Linear arithmetic theories:
algorithms and applications

Christoph Haase   Alessio Mansutti

ESSLLI 2023

This course

Goals:

- Introduction to logical, algorithmic and geometric aspects of arithmetic theories
- Showcase how arithmetic theories can be approached with different techniques (formal logic, automata theory and geometry)

Content:

- Classical algorithms and decision procedures
- Geometric description of the sets definable in arithmetic theories
- Recent research developments

Course overview

Monday	Introduction to linear arithmetic
Tuesday	Linear Programming and Integer Linear Programming
Wednesday	Quantifier elimination procedures
Thursday	Automata-based procedures
Friday	Geometric procedures

Required background

Basic familiarity with following topics is helpful:

- Mathematical logic
- Linear algebra
- Automata theory
- Algorithms and computational complexity

Today's lecture

Introduction to linear arithmetic:

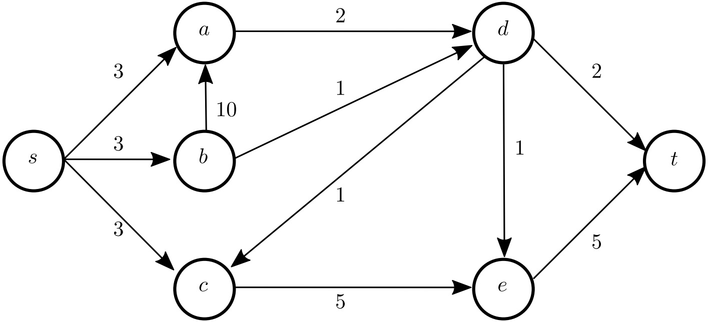
- Applications of arithmetic theories
- Syntax, semantics, normal forms

Convex geometry:

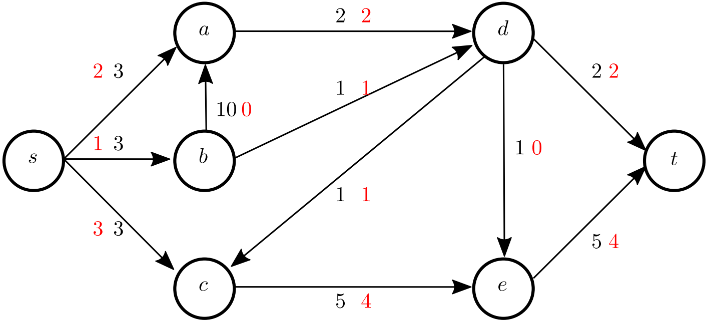
- Basic notions: hyperplanes, (convex) cones and polyhedra, hulls, ...
- Farkas' Lemma
- Minkowski-Weyl Theorem

Applications of arithmetic theories

Maximum flow



Maximum flow



Maximum flow

Directed weighted graph $G = (V, E, w)$ such that $w\colon E \to \mathbb{R}$:

- w assigns maximum flow capacity to edges in G
- flow is function $f\colon E \to \mathbb{R}$
- value of flow is sum of flow leaving s
- goal: find flow with maximum value

Maximum flow

Directed weighted graph $G = (V, E, w)$ such that $w \colon E \to \mathbb{R}$:

- w assigns maximum flow capacity to edges in G
- flow is function $f \colon E \to \mathbb{R}$
- value of flow is sum of flow leaving s
- goal: find flow with maximum value

For edge $e \in E$, introduce variables f_e encoding flow conditions:

$$\bigwedge_{e \in E} 0 \leq f_e \leq w(e) \qquad \wedge \qquad \bigwedge_{v \in V \setminus \{s,t\}} \sum_{(u,v) \in E} f_{u,v} = \sum_{(v,u) \in E} f_{v,u}$$

Maximum flow

Directed weighted graph $G = (V, E, w)$ such that $w \colon E \to \mathbb{R}$:

- w assigns maximum flow capacity to edges in G
- flow is function $f \colon E \to \mathbb{R}$
- value of flow is sum of flow leaving s
- goal: find flow with maximum value

For edge $e \in E$, introduce variables f_e encoding flow conditions:

$$\text{maximize} \sum_{(s,v) \in E} f_{s,v}$$

$$\bigwedge_{e \in E} 0 \leq f_e \leq w(e) \qquad \wedge \qquad \bigwedge_{v \in V \setminus \{s,t\}} \sum_{(u,v) \in E} f_{u,v} = \sum_{(v,u) \in E} f_{v,u}$$

The Frobenius problem

Given coins in denominations

$$m_1 < \cdots < m_k \in \mathbb{N},$$

what is the largest value c that cannot be generated? Does such a c exist?

