Linear arithmetic: Geometry, algorithms, and logic

Monday

Dmitry Chistikov Christoph Haase

Centre for Discrete Mathematics and its Applications (DIMAP) &
Department of Computer Science, University of Warwick, UK

Department of Computer Science
University of Oxford, UK

ESSLLI 2018

Objectives of this course

- Self-contained introduction to logical, algorithmic and geometric aspects of arithmetic theories
- Classical algorithms and decision procedures
- Geometry of sets definable in arithmetic theories
- Recent research developments

Course overview

Monday	Introduction to linear arithmetic
Tuesday	Linear programming
Wednesday	Integer programming
Thursday	Decision procedures for arithmetic theories
Friday	Expressive power of arithmetic theories

Required background

Basic familiarity with following topics is helpful:

- Linear algebra
- Algorithms
- Mathematical logic
- Discrete mathematics
- Computational complexity

Today's lecture

Introduction to linear arithmetic:

- Applications of arithmetic theories
- Syntax and semantics
- Normal forms
- Convex polyhedra and convex polytopes
- Minkowski-Weyl theorem
- Hybrid linear sets

Applications of arithmetic theories

A scheduling problem

Four trucks serve two clients in the morning and afternoon:

A scheduling problem

Four trucks serve two clients in the morning and afternoon:

- cost of truck i serving client j is $c_{i,j} \in \mathbb{N}$
- every client is served exactly once

A scheduling problem

Four trucks serve two clients in the morning and afternoon:

- cost of truck i serving client j is $c_{i,j} \in \mathbb{N}$
- every client is served exactly once

Variables $x_{i,j,t} \in \{0, 1\}$: "truck i serves client j at time $t \in \{0, 1\}$"

A scheduling problem

Four trucks serve two clients in the morning and afternoon:

- cost of truck i serving client j is $c_{i,j} \in \mathbb{N}$
- every client is served exactly once

Variables $x_{i,j,t} \in \{0,1\}$: "truck i serves client j at time $t \in \{0,1\}$"

$$\sum_{i=1}^{4} \sum_{t=0}^{1} x_{i,j,t} = 1 \qquad j \in \{1,2\}$$

A scheduling problem

Four trucks serve two clients in the morning and afternoon:

- cost of truck i serving client j is $c_{i,j} \in \mathbb{N}$
- every client is served exactly once
- trucks only serve one client in mornings and afternoons

Variables $x_{i,j,t} \in \{0,1\}$: "truck i serves client j at time $t \in \{0,1\}$"

$$\sum_{i=1}^{4} \sum_{t=0}^{1} x_{i,j,t} = 1 \qquad j \in \{1,2\}$$

A scheduling problem

Four trucks serve two clients in the morning and afternoon:

- cost of truck i serving client j is $c_{i,j} \in \mathbb{N}$
- every client is served exactly once
- trucks only serve one client in mornings and afternoons

Variables $x_{i,j,t} \in \{0,1\}$: "truck i serves client j at time $t \in \{0,1\}$"

$$\sum_{i=1}^{4}\sum_{t=0}^{1} x_{i,j,t} = 1 \qquad j \in \{1,2\}$$

$$x_{i1t} + x_{i2t} \leq 1 \qquad i \in [1,4], t \in \{0,1\}$$

A scheduling problem

Four trucks serve two clients in the morning and afternoon:

- cost of truck i serving client j is $c_{i,j} \in \mathbb{N}$
- every client is served exactly once
- trucks only serve one client in mornings and afternoons
- truck drivers are loyal to their client

Variables $x_{i,j,t} \in \{0,1\}$: "truck i serves client j at time $t \in \{0,1\}$"

$$\sum_{i=1}^{4}\sum_{t=0}^{1} x_{i,j,t} = 1 \qquad j \in \{1,2\}$$

$$x_{i1t} + x_{i2t} \leq 1 \qquad i \in [1,4], t \in \{0,1\}$$

A scheduling problem

Four trucks serve two clients in the morning and afternoon:

- cost of truck i serving client j is $c_{i,j} \in \mathbb{N}$
- every client is served exactly once
- trucks only serve one client in mornings and afternoons
- truck drivers are loyal to their client

Variables $x_{i,j,t} \in \{0,1\}$: "truck i serves client j at time $t \in \{0,1\}$"

$$\sum_{i=1}^{4}\sum_{t=0}^{1} x_{i,j,t} = 1 \qquad j \in \{1,2\}$$

$$x_{i1t} + x_{i2t} \leq 1 \qquad i \in [1,4], t \in \{0,1\}$$

$$x_{i,(j+1 \bmod 2),2} \leq 1 - x_{i,j,1} \qquad i \in [1,4], j \in \{0,1\}$$

A scheduling problem

Four trucks serve two clients in the morning and afternoon:

- cost of truck i serving client j is $c_{i,j} \in \mathbb{N}$
- every client is served exactly once
- trucks only serve one client in mornings and afternoons
- truck drivers are loyal to their client

Variables $x_{i,j,t} \in \{0,1\}$: "truck i serves client j at time $t \in \{0,1\}$"

$$\bigwedge_{j \in \{1,2\}} \sum_{i=1}^{4} \sum_{t=0}^{1} x_{i,j,t} = 1 \qquad j \in \{1,2\}$$

$$\bigwedge_{i \in [1,4], t \in \{0,1\}} x_{i1t} + x_{i2t} \leq 1 \qquad i \in [1,4], t \in \{0,1\}$$

$$\bigwedge_{i \in [1,4]} \bigwedge_{j \in \{0,1\}} x_{i,(j+1 \bmod 2),2} \leq 1 - x_{i,j,1} \qquad i \in [1,4], j \in \{0,1\}$$

A scheduling problem

Four trucks serve two clients in the morning and afternoon:

- cost of truck i serving client j is $c_{i,j} \in \mathbb{N}$
- every client is served exactly once
- trucks only serve one client in mornings and afternoons
- truck drivers are loyal to their client

Variables $x_{i,j,t} \in \{0,1\}$: "truck i serves client j at time $t \in \{0,1\}$"

$$\bigwedge_{j \in \{1,2\}} \sum_{i=1}^{4} \sum_{t=0}^{1} x_{i,j,t} = 1$$

$$\bigwedge_{i \in [1,4], t \in \{0,1\}} x_{i1t} + x_{i2t} \leq 1$$

$$\bigwedge_{i \in [1,4]} \bigwedge_{j \in \{0,1\}} x_{i,(j+1 \bmod 2),2} \leq 1 - x_{i,j,1}$$

A scheduling problem

Four trucks serve two clients in the morning and afternoon:

- cost of truck i serving client j is $c_{i,j} \in \mathbb{N}$
- every client is served exactly once
- trucks only serve one client in mornings and afternoons
- truck drivers are loyal to their client

Variables $x_{i,j,t} \in \{0,1\}$: "truck i serves client j at time $t \in \{0,1\}$"

$$\bigwedge_{j \in \{1,2\}} \sum_{i=1}^{4} \sum_{t=0}^{1} x_{i,j,t} = 1$$

$$\bigwedge_{i \in [1,4], t \in \{0,1\}} x_{i1t} + x_{i2t} \leq 1$$

$$\bigwedge_{i \in [1,4]} \bigwedge_{j \in \{0,1\}} x_{i,(j+1 \bmod 2),2} \leq 1 - x_{i,j,1}$$

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?

