Satisfiability Checking

Gröbner Bases

Prof. Dr. Erika Ábrahám

RWTH Aachen University
Informatik 2
LuFG Theory of Hybrid Systems

WS 19/20

Motivation

For simplicity, we restrict to equations.

$$p_1(x_1, \ldots, x_n) = 0 \land \cdots \land p_k(x_1, \ldots x_n) = 0$$

A solution is

Motivation

For simplicity, we restrict to equations.

$$p_1(x_1, \ldots, x_n) = 0 \land \cdots \land p_k(x_1, \ldots x_n) = 0$$

A solution is *a common root for all* p_i.

Motivation

For simplicity, we restrict to equations.

$$p_1(x_1, \ldots, x_n) = 0 \wedge \cdots \wedge p_k(x_1, \ldots x_n) = 0$$

A solution is *a common root for all* p_i.

This is a well-studied problem in algebra!
One approach: Gröbner bases.

Common roots = Varieties

Let $P = \{p_1, ..., p_k\} \subseteq \mathbb{R}[x_1, ..., x_n]$ and $\mathcal{V}(P)$ be the set of common real roots:

$$\mathcal{V}(P) = \bigcap_{p \in P} roots_{\mathbb{R}}(p)$$

Common roots = Varieties

Let $P = \{p_1, ..., p_k\} \subseteq \mathbb{R}[x_1, ..., x_n]$ and $\mathcal{V}(P)$ be the set of common real roots:

$$\mathcal{V}(P) = \bigcap_{p \in P} roots_{\mathbb{R}}(p)$$

Observation

Let $p_1, p_2 \in P$ and $q \in \mathbb{R}[x_1, ..., x_n]$.

$$\mathcal{V}(P) = \mathcal{V}(P \cup \{p_1 + p_2\}) = \mathcal{V}(P \cup \{p_1 \cdot q\})$$

Common roots = Varieties

Let $P = \{p_1, ..., p_k\} \subseteq \mathbb{R}[x_1, ..., x_n]$ and $\mathcal{V}(P)$ be the set of common real roots:

$$\mathcal{V}(P) = \bigcap_{p \in P} roots_{\mathbb{R}}(p)$$

Observation

Let $p_1, p_2 \in P$ *and* $q \in \mathbb{R}[x_1, ..., x_n]$.

$$\mathcal{V}(P) = \mathcal{V}(P \cup \{p_1 + p_2\}) = \mathcal{V}(P \cup \{p_1 \cdot q\})$$

$$\mathcal{V}(P) = \mathcal{V}(P \cup \{p_1 - q \cdot p_2\}) = \mathcal{V}(P \cup \{p_1 \mod p_2\})$$

Common roots = Varieties

Let $P = \{p_1, ..., p_k\} \subseteq \mathbb{R}[x_1, ..., x_n]$ and $\mathcal{V}(P)$ be the set of common real roots:

$$\mathcal{V}(P) = \bigcap_{p \in P} roots_{\mathbb{R}}(p)$$

Observation

Let $p_1, p_2 \in P$ and $q \in \mathbb{R}[x_1, ..., x_n]$.

$$\mathcal{V}(P) = \mathcal{V}(P \cup \{p_1 + p_2\}) = \mathcal{V}(P \cup \{p_1 \cdot q\})$$

$$\mathcal{V}(P) = \mathcal{V}(P \cup \{p_1 - q \cdot p_2\}) = \mathcal{V}(P \cup \{p_1 \mod p_2\})$$

We can simplify polynomials, maintaining $\mathcal{V}$!

Analogon: Euclidean algorithm

$\mathbb{R}[x_1, ..., x_n]$ is just a ring like $\mathbb{Z}$.

Analogon: Euclidean algorithm

$\mathbb{R}[x_1, ..., x_n]$ is just a ring like $\mathbb{Z}$.

Euclidean algorithm

$a, b \in \mathbb{Z}$

while $b \neq 0$

  $tmp := b$

  $b := a \mod b$

  $a := tmp$

return a

Analogon: Euclidean algorithm

$\mathbb{R}[x_1, ..., x_n]$ is just a ring like $\mathbb{Z}$.