The Frobenius problem

Given coins in denominations

$$m_1 < \cdots < m_k \in \mathbb{N},$$

what is the largest value c that cannot be generated? Does such a c exist?

$$n \;=\; m_1 \cdot x_1 + \cdots + m_k \cdot x_k$$

The Frobenius problem

Given coins in denominations

$$m_1 < \cdots < m_k \in \mathbb{N},$$

what is the largest value c that cannot be generated? Does such a c exist?

$$\exists x_1 \exists x_2 \cdots \exists x_k \ : \ n = m_1 \cdot x_1 + \cdots + m_k \cdot x_k$$

The Frobenius problem

Given coins in denominations

$$m_1 < \cdots < m_k \in \mathbb{N},$$

what is the largest value c that cannot be generated? Does such a c exist?

$$\forall n \;:\; c < n \;\rightarrow\; \exists x_1 \exists x_2 \cdots \exists x_k \;:\; n = m_1 \cdot x_1 + \cdots + m_k \cdot x_k$$

The Frobenius problem

Given coins in denominations

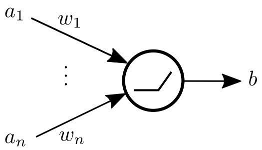
$$m_1 < \cdots < m_k \in \mathbb{N},$$

what is the largest value c that cannot be generated? Does such a c exist?

$$\exists c \ : \ \forall n \ : \ c \ < \ n \ \rightarrow \ \exists x_1 \exists x_2 \cdots \exists x_k \ : \ n \ = \ m_1 \cdot x_1 + \cdots + m_k \cdot x_k$$

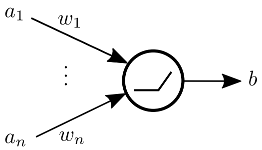
Artificial neural networks

Artificial neuron:



Artificial neural networks

Artificial neuron:

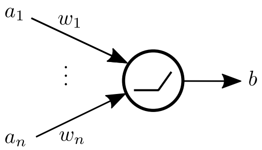


Ouput:

$$b = \begin{cases} 0 & \text{if } \sum_{i=1}^{n} w_i \cdot a_i < 0 \\ \sum_{i=1}^{n} w_i \cdot a_i & \text{otherwise} \end{cases}$$

Artificial neural networks

Artificial neuron:



Ouput:

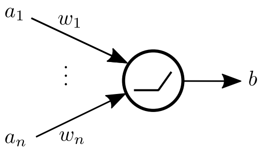
$$b = \begin{cases} 0 & \text{if } \sum_{i=1}^{n} w_i \cdot a_i < 0 \\ \sum_{i=1}^{n} w_i \cdot a_i & \text{otherwise} \end{cases}$$

In logic for $\boldsymbol{w} \in \mathbb{R}^n$

$$\Phi_{\boldsymbol{w}}(\boldsymbol{x}, y) := (\boldsymbol{w}^\mathsf{T} \cdot \boldsymbol{x} < 0 \to y = 0) \wedge (\boldsymbol{w}^\mathsf{T} \cdot \boldsymbol{x} \geq 0 \to y = \boldsymbol{w}^\mathsf{T} \cdot \boldsymbol{x})$$

Artificial neural networks

Artificial neuron:



Ouput:

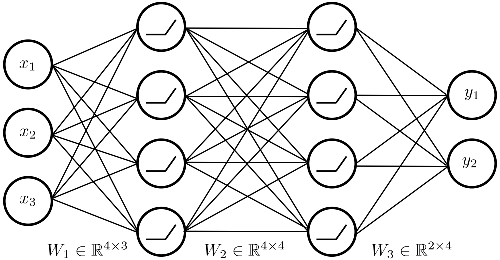
$$b = \begin{cases} 0 & \text{if } \sum_{i=1}^{n} w_i \cdot a_i < 0 \\ \sum_{i=1}^{n} w_i \cdot a_i & \text{otherwise} \end{cases}$$

In logic for $\boldsymbol{w} \in \mathbb{R}^n$ and $W \in \mathbb{R}^{m \times n}$:

$$\Phi_{\boldsymbol{w}}(\boldsymbol{x}, y) := (\boldsymbol{w}^\intercal \cdot \boldsymbol{x} < 0 \to y = 0) \wedge (\boldsymbol{w}^\intercal \cdot \boldsymbol{x} \geq 0 \to y = \boldsymbol{w}^\intercal \cdot \boldsymbol{x})$$

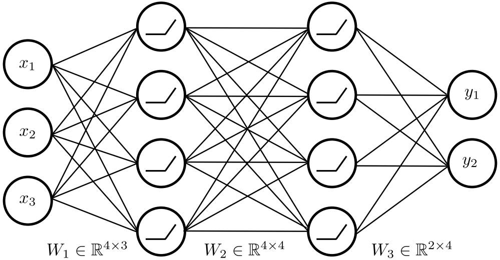
$$\Phi_W(\boldsymbol{x}, \boldsymbol{y}) := \bigwedge_{1 \leq i \leq m} \Phi_{\boldsymbol{w}_i}(\boldsymbol{x}, y_i) \quad \text{where } W = \begin{pmatrix} \boldsymbol{w}_1 \\ \vdots \\ \boldsymbol{w}_m \end{pmatrix}$$

Artificial neural networks



$$\Phi(\boldsymbol{x}, \boldsymbol{y}) = \exists z_1 \exists z_2 : \Phi_{W_1}(\boldsymbol{x}, \boldsymbol{z}_1) \wedge \Phi_{W_2}(\boldsymbol{z}_1, \boldsymbol{z}_2) \wedge \Phi_{W_3}(\boldsymbol{z}_2, \boldsymbol{y})$$