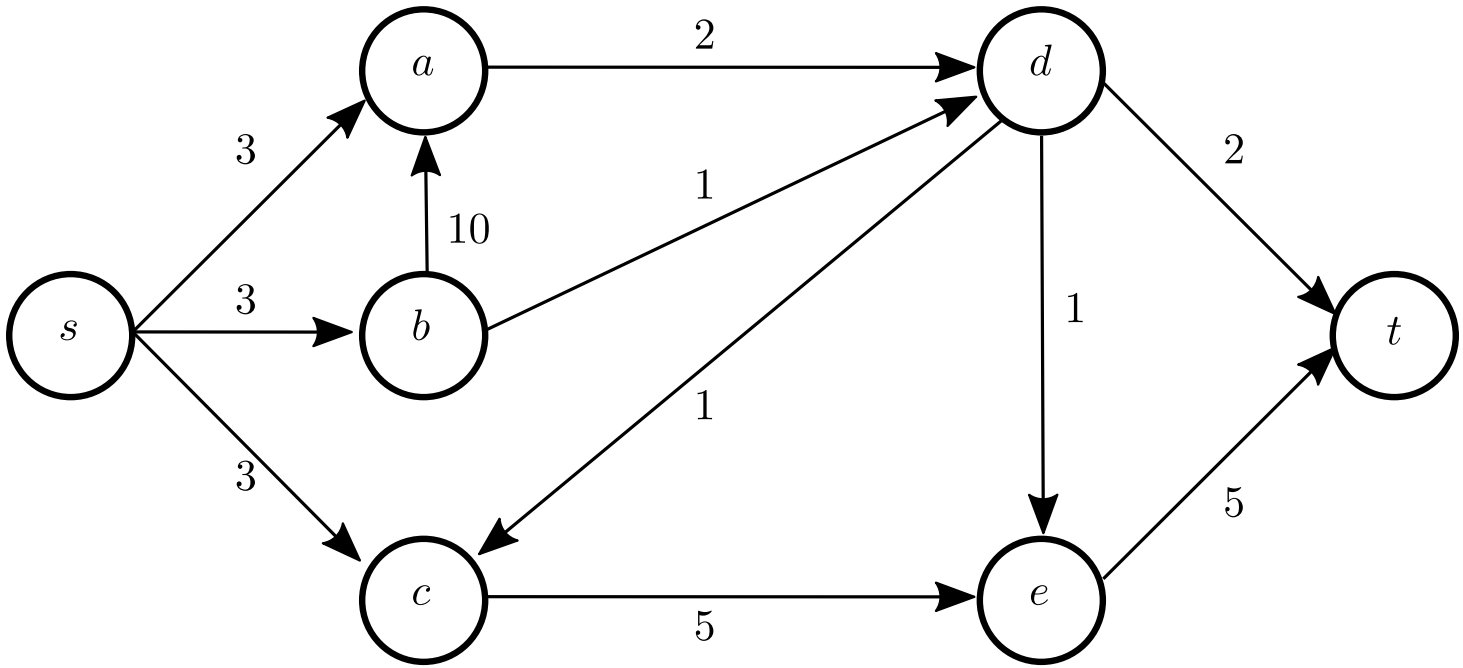
$$\forall n : c < n \to \exists x_1 \exists x_2 \cdots \exists x_k : n = m_1 \cdot x_1 + \cdots + m_k \cdot x_k$$

The Frobenius problem

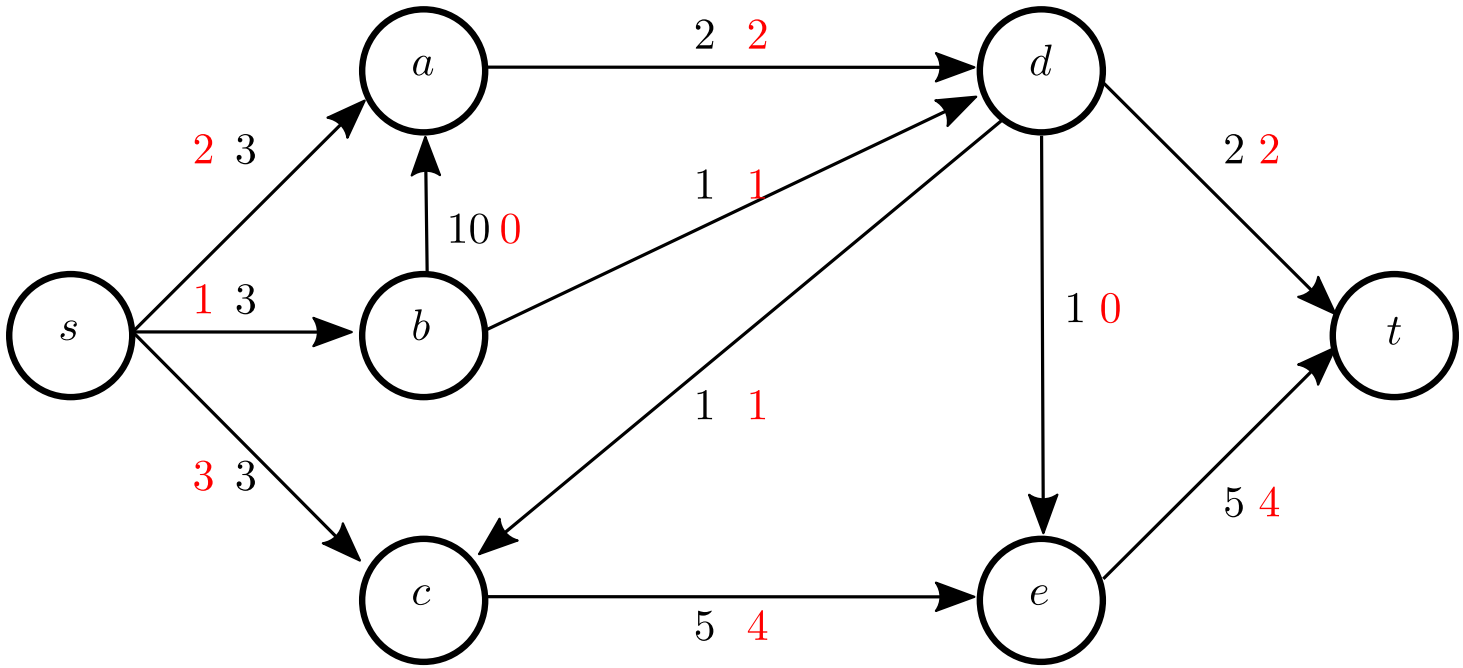
Given coins in denominations $m_1 < \cdots < m_k \in \mathbb{N}$, what is the largest value c that cannot be generated? Does such a c exist?

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

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:

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

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

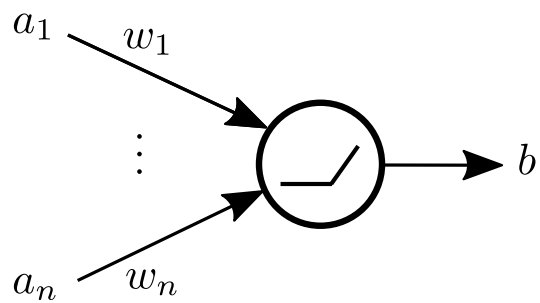
For edge $e \in E$, introduce variables f_e encoding flow conditions:

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

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

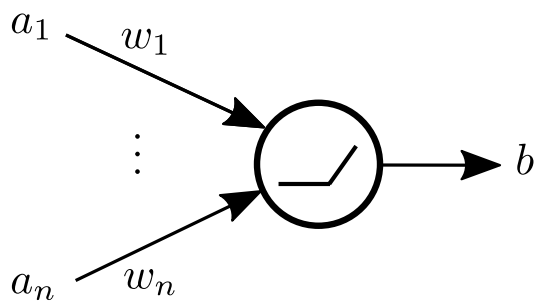
Artificial neural networks

Artificial neuron:



Artificial neural networks

Artificial neuron:

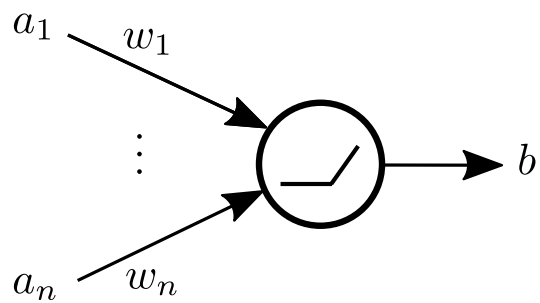


Ouput:

