive invariant.
Main contribution

Theorem

Given a finite set of rational square matrices of the same dimension, we can compute the Zariski closure of the semigroup that they generate.

Corollary

Given an affine program, we can compute for each location the ideal of all polynomial relations that hold at that location.
Summary

▶ invariant = overapproximation of reachable states
▶ invariants allow verification of safety properties
▶ affine program:
  ▶ nondeterministic branching, no guards, affine assignments

Theorem

There is an algorithm which computes, for any given affine program over \( \mathbb{Q} \), its strongest polynomial inductive invariant.
Introduction to Algebraic Geometry
(for computer scientists)

Amaury Pouly

Université de Paris, IRIF, CNRS
Overview of this tutorial

A very incomplete introduction to

- Polynomial ideals
- Affine varieties
- Zariski topology
- Constructible sets
- Regular maps

And algorithmic aspects of the above topics.

Everywhere $\mathbb{K}$ is a field, most of the time $\mathbb{K} = \mathbb{C}$. 
Motivating examples

Solutions to $x^2 + x = 1$?

$S = \left\{ -\frac{1}{2} + \frac{1}{2} \sqrt{5}, -\frac{1}{2} - \frac{1}{2} \sqrt{5} \right\}$
Motivating examples

Solutions to $x^3 + x = 1$?

$S = \left\{ \frac{1}{6} \sqrt[3]{108} + 12\sqrt[3]{93} - \frac{2}{\sqrt[3]{108} + 12\sqrt[3]{93}} \right\}$
Motivating examples

Solutions to $x^4 + x = 1$?

- 2 isolated real roots
- we can approximate them
- algebraic numbers: arithmetic and comparisons are decidable

$S = \{\text{no formula}\}$
Motivating examples

Solutions to $xy = 1$?

$S = \{(x, \frac{1}{x}) : x \neq 0\}$

Although we have a formula, the geometry is more interesting.
Motivating examples

Solutions to \((x - 1)^2 + (y - 1)^2)(x^4 + x - 1) = 0\)?

\[ S = \{ \text{no formula} \} \]

No formula in general, but geometry:

- one isolated point
- two infinite curves

Algebraic Geometry is about manipulating those objects, 

without having explicit solutions.
What is Algebraic Geometry?

Study systems of multivariate polynomial equations using abstract algebraic techniques, with applications to geometry.

Examples

\[ x^2 + y^2 + z^2 - 1 = 0 \quad \sim \quad \text{sphere in } \mathbb{R}^3 \]
What is Algebraic Geometry?

Study **systems of multivariate polynomial equations** using abstract algebraic techniques, with applications to geometry.

**Examples**

\[
x^2 + y^2 + z^2 - 1 = 0 \quad \sim \quad \text{sphere in } \mathbb{R}^3
\]

\[
x^2 + y^2 + z^2 = 1 \land x + y + z = 1 \quad \sim \quad \text{“sliced” sphere in } \mathbb{R}^3
\]
What is Algebraic Geometry?

Study systems of multivariate polynomial equations using abstract algebraic techniques, with applications to geometry.

Examples

\[ x^2 + y^2 + z^2 - 1 = 0 \, \sim \, \text{sphere in } \mathbb{R}^3 \]
\[ x^2 + y^2 + z^2 = 1 \, \land \, x + y + z = 1 \, \sim \, \text{“sliced” sphere in } \mathbb{R}^3 \]
\[ x^2 + 1 = 0 \, \sim \, \emptyset \text{ in } \mathbb{R} \]
What is Algebraic Geometry?

Study systems of multivariate polynomial equations using abstract algebraic techniques, with applications to geometry.

Examples

\[
\begin{align*}
  x^2 + y^2 + z^2 - 1 &= 0 & \mapsto & \text{sphere in } \mathbb{R}^3 \\
  x^2 + y^2 + z^2 = 1 & \land x + y + z = 1 & \mapsto & \text{“sliced” sphere in } \mathbb{R}^3 \\
  x^2 + 1 &= 0 & \mapsto & \emptyset \text{ in } \mathbb{R} \\
  x^2 + 1 &= 0 & \mapsto & \{i, -i\} \text{ in } \mathbb{C}
\end{align*}
\]
What is Algebraic Geometry?

Study systems of multivariate polynomial equations using abstract algebraic techniques, with applications to geometry.

Examples

\[ x^2 + y^2 + z^2 - 1 = 0 \quad \sim \quad \text{sphere in } \mathbb{R}^3 \]
\[ x^2 + y^2 + z^2 = 1 \land x + y + z = 1 \quad \sim \quad \text{“sliced” sphere in } \mathbb{R}^3 \]
\[ x^2 + 1 = 0 \quad \sim \quad \emptyset \text{ in } \mathbb{R} \]
\[ x^2 + 1 = 0 \quad \sim \quad \{i, -i\} \text{ in } \mathbb{C} \]

The field \( \mathbb{K} \) is very important:

- real algebraic geometry: more “intuitive” but more difficult, really requires the study of semi-algebraic sets
- mainstream algebraic geometry: \( \mathbb{K} \) is algebraically closed\(^\dagger\), e.g. \( \mathbb{C} \)