Artificial neural networks

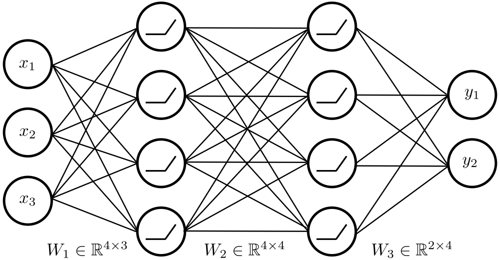


$$\Phi(\boldsymbol{x}, \boldsymbol{y}) = \exists z_1 \exists z_2 : \Phi_{W_1}(\boldsymbol{x}, \boldsymbol{z}_1) \wedge \Phi_{W_2}(\boldsymbol{z}_1, \boldsymbol{z}_2) \wedge \Phi_{W_3}(\boldsymbol{z}_2, \boldsymbol{y})$$

All inputs giving output $(1, 0)$:

$$\left\{\boldsymbol{r} = (r_1, r_2, r_3) \in \mathbb{R}^3 : \Phi[\boldsymbol{r}/\boldsymbol{x}, (1,0)/\boldsymbol{y}] \text{ is true}\right\}$$

Artificial neural networks



$$\Phi(\boldsymbol{x}, \boldsymbol{y}) = \exists z_1 \exists z_2 : \Phi_{W_1}(\boldsymbol{x}, \boldsymbol{z}_1) \wedge \Phi_{W_2}(\boldsymbol{z}_1, \boldsymbol{z}_2) \wedge \Phi_{W_3}(\boldsymbol{z}_2, \boldsymbol{y})$$

All inputs giving output $(1, 0)$:

$$\{\boldsymbol{r} = (r_1, r_2, r_3) \in \mathbb{R}^3 : \Phi[\boldsymbol{r}/\boldsymbol{x}, (1,0)/\boldsymbol{y}] \text{ is true}\}$$

Artificial neuron network outputs probability distribution:

$$\forall x_1 \forall x_2 \forall x_3 \forall y_1 \forall y_2 : \Phi(\boldsymbol{x}, \boldsymbol{y}) \to (y_1 + y_2 = 1 \wedge 0 \le y_1 \wedge 0 \le y_2)$$

Twin prime conjecture

There are infinitely many primes p such that $p + 2$ is also prime:

Twin prime conjecture

There are infinitely many primes p such that $p+2$ is also prime:

$$\forall n \exists p : n < p \land \Phi_{\mathsf{prime}}(p) \land \Phi_{\mathsf{prime}}(p+2)$$

Twin prime conjecture

There are infinitely many primes p such that $p + 2$ is also prime:

$$\forall n \exists p : n < p \wedge \Phi_{\mathsf{prime}}(p) \wedge \Phi_{\mathsf{prime}}(p+2)$$

$$\Phi_{\mathsf{prime}}(x) := x > 1 \wedge \forall y \forall z : x = y \cdot z \rightarrow (y = 1 \vee y = x)$$

What do we want from arithmetic theories?

problem	domain	arithmetic functions	relations	Boolean connectives	quantifiers
max-flow	$\mathbb{R}$	$+$	$=, \leq$	$\wedge$	$\exists$
Frobenius	$\mathbb{N}$	$+$	$=, <$	$\wedge, \rightarrow$	$\exists\forall\exists$
ANN	$\mathbb{R}$	$+$	$=, <$	$\wedge, \rightarrow$	$\forall\exists$
twin primes	$\mathbb{N}$	$+, \cdot$	$=, <$	$\wedge, \vee, \rightarrow$	$\forall\exists$

What do we want from arithmetic theories?

problem	domain	arithmetic functions	relations	Boolean connectives	quantifiers
max-flow	$\mathbb{R}$	$+$	$=, \leq$	$\wedge$	$\exists$
Frobenius	$\mathbb{N}$	$+$	$=, <$	$\wedge, \rightarrow$	$\exists\forall\exists$
ANN	$\mathbb{R}$	$+$	$=, <$	$\wedge, \rightarrow$	$\forall\exists$
twin primes	$\mathbb{N}$	$+, \cdot$	$=, <$	$\wedge, \vee, \rightarrow$	$\forall\exists$

Problems of interest:

- Validity: Is a given formula true?
- Satisfiability: Does a satisfying assignment exist?
- Optimization: Maximize an objective function.
- Geometry: Properties of sets definable in arithmetic theories.

Syntax and semantics of linear arithmetic theories

Syntax

- $x, y, z, x_1, \ldots, x_n \in X$ are first-order variables
- Atomic formulas, where $a_1, \ldots, a_n, b \in \mathbb{Z}$:

$$a_1 \cdot x_1 + \cdots + a_n \cdot x_n = b, \qquad \sum_{i=1}^{n} a_i \cdot x_i \leq b, \qquad \boldsymbol{a}^\intercal \cdot \boldsymbol{x} \sim b$$

- Boolean connectives:

$$\neg \qquad \wedge \qquad \vee \qquad \rightarrow$$

- Quantifiers:

$$\exists x : \Phi(x) \qquad \forall x : \Phi(x)$$

Linear arithmetic theories: semantics

Domain of variables are reals ($\mathbb{R}$) or integers ($\mathbb{Z}$), or subsets thereof. Write $\mathbb{D}$ for arbitrary domain.

