Automated Reasoning 2018

Lecture 13: Integer

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2018-09-04

Linear integer arithmetic (LIA)

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

Note: We have seen the axioms in the third lecture.

Example 13.1

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

- $x \geq 0 \vee y + z \approx 5$
- $x < 300 \wedge x - z \not\approx 5$

Syntactically, looks very similar to rational arithmetic.

Presburger arithmetic

Let us consider the following theory for arithmetic.

Decidable

Presburger [3EXPTIME]

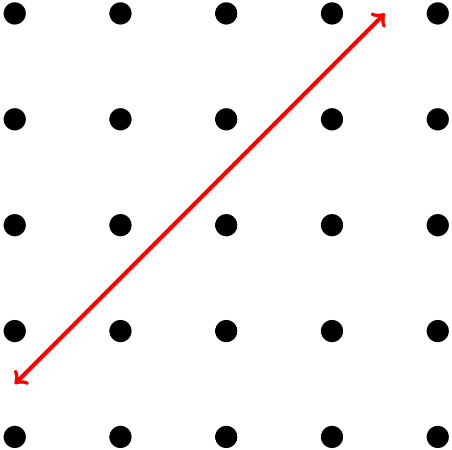
$$\begin{cases} \forall x \neg(x + 1 \approx 0) \\ \forall x \forall y (x + 1 \approx y + 1 \Rightarrow x \approx y) \\ F(0) \wedge (\forall x (F(x) \Rightarrow F(x+1)) \Rightarrow \forall x F(x)) \\ \forall x (x + 0 \approx x) \\ \forall x \forall y (x + (y+1) \approx (x+y) + 1) \end{cases}$$

Note that the theory does not have multiplication.

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

Difference in reasoning

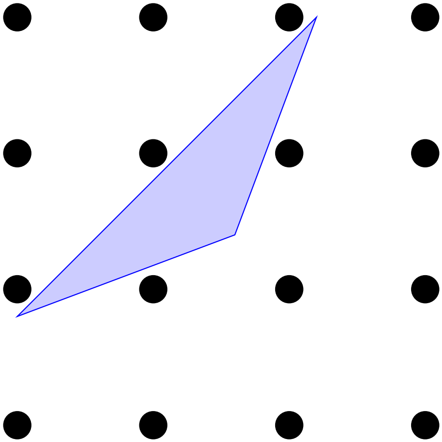
Integers are not dense. They are like a lattice in the space.



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?

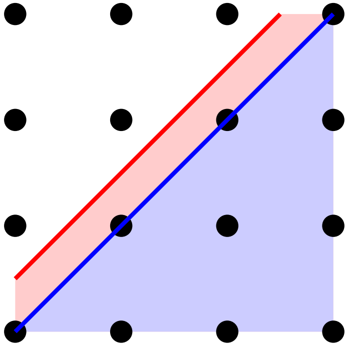
Reasoning over integer

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

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

Example: application of DIV rule

Example 13.2



$$[\text{DIV}]\frac{2x_1 + 2x_2 \leq 1}{\frac{2}{2}a_1x_1 + \frac{2}{2}x_2 \leq \left\lfloor \frac{1}{2} \right\rfloor} 2 = gcd(2,2)$$

Completeness

Are the two rules complete?

Topic 13.1

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 13.1

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 13.1

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 13.2

The following are elementary unimodular column operations

- *exchange two columns*
- *multiplying a column by* -1
- *adding* integral multiple *of a column to another*

Exercise 13.2

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

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

Exercise 13.3

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

There is a Hermite normal form

Theorem 13.1

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.

Let us suppose we have already 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 $D = \begin{bmatrix} \delta_1 & \dots & \delta_k \\ \vdots & \vdots & \vdots \end{bmatrix}$.

Apply elementary operations to make the top row positive.

We maximally apply the following operations iteratively.

If $\delta_i \geq \delta_j > 0$, we subtract column j in column i.

After finishing the iterations, exactly one column of D has positive entry at the top and we move the column to the first column.

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

Exercise 13.4

Why the repeated operations will finish?

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 13.3
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

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

Condition of satisfiability

Theorem 13.2

$Ax = b$ 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.

