Satisfiability Checking

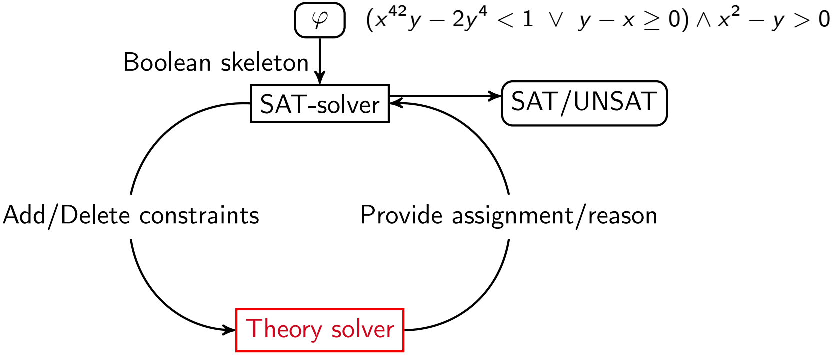
Subtropical Satisfiability

Prof. Dr. Erika Ábrahám

RWTH Aachen University
Informatik 2
LuFG Theory of Hybrid Systems

WS 19/20

Reminder: SMT



Solves $\begin{pmatrix} x^{42}y - 2y^4 < 1 \\ y - x \geq 0 \\ x^2 - y > 0 \end{pmatrix}$

The subtropical method is an efficient but incomplete way to check for satisfiability of some of these constraints.

Subtropical Satisfiability

- Let f be a multivariate polynomial and $f \sim 0$ with $\sim \in \{>, \geq, =\}$.
- The subtropical method quickly finds a solution to $f \sim 0$ with strictly positive real variables or returns unknown.
  If a solution is found: The constraint is satisfiable.
  Else: $f \sim 0$ might still hold.
- The method is incomplete and thus can be used in conjunction with other techniques.

Subtropical Real Root Finding

Find real roots (with all positive coordinates) for a polynomial f.

Subtropical Real Root Finding

Find real roots (with all positive coordinates) for a polynomial f.

1. If $f(1, ..., 1) = 0$ we are done.
   If $f(1, ..., 1) > 0$, consider $-f$ instead of f.
   Assume we now have $f(1, ..., 1) < 0$.

Subtropical Real Root Finding

Find real roots (with all positive coordinates) for a polynomial f.

1. If $f(1, ..., 1) = 0$ we are done.
   If $f(1, ..., 1) > 0$, consider $-f$ instead of f.
   Assume we now have $f(1, ..., 1) < 0$.
2. Find a solution p with all positive coordinates for $f(p) > 0$.

Subtropical Real Root Finding

Find real roots (with all positive coordinates) for a polynomial f.

1. If $f(1, ..., 1) = 0$ we are done.
   If $f(1, ..., 1) > 0$, consider $-f$ instead of f.
   Assume we now have $f(1, ..., 1) < 0$.
2. Find a solution p with all positive coordinates for $f(p) > 0$.
3. By the Intermediate Value Theorem (a continuous function with positive and negative values has a zero) we are now able to construct a root of f using the knowledge gained in steps 1 and 2.

Subtropical Real Root Finding

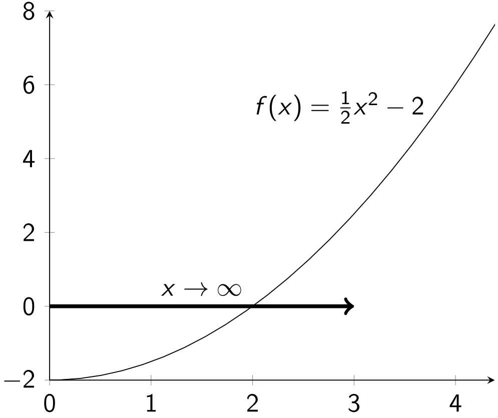
Find real roots (with all positive coordinates) for a polynomial f.

1. If $f(1, ..., 1) = 0$ we are done.
   If $f(1, ..., 1) > 0$, consider $-f$ instead of f.
   Assume we now have $f(1, ..., 1) < 0$.
2. Find a solution p with all positive coordinates for $f(p) > 0$.
3. By the Intermediate Value Theorem (a continuous function with positive and negative values has a zero) we are now able to construct a root of f using the knowledge gained in steps 1 and 2.

