Satisfiability Checking

Cylindrical Algebraic Decomposition

Prof. Dr. Erika Ábrahám

RWTH Aachen University
Informatik 2
LuFG Theory of Hybrid Systems

WS 14/15

Reminder: Non-linear real arithmetic (NRA)

Syntax

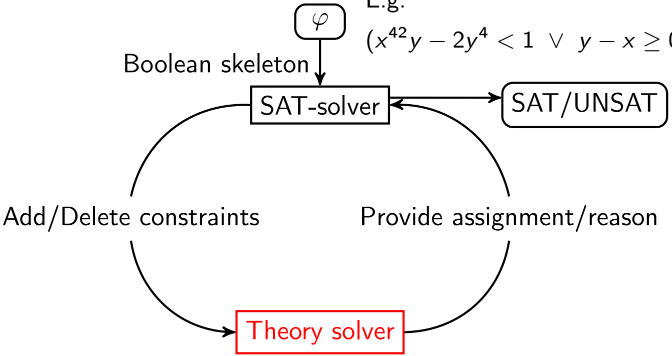
$$
\begin{array}{rlllllll}
\text{Polynomials: } p & ::= & 0 & \mid 1 & \mid x & \mid p+p & \mid p-p & \mid (p \cdot p) \\
\text{Constraints: } c & ::= & p=0 & \mid p<0 & \mid p>0 & & & \\
\text{Formulas: } \varphi & ::= & c & \mid \neg\varphi & \mid \varphi \wedge \varphi & \mid \exists x \varphi & &
\end{array}
$$

where x is a variable.

- Syntactic sugar: $\leq$, $\geq$, $\neq$, $\forall$, $\vee$, $\rightarrow$, $\ldots$
- Though CAD can be applied to general NRA formulas, for simplicity, we consider only the satisfiability check of quantifier-free formulas (existential fragment of NRA).
- $p = a_1 x_1^{e_{1,1}} \cdots x_n^{e_{n,1}} + \cdots + a_k x_1^{e_{1,k}} \cdots x_n^{e_{n,k}}$,
  $\deg(p) := \max_{1 \leq j \leq k}(\sum_{i=1}^{n} e_{i,j})$ degree of p
- φ non-linear, if there is a polynomial p in φ with $\deg(p) > 1$.

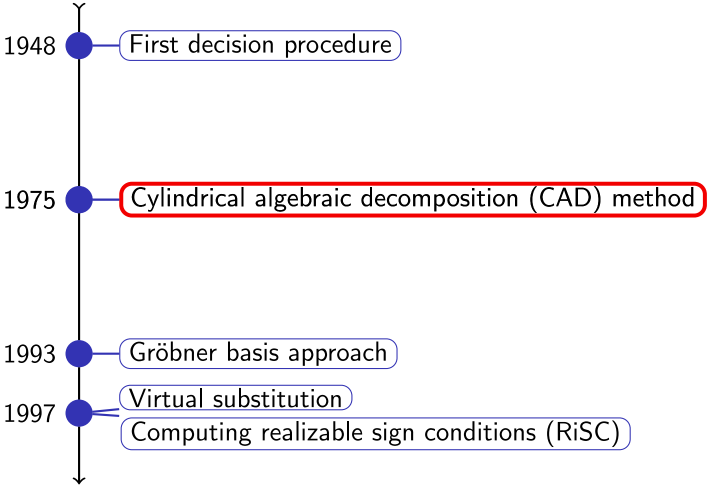
  Linear real arithmetic (LRA): $\deg(p) \leq 1$ for all polynomials p in φ.

E.g.
$(x^{42}y - 2y^4 < 1 \;\vee\; y - x \geq 0) \wedge x^2 - y > 0$



Solves $\begin{pmatrix} p_1 & \sim_1 & 0 \\ & \vdots & \\ p_m & \sim_m & 0 \end{pmatrix}$ where $\begin{array}{ll} p_i & \in \mathbb{Z}[x_1, \ldots, x_n], \\ \sim_i & \in \{<, =, >\} \end{array}$ for $1 \leq i \leq m$.

