IE 511: Integer Programming, Spring 2021 **18 Mar, 2021**

Lecture 16: Integer Farkas, Lattices

Lecturer: Karthik Chandrasekaran *Scribe: Karthik*

16.1 Linear Equations Integer Feasibility Problem

We were interested in the linear equations integer feasibility problem.

Recap: Linear Equations Integer Feasibility Problem (LEIF)

Given: $A \in \mathbb{Z}^{m \times n}, b \in \mathbb{Z}^m$
Goal: Does there exist $x \in \mathbb{Z}^n : Ax = b$?

Let us recap the example from the previous lecture. We were interested in knowing whether the following system of equations had an integral solution.

$$\begin{bmatrix} 2 & 1 & 6 & 4 \\ 7 & 2 & 5 & 5 \\ 8 & 3 & 33 & 10 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ 1 \end{bmatrix} \tag{16.1}$$

In the previous lecture, we saw a proof that this system does not have an integral solution. Today, we will discuss how to obtain a short proof/certificate that a linear system of equations has no integral solution.

A short certificate of no integral solution x for system (16.1) can be obtained via the following proposition.

Proposition 1. *Consider the system $Ax = b$. If there exists a vector y such that $y^T A$ is integral, but $y^T b$ is not an integer, then the system $Ax = b$ has no integral solution.*

Proof. Say $Ax = b$ had an integral solution $\bar{x}$. We should have $y^T A\bar{x} = y^T b$ for every vector y. Since $\bar{x}$ is integral and the vector y is such that $y^T A$ is integral, it follows that $y^T b$ (which is equal to $y^T A\bar{x}$) should be an integer. This contradicts the choice of y in the proposition and hence, $Ax = b$ has no integral solution. □

Let us reconsider the example again and see how to obtain a vector y satisfying the hypothesis of Proposition 1. Consider the final matrix B which was obtained by column operations in the previous lecture, i.e.,

$$B = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & -19 & 59 \end{bmatrix}.$$

Compute

$$B^{-1} = \begin{bmatrix} -1 & 0 & 0 \\ -2 & 1 & 0 \\ -\frac{41}{59} & \frac{19}{59} & \frac{1}{59} \end{bmatrix}.$$

Consider the transpose of the last row,

$$y := \begin{bmatrix} -\frac{41}{59} \\ \frac{19}{59} \\ \frac{1}{59} \end{bmatrix}.$$

Note that $y^T A = \begin{bmatrix} 1 & 0 & 1 & -2 \end{bmatrix}$ is integral where A is the constraint matrix of system (16.1), but $y^T b = \frac{17}{59}$ is not an integer; so, y is a short certificate of no integral solution for the system (16.1).

Next, let us formalize how to obtain such a short certificate of no solution to the linear equations feasibility problem (LEIF). In particular, we will see that the converse of Proposition 1 also holds—i.e., if there is no y such that $y^T A$ is integral but $y^T b$ is not an integer, then the system $Ax = b$ indeed has an integral solution.

In the example, we essentially did an integral version of Gaussian elimination to obtain the short certificate for no integral solution. In Gaussian elimination, we end up with a matrix that is in *row-reduced echelon form*. For Linear Equations *Integer* Feasibility Problem, matrices in the following form are helpful to derive a short certificate of no solution.

Definition 2. Let A be a $m \times n$ rational matrix. The matrix A is in *Hermite Normal Form* (HNF) if $A = \begin{bmatrix} B & 0 \end{bmatrix}$ where B is lower-triangular, has non-negative entries, with the diagonal entry being the unique maximum entry in each row.

Similar to Gaussian elimination which converts a matrix to row-reduced echelon form by elementary row operations, we can convert a rational matrix to HNF by certain elementary column operations. Note what we call as "elementary column operations" in the following theorem.

Theorem 3. *Any rational matrix M of full row rank can be converted to HNF by a sequence of elementary column operations which involve:*

(i) exchanging columns,

(ii) multiplying a column by -1, and

(iii) adding an integral multiple of one column to another.

Proof. **Exercise.**

By this theorem, $\text{HNF}(M) = MC$ for some integral matrix C. Hence, the HNF of an integral matrix will always be integral. This is summarized in the following corollary.

