15.083J/6.859J Integer Optimization

Lecture 3: Methods to enhance formulations

1 Outline

SLIDE 1

- Polyhedral review
- Methods to generate valid inequalities
- Methods to generate facet defining inequalities

2 Polyhedral review

2.1 Dimension of polyhedra

SLIDE 2

- Definition: The vectors $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^k \in \Re^n$ are **affinely independent** if the unique solution of the linear system

$$\sum_{i=1}^{k} a_i \boldsymbol{x}^i = \boldsymbol{0}, \qquad \sum_{i=1}^{k} a_i = 0,$$

  is $a_i = 0$ for all $i = 1, \ldots, k$.

- Proposition: The vectors $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^k \in \Re^n$ are affinely independent if and only if the vectors $\boldsymbol{x}^2 - \boldsymbol{x}^1, \ldots, \boldsymbol{x}^k - \boldsymbol{x}^1$ are linearly independent.

SLIDE 3

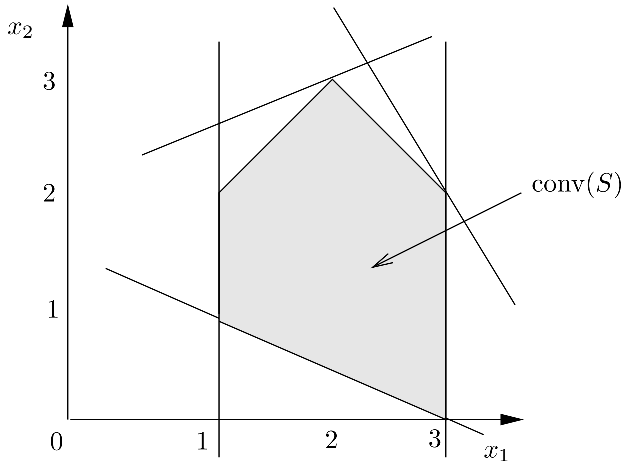
- Definition: Let $P = \{\boldsymbol{x} \in \Re^n \mid \boldsymbol{A}\boldsymbol{x} \geq \boldsymbol{b}\}$. Then, the polyhedron P has **dimension** k, denoted $\dim(P) = k$, if the maximum number of affinely independent points in P is $k+1$.
- $P = \{(x_1, x_2) \mid x_1 - x_2 = 0,\ 0 \leq x_1 \leq 1,\ 0 \leq x_2 \leq 1\}$, $\dim(P) =?$

2.2 Valid Inequalities

2.2.1 Definitions

SLIDE 4

- $\boldsymbol{a}'\boldsymbol{x} \geq b$ is called a **valid inequality** for a set P if it is satisfied by all points in P.
- Let $\boldsymbol{f}'\boldsymbol{x} \geq g$ be a valid inequality for a polyhedron P, and let $F = \{x \in P \mid \boldsymbol{f}'\boldsymbol{x} = g\}$. Then, F is called a **face** of P and we say that $\boldsymbol{f}'\boldsymbol{x} \geq g$ **represents** F. A face is called **proper** if $F \neq \emptyset, P$.
- A face F of P represented by the inequality $\boldsymbol{f}'\boldsymbol{x} \geq g$, is called a **facet** of P if $\dim(F) = \dim(P) - 1$. We say that the inequality $\boldsymbol{f}'\boldsymbol{x} \geq g$ is **facet defining**.



2.2.2 Theorem

SLIDE 5

- For each facet F of P, at least one of the inequalities representing F is necessary in any description of P.
- Every inequality representing a face of P of dimension less than $\dim(P)-1$ is not necessary in the description of P, and can be dropped.

