CS 433 Automated Reasoning 2025

Lecture 17: Thinking Integer

Instructor: Ashutosh Gupta

IITB India

Compile date: 2025-04-09

Topic 17.1

Linear integer arithmetic (LIA)

Linear integer arithmetic (LIA)

Formulas with structure $\Sigma = (\{+/2, 0, 1, \ldots\}, \{< /2\})$ with a set of axioms

Decidable

Presburger [3EXPTIME]

$$\begin{cases} \forall x \neg(x+1=0) \\ \forall x \forall y (x+1=y+1 \Rightarrow x=y) \\ F(0) \wedge (\forall x (F(x) \Rightarrow F(x+1)) \Rightarrow \forall x F(x)) \\ \forall x (x+0=x) \\ \forall x \forall y (x+(y+1)=(x+y)+1) \end{cases}$$

Syntactically, looks very similar to rational arithmetic.

Note that the theory does not have multiplication.

However, one can simulate multiplication by constants in the theory.

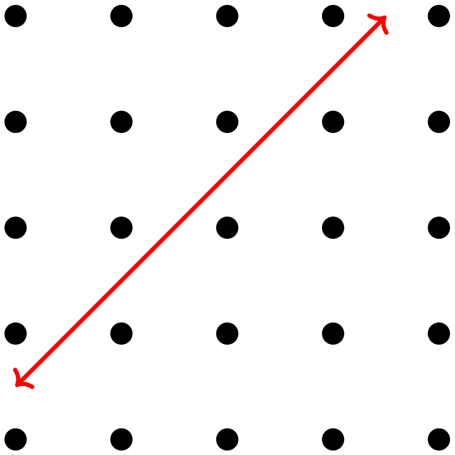
Example 17.1

The following formulas are in the quantifier-free fragment of the theory (QF_LIA), where x, y, and z are the integers.

- $x \geq 0 \vee y + z = 5$
- $x < 300 \wedge x - z \neq 5$

Difference in reasoning

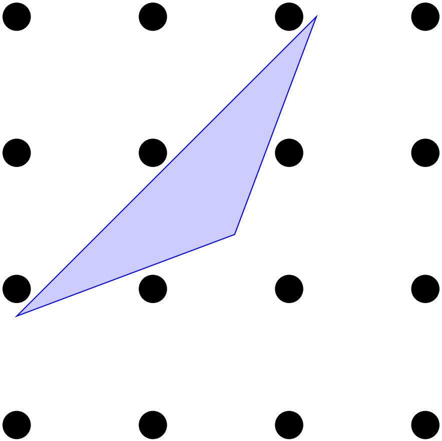
Integers are not dense. They are like a lattice in the space.



Subspaces may exist that do not contain any integer.

Polyhedrons without integers!

We may also have polyhedrons that do not contain integers.



How to reason absence of integers?

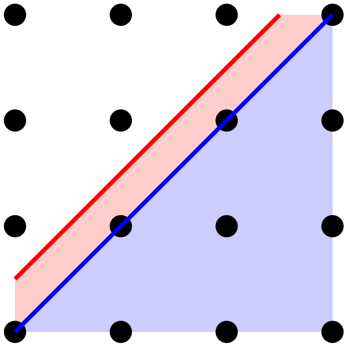
Reasoning over integer

$$[\textsc{Comb}]\frac{t_1 \leq 0 \quad t_2 \leq 0}{t_1\lambda_1 + t_2\lambda_2 - \lambda_3 \leq 0}\lambda_1, \lambda_2, \lambda_3 \geq 0$$

$$[\textsc{Div}]\frac{a_1x_1 + \dots + a_nx_n \leq b}{\frac{a_1}{g}x_1 + \dots + \frac{a_n}{g}x_n \leq \left\lfloor \frac{b}{g} \right\rfloor} g = gcd(a_1, ..., a_n)$$

Example: application of DIV rule

Example 17.2



$$[\textsc{Div}]\frac{2x_1 + 2x_2 \le 1}{\frac{2}{2}x_1 + \frac{2}{2}x_2 \le \left\lfloor \frac{1}{2} \right\rfloor} 2 = gcd(2,2)$$

Completeness

Are the two rules complete?

We will not do the full completeness. However, we will discuss key ideas when thinking integer.

Topic 17.2

Greatest common divisor

Euclid's method for computing gcd(x,y)

1. If $x = 0$, return y
2. If $y = 0$, return x
3. If $x > y$, $x := x - y\lfloor\frac{x}{y}\rfloor$ else $y := y - x\lfloor\frac{y}{x}\rfloor$
4. goto 1

Theorem 17.1
Euclid's method runs in polynomial time.

Proof.
In each step one of x and y is reduced by half.

Bound on number of iterations: $log_2(x) + log_2(y) + 1$ □

Topic 17.3

Hermite normal form

Find integer solution of equations

Consider a rational matrix A and vector b, find integral solution for x such that

$$Ax = b.$$

Hermite normal form (HNF)

Definition 17.1

A rational matrix is in Hermite normal form if it has the form $[B\ 0]$, where B is

- lower triangular,
- nonnegative matrix, and
- the unique maximum entry in each row is at diagonal.

Exercise 17.1

Are the following matrices in Hermite normal form?