Reminder: NRA solving history



Outline

1. Preliminaries
2. Cylindrical Algebraic Decomposition for $\mathbb{R}$
3. Cylindrical Algebraic Decomposition for $\mathbb{R}^n$

Outline

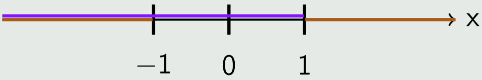
NRA solution space (12)

Solution set: $\mathcal{S}\begin{pmatrix} p_1 & \sim_1 & 0 \\ & \vdots & \\ p_m & \sim_m & 0 \end{pmatrix} = \{a \in \mathbb{R}^n \mid p_i(a) \sim_i 0, 1 \leq i \leq m\}$, where

$p_i \in \mathbb{Z}[x_1, \ldots, x_n]$, $\sim_i \in \{<, =, >\}$ for $1 \leq i \leq m$.

Example (one-dimensional)

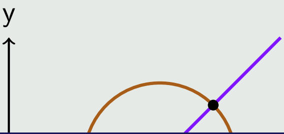
$$\mathcal{S}\begin{pmatrix} x^2 - 1 > 0 \\ 1 - x > 0 \end{pmatrix}$$



$$= \,]-\infty, -1[$$

Example (two-dimensional)

$$\mathcal{S}\begin{pmatrix} (x-2)^2 + \\ (y-2)^2 - 1 = 0 \\ \\ x - y = 0 \end{pmatrix}$$



Sign-invariance

Sign of a polynomial

Given a polynomial $p \in \mathbb{Z}[x_1, \dots, x_n]$, $a \in \mathbb{R}^n$,

$$\mathrm{sgn}(p(a)) \quad := \quad \begin{cases} -1, & p(a) < 0, \\ 0, & p(a) = 0, \\ 1, & p(a) > 0. \end{cases}$$

Let $P = (p_1, \dots, p_m) \in \mathbb{Z}[x_1, \dots, x_n]^m$. A region $R \subseteq \mathbb{R}^n$ is *P*-sign-invariant if $\mathrm{sgn}(p_i)(a) = \mathrm{sgn}(p_i)(b)$ for all $i \in \{1, \dots, m\}$ and $a, b \in R$.

Sign-invariance

Solution sets are sign-invariant sets

Given $P = (p_1, \ldots, p_m) \in \mathbb{Z}[x_1, \ldots, x_n]^m$, $\sim_i \in \{<, =, >\}$ for $1 \leq i \leq m$, then

$$\mathcal{S}\begin{pmatrix} p_1 \sim_1 0 \\ \vdots \\ p_m \sim_m 0 \end{pmatrix} = \mathcal{S}\begin{pmatrix} \mathrm{sgn}(p_1) = \sigma_1 \\ \vdots \\ \mathrm{sgn}(p_m) = \sigma_m \end{pmatrix} =: \mathcal{S}_\sigma(P)$$

with $\sigma = (\sigma_1, \ldots, \sigma_m)$ and $\sigma_i = \begin{cases} -1 & \textit{if } \sim_i \textit{ is } < \\ 0 & \textit{if } \sim_i \textit{ is } = \\ 1 & \textit{if } \sim_i \textit{ is } > \end{cases}$.

Sign-invariant regions

Region

$R \in \mathbb{R}^n$ is called a region if

$$R \neq (A \cap R) \cup (B \cap R)$$

with $A \cap R \neq \emptyset$ and $B \cap R \neq \emptyset$ for all open, $\emptyset \neq A, B \subseteq \mathbb{R}^n$ with $A \cap B = \emptyset$.

Example

- For $a, b \in \mathbb{R}$, $]a, b[$, $\{a\}$, are regions, and $R \times R'$ for regions R, R'.