2.2.3 Example

SLIDE 6

- $S = \{(x_1, x_2) \in \mathcal{Z}^2 \mid x_1 \leq 3, x_1 \geq 1, -x_1+2x_2 \leq 4, 2x_1+x_2 \leq 8, x_1+2x_2 \geq 3\}$.
- Facets for $\text{conv}(S)$: $x_1 \leq 3$, $x_1 \geq 1$, $x_1 + 2x_2 \geq 3$, $x_1 + x_2 \leq 5$, $-x_1 + x_2 \leq -1$.
- Faces of dimension one: $-x_1 + 2x_2 \leq 4$, and $2x_1 + x_2 \leq 8$.

3 Methods to generate valid inequalities

3.1 Rounding

SLIDE 7

- Choose $\boldsymbol{u} = (u_1, \dots, u_m)' \geq \boldsymbol{0}$; Multiply ith constraint with u_i and sum:

$$\sum_{j=1}^{n} (\boldsymbol{u}'\boldsymbol{A}_j)x_j \leq \boldsymbol{u}'\boldsymbol{b}.$$

- Since $\lfloor \boldsymbol{u}'\boldsymbol{A}_j \rfloor \leq \boldsymbol{u}'\boldsymbol{A}_j$ and $x_j \geq 0$:

$$\sum_{j=1}^{n} \left(\lfloor \boldsymbol{u}'\boldsymbol{A}_j \rfloor\right)x_j \leq \boldsymbol{u}'\boldsymbol{b}.$$

- As $\boldsymbol{x} \in \mathcal{Z}_+^n$: $\sum_{j=1}^{n} \left(\lfloor \boldsymbol{u}'\boldsymbol{A}_j \rfloor\right)x_j \leq \lfloor \boldsymbol{u}'\boldsymbol{b} \rfloor$.

3.1.1 Matching

SLIDE 8

- $S = \left\{ \boldsymbol{x} \in \{0,1\}^{|E|} \;\middle|\; \sum_{e \in \delta(\{i\})} x_e \leq 1,\ i \in V \right\}$.
- $U \subset V$, $|U| = 2k+1$. For each $i \in U$, multiply $\sum_{e \in \delta(\{i\})} x_e \leq 1$ by 1/2, and add:

$$\sum_{e \in E(U)} x_e + \frac{1}{2} \sum_{e \in \delta(U)} x_e \leq \frac{1}{2}|U|.$$

- Since $x_e \geq 0$, $\sum_{e \in E(U)} x_e \leq \frac{1}{2}|U|$.
- Round to ($|U|$ is odd)

$$\sum_{e \in E(U)} x_e \leq \left\lfloor \frac{1}{2}|U| \right\rfloor = \frac{|U|-1}{2},$$

3.2 Superadditivity

3.2.1 Definition

SLIDE 9

A function $F : D \subset \Re^n \mapsto \Re$ is **superadditive** if for $\boldsymbol{a}_1, \boldsymbol{a}_2 \in D$,: $\boldsymbol{a}_1 + \boldsymbol{a}_2 \in D$:

$$F(\boldsymbol{a}_1) + F(\boldsymbol{a}_2) \leq F(\boldsymbol{a}_1 + \boldsymbol{a}_2),$$

It is **nondecreasing** if

$$F(\boldsymbol{a}_1) \leq F(\boldsymbol{a}_2),\ \text{if } \boldsymbol{a}_1 \leq \boldsymbol{a}_2 \text{ for all } \boldsymbol{a}_1, \boldsymbol{a}_2 \in D.$$

3.2.2 Theorem

SLIDE 10

If $F : \Re^m \mapsto \Re$ is superadditive and nondecreasing with $F(\mathbf{0}) = 0$, $\sum_{j=1}^n F(\boldsymbol{A}_j) x_j \leq F(\boldsymbol{b})$ is valid for the set $S = \left\{ \boldsymbol{x} \in \mathcal{Z}_+^n \;\middle|\; \boldsymbol{A}\boldsymbol{x} \leq \boldsymbol{b} \right\}$.