\(^\dagger\mathbb{K} \) is algebraically closed if every non-constant polynomial has a root in \( \mathbb{K} \).
Polynomial ideals

A set of polynomials \( I \subseteq \mathbb{K}[x_1, \ldots, x_n] \) is an ideal if

- \( \forall f, g \in I \cdot f + g \in I \)
- \( \forall f \in I \cdot \forall g \in \mathbb{K}[x_1, \ldots, x_n] : fg, gf \in I \)

- \( I \) is stable under addition
- \( I \) absorbs multiplication
Polynomial ideals

A set of polynomials $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is an ideal if

- $\forall f, g \in I. f + g \in I$  \hspace{1cm} $\Rightarrow$ $I$ is stable under addition
- $\forall f \in I. \forall g \in \mathbb{K}[x_1, \ldots, x_n] : fg, gf \in I$  \hspace{1cm} $\Rightarrow$ $I$ absorbs multiplication

Example: $I = \{ p \in \mathbb{K}[x] : p(1) = 0 \}$

- if $f(1) = g(1) = 0$ then $(f + g)(1) = f(1) + g(1) = 0$
- if $f(1) = 0$ then for any $g \in \mathbb{K}[x]$, $(fg)(1) = f(1)g(1) = 0$
Polynomial ideals

A set of polynomials \( I \subseteq \mathbb{K}[x_1, \ldots, x_n] \) is an ideal if

\[ \forall f, g \in I. f + g \in I \quad \text{\( I \) is stable under addition} \]
\[ \forall f \in I. \forall g \in \mathbb{K}[x_1, \ldots, x_n] : fg, gf \in I \quad \text{\( I \) absorbs multiplication} \]

Two main ways to create ideals:

\[ \text{The vanishing polynomials on } S \subseteq \mathbb{K}^n \text{ is an ideal:} \]
\[ I(S) := \{ f \in \mathbb{K}[x_1, \ldots, x_n] : \forall x \in S. f(x) = 0 \} \]

Remark: \( I \) is inclusion reversing, \( S \subseteq S' \Rightarrow I(S) \supseteq I(S') \)
Polynomial ideals

A set of polynomials $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is an ideal if

- $\forall f, g \in I. f + g \in I$  \quad \text{\textit{\small{$\Rightarrow$}} I is stable under addition}
- $\forall f \in I. \forall g \in \mathbb{K}[x_1, \ldots, x_n] : fg, gf \in I$  \quad \text{\textit{\small{$\Rightarrow$}} I absorbs multiplication}

Two main ways to create ideals:

- The vanishing polynomials on $S \subseteq \mathbb{K}^n$ is an ideal:

  $$I(S) := \{ f \in \mathbb{K}[x_1, \ldots, x_n] : \forall x \in S. f(x) = 0 \}$$

  
  \textbf{Remark:} $I$ is inclusion reversing, $S \subseteq S' \Rightarrow I(S) \supseteq I(S')$

- The ideal generated by $f_1, \ldots, f_k \in \mathbb{K}[x_1, \ldots, x_n]$ is

  $$\langle f_1, \ldots, f_k \rangle := \text{smallest ideal containing } f_1, \ldots, f_k$$
  
  $$:= \{ p_1 f_1 + \cdots + p_k f_k : p_1, \ldots, p_k \in \mathbb{K}[x_1, \ldots, x_n] \}$$
Polynomial ideals

A set of polynomials \( I \subseteq \mathbb{K}[x_1, \ldots, x_n] \) is an ideal if

\begin{itemize}
  \item \( \forall f, g \in I. f + g \in I \) \quad \text{▶} \quad l \text{ is stable under addition}
  \item \( \forall f \in I. \forall g \in \mathbb{K}[x_1, \ldots, x_n] : fg, gf \in I \) \quad \text{▶} \quad l \text{ absorbs multiplication}
\end{itemize}

Two main ways to create ideals:

\begin{itemize}
  \item The vanishing polynomials on \( S \subseteq \mathbb{K}^n \) is an ideal:
    \[ l(S) := \{ f \in \mathbb{K}[x_1, \ldots, x_n] : \forall x \in S. f(x) = 0 \} \]
    \textbf{Remark:} \( l \) is inclusion reversing, \( S \subseteq S' \Rightarrow l(S) \supseteq l(S') \)
  \item The ideal generated by \( f_1, \ldots, f_k \in \mathbb{K}[x_1, \ldots, x_n] \) is
    \[ \langle f_1, \ldots, f_k \rangle := \text{smallest ideal containing } f_1, \ldots, f_k \]
    \[ := \{ p_1 f_1 + \cdots + p_k f_k : p_1, \ldots, p_k \in \mathbb{K}[x_1, \ldots, x_n] \} \]
\end{itemize}

Example: \( \{ p \in \mathbb{K}[x] : p(1) = 0 \} = l(\{1\}) = \langle x - 1 \rangle. \)
Polynomial ideals: important facts

A set of polynomials \( I \subseteq \mathbb{K}[x_1, \ldots, x_n] \) is an ideal if

