15.083J/6.859J Integer Optimization

Lecture 13: Lattices I

1 Outline

Slide 1

- Integer points in lattices.
- Is $\{\boldsymbol{x} \in \mathcal{Z}^n \mid \boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}\}$ nonempty?

2 Integer points in lattices

Slide 2

- $\boldsymbol{B} = [\boldsymbol{b}^1, \ldots, \boldsymbol{b}^d] \in \mathcal{R}^{n \times d}$, $\boldsymbol{b}^1, \ldots, \boldsymbol{b}^d$ are linearly independent.

$$\mathcal{L} = \mathcal{L}(\boldsymbol{B}) = \{\boldsymbol{y} \in \mathcal{R}^n \mid \boldsymbol{y} = \boldsymbol{B}\boldsymbol{v}, \quad \boldsymbol{v} \in \mathcal{Z}^d\}$$

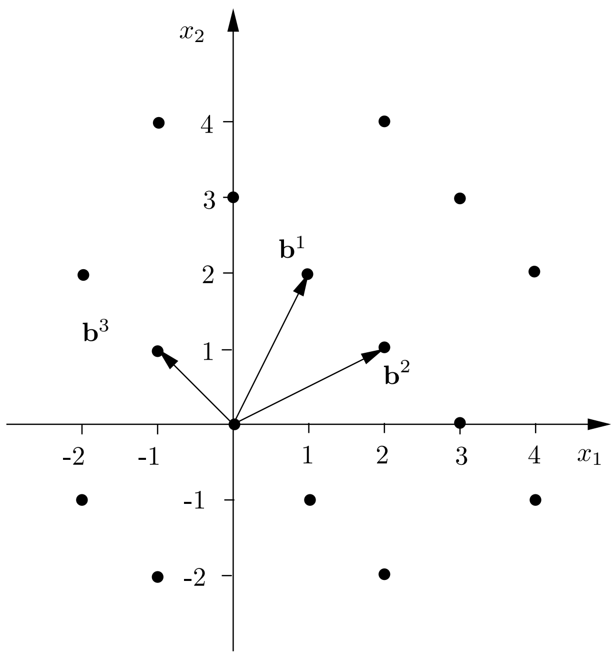
  is called the **lattice** generated by $\boldsymbol{B}$. $\boldsymbol{B}$ is called a **basis** of $\mathcal{L}(\boldsymbol{B})$.

- $\boldsymbol{b}^i = \boldsymbol{e}_i$, $i = 1, \ldots, n$ $\boldsymbol{e}_i$ is the i-th unit vector, then $\mathcal{L}(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n) = \mathcal{Z}^n$.
- $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{L}(\boldsymbol{B})$ and $\lambda, \mu \in \mathcal{Z}$, $\lambda\boldsymbol{x} + \mu\boldsymbol{y} \in \mathcal{L}(\boldsymbol{B})$.

2.1 Multiple bases

Slide 3

$\boldsymbol{b}^1 = (1,2)'$, $\boldsymbol{b}^2 = (2,1)'$, $\boldsymbol{b}^3 = (1,-1)'$. Then, $\mathcal{L}(\boldsymbol{b}^1, \boldsymbol{b}^2) = \mathcal{L}(\boldsymbol{b}^2, \boldsymbol{b}^3)$.



2.2 Alternative bases

SLIDE 4

Let $\boldsymbol{B} = [\boldsymbol{b}^1, \ldots, \boldsymbol{b}^d]$ be a basis of the lattice $\mathcal{L}$.

- If $\boldsymbol{U} \in \mathcal{R}^{d\times d}$ is unimodular, then $\overline{\boldsymbol{B}} = \boldsymbol{BU}$ is a basis of the lattice $\mathcal{L}$.
- If $\boldsymbol{B}$ and $\overline{\boldsymbol{B}}$ are bases of $\mathcal{L}$, then there exists a unimodular matrix $\boldsymbol{U}$ such that $\overline{\boldsymbol{B}} = \boldsymbol{BU}$.
- If $\boldsymbol{B}$ and $\overline{\boldsymbol{B}}$ are bases of $\mathcal{L}$, then $|\det(\boldsymbol{B})| = |\det(\overline{\boldsymbol{B}})|$.