3.2.3 Proof

SLIDE 11

By induction on x_j, we show: $F(\boldsymbol{A}_j)x_j \leq F(\boldsymbol{A}_j x_j)$. For $x_j = 0$ it is clearly true. Assuming it is true for $x_j = k-1$, then

$$\begin{aligned} F(\boldsymbol{A}_j)k &= F(\boldsymbol{A}_j) + F(\boldsymbol{A}_j)(k-1) \\ &\leq F(\boldsymbol{A}_j) + F(\boldsymbol{A}_j(k-1)) \\ &\leq F(\boldsymbol{A}_j + \boldsymbol{A}_j(k-1)), \end{aligned}$$

by superadditivity, and the induction is complete. SLIDE 12

Therefore,

$$\sum_{j=1}^n F(\boldsymbol{A}_j) x_j \leq \sum_{j=1}^n F(\boldsymbol{A}_j x_j).$$

By superadditivity,

$$\sum_{j=1}^{n} F(\boldsymbol{A}_j x_j) \leq F\left(\sum_{j=1}^{n} \boldsymbol{A}_j x_j\right) = F(\boldsymbol{A}\boldsymbol{x}).$$

Since $\boldsymbol{A}\boldsymbol{x} \leq \boldsymbol{b}$ and F is nondecreasing

$$F(\boldsymbol{A}\boldsymbol{x}) \leq F(\boldsymbol{b}).$$

3.3 Modular arithmetic

SLIDE 13

$$S = \left\{\boldsymbol{x} \in \mathcal{Z}_+^n \;\middle|\; \sum_{j=1}^{n} a_j x_j = a_0\right\},$$

$d \in \mathcal{Z}_+$. We write $a_j = b_j + u_j d$, where b_j $(0 \leq b_j < d,\ b_j \in \mathcal{Z}_+)$. Then,

$$\sum_{j=1}^{n} b_j x_j = b_0 + rd, \text{ for some integer } r.$$

Since $\sum_{j=1}^{n} b_j x_j \geq 0$ and $b_0 < d$, we obtain $r \geq 0$. Then, $\sum_{j=1}^{n} b_j x_j \geq b_0$ is valid for S.

3.3.1 Examples

SLIDE 14

- $S = \{\boldsymbol{x} \in \mathcal{Z}_+^4 \mid 27x_1 + 17x_2 - 64x_3 + x_4 = 203\}$. For $d = 13$, inequality $x_1 + 4x_2 + x_3 + x_4 \geq 8$ is valid for S.
- For $d = 1$, and a_j are not integers. In this case, since $\boldsymbol{x} \geq \boldsymbol{0}$, we obtain $\sum_{j=1}^{n} \lfloor a_j \rfloor x_j \leq a_0$. Since $\boldsymbol{x} \in \mathcal{Z}$, $\sum_{j=1}^{n} \lfloor a_j \rfloor x_j \leq \lfloor a_0 \rfloor$, and thus the following inequality is valid for S

$$\sum_{j=1}^{n} (a_j - \lfloor a_j \rfloor) x_j \geq a_0 - \lfloor a_0 \rfloor.$$

3.4 Disjunctions

3.4.1 Proposition

SLIDE 15

If the inequality $\sum_{j=1}^{n} a_j x_j \leq b$ is valid for $S_1 \subset \Re_+^n$, and the inequality $\sum_{j=1}^{n} c_j x_j \leq d$ is valid for $S_2 \subset \Re_+^n$, then the inequality

$$\sum_{j=1}^{n} \min(a_j, c_j) x_j \leq \max(b, d)$$

is valid for $S_1 \cup S_2$.

