CS615: Formal Specification and Verification of Programs 2019

Lecture 15: Abstract domains - Polyhedra domain

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2019-10-07

Polyhedral domain

Let us assume $V = \{x_1, \ldots, x_n\}$.

$D = \{AV \leq b | A \in \mathbb{Q}^{m\times n} \wedge b \in \mathbb{Q}^{m\times 1}\}$

D has natural complete lattice structure.

However, there is no canonical representation of polyhedra

We will first discuss the representation to use to implement various operators efficiently.

Exercise 15.1

Define a complete lattice over polyhedra

Dual representation

Representation by constraints:

(A, b) where $A \in \mathbb{Q}^{m \times n}$ and $b \in \mathbb{Q}^{m \times 1}$ representing

$$\gamma((A, b)) = \{v | Av \leq b\}$$

Representation by generators:

(Q, R) where $Q = \{v_1, \ldots, v_p\}$ is a set of vertices and $R = \{r_1, \ldots, r_m\}$ set of rays in $\mathbb{Q}^n$.

$$\gamma((Q, R)) = \{\sum_{i=1}^{p} \lambda_i v_i + \sum_{j=1}^{m} \mu_j r_j | \forall i \in 1..r.\ \mu_i \geq 0 \wedge$$

$$\forall i \in 1..p.\ \lambda_i \geq 0 \wedge \sum_{i=1}^{p} \lambda_i = 1\}$$

Why dual representations?

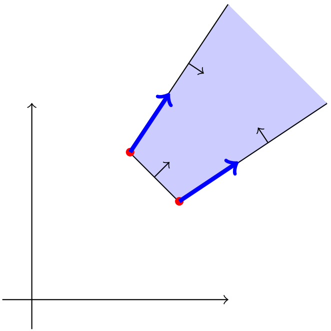
Some operations are efficient if both the representations are available.

Example : dual representation

Example 15.1

Consider the following polyhedron

$$2x - 3y \leq 0 \quad -3x + 2y \leq 0 \quad x + y \geq 25$$



Representation by constraints:

$$(A, b) = \left(\begin{bmatrix} 2 & -3 \\ -3 & 2 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ -25 \end{bmatrix} \right)$$

Representation by generators:

$$(Q, R) = (\{(15, 10), (10, 15)\}, \{(3, 2), (2, 3)\})$$

Some theory of polyhedra

Switch lecture.
Let us learn some theory of polyhedron.

Converting constraints to generators

Chernikova algorithm iteratively computes generators for a polyhedron that is given as $AV \leq b$.

- The algorithm considers inequalities of $AV \leq b$ sequentially.
- At kth iteration, it computes the generators (Q_k, R_k) for the inequalities seen so far.
- After considering all inequalities it has generators for $AV \leq b$.
- Initially, $(Q_0, R_0) := (\{0\}, \{e_1, -e_1 \dots, e_n, -e_n\})$, which spans whole vector space

kth iteration of Chernikova algorithm

Let us suppose $aV \leq c$ is being considered at kth step.

We construct (Q_k, R_k) as follows.

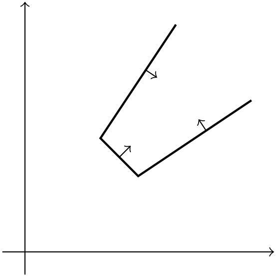
- if $v \in Q_{k-1}$ and $av \leq c$ then $v \in Q_k$
- if $r \in R_{k-1}$ and $ra \leq 0$ then $r \in R_k$
- if $v_1, v_2 \in Q_{k-1}$, $av_1 \leq c$, and $av_2 > c$ then $\frac{c-av_1}{av_2-av_1}v_1 + \frac{av_2-c}{av_2-av_1}v_2 \in Q_k$
- if $v \in Q_{k-1}$ and $r \in R_{k-1}$ such that $av < c$ and $ar > 0$ or $av > c$ and $ar < 0$ then $v + \frac{c-av}{ar}r \in Q_k$
- if $r_1, r_2 \in R_{k-1}$, $ar_1 > 0$, and $ar_2 < 0$ then $(ar_2)r_1 - (ar_1)r_2 \in R_k$