- $\begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$
- $\begin{bmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & -2 & 3 \end{bmatrix}$
- $\begin{bmatrix} 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 1 & 1.5 & 3 & 0 \end{bmatrix}$
- $\begin{bmatrix} 2 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 1 & 1 & 3 & 0 \end{bmatrix}$

Elementary unimodular column operations

Definition 17.2

The elementary unimodular column operations are

- exchanging two columns,
- multiplying a column by -1, and
- adding integral multiple of a column to another

Exercise 17.2

Can we get the following by applying a single operation on $\begin{bmatrix} 2 & 3 & 6 \\ 2 & 1 & -3 \\ 1 & 1 & 3 \end{bmatrix}$?

$$\begin{bmatrix} 3 & 2 & 6 \\ 1 & 2 & -3 \\ 1 & 1 & 3 \end{bmatrix} \quad \begin{bmatrix} 2 & 3 & -6 \\ 2 & 1 & 3 \\ 1 & 1 & -3 \end{bmatrix} \quad \begin{bmatrix} 0 & 3 & 6 \\ 3 & 1 & -3 \\ 0 & 1 & 3 \end{bmatrix} \quad \begin{bmatrix} 2 & 3 & 8 \\ 2 & 1 & -1 \\ 1 & 1 & 4 \end{bmatrix}$$

Exercise 17.3

The elementary operations on A preserve integral satisfiability of $Ax = b$.

There is a Hermite normal form

Theorem 17.2

Each rational matrix A of full row rank can be transformed into HNF by a sequence of elementary unimodular column operations.

Proof.

Wlog A is an integer matrix. The transformation proceeds in two phases

Phase 1:we can transform to lower triangular matrix with positive diagonal.

Assume we have obtained $\begin{bmatrix} B & 0 \\ C & D \end{bmatrix}$ where B is lower triangular matrix with positive diagonal.

Now we will apply the elementary operations on the columns of D to make top row zero except the first entry in the row. ...

Commentary: Theorem 4.1 in Schrijver

There is a Hermite normal form II

Proof.

Let $D = \begin{bmatrix} \delta_1 & \dots & \delta_k \\ \vdots & \vdots & \vdots \end{bmatrix}$. We apply elementary operations to make the top row positive.

We maximally apply the following iteratively: If $\delta_i \geq \delta_j > 0$, we subtract column j in column i.

After finishing the above, exactly one column of D has positive entry at the top. We move the column to the first column.

Now we have larger lower triangular matrix with positive diagonal. ...

Exercise 17.4

Why will the repeated operations terminate?

There is a Hermite normal form III

Proof.

$$\begin{bmatrix} \beta_{11} & 0 & 0 & 0 & 0 \\ \vdots & \ddots & 0 & 0 & 0 \\ \vdots & \dots & \beta_{ii} & 0 & 0 \\ \vdots & \dots & \dots & \ddots & 0 \\ \vdots & \dots & \dots & \dots & \beta_{nn} \end{bmatrix}$$

Phase 2: We can transform to $0 \leq \beta_{ij} < \beta_{ii}$

Now we apply column operations to bring non-diagonal entries in the range.

For each $i \in 2..n$ and $j \in 1..(i-1)$, we subtract jth column by $\lfloor \frac{\beta_{ij}}{\beta_{ii}} \rfloor$ times ith column.

The matrix is in HNF. □

Example : HNF

Example 17.3

Consider integral matrix $\begin{bmatrix} 2 & 3 & 6 \\ 2 & 1 & -3 \\ 1 & 1 & 3 \end{bmatrix}$

Phase 1: Make top row lower triangular

$$\rightsquigarrow \begin{bmatrix} 2 & 3 & 0 \\ 2 & 1 & -9 \\ 1 & 1 & 0 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & 1 & 0 \\ 2 & -1 & -9 \\ 1 & 0 & 0 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 0 & 1 & 0 \\ 4 & -1 & -9 \\ 1 & 0 & 0 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 & 0 \\ -1 & 4 & -9 \\ 0 & 1 & 0 \end{bmatrix}$$

Phase 1: Make middle row lower triangular

$$\rightsquigarrow \begin{bmatrix} 1 & 0 & 0 \\ -1 & 4 & 9 \\ 0 & 1 & 0 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 & 0 \\ -1 & 4 & 1 \\ 0 & 1 & -2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 & 0 \\ -1 & 0 & 1 \\ 0 & 9 & -2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -2 & 9 \end{bmatrix}$$

Phase 2: make non-diagonal nonnegative

$$\rightsquigarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & -2 & 9 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 7 & 7 & 9 \end{bmatrix}$$

Topic 17.4

Condition of satisfiability

Condition of satisfiability

Theorem 17.3

$Ax = b$ has an integral solution x, iff

$$\text{for each rational vector } y, \quad yA \text{ is integral} \Rightarrow yb \text{ is an integer.}$$

Proof.

($\Rightarrow$)

Let x_0 be a solution. If yA is integral, yAx_0 is an integer. Therefore, yb is an integer.

($\Leftarrow$)

Assumption implies $\forall y.\ yA = 0 \Rightarrow yb = 0$.(Why?)

Therefore, $Ax = b$ has rational solutions and we can assume A is full rank. ...

Commentary: Theorem 4.1a in Schrijver

Condition of satisfiability II

Proof(contd.)

Since the elementary operations do not affect the truth values of both sides,(Why?) we assume $A = [B\,0]$ is in HNF.

Since $B^{-1}[B\,0] = [\mathtt{I}\ 0]$, our assumption implies $B^{-1}b$ is integral.