Euclidean algorithm

$a, b \in \mathbb{Z}$

while $b \neq 0$

  $tmp := b$

  $b := a \mod b$

  $a := tmp$

return a

Generalized version

$A \subset \mathbb{Z}$

do

  $A' := A$

  foreach $a, b \in A'$

    if $a \mod b \neq 0$

      $A := A \cup \{a \mod b\}$

until $A = A'$

return $\min A$

Buchberger algorithm

Going back to polynomials:

Generalized version

$A \subset \mathbb{Z}$
do
  $A' := A$
  foreach $a, b \in A'$
    if $a \mod b \neq 0$
      $A := A \cup \{a \mod b\}$
until $A = A'$
return $\min A$

Buchberger algorithm

Going back to polynomials:

Buchberger algorithm

$P = \{p_1, ..., p_k\}$
do
  $P' := P$
  foreach $p, q \in P'$
    if $p \mod q \neq 0$
      $P := P \cup \{p \mod q\}$
until $P = P'$
return $\min P$

Generalized version

$A \subset \mathbb{Z}$
do
  $A' := A$
  foreach $a, b \in A'$
    if $a \mod b \neq 0$
      $A := A \cup \{a \mod b\}$
until $A = A'$
return $\min A$

Buchberger algorithm

Going back to polynomials:

Buchberger algorithm

$P = \{p_1, ..., p_k\}$

do

$\quad P' := P$

$\quad$ foreach $p, q \in P'$

$\quad\quad$ if $p \mod q \neq 0$

$\quad\quad\quad P := P \cup \{p \mod q\}$

until $P = P'$

return $\min P$

Optimizations

- Normalize polynomials,
- Remove polynomials if factors have been found,

Result

Euclidean algorithm yields:

Result

Euclidean algorithm yields: GCD, i.e. largest common factor of all numbers.

Result

Euclidean algorithm yields: GCD, i.e. largest common factor of all numbers.
Buchbergers algorithm yields the largest common factor of all polynomials.

Result

Euclidean algorithm yields: GCD, i.e. largest common factor of all numbers.
Buchbergers algorithm yields the largest common factor of all polynomials.

A root r of a polynomial $p(x)$ corresponds to the linear factor $(x - r)$.
If this one has no roots, the polynomials have no common roots.

Result

Euclidean algorithm yields: GCD, i.e. largest common factor of all numbers.
Buchbergers algorithm yields the largest common factor of all polynomials.

A root r of a polynomial $p(x)$ corresponds to the linear factor $(x - r)$.
If this one has no roots, the polynomials have no common roots.

Formally:

Theorem (Hilbert's weak Nullstellensatz)

Let I be an ideal in $K[x_1, x_2, ..., x_n]$, then

$$1 \in I \Leftrightarrow \bigcap_{p \in I} roots_K(p) = \emptyset$$

Buchbergers algorithm *partially expands* I to check if $1 \in I$.

That’s it?

Unfortunately, K must be *algebraically closed*, i.e. $K \neq \mathbb{R}$, $K = \mathbb{C}$.

That's it?

Unfortunately, K must be *algebraically closed*, i.e. $K \neq \mathbb{R}$, $K = \mathbb{C}$.

$$roots_{\mathbb{C}}(P) = \emptyset \Rightarrow roots_{\mathbb{R}}(P) = \mathcal{V}(P) = \emptyset$$

That's it?

Unfortunately, K must be *algebraically closed*, i.e. $K \neq \mathbb{R}$, $K = \mathbb{C}$.

$$\mathit{roots}_{\mathbb{C}}(P) = \emptyset \Rightarrow \mathit{roots}_{\mathbb{R}}(P) = \mathcal{V}(P) = \emptyset$$

This method gives us no possibility to construct the actual solution!
(If $\mathcal{V}(P)$ is finite, we can do this.)

That's it?

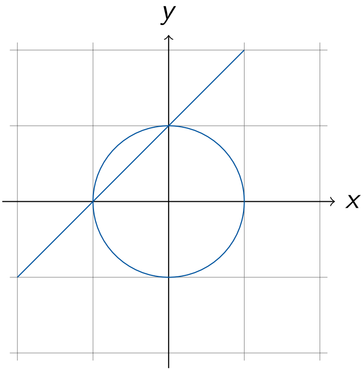
Unfortunately, K must be *algebraically closed*, i.e. $K \neq \mathbb{R}$, $K = \mathbb{C}$.

$$\mathit{roots}_{\mathbb{C}}(P) = \emptyset \Rightarrow \mathit{roots}_{\mathbb{R}}(P) = \mathcal{V}(P) = \emptyset$$

This method gives us no possibility to construct the actual solution!
(If $\mathcal{V}(P)$ is finite, we can do this.)
$\Rightarrow$ We can determine unsatisfiability, not satisfiability.

