Lecture evaluation

https://www.campus.rwth-aachen.de/evasys/online.php?pswd=5Z9VAR2JM2

Satisfiability Checking
20 Subtropical satisfiability

Prof. Dr. Erika Ábrahám

RWTH Aachen University
Informatik 2
LuFG Theory of Hybrid Systems

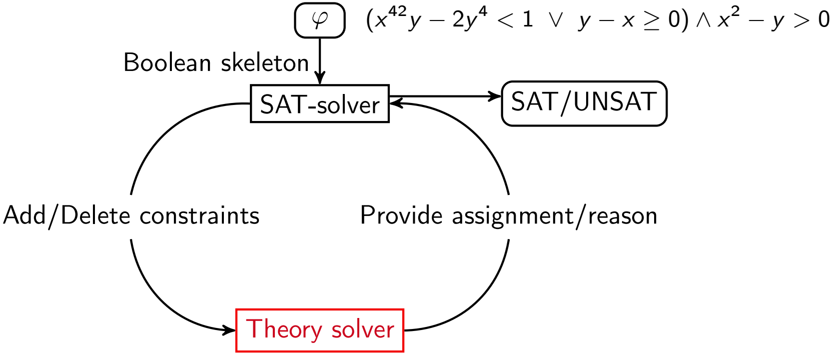
WS 22/23

	$+$	$+\ ,\ \cdot$
Reals $\mathbb{R}$	linear real arithmetic decidable Gauß+ Fourier-Motzkin Simplex	non-linear real arithmetic decidable Interval constraint propagation Subtropical satisfiability Virtual substitution Cylindrical algebraic decomposition
Integers $\mathbb{Z}$	linear integer arithmetic decidable Branch-and-bound	non-linear integer arithmetic undecidable Bit-blasting Branch-and-bound Interval constraint propagation

Notations

- Unless noted otherwise, vectors are row vectors.
- Assume: variables $x_1, \ldots, x_d$, coefficient domain D (we use $\mathbb{Q}$).
- Monomial: product of variables (the empty product represents the constant 1).
  Examples: xy^2, u^3vz^2, 1
  变量乘积
- Term: product of a coefficient and a monomial.
  Examples: $2xy^2$, $3u^3vz^2$, -5
  变量乘积× 系数
- Polynomial (in normal form): sum of terms with pairwise different monomials.
  Example: $2xy^2 + 3u^3vz^2 - 5$
  $D[x_1, \ldots, x_d]$ ($d \geq 1$): set of all polynomials in variables $x_1, \ldots, x_d$ with coefficients from D.
  最简式
- Polynomial constraint (in canonical form): $p \sim 0$, $\sim \in \{<, \leq, =, \geq, >\}$.
  Example: $2xy^2 + 3u^3vz^2 - 5 < 0$
- A polynomial in one variable is called univariate.
  A polynomial in more than one variables is called multivariate.
  Multivariate polynomials can be seen as univariate polynomials with polynomial coefficients (notation: $p \in \mathbb{D}[x_1, \ldots, x_{d-1}][x_d]$).
  $x + xy^2 + 2 = 0$
  $\Rightarrow (1) \cdot x + (y)^2 \cdot x + 2 = 0$ 转化为x为变元, y^2为系数

Reminder: SMT



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

The subtropical method is an efficient but incomplete way to check polynomial constraint sets for satisfiability.

Subtropical satisfiability

In this lecture:

- Let $p \sim 0$ with $p \in \mathbb{Q}[x_1, \ldots, x_d]$ $(d \geq 1)$ and $\sim \in \{>, \geq, =, \leq, <\}$.
- Either quickly find a positive solution to $p \sim 0$ or return unknown.

  If a solution is found: The constraint is satisfiable.

  Else: $p \sim 0$ might still be satisfiable

  $\rightsquigarrow$ combine with a complete technique.

Not shown here:

1. extension to the negative space;
2. deal with multiple constraints at once.

