Automated Reasoning 2020

Lecture 13: Linear rational arithmetic (basics)

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2020-10-08

Reasoning over linear arithmetic

Nonnegative linear combination of inequalities derives new inequalities.

Example 13.1

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

One needs to know the following

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

Cone

Definition 13.1

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

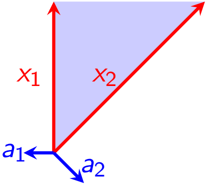
Definition 13.2

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

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

Example 13.2

$$C = \{x | \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} x \leq 0\} = \{\lambda_1 x_1 + \lambda_2 x_2 | \lambda_1, \lambda_2 \geq 0\}$$



Exercise 13.1

Give an example of cone that is not finitely generated.

Topic 13.1

Fundamental theorem of linear inequality

Fundamental theorem of linear inequality

Theorem 13.1

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

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

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

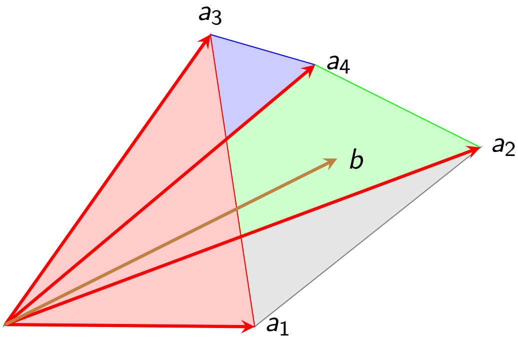
where $t := rank\{a_1, \dots, a_m, b\}$.

Observation:

- c is a row vector
- Wlog, we assume $t = n$.(why?)
- Both possibilities cannot be true at the same time.(why?)
- We are left to prove that both possibilities cannot be false at the same time.

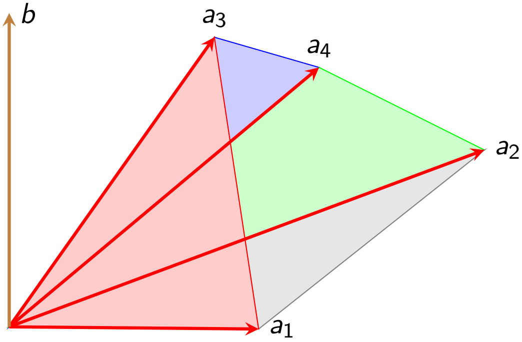
Geometrically, theorem case 1

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 13.2

Give a c?

Proof: fundamental theorem of linear inequality

Proof.

Consider the following iterative algorithm to decide case 1 or 2.
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 $ca_{i_h} = 1$.

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

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.

...

Exercise 13.3

a. *Why does λs exist in step 1?* b. *Why does c exist in step 4?*

c. *Why does D remain linearly independent over time?*

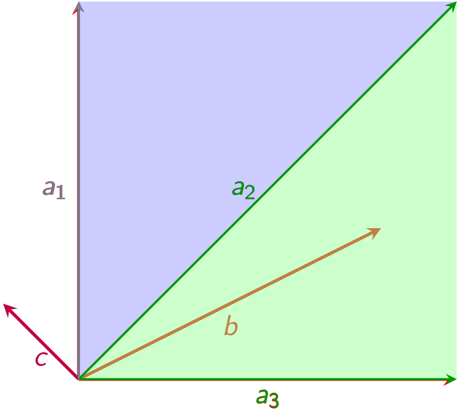
d. *Why not simply enumerate all linearly independent subsets from $a_1, ..., a_m$?*

Example: iterations for D

Example 13.3

Let us have a set of vectors $\{a_1, a_2, a_3\}$ in 2-dimensional vector space and also vector b. We are looking for a subset D that contains b in its cone.

1. Initial guess, $D = \{a_1, a_2\}$.
2. If we write $b = \lambda_1 a_1 + \lambda_2 a_2$, then $\lambda_1 < 0$.
3. Clearly b is not in the cone of D.
4. We get c such that $ca_2 = 0$ and $ca_1 > 0$.
5. Since $cb = c(\lambda_1 a_1 + \lambda_2 a_2) = \lambda_1 ca_1$, $cb < 0$.
6. We find a_3 such that $ca_3 < 0$
   (Intuition: a_3 is likely to be closer to b)
7. Now $D := D \setminus \{a_1\} \cup \{a_3\} = \{a_2, a_3\}$
8. b is in the cone of D. Terminate.