- \( \forall f, g \in I : f + g \in I \)  \( \rightarrow \) \( I \) is stable under addition
- \( \forall f \in I, \forall g \in \mathbb{K}[x_1, \ldots, x_n] : fg, gf \in I \)  \( \rightarrow \) \( I \) absorbs multiplication

Theorem (Hilbert’s basis theorem)

For any field \( \mathbb{K} \), \( \mathbb{K}[x_1, \ldots, x_n] \) is Noetherian: any chain of ideals

\[ I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \]

eventually stabilizes: \( \exists k \in \mathbb{N} \) such that \( I_k = I_{k+1} = I_{k+2} = \cdots \).
Polynomial ideals: important facts

A set of polynomials $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is an ideal if

- $\forall f, g \in I : f + g \in I$
- $\forall f \in I, \forall g \in \mathbb{K}[x_1, \ldots, x_n] : fg, gf \in I$

$\Rightarrow I$ is stable under addition
$\Rightarrow I$ absorbs multiplication

Theorem (Hilbert’s basis theorem)

For any field $\mathbb{K}$, $\mathbb{K}[x_1, \ldots, x_n]$ is Noetherian: any chain of ideals

$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$

eventually stabilizes: $\exists k \in \mathbb{N}$ such that $I_k = I_{k+1} = I_{k+2} = \cdots$

Corollary

Every polynomial ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is finitely generated:

$\exists f_1, \ldots, f_k \in \mathbb{K}[x_1, \ldots, x_n]$ such that $I = \langle f_1, \ldots, f_k \rangle$.

We can represent ideals by a finite set of generators.
A set of polynomials $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is an ideal if

- $\forall f, g \in I. f + g \in I$ — $I$ is stable under addition
- $\forall f \in I, \forall g \in \mathbb{K}[x_1, \ldots, x_n]. fg, gf \in I$ — $I$ absorbs multiplication

Once we have some ideals, we can build new ones from them by

- Addition: $I + J := \{f + g : f \in I, g \in J\}$
- Intersection: $I \cap J$
- Multiplication: $IJ := \langle fg : f \in I, g \in J \rangle$
- Quotient: $(I:J) := \{r : rJ \subseteq I\}$

Remark: $I \cup J$ is not an ideal but $I + J = \langle I \cup J \rangle$

All these operations are effective.
Polynomial ideals: important operations

A set of polynomials $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is an ideal if

- $\forall f, g \in I. f + g \in I$  $\Rightarrow$ $I$ is stable under addition
- $\forall f \in I, \forall g \in \mathbb{K}[x_1, \ldots, x_n] : fg, gf \in I$  $\Rightarrow$ $I$ absorbs multiplication

Once we have some ideals, we can build new ones from them by

- addition: $I + J := \{ f + g : f \in I, g \in J \}$

Remark: $I \cup J$ is not an ideal but $I + J = \langle I \cup J \rangle$.

All these operations are effective.
Polynomial ideals: important operations

A set of polynomials $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is an ideal if

- $\forall f, g \in I. f + g \in I$  
  $\Rightarrow$ $I$ is stable under addition

- $\forall f \in I, \forall g \in \mathbb{K}[x_1, \ldots, x_n] : fg, gf \in I$  
  $\Rightarrow$ $I$ absorbs multiplication

Once we have some ideals, we can build new ones from them by

- addition: $I + J := \{ f + g : f \in I, g \in J \}$

- intersection: $I \cap J$
Polynomial ideals: important operations

A set of polynomials $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is an ideal if

- $\forall f, g \in I. f + g \in I$  $\Rightarrow$ $I$ is stable under addition
- $\forall f \in I, \forall g \in \mathbb{K}[x_1, \ldots, x_n] : fg, gf \in I$  $\Rightarrow$ $I$ absorbs multiplication

Once we have some ideals, we can build new ones from them by

- addition: $I + J := \{f + g : f \in I, g \in J\}$
- intersection: $I \cap J$
- multiplication: $IJ := \langle fg : f \in I, g \in J \rangle$
A set of polynomials \( I \subseteq \mathbb{K}[x_1, \ldots, x_n] \) is an **ideal** if

- \( \forall f, g \in I. f + g \in I \)  
- \( \forall f \in I, \forall g \in \mathbb{K}[x_1, \ldots, x_n] : fg, gf \in I \)

Once we have some ideals, we can build new ones from them by

- **addition**: \( I + J := \{ f + g : f \in I, g \in J \} \)
- **intersection**: \( I \cap J \)
- **multiplication**: \( IJ := \langle fg : f \in I, g \in J \rangle \)
- **quotient**: \( (I : J) := \{ r : rJ \subseteq I \} \)

Remark: \( I \cup J \) is not an ideal but \( I + J = \langle I \cup J \rangle \)

All these operations are effective.
Polynomial ideals: important operations

A set of polynomials \( I \subseteq \mathbb{K}[x_1, \ldots, x_n] \) is an ideal if

- \( \forall f, g \in I. f + g \in I \) \( \quad \Rightarrow \) \( I \) is stable under addition
- \( \forall f \in I, \forall g \in \mathbb{K}[x_1, \ldots, x_n] : fg, gf \in I \) \( \quad \Rightarrow \) \( I \) absorbs multiplication