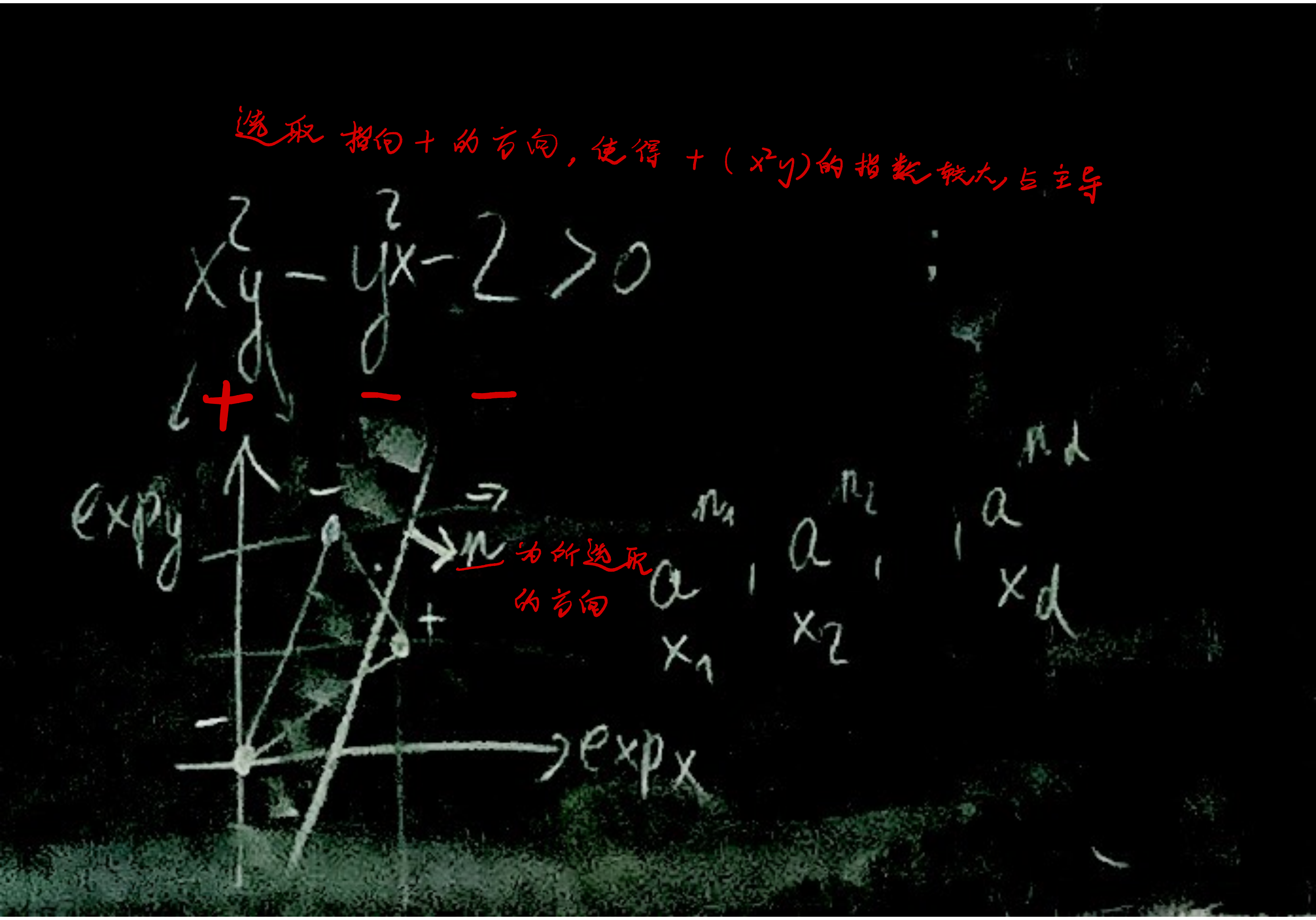
Subtropical satisfiability

$p>0$

$2x^5 + x^2 + 2^{200}\cdot x^0$ 最低次项, x 减小($x\to 0$), dominate

最高次项, x足够大, dominate

- First we discuss We now know a method to find a (positive) solution for $p > 0$.
- Constraints $p < 0$ can be transformed to $-p > 0$, to which the previous method can be applied.
- Handle $p \leq 0$ resp. $p \geq 0$ strict as $p < 0$ resp. $p > 0$.
- For equalities $p = 0$:
  1. If $p(1, ..., 1) = 0$ we have a solution.
     If $p(1, ..., 1) > 0$, consider $-p = 0$ instead of $p = 0$.
     Assume we now have $p(1, ..., 1) < 0$.
  2. Find a (positive) solution v for $p(v) > 0$.