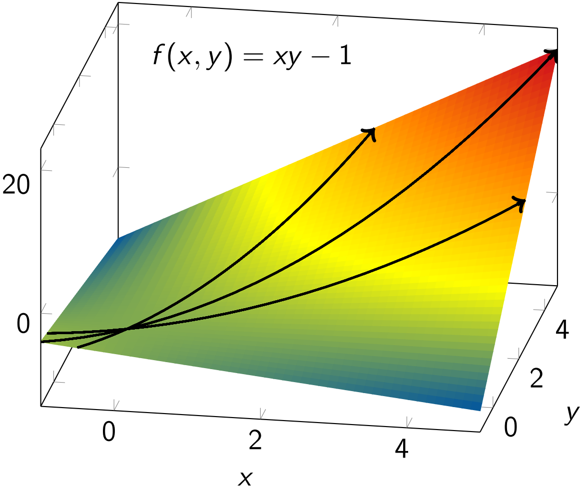
If the constraint is not an equality, we are done after step 2.

We observe for a univariate $f(x)$:

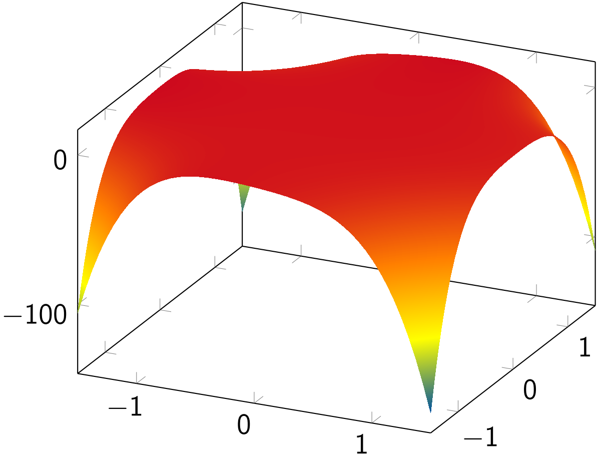
$$\lim_{x \to \infty} f(x) = \begin{cases} \infty & \textit{if the leading coefficient is positive} \\ -\infty & \textit{else} \end{cases}$$



Intuition – multivariate 1



Intuition – multivariate 2



$$f(x, y) = y + 2xy^3 - 3x^2y^2 - x^3 - 4x^4y^4$$

Handling multivariate polynomials

- Consider $f(x, y)$ and have (x, y) "growing in some direction".
- For this direction the two variables x and y can be parameterised by a single variable t to construct f^* (starting from $f(1, 1)$).
- Instead of having f on $\mathbb{R}^2$, we consider f restricted to a line as f^* and have the simple case from before.

Handling multivariate polynomials

- Consider $f(x, y)$ and have (x, y) "growing in some direction".
- For this direction the two variables x and y can be parameterised by a single variable t to construct f^* (starting from $f(1, 1)$).
- Instead of having f on $\mathbb{R}^2$, we consider f restricted to a line as f^* and have the simple case from before.
- We need to find a direction such that the leading coefficient for the parameterisation f^* is positive.

Handling multivariate polynomials

- Consider $f(x, y)$ and have (x, y) "growing in some direction".
- For this direction the two variables x and y can be parameterised by a single variable t to construct f^* (starting from $f(1, 1)$).
- Instead of having f on $\mathbb{R}^2$, we consider f restricted to a line as f^* and have the simple case from before.
- We need to find a direction such that the leading coefficient for the parameterisation f^* is positive.

How do we find a "direction" which has a positive leading coefficient?

The frame of a multivariate polynomial f

Definition

For $f = \sum_{i=1,2,..,n} f_i x_1^{e_{i,1}} \ldots x_d^{e_{i,d}} \in \mathbb{Z}[x_1, \ldots, x_d]$ with
(i) $n > 0$,
(ii) $(e_{i,1}, ldots, e_{i,d}) \neq (e_{j,1} \ldots, e_{j,d})$ for $i \neq j$ and
(iii) $f_i \neq 0$ for $i = 1, \ldots, n$ we define:

$$\begin{aligned} frame(f) &= \{(e_{i,1}, \ldots, e_{i,d}) \mid i \in \{1, \ldots, n\}\} \\ frame^+(f) &= \{(e_{i,1}, \ldots, e_{i,d}) \mid i \in \{1, \ldots, n\} \wedge f_i > 0\} \\ frame^-(f) &= \{(e_{i,1}, \ldots, e_{i,d}) \mid i \in \{1, \ldots, n\} \wedge f_i < 0\} \end{aligned}$$

The frame of a multivariate polynomial f

Definition

For $f = \sum_{i=1,2,..,n} f_i x_1^{e_{i,1}} \ldots x_d^{e_{i,d}} \in \mathbb{Z}[x_1, \ldots, x_d]$ with
(i) $n > 0$,
(ii) $(e_{i,1}, ldots, e_{i,d}) \neq (e_{j,1} \ldots, e_{j,d})$ for $i \neq j$ and
(iii) $f_i \neq 0$ for $i = 1, \ldots, n$ we define:

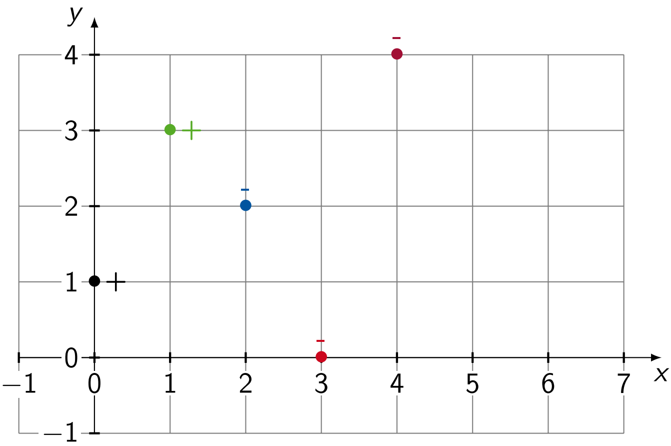
$$\begin{aligned} frame(f) &= \{(e_{i,1}, \ldots, e_{i,d}) \mid i \in \{1, \ldots, n\}\} \\ frame^+(f) &= \{(e_{i,1}, \ldots, e_{i,d}) \mid i \in \{1, \ldots, n\} \wedge f_i > 0\} \\ frame^-(f) &= \{(e_{i,1}, \ldots, e_{i,d}) \mid i \in \{1, \ldots, n\} \wedge f_i < 0\} \end{aligned}$$

$$f = y + 2xy^3 - 3x^2y^2 - x^3 - 4x^4y^4$$
$$frame(f) = \{(0,1), (1,3), (2,2), (3,0), (4,4)\}$$

And we define based on the signs of the coefficients:

$$frame^+(f) = \{(0,1), (1,3)\}$$
$$frame^-(f) = \{(2,2), (3,0), (4,4)\}$$

The frame of a multivariate polynomial f visualized



$$f = y + 2xy^3 - 3x^2y^2 - x^3 - 4x^4y^4$$

$$frame(f) = \{(0,1), (1,3), (2,2), (3,0), (4,4)\}$$

The Newton polytope of a polynomial f

Convex hull

Given $S \subseteq \mathbb{R}^d$, the *convex hull* $conv(S) \subseteq \mathbb{R}^d$ is the smallest (inclusion-minimal) convex set containing S.

The Newton polytope of a polynomial f

Convex hull

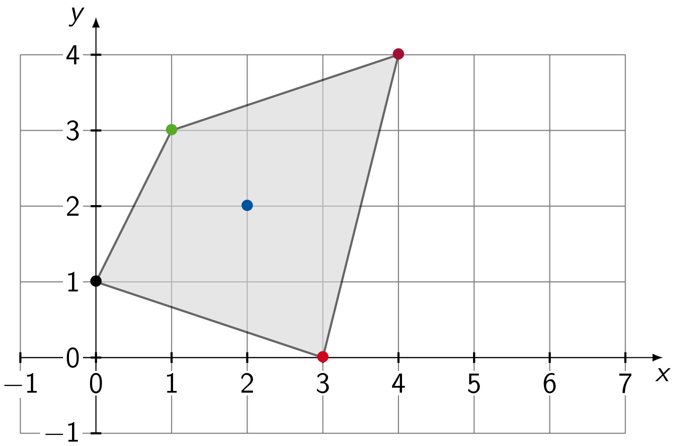
Given $S \subseteq \mathbb{R}^d$, the *convex hull* $conv(S) \subseteq \mathbb{R}^d$ is the smallest (inclusion-minimal) convex set containing S.

Newton polytope

The *Newton polytope* of a polynomial $f \not\equiv 0$ is the convex hull of its frame: $Newton(f) = conv(frame(f))$

This is indeed a polytope because the convex hull of finite non-empty set of points is bounded.

The Newton polytope of a polynomial f visualized



$$f = y + 2xy^3 - 3x^2y^2 - x^3 - 4x^4y^4$$

The shaded region is the Newton polytope $Newton(f)$ of f.

The vertices of a Newton polytope

Faces of a polytope

Given a polytope $P \subseteq \mathbb{R}^d$, the *face* of P with respect to a vector $n \in \mathbb{R}^d$ is:

$$\mathit{face}(n, P) = \{p \in P \mid n^T p \geq n^T q \text{ for all } q \in P\}.$$

The vertices of a Newton polytope

Faces of a polytope

Given a polytope $P \subseteq \mathbb{R}^d$, the *face* of P with respect to a vector $n \in \mathbb{R}^d$ is:

$$face(n, P) = \{p \in P \mid n^T p \geq n^T q \text{ for all } q \in P\}.$$

Vertices of a polytope

The faces of dimension 0 are called *vertices*. The set of all *vertices* of a given polytope P is $V(P)$.