Proof: fundamental theorem of linear inequality II

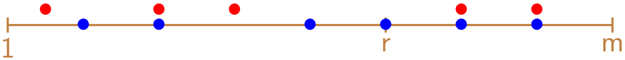
Proof.

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.

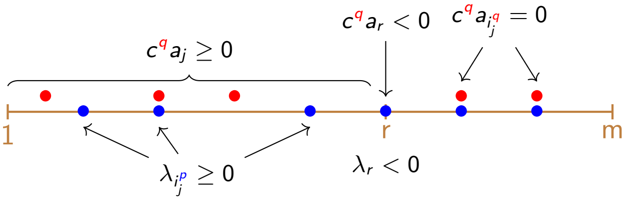
$D^p := \{a_{i_1^p}, \dots, a_{i_n^p}\}$
Let $b = \lambda_{i_1^p} a_{i_1^p} + \dots + \lambda_{i_n^p} a_{i_n^p}$.

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

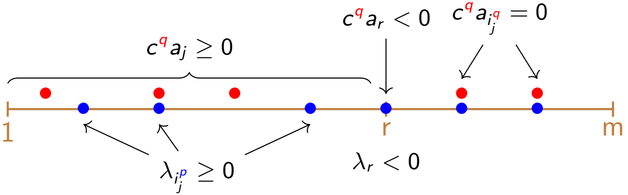
At qth iteration, we have $c^q b < 0$.

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

$\dots$



Proof: fundamental theorem of linear inequality IV



Proof.

Consider

$$0 > c^q b = c^q(\lambda_{i^p_1} a_{i^p_1} + \dots + \lambda_{i^p_n} a_{i^p_n})$$

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

Three cases

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

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

Topic 13.2

Satisfiability conditions

Satisfiability check

Using the previous theorem, we will prove two theorems for the conditions of satisfiability.

The theorem allows us to produce certificate of unsatisfiability.

Nonnegative satisfiability check for equalities

Theorem 13.2

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 all 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 $a_1, \ldots, a_n$ be columns of A. Therefore, $b \notin cone\{a_1, \ldots, a_n\}$.(why?)

Due to Theorem 13.1, there is a y such that $yA \geq 0$ and $yb < 0$. □

Commentary: The theorem is also called Farkas lemma (version I)

Unsatisfiability certificate

If we find y such that $yA \geq 0 \wedge yb < 0$, then $x \geq 0 \wedge Ax = b$ is unsatisfiable.

We may use y as certificate of unsatisfiability.

Example : satisfiability condition and unsatisfiability certificate

Example 13.4

Consider $x_1 + x_2 = 3$.
Therefore, $A = [1 \;\; 1]$ *and* $b = [3]$
Let us apply theorem 13.2, we obtain

$$y[1 \;\; 1] \geq 0 \Rightarrow y[3] \geq 0.$$

After simplification, $y \geq 0 \Rightarrow 3y \geq 0$.

Since the above implication is valid, the equality is satisfiable by some $x_1, x_2 \geq 0$.

Example 13.5

Consider $x_1 + x_2 = -3$.
Therefore, $A = [1 \;\; 1]$ *and* $b = [-3]$
Let us apply theorem 13.2, we obtain

$$y[1 \;\; 1] \geq 0 \Rightarrow y[-3] \geq 0.$$

After simplification, $y \geq 0 \Rightarrow -3y \geq 0$.

Since the above implication does not hold for $y = 1$, *the equality is unsatisfiable for any* $x_1, x_2 \geq 0$.

Exercise 13.4

Show if a_1 *and* a_2 *are non-zero and of opposite sign, then* $a_1x_1 + a_2x_2 = b$ *have nonnegative solution for any* b.

Satisfiability check for inequalities

Theorem 13.3

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 $A' = [\mathtt{I} \;\; A \;\; -A]$. $A'x' = b$ with $x' \geq 0$ has a solution iff $Ax \leq b$ has.(why?)
Due to theorem 13.2, the left hand side is equivalent to

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

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

Exercise 13.5

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

Commentary: The theorem is also called Farkas lemma (version II)

Example: unsatisfiability certificate

Example 13.6

Consider unsatisfiable constraints $x_1 \leq 0 \wedge x_2 \leq 0 \wedge x_1 + x_2 \geq 3$

In the matrix form

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ -1 & -1 \end{bmatrix} \quad b = \begin{bmatrix} 0 \\ 0 \\ -3 \end{bmatrix}$$

For $y = [1 \ \ 1 \ \ 1] \geq 0$, we have $yA = 0$ and $yb = -3 < 0$.

y is the certificate of unsatisfiability.