Since $[B\,0]\begin{bmatrix} B^{-1}b \\ 0 \end{bmatrix} = b$, $x := \begin{bmatrix} B^{-1}b \\ 0 \end{bmatrix}$ is a solution of $Ax = b$. □

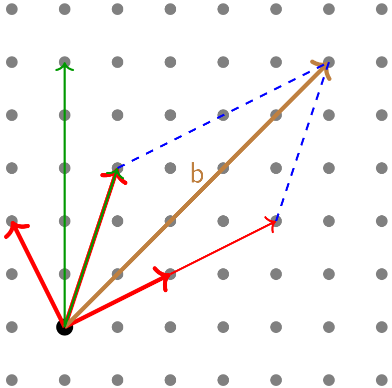
Example: solving equation

Example 17.4

Consider problem $\begin{bmatrix} 2 & 1 & -1 \\ 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 5 \\ 5 \end{bmatrix}$.

HNF of $\begin{bmatrix} 2 & 1 & -1 \\ 1 & 3 & 2 \end{bmatrix}$ is $\begin{bmatrix} 1 & 0 & 0 \\ 3 & 5 & 0 \end{bmatrix}$.

Solution of $\begin{bmatrix} 1 & 0 & 0 \\ 3 & 5 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 5 \\ 5 \end{bmatrix}$ is $\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 5 \\ -2 \\ 0 \end{bmatrix}$.



Exercise 17.5

What is the solution in terms of the original x_1, x_2, and x_3.

Topic 17.5

Lattice

Lattice

Definition 17.3

A set S of $\mathbb{R}^n$ is called additive group if

- $0 \in S$
- if $x \in S$, then $-x \in S$, and
- if $x, y \in S$, then $x + y \in S$.

Definition 17.4

A group S is generated by $a_1, \dots, a_m$ if $S = \{\lambda_1 a_1 + \dots + \lambda_m a_m | \lambda_1, \dots, \lambda_m \in \mathbb{Z}\}$

Definition 17.5

A group S is called lattice if it can be generated by linearly independent $a_1, \dots, a_m$. The vectors are called basis of S.

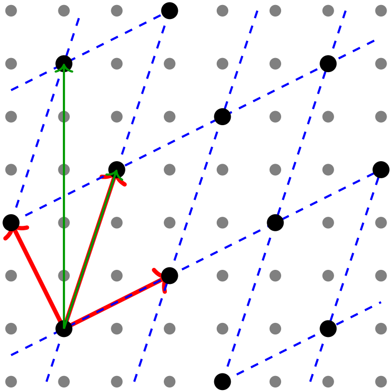
Exercise 17.6

Prove: If A is obtained by applying elementary operations on B, the group generated by A and B are same.

Example: HNF has same lattice

Example 17.5

Consider our earlier matrix $\begin{bmatrix} 2 & 1 & -1 \\ 1 & 3 & 2 \end{bmatrix}$ and its HNF $\begin{bmatrix} 1 & 0 & 0 \\ 3 & 5 & 0 \end{bmatrix}$



The HNF produces same lattice.

Exercise

Exercise 17.7

a) Give Hermite normal form of the following matrices.

$$\begin{bmatrix} 2 & 1 & 2 \\ -2 & -3 & 6 \end{bmatrix} \quad \begin{bmatrix} 6 & 3 & -9 \\ -3 & 8 & 4 \end{bmatrix}$$

b) Consider the lattices generated by the columns of the above matrices in 2-D space. What fraction of the integral points are not on each of the lattices?

c) If each of entry in the above matrices is multiplied by two, what would be the answers of (b).

A generated group is a lattice

Theorem 17.4
If a group S is generated by $a_1, ...a_m$, S is lattice.

Proof.
Let $a_1, ..., a_m$ be columns of A.

Wlog, let us suppose A is full row rank matrix.

We can convert A into HNF $[B\, 0]$.

Since columns of B are linearly independent, S is lattice. □

Exercise 17.8
Prove: If system $Ax = b$ has an integral solution, $B^{-1}b$ is integral.

Commentary: Theorem 4.1b in Schrijver

Hermite normal form is unique

Theorem 17.5

Let A and A' be rational matrices of full row rank, with HNFs $[B\ 0]$ and $[B'\ 0]$, respectively. If columns of A and A' generate same lattice, iff $B = B'$.

Proof.

($\Leftarrow$) trivial.

($\Rightarrow$)
Let lattice S be generated by columns of each A, B, A' and B'. Let $B := (\beta_{ij})$ and $B' := (\beta'_{ij})$.

Consider i be the first row where B and B' are different. Let it be at jth column.

Let b_j and b'_j be the jth column of B and B' respectively. …

Commentary: Theorem 4.2 in Schrijver

Hermite normal form is unique II

Proof(contd.)

$$
\begin{array}{c}
 \quad b_j \\
\begin{bmatrix}
\dots & \boxed{0} & 0 & 0 & 0 \\
\ddots & \ddots & 0 & 0 & 0 \\
\dots & \dots & \ddots & 0 & 0 \\
\dots & {\color{red}\beta_{ij}} & \dots & {\color{blue}\beta_{ii}} & 0 \\
\dots & \dots & \dots & \ddots & \ddots
\end{bmatrix}
\end{array}
\qquad
\begin{array}{c}
 \quad b'_j \\
\begin{bmatrix}
\dots & \boxed{0} & 0 & 0 & 0 \\
\ddots & \ddots & 0 & 0 & 0 \\
\dots & \dots & \ddots & 0 & 0 \\
\dots & {\color{red}\beta'_{ij}} & \dots & \beta'_{ii} & 0 \\
\dots & \dots & \dots & \ddots & \ddots
\end{bmatrix}
\end{array}
$$

Wlog $\beta_{ii} \geq \beta'_{ii}$.(Why?)

