Automated Reasoning 2018

Lecture 10: Linear Rational Arithmetic (Background)

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2018-08-18

Reasoning over linear arithmetic

Example 10.1

Consider the following proof step

$$\frac{2x - y \leq 1 \quad 4y - 2x \leq 6}{x + y \leq 5}$$

Is the above proof step complete?

Basic concepts

- Linearly independent
- Rank of a set of vectors
- Vector vs. Row vector
- Hyperplane

Fundamental theorem of linear inequality

Theorem 10.1

Let $a_1, \ldots, a_m, b$ be n-dimensional vectors. Then, one of the following is true.

1. $b := \lambda_1 a_{i_1} + \cdots + \lambda_k a_{i_k}$ *for* $\lambda_j \geq 0$ *and* $a_{i_1}, \ldots, a_{i_k}$ *are linearly independent*
2. *There exists a hyperplane* $\{x | cx = 0\}$ *containing* $t-1$ *linearly independent vectors from* $a_1, \ldots, a_m$ *such that*

$$ca_1 \geq 0, \ldots, ca_m \geq 0 \text{ and } cb < 0,$$

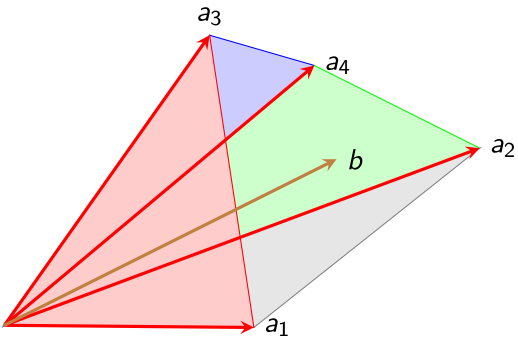
where $t := rank\{a_1, \ldots, a_m, b\}$.

Observation:

- c is a row vector
- Wlog, we assume $t = n$. (why?)
- Both possibilities cannot be true at the same time. (why?)

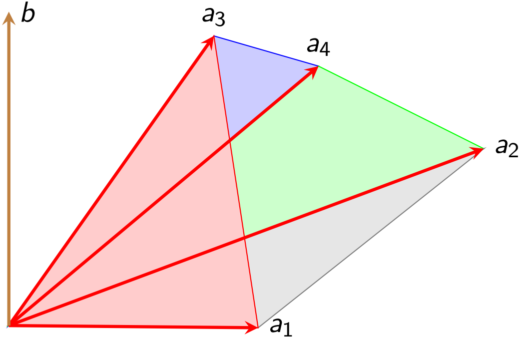
Geometrically, theorem case 1

In the first case, b is in the cone of $a_1, \ldots, a_m$.



Geometrically theorem case 2

In the second case, b is outside of the cone of $a_1, \ldots, a_m$.
Furthermore, $a_1, \ldots, a_m$ are in one side of $\{x | cx = 0\}$ and b is on the other.



Exercise 10.1

Give a c?

Proof: fundamental theorem of linear inequality

Proof.

Consider the following iterative algorithm.

Initially choose n independent vectors $D := \{a_{i_1}, \dots, a_{i_n}\}$ from $a_1, \dots, a_m$.

1. Let $b = \lambda_{i_1} a_{i_1} + \dots + \lambda_{i_n} a_{i_n}$.
2. If $\lambda_{i_1}, \dots, \lambda_{i_n} \geq 0$, case 1 and exit.
3. Otherwise, choose smallest i_h such that $\lambda_{i_h} < 0$.
4. Choose c such that $ca = 0$ for each $a \in D \setminus \{a_{i_h}\}$ and $ca_{i_h} = 1$.
5. If $ca_1, \dots, ca_m \geq 0$, case 2 and exit. (why?)
6. Otherwise, choose smallest s such that $ca_s < 0$.
7. $D := D \setminus \{a_{i_h}\} \cup \{a_s\}$. goto 1.

Clearly, $cb < 0$.(why?)

...

Exercise 10.2

a. Why λs exists in step 1? b. Why c exists in step 4?

c. Why D remains linearly independent over time?

d. Why not simply enumerate all linearly independent subsets from $a_1, ..., a_m$?

Proof: fundamental theorem of linear inequality II

Proof.

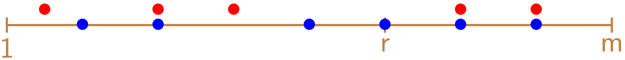
We are yet to prove termination of the algorithm.

Let D^k be the set D at iteration k.

claim: D^k will not repeat in any future iterations. (Therefore, termination.)
Contrapositive: For some $\ell > k$, $D^\ell = D^k$.

Let r be the highest index such that a_r left D at pth iteration and came back at qth iteration for $k \leq p < q \leq \ell$

Therefore, $D^p \cap \{a_{r+1}, \dots, a_m\} = D^q \cap \{a_{r+1}, \dots, a_m\}$ ...



Blue dots are indexes for D^p. Red dots are indexes for D^q.

Proof: fundamental theorem of linear inequality III

Proof.