2.3 Proof

SLIDE 5

- For all $\boldsymbol{x} \in \mathcal{L}$: $\boldsymbol{x} = \boldsymbol{Bv}$ with $\boldsymbol{v} \in \mathcal{Z}^d$.
- $\det(\boldsymbol{U}) = \pm 1$, and $\det(\boldsymbol{U}^{-1}) = 1/\det(\boldsymbol{U}) = \pm 1$.
- $\boldsymbol{x} = \boldsymbol{BUU}^{-1}\boldsymbol{v}$.
- From Cramer's rule, $\boldsymbol{U}^{-1}$ has integral coordinates, and thus $\boldsymbol{w} = \boldsymbol{U}^{-1}\boldsymbol{v}$ is integral.
- $\overline{\boldsymbol{B}} = \boldsymbol{BU}$. Then, $\boldsymbol{x} = \overline{\boldsymbol{B}}\boldsymbol{w}$, with $\boldsymbol{w} \in \mathcal{Z}^d$, which implies that $\overline{\boldsymbol{B}}$ is a basis of $\mathcal{L}$.
- $\boldsymbol{B} = [\boldsymbol{b}^1, \ldots, \boldsymbol{b}^d]$ and $\overline{\boldsymbol{B}} = [\overline{\boldsymbol{b}}^1, \ldots, \overline{\boldsymbol{b}}^d]$ be bases of $\mathcal{L}$. Then, the vectors $\boldsymbol{b}^1, \ldots, \boldsymbol{b}^d$ and the vectors $\overline{\boldsymbol{b}}^1, \ldots, \overline{\boldsymbol{b}}^d$ are both linearly independent.
- $V = \{\boldsymbol{By} \mid \boldsymbol{y} \in \mathcal{R}^n\} = \{\overline{\boldsymbol{B}}\boldsymbol{y} \mid \boldsymbol{y} \in \mathcal{R}^n\}$.
- There exists an invertible $d \times d$ matrix $\boldsymbol{U}$ such that
$$\boldsymbol{B} = \overline{\boldsymbol{B}}\boldsymbol{U} \text{ and } \overline{\boldsymbol{B}} = \boldsymbol{BU}^{-1}.$$
- $\boldsymbol{b}^i = \overline{\boldsymbol{B}}\boldsymbol{U}_i$, $\boldsymbol{U}_i \in \mathcal{Z}^d$ and $\overline{\boldsymbol{b}}^i = \boldsymbol{BU}_i^{-1}$, $\boldsymbol{U}_i^{-1} \in \mathcal{Z}^d$.
- $\boldsymbol{U}$ and $\boldsymbol{U}^{-1}$ are both integral, and thus both $\det(\boldsymbol{U})$ and $\det(\boldsymbol{U}^{-1})$ are integral, leading to $\det(\boldsymbol{U}) = \pm 1$.
- $|\det(\overline{\boldsymbol{B}})| = |\det(\boldsymbol{B})||\det(\boldsymbol{U})| = |\det(\boldsymbol{B})|$.

2.4 Convex Body Theorem

SLIDE 6

Let $\mathcal{L}$ be a lattice in $\mathcal{R}^n$ and let $A \in \mathcal{R}^n$ be a convex set such that $\text{vol}(A) > 2^n \det(\mathcal{L})$ and A is symmetric around the origin, i.e., $\boldsymbol{z} \in A$ if and only if $-\boldsymbol{z} \in A$. Then A contains a non-zero lattice point.