Topic 13.3

Linear programming and duality

Linear programming problem

Definition 13.3

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

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

Commentary: We will be proving completeness using the property of duality involving linear programming.

Duality condition

Definition 13.4

The following is called LP-duality condition

We will prove the following always holds.

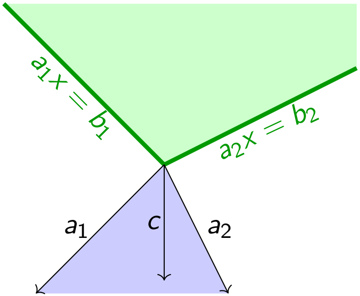
$$max\{cx|Ax \leq b\} = min\{yb|y \geq 0 \wedge yA = c\}.$$

Example 13.7

Consider the green polyhedron with a corner.

max achieves the optima at the corner, if c is in the blue cone.(why?)

c is nonnegative combination of rows of A, i.e., y.



Duality theorem

Theorem 13.4

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

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

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.

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

Duality theorem (contd.)

Proof(contd.) Writing $Ax \leq b \wedge y \geq 0 \wedge yA = c \wedge cx \geq yb$ as follows.

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

To show the above is nonempty, we apply theorem 13.3 and show that for each $u, t, v, w, \lambda \geq 0$

$$\begin{bmatrix} u & t & v & w & \lambda \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & -\mathrm{I} \\ 0 & A^T \\ 0 & -A^T \\ -c & b^T \end{bmatrix} = 0 \quad \Rightarrow \begin{bmatrix} u & t & v & w & \lambda \end{bmatrix} \begin{bmatrix} b \\ 0 \\ c^T \\ -c^T \\ 0 \end{bmatrix} \geq 0$$

Duality theorem(contd.)

Proof(contd.)

After multiplying matrices, we obtain the following implication

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

for each $u, t, v, w, \lambda \geq 0$.

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

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

where $v' = v - w$.

Reduced the number of variables and constraints to analyze

...

Exercise 13.6

a. Why are there no non-negativity constraints on v'?

b. How is t removed?

Duality theorem (contd.)

Proof(contd.)

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 $\lambda b^T + v'A^T \geq 0$

$\rightsquigarrow b^T + v'A^T/\lambda \geq 0$ // divided by λ

$\rightsquigarrow b + Av'^T/\lambda \geq 0$ // take transpose

$\rightsquigarrow ub + uAv'^T/\lambda \geq 0$(why?) // multiply by u

$\rightsquigarrow ub + \lambda cv'^T/\lambda \geq 0$ // use $uA = \lambda c$

$\rightsquigarrow ub + cv'^T \geq 0$

$\rightsquigarrow ub + v'c^T \geq 0$(why?) ...

Duality theorem (contd.)

Proof(contd.)

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

claim: $ub \geq 0$
By assumption, $Ax \leq b$ is sat. Due to theorem 13.3, $uA = 0 \Rightarrow ub \geq 0$.

claim: $v'c^T \geq 0$
By assumption $y \geq 0 \wedge yA = c$ is sat. Therefore, $y^T \geq 0 \wedge A^T y^T = c^T$ is sat.
Due to theorem 13.2, $v'A^T \geq 0 \Rightarrow v'c^T \geq 0$.

Therefore, $ub + v'c^T \geq 0$.

$\square$

Commentary: $\lambda = 0$ case is a trivial case. $\lambda = 0$ indicates that $cx \geq yb$ in $Ax \leq b \wedge y \geq 0 \wedge yA = c \wedge cx \geq yb$ is being ignored for the search contradictory linear combination. Then the satisfiability question reduces into two separate problems, which are satisfiable by assumption. The above calculation plays out this intuition.

Emptiness of dual space

Definition 13.5

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

Theorem 13.5

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

Proof.

Let us suppose the dual space $y \geq 0 \wedge yA = c$ is empty.
Due to theorem 13.2, there is a z such that

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

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

$\square$

Topic 13.4

Implication completeness

Farkas lemma (Affine version)

Theorem 13.6

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,

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

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

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

Topic 13.5

Problems

Replace more vectors in each iteration

Exercise 13.7

We replace one vector at a time in the fundamental theorem of linear inequalities. Can we replace two vectors in some iterations? Give conditions when this is possible.

Exercise: Farkas lemmas variations

Exercise 13.8

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

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

Exercise 13.9

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

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

Strict inequalities

Exercise 13.10

Modify theorems 13.1, 13.2, and 13.3 to support strict inequalities in theorem 13.3.