Corollary 3.1. *If M is integral, then HNF(M) is also integral.*

Moreover, if A has full row rank, then we can assume C to be a unimodular matrix. This is summarized in Theorem 5. Recall the definition of unimodular matrix:

Definition 4. A matrix U is *unimodular* if it is integral and $\det(U) \in \{\pm 1\}$.

Note: U is unimodular iff U^{-1} is unimodular. Also, unimodular is different from totally unimodular.

Theorem 5. *If A has full row rank, then*

(i) HNF(A) is unique and

(ii) there exists a unimodular matrix U such that HNF(M) $= MU$.

Proof. **Exercise.** *Hint: Revisit the proof of Theorem 3.*

With this background, we can now derive a Farkas type theorem for Linear Equations Integer Feasibility Problem.

Theorem 6 (Integer Farkas Lemma)**.** *Let $Ax = b$ be a rational linear system. There exists an integral solution x satisfying $Ax = b$ iff $y^T b$ is an integer for each rational vector y such that $y^T A$ is integral.*

Proof. The forward direction follows by Proposition 1. We prove the reverse direction. Suppose $y^T b$ is an integer for all y such that $y^T A$ is integral. This means that there is no y such that $y^T A = 0$ and $y^T b$ is not an integer. This implies that there is no y such that $y^T A = 0$ and $y^T b \neq 0$ (otherwise, scale y to violate the previous statement).

By theorem of alternatives (i.e., Linear Equations Feasibility Characterization), this implies that $Ax = b$ has a solution $x \in \mathbb{R}^n$.

We may assume that rows(A) are linearly independent (otherwise, work with a linearly independent subset of rows of A and the corresponding columns of b), i.e., A has full row rank.

Let $\text{HNF}(A) = AU$ for some unimodular matrix U. Then $AU = \begin{bmatrix} B & 0 \end{bmatrix}$ where B is invertible. Then $B^{-1} \begin{bmatrix} B & 0 \end{bmatrix} = \begin{bmatrix} I & 0 \end{bmatrix}$. Therefore, by taking $y^T = [B^{-1}]_j$ for any row j of the matrix B^{-1} makes $y^T B$ integral. That is, $y^T \begin{bmatrix} B & 0 \end{bmatrix}$ is integral which means that $y^T AU$ is integral, i.e., $y^T AUU^{-1}$ is integral (since U is unimodular). Therefore, $y^T A$ is integral and hence, $y^T b$ should be an integer. Thus, $y^T b$ is an integer for all rows y^T of B^{-1}.

Therefore, $B^{-1}b$ is an integral vector. Now we observe that

$$\text{HNF}(A) \begin{bmatrix} B^{-1}b \\ 0 \end{bmatrix} = \begin{bmatrix} B & 0 \end{bmatrix} \begin{bmatrix} B^{-1}b \\ 0 \end{bmatrix} = b.$$

This implies that $\begin{bmatrix} B^{-1}b \\ 0 \end{bmatrix}$ is an integral solution to the system $\text{HNF}(A)y = b$. Therefore, there exists an integral solution y to $AUy = b$. Consequently, there exists an integral solution x to $Ax = b$ (by setting $x = Uy$).

□

A feature of the proof. Note that the above proof is constructive in nature: Suppose we can find HNF(A). Then the proof tells us (1) how to find integral x satisfying $Ax = b$ or (2) how to find a certificate y to show that no such x exists—by computing HNF(A).

Next, in order to solve the Linear Equations Integer Feasibility Problem, we need to understand

1. how to compute the HNF of a given rational matrix efficiently and
2. does HNF(A) have entries bounded in the size of the entries of A?

The next theorem answers these two questions. Its proof is left as an exercise.

Theorem 7. *Given a full row ranked rational matrix A, let HNF$(A) = AU$ for some unimodular matrix U. Then,*

(i) size(U) = poly(size(A)) and hence size(HNF(A)) = poly(size(A)) and

(ii) U can be found efficiently.

Corollary 7.1. *If a rational linear system $Ax = b$ has an integral solution, then it has one whose size is bounded by a polynomial in the size of A and b and it can be found efficiently.*

Next, let us see a broader theory of linear equations integer feasibility. We will see some important problems which themselves are related to integer optimization. These problems are themselves integer optimization problems and hence are very much within the scope of this course. These are active areas of research so we will see some research problems as well.