3.4.2 Theorem

SLIDE 16

If the inequality $\sum_{j=1}^n a_j x_j - d(x_k - \alpha) \le b$ is valid for S for some $d \ge 0$, and the inequality $\sum_{j=1}^n a_j x_j + c(x_k - \alpha - 1) \le b$ is valid for S for some $c \ge 0$, then the inequality $\sum_{j=1}^n a_j x_j \le b$ is valid for S.
Example: In previous example, we write $-x_1 + 2x_2 \le 4$ and $-x_1 \le -1$ as follows:

$$(-x_1 + x_2) + (x_2 - 3) \le 1, \quad (-x_1 + x_2) - (x_2 - 2) \le 1.$$

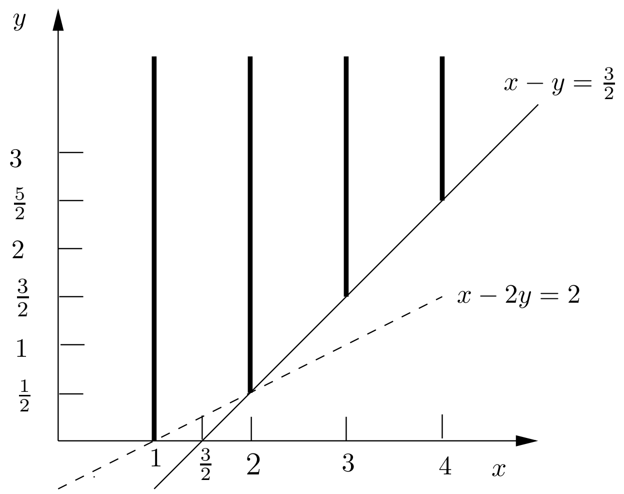
$\alpha = 2$, $-x_1 + x_2 \le 1$ is valid.

3.5 Mixed integer rounding

3.5.1 Proposition

SLIDE 17

- For $v \in \Re$, $f(v) = v - \lfloor v \rfloor$, $v^+ = \max\{0, v\}$.
- $X = \{(x, y) \in \mathcal{Z} \times \Re_+ \mid x - y \le b\}$



- The inequality $x - \frac{1}{1-f(b)}\, y \le \lfloor b \rfloor$ is valid for $\mathrm{conv}(X)$.

3.5.2 Proof

SLIDE 18

- $P^1 = X \cap \{(x, y) \mid \boldsymbol{x} \le \lfloor b \rfloor\}$,
- $P^2 = X \cap \{(x, y) \mid \boldsymbol{x} \ge \lfloor b \rfloor + 1\}$.
- Add $1 - f(b)$ times the inequality $x - \lfloor b \rfloor \le 0$ and $0 \le y$: $(x - \lfloor b \rfloor)\,(1 - f(b)) \le y$ is valid for P^1.
- For P^2 we combine $-(x - \lfloor b \rfloor) \le -1$ and $x - y \le b$ with multipliers $f(b)$ and 1: $(x - \lfloor b \rfloor)(1 - f(b)) \le y$. By disjunction, $(x - \lfloor b \rfloor)(1 - f(b)) \le y$ is valid for $\mathrm{conv}(P^1 \cup P^2) = \mathrm{conv}(X)$.

3.5.3 Theorem

SLIDE 19

$S = \left\{ \boldsymbol{x} \in \mathcal{Z}_+^n \;\middle|\; \sum_{j=1}^n \boldsymbol{A}_j x_j \leq \boldsymbol{b}, \quad j = 1, \ldots, n \right\}$. For every $\boldsymbol{u} \in \mathcal{Q}_+^m$ the inequality $\sum_{j=1}^n \left(\lfloor \boldsymbol{u}'\boldsymbol{A}_j \rfloor + \frac{[f(\boldsymbol{u}'\boldsymbol{A}_j) - f(\boldsymbol{u}'\boldsymbol{b})]^+}{1 - f(\boldsymbol{u}'\boldsymbol{b})} \right) x_j \leq \lfloor \boldsymbol{u}'\boldsymbol{b} \rfloor$ is valid for conv(S).

4 Facets

4.1 By the definition

4.1.1 Stable set

SLIDE 20

$$\begin{aligned} \max \quad & \sum_{i \in V} w_i x_i \\ \text{s. t.} \quad & x_i + x_j \leq 1, && \forall \{i, j\} \in E, \\ & x_i \in \{0, 1\}, && i \in V. \end{aligned}$$

A collection of nodes U, such that for all $i, j \in U$, $\{i, j\} \in E$ is called a **clique**.

$$\sum_{i \in U} x_i \leq 1, \qquad \text{for any clique } U \ (*)$$

is valid.