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

Artificial neural networks

Artificial neuron:



Ouput:

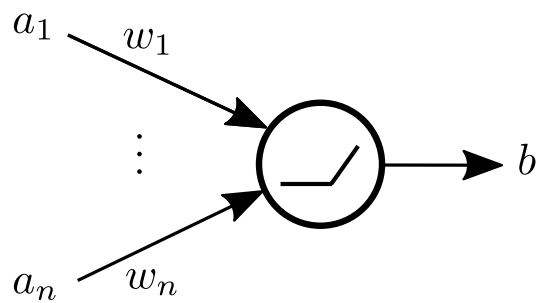
$$b = \begin{cases} 0 & \text{if } \sum_{i=1}^{n} w_i \cdot a_i < 0 \\ \sum_{i=1}^{n} w_i \cdot a_i & \text{otherwise} \end{cases}$$

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

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

Artificial neural networks

Artificial neuron:



Ouput:

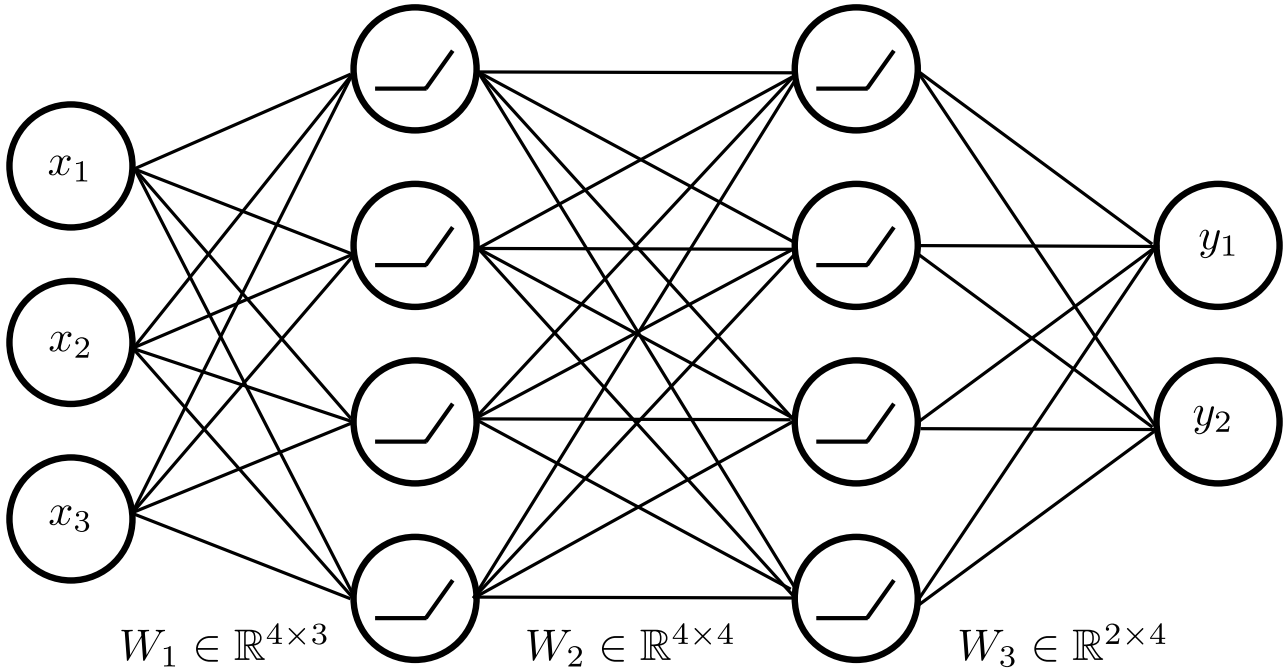
$$b = \begin{cases} 0 & \text{if } \sum_{i=1}^{n} w_i \cdot a_i < 0 \\ \sum_{i=1}^{n} w_i \cdot a_i & \text{otherwise} \end{cases}$$

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

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

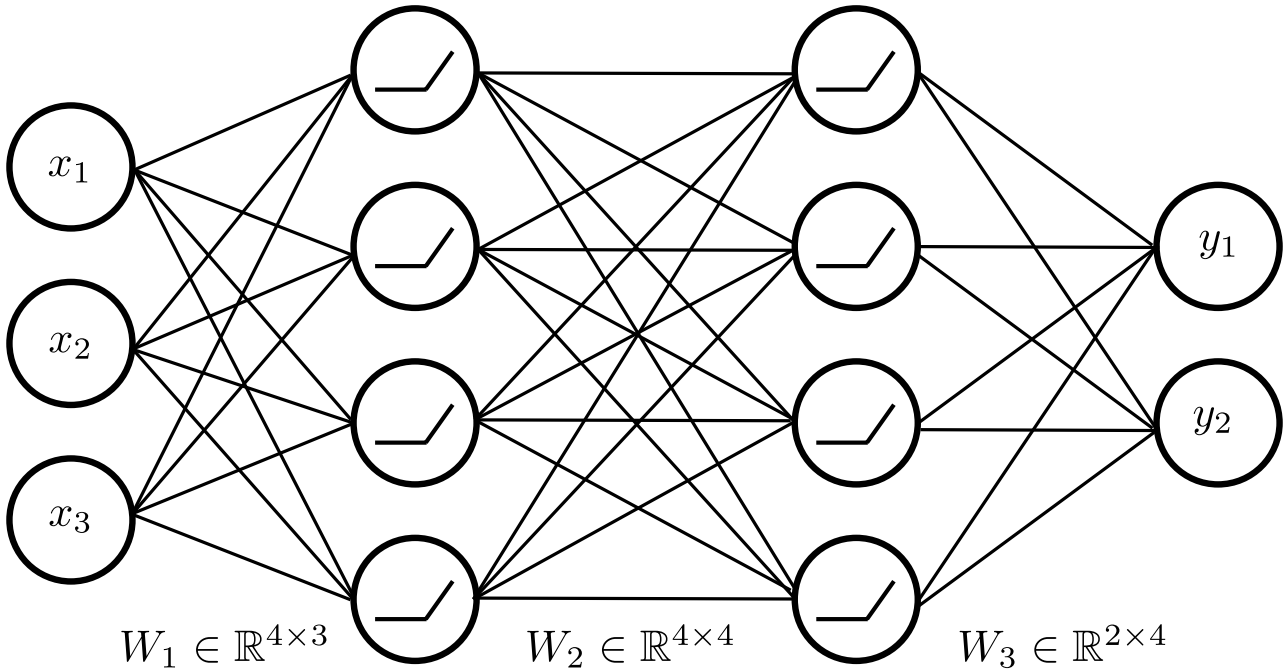
$$\Phi_W(\boldsymbol{x}, \boldsymbol{y}) := \bigwedge_{1 \leq i \leq m} \Phi_{\boldsymbol{w}_i}(\boldsymbol{x}, y_i) \quad \text{where } W = \begin{pmatrix} \boldsymbol{w}_1 \\ \vdots \\ \boldsymbol{w}_m \end{pmatrix}$$