2.5 Integer normal form

SLIDE 7

- $\boldsymbol{A} \in \mathcal{Z}^{m\times n}$ of full row rank is in **integer normal form**, if it is of the form $[\boldsymbol{B}, \boldsymbol{0}]$, where $\boldsymbol{B} \in \mathcal{Z}^{m\times m}$ is invertible, has integral elements and is lower triangular.
- Elementary operations:
  (a) Exchanging two columns;
  (b) Multiplying a column by -1.
  (c) Adding an integral multiple of one column to another.
- Theorem: (a) A full row rank $\boldsymbol{A} \in \mathcal{Z}^{m\times n}$ can be brought into the integer normal form $[\boldsymbol{B}, \boldsymbol{0}]$ using elementary column operations;
  (b) There is a unimodular matrix $\boldsymbol{U}$ such that $[\boldsymbol{B}, \boldsymbol{0}] = \boldsymbol{AU}$.

2.6 Proof

- We show by induction that by applying elementary column operations (a)-(c), we can transform $\boldsymbol{A}$ to
$$\begin{bmatrix} \alpha & \boldsymbol{0} \\ \boldsymbol{v} & \boldsymbol{C} \end{bmatrix}, \tag{1}$$
where $\alpha \in \mathcal{Z}_+ \setminus \{0\}$, $\boldsymbol{v} \in \mathcal{Z}^{m-1}$ and $\boldsymbol{C} \in \mathcal{Z}^{(m-1)\times(n-1)}$ is of full row rank. By proceeding inductively on the matrix $\boldsymbol{C}$ we prove part (a).
- By iteratively exchanging two columns of $\boldsymbol{A}$ (Operation (a)) and possibly multiplying columns by -1 (Operation (b)), we can transform $\boldsymbol{A}$ (and renumber the column indices) such that
$$a_{1,1} \geq a_{1,2} \geq \ldots \geq a_{1,n} \geq 0.$$
- Since $\boldsymbol{A}$ is of full row rank, $a_{1,1} > 0$. Let $k = \max\{i : \ a_{1,i} > 0\}$. If $k = 1$, then we have transformed $\boldsymbol{A}$ into a matrix of the form (1). Otherwise, $k \geq 2$ and by applying $k-1$ operations (c) we transform $\boldsymbol{A}$ to
$$\overline{\boldsymbol{A}} = \left[\boldsymbol{A}_1 - \left\lfloor \frac{a_{1,1}}{a_{1,2}} \right\rfloor \boldsymbol{A}_2, \ldots, \boldsymbol{A}_{k-1} - \left\lfloor \frac{a_{1,k-1}}{a_{1,k}} \right\rfloor \boldsymbol{A}_k, \boldsymbol{A}_k, \boldsymbol{A}_{k+1}, \ldots, \boldsymbol{A}_n\right].$$
- Repeat the process to $\overline{\boldsymbol{A}}$, and exchange two columns of $\overline{\boldsymbol{A}}$ such that
$$\overline{a}_{1,1} \geq \overline{a}_{1,2} \geq \ldots \geq \overline{a}_{1,n} \geq 0.$$
- $\max\{i : \ \overline{a}_{1,i} > 0\} \leq k$
$$\sum_{i=1}^{k} \overline{a}_{1,i} \leq \sum_{i=1}^{k-1} (a_{1,i} - a_{1,i+1}) + a_{1,k} = a_{1,1} < \sum_{i=1}^{k} a_{1,i},$$
which implies that after a finite number of iterations $\boldsymbol{A}$ is transformed by elementary column operations (a)-(c) into a matrix of the form (1).
- Each of the elementary column operations corresponds to multiplying matrix $\boldsymbol{A}$ by a unimodular matrix as follows:

  (i) Exchanging columns k and j of matrix $\boldsymbol{A}$ corresponds to multiplying matrix $\boldsymbol{A}$ by a unimodular matrix $\boldsymbol{U}_1 = \boldsymbol{I} + \boldsymbol{I}_{k,j} + \boldsymbol{I}_{j,k} - \boldsymbol{I}_{k,k} - \boldsymbol{I}_{j,j}$. $\det(\boldsymbol{U}_1) = -1$.

  (ii) Multiplying column j by -1 corresponds to multiplying matrix $\boldsymbol{A}$ by a unimodular matrix $\boldsymbol{U}_2 = \boldsymbol{I} - 2\boldsymbol{I}_{j,j}$, that is an identity matrix except that element (j,j) is -1. $\det(\boldsymbol{U}_2) = -1$.