SLIDE 21

- A clique U is maximal if for all $i \in V \setminus U$, $U \cup \{i\}$ is not a clique.
- (*) is facet defining if and only if U is a maximal clique.
- $U = \{1, \ldots, k\}$. Then, $\boldsymbol{e}_i$, $i = 1, \ldots, k$ satisfy (*) with equality.
- For each $i \notin U$, there is a node $j = r(i) \in U$, such that $(i, r(i)) \notin E$. $\boldsymbol{x}^i$ with $x_i^i = 1$, $x_{r(i)}^i = 1$, and zero elsewhere is in S, and satisfies inequality (*) with equality.
- $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k, \boldsymbol{x}^{k+1}, \ldots, \boldsymbol{x}^n$ are linearly independent; hence, affinely independent.

SLIDE 22

Conversely, since U is not maximal, there is a node $i \notin U$ such that $U \cup \{i\}$ is a clique, and thus $\sum_{j \in U \cup \{i\}} x_j \leq 1$ $(**)$ is valid for conv(S). Since inequality (*) is the sum of $-x_i \leq 0$ and inequality (**), then (*) is not facet defining.

4.2 Lifting

SLIDE 23

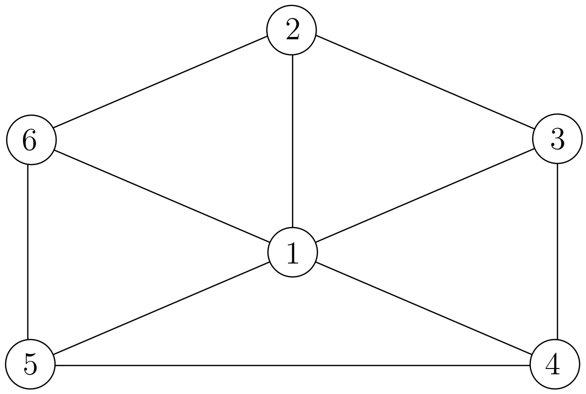
SLIDE 24

$$\max \sum_{i=1}^{6} x_i$$

$$\begin{array}{lllllllll} x_1 & + & x_2 & + & x_3 & & & & \leq 1 \\ x_1 & & & + & x_3 & + & x_4 & & \leq 1 \\ x_1 & + & & & & & x_4 & + x_5 & \leq 1 \\ x_1 & + & & & & & & x_5 + x_6 & \leq 1 \\ x_1 & + & x_2 & & & & & + x_6 & \leq 1. \end{array}$$

unique optimal solution $\boldsymbol{x}^0 = (1/2)(0, 1, 1, 1, 1, 1)'$. Do maximal clique inequalities describe convex hull?

SLIDE 25



- $\boldsymbol{x}^0$ does not satisfy
$$x_2 + x_3 + x_4 + x_5 + x_6 \leq 2. \ (1)$$
- Stable sets $\{2,4\}$, $\{2,5\}$, $\{3,5\}$, $\{3,6\}$, $\{4,6\}$ satisfy it with equality. Not facet, since there are no other stable sets that satisfy (1) with equality.
- (1) is facet defining for $S \cap \{\boldsymbol{x} \in \{0,1\}^6 \mid x_1 = 0\}$.
- Consider $ax_1 + x_2 + x_3 + x_4 + x_5 + x_6 \leq 2$, $a > 0$.
- Select a in order for (1) to be still valid, and to define a facet for S.