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

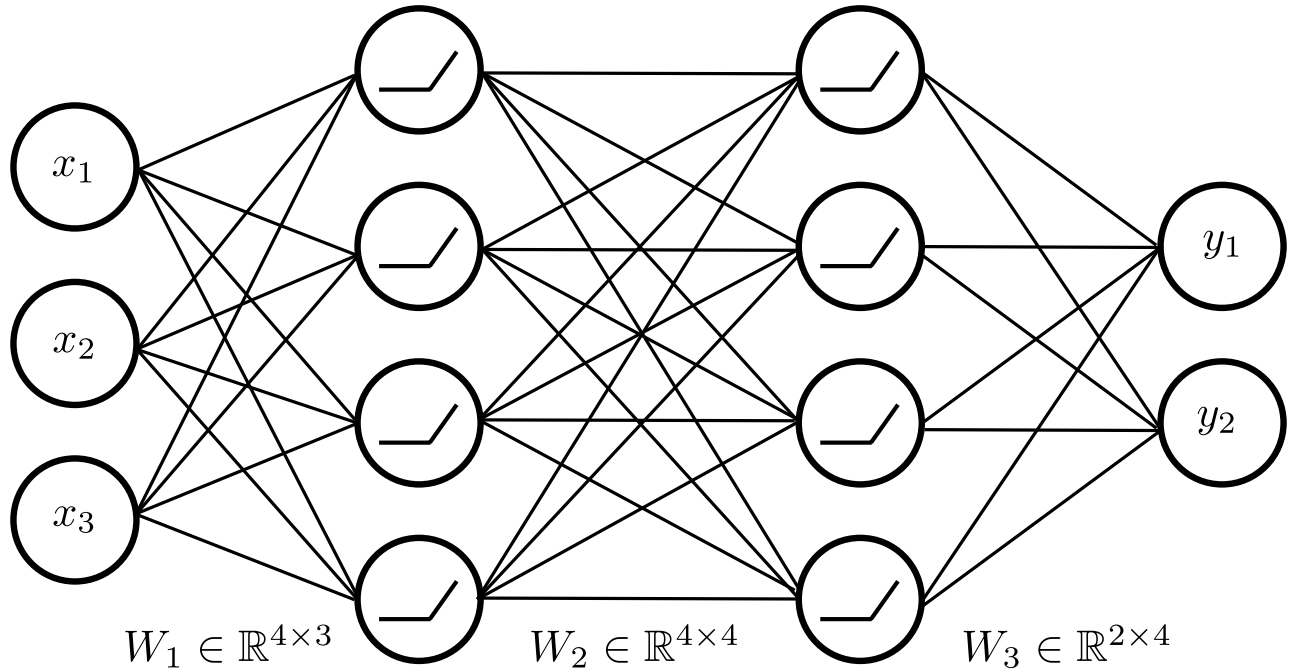


$$\Phi(\boldsymbol{x}, \boldsymbol{y}) = \exists \boldsymbol{z}_1 \exists \boldsymbol{z}_2 : \Phi_{W_1}(\boldsymbol{x}, \boldsymbol{z}_1) \wedge \Phi_{W_2}(\boldsymbol{z}_1, \boldsymbol{z}_2) \wedge \Phi_{W_3}(\boldsymbol{z}_2, \boldsymbol{y})$$

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 neural networks



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

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 neuron network outputs probability distribution:

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

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:

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

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
trucks	$\{0,1\}$	$+$	$=,\leq$	$\wedge$	$\exists$
Frobenius	$\mathbb{N}$	$+$	$=,<$	$\wedge,\rightarrow$	$\exists\forall\exists$
max-flow	$\mathbb{R}$	$+$	$=,\leq$	$\wedge$	$\exists$
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
trucks	$\{0,1\}$	$+$	$=,\leq$	$\wedge$	$\exists$
Frobenius	$\mathbb{N}$	$+$	$=,<$	$\wedge,\rightarrow$	$\exists\forall\exists$
max-flow	$\mathbb{R}$	$+$	$=,\leq$	$\wedge$	$\exists$
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 $a_1, \ldots, a_n, b \in \mathbb{Z}$:

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

- 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 $a \in \mathbb{D}$, $\mathcal{A} \models \Phi[a/x]$

Linear arithmetic theories: geometry

Let $\boldsymbol{x} = (x_1, \ldots, x_n)$, a formula $\Phi(\boldsymbol{x})$ defines subset of $\mathbb{D}^n$:

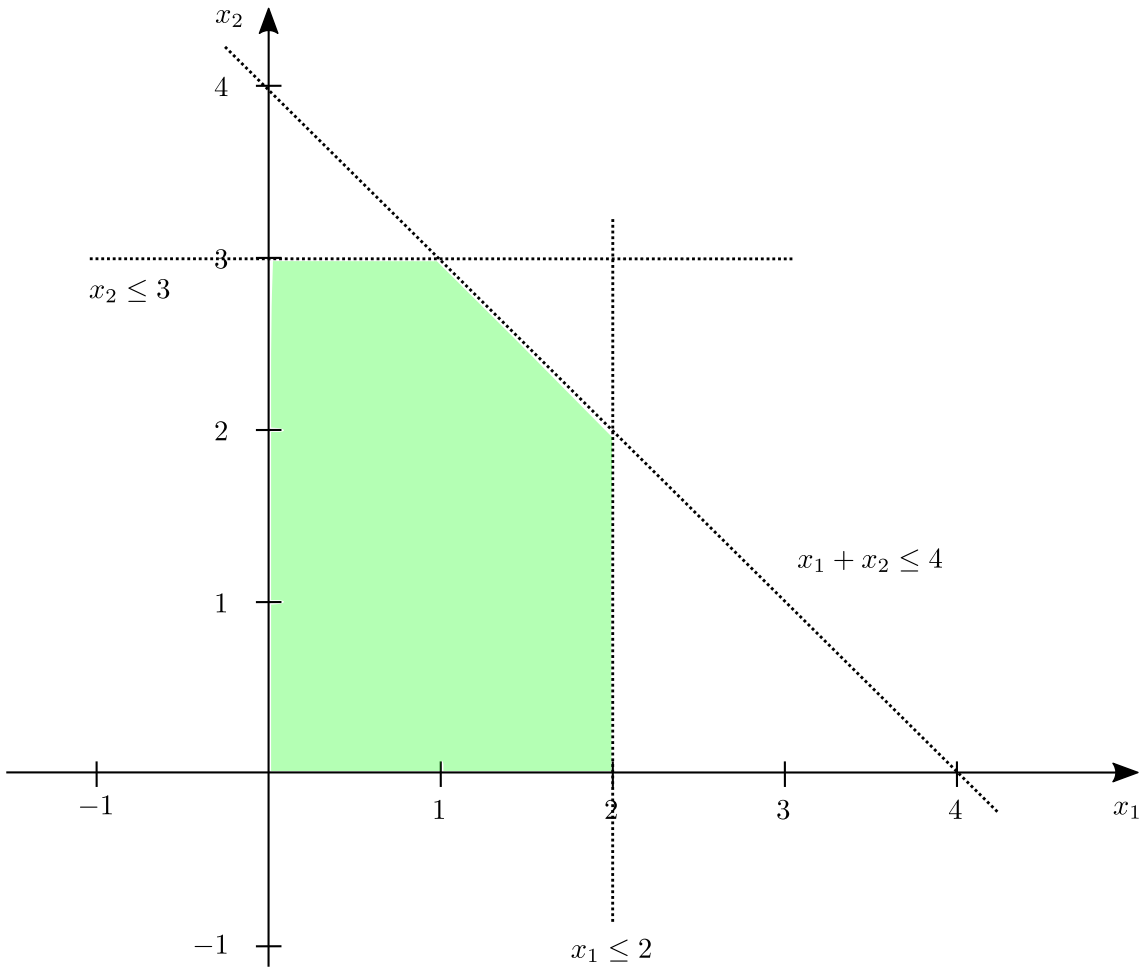
$$[\![\Phi(\boldsymbol{x})]\!] := \{\boldsymbol{a} \in \mathbb{D}^n : \Phi[\boldsymbol{a}/\boldsymbol{x}] \text{ is true}\}$$

Example

$$[\![x_1 \leq 2 \wedge x_2 \leq 3 \wedge x_1 + x_2 \leq 4 \wedge x_1 \geq 0 \wedge x_2 \geq 0]\!] \text{ with } \mathbb{D} = \mathbb{Q}$$