Remarks

Let $P \in \mathbb{Z}[x_1, \ldots, x_n]^m$ and $\sigma \in \{-1, 0, 1\}^m$.

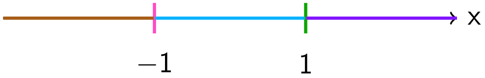
- $\mathcal{S}_\sigma(P)$ can be decomposed into maximal regions.
- $\mathbb{R}^n$ can be decomposed into maximal P-sign-invariant regions.

Cylindrical algebraic decomposition: Idea

- Assume a set P of polynomials in n variables together with a sign condition for each polynomial in P.
- The cylindrical algebraic decomposition (CAD) method produces a decomposition of $\mathbb{R}^n$ into a finite number of P-sign-invariant regions (CAD cells).
- Take an arbitrary element (sample point) from each of the CAD cells.
- If all sign conditions are satisfied for at least one sample point then the problem is satisfiable.
- Otherwise the problem is unsatisfiable.

Example: Sign-invariant regions

$P = (x^2 - 1,\ 1 - x)$



Non-trivial roots

Remark

Let $p \in \mathbb{Z}[x]$.

- p has between 0 and $\deg(p)$ real roots.

Example

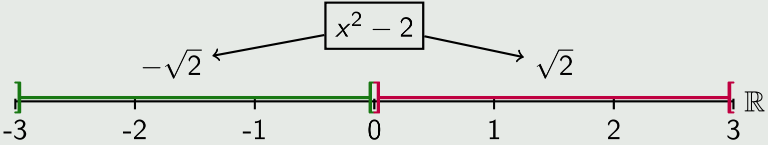
- $x^3 - 6x^2 + 11x - 6$ has rational roots: 1, 2 and 3.
- $x^3 - x^2 - 2x + 2$ has one rational and two irrational roots: 1, $-\sqrt{2}$ and $\sqrt{2}$.
- $x^5 - 3x^4 + x^3 - x^2 + 2x - 2$ has only one real root ≈ 2.70312, not representable by radicals.

Representing a real algebraic number

Interval representation

$$\Big(\underbrace{p,}_{\in \mathbb{Z}[x]} \qquad \underbrace{]\; l, \quad r \;[}_{\text{exactly one real root of } p \text{ in } (l,r)}\Big)$$

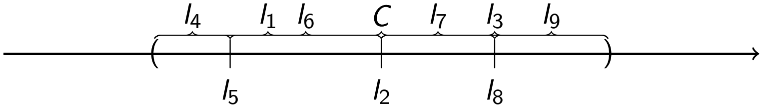
Example



Outline

CAD for $\mathbb{R}$

- Assume a set $P = \{p_1 \sim_1 0, \ldots, p_k \sim_k\}$ of univariate polynomial constraints with $p_i \in \mathbb{Z}[x]$ and $\sim_i \in \{<, \leq, =, \neq, \geq, >\}$.
- Cauchy bound $\Rightarrow$ Interval C containing all real roots of $p_1, \ldots, p_k$.
- Sturm sequence $\Rightarrow$ count the real roots of each p_i in an interval.
- Split C until each sub-interval I contains at most one real root.



CAD for $\mathbb{R}$ with respect to $p_1, \ldots, p_k$:
$[(p_i, I_j), (p_i, I_j)]$ for each I_j containing a real root of a p_i and open intervals between them.

Cauchy bound

Assume a univariate polynomial

$$p = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x^1 + a_0 x^0 \in \mathbb{Z}[x]$$

with $a_k \neq 0$. If $\xi \in \mathbb{R}$ is a (real) root of p (i.e. $p(\xi) = 0$) then

$$|\xi| \leq 1 + \max_{i=1,\ldots,k} \frac{|a_i|}{|a_k|} := C \ .$$

C is called the Cauchy bound for p.