16.2 Lattices

Recall the linear equations integer feasibility problem: Does there exist $x \in \mathbb{Z}^n : Ax = b$? This question is equivalent to asking if b can be expressed as an *integer* linear combination of columns of A? This leads us to the notion of lattices.

Observation. Let $a_1, \ldots, a_m \in \mathbb{R}^n$. Consider $\mathcal{L}(a_1, \ldots, a_m) := \{\sum_{i=1}^m \lambda_i a_i : \lambda_1, \ldots, \lambda_m \in \mathbb{Z}\}$. Then, $\mathcal{L}(a_1, \ldots, a_m)$ is a *group* under addition. i.e., $\mathcal{L}$ satisfies the following properties:

(i) closure, i.e., $x, y \in \mathcal{L} \implies x + y \in \mathcal{L}$,

(ii) associativity, i.e., $\forall x, y, z \in \mathcal{L}, (x + y) + z = x + (y + z)$,

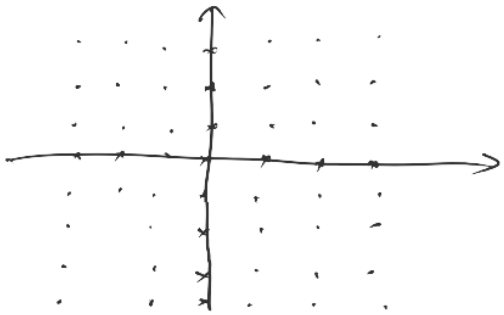
(iii) has an identity element, i.e., $0 \in \mathcal{L}$ and $0 + x = x \ \forall x \in \mathcal{L}$, and

(iv) has an inverse, i.e., $x \in \mathcal{L} \implies -x \in \mathcal{L}$.

The set $\mathcal{L}(a_1, \ldots, a_m)$ is called a lattice.

Definition 8. A set $\mathcal{L} \subseteq \mathbb{R}^n$ is a *lattice* if it is the collection of integer linear combinations of a linearly independent set of vectors. This linearly independent set of vectors is called a *basis/generator* of the lattice.

Example: $a_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $a_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \implies \mathcal{L}(a_1, a_2) = \mathbb{Z}^2$



Note: A lattice has multiple basis.

Example:

$$b_1 = \begin{bmatrix}1\\0\end{bmatrix}, \qquad b_2 = \begin{bmatrix}1\\1\end{bmatrix}, \qquad a_1 = \begin{bmatrix}1\\0\end{bmatrix}, \qquad a_2 = \begin{bmatrix}0\\1\end{bmatrix}$$

Then $\mathcal{L}(b_1, b_2) = \mathbb{Z}^2 = \mathcal{L}(a_1, a_2)$.

We have the following proposition about the elementary column operations from Theorem 3. Its proof is left as an **exercise**.

Proposition 9. *If matrix B is obtained by applying elementary column operations (i), (ii), (iii) mentioned in Theorem 3 to a matrix A, then the columns of A generate the same lattice as the columns of B.*

Lattices were initially studied in geometry and in other areas. They were also studied in IP literature because we can rephrase IP in the following equivalent form: is $Ax = b, x \geq 0, x \in \mathbb{Z}^n$ feasible? This is equivalent to asking whether b lies in the lattice generated by the columns of A and moreover, whether b is obtained as a non-negative integer linear combination of columns of A. More recently, lattices have found applications in coding theory and cryptography. In fact, the Abel prize in 2021 was awarded to Lovasz for his work on lattices. Let us understand some basic computational problems related to lattices which lead to these applications.

Before we see these problems, let us summarize some properties of lattices.