Example - Graphical

$$x^2 + y^2 - 1 = 0 \wedge x - y + 1 = 0$$



Common roots: $(-1, 0)$, $(0, 1)$

Example - Algorithm

$$
\begin{aligned}
P = \{ & \\
& p_1 = x^2 + y^2 - 1, \\
& p_2 = x - y + 1 \\
& \}
\end{aligned}
$$

Example - Algorithm

$$p_1 \mod p_2 = 2y^2 - 2y$$

$$P = \{$$
$$p_1 = x^2 + y^2 - 1,$$
$$p_2 = x - y + 1,$$
$$p_3 = 2y^2 - 2y$$
$$\}$$

Example - Algorithm

$$p_1 \mod p_2 = 2y^2 - 2y$$
$$p_2 \mod p_1 = x - y + 1$$

$$P = \{$$
$$p_1 = x^2 + y^2 - 1,$$
$$p_2 = x - y + 1,$$
$$p_3 = 2y^2 - 2y$$
$$\}$$

Example - Algorithm

$$P = \{$$
$$p_1 = x^2 + y^2 - 1,$$
$$p_2 = x - y + 1,$$
$$p_3 = 2y^2 - 2y,$$
$$p_4 = x^2 + y - 1$$
$$\}$$

$$p_1 \mod p_2 = 2y^2 - 2y$$
$$p_2 \mod p_1 = x - y + 1$$
$$p_1 \mod p_3 = x^2 + y - 1$$

Example - Algorithm

$$P = \{$$
$$p_1 = x^2 + y^2 - 1,$$
$$p_2 = x - y + 1,$$
$$p_3 = 2y^2 - 2y,$$
$$p_4 = x^2 + y - 1$$
$$\}$$

$$p_1 \mod p_2 = 2y^2 - 2y$$
$$p_2 \mod p_1 = x - y + 1$$
$$p_1 \mod p_3 = x^2 + y - 1$$
$$p_2 \mod p_3 = x - y + 1$$
$$p_3 \mod p_1 = 2y^2 - 2y$$
$$p_3 \mod p_2 = 2y^2 - 2y$$

Example - Algorithm

$$P = \{ p_1 = x^2 + y^2 - 1,\; p_2 = x - y + 1,\; p_3 = y^2 - y,\; p_4 = x^2 + y - 1 \}$$

$$\begin{aligned}
p_1 \mod p_2 &= 2y^2 - 2y \\
p_2 \mod p_1 &= x - y + 1 \\
p_1 \mod p_3 &= x^2 + y - 1 \\
p_2 \mod p_3 &= x - y + 1 \\
p_3 \mod p_1 &= 2y^2 - 2y \\
p_3 \mod p_2 &= 2y^2 - 2y \\
p_1 \mod p_4 &= y^2 - y \\
p_2 \mod p_4 &= x - y + 1 \\
p_3 \mod p_4 &= 2y^2 - 2y \\
p_4 \mod p_1 &= -y^2 + y \\
p_4 \mod p_2 &= y^2 - y \\
p_4 \mod p_3 &= x^2 + y - 1
\end{aligned}$$

Example - Algorithm

$$P = \{ \quad p_1 = x^2 + y^2 - 1, \quad p_2 = x - y + 1, \quad p_3 = y^2 - y, \quad p_4 = x^2 + y - 1 \quad \}$$

$$\begin{aligned}
p_1 \mod p_2 &= 2y^2 - 2y \\
p_2 \mod p_1 &= x - y + 1 \\
p_1 \mod p_3 &= x^2 + y - 1 \\
p_2 \mod p_3 &= x - y + 1 \\
p_3 \mod p_1 &= 2y^2 - 2y \\
p_3 \mod p_2 &= 2y^2 - 2y \\
p_1 \mod p_4 &= y^2 - y \\
p_2 \mod p_4 &= x - y + 1 \\
p_3 \mod p_4 &= 2y^2 - 2y \\
p_4 \mod p_1 &= -y^2 + y \\
p_4 \mod p_2 &= y^2 - y \\
p_4 \mod p_3 &= x^2 + y - 1
\end{aligned}$$

$1 \notin P$, hence no result in general.