Example

$[\![x_1 \leq 2 \wedge x_2 \leq 3 \wedge x_1 + x_2 \leq 4 \wedge x_1 \geq 0 \wedge x_2 \geq 0]\!]$ with $\mathbb{D} = \mathbb{Q}$

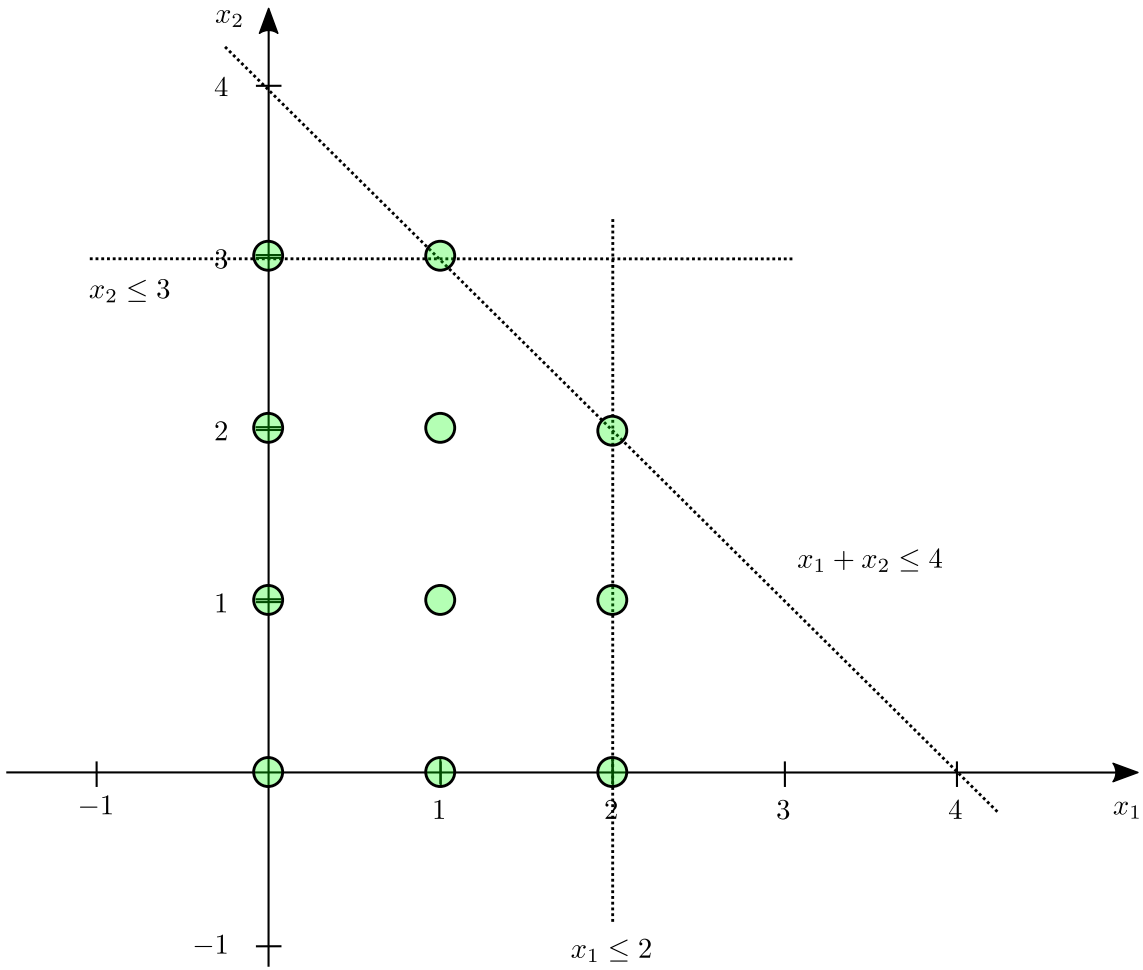


Example

$$[\![x_1 \leq 2 \wedge x_2 \leq 3 \wedge x_1 + x_2 \leq 4 \wedge x_1 \geq 0 \wedge x_2 \geq 0]\!] \text{ with } \mathbb{D} = \mathbb{Z}$$

Example

$[\![x_1 \leq 2 \wedge x_2 \leq 3 \wedge x_1 + x_2 \leq 4 \wedge x_1 \geq 0 \wedge x_2 \geq 0]\!]$ with $\mathbb{D} = \mathbb{Z}$



Simplifications and normal forms

Simplifying formulas (1)

- Can assume negation-free formulas:

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

- Equality not needed:

$$a = b \iff a \leq b \wedge b \leq a$$

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

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

Simplifying formulas (2)

Prenex form:

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

Simplifying formulas (2)

Prenex form:

$$Q_1 x_1 \, Q_2 x_2 \cdots Q_k x_k : \Phi(x_1, \ldots, x_k)$$ and Φ 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

Course overview

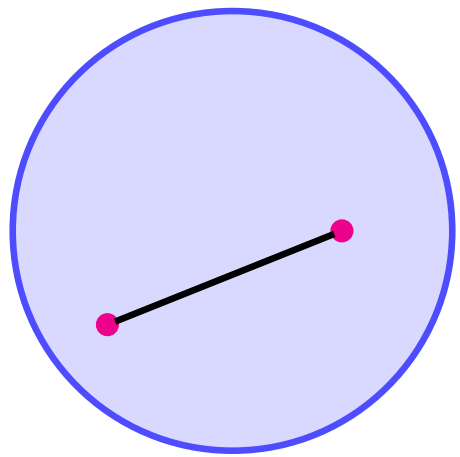
Monday	Introduction to linear arithmetic ($\exists$; $\mathbb{R}$, $\mathbb{Z}$)
Tuesday	Linear programming ($\exists$; $\mathbb{R}$)
Wednesday	Integer programming ($\exists$; $\mathbb{R}$, $\mathbb{Z}$)
Thursday	Decision procedures for arithm. theories ($\{\exists, \forall\}^*$; $\mathbb{R}$, $\mathbb{Z}$)
Friday	Expressive power of arithmetic theories ($\{\exists, \forall\}^*$; $\mathbb{Z}$)

Geometry of linear arithmetic

Convex sets

A set $S \subseteq \mathbb{R}^d$ is convex if

$$\forall\, x, y \in S \qquad [x, y] \subseteq S.$$



For $S \subseteq \mathbb{R}^d$, the convex hull 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:

$$\operatorname{conv}(S) := \bigcup_{\substack{\boldsymbol{v}_1,\ldots,\boldsymbol{v}_n \in S \\ n \geq 1}} \operatorname{conv}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n),$$

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

Cones

A (convex) cone in $\mathbb{R}^d$ is a subset $C \subseteq \mathbb{R}^d$ such that

- $\boldsymbol{x} + \boldsymbol{y} \in C$ for all $\boldsymbol{x}, \boldsymbol{y} \in C$ and
- $\lambda \boldsymbol{x} \in C$ for all $\boldsymbol{x} \in C$ and $\lambda \geq 0$.

Cones

A (convex) cone in $\mathbb{R}^d$ is a subset $C \subseteq \mathbb{R}^d$ such that

- $\boldsymbol{x} + \boldsymbol{y} \in C$ for all $\boldsymbol{x}, \boldsymbol{y} \in C$ and
- $\lambda \boldsymbol{x} \in C$ for all $\boldsymbol{x} \in C$ and $\lambda \geq 0$.

The cone generated by $\boldsymbol{v}_1, , \ldots, \boldsymbol{v}_n \in \mathbb{R}^d$ is

$$\operatorname{cone}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) := \{\lambda_1 \boldsymbol{v}_1 + \ldots + \lambda_n \boldsymbol{v}_n \colon \lambda_1, \ldots, \lambda_n \geq 0\}\,.$$

Cones

A (convex) cone in $\mathbb{R}^d$ is a subset $C \subseteq \mathbb{R}^d$ such that

- $\boldsymbol{x} + \boldsymbol{y} \in C$ for all $\boldsymbol{x}, \boldsymbol{y} \in C$ and
- $\lambda \boldsymbol{x} \in C$ for all $\boldsymbol{x} \in C$ and $\lambda \geq 0$.