Slide 26

- For $x_1 = 0$, (1) is valid for all a.
- If $x_1 = 1$, $a \leq 2 - x_2 - x_3 - x_4 - x_5 - x_6$. Since $x_1 = 1$ implies $x_2 = \cdots = x_6 = 0$, then $a \leq 2$. Therefore, if $0 \leq a \leq 2$, (1) is valid.
- For $a = 2$, $\{2,4\}$, $\{2,5\}$, $\{3,5\}$, $\{3,6\}$, $\{4,6\}$, and $\{1\}$ satisfy it with equality.
- $2x_1 + x_2 + x_3 + x_4 + x_5 + x_6 \leq 2$, is valid and defines a facet conv(S).

4.2.1 General principle

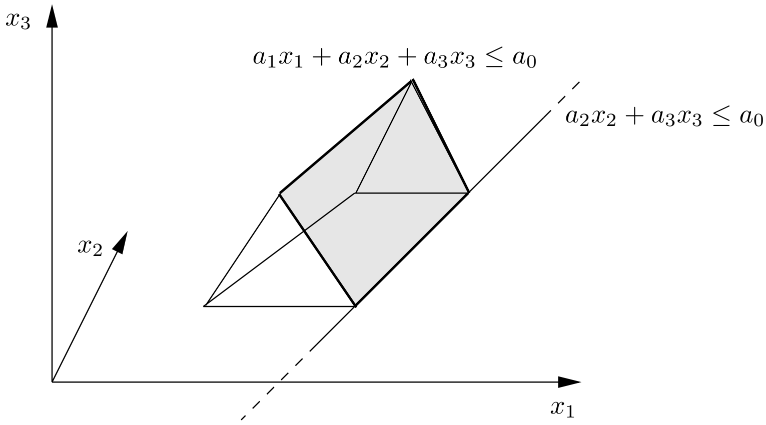
Slide 27

Suppose $S \subset \{0,1\}^n$, $S^i = S \cap \{\boldsymbol{x} \in \{0,1\}^n \mid x_1 = i\}$, $i = 0, 1$, and $\sum_{j=2}^n a_j x_j \leq a_0$ (2) is valid for S^0.

- If $S^1 = \emptyset$, then $x_1 \leq 0$ is valid for S.
- If $S^1 \neq \emptyset$, then $a_1 x_1 + \sum_{j=2}^n a_j x_j \leq a_0$ (3) is valid for S for any $a_1 \leq a_0 - Z$, $Z = \sum_{j=2}^n a_j x_j$ s.t. $\boldsymbol{x} \in S^1$.
- If $a_1 = a_0 - Z$ and (2) defines a face of dimension k of conv(S^0), then (3) gives a face of dimension $k+1$ of conv(S).

4.2.2 Geometry

Slide 28



4.2.3 Order of lifting

SLIDE 29

- $P = \text{conv}\,\{\boldsymbol{x} \in \{0,1\}^6 \mid 5x_1 + 5x_2 + 5x_3 + 5x_4 + 3x_5 + 8x_6 \le 17\}$.
- $x_1 + x_2 + x_3 + x_4 \le 3$ is valid for $P \cap \{x_5 = x_6 = 0\}$.
- Lifting on x_5 and then on x_6, yields $x_1 + x_2 + x_3 + x_4 + x_5 + x_6 \le 3$.
- Lifting on x_6 and then on x_5, yields $x_1 + x_2 + x_3 + x_4 + 2x_6 \le 3$.

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.