Therefore, $b_j - b'_j \in S$. $b_j - b'_j$ has zeros in the first $i-1$ entries.(Why?)

$b_j - b'_j$ is integer combination of $b_i, \dots, b_n$.(Why?)

Therefore, $\beta_{ij} - \beta'_{ij}$ is integer multiple of β_{ii}.

Since $0 \leq \beta_{ij} < \beta_{ii}$ and $0 \leq \beta'_{ij} < \beta'_{ii}$, $|\beta_{ij} - \beta'_{ij}| < \beta_{ii}$. Contradiction. □

Exercise 17.9

Prove: a full row rank matrix A has a unique HNF.

Exercise: Proof generation

Exercise 17.10

If there is no solution of $Ax = b$, how do we present the proof of unsatisfiability?

Topic 17.6

Hilbert basis

Hilbert basis

Definition 17.6

A finite set of vectors $a_1, \dots, a_m$ is Hilbert basis if each integral vector b in the cone generated by $\{a_1, \dots, a_m\}$ is nonnegative integral combination of $a_1, \dots, a_m$.

Example 17.6

Is the following an Hilbert basis?

- $\{\begin{bmatrix}2\\2\end{bmatrix}\}$
- $\{\begin{bmatrix}1\\1\end{bmatrix}\}$
- $\{\begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\}$
- $\{\begin{bmatrix}1\\-1\end{bmatrix}, \begin{bmatrix}1\\1\end{bmatrix}\}$

There is a Hilbert basis for each cone

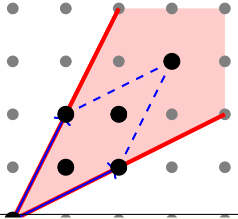
Theorem 17.6

Each rational cone C is generated by an integral Hilbert basis.

Proof.

Wlog, let $b_1, ..., b_m$ be a set of integral vectors that generate C.
Let $a_1, ..., a_t$ be all the integral vectors in $\{\lambda_1 b_1 + \cdots + \lambda_m b_m | 0 \leq \lambda_1, \ldots, \lambda_m \leq 1\}$. ...

Example 17.7



Black dots are a_is.

Commentary: Theorem 16.4 in Schrijver.

There is a Hilbert basis for each cone II

Proof(contd.)

Claim: $a_1, ..., a_t$ form a Hilbert basis

By definitions $\{b_1, ...b_m\} \subseteq \{a_1, ..., a_t\}$.

Consider integral vector $c \in C$. Therefore, $c = \lambda_1 b_1 + \cdots + \lambda_m b_m$ for $\lambda_i \geq 0$.

$$c = (\lfloor\lambda_1\rfloor b_1 + \cdots + \lfloor\lambda_m\rfloor b_m) + \underbrace{((\lambda_1 - \lfloor\lambda_1\rfloor)b_1 + \cdots + (\lambda_m - \lfloor\lambda_m\rfloor)b_m)}_{\in\{a_1,...,a_t\} \text{ (Why?)}}$$

c is nonnegative integral combination of $a_1, ..., a_t$. □

Exercise 17.11

Why the underbraced vector is integral?

Uniqueness of Hilbert basis

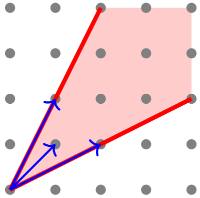
Theorem 17.7

Let C be a rational cone. If C has zero dimensional vertices, there is a unique minimal Hilbert basis for C.

Proof.

Let H be a set of integral vectors defined as follows. $a \in H$ iff

- $a \in C$,
- $a \neq 0$, and
- a is not sum of any of the other two nonzero integral vectors in C. ...



Exercise 17.12

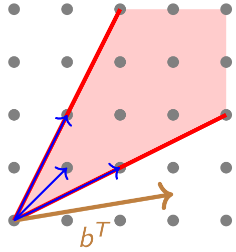
Show: H is subset of any Hilbert basis generating C.

Commentary: Theorem 16.4 in Schrijver. (second half)

Uniqueness of Hilbert basis II

Proof(contd.)

Claim: H is a Hilbert basis generating C.



Choose b such that $bx > 0$ for each $x \in C$.(Why exists?)
Choose $c \in C$ such that c is not a nonnegative integral combination of H.
Let bc be smallest.

Since $c \notin H$, $c_1 + c_2 = c$ for some nonzero integral $c_1, c_2 \in C$.
Therefore, $bc_1 < bc$ and $bc_2 < bc$.
Therefore, c_1 and c_2 are nonnegative integral combinations of H.
Therefore, c is nonnegative integral combination of H. Contradiction. □

Exercise 17.13

a. Why smallest bc? b. Show if C does not have zero dimensional vertices, H is not unique.

Topic 17.7

Problems

Finite infinite

Exercise 17.14

Consider formula F with single free variable in presburger arithmetic. Let $S = \{k | \mathcal{T}_{\mathbb{Z}} \models F(k)\}$.

- find a formula such that $S \cap \mathbb{Z}^+$ is finite.
- find a formula such that $\mathbb{Z}^+ - S$ is finite.

Topic 17.8

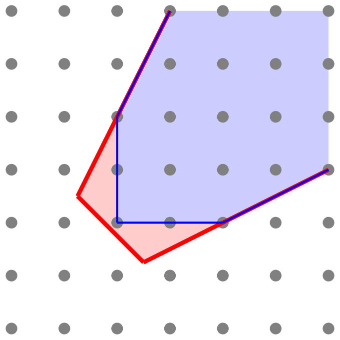
Extra slides : Integer hull

Integer hull

Let P be a polyhedron.