The vertices of a Newton polytope

Faces of a polytope

Given a polytope $P \subseteq \mathbb{R}^d$, the *face* of P with respect to a vector $n \in \mathbb{R}^d$ is:

$$face(n, P) = \{p \in P \mid n^T p \geq n^T q \text{ for all } q \in P\}.$$

Vertices of a polytope

The faces of dimension 0 are called *vertices*. The set of all *vertices* of a given polytope P is $V(P)$.

Note: $p \in V(P)$ *iff* there exists $n \in \mathbb{R}^d$ with $n^T p > n^T q$ for all $q \in P \setminus \{p\}$.

The vertices of a Newton polytope

Faces of a polytope

Given a polytope $P \subseteq \mathbb{R}^d$, the *face* of P with respect to a vector $n \in \mathbb{R}^d$ is:

$$face(n, P) = \{p \in P \mid n^T p \geq n^T q \text{ for all } q \in P\}.$$

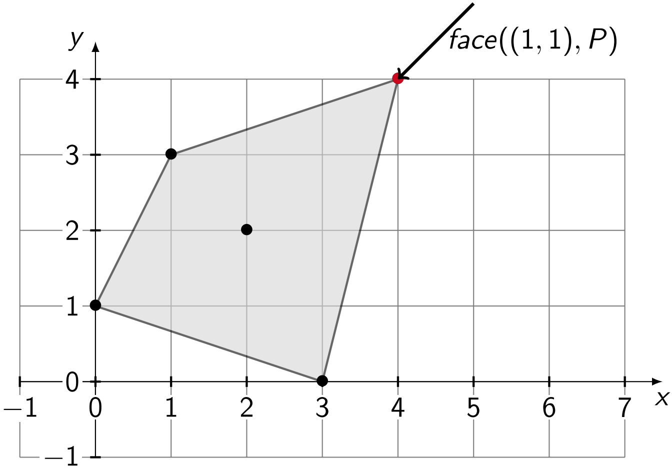
Vertices of a polytope

The faces of dimension 0 are called *vertices*. The set of all *vertices* of a given polytope P is $V(P)$.

Note: $p \in V(P)$ *iff* there exists $n \in \mathbb{R}^d$ with $n^T p > n^T q$ for all $q \in P \setminus \{p\}$.

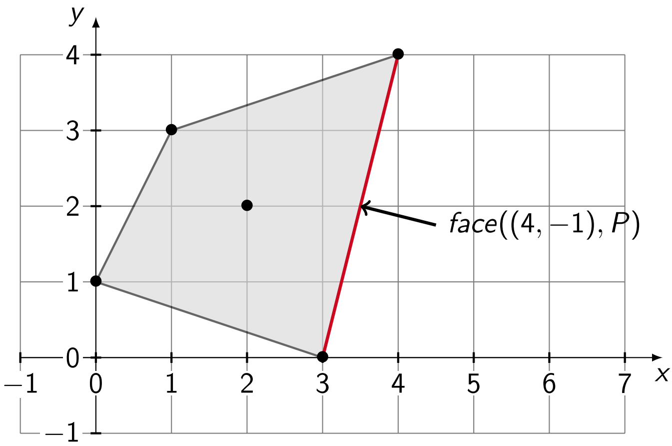
Because $frame(f)$ is finite, it is true that:
$V(Newton(f)) \subseteq frame(f) \subseteq Newton(f))$.

The faces of a Newton polytope visualized



The shaded region is the Newton polytope P of f.
$\mathit{face}((1,1),P) = \{(4,4)\}$ has dimension 0.

The faces of a Newton polytope visualized



The shaded region is the Newton polytope P of f.

$face((4,-1),P) = \{(3,0) + t(1,4) | 0 \leq t \leq 1\}$ has dimension 1.

Hyperplanes separating vertices of the polytope

Hyperplanes

A *hyperplane* is a subspace whose dimension is one less than that of its surrounding space. Such a *hyperplane* H can be described by the following equation:

$$H : n^T x + c = 0$$

Hyperplanes separating vertices of the polytope

Hyperplanes

A *hyperplane* is a subspace whose dimension is one less than that of its surrounding space. Such a *hyperplane* H can be described by the following equation:

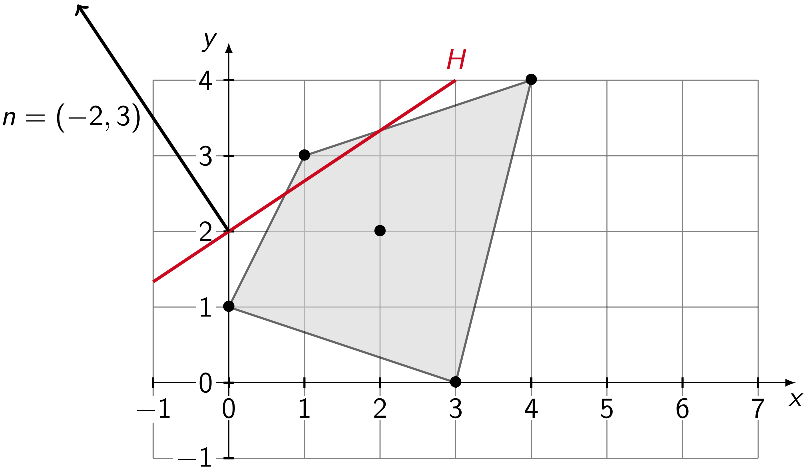
$$H : n^T x + c = 0$$

Lemma 1

Let f be a polynomial, $p \in \mathit{frame}(f)$ and $n \in \mathbb{R}^d$. Then the following are equivalent:

1. $p \in V(\mathit{Newton}(f))$ with respect to n.
2. There exists $c \in \mathbb{R}$ such that the hyperplane $H : n^T x + c = 0$ strictly separates p from $\mathit{frame}(f) \setminus \{p\}$. The normal vector n is directed from H towards p.

Hyperplanes separating vertices of the polytope visualized



The shaded region is the Newton polytope P of f.

$H : (-2,3)^T x - 6 = 0$ strictly separates $(1,3)$ from the *frame*(f).

Vertices as dominating monomials

If p is a vertex of the Newton polytope with respect to n, then the corresponding monomial will dominate the entire polynomial in the direction of n.

Vertices as dominating monomials

If p is a vertex of the Newton polytope with respect to n, then the corresponding monomial will dominate the entire polynomial in the direction of n.

Lemma 2

Let f be a polynomial and $p \in frame(f)$ be a vertex of $Newton(f)$ with respect to $n \in \mathbb{R}^d$. Then there exists $a_0 \in \mathbb{R}^+$ such that for all $a \in \mathbb{R}^+$ with $a \geq a_0$ the following holds:

1. $|f_p a^{n^T p}| > |\sum_{q \in frame(f) \setminus \{p\}} f_q a^{n^T q}|$
2. $sign(f(a^{n_1}, \ldots, a^{n_d})) = sign(f_p)$

where f_p is the corresponding coefficient to p and $f_p a^{n^T p} = f_p (a^{n_1})^{p_1} (a^{n_2})^{p_2} \ldots (a^{n_d})^{p_d}$.

Vertices as dominating monomials

If p is a vertex of the Newton polytope with respect to n, then the corresponding monomial will dominate the entire polynomial in the direction of n.

Lemma 2

Let f be a polynomial and $p \in frame(f)$ be a vertex of $Newton(f)$ with respect to $n \in \mathbb{R}^d$. Then there exists $a_0 \in \mathbb{R}^+$ such that for all $a \in \mathbb{R}^+$ with $a \geq a_0$ the following holds:

1. $|f_p a^{n^T p}| > |\sum_{q \in frame(f) \setminus \{p\}} f_q a^{n^T q}|$
2. $sign(f(a^{n_1}, \ldots, a^{n_d})) = sign(f_p)$

where f_p is the corresponding coefficient to p and $f_p a^{n^T p} = f_p (a^{n_1})^{p_1} (a^{n_2})^{p_2} \ldots (a^{n_d})^{p_d}$.

To find a point with all positive coordinates where $f > 0$ we now just need to find a $p \in frame^+(f)$ and check if it is also a vertex of $Newton(f)$.

Recap

Let f a multivariate polynomial. If

- H is a hyperplane with normal vector n,
- $p \in \mathit{frame}^+(f)$ and
- H separates p from the remaining frame of f

then

Recap

Let f a multivariate polynomial. If

- H is a hyperplane with normal vector n,
- $p \in \mathit{frame}^+(f)$ and
- H separates p from the remaining frame of f

then

- f_p eventually dominates f (going towards n),
- thus f eventually becomes positive and
- we can construct a solution.

Recap

Let f a multivariate polynomial. If

- H is a hyperplane with normal vector n,
- $p \in \mathit{frame}^+(f)$ and
- H separates p from the remaining frame of f

then

- f_p eventually dominates f (going towards n),
- thus f eventually becomes positive and
- we can construct a solution.

How do we find n and H?

Example

- Let f again be a multivariate polynomial with:

$$f = y + 2xy^3 - 3x^2y^2 - x^3 - 4x^4y^4$$

- As we have seen the point $(1, 3)$ is a vertex of $Newton(f)$ with respect to the normal vector $(-2, 3)$.
- Lemma 2 guarantees that $f(a^{-2}, a^3) > 0$ for sufficiently large positive values of a.
- For example: $a = 2$, $f(2^{-2}, 2^3) = \frac{51193}{256}$.
- Generally, a suitable a can be found by starting with $a = 2$ and doubling a until the constraint is satisfied.