Once we have some ideals, we can build new ones from them by

- addition: \( I + J := \{ f + g : f \in I, g \in J \} \)
- intersection: \( I \cap J \)
- multiplication: \( IJ := \langle fg : f \in I, g \in J \rangle \)
- quotient: \( (I : J) := \{ r : rJ \subseteq I \} \)

Remark: \( I \cup J \) is not an ideal but \( I + J = \langle I \cup J \rangle \)

All these operations are effective.
Algebraic sets

**Algebraic set**: set of the common zeroes of polynomials

\[
V(S) = \{ x \in \mathbb{K}^n : \forall p \in S. p(x) = 0 \} \text{ where } S \subseteq \mathbb{K}[x_1, \ldots, x_n]
\]
Algebraic sets

**Algebraic set**: set of the common zeroes of polynomials

\[ V(S) = \{ x \in \mathbb{K}^n : \forall p \in S. p(x) = 0 \} \text{ where } S \subseteq \mathbb{K}[x_1, \ldots, x_n] \]

**Examples**

- \{ (x, y) \in \mathbb{K}^2 : y = x^2 \} 
- \{ (x, y, z) \in \mathbb{K}^3 : x = y^2 \land y = z \} 
- \mathbb{K}^n = \{ x \in \mathbb{K}^n : 0 = 0 \} 
- \emptyset = \{ x \in \mathbb{K}^n : 1 = 0 \} 
- \{ a \} = \{ x : x_1 - a_1 = \ldots = x_n - a_n = 0 \}
Algebraic sets

**Algebraic set**: set of the common zeroes of polynomials

\[ V(S) = \{ x \in \mathbb{K}^n : \forall p \in S. p(x) = 0 \} \text{ where } S \subseteq \mathbb{K}[x_1, \ldots, x_n] \]

**Examples**

- \((x, y) \in \mathbb{K}^2 : y = x^2\)
- \((x, y, z) \in \mathbb{K}^3 : x = y^2 \land y = z\)
- \(\mathbb{K}^n = \{ x \in \mathbb{K}^n : 0 = 0 \}\)
- \(\emptyset = \{ x \in \mathbb{K}^n : 1 = 0 \}\)
- \(\{ a \} = \{ x : x_1 - a_1 = \ldots = x_n - a_n = 0 \}\)

For arbitrary \(S\), \(V(S) = V(I)\) where \(I = \langle S \rangle\) is the ideal generated by \(S\).

\(\sim\) Always take \(S\) to be an ideal, this gives us a finite representation of algebraic sets.
Algebraic set: set of the common zeroes of an ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$

$V(I) = \{x \in \mathbb{K}^n : \forall p \in I. p(x) = 0\}$
Algebraic sets / Zariski topology

**Algebraic set**: set of the common zeroes of an ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$

$$V(I) = \{ x \in \mathbb{K}^n : \forall p \in I. p(x) = 0 \}$$

**Basic properties:**

- stable under **finite** unions: $V(I) \cup V(J) = V(I \cap J) = V(IJ)$
- stable under **arbitrary** intersections: $\cap_i V(I_i) = V(\cup_i I_i) = V(\sum_i I_i)$
Algebraic sets / Zariski topology

**Algebraic set**: set of the common zeroes of an ideal \( I \subseteq \mathbb{K}[x_1, \ldots, x_n] \)

\[
V(I) = \{ x \in \mathbb{K}^n : \forall p \in I. p(x) = 0 \}
\]

**Basic properties:**

- stable under **finite** unions: \( V(I) \cup V(J) = V(I \cap J) = V(IJ) \)
- stable under **arbitrary** intersections: \( \bigcap_i V(I_i) = V(\bigcup_i I_i) = V(\sum_i I_i) \)

**Zariski topology**: the closed set are the algebraic sets

**Examples**

- \( \{(x, y) \in \mathbb{K}^2 : y = x^2\} = V(y - x^2) \) is **closed**
- \( \{(x, y) \in \mathbb{K}^2 : y \neq x^2\} = \mathbb{K}^2 \setminus V(y - x^2) \) is **open**
Irreducible sets

**Algebraic set**: set of the common zeroes of an ideal \( I \subseteq \mathbb{K}[x_1, \ldots, x_n] \)

\[
V(I) = \{ x \in \mathbb{K}^n : \forall p \in I. p(x) = 0 \}
\]

**Zariski topology**: the closed set are the algebraic sets

Examples

- \( \{(x, y) : y = x^2\} \) is irreducible
- \( \{(x, y) : xy = 0\} \) is reducible: \( \{(x, y) : x = 0\} \cup \{(x, y) : y = 0\} \)
Irreducible sets

Algebraic set: set of the common zeroes of an ideal \( I \subseteq \mathbb{K}[x_1, \ldots, x_n] \)

\[
V(I) = \{ x \in \mathbb{K}^n : \forall p \in I. p(x) = 0 \}
\]

Zariski topology: the closed set are the algebraic sets

\( Y \subseteq \mathbb{K}^n \) is irreducible if it is not the union of two proper closed subsets.