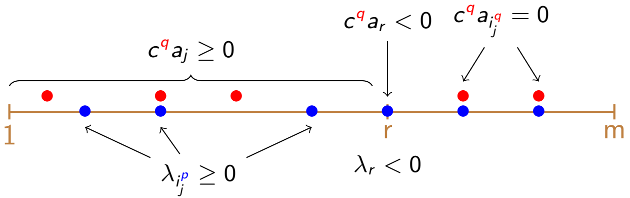
$D^p := \{a_{i_1^p}, \ldots, a_{i_n^p}\}$
Let $b = \lambda_{i_1^p} a_{i_1^p} + \cdots + \lambda_{i_n^p} a_{i_n^p}$.

Since r left D^p,
if $i_j^p < r$, $\lambda_{i_j^p} \geq 0$ and
if $i_j^p = r$, $\lambda_r < 0$.

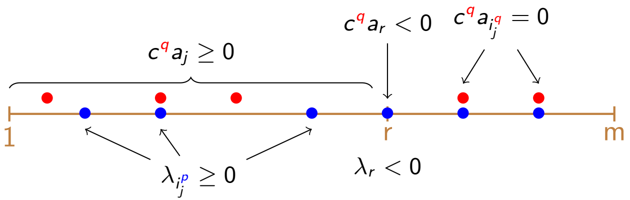
At qth iteration, we have $c^q b < 0$.

Since r entered in D^q,
for each $j < r$, $c^q a_j \geq 0$,
for each $j = r$, $c^q a_r < 0$, and
for each $i_j^q > r$, $c^q a_{i_j^q} = 0$.

…



Proof: fundamental theorem of linear inequality IV



Proof.

Consider

$$0 > c^q b = c^q(\lambda_{i_1^p} a_{i_1^p} + \cdots + \lambda_{i_n^p} a_{i_n^p})$$

Let us show for each j, $\lambda_{i_j^p}(c^q a_{i_j^p})$ is nonnegative.

Three cases

- $i_j^p < r$: $\lambda_{i_j^p} \geq 0$ and $c^q a_{i_j^p} \geq 0$
- $i_j^p = r$: $\lambda_r < 0$ and $c^q a_r < 0$
- $i_j^p > r$: $c^q a_{i_j^p} = 0$(why?)

Therefore, $c^q b \geq 0$. Contradiction. □

Cone,Polyhedra

Definition 10.1

A set C of vectors is a cone if $x, y \in C$ then $\lambda_1 x + \lambda_2 y \in C$ for each $\lambda_1, \lambda_2 \geq 0$.

Definition 10.2

A cone C is a polyhedral if $C = \{x | Ax \leq 0\}$ for some matrix A.

Definition 10.3

A cone C is finitely generated by vectors $x_1, \ldots, x_m$ is the set

$$cone\{x_1, \ldots, x_m\} := \{\lambda_1 x_1 + \cdots + \lambda_m x_m | \lambda_1, \ldots, \lambda_m \geq 0\}$$

Polyhedron, affine half space, polytope

Definition 10.4

A set of vectors P is called polyhedron if

$$P = \{x | Ax \leq b\}$$

for some matrix A and vector b.

Definition 10.5

A set of vectors H is called affine half-space if

$$H = \{x | wx \leq \delta\}$$

for some nonzero row vector w and number δ.

Farkas lemma (version I)

Theorem 10.2

Let A be a matrix and b be a vector. Then, there is a vector $x \geq 0$ such that $Ax = b$ iff

$$\textit{for all } y, \quad yA \geq 0 \Rightarrow yb \geq 0.$$

Proof.

($\Rightarrow$)

Let $x_0 \geq 0$ be such that $Ax_0 = b$.
Therefore, for some row vector y, $yAx_0 = yb$.
Since $x_0 \geq 0$, if $yA \geq 0$ then $yb \geq 0$.

($\Leftarrow$)

Let us suppose there is no such x.
Let $a_1, \dots, a_n$ be columns of A.
Therefore, $b \not\in cone\{a_1, \dots, a_n\}$.(why?)
Due to Theorem 10.1, there is a y such that $yA \geq 0$ and $yb < 0$. □

Farkas lemma (version II)

Theorem 10.3

Let A be a matrix and b be a vector. Then, there is a vector x such that $Ax \leq b$ iff

$$\textit{for all } y, \quad y \geq 0 \wedge yA = 0 \Rightarrow yb \geq 0.$$

Proof.

Consider matrix $A' = [I \;\; A \;\; -A]$.

$A'x' = b$ with $x' \geq 0$ has a solution iff $Ax \leq b$ has.(why?)

Due to theorem 10.2, The left hand side is equivalent to

$$\text{for all } y, \quad y[I \;\; A \;\; -A] \geq 0 \Rightarrow yb \geq 0.$$

Therefore, for all y, $\quad y \geq 0 \wedge yA \geq 0 \wedge -yA \geq 0 \Rightarrow yb \geq 0.$

Therefore, for all y, $\quad y \geq 0 \wedge yA = 0 \Rightarrow yb \geq 0.$ □

Exercise 10.3

Find the relation between solutions of $A'x' = b \wedge x' \geq 0$ and $Ax \leq b$.