Definition 17.7

Let P_I be the convex hull of integers in P.



Exercise 17.15

Show: for a polyhedral cone C, $C = C_I$.

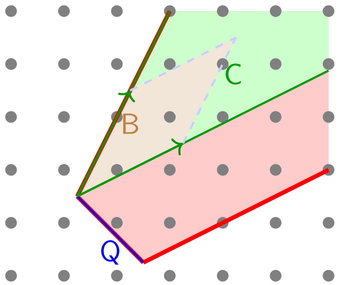
P_I is a polyhedron

Theorem 17.8

Let P be a rational polyhedron. P_I is also a polyhedron.

Proof.

Let $Q + C$, where Q is a polytope and C is the characteristic cone.



Let C be generated by integral vectors $a_1, ...a_s$. Let

$$B := \{\lambda_1 a_1 + \cdots + \lambda_s a_s | 0 \leq \lambda_1, \ldots, \lambda_s \leq 1\}.$$

Exercise 17.16

Draw $Q + B$.

...

Commentary: Theorem 16.1 in Schrijver. Please read 17.3 and 17.4 if possible.

P_I is a polyhedron

Proof(contd.)

Claim: $P_I = (Q+B)_I + C$

Clearly $(Q+B)_I \subseteq P_I$. Therefore, $(Q+B)_I + C \subseteq P_I + C \subseteq P_I + C_I \subseteq P_I$.

Let integral vector $p \in P$ such that $p = q + c$ for some $q \in Q$ and $c \in C$.

Let $c = \lambda_1 a_1 + \cdots + \lambda_s a_s$ for $\lambda_i \geq 0$.

Let $c' = \lfloor \lambda_1 \rfloor a_1 + \cdots + \lfloor \lambda_s \rfloor a_s \in C$.

Therefore $(c - c') \in B$ and $q + (c - c')$ is integral.

$q + (c - c') \in (Q+B)_I$. Hence, $P_I \subseteq (Q+B)_I + C$.

P_I is polyhedron and can be represented by some $Ax \leq b$. □

Topic 17.9

Extra slides : Total duality integrality

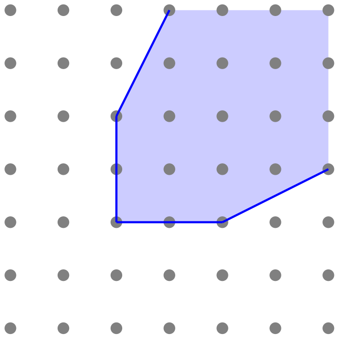
Integral

Definition 17.8

A polyhedron P is integral if all faces of P have integral vectors.

Faces include any thing that is facing exterior

- Vertices (minimal face)
- Edges
- Many dimensional surfaces



Some properties of faces

- Faces are obtained by converting one or more inequalities to equality.
- Faces are polyhedron themselves.
- Faces have subfaces
- There are minimal dimensional faces.
- All minimal dimensional faces
  - must have same dimension,
  - are affine spaces, and
  - are translation of each other.

Condition for being integral

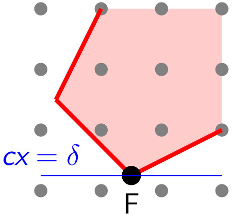
The hyperplanes that are "touching" P

Theorem 17.9

A rational polyhedron P is integral, iff each supporting hyperplane of P has integral vectors.

Proof.

($\Rightarrow$) trivial.



($\Leftarrow$) Assume $\neg$LHS. We prove $\neg$RHS.
Let $P = \{x | Ax \leq b\}$ for integral A and b, and
$F = \{x | A'x = b'\}$ be a minimal face of P, where $A'x \leq b'$ is a subsystem of $Ax \leq b$, without integral vectors.

Due to theorem 17.3, there is a y such that yA' is integral and yb' is not.
We add positive integers to components of y to make it positive.
Still yA' is integral and yb' is not. Let $c = yA'$ and $\delta = yb'$.
Clearly, $cx = \delta$ has no integral vectors.
Since $F \subseteq cx = \delta$ and $P \subseteq cx \leq \delta_{\text{(Why?)}}$, $cx = \delta$ is a supporting hyperplane. □

Commentary: Theorem 22.1 in Schrijver

Total duality integrality(TDI)

Definition 17.9
A rational system $Ax \leq b$ is totally dual integral if the minimum in the LP-duality equation

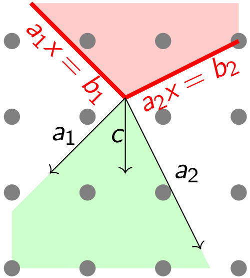
$$max\{cx | Ax \leq b\} = min\{yb | y \geq 0 \wedge yA = c\}$$

has an integral optimum y for each integral c for which the minimum is finite.

Example 17.8

max reaches optima at the corner of the red polyhedron,
if c is in the green cone.
TDI says that integral c is nonnegative integral combination of a_1 and a_2.

Therefore, a_1 and a_2 form an Hilbert basis.



Exercise 17.17
Prove: If $Ax \leq b$ is TDI, and $Ax \leq b \Rightarrow ax \leq \beta$, $Ax \leq b \wedge ax \leq \beta$ is a TDI.