Examples

- \( \{(x, y) : y = x^2\} \) is irreducible
- \( \{(x, y) : xy = 0\} \) is reducible: \( \{(x, y) : x = 0\} \cup \{(x, y) : y = 0\} \)

![Graph of y = x^2 and x = 0](image-url)
Irreducible sets

**Algebraic set**: set of the common zeroes of an ideal $I \subseteq K[x_1, \ldots, x_n]$

$$V(I) = \{ x \in K^n : \forall p \in I. p(x) = 0 \}$$

**Zariski topology**: the closed set are the algebraic sets

$Y \subseteq K^n$ is irreducible if it is not the union of two proper closed subsets.

**Examples**

- $\{(x, y) : y = x^2\}$ is irreducible
- $\{(x, y) : xy = 0\}$ is reducible: $\{(x, y) : x = 0\} \cup \{(x, y) : y = 0\}$

**Theorem**

Any algebraic set can be written as the **finite** union of irreducible algebraic sets.
Ascending/Descending chains

Polynomial ideals satisfy the **ascending chain condition (ACC)**: there is no infinite chain of strictly increasing ideals

\[ I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_k \subsetneq \cdots \]

Remark: the last fact comes from the notion of dimension of an algebraic set. It is geometrically "what one would expect": a curve has dimension 1, a hypersurface $n-1$, the whole space $n$. 
Ascending/Descending chains

Polynomial ideals satisfy the **ascending chain condition (ACC)**: there is no infinite chain of strictly increasing ideals

\[ I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_k \subsetneq \cdots \]

Algebraic sets satisfy the **descending chain condition (DCC)**: there is no infinite chain of strictly decreasing algebraic sets

\[ V_1 \supsetneq V_2 \supsetneq \cdots \supsetneq V_k \supsetneq \cdots \]

Remark: the last fact comes from the notion of dimension of an algebraic set. It is geometrically “what one would expect”: a curve has dimension 1, a hypersurface \( n-1 \), the whole space \( n \).
Ascending/Descending chains

Polynomial ideals satisfy the ascending chain condition (ACC): there is no infinite chain of strictly increasing ideals

\[ I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_k \subsetneq \cdots \]

Algebraic sets satisfy the descending chain condition (DCC): there is no infinite chain of strictly decreasing algebraic sets

\[ V_1 \supsetneq V_2 \supsetneq \cdots \supsetneq V_k \supsetneq \cdots \]

Irreducible algebraic sets satisfy the ACC: there is no infinite chain of strictly increasing irreducible algebraic sets:

\[ V_1 \subsetneq V_2 \subsetneq \cdots \subsetneq V_k \subsetneq \cdots \]
Ascending/Descending chains

Polynomial ideals satisfy the ascending chain condition (ACC): there is no infinite chain of strictly increasing ideals

\[ I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_k \subsetneq \cdots \]

Algebraic sets satisfy the descending chain condition (DCC): there is no infinite chain of strictly decreasing algebraic sets

\[ V_1 \supsetneq V_2 \supsetneq \cdots \supsetneq V_k \supsetneq \cdots \]

Irreducible algebraic sets satisfy the ACC: there is no infinite chain of strictly increasing irreducible algebraic sets:

\[ V_1 \subsetneq V_2 \subsetneq \cdots \subsetneq V_k \subsetneq \cdots \]

Remark: the last fact comes from the notion of dimension of an algebraic set. It is geometrically “what one would expect”: a curve has dimension 1, a hypersurface \( n - 1 \), the whole space \( n \).
Affine varieties

**Algebraic set:** set of the common zeroes of an ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$

$$V(I) = \{x \in \mathbb{K}^n : \forall p \in I. p(x) = 0\}$$

**Zariski topology:** the closed set are the algebraic sets
Affine varieties

**Algebraic set:** set of the common zeroes of an ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$

$$V(I) = \{ x \in \mathbb{K}^n : \forall p \in I. p(x) = 0 \}$$

**Zariski topology:** the closed set are the algebraic sets

$Y \subseteq \mathbb{K}^n$ is **irreducible** if it is not the union of two proper closed subsets.
Affine varieties

**Algebraic set**: set of the common zeroes of an ideal \( I \subseteq \mathbb{K}[x_1, \ldots, x_n] \)

\[
V(I) = \{ x \in \mathbb{K}^n : \forall p \in I. p(x) = 0 \}
\]

**Zariski topology**: the closed set are the algebraic sets

\( Y \subseteq \mathbb{K}^n \) is **irreducible** if it is not the union of two proper closed subsets.

⚠️ The term **affine variety** is ambiguous, it can mean

- algebraic set
- irreducible algebraic set

---

In this lecture

affine variety = algebraic set
Let $X \subseteq \mathbb{K}^n$ be a variety. The Zariski topology on $X$ has as closed sets the subvarieties of $X$: the sets $A \subseteq X$ that are varieties in $\mathbb{K}^n$.

Examples

- $X = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}$ is closed in $\mathbb{R}^3$
- $S = X \cap \{(x, y, z) \in \mathbb{R}^3 : x + y + z = 1\}$ is closed in $X$
Let $X \subseteq K^n$ be a variety. The Zariski topology on $X$ has as closed sets the subvarieties of $X$: the sets $A \subseteq X$ that are varieties in $K^n$.