  3. By the Intermediate Value Theorem (a continuous function with positive and negative values has a root) we are now able to construct a root of p using the knowledge gained in steps 1 and 2.

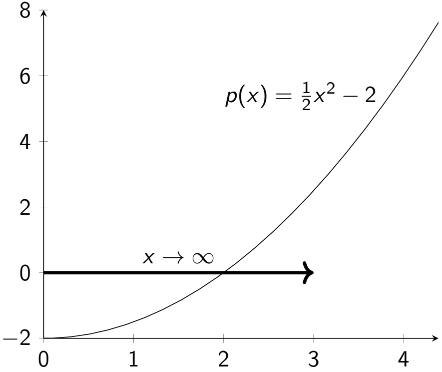

选取指向+的方向，使得+(x²y)的指数较大，占主导
x²y − y²x − 2 > 0
+ − −
exp y
exp x
n 为所选取的方向
a^{n1}_{x1}, a^{n2}_{x2}, ..., a^{nd}_{xd}

Intuition: The univariate case

单变量

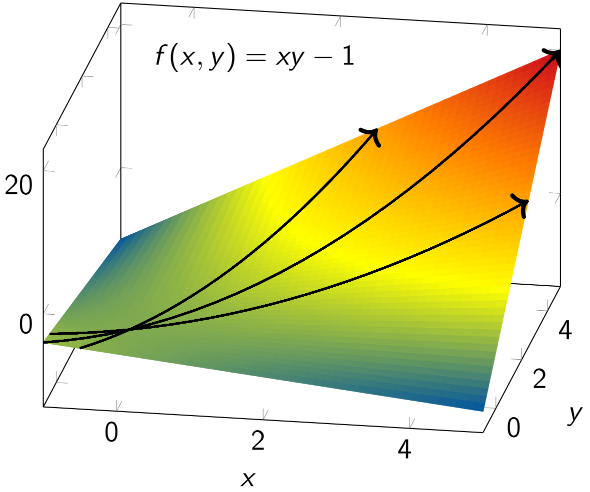
We observe for a univariate $p(x)$:

$$\lim_{x\to\infty} p(x) = \begin{cases} \infty & \textit{if the coefficient of the monomial with the} \\ & \textit{largest exponent is positive} \\ -\infty & \textit{else} \end{cases}$$



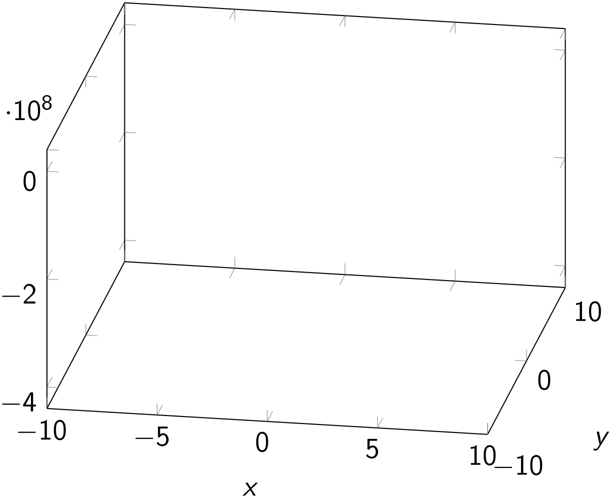
Leading coefficient in $p(x)$ is positive $\Rightarrow$ Large enough x satisfies $p(x) > 0$.