TDI has integral optimum solutions

Theorem 17.10

If $Ax \leq b$ is TDI and b is integral, $\{x|Ax \leq b\}$ is integral.

Proof.

Let c be an integral row vector such that $max\{cx|Ax \leq b\}$ is finite.
Since $Ax \leq b$ is TDI and b is integral, $min\{yb|y \geq 0 \wedge yA = c\}$ is integer.(Why?)
$\delta = max\{cx|Ax \leq b\}$ is integer.
Let $H = \{x|cx = \delta\}$. H is a supporting hyperplane.
Wlog, we assume $gcd(c) = 1$. Therefore, $cx = \delta$ has integer solutions.

Due to theorem 17.9, $\{x|Ax \leq b\}$ is integral. □

Exercise 17.18

Let $Ax \leq b$ be TDI. If b and c are integral, and $max\{cx|Ax \leq b\}$ is finite, the max achieves optima at integral x.

Commentary: Theorem 22.1a-c in Schrijver

A face of TDI-system is TDI-system

Theorem 17.11

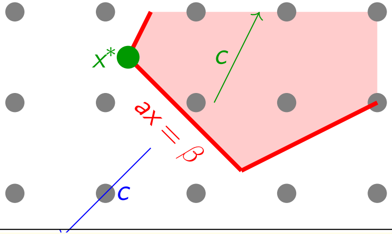
Let $Ax \leq b \wedge ax \leq \beta$ be TDI. Then, $Ax \leq b \wedge ax = \beta$ is also TDI.

Proof.

Let c be an integral vector, with

$$max\{cx|Ax \leq b \wedge ax = \beta\} = min\{yb + (\lambda - \mu)\beta|y, \lambda, \mu \geq 0 \wedge yA + (\lambda - \mu)a = c\}.$$

Let x^*, y^*, λ^* and μ^* attain the optima. ...



Two possibilities:

1. $\lambda * - \mu * \geq 0$
2. $\lambda * - \mu * < 0$

The second case can be handled by rotating c. No need of cases.

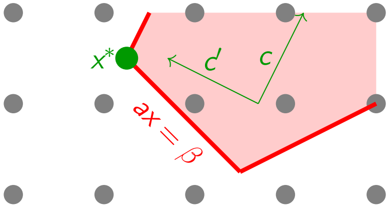
Commentary: Theorem 22.2 in Schrijver

A face of TDI-system is TDI-system II

Proof(contd.)

Let $c' = c + Na$ for some integer N such that $N \geq \mu*$ and Na is integral.

Removes negative a component from c



Then optima $max\{c'x | Ax \leq b \wedge ax \leq \beta\} = min\{yb + \lambda\beta | y, \lambda \geq 0 \wedge yA + \lambda a = c'\}$ is finite because

- $x := x^*$ satisfies $Ax \leq b \wedge ax \leq \beta$
- $y := y^*$, and $\lambda := \lambda^* + N - \mu^*$ satisfies $y, \lambda \geq 0 \wedge yA + \lambda a = c'$.

Commentary: N can vary well be $|max(0, \lambda^* - \mu^*)|$

A face of TDI-system is TDI-system III

Proof(contd.)

Since $Ax \leq b \wedge ax \leq \beta$ is TDI, the minimum in the above is attained by integral solution, say y_0, λ_0. Therefore, $y_0 b + \lambda_0 \beta \leq y^* b + (\lambda^* + N - \mu^*)\beta$.

Claim: $y = y_0$,$\lambda = \lambda_0$, $\mu = N$ also attains minimum in

$$max\{cx | Ax \leq b \wedge ax = \beta\} = min\{yb + (\lambda - \mu)\beta | y, \lambda, \mu \geq 0 \wedge yA + (\lambda - \mu)a = c\}.$$

Since $y_0 b + \lambda_0 \beta \leq y^* b + (\lambda^* + N - \mu^*)\beta$, after moving $N\beta$ rhs to lhs

$$y_0 b + (\lambda_0 - N)\beta \leq y^* b + (\lambda^* - \mu^*)\beta$$

Since $y = y^*, \lambda = \lambda^*, \mu = \mu^*$ attains the minimum, therefore $y = y_0$,$\lambda = \lambda_0$, $\mu = N$ attains the minimum. □

Hilbert basis and TDI

An inequality $ax \leq \delta$ of $Ax \leq b$ is active in F if $F \Rightarrow ax = \delta$

Theorem 17.12

Let $Ax \leq b$ be TDI iff, for each face F of $\{x | Ax \leq b\}$, the inequalities of $Ax \leq b$ that are active in F form a Hilbert basis.

Proof.

($\Rightarrow$)

Let $a_1 \leq \delta_1, \ldots, a_t \leq \delta_t$ be active on F.

Choose an integral vector c in the cone of $\{a_1, .., a_t\}$.

The maximum attained in the following

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

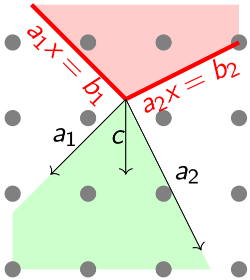
is achieved by x in F.(Why?)

Since $Ax \leq b$ is TDI, the minimum is achieved by integral y.

Due to complementary slackness, the components of y for non-active rows is 0.

Hence c is nonnegative integral combination of $a_1, ...a_t$.

...



Commentary: Theorem 22.5 in Schrijver

Hilbert basis and TDI

Proof(contd.)

($\Leftarrow$)
Let c be an integral row vector for which the following is finite.