Examples

- $X = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}$ is closed in $\mathbb{R}^3$
- $S = X \cap \{(x, y, z) \in \mathbb{R}^3 : x + y + z = 1\}$ is closed in $X$

Given a set $S \subseteq X$, its Zariski closure $\overline{S}^X$ (or just $\overline{S}$) is the closure in the above topology: the smallest closed set containing $S$. 
Let $X \subseteq \mathbb{K}^n$ be a variety. The Zariski topology on $X$ has as closed sets the subvarieties of $X$: the sets $A \subseteq X$ that are varieties in $\mathbb{K}^n$.

Examples

- $X = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}$ is closed in $\mathbb{R}^3$
- $S = X \cap \{(x, y, z) \in \mathbb{R}^3 : x + y + z = 1\}$ is closed in $X$

Given a set $S \subseteq X$, its Zariski closure $\overline{S}^X$ (or just $\overline{S}$) is the closure in the above topology: the smallest closed set containing $S$.

Examples

- $[-1, 1]^{\mathbb{R}} = \mathbb{R}$
- $\overline{\mathbb{N}}^{\mathbb{R}} = \mathbb{R}$
- $\left\{(x, y) \in \mathbb{R}^2 : x \geq 0 \land x = y^2\right\}^{\mathbb{R}} = \left\{(x, y) \in \mathbb{R}^2 : x = y^2\right\}$
A quick summary of what we have seen so far

- **Ideal**: set of polynomials, stable under $+$, absorbing $\times$
- **Algebraic set**: common zeroes of a set of polynomials/ideal
- **Irreducible set**: not the union of two proper algebraic subsets
- **Affine variety**: (irreducible) algebraic set (author dependent)
- **Zariski topology**: the closed sets are the algebraic sets
- **Zariski closure**: $\overline{S} =$ smallest closed set containing $X$
- **Effective operations**: union and intersection of closed sets
Quantifier Elimination (QE): $\mathbb{R}$ vs $\mathbb{C}$

Let $S = \{(x, y) \in \mathbb{K}^2 : x^2 + y^2 = 1\}$. 

Two very different behaviors:
- For $\mathbb{K} = \mathbb{R}$:
  $S' = [-1, 1] = \{x \in \mathbb{R} : x^2 \leq 1\}$
- For $\mathbb{K} = \mathbb{C}$:
  $S' = \mathbb{C}$

In $\mathbb{R}$ we need to introduce inequalities.
Quantifier Elimination (QE): $\mathbb{R}$ vs $\mathbb{C}$

Let $S = \{(x, y) \in \mathbb{K}^2 : x^2 + y^2 = 1 \}$.  

Projection of $S$ on $x$:  
$S' = \{ x \in \mathbb{K} : \exists y : (x, y) \in S \}$
Quantifier Elimination (QE): $\mathbb{R}$ vs $\mathbb{C}$

Let $S = \{(x, y) \in \mathbb{K}^2 : x^2 + y^2 = 1\}$.

Projection of $S$ on $x$:
$S' = \{x \in \mathbb{K} : \exists y : (x, y) \in S\}$

Two very different behaviors:

- For $\mathbb{K} = \mathbb{R}$:
  
  $S' = [-1, 1] = \{x \in \mathbb{R} : x^2 \leq 1\}$

- For $\mathbb{K} = \mathbb{C}$:
  
  $S' = \mathbb{C}$

In $\mathbb{R}$ we need to introduce inequalities.
Quantifier Elimination (QE): $\mathbb{R}$ vs $\mathbb{C}$

Let $S = \{(x, y) \in \mathbb{K}^2 : x^2 + y^2 = 1\}$.

Projection of $S$ on $x$:
$S' = \{x \in \mathbb{K} : \exists y : (x, y) \in S\}$

Two very different behaviors:

- For $\mathbb{K} = \mathbb{R}$:
  $S' = [-1, 1] = \{x \in \mathbb{R} : x^2 \leq 1\}$

- For $\mathbb{K} = \mathbb{C}$:
  $S' = \mathbb{C}$

In $\mathbb{R}$ we need to introduce inequalities.

Theorem (QE over $\mathbb{R}$)
$(\mathbb{R}, +, \times, 0, 1, \leq) \text{ admits QE.}$

Theorem (QE over $\mathbb{C}$)
$(\mathbb{C}, +, \times, 0, 1, =) \text{ admits QE.}$
Definable/Constructible sets: motivation

\[ S = \{(x, y) \in \mathbb{R}^2 : xy = 1\} \]

variety/closed set
Definable/Constructible sets: motivation

\[ S = \{(x, y) \in \mathbb{R}^2 : xy = 1\} \]

variety/closed set

\[ p(x, y) = x \]

“nice” function (polynomial)

We need something more general than varieties: the above sets are definable:

\[ \{x \in K^n : \phi(x)\} \]

constructible: intersections/unions of open/closed sets
Definable/Constructible sets: motivation

\[ S = \{ (x, y) \in \mathbb{R}^2 : xy = 1 \} \]

variety/closed set

\[ p(x, y) = x \]