Linear arithmetic theories: semantics

Domain of variables are reals ($\mathbb{R}$) or integers ($\mathbb{Z}$), or subsets thereof. Write $\mathbb{D}$ for arbitrary domain. Assignments are mappings $\mathcal{A}\colon X \to \mathbb{D}$.

Linear arithmetic theories: semantics

Domain of variables are reals ($\mathbb{R}$) or integers ($\mathbb{Z}$), or subsets thereof. Write $\mathbb{D}$ for arbitrary domain. Assignments are mappings $\mathcal{A}\colon X \to \mathbb{D}$. Semantics:

- $\mathcal{A} \models \sum_{i=1}^{n} a_i \cdot x_i \sim b \iff \sum_{i=1}^{n} a_i \cdot \mathcal{A}(x_i) \sim b$
- $\mathcal{A} \models \neg\Phi \iff \mathcal{A} \not\models \Phi$
- $\mathcal{A} \models \Phi \wedge \Psi \iff \mathcal{A} \models \Phi$ and $\mathcal{A} \models \Psi$
- $\mathcal{A} \models \Phi \vee \Psi \iff \mathcal{A} \models \Phi$ or $\mathcal{A} \models \Psi$
- $\mathcal{A} \models \Phi \to \Psi \iff \mathcal{A} \models \neg\Phi$ or $\mathcal{A} \models \Psi$
- $\mathcal{A} \models \exists x : \Phi(x) \iff$ there is $a \in \mathbb{D}$ such that $\mathcal{A} \models \Phi[a/x]$
- $\mathcal{A} \models \forall x : \Phi(x) \iff$ for all $a \in \mathbb{D}$, $\mathcal{A} \models \Phi[a/x]$

Simplifying formulas (1)

- Can assume negation-free formulas:

$$\begin{aligned}\neg(a = b) &\iff a < b \lor b < a \\ \neg(a < b) &\iff b \leq a \\ \neg(a \leq b) &\iff b < a\end{aligned}$$

- Equality not needed:

$$a = b \iff a \leq b \land b \leq a$$

- Over $\mathbb{Z}$ only one of $\leq$ and $<$ needed:

$$a < b \iff a + 1 \leq b$$

Simplifying formulas (2)

Prenex form:

$$Q_1 x_1\, Q_2 x_2 \cdots Q_k x_k : \Phi(x_1, \ldots, x_k) \text{ and } \Phi \text{ is quantifier-free}$$

Simplifying formulas (2)

Prenex form:

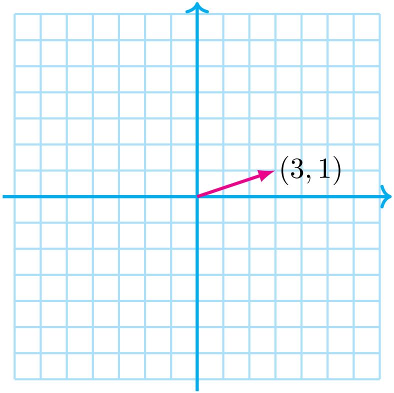
$$Q_1 x_1\, Q_2 x_2 \cdots Q_k x_k : \Phi(x_1, \ldots, x_k) \text{ and } \Phi \text{ is quantifier-free}$$

Can wlog assume formula to be in prenex form:

- push negations in front of atomic formulas
- apply equivalences from previous slide to remove negation
- ensure no two quantifiers refer to the same variable
- pull quantifiers outwards

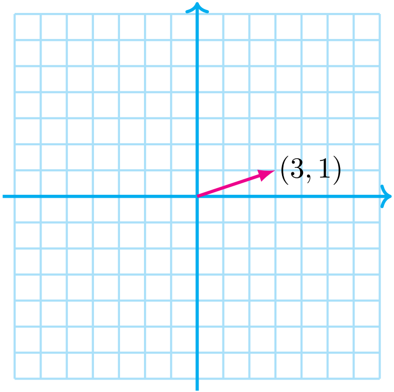
Convex geometry

Hyperplanes



Two vectors $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^d$ are orthogonal whenever $\boldsymbol{v}^\intercal \cdot \boldsymbol{w} = 0$.

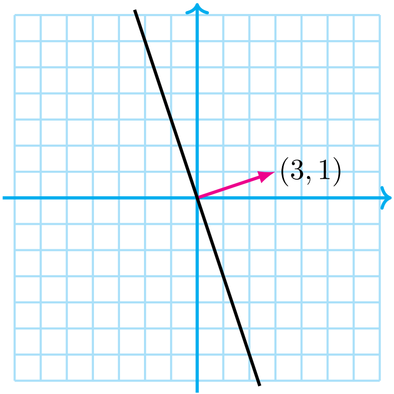
Hyperplanes



Two vectors $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^d$ are orthogonal whenever $\boldsymbol{v}^\intercal \cdot \boldsymbol{w} = 0$.