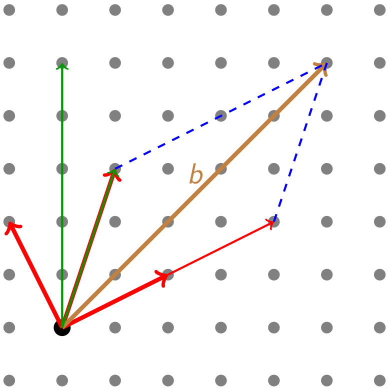
Since $B^{-1}[B\ 0] = [\mathtt{I}\ 0]$, our assumption implies $B^{-1}b$ is integral.

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 13.4

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 13.5

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

Lattice

Definition 13.3

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 13.4

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 13.5

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.

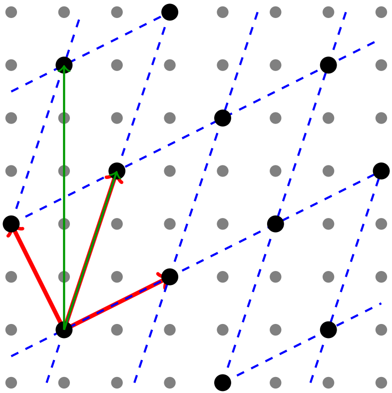
Exercise 13.6

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 13.5

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.

A generated group is a lattice

Theorem 13.3
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 13.7
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 13.4

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. ...

Commentary: Theorem 4.2 in Schrijver

Hermite normal form is unique II

Proof(contd.)

$$\begin{bmatrix} \dots & 0 & 0 & 0 & 0 \\ \ddots & \ddots & 0 & 0 & 0 \\ \dots & \dots & \ddots & 0 & 0 \\ \dots & \beta_{ij} & \dots & \beta_{ii} & 0 \\ \dots & \dots & \dots & \ddots & \ddots \end{bmatrix} \quad \begin{bmatrix} \dots & 0 & 0 & 0 & 0 \\ \ddots & \ddots & 0 & 0 & 0 \\ \dots & \dots & \ddots & 0 & 0 \\ \dots & \beta'_{ij} & \dots & \beta'_{ii} & 0 \\ \dots & \dots & \dots & \ddots & \ddots \end{bmatrix}$$

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

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

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

Topic 13.2

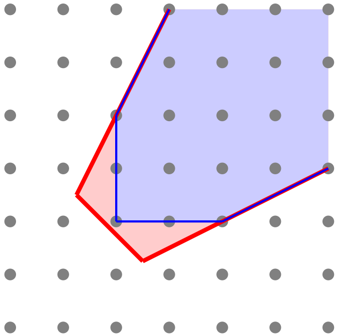
Integer hull

Integer hull

Let P be a polyhedron.

Definition 13.6

Let P_I be the convex hull of integers in P.



Exercise 13.9

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

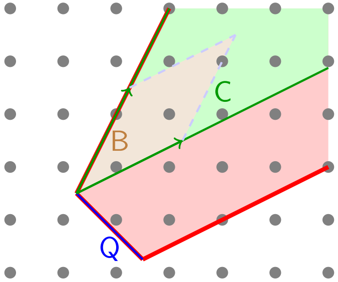
P_I is a polyhedron

Theorem 13.5

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 13.10 *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 13.3

Hilbert basis

Hilbert basis

Definition 13.7

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 13.6

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

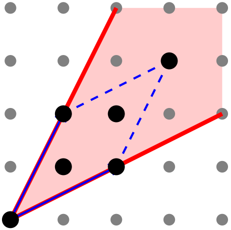
Theorem 13.6

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 appearing in

$$\{\lambda_1 b_1 + \cdots + \lambda_m b_m | 0 \leq \lambda_1, \ldots, \lambda_m \leq 1\}. \quad ...$$



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 13.11

Why the underbraced vector is integral?

Uniqueness of Hilbert basis

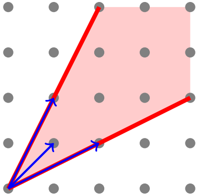
Theorem 13.7

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 integral vectors in C. ...



Exercise 13.12

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

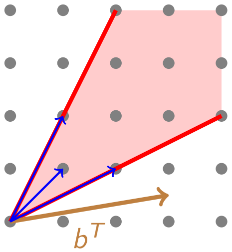
Commentary: Theorem 16.4 in Schrijver. (second half)

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?)
Let us choose $c \in C$, which is not any 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 13.13

Why smallest bc?

End of Lecture 13