The cone generated by $\boldsymbol{v}_1, , \ldots, \boldsymbol{v}_n \in \mathbb{R}^d$ is

$$\operatorname{cone}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) := \{\lambda_1 \boldsymbol{v}_1 + \ldots + \lambda_n \boldsymbol{v}_n \colon \lambda_1, \ldots, \lambda_n \geq 0\}.$$

A cone is polyhedral if it has the form

$$\{\boldsymbol{x} \colon A \cdot \boldsymbol{x} \geq \boldsymbol{0}\}$$

for some matrix A.

Minkowski sum

$$A + B = \{a + b \colon a \in A, b \in B\}$$

The Minkowski–Weyl theorem (1896, 1935)

Theorem

The following are equivalent:

1. $P = \{\boldsymbol{x} \colon A \cdot \boldsymbol{x} \geq \boldsymbol{c}\}$ for some matrix A and vector $\boldsymbol{c}$; and
2. $P = \operatorname{conv}(E) + \operatorname{cone}(F)$ for some finite sets E, F.

"*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 Minkowski–Weyl theorem (1896, 1935)

Theorem

The following are equivalent:

1. $P = \{\boldsymbol{x} : A \cdot \boldsymbol{x} \geq \boldsymbol{c}\}$ for some matrix A and vector $\boldsymbol{c}$; and
2. $P = \operatorname{conv}(E) + \operatorname{cone}(F)$ for some finite sets E, F.

"*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)

These are two equivalent definitions of a (convex) polyhedron.

(Convex) polytopes are bounded polyhedra.

Hyperplane and half-space

Fix $\boldsymbol{a} \in \mathbb{R}^d \setminus \{\mathbf{0}\}$ and $c \in \mathbb{R}$.

A hyperplane in $\mathbb{R}^d$ is a set of the form $\{\boldsymbol{x} \colon \boldsymbol{a} \cdot \boldsymbol{x} = c\}$.

A half-space in $\mathbb{R}^d$ is a set of the form $\{\boldsymbol{x} \colon \boldsymbol{a} \cdot \boldsymbol{x} \geq c\}$.

Let $S \subseteq \mathbb{R}^d$ be any set.
Suppose $H = \{\boldsymbol{x} : \boldsymbol{a} \cdot \boldsymbol{x} = c\}$ and $H^+ = \{\boldsymbol{x} : \boldsymbol{a} \cdot \boldsymbol{x} \geq c\}$.

Definition:

- H is a valid hyperplane for S if $S \subseteq H^+$.
- H is a supporting hyperplane for S if $S \subseteq H^+$ and $S \cap H \neq \varnothing$.

Faces of polyhedra

Let P be a polyhedron.

Definition

$F \subseteq P$ is a face of P if

- either $F = P$,
- or $F = P \cap H$ for some valid hyperplane H.

Faces of polyhedra

Let P be a polyhedron.

Definition

$F \subseteq P$ is a face of P if

- either $F = P$,
- or $F = P \cap H$ for some valid hyperplane H.

Faces are sets of optimal solutions to **linear programs**.
Faces form a partial order with respect to set inclusion.

Intermezzo: definition of dimension

Suppose $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in \mathbb{R}^d$ and $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$.

The vector $\lambda_1 \boldsymbol{v}_1 + \ldots + \lambda_n \boldsymbol{v}_n$ is

- a linear combination [of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$];
- an affine combination [...] if $\sum_{i=1}^n \lambda_i = 1$;
- a conic combination [...] if all $\lambda_i \geq 0$;
- a convex combination [...] if it is affine and conic.

The linear (affine, conic, convex) hull of S is the set of all linear (affine, conic, convex) combinations of vectors of S.

The linear (affine, conic, convex) hull of S is the set of all linear (affine, conic, convex) combinations of vectors of S.

A set that is equal to its $\square$ hull is:

- linear (a linear (sub)space),
- affine (an affine (sub)space),
- conic (a cone), or
- convex (a convex set), respectively.

The linear (affine, conic, convex) hull of S is the set of all linear (affine, conic, convex) combinations of vectors of S.

A set that is equal to its [ ] hull is:

- linear (a linear (sub)space),
- affine (an affine (sub)space),
- conic (a cone), or
- convex (a convex set), respectively.

The [ ] hull of S is the unique smallest [ ] set containing S.

Affine sets

(affine subspaces, affine manifolds, affine/linear varieties, flats)

Theorem

1. A set $M \subseteq \mathbb{R}^d$ is affine if and only if

$$M = \boldsymbol{v} + L$$

   where $L \subseteq \mathbb{R}^d$ is a linear (sub)space and $\in \mathbb{R}^d$.

2. The space L is determined uniquely.
   The vector $\boldsymbol{v}$ can be chosen as an arbitrary vector from M.

Dimension of affine subspaces

Definition

The dimension of an affine subspace M is the dimension of the linear subspace L in the representation $M = \boldsymbol{v} + L$.

Affine subspaces of dimension 0, 1, and 2 are called points, lines, and planes, respectively.

Affine subspaces of $\mathbb{R}^d$ of dimension $d-1$ are hyperplanes.

Dimension of polyhedra

Definition

Let $P \subseteq \mathbb{R}^d$ be a polyhedron.
The dimension of P is the dimension of $\operatorname{aff}(P)$.

Faces of dimension 0, 1, and $\dim P - 1$ are called vertices, edges, and facets, respectively.

Characterization for faces

Theorem

Let $P = \{\boldsymbol{x} \colon A \cdot \boldsymbol{x} \geq \boldsymbol{c}\}$ be a polyhedron.
A non-empty subset $F \subseteq P$ is a face of P if and only if

$$F = P \cap \{\boldsymbol{x} \colon A' \cdot \boldsymbol{x} = \boldsymbol{c}'\},$$

that is, F is the set of solutions to a system of inequalities and equalities obtained from $A \cdot \boldsymbol{x} \geq \boldsymbol{c}$ by changing some of the inequalities to equalities.

Geometry in integers: Hybrid linear sets

$\mathbb{N}^d$: Linear, hybrid linear, and semi-linear sets

[Parikh (1961)]

$\mathbb{N}^d$: Linear, hybrid linear, and semi-linear sets

[Parikh (1961)]

Vectors $\boldsymbol{b}$ in B: base vectors
Vectors $\boldsymbol{p}_i$ in P: period vectors
} generators

Linear set:

$$L(\boldsymbol{b}, P) = \{\boldsymbol{b} + \lambda_1 \boldsymbol{p}_1 + \ldots \lambda_s \boldsymbol{p}_s : \\ \boldsymbol{p}_1, \ldots, \boldsymbol{p}_s \in P,\ \lambda_1, \ldots, \lambda_s \in \mathbb{N},\ s \geq 0\}$$

Hybrid linear set:

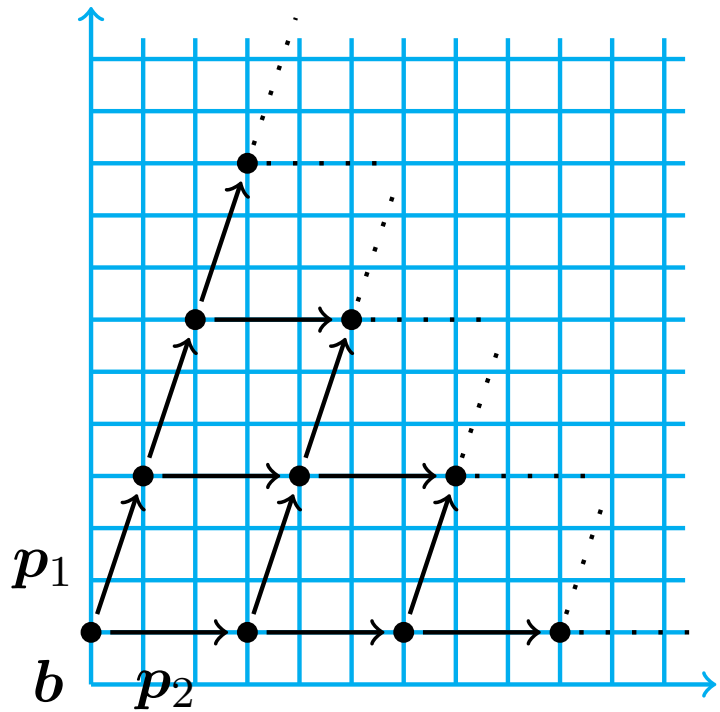
$$L(B, P) = \bigcup_{\boldsymbol{b} \in B} L(\boldsymbol{b}, P)$$