Intuition: The multivariate case I



Intuition: The multivariate case II

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



Handling multivariate polynomials

多变量

- Let $p \in \mathbb{Q}[x_1, \ldots, x_d]$ and $n = (n_1, \ldots, n_d) \in \mathbb{R}^d$.
- We consider the value of

  $$p(a^{n_1}, \ldots, a^{n_d})$$

  for increasing $a \in \mathbb{R}_{>0}$.
- For large enough a, one of p's terms will become "dominating": its absolute value will be larger than the sum of the absolute values of all other terms.
- Thus the coefficient of the dominating term will determine the sign of the polynomial.
- Since we want to satisfy $p > 0$, we search for a direction for which the dominating term has a positive coefficient.

How do we find such a direction?

The frame of a multivariate polynomial p

Definition

For $p = \sum_{i=1,2,..,k} c_i x_1^{e_{i,1}} \ldots x_d^{e_{i,d}} \in \mathbb{Q}[x_1, \ldots, x_d]$ with $k > 0$ and $(e_{i,1}, \ldots, e_{i,d}) \neq (e_{j,1} \ldots, e_{j,d})$ for $i \neq j$ we define:

$$\begin{array}{rcl} \mathit{frame}(p) & = & \{(e_{i,1}, \ldots, e_{i,d}) \mid i \in \{1, \ldots, k\} \wedge c_i \neq 0\} \\ \mathit{frame}^{+}(p) & = & \{(e_{i,1}, \ldots, e_{i,d}) \mid i \in \{1, \ldots, k\} \wedge c_i > 0\} \\ \mathit{frame}^{-}(p) & = & \{(e_{i,1}, \ldots, e_{i,d}) \mid i \in \{1, \ldots, k\} \wedge c_i < 0\} \end{array}$$

Example:

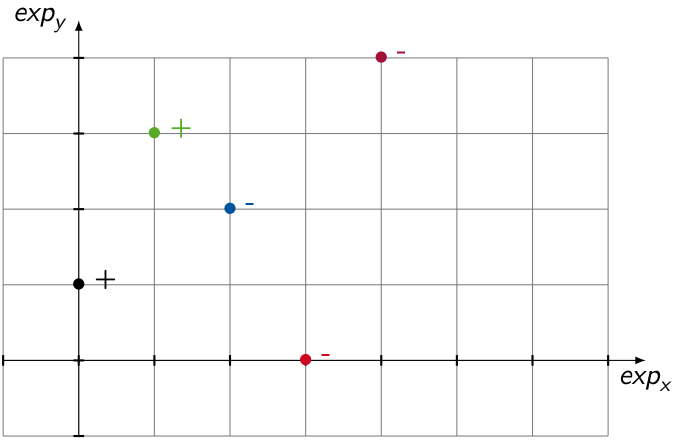
$$p(x, y) = y + 2xy^3 - 3x^2y^2 - x^3 - 4x^4y^4$$

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

$$\mathit{frame}^{+}(p) = \{(0, 1), (1, 3)\}$$

$$\mathit{frame}^{-}(p) = \{(2, 2), (3, 0), (4, 4)\}$$

The frame of a multivariate polynomial p



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

$$\mathit{frame}(p) = \{\underbrace{(0,1)}_{+}, \underbrace{(1,3)}_{+}, \underbrace{(2,2)}_{-}, \underbrace{(3,0)}_{-}, \underbrace{(4,4)}_{-}\}$$

The Newton polytope of a polynomial p

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.