  (iii) Adding $f \in \mathcal{Z}$ times column k to column j, corresponds to multiplying matrix $\boldsymbol{A}$ by a unimodular matrix $\boldsymbol{U}_3 = \boldsymbol{I} + f\boldsymbol{I}_{k,j}$. Since $\det(\boldsymbol{U}_3) = 1$, $\boldsymbol{U}_3$ is unimodular.
- Performing two elementary column operations corresponds to multiplying the corresponding unimodular matrices resulting in another unimodular matrix.

2.7 Example

SLIDE 9

- $$\begin{bmatrix} 3 & -4 & 2 \\ 1 & 0 & 7 \end{bmatrix} \longrightarrow \begin{bmatrix} 4 & 3 & 2 \\ 0 & 1 & 7 \end{bmatrix}$$

- $$\begin{bmatrix} 1 & 1 & 2 \\ -1 & -6 & 7 \end{bmatrix}$$

- Reordering the columns
$$\begin{bmatrix} 2 & 1 & 1 \\ 7 & -6 & -1 \end{bmatrix}$$

- Replacing columns one and two by the difference of the first and twice the second column and the second and third column, respectively, yields
$$\begin{bmatrix} 0 & 0 & 1 \\ 19 & -5 & -1 \end{bmatrix}.$$

- Reordering the columns
$$\begin{bmatrix} 1 & 0 & 0 \\ -1 & 19 & -5 \end{bmatrix}.$$

- Continuing with the matrix $\boldsymbol{C} = [19, -5]$, we obtain successively, the matrices $[19, 5]$, $[4, 5]$, $[5, 4]$, $[1, 4]$, $[4, 1]$, $[0, 1]$, and $[1, 0]$. The integer normal form is:
$$\begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \end{bmatrix}.$$

2.8 Characterization

SLIDE 10

$\boldsymbol{A} \in \mathcal{Z}^{m\times n}$, full row rank; $[\boldsymbol{B}, \boldsymbol{0}] = \boldsymbol{AU}$. Let $\boldsymbol{b} \in \mathcal{Z}^m$ and $S = \{\boldsymbol{x} \in \mathcal{Z}^n \mid \boldsymbol{Ax} = \boldsymbol{b}\}$.

(a) The set S is nonempty if and only if $\boldsymbol{B}^{-1}\boldsymbol{b} \in \mathcal{Z}^m$.

(b) If $S \neq \emptyset$, every solution of S is of the form

$$\boldsymbol{x} = \boldsymbol{U}_1\boldsymbol{B}^{-1}\boldsymbol{b} + \boldsymbol{U}_2\boldsymbol{z},\ \ \boldsymbol{z} \in \mathcal{Z}^{n-m},$$

where $\boldsymbol{U}_1$, $\boldsymbol{U}_2$: $\boldsymbol{U} = [\boldsymbol{U}_1, \boldsymbol{U}_2]$.

(c) $\mathcal{L} = \{\boldsymbol{x} \in \mathcal{Z}^n \mid \boldsymbol{Ax} = \boldsymbol{0}\}$ is a lattice and the column vectors of $\boldsymbol{U}_2$ constitute a basis of $\mathcal{L}$.

2.9 Proof

SLIDE 11

- $\boldsymbol{y} = \boldsymbol{U}^{-1}\boldsymbol{x}$. Since $\boldsymbol{U}$ is unimodular, $\boldsymbol{y} \in \mathcal{Z}^n$ if and only if $\boldsymbol{x} \in \mathcal{Z}^n$. Thus, S is nonempty if and only if there exists a $\boldsymbol{y} \in \mathcal{Z}^n$ such that $[\boldsymbol{B}, \boldsymbol{0}]\boldsymbol{y} = \boldsymbol{b}$. Since $\boldsymbol{B}$ is invertible, the latter is true if and only $\boldsymbol{B}^{-1}\boldsymbol{b} \in \mathcal{Z}^m$.