“nice” function (polynomial)

\[ S' = p(S) = \{ x : x \neq 0 \} = \mathbb{R} \setminus \{0\} \]

open subset of \( \mathbb{R} \)
Definable/Constructible sets: motivation

$S = \{(x, y) \in \mathbb{R}^2 : xy = 1\}$

variety/closed set

$p(x, y) = x$

“nice” function (polynomial)

$S' = p(S) = \{x : x \neq 0\} = \mathbb{R} \setminus \{0\}$

open subset of $\mathbb{R}$

$q(x, y) = (x, xy)$

“nice” function (polynomial)
Definable/Constructible sets: motivation

$S = \{(x, y) \in \mathbb{R}^2 : xy = 1\}$

variety/closed set

$p(x, y) = x$

“nice” function (polynomial)

$S' = p(S) = \{x : x \neq 0\} = \mathbb{R} \setminus \{0\}$

open subset of $\mathbb{R}$

$q(x, y) = (x, xy)$

“nice” function (polynomial)

$S'' = q(S) = \{(x, 1) : x \neq 0\}$

not open, not closed in $\mathbb{R}^2$
Definable/Constructible sets: motivation

\[ S = \{(x, y) \in \mathbb{R}^2 : xy = 1\} \]

- variety/closed set

\[ p(x, y) = x \]

- “nice” function (polynomial)

\[ S' = p(S) = \{x : x \neq 0\} = \mathbb{R} \setminus \{0\} \]

- open subset of \( \mathbb{R} \)

\[ q(x, y) = (x, xy) \]

- “nice” function (polynomial)

\[ S'' = q(S) = \{(x, 1) : x \neq 0\} \]

- not open, not closed in \( \mathbb{R}^2 \)

We need something more general than varieties: the above sets are

- definable: \( \{x \in \mathbb{K}^n : \phi(x)\} \)

- constructible: intersections/unions of open/closed sets
A set $S$ is **definable** if $S = \{ x \in \mathbb{K}^n : \phi(x) \}$ for $\phi$ first-order formula\(^\dagger\).

**Examples**

- any variety: $\phi(x) \equiv \bigwedge_i p_i(x) = 0$
- any open set: $\phi(x) \equiv \neg \bigwedge_i p_i(x) = 0$
- $S = \{ (x, y) : y = 1 \land x \neq 0 \}$
- $S = \{ x : \exists y. xy = 1 \}$

\(^\dagger\)On the signature $(\mathbb{K}, +, \times, 0, 1, =)$: we have $\exists, \forall, \neg$ and equality of polynomials.
Constructible/Definable sets

A set $S$ is **definable** if $S = \{ x \in \mathbb{K}^n : \phi(x) \}$ for $\phi$ first-order formula\(^\ddagger\).

**Examples**

- any variety: $\phi(x) \equiv \bigwedge_i p_i(x) = 0$
- any open set: $\phi(x) \equiv \neg \bigwedge_i p_i(x) = 0$
- $S = \{(x, y) : y = 1 \land x \neq 0\}$
- $S = \{x : \exists y. xy = 1\}$

The **constructible sets** are all Boolean combinations (including complementation) of Zariski closed sets.

**Examples**

- any closed or open set
- $S = \{(x, 1) : x \neq 0\} = \{(x, y) : y = 1\} \cap \{(x, y) : x = 0\}^\complement$
- $S = \{(x, y) : x = 0\}^\complement \cup \{(0, 0)\}$

\(^\ddagger\)On the signature $(\mathbb{K}, +, \times, 0, 1, =)$: we have $\exists, \forall, \neg$ and equality of polynomials.
A set $S$ is **definable** if $S = \{ x \in \mathbb{K}^n : \phi(x) \}$ for $\phi$ first-order formula.

The **constructible sets** are all Boolean combinations (including complementation) of Zariski closed sets.

**Theorem (Consequence of quantifier elimination)**

*For $\mathbb{K} = \mathbb{C}$, the constructible sets are exactly the definable sets.*
A set \( S \) is **definable** if \( S = \{ x \in \mathbb{K}^n : \phi(x) \} \) for \( \phi \) first-order formula.

The **constructible sets** are all Boolean combinations (including complementation) of Zariski closed sets.

**Theorem (Consequence of quantifier elimination)**

*For \( \mathbb{K} = \mathbb{C} \), the constructible sets are exactly the definable sets.*

**In this lecture**

We use **constructible sets** over \( \mathbb{C} \) everywhere.
Constructible/Definable sets (continued)

A set $S$ is **definable** if $S = \{x \in \mathbb{K}^n : \phi(x)\}$ for $\phi$ first-order formula.

The **constructible sets** are all Boolean combinations (including complementation) of Zariski closed sets.

**Theorem (Consequence of quantifier elimination)**

*For $\mathbb{K} = \mathbb{C}$, the constructible sets are exactly the definable sets.*

**In this lecture**

We use constructible sets over $\mathbb{C}$ everywhere.