Strum sequence

Definition (Sturm sequence)

Assume a square-free (no square factors, i.e., no repeated roots) univariate polynomial

$$p = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x^1 + a_0 x^0 \in \mathbb{Z}[x]$$

with $a_k \neq 0$. A Sturm sequence for p is a finite sequence of polynomials $p_0, p_1, \ldots, p_l$ of decreasing degree with the following properties:

- $p_0 = p$,
- if $p(a) = 0$ then $\mathrm{sgn}(p_1(a)) = \mathrm{sgn}(p'(a))$,
- if $p_i(a) = 0$ for $0 < i < l$ then $\mathrm{sgn}(p_{i-1}(a)) = -\mathrm{sgn}(p_{i+1}(a))$,
- p_l does not change its sign.

Strum sequence

A Sturm sequence for p allows us to count the number of real zeros of p in an interval.

Sturm's theorem

Assume a square-free (no square factors, i.e., no repeated roots) univariate polynomial

$$p = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x^1 + a_0 x^0 \in \mathbb{Z}[x]$$

with $a_k \neq 0$ and a Sturm sequence $p_0, p_1, \ldots, p_l$ for p. Let furthermore $\sigma(\xi)$ denote the number of sign changes (ignoring zeroes) in the sequence

$$p_0(\xi), p_1(\xi), p_2(\xi), \ldots, p_l(\xi) \ .$$

Then for each $a, b \in \mathbb{R}$ with $a < b$, $p(a) \neq 0$ and $p(b) \neq 0$, the number of distinct real roots of p in (a, b) is $\sigma(a) - \sigma(b)$.

Strum sequence

Computing a Sturm sequence

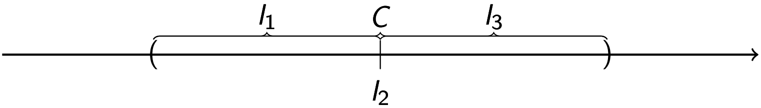
The polynomial sequence $p_0,\ p_1, \ldots, p_l$ with

- $p_0 = p$
- $p_1 = p'$ (where p' is the derivative of p)
- $p_i = -rem(p_{i-2}, p_{i-1})$ for $i = 2, \ldots, l$ (where *rem* is the remainder of the polynomial division of p_0 by p_1)
- $rem(p_{l-1}, p_l) = 0$

is a Sturm sequence for p.

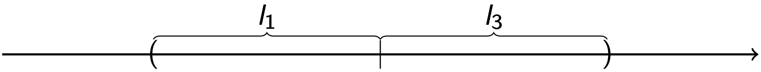
CAD for $\mathbb{R}$: Example

- $\underbrace{x^2 - 2}_{p_1} > 0$
- Cauchy bound: $C = (-3, 3)$
- Sturm sequence: $P_1 = (x^2 - 2, 2x, 2)$
- Number of real roots in $(-3, 3)$: 2
- Split $(-3, 3)$ into $(-3, 0), [0, 0], (0, 3)$
- Number of real roots in $I_1 = (-3, 0)$: 1
- Number of real roots in $I_2 = [0, 0]$: 0
- Number of real roots in $I_3 = (0, 3)$: 1
- CAD: $[(p_1, I_1), (p_1, I_1)]$, $[(p_1, I_3), (p_1, I_3)]$,
  $(-\infty, (p_1, I_1))$, $((p_1, I_1), (p_1, I_3))$, $((p_1, I_3), \infty)$