What is the set of vectors/points orthogonal to a non-zero vector $\boldsymbol{v} \in \mathbb{R}^d$?

Hyperplanes

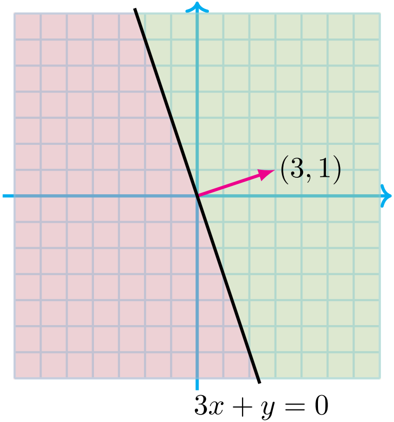


Two vectors $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^d$ are orthogonal whenever $\boldsymbol{v}^\mathsf{T} \cdot \boldsymbol{w} = 0$.

What is the set of vectors/points orthogonal to a non-zero vector $\boldsymbol{v} \in \mathbb{R}^d$?

$$H := \left\{ \boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{v}^\mathsf{T} \cdot \boldsymbol{x} = 0 \right\} \leftarrow \text{a hyperplane!}$$

Hyperplanes



Two vectors $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^d$ are orthogonal whenever $\boldsymbol{v}^\intercal \cdot \boldsymbol{w} = 0$.

What is the set of vectors/points orthogonal to a non-zero vector $\boldsymbol{v} \in \mathbb{R}^d$?

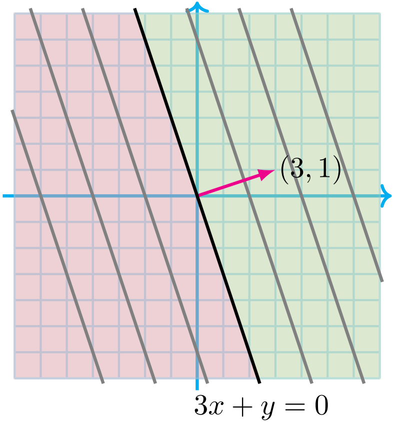
$$H := \left\{ \boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{v}^\intercal \cdot \boldsymbol{x} = 0 \right\}$$ $\leftarrow$ a hyperplane!

$H^+ := \left\{ \boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{v}^\intercal \cdot \boldsymbol{x} \geq 0 \right\}$ and

$H^- := \left\{ \boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{v}^\intercal \cdot \boldsymbol{x} \leq 0 \right\}$ are its half-spaces

($\boldsymbol{v}$ is always in H^+)

Hyperplanes



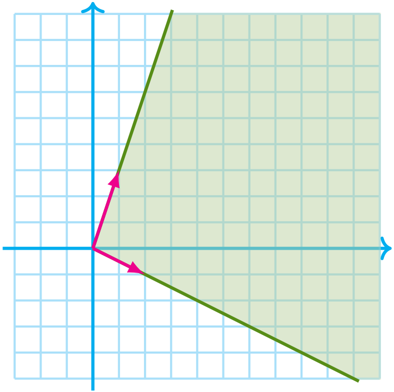
$$H := \left\{ \boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{v}^\mathsf{T} \cdot \boldsymbol{x} = 0 \right\} \leftarrow \text{hyperplane}$$

Given $c \in \mathbb{Z} \setminus \{0\}$,

$$H_c := \left\{ \boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{v}^\mathsf{T} \cdot \boldsymbol{x} = c \right\} \leftarrow \text{affine hyperplane!}$$

If $c > 0$ then $H_c \subseteq H^+$ else $H_c \subseteq H^-$

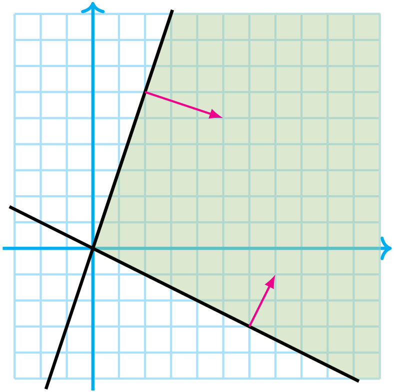
(Polyhedral) cones



$$\mathbf{C} \coloneqq \left\{ A \cdot \boldsymbol{\lambda} : \boldsymbol{\lambda} \in \mathbb{R}^d \text{ and } \boldsymbol{\lambda} \geq \mathbf{0} \right\} \leftarrow \text{a cone!}$$

We denote this set by $\operatorname{cone}(A)$.

(Polyhedral) cones



$$\mathbf{C} := \left\{ A \cdot \boldsymbol{\lambda} : \boldsymbol{\lambda} \in \mathbb{R}^d \text{ and } \boldsymbol{\lambda} \geq \mathbf{0} \right\}$$ $\leftarrow$ a cone!

We denote this set by $\mathrm{cone}(A)$.

Equivalently,

$$\mathbf{C} := \left\{ \boldsymbol{x} \in \mathbb{R}^d : B \cdot \boldsymbol{x} \geq \mathbf{0} \right\}$$ $\leftarrow$ also a cone!