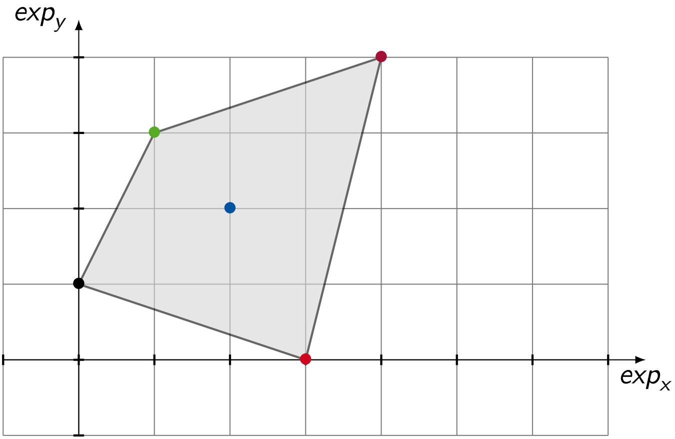
Newton polytope

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

newton polytope牛顿凸包: 以次幂数Frame为点集的凸包

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

The Newton polytope of a polynomial p visualized



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

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

The vertices of a Newton polytope

A face of a convex polytope is any intersection of the polytope with a halfspace, such that, none of the interior points of the polytope lie on the boundary of the halfspace.

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:

$$face(n, P) = \{v \in P \mid nv^T \geq nu^T \text{ for all } u \in P\}.$$

face为凸包在某一向量上的边界

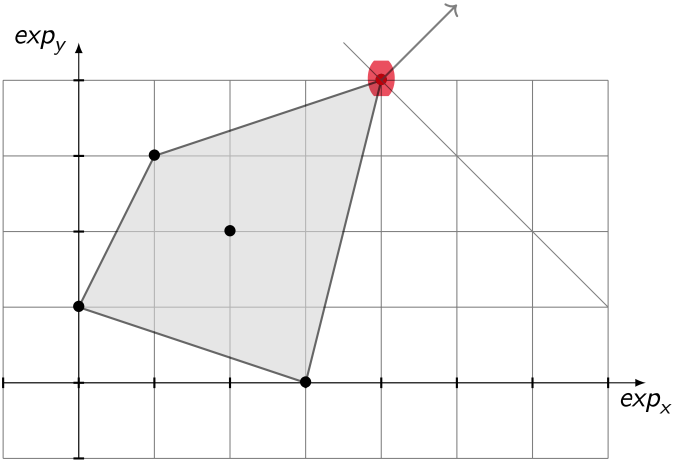
Vertices of a polytope

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

vertex: 0维 face
edge: 1维face

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

The faces of a Newton polytope visualized



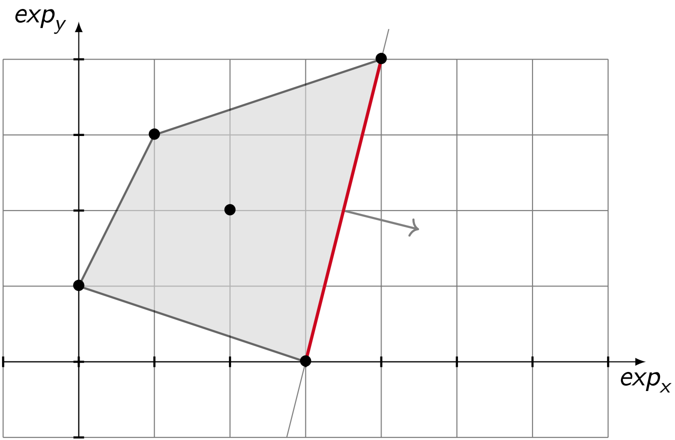
The shaded region is the Newton polytope P of p.

$face((1,1), P) = \{(4,4)\}$ has dimension 0.

(1,1)为向量

I.e. $(4,4)$ is a vertex of P.