Example - Algorithm

$$P = \{ \quad p_1 = x^2 + y^2 - 1, \quad p_2 = x - y + 1, \quad p_3 = y^2 - y, \quad p_4 = x^2 + y - 1 \quad \}$$

$$\begin{aligned}
p_1 &\mod p_2 = 2y^2 - 2y \\
p_2 &\mod p_1 = x - y + 1 \\
p_1 &\mod p_3 = x^2 + y - 1 \\
p_2 &\mod p_3 = x - y + 1 \\
p_3 &\mod p_1 = 2y^2 - 2y \\
p_3 &\mod p_2 = 2y^2 - 2y \\
p_1 &\mod p_4 = y^2 - y \\
p_2 &\mod p_4 = x - y + 1 \\
p_3 &\mod p_4 = 2y^2 - 2y \\
p_4 &\mod p_1 = -y^2 + y \\
p_4 &\mod p_2 = y^2 - y \\
p_4 &\mod p_3 = x^2 + y - 1
\end{aligned}$$

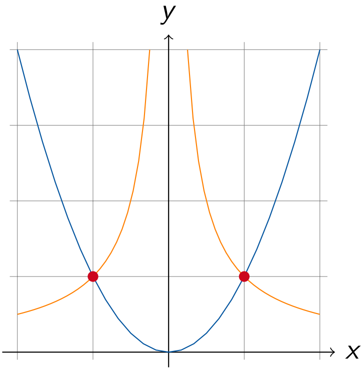
$1 \notin P$, hence no result in general.
With $y^2 - y = 0$ and $x - y + 1 = 0$ we can obtain $(-1, 0)$ and $(0, 1)$.

Example 1 – Finitely many common roots in $\mathbb{R}$

$$x^2 \cdot y^2 - 1 = 0 \wedge x^2 - y = 0$$

The Gröbner basis is:

$$P = \{x^2 - y, y^3 - 1\}$$



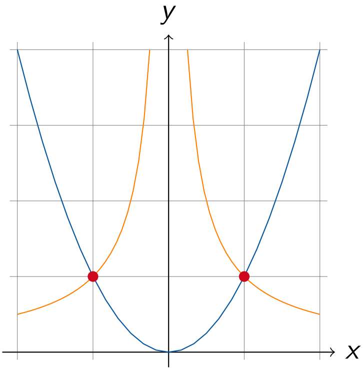
Example 1 – Finitely many common roots in $\mathbb{R}$

$$x^2 \cdot y^2 - 1 = 0 \wedge x^2 - y = 0$$

The Gröbner basis is:

$$P = \{x^2 - y, y^3 - 1\}$$

$1 \notin P$, hence there exists a solution in $\mathbb{C}$. The number of roots is finite, hence we can use the basis to obtain the solutions $(-1, 1)$ and $(1, 1)$ which are in $\mathbb{R}^2$.

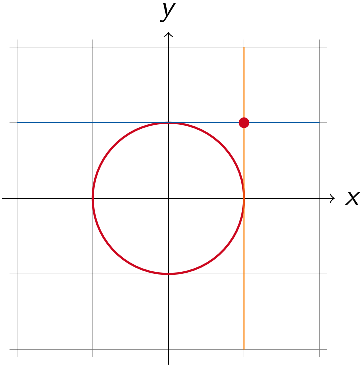


Example 2 – Infinitely many common roots in $\mathbb{R}$

$$x^2y - x^2 + y^3 - y^2 - y + 1 = 0 \wedge x^3 - x^2 + xy^2 - y - y^2 + 1 = 0$$

The Gröbner basis is:

$$P = \{p_1, p_2\}$$



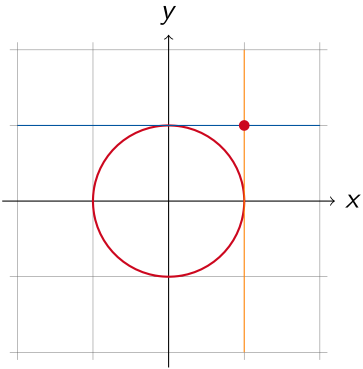
Example 2 – Infinitely many common roots in $\mathbb{R}$

$$x^2y - x^2 + y^3 - y^2 - y + 1 = 0 \land x^3 - x^2 + xy^2 - y - y^2 + 1 = 0$$

The Gröbner basis is:

$$P = \{p_1, p_2\}$$

$1 \notin P$, hence there exists a solution in $\mathbb{C}^2$. The number of roots is infinite, hence there is no general way to obtain the actual solutions.

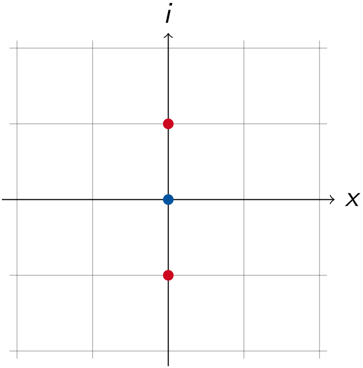


Example 3 – Common roots in $\mathbb{C}$

$x^2 + 1 = 0 \wedge x^3 + x = 0$

The Gröbner basis is:

$$P = \{x^2 + 1\}$$



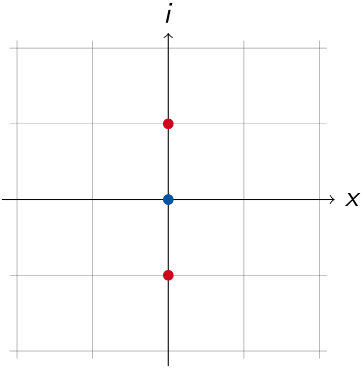
Example 3 – Common roots in $\mathbb{C}$

$$x^2 + 1 = 0 \land x^3 + x = 0$$

The Gröbner basis is:

$$P = \{x^2 + 1\}$$

$1 \notin P$, hence there exists a solution, i.e. a common root, in $\mathbb{C}$. However, this solution is in $\mathbb{C} \setminus \mathbb{R}$.



Extra: Handling inequalities

We only handled $=$. What about $\leq, \geq, <, >, \neq$?

Extra: Handling inequalities

We only handled $=$. What about $\leq, \geq, <, >, \neq$?

$$p(x) \leq 0 \Leftrightarrow p(x) + y^2 = 0$$
$$p(x) \geq 0 \Leftrightarrow p(x) - y^2 = 0$$
$$p(x) < 0 \Leftrightarrow p(x) \cdot y^2 + 1 = 0$$
$$p(x) > 0 \Leftrightarrow p(x) \cdot y^2 - 1 = 0$$
$$p(x) \neq 0 \Leftrightarrow p(x) \cdot y - 1 = 0$$

Extra: Ring

Let $(R, +, \cdot)$ be a ring, that is:

- $+$ is associative,
- $+$ is commutative,
- there is an additive identity 0,
- there is an additive inverse $-a$ for every $a \in R$,
- $\cdot$ is associative,
- there is a multiplicative identity 1,
- addition and multiplication distribute.

Examples:

- $\mathbb{Z}$ ($\cdot$ is commutative)
- $\mathbb{R}$ (is a field)
- $K[x_1, ..., x_n]$ (polynomial ring over field K)
- Our application: $\mathbb{R}[x_1, ..., x_n]$

Extra: Ideals

Ideal: A subset of a ring, that is *closed* under $+$ and *absorbs* $\cdot$.
Formally:

- $I \subseteq R$,
- $(I, +)$ is a subgroup of $(R, +)$, that is $0 \in I$, $-a \in I$ for all $a \in I$, $a + b \in I$ for all $a, b \in I$,
- $a \cdot b \in I$ for all $a \in I, b \in R$,
- $a \cdot b \in I$ for all $a \in R, b \in I$,

Examples:

- R is an ideal of R
- Even integers: $R = \mathbb{Z}$, $I = 2\mathbb{Z}$
- All polynomials divisible by $x^2 + 1$: $R = \mathbb{R}[x]$, $I = R/(x^2 + 1)$