- We can express the set S as follows:

$$\begin{aligned} S &= \{\boldsymbol{x} \in \mathcal{Z}^n \mid \boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}\} \\ &= \{\boldsymbol{x} \in \mathcal{Z}^n \mid \boldsymbol{x} = \boldsymbol{U}\boldsymbol{y},\ [\boldsymbol{B}, \boldsymbol{0}]\boldsymbol{y} = \boldsymbol{b},\ \boldsymbol{y} \in \mathcal{Z}^n\} \\ &= \{\boldsymbol{x} \in \mathcal{Z}^n \mid \boldsymbol{x} = \boldsymbol{U}_1\boldsymbol{w} + \boldsymbol{U}_2\boldsymbol{z},\ \boldsymbol{B}\boldsymbol{w} = \boldsymbol{b},\ \boldsymbol{w} \in \mathcal{Z}^m,\ \boldsymbol{z} \in \mathcal{Z}^{n-m}\}. \end{aligned}$$

  Thus, if $S \neq \emptyset$, then $\boldsymbol{B}^{-1}\boldsymbol{b} \in \mathcal{Z}^m$ from part (a) and hence,

$$S = \{\boldsymbol{x} \in \mathcal{Z}^n \mid \boldsymbol{x} = \boldsymbol{U}_1\boldsymbol{B}^{-1}\boldsymbol{b} + \boldsymbol{U}_2\boldsymbol{z},\ \boldsymbol{z} \in \mathcal{Z}^{n-m}\}.$$

- Let $\mathcal{L} = \{\boldsymbol{x} \in \mathcal{Z}^n \mid \boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}\}$. By setting $\boldsymbol{b} = \boldsymbol{0}$ in part (b) we obtain that

$$\mathcal{L} = \{\boldsymbol{x} \in \mathcal{Z}^n \mid \boldsymbol{x} = \boldsymbol{U}_2\boldsymbol{z},\ \boldsymbol{z} \in \mathcal{Z}^{n-m}\}.$$

  Thus, by definition, $\mathcal{L}$ is a lattice with basis $\boldsymbol{U}_2$.

2.10 Example

SLIDE 12

- Is $S = \{\boldsymbol{x} \in \mathcal{Z}^3 \mid \boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}\}$ is nonempty

$$\boldsymbol{A} = \begin{bmatrix} 3 & 6 & 1 \\ 4 & 5 & 5 \end{bmatrix} \text{ and } \boldsymbol{b} = \begin{bmatrix} 3 \\ 2 \end{bmatrix}.$$

- Integer normal form: $[\boldsymbol{B}, \boldsymbol{0}] = \boldsymbol{A}\boldsymbol{U}$, with

$$[\boldsymbol{B}, \boldsymbol{0}] = \begin{bmatrix} 1 & 0 & 0 \\ 5 & 1 & 0 \end{bmatrix} \text{ and } \boldsymbol{U} = \begin{bmatrix} 0 & 9 & -25 \\ 0 & -4 & 11 \\ 1 & -3 & 9 \end{bmatrix}.$$

  Note that $\det(\boldsymbol{U}) = -1$. Since $\boldsymbol{B}^{-1}\boldsymbol{b} = (3, -13)' \in \mathcal{Z}^2$, $S \neq \emptyset$.
- All integer solutions of S are given by

$$\boldsymbol{x} = \begin{bmatrix} 0 & 9 \\ 0 & -4 \\ 1 & -3 \end{bmatrix} \begin{bmatrix} 3 \\ -13 \end{bmatrix} + \begin{bmatrix} -25 \\ 11 \\ 9 \end{bmatrix} z = \begin{bmatrix} -117 & - & 25z \\ 52 & + & 11z \\ 42 & + & 9z \end{bmatrix}, \quad z \in \mathcal{Z}.$$

2.11 Integral Farkas lemma

SLIDE 13

Let $\boldsymbol{A} \in \mathcal{Z}^{m \times n}$, $\boldsymbol{b} \in \mathcal{Z}^m$ and $S = \{\boldsymbol{x} \in \mathcal{Z}^n \mid \boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}\}$.