CAD for $\mathbb{R}$: Example

- $\underbrace{x^2 - 2}_{p_1} > 0 \quad (p_1 = x^2 - 2,\ \sigma_1 = 1)$
- $I_1 = (-3, 0),\ I_3 = (0, 3)$
- CAD: $[(p_1, I_1), (p_1, I_1)],\quad [(p_1, I_3), (p_1, I_3)],$
  $(-\infty, (p_1, I_1)),\quad ((p_1, I_1), (p_1, I_3)),\quad ((p_1, I_3), \infty)$
- Take a sample point from each CAD cell and test the sign conditions.
- $[(p_1, (-3, 0)), (p_1, (-3, 0))]$: sample point $(p_1, (-3, 0))$, sign 0
- $[(p_1, (0, 3)), (p_1, (0, 3))]$: sample point $(p_1, (0, 3))$, sign 0
- $(-\infty, (p_1, (-3, 0)))$: sample point -4, sign 1
- $((p_1, (-3, 0)), (p_1, (0, 3)))$: sample point 0, sign -1
- $((p_1, (0, 3)), \infty)$: sample point 4, sign 1



CAD for $\mathbb{R}$: Incrementality

- The original method is not incremental.
- We achieve incrementality by refining the CAD.
- Previous split: $I_1 = (-3, 0)$, $I_2 = [0, 0]$, $I_3 = (0, 3)$
- New constraint: $\underbrace{x^2 - x - 1}_{p_2} > 0$
- Cauchy bound (maximum for p_1 and p_2): $C_2 = (-3, 3)$
- Sturm sequence: $P_2 = (x^2 - x - 1, 2x - 1, \frac{5}{4})$
- Number of real roots in $I_1 = (-3, 0)$: 1

  $(p_1, I_1) \neq (p_2, I_1) \Rightarrow$ split
- Number of real roots in $I_2 = [0, 0]$: 0
- Number of real roots in $I_3 = (0, 3)$: 1

  $(p_1, I_3) \neq (p_2, I_3) \Rightarrow$ split

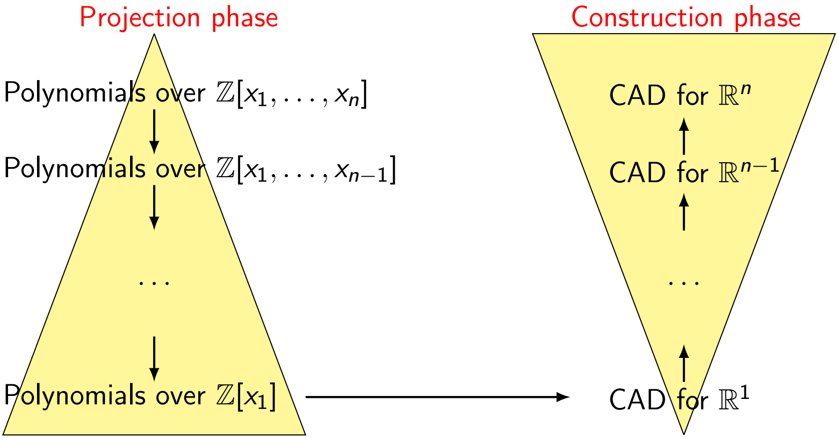
CAD for $\mathbb{R}$: Infeasible subsets

- The original method cannot generate infeasible subsets.
- For $\mathbb{R}$ we collect for each CAD interval one constraint whose sign condition is not satisfied by the interval.
- The case for higher dimensions is more involved, but the basic idea is still similar...

Outline

CAD for $\mathbb{R}^n$

A CAD for a set of polynomials from $\mathbb{Z}[x_1, \ldots, x_n]$ splits $\mathbb{R}^n$ into sign-invariant regions.



Delineability

Let $R \subseteq \mathbb{R}^{n-1}$ be a region and $P = (p_1, \ldots, p_m) \in \mathbb{Z}[x_1, \ldots, x_n]^m$, where $m \geq 1$ and $n \geq 2$.

Intuition: If P is delineable on R then the real roots of P vary continuously over R, while maintaining their order (and are therefore also constant in number).