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

Consider the largest F such that all x in F attain the maximum.(Why?)
Let $a_1 \leq \delta_1, \ldots, a_t \leq \delta_t$ be active on F.
c must be in the cone of $a_1, ..., a_t$.
Since they form an Hilbert basis $c = \lambda_1 a_1 + \cdots + \lambda_t a_t$ for $\lambda_1, ..., \lambda_t \geq 0$.
By zero padding, we can construct integral y such that $yA = c$ and $yb = yAx = cx$ for each x in F.
Therefore, y achives the minimum. Therefore, $Ax \leq b$ is TDI. □

Exercise 17.19

Why we need largest face F?

There is a TDI-system for each polyhedron

Theorem 17.13

For each rational polyhedron P, there is a TDI-system $Ax \leq b$ with A integral matrix and rational vector b such that $P = \{x | Ax \leq b\}$.

Proof.

Consider a minimal face F of P.

Let C_F be the cone of vectors c such that $max\{cx | x \in P\}$ is attained by $x \in F$

Let $a_1, \dots, a_t$ be integral Hilbert basis of C_F.

Let $x_0 \in F$. Therefore, for $1 \leq i \leq t$, $P \Rightarrow a_i x \leq a_i x_0$.

Let $A_F = \{a_1 x \leq a_1 x_0, ..., a_t x \leq a_t x_0\}$.

Let $Ax \leq b$ be union of inequalities A_F for each minimal F.

$Ax \leq b$ defines P(Why?) and is TDI due to theorem 17.12. □

Exercise 17.20

a. Why we need minimal face F?

Commentary: Theorem 22.6 in Schrijver

Topic 17.10

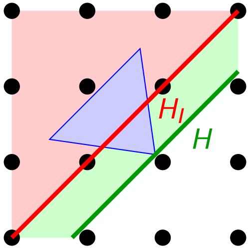
Extra slides: cutting planes

Cutting half spaces

Let $H = \{x | cx \leq \beta\}$ be half space, where $gcd(c) = 1$.

Definition 17.10

For a polyhedron P. Let $P' = \bigcap_{P \implies H} H_I$



Clearly, $P \supseteq P' \supseteq P'' ... \supseteq P^t \supseteq ... \supseteq P_I$.

We will show that the chain will saturate in finite steps.

Exercise 17.21

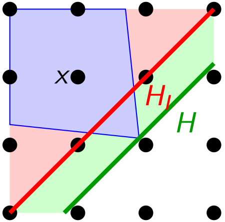
Give a P such that the saturation takes take multiple steps.

TDI-systems quickly finds P'

Theorem 17.14

Let $Ax \leq b$ be TDI and A is integral. Let $P = \{x | Ax \leq b\}$. $P' = \{x | Ax \leq \lfloor b \rfloor\}$

Proof.



If $P = \emptyset$, trivial.(Why?)

Let us assume $P \neq \emptyset$.

Clearly, $P' \subseteq \{x | Ax \leq \lfloor b \rfloor\}$.(Why?)

Claim: $P' \supseteq \{x | Ax \leq \lfloor b \rfloor\}$

Let $H = \{x | cx \leq \delta\}$ be a rational half-space such that $P \subseteq H$.

Wlog we assume $gcd(c) = 1$. Then, $H_I = \{x | cx \leq \lfloor \delta \rfloor\}$.

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

Since $Ax \leq b$ is TDI, the above min is attained by an integral y_0.

Chose x such that $Ax \leq \lfloor b \rfloor$. Therefore, $cx = y_0 Ax \leq y_0 \lfloor b \rfloor \leq \lfloor y_0 b \rfloor \leq \lfloor \delta \rfloor$.

So $\{x | Ax \leq \lfloor b \rfloor\} \subseteq H_I$.

As this is true for each rational half-space, the claim holds. □

Commentary: Theorem 23.1 in Schrijver

P' carries over to faces

Theorem 17.15

Let F be face of a rational polyhedron P. Then $F' = P' \cap F$

Proof.

Let $P = \{x | Ax \leq b\}$, with A integral and $Ax \leq b$ TDI.
Let $F = \{x | Ax \leq b \wedge ax = \beta\}$ for integral a and β and $P \Rightarrow ax \leq \beta$.(Why?)

Since $Ax \leq b \wedge ax \leq \beta$ is TDI(Why?), $Ax \leq b \wedge ax = \beta$ is TDI.

Therefore,

$$P' \cap F = \{x | Ax \leq \lfloor b \rfloor \wedge ax = \beta\} = \{x | Ax \leq \lfloor b \rfloor \wedge ax \leq \lfloor \beta \rfloor \wedge ax \geq \lfloor \beta \rfloor\} = F'$$

□

Commentary: Lemma of Theorem 23.1 in Schrijver

$P^t = P_I$

Theorem 17.16
For each rational polyhedron P, there exists a number t such that $P^t = P_I$.

Proof.
We apply induction over dimension d of P.

The case $P = \emptyset$ and $d = 0$ are trivial.

case: Let us suppose $affine.Hull(P)$ has no integers.

Therefore, there is integral vector c and non-integer δ such that $affine.Hull(P) \subseteq \{x | cx = \delta\}$.
Hence,

$$P' \subseteq \{x | cx \leq \lfloor \delta \rfloor \wedge cx \geq \lceil \delta \rceil\} = \emptyset.$$

Therefore, $P' = P_I$. ...

Commentary: Theorem 23.2 in Schrijver

$P^t = P_I$ II

Proof(contd).

case: Let us suppose *affine.Hull*(P) has integers.