The faces of a Newton polytope visualized



The shaded region is the Newton polytope P of p.

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

I.e., it is a face but not a vertex of P.

Hyperplanes separating vertices of the polytope

Hyperplanes

A *hyperplane* H is the solution set of an equation $nx^T = b$ for some $d > 0$, $x = (x_1, \ldots, x_d)$, $n \in \mathbb{R}^d$ and $b \in \mathbb{R}$.

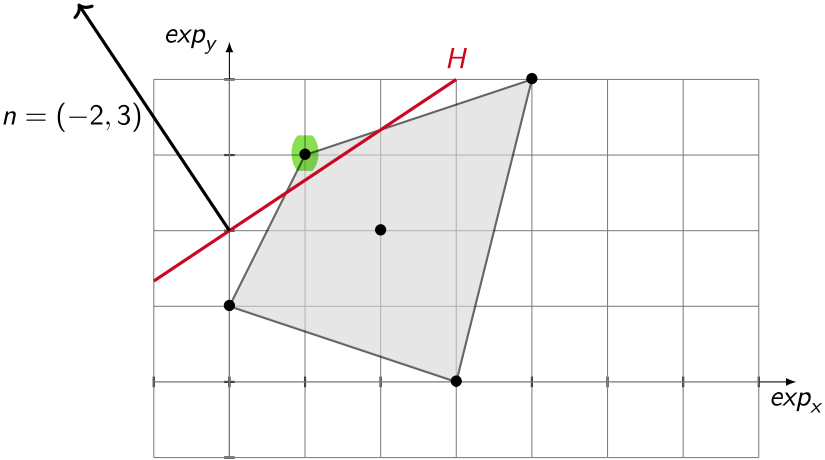
Lemma 1

For each $p \in \mathbb{Q}[x_1, \ldots, x_d]$, $v \in frame(p)$ and $n \in \mathbb{R}^d$, the following are equivalent:

1. v is a vertex of $Newton(p)$ with respect to n.
2. There exists $b \in \mathbb{R}$ such that the hyperplane $H : nx^T = b$ strictly separates v from $frame(p) \setminus \{v\}$. The normal vector n is directed from H towards v. hyperplane H将v从点集中分开

从H指向v的为正交向量n

Hyperplanes separating vertices of the polytope visualized



The shaded region is the Newton polytope P of p.

$-2x + 3y - 6 = 0$ strictly separates $(1, 3)$ from $\mathit{frame}(p) \setminus \{(1, 3)\}$.

Vertices as dominating monomials

If v 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

v是n方向上的face且为vertex, 则v会在n方向上dominate

Assume

- a polynomial $p \in \mathbb{Q}[x_1, \ldots, x_d]$, $p \not\equiv 0$;
- a vertex $v \in \mathit{frame}(p)$ of $\mathit{Newton}(p)$ with respect to $n \in \mathbb{R}^d$, where
- c_v is the corresponding coefficient to v in p;
- $(a^n)^v = (a^{n_1})^{v_1}(a^{n_2})^{v_2} \ldots (a^{n_d})^{v_d}$.

Then there exists $a_0 \in \mathbb{R}_{>0}$ such that for all $a \in \mathbb{R}$ with $a \geq a_0$:

绝对值

1. $|c_v(a^n)^v| > |\sum_{u \in \mathit{frame}(p)\setminus\{v\}} c_u(a^n)^u|$ and

   rest of the polytype的绝对值

2. $\mathit{sign}(p(a^{n_1}, \ldots, a^{n_d})) = \mathit{sign}(c_v)$.

Thus solution for $p > 0$ can be given based on some $v \in \mathit{frame}^+(p)$ that is a vertex of $\mathit{Newton}(p)$.