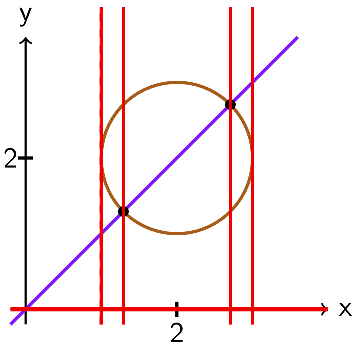
Definition

P is delineable on R if for $1 \leq i, j \leq m$ with $i \neq j$ and for all $a \in R$:

1. the number of roots of $p_i(a)$ is constant,
2. the number of different roots of $p_i(a)$ is constant,
3. the number of common roots of $p_i(a)$ and $p_j(a)$ is constant.

Example: Delineability

$$P = \begin{pmatrix} (x-2)^2 + \\ (y-2)^2 - 1, \\ \\ x - y \end{pmatrix}$$



P-delineable regions:

- $]2 - \frac{\sqrt{2}}{2}, 2 + \frac{\sqrt{2}}{2}[$
- $\{2 - \frac{\sqrt{2}}{2}\}$, $\{2 + \frac{\sqrt{2}}{2}\}$
- $]1, 2 - \frac{\sqrt{2}}{2}[$, $]2 + \frac{\sqrt{2}}{2}, 3[$
- $\{1\}$, $\{3\}$
- $]-\infty, 1[$, $]3, \infty[$

Cylindrical algebraic decomposition

Let $P = (p_1, \ldots, p_m) \in \mathbb{Z}[x_1, \ldots, x_n]^m$ and $\mathcal{C} \subseteq 2^{\mathbb{R}^n}$ finite with $m, n \geq 1$.

Definition

$\mathcal{C}$ is called cylindrical algebraic decomposition (CAD) of $\mathbb{R}^n$ for P if the following holds:

1. $\bigcup \mathcal{C} = \mathbb{R}^n$,
2. $C \cap C' = \emptyset$ for all $C, C' \in \mathcal{C}$ with $C \neq C'$,
3. If $n = 1$, then every $C \in \mathcal{C}$ is a maximal P-sign invariant region.
4. If $n > 1$ and $\mathcal{C}'$ is a cylindrical algebraic decomposition of $\mathbb{R}^{n-1}$ such that any $C' \in \mathcal{C}'$ is P-delineable, then for every $C \in \mathcal{C}$ there is a $C' \in \mathcal{C}'$ such that $C \subseteq C' \times \mathbb{R}$ is a maximal P-sign invariant region in $C' \times \mathbb{R}$.

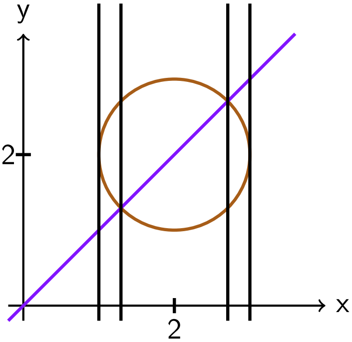
An element $C \in \mathcal{C}$ is called a cell.

Remark

One sample point per cell is sufficient in order to represent a CAD.

Example: CAD with 47 cells

$$P = \begin{pmatrix} (x-2)^2 + \\ (y-2)^2 - 1, \\ \\ x - y \end{pmatrix}$$



P-delineable regions:

- $]2 - \frac{\sqrt{2}}{2}, 2 + \frac{\sqrt{2}}{2}[$
- $\{2 - \frac{\sqrt{2}}{2}\}$, $\{2 + \frac{\sqrt{2}}{2}\}$
- $]1, 2 - \frac{\sqrt{2}}{2}[$, $]2 + \frac{\sqrt{2}}{2}, 3[$
- $\{1\}$, $\{3\}$
- $]-\infty, 1[$, $]3, \infty[$

CAD projection

Let $P = (p_1, \ldots, p_m) \in \mathbb{Z}[x_1, \ldots, x_n]^m$ where $n \geq 2$ and $m, m' \geq 1$.