Farkas' lemma

Lemma (Farkas; 1902)

Let $A \in \mathbb{R}^{m \times d}$ and $\boldsymbol{b} \in \mathbb{R}^m$. Exactly one of the following two assertions holds:

1. *There is $\boldsymbol{x} \in \mathbb{R}^d$ such that $A \cdot \boldsymbol{x} = \boldsymbol{b}$ and $\boldsymbol{x} \geq \mathbf{0}$.*
2. *There is $\boldsymbol{v} \in \mathbb{R}^m$ such that $\boldsymbol{v}^\intercal \cdot A \geq \mathbf{0}$ and $\boldsymbol{v}^\intercal \cdot \boldsymbol{b} < 0$.*

Farkas' lemma

Lemma (Farkas; 1902)

Let $A \in \mathbb{R}^{m \times d}$ and $\boldsymbol{b} \in \mathbb{R}^m$. Exactly one of the following two assertions holds:

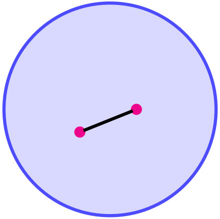
1. *There is $\boldsymbol{x} \in \mathbb{R}^d$ such that $A \cdot \boldsymbol{x} = \boldsymbol{b}$ and $\boldsymbol{x} \geq \mathbf{0}$.*
2. *There is $\boldsymbol{v} \in \mathbb{R}^m$ such that $\boldsymbol{v}^\intercal \cdot A \geq \mathbf{0}$ and $\boldsymbol{v}^\intercal \cdot \boldsymbol{b} < 0$.*

Proof.

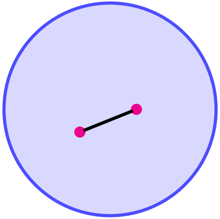
Either $\boldsymbol{b}$ belongs to $\mathrm{cone}(A) = \{A \cdot \boldsymbol{\lambda} : \boldsymbol{\lambda} \in \mathbb{R}^d \text{ and } \boldsymbol{\lambda} \geq \mathbf{0}\}$ or there is a hyperplane separating $\mathrm{cone}(A)$ from $\boldsymbol{b}$. The former case implies (1), the latter implies (2). ■

Convex sets and convex hulls

A set $S \subseteq \mathbb{R}^d$ is convex whenever $[x, y] \subseteq S$ for every $x, y \in S$



Convex sets and convex hulls



A set $S \subseteq \mathbb{R}^d$ is convex whenever $[x, y] \subseteq S$ for every $x, y \in S$

For $S \subseteq \mathbb{R}^d$, the convex hull $\operatorname{conv}(S)$ of S is:

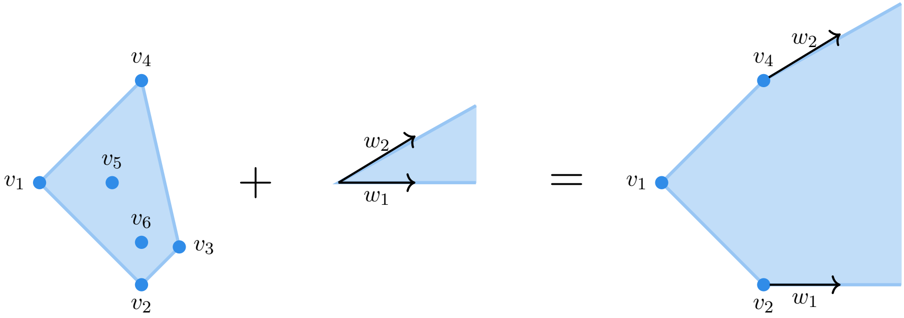
- the (unique) smallest convex set containing S, or
- the intersection of all convex sets containing S, or
- the set of all convex combinations of elements of S:

$$\operatorname{conv}(S) := \left\{ \lambda_1 \boldsymbol{v}_1 + \ldots + \lambda_n \boldsymbol{v}_n : \boldsymbol{v}_1, \ldots \boldsymbol{v}_n \in S,\ \sum_{i=1}^{n} \lambda_i = 1 \text{ and } \lambda_1, \ldots, \lambda_n \geq 0 \right\}.$$

Convex polyhedra

A set S is a polyhedron if:

- $S = \{\boldsymbol{x} \in \mathbb{R}^d : A \cdot \boldsymbol{x} \geq \boldsymbol{b}\}$ for some matrix $A \in \mathbb{Q}^{n \times d}$ and vector $\boldsymbol{b} \in \mathbb{Q}^d$, **or**
- $S = \mathrm{conv}(V) + \mathrm{cone}(W)$ for some finite sets $V, W \subseteq \mathbb{Q}^d$.