Example: chernikova algorithm

Example 15.2

Consider the following polyhedron

$$2x - 3y \leq 0 \quad -3x + 2y \leq 0 \quad x + y \geq 25$$



$(Q_0, R_0) = (\{(0,0)\}, \{(1,0), (-1,0), (0,1), (0,-1)\})$
Consider $2x - 3y \leq 0$
$(Q_1, R_1) = (\{(0,0)\}, \{(3,2), (-3,-2), (-1,0), (0,1)\})$
Consider $-3x + 2y \leq 0$
$(Q_2, R_2) = (\{(0,0)\}, \{(3,2), (2,3)\})$
Consider $x + y \geq 25$
$(Q_3, R_3) = (\{(10,15), (15,10)\}, \{(3,2), (2,3)\})$

A few points about Chernikova algorithm

- The algorithm generates redundant vertices and rays.
- Worst case blow up 2^m, if the number of constraints is $2m$. Need to remove redundancies during the construction, e.g., Le. Verge algorithm `https://www.researchgate.net/publication/2879547_A_note_on_Chernikova's_Algorithm`
- By duality, this algorithm can be used to convert generators into constraints.

Exercise 15.2

Give the duality construction

Minimal representations

A constraint representation (A, b) is minimal if one can not drop a row from A and b without changing the corresponding polyhedron $\gamma((A, b))$

A generator representation (Q, R) is minimal if one can not drop a vertices or ray from Q and R without changing the corresponding polyhedron $\gamma((A, b))$

We assume that the representations are minimal. However it is not strictly needed in implementing various operations.

Lattice operations in polyhedra

- is $\bot = (Q, R)$: if Q is empty
- $(Q, R) \sqsubseteq (A, b) \triangleq \forall v \in Q.\ Av \leq b \land \forall r \in R.\ Ar \leq 0$
- $(A_1, b_1) \sqcap (A_2, b_2) \triangleq (\begin{bmatrix} A_1 \\ A_2 \end{bmatrix}, \begin{bmatrix} b_1 \\ b_2 \end{bmatrix})$
- $(Q_1, R_1) \sqcup (Q_2, R_2) \triangleq (Q_1 \cup Q_2, R_1 \cup R_2)$
- $sp^{\#}(V' = AV + b, (Q, R)) = (\{Av + b | v \in Q\}, \{Ar | r \in R\})$
- $sp^{\#}(A_2 V \leq b_2 \land V' = V, (A_1, b_1)) = (\begin{bmatrix} A_1 \\ A_2 \end{bmatrix}, \begin{bmatrix} b_1 \\ b_2 \end{bmatrix})$

Both representations are useful for efficient implementations.

Polyhedral widening

Consider polyhedron $L = (A^1, b^1)$ and $M = (A^2, b^2)$.
If L is empty then, $L \triangledown M = M$.
Otherwise, $L \triangledown M = \beta_1 \cup \beta_2$, where

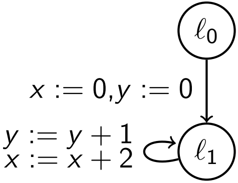
- $\beta_1 \triangleq \{aV \leq c \in L | aV \leq c \text{ contains } M\}$
- $\beta_2 \triangleq \{aV \leq c \in M | \; aV \leq c$ can replace some inequality in L without changing L $\}$

Example: Polyhedral widening

$L = \{(x, y) | 0 \leq x \wedge x \leq y \wedge y \leq x\}$
$M = \{(x, y) | 0 \leq x \wedge x \leq y \wedge y \leq x + 1\}$
$L \triangledown M = \{(x, y) | 0 \leq x \wedge x \leq y\}$

$L = \{(x, y) | 0 \leq x \wedge x \geq 0 \wedge 0 \leq y \wedge y \geq 0\}$
$M = \{(x, y) | 0 \leq y \leq x \leq 1\}$
$L \triangledown M = \{(x, y) | 0 \leq y \leq x\}$

Example: polyhedral domain



$$
\begin{aligned}
X^1_{\ell_1} &= \{0 \leq x \leq 0, 0 \leq y \leq 0\} \\
X^2_{\ell_1} &= X^1_{\ell_1} \nabla (\{0 \leq x \leq 0, 0 \leq y \leq 0\} \sqcup \\
&\qquad\qquad \{1 \leq x \leq 1, 2 \leq y \leq 2\}) \\
&= X^1_{\ell_1} \nabla \{0 \leq x \leq 2, x \leq 2y, x \geq 2y\} \\
&= \{0 \leq x, x \leq 2y, x \geq 2y\}
\end{aligned}
$$

... fixed point reached

Topic 15.1

Problems

Apply Chernikova algorithm

Exercise 15.3

Apply Chernikova algorithm on the following polyhedron

$$\{x - y \leq 0 \land x + y \leq 4 \land 0 \leq x\}$$

Show intermediate steps

End of Lecture 15