Example

- Assume

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

- $(1, 3) \in V(Newton(p))$ with normal vector $(-2, 3)$.
- Lemma 2 $\Rightarrow$ $p(a^{-2}, a^3) > 0$ for sufficiently large a.
- For example: $a = 2,\ p(2^{-2}, 2^3) = \frac{51193}{256}$.
- Generally, a suitable a can be found by starting with $a = 2$ and doubling a until the constraint is satisfied.

a从2开始, 2^1, 2^2, 2^3 … 2^n

The linear problem

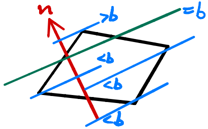
- Remaining problem: Find a hyperplane $H : nx^T = b$ separating a $v \in frame^+(p)$ from $frame(p) \setminus \{v\}$ where $frame(p) \subset \mathbb{R}^d$ and $n \in \mathbb{R}^d$ points from H towards v.
- This can be expressed as a linear problem with $d + 1$ real variables $n_1 \dots, n_d, b$:

$$nv^T > b \wedge \bigwedge_{u \in frame(p) \setminus \{v\}} nu^T < b$$

Example: 有2个frame+,选择hyperplane使得法向量指向其中一个即可

- Constraint: $p(x, y) = y + 2xy^3 - 3x^2y^2 - x^3 - 4x^4y^4 > 0$
- Check the separating hyperplane existence for each $v \in frame^+(p)$.
- Encoding for $(1, 3) \in frame^+(p)$:

$$1 \cdot n_x + 3 \cdot n_y > b \quad \wedge 0 \cdot n_x + 1 \cdot n_y < b$$
$$\wedge 2 \cdot n_x + 2 \cdot n_y < b$$
$$\wedge 3 \cdot n_x + 0 \cdot n_y < b$$
$$\wedge 4 \cdot n_x + 4 \cdot n_y < b$$



$\rightsquigarrow (n_x, n_y) = (-2, 3)$, $b = 6$ is a solution

Example I

- Constraint: $\underbrace{2x^2y-3x-4y}_{p(x,y)} > 0$
- $frame^+(p) = \{(2,1)\}$, $frame^-(p) = \{(1,0),(0,1)\}$
- Halfplane encoding for the only positive frame point $(2,1)$:

$$2n_x + 1n_y > b \wedge 1n_x + 0n_y < b \wedge 0n_x + 1n_y < b$$

$n = (n_x, n_y)$ 为 normal vector，指向 V

- Solution: $n_x = 1$, $n_y = 0$, $b = 1.5$
- $p(a^1, a^0) = 2a^2 - 3a - 4$
- Check $a = 2$: $p(a^1, a^0) = 2 \cdot 2^2 - 3 \cdot 2 - 4 = -2 < 0$
- Check $a = 4$: $p(a^1, a^0) = p(4,1) = 2 \cdot 4^2 - 3 \cdot 4 - 4 = 16 > 0$
- Solution found: $x = a^1 = 4$, $y = a^0 = 1$

Example II

- Constraint: $\underbrace{2x^3y^2 - 3x^4y}_{p(x,y)} > 0$
- $\mathit{frame}^+(p) = \{(3,2)\}$, $\mathit{frame}^-(p) = \{(4,1)\}$
- Halfplane encoding for only positive frame point $(3,2)$:

$$3n_x + 2n_y > b \land 4n_x + 1n_y < b$$

- Solution: $n_x = -1$, $n_y = 1$, $b = -2$
- $p(a^{-1}, a^1) = 2a^{-3}a^2 - 3a^{-4}a = 2a^{-1} - 3a^{-3}$
- Check $a = 2$: $p(a^{-1}, a^1) = 2 \cdot 2^{-1} - 3 \cdot 2^{-3} = 1 - 3/8 = 5/8 > 0$
- Solution found: $x = a^{-1} = 0.5$, $y = a^1 = 2$

Subtropical satisfiability

- First we discuss We now know a method to find a (positive) solution for $p > 0$.
- Constraints $p < 0$ can be transformed to $-p > 0$, to which the previous method can be applied.
- Handle $p \leq 0$ resp. $p \geq 0$ strict as $p < 0$ resp. $p > 0$.
- For equalities $p = 0$:
  1. If $p(1, ..., 1) = 0$ we have a solution.