The linear problem

- Problem: Given a polynomial f, does a point with all positive coordinates exist with $f > 0$?
- By Lemma 1 the problem can be reduced to finding a hyperplane $H : n^T x + c = 0$ separating a $p \in \mathit{frame}^+(f)$ from $\mathit{frame}(f) \setminus \{p\}$ where $\mathit{frame}(f) \subset \mathbb{R}^d$ and $n \in \mathbb{R}^d$ is a vector pointing from H to p.
- This can be expressed as a linear problem with $d + 1$ real variables n and c:

$$\varphi(p, \mathit{frame}(f), n, c) = n^T p + c > 0 \wedge \bigwedge_{q \in \mathit{frame}(f) \setminus p} n^T q + c < 0$$

The linear problem: example

- Let f again be a multivariate polynomial with:

$$f = y + 2xy^3 - 3x^2y^2 - x^3 - 4x^4y^4$$

- Problem: Does a point with all positive coordinates exist with $f > 0$
- By Lemma 1 the problem can be reduced to finding a hyperplane $H : n^T x + c = 0$ separating a $p \in \mathit{frame}^+(f)$ from $\mathit{frame}(f) \setminus \{p\}$ where $\mathit{frame}(f) \subset \mathbb{R}^2$ and $n \in \mathbb{R}^2$ is a vector pointing from H to p.
- Encoding :

$$\exists n_x, n_y, c : p_x n_x + p_y n_y + c > 0 \wedge \bigwedge_{q \in \mathit{frame}(f) \setminus p} q_x n_x + q_y n_y + c < 0$$

for a given $p \in \mathit{frame}^+(f)$.

The last step (for equalities)

- We have $f(1, ..., 1) < 0$.
- And we found a such that $f(a^n) > 0$ for some direction n.
- What do we need to do now?

The last step (for equalities)

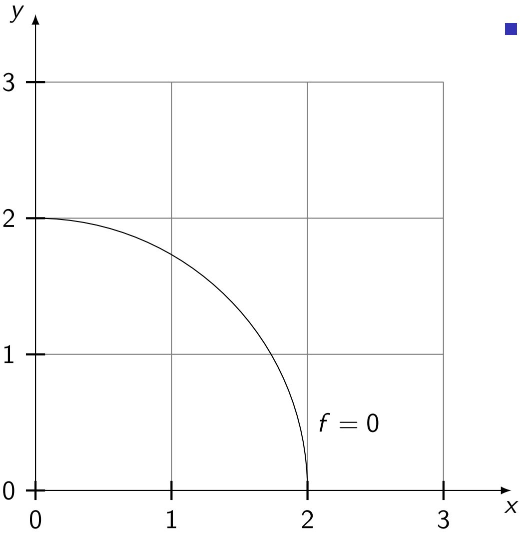
- We have $f(1, ..., 1) < 0$.
- And we found a such that $f(a^n) > 0$ for some direction n.
- What do we need to do now?
- *Find solution to:* $f = 0$.

Constructing the root

Given: $f(1, ..., 1) < 0 < f(p)$ for some real coordinates p.
Find root of f on the line from $(1, ..., 1)$ to p.
The Intermediate Value Theorem tells us this root exists.

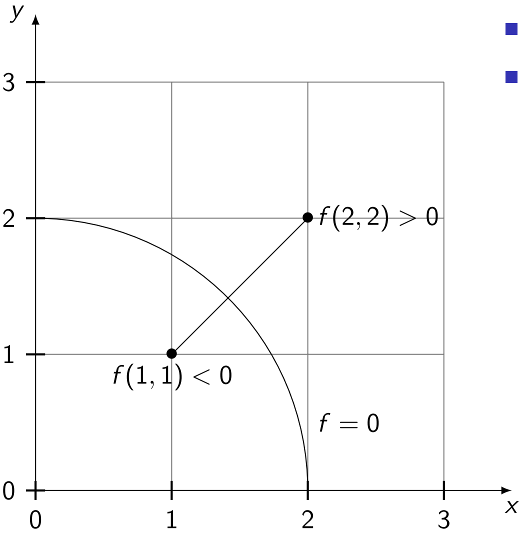
1. Construct a new univariate polynomial f^* from f by parameterising the variables in a new variable t such that we traverse the line from $(1, ..., 1)$ to p for $t \in [0, 1]$.
2. Find root t_0 of this new polynomial f^* by common techniques e.g. bisection.
3. Construct root of f as point on the line from $(1, ..., 1)$ to p for parameter t_0.