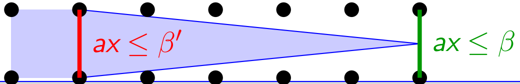
If *affine.Hull*(P) is not full dimensional, we project it to lower dimensions using Hermite Normal form and apply induction hypothesis.(How?)

Therefore, we may assume *affine.Hull*(P) is full dimensional.

Due to theorem **??**, we know $P_I = \{x | Ax \leq b'\}$ and $P = \{x | Ax \leq b\}$.

Let $ax \leq \beta'$ in $Ax \leq b'$, and there is a corresponding $ax \leq \beta$ in $Ax \leq b$.

Let $H = \{x | ax \leq \beta'\}$. ...



$P^t = P_I$ III

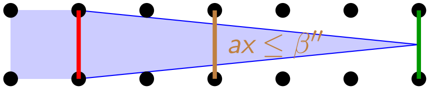
Proof(contd.)

Claim: $P^s \subseteq H$ for some s

Let us suppose for each s, we have $P^s \not\subseteq H$.

Therefore, there is an integer β'' and an integer r such that $\beta' < \beta'' \leq \lfloor \beta \rfloor$.

$$\{x|ax \leq \beta'' - 1\} \not\supseteq P^s \subseteq \{x|ax \leq \beta''\} \qquad \text{for each } s \geq r$$



Let $F = P^r \cap \{x|ax = \beta''\}$.

Due to $dim(F) < dim(P)$, F does not contain any integer(Why?), and induction hypothesis, $F^u = \emptyset$ for some u.

Therefore,

$$\emptyset = F^u = P^{(r+u)} \cap F = P^{(r+u)} \cap \{x|ax = \beta''\}$$

Therefore, $P^{(r+u)} \subseteq \{x|ax < \beta''\}$.

Cutting plane proofs

Let $Ax \leq b$ be a system of inequalities, and let $cx \leq \delta$ be an inequality.

Definition 17.11

A sequence of inequalities $c_1x \leq \delta_1, \dots, c_mx \leq \delta_m$ is a cutting plane proof of $cx \leq \delta$ from $Ax \leq b$ if

- $c_m = c$, $\delta_m = \delta$,
- c_1,....c_m are integral,
- $c_i = \Lambda A + \lambda_1 c_1 + \dots + \lambda_{i-1} c_{i-1}$, and
- $\delta_i \geq \lfloor \Lambda\delta + \lambda_1\delta_1 + \dots + \lambda_{i-1}\delta_{i-1} \rfloor$, where $\Lambda, \lambda_1, \dots, \lambda_{i-1} \geq 0$.

m is the length of the proof.

Cutting plane proofs always exist

Theorem 17.17

Let $P = \{x | Ax \leq b\}$ be a nonempty rational polyhedron.

- If $P_I \neq \emptyset$ and $P_I \Rightarrow cx \leq \delta$, then there is a cutting plane proof of $cx \leq \delta$ from $Ax \leq b$.
- If $P_I = \emptyset$, then there is a cutting plane proof of $0 \leq -1$ from $Ax \leq b$.

Proof.

Let t be such that $P^t = P_I$.

For each $i \geq 1$, there is a system $A_i x \leq b_i$ that defines P^i such that

- For each $\alpha x \leq \beta$ in $A_i x \leq b_i$, there is $yA_{i-1} = \alpha$ and $\beta = \lfloor yb_{i-1} \rfloor$.
- $A_0 = A$ and $b_0 = b$.

...

Commentary: Theorem 23.2b in Schrijver

Cutting plane proofs always exist

Proof(contd.)

If $P_I \neq \emptyset$ and $P_I \Rightarrow cx \leq \delta$, due to the Farkas lemma (affine form) $yA_t = c$ and $\delta \geq yb_t$.
Therefore, the following is the cutting proof of $cx \leq b$ from $Ax \leq b$,

$$A_1x \leq b_1, ..., A_tx \leq b_t, cx \leq b.$$

If $P_I = \emptyset$, then $yA_t = 0$ and $yb_t = -1$ for some $y \geq 0$.
Therefore, the following is the cutting proof of $0 \leq -1$ from $Ax \leq b$.

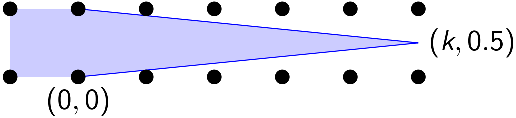
$$A_1x \leq b_1, ..., A_tx \leq b_t, 0x \leq -1.$$

□

Length of cutting plane proofs

The number of cutting planes depends on the size of numbers!

The following will trigger at least k cuts.



Topic 17.11

Problems

Find a TDI-system

Exercise 17.22

Write a program that takes an integral system $Ax \leq b$ as input, and finds a TDI-system that also defines polyhedron $\{x|Ax \leq b\}$.

- All groups will implement the program in C++
- Please feel free to consult any literature to implement the procedure efficiently but refrain from using high level libraries.
- Each group will submit 30 random inputs in the following format

```
A 2 3
1 3 4
3 3 5
b
6
8
```

- First row defines the size of matrix A [row_size] [column_size]
- Afterwards rows of integral A are written one after another
- Afterwards `b` indicates the start of vector b.
- Afterwards entries of b are listed.

Evaluation:

- We will pool submitted inputs and run all the submissions on the inputs
- The marks will be decided on the correctness of the submissions, their relative performances, and size of the found TDI-systems

End of Lecture 17