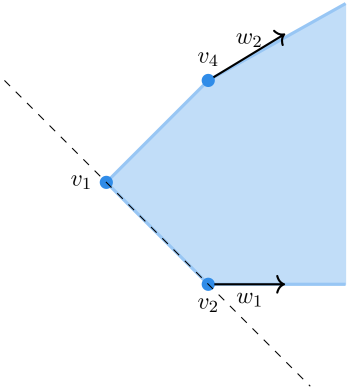
conv$\{v_1, \ldots, v_6\}$ cone$\{w_1, w_2\}$

Convex polyhedra

A set S is a polyhedron if:

- $S = \{\boldsymbol{x} \in \mathbb{R}^d : A \cdot \boldsymbol{x} \geq \boldsymbol{b}\}$ for some matrix $A \in \mathbb{Q}^{n \times d}$ and vector $\boldsymbol{b} \in \mathbb{Q}^d$, **or**
- $S = \mathrm{conv}(V) + \mathrm{cone}(W)$ for some finite sets $V, W \subseteq \mathbb{Q}^d$.

H is a supporting hyperplane of S whenever $S \cap H \neq \varnothing$ and $S \subseteq H^+$.



Convex polyhedra

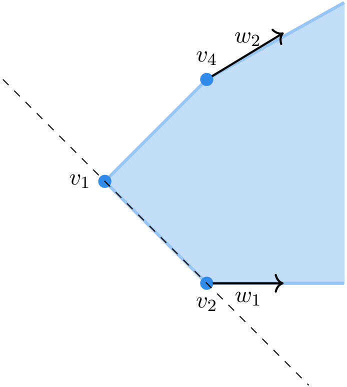
A set S is a polyhedron if:

- $S = \{\boldsymbol{x} \in \mathbb{R}^d : A \cdot \boldsymbol{x} \geq \boldsymbol{b}\}$ for some matrix $A \in \mathbb{Q}^{n \times d}$ and vector $\boldsymbol{b} \in \mathbb{Q}^d$, **or**
- $S = \operatorname{conv}(V) + \operatorname{cone}(W)$ for some finite sets $V, W \subseteq \mathbb{Q}^d$.

H is a supporting hyperplane of S whenever $S \cap H \neq \varnothing$ and $S \subseteq H^+$.

A set F is a face of S if

- either $F = S$, or
- $F = S \cap H$ for some supporting hyperplane H of S.



The geometry of a system of inequalities over the **reals**

Theorem (Minkowski-Weyl; 1897, 1935)

Consider $S \subseteq \mathbb{R}^d$. The two following statements are equivalent:

(H) $S = \{\boldsymbol{x} \in \mathbb{R}^d : A \cdot \boldsymbol{x} \geq \boldsymbol{b}\}$ *for some matrix $A \in \mathbb{Q}^{n \times d}$ and vector $\boldsymbol{b} \in \mathbb{Q}^d$*

(V) $S = \mathrm{conv}(V) + \mathrm{cone}(W)$ *for some finite sets $V, W \subseteq \mathbb{Q}^d$.*

The geometry of a system of inequalities over the **reals**

Theorem (Minkowski-Weyl; 1897, 1935)

Consider $S \subseteq \mathbb{R}^d$. *The two following statements are equivalent:*

(H) $S = \{\boldsymbol{x} \in \mathbb{R}^d : A \cdot \boldsymbol{x} \geq \boldsymbol{b}\}$ *for some matrix* $A \in \mathbb{Q}^{n \times d}$ *and vector* $\boldsymbol{b} \in \mathbb{Q}^d$

(V) $S = \mathrm{conv}(V) + \mathrm{cone}(W)$ *for some finite sets* $V, W \subseteq \mathbb{Q}^d$.

Proof by authority.

"This classical result is an outstanding example of a fact which is completely obvious to geometric intuition, but which wields important algebraic content and is not trivial to prove." (R. T. Rockafellar) ∎

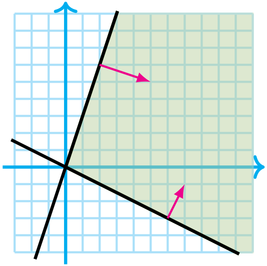
The two definitions of convex cones are equivalent

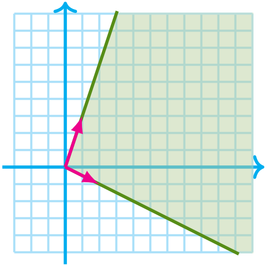
Minkowski-Weyl theorem for cones

Consider $S \subseteq \mathbb{R}^d$. The two following statements are equivalent:

(H) $S = \{\boldsymbol{x} \in \mathbb{R}^d : A \cdot \boldsymbol{x} \geq \mathbf{0}\}$ for some matrix $A \in \mathbb{Q}^{n \times d}$

(V) $S = \mathrm{cone}(W)$ for some finite sets $W \subseteq \mathbb{Q}^d$.





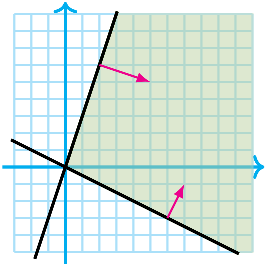
The two definitions of convex cones are equivalent

Minkowski-Weyl theorem for cones

Consider $S \subseteq \mathbb{R}^d$. The two following statements are equivalent:

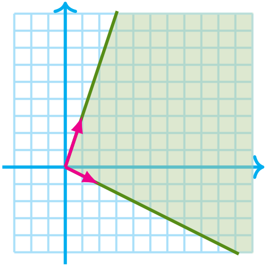
(H) $S = \{\boldsymbol{x} \in \mathbb{R}^d : A \cdot \boldsymbol{x} \geq \boldsymbol{0}\}$ for some matrix $A \in \mathbb{Q}^{n \times d}$

(V) $S = \mathrm{cone}(W)$ for some finite sets $W \subseteq \mathbb{Q}^d$.