Constructing the root



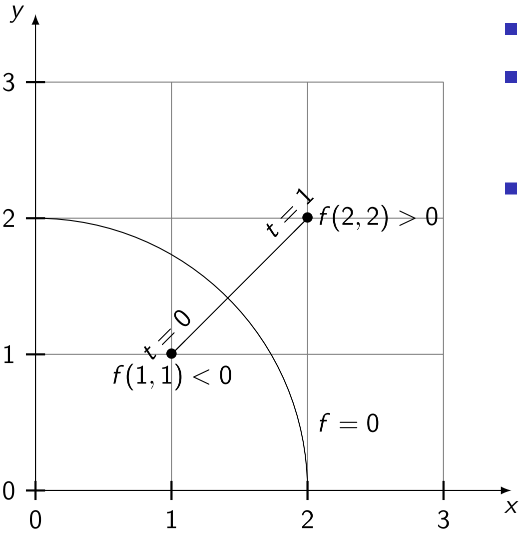
- Let $f = x^2 + y^2 - 4$.

Constructing the root



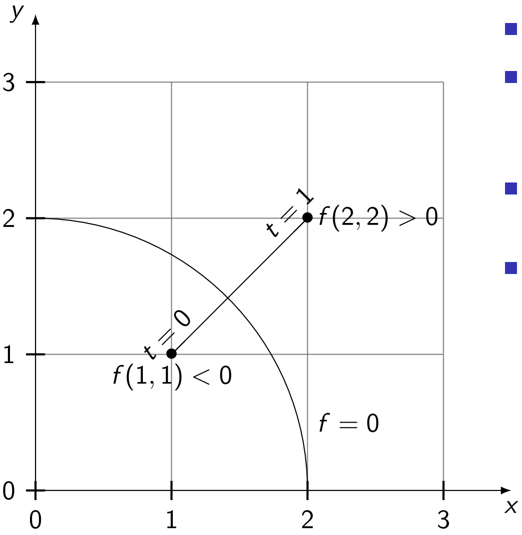
- Let $f = x^2 + y^2 - 4$.
- We have $f(1,1) < 0$ and $f(2,2) > 0$ and can construct a root of f on $(1,1)$—$(2,2)$.

Constructing the root



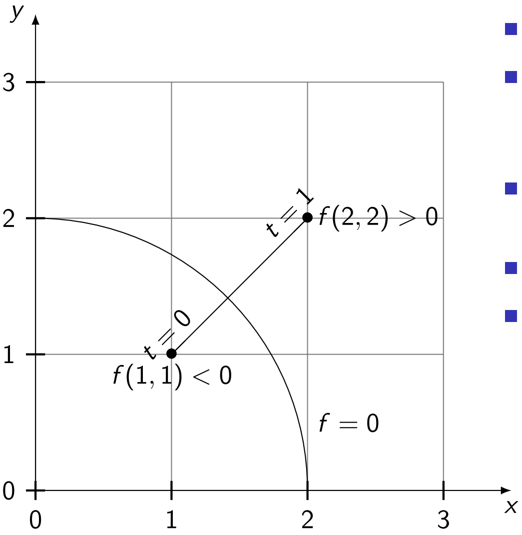
- Let $f = x^2 + y^2 - 4$.
- We have $f(1,1) < 0$ and $f(2,2) > 0$ and can construct a root of f on $(1,1)$—$(2,2)$.
- $x \to 1 + (2-1) * t = 1 + t$
  $y \to 1 + (2-1) * t = 1 + t$

Constructing the root



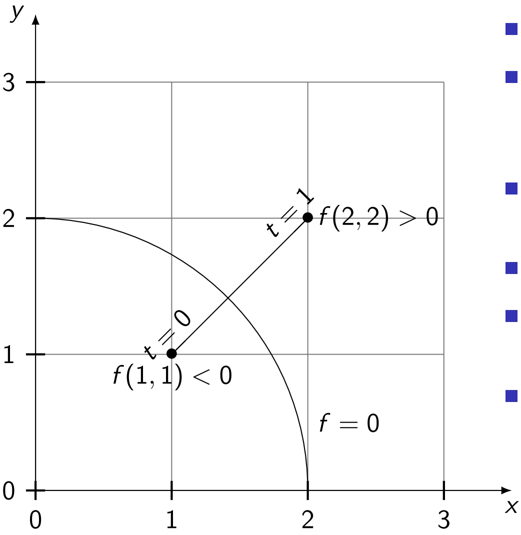
- Let $f = x^2 + y^2 - 4$.
- We have $f(1,1) < 0$ and $f(2,2) > 0$ and can construct a root of f on $(1,1)$—$(2,2)$.
- $x \to 1 + (2-1) * t = 1 + t$
  $y \to 1 + (2-1) * t = 1 + t$
- Then $f^* = (1+t)^2 + (1+t)^2 - 4$.