- The set $S = \emptyset$ if and only if there exists a $\boldsymbol{y} \in \mathcal{Q}^m$, such that $\boldsymbol{y}'\boldsymbol{A} \in \mathcal{Z}^m$ and $\boldsymbol{y}'\boldsymbol{b} \notin \mathcal{Z}$.
- The set $S = \emptyset$ if and only if there exists a $\boldsymbol{y} \in \mathcal{Q}^m$, such that $\boldsymbol{y} \geq \boldsymbol{0}$, $\boldsymbol{y}'\boldsymbol{A} \in \mathcal{Z}^m$ and $\boldsymbol{y}'\boldsymbol{b} \notin \mathcal{Z}$.

2.12 Proof

SLIDE 14

- Assume that $S \neq \emptyset$. If there exists $\boldsymbol{y} \in \mathcal{Q}^m$, such that $\boldsymbol{y}'\boldsymbol{A} \in \mathcal{Z}^m$ and $\boldsymbol{y}'\boldsymbol{b} \notin \mathcal{Z}$, then $\boldsymbol{y}'\boldsymbol{A}\boldsymbol{x} = \boldsymbol{y}'\boldsymbol{b}$ with $\boldsymbol{y}'\boldsymbol{A}\boldsymbol{x} \in \mathcal{Z}$ and $\boldsymbol{y}'\boldsymbol{b} \notin \mathcal{Z}$.
- Conversely, if $S = \emptyset$, then by previous theorem, $\boldsymbol{u} = \boldsymbol{B}^{-1}\boldsymbol{b} \notin \mathcal{Z}^m$, that is there exists an i such that $u_i \notin \mathcal{Z}$. Taking $\boldsymbol{y}$ to be the ith row of $\boldsymbol{B}^{-1}$ proves the theorem.

2.13 Reformulations

SLIDE 15

- max $\boldsymbol{c}'\boldsymbol{x},\ \boldsymbol{x} \in S = \{\boldsymbol{x} \in \mathcal{Z}_+^n \mid \boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}\}$.
- $[\boldsymbol{B}, \boldsymbol{0}] = \boldsymbol{A}\boldsymbol{U}$. There exists $\boldsymbol{x}^0 \in \mathcal{Z}^n$: $\boldsymbol{A}\boldsymbol{x}^0 = \boldsymbol{b}$ iff $\boldsymbol{B}^{-1}\boldsymbol{b} \notin \mathcal{Z}^m$.
- $$\boldsymbol{x} \in S \iff \boldsymbol{x} = \boldsymbol{x}^0 + \boldsymbol{y} :\ \boldsymbol{A}\boldsymbol{y} = \boldsymbol{0},\ -\boldsymbol{x}^0 \le \boldsymbol{y}.$$

  Let
  $$\mathcal{L} = \{\boldsymbol{y} \in \mathcal{Z}^n \mid \boldsymbol{A}\boldsymbol{y} = \boldsymbol{0}\}.$$
  Let $\boldsymbol{U}_2$ be a basis of $\mathcal{L}$, i.e.,
  $$\mathcal{L} = \{\boldsymbol{y} \in \mathcal{Z}^n \mid \boldsymbol{y} = \boldsymbol{U}_2\boldsymbol{z},\ \boldsymbol{z} \in \mathcal{Z}^{n-m}\}.$$
- $$\begin{array}{rl} \max & \boldsymbol{c}'\boldsymbol{U}_2\boldsymbol{z} \\ \text{s.t} & \boldsymbol{U}_2\boldsymbol{z} \ge -\boldsymbol{x}^0 \\ & \boldsymbol{z} \in \mathcal{Z}^{n-m}. \end{array}$$
- Different bases give rise to alternative reformulations
  $$\begin{array}{rl} \max & \boldsymbol{c}'\overline{\boldsymbol{B}}\boldsymbol{z} \\ \text{s.t.} & \overline{\boldsymbol{B}}\boldsymbol{z} \ge -\boldsymbol{x}^0 \\ & \boldsymbol{z} \in \mathcal{Z}^{n-m}. \end{array}$$