$\Longleftarrow$

Smart calls to Farkas' Lemma



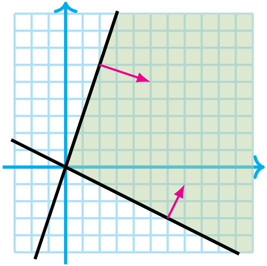
The two definitions of convex cones are equivalent

Minkowski-Weyl theorem for cones

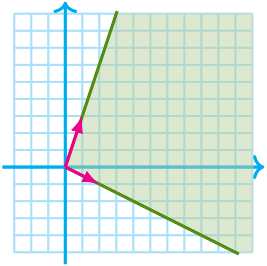
Consider $S \subseteq \mathbb{R}^d$. The two following statements are equivalent:

(H) $S = \{\boldsymbol{x} \in \mathbb{R}^d : A \cdot \boldsymbol{x} \geq \boldsymbol{0}\}$ for some matrix $A \in \mathbb{Q}^{n \times d}$

(V) $S = \text{cone}(W)$ for some finite sets $W \subseteq \mathbb{Q}^d$.



$\Longrightarrow$ Linear algebra magic



Minkowski-Weyl theorem: reducing polyhedra to cones

Minkowski-Weyl theorem for cones

Consider $S \subseteq \mathbb{R}^d$. The two following statements are equivalent:

(H) $S = \{\boldsymbol{x} \in \mathbb{R}^d : A \cdot \boldsymbol{x} \geq \mathbf{0}\}$ for some matrix $A \in \mathbb{Q}^{n \times d}$

(V) $S = \mathrm{cone}(W)$ for some finite sets $W \subseteq \mathbb{Q}^d$.

Minkowski-Weyl theorem for polyhedra

Consider $S \subseteq \mathbb{R}^d$. The two following statements are equivalent:

(H) $S = \{\boldsymbol{x} \in \mathbb{R}^d : A \cdot \boldsymbol{x} \geq \boldsymbol{b}\}$ for some matrix $A \in \mathbb{Q}^{n \times d}$ and vector $\boldsymbol{b} \in \mathbb{Q}^d$

(V) $S = \mathrm{conv}(V) + \mathrm{cone}(W)$ for some finite sets $V, W \subseteq \mathbb{Q}^d$.

Minkowski-Weyl theorem: reducing polyhedra to cones

Mi

Co

(H)

(V)

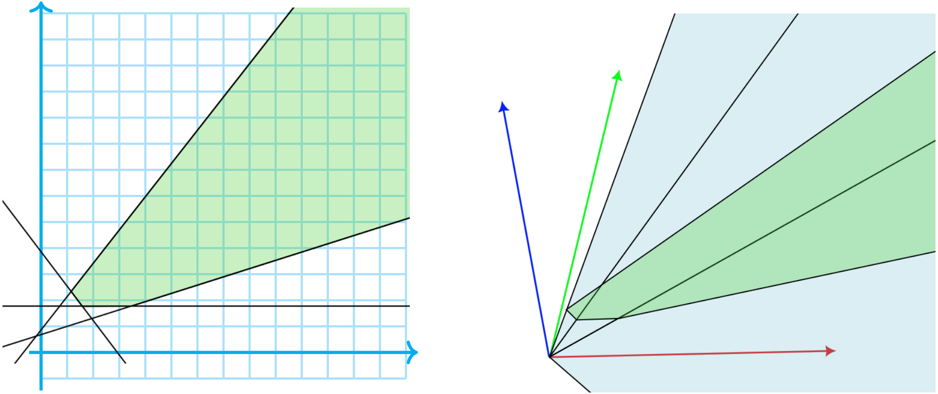
Mi

Co

(H)

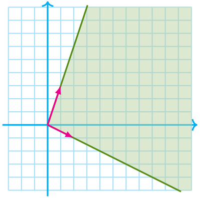
(V)

Every polyhedron in dimension d is the slice of a cone in dimension $d+1$



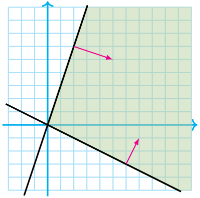
Summary of today's lecture

- Applications of arithmetic theories
- Syntax and semantics of linear arithmetic theories
- Convex geometric objects
- Farkas' lemma
- Minkowski—Weyl theorem



Summary of today's lecture

- Applications of arithmetic theories
- Syntax and semantics of linear arithmetic theories
- Convex geometric objects
- Farkas' lemma
- Minkowski—Weyl theorem



Agenda for the rest of the week

Tomorrow	Linear programming and Integer linear programming
Wednesday	Quantifier elimination procedures
Thursday	Automata-based procedures
Friday	Geometric procedures