Constructing the root

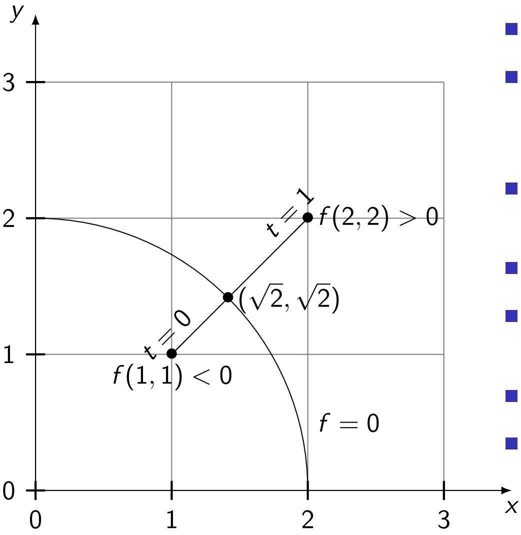


- Let $f = x^2 + y^2 - 4$.
- We have $f(1,1) < 0$ and $f(2,2) > 0$ and can construct a root of f on $(1,1)$—$(2,2)$.
- $x \to 1 + (2-1) * t = 1 + t$
  $y \to 1 + (2-1) * t = 1 + t$
- Then $f^* = (1+t)^2 + (1+t)^2 - 4$.
- There ex. $t \in [0,1]$ such that $f^*(t) = 0$.

Constructing the root



- Let $f = x^2 + y^2 - 4$.
- We have $f(1,1) < 0$ and $f(2,2) > 0$ and can construct a root of f on $(1,1)$—$(2,2)$.
- $x \to 1 + (2-1) * t = 1 + t$
  $y \to 1 + (2-1) * t = 1 + t$
- Then $f^* = (1+t)^2 + (1+t)^2 - 4$.
- There ex. $t \in [0,1]$ such that $f^*(t) = 0$.
- Here we have: $t = \sqrt{2} - 1$.



- Let $f = x^2 + y^2 - 4$.
- We have $f(1,1) < 0$ and $f(2,2) > 0$ and can construct a root of f on $(1,1)$—$(2,2)$.
- $x \to 1 + (2-1) * t = 1 + t$
  $y \to 1 + (2-1) * t = 1 + t$
- Then $f^* = (1+t)^2 + (1+t)^2 - 4$.
- There ex. $t \in [0,1]$ such that $f^*(t) = 0$.
- Here we have: $t = \sqrt{2} - 1$.
- $(1 + (\sqrt{2} - 1), 1 + (\sqrt{2} - 1)) = (\sqrt{2}, \sqrt{2})$ is a root of f.

Summary

- For constraints of the form $f > 0$ (or $f \geq 0$):
  Solve the linear problem of finding a hyperplane separating a $p \in \mathit{frame}^+(f)$ from the rest of $\mathit{frame}(f)$.
  Construct a point for which $f > 0$ (or $f \geq 0$) by choosing large enough values going in the direction of the normal vector of the hyperplane.

Summary

- For constraints of the form $f > 0$ (or $f \geq 0$):
  Solve the linear problem of finding a hyperplane separating a $p \in \mathit{frame}^+(f)$ from the rest of $\mathit{frame}(f)$.
  Construct a point for which $f > 0$ (or $f \geq 0$) by choosing large enough values going in the direction of the normal vector of the hyperplane.
- For equalities of the form $f = 0$ (assuming $f(1, ..., 1) < 0$):
  Find a point for which $f > 0$ like above, then construct a root of f as a point on the line from $(1, .., 1)$ to this point.

Summary

- For constraints of the form $f > 0$ (or $f \geq 0$):
  Solve the linear problem of finding a hyperplane separating a $p \in \mathit{frame}^+(f)$ from the rest of $\mathit{frame}(f)$.
  Construct a point for which $f > 0$ (or $f \geq 0$) by choosing large enough values going in the direction of the normal vector of the hyperplane.
- For equalities of the form $f = 0$ (assuming $f(1, ..., 1) < 0$):
  Find a point for which $f > 0$ like above, then construct a root of f as a point on the line from $(1, .., 1)$ to this point.

Not shown here: deal with multiple constraints at once.
How?

Summary

- For constraints of the form $f > 0$ (or $f \geq 0$):
  Solve the linear problem of finding a hyperplane separating a $p \in \mathit{frame}^+(f)$ from the rest of $\mathit{frame}(f)$.
  Construct a point for which $f > 0$ (or $f \geq 0$) by choosing large enough values going in the direction of the normal vector of the hyperplane.
- For equalities of the form $f = 0$ (assuming $f(1, ..., 1) < 0$):
  Find a point for which $f > 0$ like above, then construct a root of f as a point on the line from $(1, .., 1)$ to this point.

Not shown here: deal with multiple constraints at once.
How? Search for one direction that works for all constraints.