Topic 13.6

Extra slides: Cone, Polyhedra, Polytope, Polyhedron

Polyhedra == finitely generated cone

Definition 13.6

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

Theorem 13.7

A convex cone is polyhedral iff it is finitely generated.

Proof.

Intuitively, obvious.

We are skipping the proof here. □

Polyhedron, affine half space, polytope

Definition 13.7

A set of vectors P is called polyhedron if

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

for some matrix A and vector b.

Definition 13.8

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.

Polytope

Definition 13.9

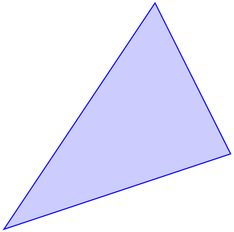
A set of vectors Q is called polytope if

$$Q = hull(\{x_1, .., x_m\}) = \{\lambda_1 x_1 + \cdots + \lambda_m x_m | \lambda_1 + \cdots + \lambda_m = 1 \land \lambda_1, \ldots, \lambda_m \geq 0\}$$

for some nonzero vectors $x_1, \ldots, x_m$.

Example 13.8

The following is $hull(\{(2,3),(0,0),(3,1)\})$



polyhedron = polytope + polyhedral

Theorem 13.8 (Decomposition theorem)

Let $P = \{x | Ax \leq b\}$ be a polyhedron iff $P = Q + C$ for some polytope Q and polyhedral C.

Proof.

Let us consider the forward direction.

Let us construct the following cone in one higher dimension.

$$P' = \{ \begin{bmatrix} x \\ \lambda \end{bmatrix} | Ax - \lambda b \leq 0 \wedge \lambda \geq 0\}$$

Clearly, the following holds

$$x \in P \qquad \text{iff} \qquad \begin{bmatrix} x \\ 1 \end{bmatrix} \in P'$$

Exercise 13.11

Prove the reverse direction

...

polyhedron = polytope + polyhedral (contd.)

Proof(contd.)

Let the following $q + c$ vectors generate P'.(why exists?)

$$\underbrace{\begin{bmatrix} x_1 \\ 1 \end{bmatrix} \dots \begin{bmatrix} x_q \\ 1 \end{bmatrix}}_{q}, \underbrace{\begin{bmatrix} y_1 \\ 0 \end{bmatrix} \dots \begin{bmatrix} y_c \\ 0 \end{bmatrix}}_{c}$$

Let $Q = hull(\{x_1, ...x_q\})$ and $C = cone(\{y_1, ..., y_c\})$

claim: $P = Q + C$

Let $x \in P \Leftrightarrow$ By definition of P', for some $\mu_1, ..\mu_q, \lambda_1, ...\lambda_c \geq 0$ the following holds.

$$\begin{bmatrix} x \\ 1 \end{bmatrix} = \mu_1 \begin{bmatrix} x_1 \\ 1 \end{bmatrix} + \dots + \mu_q \begin{bmatrix} x_q \\ 1 \end{bmatrix} + \lambda_1 \begin{bmatrix} y_1 \\ 0 \end{bmatrix} + \dots + \lambda_c \begin{bmatrix} y_c \\ 0 \end{bmatrix}.$$

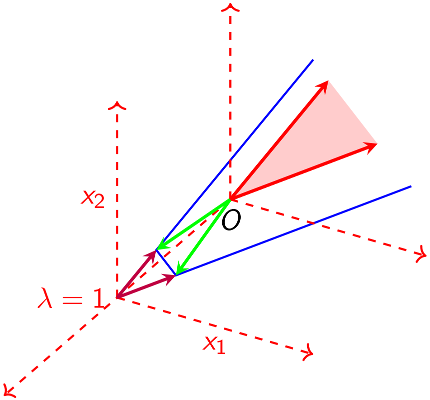
$\Leftrightarrow \mu_1 x_1 + ...\mu_q x_q \in Q$, $\mu_1 + ... + \mu_q = 1$, and $\lambda_1 y_1 + \dots + \lambda_c y_c \in C$(why?) $\square$

Example: $P = Q + C$

Example 13.9

Consider the following polyhedron P.

1. Green + red vectors are generators of P'
2. Red vectors have no λ component, they form the cone C
3. Green vectors have $\lambda = 1$.
4. Projecting green vectors on x_1 and x_2 plane we get purple vectors.
5. Q is the hull of the purple vectors



End of Lecture 13