Farkas lemma (version III)

Exercise 10.4

Prove that:

Let A be a matrix and b be a vector. Then, there is a vector $x \geq 0$ such that $Ax \leq b$ iff

$$\text{for all } y, \quad y \geq 0 \land yA \geq 0 \Rightarrow yb \geq 0.$$

Linear programming problem

Definition 10.6

Linear programming (LP) is the problem of maximizing or minimizing linear functions over a polyhedron. For example,

$$min\{cx|Ax \leq b\}$$

Duality theorem

Theorem 10.4

Let A be a matrix, and let b and c be vectors. Then,

$$max\{cx|Ax \leq b\} = min\{yb|y \geq 0 \wedge yA = c\}$$

provided both sets are nonempty.

Proof.

claim: *max* will be less than or equal to *min*

Let us suppose $Ax \leq b$, $y \geq 0$, and $yA = c$.

After multiply x in $yA = c$, we obtain $yAx = cx$.

Since $y \geq 0$ and $Ax \leq b$, $yb \geq cx$.

We need to show that the following is nonempty.

$$Ax \leq b \wedge y \geq 0 \wedge yA = c \wedge \underbrace{cx \geq yb}_{\text{makes min and max equal}}$$

...

Duality theorem (contd.)

Proof.

Writing $Ax \leq b \land y \geq 0 \land yA = c \land cx \geq yb$ as follows.

$$\begin{bmatrix} A & 0 \\ 0 & -I \\ 0 & A^T \\ 0 & -A^T \\ -c & b^T \end{bmatrix} \begin{bmatrix} x \\ y^T \end{bmatrix} \leq \begin{bmatrix} b \\ 0 \\ c^T \\ -c^T \\ 0 \end{bmatrix}$$

To show the above is nonempty, we apply theorem 10.3. Now we need to show that for each $u, t, v, w, \lambda \geq 0$

$$uA - \lambda c = 0 \land \lambda b^T + (v - w)A^T - t = 0 \Rightarrow ub + (v - w)c^T \geq 0.$$

After simplifications, we need to show that for each $u, \lambda \geq 0$ and v'

$$uA = \lambda c \land \lambda b^T + v'A^T \geq 0 \Rightarrow ub + v'c^T \geq 0.$$

Duality theorem (contd.)

Proof.

We need to show that for each $u, \lambda \geq 0$ and v'

$$uA = \lambda c \wedge \lambda b^T + v'A^T \geq 0 \Rightarrow ub + v'c^T \geq 0.$$

We assume left hand side and case split on number λ.

case $\lambda > 0$**:**

Consider $\lambda b^T + v'A^T \geq 0 \quad \rightsquigarrow \quad b^T + v'A^T/\lambda \geq 0 \quad \rightsquigarrow \quad b + Av'^T/\lambda \geq 0$
$\rightsquigarrow \quad ub + \lambda cv'^T/\lambda \geq 0 \quad \rightsquigarrow \quad ub + cv'^T \geq 0 \quad \rightsquigarrow \quad ub + v'c^T \geq 0$(why?)

case $\lambda = 0$**:**

Left hand side reduces to $uA = 0 \wedge v'A^T \geq 0$.

claim: $ub \geq 0$

There is a x_0 such that $Ax_0 \leq b$.

Therefore, $ub \geq uAx_0 = 0$.

claim: $v'c^T \geq 0$

There is a y_0 such that $y_0 \geq 0 \wedge y_0 A = c$.

$y_0^T \geq 0 \wedge v'A^T y_0^T = v'c^T$.

Therefore, $v'c^T \geq 0$. □

Emptiness of dual space

Definition 10.7

For an LP problem $max\{cx | Ax \leq b\}$, *the set* $\{y | y \geq 0 \land yA = c\}$ *is called dual space.*

Theorem 10.5

If the dual space of LP problem $max\{cx | Ax \leq b\}$ *is empty. Then, the maximum vaule is unbounded.*

Proof.

Let us suppose the dual space $y \geq 0 \land yA = c$ is empty.
Due to theorem 10.2, there is a z such that

$$Az \geq 0 \land cz < 0.$$

We can use $-z$ to arbitrarily increase the value of cx. Therefore, the max value is unbounded. □

Farkas lemma (Affine version)

Theorem 10.6

Let the system $Ax \leq b$ is nonempty and let c be a row vector and δ be a number. Let us suppose for each x

$$Ax \leq b \Rightarrow cx \leq \delta.$$

Then there exists $\delta' \leq \delta$ such that $cx \leq \delta'$ is a nonnegative linear combination of the inequalities in $Ax \leq b$.

Proof.

Since the max is bounded, the dual space is nonempty and let the max be δ'.

Since both the spaces are nonempty and due to the duality theorem,

$$max\{cx|Ax \leq b\} = min\{yb|y \geq 0 \land yA = c\}$$

Therefore, there exists y_0, such that $y_0 b = \delta' \land y_0 \geq 0 \land y_0 A = c$.(why?)

Therefore, $cx \leq \delta'$ is nonnegative linear combination of $Ax \leq c$.(why?) □

End of Lecture 10