     If $p(1, ..., 1) > 0$, consider $-p = 0$ instead of $p = 0$.

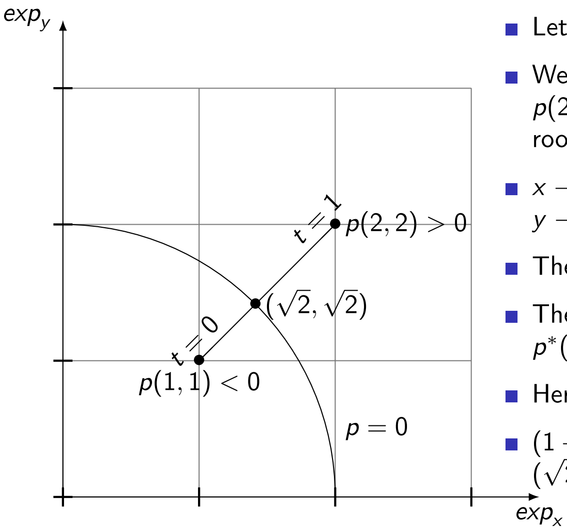
     Assume we now have $p(1, ..., 1) < 0$.
  2. Find a (positive) solution v for $p(v) > 0$.
  3. By the Intermediate Value Theorem (a continuous function with positive and negative values has a root) we are now able to construct a root of p using the knowledge gained in steps 1 and 2.

Constructing the root

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

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

Constructing the root



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

Example III

- Constraint: $\underbrace{x - 2y}_{p(x,y)} = 0$
- $p(1,1) = 1 - 2 \cdot 1 = -1 < 0$
- Assume we computed solution for $p(x, y) > 0$: $x = 1$, $y = 0$
- Connecting line: $(x, y) = (1, 1) + t \cdot (1 - 1, 0 - 1)$ for some $0 \leq t \leq 1$
  $\rightsquigarrow$ $\boxed{x = 1}$, $\boxed{y = 1 - t}$

  Substituted in $p(x, y) = 0$:

  $$p(\boxed{1}, \boxed{1 - t}) = \boxed{1} - 2(\boxed{1 - t}) = 1 - 2 + 2t = 2t - 1 = 0$$

  Solution: $t = 0.5$
- $x_0 = 1$, $y_0 = 1 - t = 1 - 0.5 = 0.5$
- Control: $p(x_0, y_0) = p(1, 0.5) = 1 - 2 \cdot 0.5 = 0$

Example IV

- Constraint: $\underbrace{2x^2y - 3x - 4y}_{p(x,y)} = 0$
- $p(1,1) = 2 \cdot 1^2 \cdot 1 - 3 \cdot 1 - 4 \cdot 1 = -5 < 0$
- Solution for $p(x,y) > 0$ from Example I: $p(4,1) = 16 > 0$
- Connecting line: $(x,y) = (1,1) + t \cdot (4-1, 1-1) = (1,1) + t(3,0)$ for some $0 \leq t \leq 1$
  $\leadsto x = 1 + 3t,\ y = 1$
  Substituted in $p = 0$:

  $$2(1+3t)^2(1) - 3(1+3t) - 4(1) = 18t^2 + 3t - 5 = 0$$

  Solution: $t = \frac{\sqrt{41}-1}{12} \approx 0.450260353$
- $x_0 = 1 + 3t \approx 2,350781059,\ y_0 = 1$
- Control: $p(x_0, y_0) = 0$

Learning target

- Which sufficient condition is used by the subtropical satisfiability method for the existence of a real-valued solution of a multivariate polynomial constraint?
- If the sufficient condition holds, how can we construct a solution?