Semi-linear set:

$$M = \bigcup_{i \in I} L(B_i, P_i)$$

$\mathbb{N}^d$: Linear, hybrid linear, and semi-linear sets

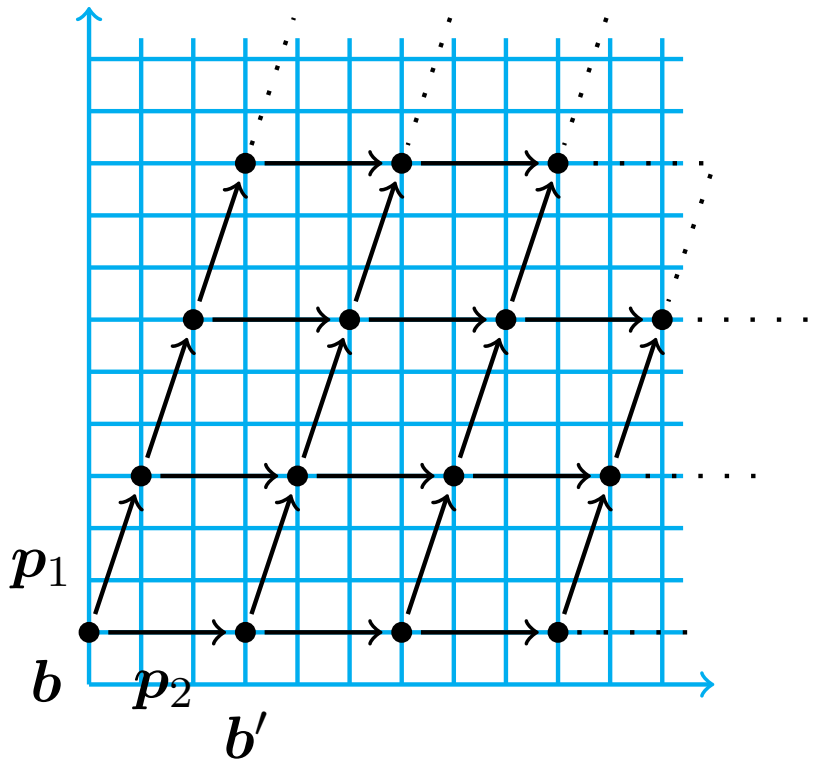
[Parikh (1961)]



Linear $<$ Hybrid linear $<$ Semi-linear

$\mathbb{N}^d$: Linear, hybrid linear, and semi-linear sets

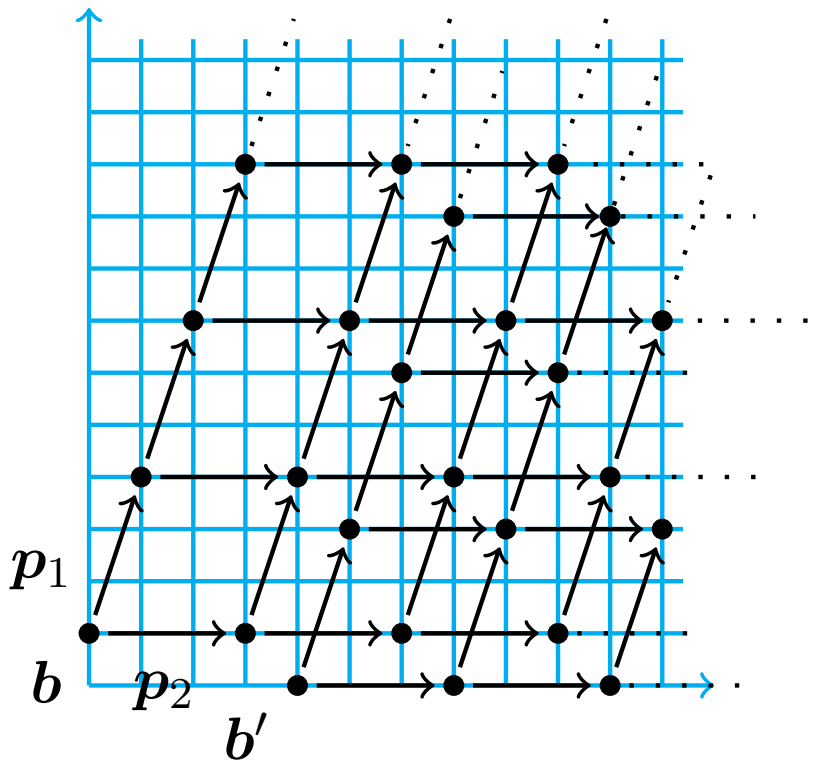
[Parikh (1961)]



Linear $<$ Hybrid linear $<$ Semi-linear

$\mathbb{N}^d$: Linear, hybrid linear, and semi-linear sets

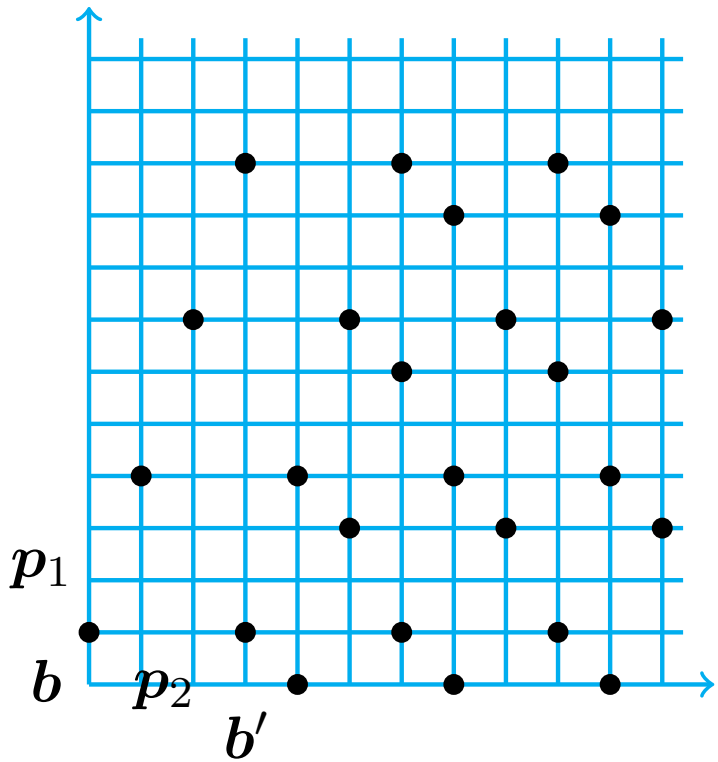
[Parikh (1961)]