Lemma 9.1. *Let $B = \begin{bmatrix} b_1 & \dots & b_n \end{bmatrix}$ where $b_i \in \mathbb{R}^n$. If B is unimodular, then $\mathcal{L}(b_1, \dots, b_n) = \mathbb{Z}^n$.*

Proof. **Exercise**. *Hint: Cramer's rule.* □

Lemma 9.2. *If $\mathcal{L}(b_1, \dots, b_n) = \mathcal{L}(b'_1, \dots, b'_n)$ then $B = B'U$ for some unimodular matrix U where $B = \begin{bmatrix} b_1 & \dots & b_n \end{bmatrix}$ and $B' = \begin{bmatrix} b'_1 & \dots & b'_n \end{bmatrix}$.*

Proof. $\mathcal{L}(b_1, \dots, b_n) = \mathcal{L}(b'_1, \dots, b'_n)$. It means that b'_i is an integer combination of $b_1, \dots, b_n$. i.e., the columns of B' are integer linear combinations of columns of B and vice-versa. It implies that $B' = BM$ and $B = B'M'$ for some integral matrices M and M'.

$B' = BM = B'M'M \implies M'M = I$.

M and M' are integral matrices. So, $\det(M)$ and $\det(M')$ are integers. Therefore,

$$\begin{aligned} & 1 = \det(I) = \det(M)\det(M') \\ \implies & \det(M), \det(M') \in \{\pm 1\} \\ \implies & M, M' \text{ are unimodular.} \end{aligned}$$

□

To define the computational problems associated with lattices, we need the notion of determinant of a lattice $\mathcal{L}$.

Definition 10. For a lattice $\mathcal{L}$, *det*$(\mathcal{L}) := \left|\det \begin{bmatrix} b_1 & \dots & b_n \end{bmatrix}\right|$ for some basis $b_1, \dots, b_n$ of $\mathcal{L}$.

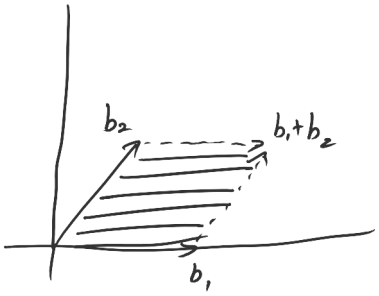
Proposition 11. *Det*$(\mathcal{L})$ *is independent of the basis.*

Proof. Suppose columns of B and columns of B' are both basis for $\mathcal{L}$. Then

$$|\det(B)| = |\det(B'U')| = |\det(B')||\det(U')| = |\det(B')|.$$

□

$\text{Det}(\mathcal{L})$ has a nice geometric interpretation. E.g., suppose $\mathcal{L} = \mathcal{L}(b_1, b_2)$. Then, $\det(\mathcal{L}) = \left|\det \begin{bmatrix} b_1 & b_2 \end{bmatrix}\right|$ is the volume of parallelepiped defined by b_1 and b_2.



More generally, $\det(\mathcal{L})$ is the volume of parallelepiped defined by the generators $b_1, \dots, b_n$. Using this interpretation we have that if $\mathcal{L}$ has a basis $b_1, \dots, b_n$ that are pairwise orthogonal, then $\det(\mathcal{L}) = \prod_{i=1}^{n} \|b_i\|$.

If they are not orthogonal, then we have the following relation.

Proposition 12 (Hadamard's inequality)**.** *Let* $\mathcal{L}$ *be a lattice. Then, det*$(\mathcal{L}) \leq \prod_{i=1}^{n} \|b_i\| \quad \forall$ *basis* $b_1, \dots, b_n$ *of* $\mathcal{L}$*.*

Hadamard's inequality can be shown using Gram-Schmidt orthogonalization.

16.3 Computational Problems on Lattices

16.3.1 Membership testing problem

Given: A basis $b_1, \ldots, b_n \in \mathbb{R}^n$ of a lattice Ł and a vector $t \in \mathbb{R}^n$.
Goal: Is $t \in \mathcal{L}(b_1, \ldots, b_n)$?

This is the linear equations integer feasibility problem (LEIF).

$$\exists x \in \mathbb{Z}^n : \begin{bmatrix} b_1 & \ldots & b_n \end{bmatrix} x = t? \tag{16.2}$$

We know how to solve (16.2) in polynomial time using the Hermite basis for the lattice.

Significance of Membership Testing Problem.

Consider the decision IP $\{Ax = b, x \geq 0, x \in \mathbb{Z}^n\}$. We can relax this IP in two ways.

- Relaxation I: $\{Ax = b, x \geq 0\}$ (LP)
- Relaxation II: $\{Ax = b, x \in \mathbb{Z}^n\}$ (LEIF)

Note that both relaxations are solvable efficiently.