Definition

A mapping

$$\mathrm{proj} : 2^{\mathbb{Z}[x_1,\ldots,x_n]} \longrightarrow 2^{\mathbb{Z}[x_1,\ldots,x_{n-1}]}$$

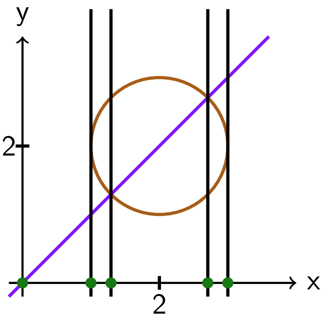
is called a CAD-Projection, if any region $R \subseteq \mathbb{R}^{n-1}$ is $\mathrm{proj}(P)$-sign invariant *iff* R is P-delineable.

Remarks

- Usually, $|\mathrm{proj}(P)| = |P|^2$. Thus, projecting recursively up to the univariate case is in $\mathcal{O}(|P|^{2^{n-1}})$.

Example: CAD projection

$$P = \begin{pmatrix} (x-2)^2 + \\ (y-2)^2 - 1, \\ \\ x - y \end{pmatrix}$$



Projection computed by GiNaCRA	... its real roots
$\mathrm{proj}(P) = \{x^2 - 4x + 3,$	$\{1,\ 3\}$
$-4x + x^2 + \frac{7}{2},$	$\{2 - \frac{\sqrt{2}}{2},\ 2 + \frac{\sqrt{2}}{2}\}$
$x^4 - 8x^3 + 30x^2 - 56x + 49,$	$\{\}$
$x^2 - 4x + 7,$	$\{\}$
$x\}$	$\{0\}$

The CAD sample construction in a nutshell

$\rightarrow P_n \subseteq \mathbb{Z}[x_1, \ldots, x_n]$

↓ eliminate x_n

$P_{n-1} \subseteq \mathbb{Z}[x_1, \ldots, x_{n-1}]$

↓ eliminate x_{n-1}

$\vdots$

↓ eliminate x_2

$P_1 \subseteq \mathbb{Z}[x_1]$

→ roots of P_1

$Z_1 \subseteq \mathbb{R}$

↑ roots of $\{p(z) \mid p \in P_2, z \in Z_1\}$

$Z_1 \times Z_2 \subseteq \mathbb{R}^2$

↑ roots of $\{p(z) \mid p \in P_3, z \in Z_1 \times Z_2\}$

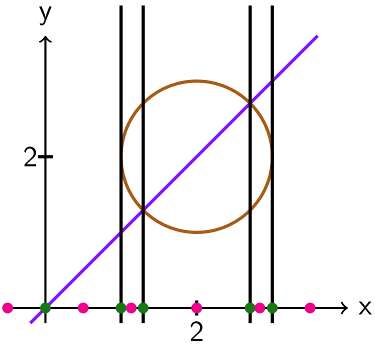
$\vdots$

↑ roots of $\{p(z) | p \in P_n, z \in Z_1 \times \cdots \times Z_{n-1}\}$

$Z_1 \times \cdots \times Z_n \subseteq \mathbb{R}^n$

Example: CAD sample construction

$$P = \begin{pmatrix} (x-2)^2 + \\ (y-2)^2 - 1, \\ \\ x - y \end{pmatrix}$$



Samples for $\mathrm{proj}(P)$:

$\{0, 1, 2 - \frac{\sqrt{2}}{2},\ 2 + \frac{\sqrt{2}}{2},\ 3\}$
$\{-0.5,\ 0.5,\ 1.135,$
$2,\ 2.835,\ 3.5\}$

Example sample constructions

- $(2-2)^2 + (y-2)^2 - 1$ yields $(2,1)$ and $(2,3)$.
- $(2 - \frac{\sqrt{2}}{2} - 2)^2 + (y-2)^2 - 1$ yields $(2 - \frac{\sqrt{2}}{2},\ 2 + \frac{\sqrt{2}}{2})$ and $(2 - \frac{\sqrt{2}}{2},\ 2 + \frac{\sqrt{2}}{2})$.