Linear $<$ Hybrid linear $<$ Semi-linear

$\mathbb{N}^d$: Linear, hybrid linear, and semi-linear sets

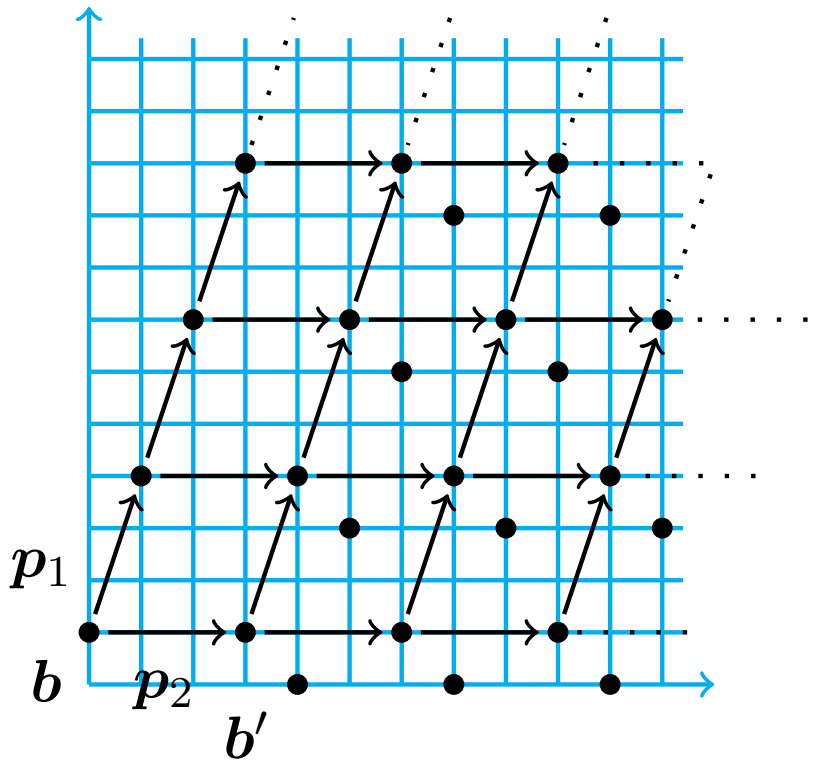
[Parikh (1961)]



Linear $<$ Hybrid linear $<$ Semi-linear

$\mathbb{N}^d$: Linear, hybrid linear, and semi-linear sets

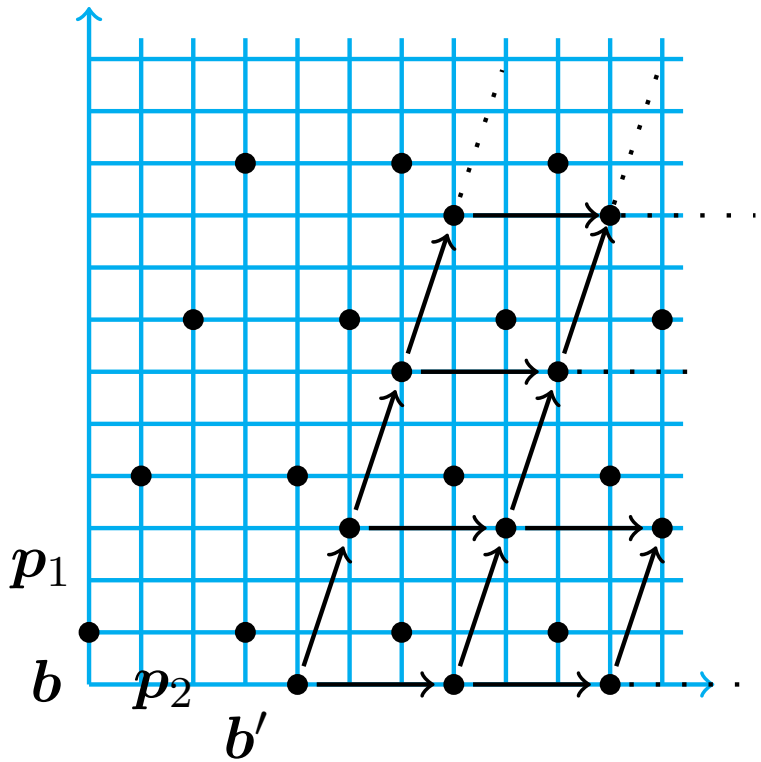
[Parikh (1961)]



Linear $<$ Hybrid linear $<$ Semi-linear

$\mathbb{N}^d$: Linear, hybrid linear, and semi-linear sets

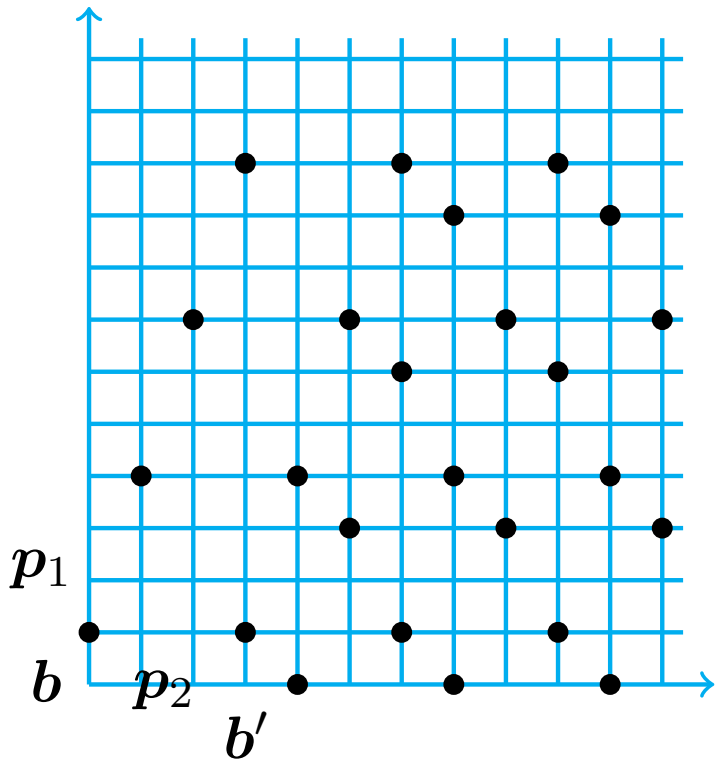
[Parikh (1961)]



Linear $<$ Hybrid linear $<$ Semi-linear

$\mathbb{N}^d$: Linear, hybrid linear, and semi-linear sets

[Parikh (1961)]



Linear $<$ Hybrid linear $<$ Semi-linear

$$\left\{\sum \lambda_i \boldsymbol{b}_i + \sum \mu_j \boldsymbol{p}_j : \quad \sum \lambda_i = 1,\ \lambda_i \geq 0,\ \mu_j \geq 0\right\}$$

$$\left\{\sum \lambda_i \boldsymbol{b}_i + \sum \mu_j \boldsymbol{p}_j : \quad \sum \lambda_i = 1,\ \lambda_i \geq 0,\ \mu_j \geq 0\right\}$$

- $\lambda_i, \mu_j \in \mathbb{R}$: convex polyhedron $\mathrm{conv}B + \mathrm{cone}P$
- $\lambda_i, \mu_j \in \mathbb{Z}$: hybrid linear set $L(B, P)$

Hybrid linear sets are "discrete convex polyhedra"!

$$\left\{\sum \lambda_i \boldsymbol{b}_i + \sum \mu_j \boldsymbol{p}_j : \quad \sum \lambda_i = 1,\ \lambda_i \geq 0,\ \mu_j \geq 0\right\}$$

- $\lambda_i, \mu_j \in \mathbb{R}$: convex polyhedron $\mathrm{conv}B + \mathrm{cone}P$
- $\lambda_i, \mu_j \in \mathbb{Z}$: hybrid linear set $L(B, P)$

Summary of today's lecture

- Syntax and semantics of linear arithmetic theories
- Convex sets and convex cones
- Convex polyhedra
- The Minkowski—Weyl theorem
- Dimension of polyhedra
- Linear and hybrid linear sets (discrete cones and polyhedra)

Agenda for the rest of the week

Tuesday	Linear programming
Wednesday	Integer programming
Thursday	Decision procedures for arithmetic theories
Friday	Expressive power of arithmetic theories