**Theorem (Chevalley)**

*The image of a constructible set under a polynomial map is constructible.*

(also follows from quantifier elimination)
Algorithmic aspects of constructible sets

The **constructible sets** are all Boolean combinations (including complementation) of Zariski closed sets. ~> **effective representation**
Algorithmic aspects of constructible sets

The **constructible sets** are all Boolean combinations (including complementation) of Zariski closed sets. \(\leadsto\) **effective representation**

Effective operations:

- union, intersection, complementation (trivial)
Algorithmic aspects of constructible sets

The constructible sets are all Boolean combinations (including complementation) of Zariski closed sets. \( \rightsquigarrow \) effective representation

Effective operations:

- union, intersection, complementation (trivial)
- any first-order definition (by quantifier elimination)
  
  **Example:** \( \{ x \in \mathbb{C} : \exists y \in \mathbb{C}. (x, y) \in S \} \) where \( S \) constructible
The **constructible sets** are all Boolean combinations (including complementation) of Zariski closed sets. **Effective representation**

**Effective operations:**
- union, intersection, complementation (trivial)
- any first-order definition (by quantifier elimination)
  - Example: \( \{ x \in \mathbb{C} : \exists y \in \mathbb{C}. (x, y) \in S \} \) where \( S \) constructible
- image under a polynomial map
  - Example: \( p(S) \) where \( S \) constructible and \( p(x, y) = x \)

\[\textit{§Important special case of first-order definition. The two examples are the same.}\]
The **constructible sets** are all Boolean combinations (including complementation) of Zariski closed sets. \(\sim\) **effective representation**

Effective operations:

- union, intersection, complementation (trivial)
- any first-order definition (by quantifier elimination)
  
  **Example:** \(\{x \in \mathbb{C} : \exists y \in \mathbb{C}. (x, y) \in S\}\) where \(S\) constructible

- image under a polynomial map§
  
  **Example:** \(p(S)\) where \(S\) constructible and \(p(x, y) = x\)

- Zariski closure: \(\overline{S}\) where \(S\) constructible
  
  **Common use:** \(\overline{p(S)}\) where \(S\) constructible and \(p\) polynomial

---

§Important special case of first-order definition. The two examples are the same.
The constructible sets are all Boolean combinations (including complementation) of Zariski closed sets.

**Lemma**

If $X$ is constructible then $\exists A_1, \ldots, A_k$ irreducible and $B_1, \ldots, B_k$ closed,

$$X = \bigcup_{i=1}^{k} A_i \setminus B_i$$
Constructible sets: decomposition and application

The **constructible sets** are all Boolean combinations (including complementation) of Zariski closed sets.

**Lemma**

*If* $X$ *is constructible then* $\exists A_1, \ldots, A_k$ *irreducible and* $B_1, \ldots, B_k$ *closed, then*

$$X = \bigcup_{i=1}^{k} A_i \setminus B_i$$

**Exercice:** if $A$ *irreducible, B closed and* $A \setminus B \neq \emptyset$ *then* $\overline{A \setminus B} = A$

$A = (A \setminus B) \cup (A \cap B) \leadsto A = \overline{A \setminus B} \cup (A \cap B)$ *then use irreducibility*
Constructible sets: decomposition and application

The constructible sets are all Boolean combinations (including complementation) of Zariski closed sets.

**Lemma**

If $X$ is constructible then $\exists A_1, \ldots, A_k$ irreducible and $B_1, \ldots, B_k$ closed,

$$X = \bigcup_{i=1}^{k} A_i \setminus B_i$$

**Exercice:** if $A$ irreducible, $B$ closed and $A \setminus B \neq \emptyset$ then $\overline{A \setminus B} = A$

$$A = (A \setminus B) \cup (A \cap B) \implies A = \overline{A \setminus B} \cup (A \cap B)$$

then use irreducibility

**Application:** Zariski closure of a constructible set $X$

$$\overline{X} = \bigcup_{i=1}^{k} A_i \setminus B_i = \bigcup_{i=1}^{k} \overline{A_i \setminus B_i} = \bigcup_{i=1}^{k} \overline{A_i}$$

assuming $A_i \setminus B_i \neq \emptyset$
Summary

- **ideal**: set of polynomials, stable under $+$, absorbing $\times$
- **algebraic set**: common zeroes of a set of polynomials/ideal
- **irreducible set**: not the union of two proper algebraic subsets
- **affine variety**: (irreducible) algebraic set (author dependent)
- **Zariski topology**: the closed sets are the algebraic sets
- **Zariski closure**: $\overline{S} =$ smallest closed set containing $X$
- **effective operations**: union and intersection of closed sets
Summary

- **ideal**: set of polynomials, stable under $+$, absorbing $\times$
- **algebraic set**: common zeroes of a set of polynomials/ideal
- **irreducible set**: not the union of two proper algebraic subsets
- **affine variety**: (irreducible) algebraic set (author dependent)
- **Zariski topology**: the closed sets are the algebraic sets
- **Zariski closure**: $\overline{S}$ = smallest closed set containing $X$
- **effective operations**: union and intersection of closed sets

- **constructible set**: Boolean combinations of closed sets
- **definable set**: first-order definable with equality
- **effective operations**: union, intersection, complementation, first-order definition, image under polynomial map, Zariski closure