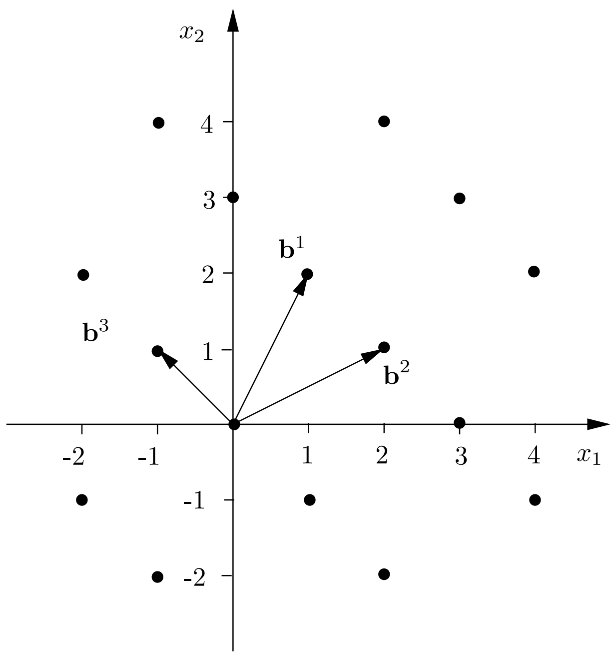
$$\mathcal{L} = \mathcal{L}(\boldsymbol{B}) = \{\boldsymbol{y} \in \mathcal{R}^n \mid \boldsymbol{y} = \boldsymbol{B}\boldsymbol{v}, \quad \boldsymbol{v} \in \mathcal{Z}^d\}$$

  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 $\overline{\boldsymbol{B}} = \boldsymbol{B}\boldsymbol{U}$ 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 $\overline{\boldsymbol{B}} = \boldsymbol{B}\boldsymbol{U}$.
- 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 $\boldsymbol{x} \in \mathcal{L}$: $\boldsymbol{x} = \boldsymbol{B}\boldsymbol{v}$ with $\boldsymbol{v} \in \mathcal{Z}^d$.
- $\det(\boldsymbol{U}) = \pm 1$, and $\det(\boldsymbol{U}^{-1}) = 1/\det(\boldsymbol{U}) = \pm 1$.
- $\boldsymbol{x} = \boldsymbol{B}\boldsymbol{U}\boldsymbol{U}^{-1}\boldsymbol{v}$.
- From Cramer's rule, $\boldsymbol{U}^{-1}$ has integral coordinates, and thus $\boldsymbol{w} = \boldsymbol{U}^{-1}\boldsymbol{v}$ is integral.
- $\overline{\boldsymbol{B}} = \boldsymbol{B}\boldsymbol{U}$. 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.
- $V = \{\boldsymbol{B}\boldsymbol{y} \mid \boldsymbol{y} \in \mathcal{R}^n\} = \{\overline{\boldsymbol{B}}\boldsymbol{y} \mid \boldsymbol{y} \in \mathcal{R}^n\}$.
- There exists an invertible $d \times d$ matrix $\boldsymbol{U}$ such that
$$\boldsymbol{B} = \overline{\boldsymbol{B}}\boldsymbol{U} \text{ and } \overline{\boldsymbol{B}} = \boldsymbol{B}\boldsymbol{U}^{-1}.$$
- $\boldsymbol{b}^i = \overline{\boldsymbol{B}}\boldsymbol{U}_i$, $\boldsymbol{U}_i \in \mathcal{Z}^d$ and $\overline{\boldsymbol{b}}^i = \boldsymbol{B}\boldsymbol{U}_i^{-1}$, $\boldsymbol{U}_i^{-1} \in \mathcal{Z}^d$.
- $\boldsymbol{U}$ 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 $\mathrm{vol}(A) > 2^n \det(\mathcal{L})$ 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 $[\boldsymbol{B}, \boldsymbol{0}] = \boldsymbol{A}\boldsymbol{U}$.

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:

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

  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 $\mathcal{L} = \{\boldsymbol{x} \in \mathcal{Z}^n \mid \boldsymbol{Ax} = \boldsymbol{0}\}$. 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 $S = \{\boldsymbol{x} \in \mathcal{Z}^3 \mid \boldsymbol{Ax} = \boldsymbol{b}\}$ 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: $[\boldsymbol{B}, \boldsymbol{0}] = \boldsymbol{AU}$, 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 $S = \{\boldsymbol{x} \in \mathcal{Z}^n \mid \boldsymbol{Ax} = \boldsymbol{b}\}$.

- 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 $\boldsymbol{y}'\boldsymbol{Ax} = \boldsymbol{y}'\boldsymbol{b}$ with $\boldsymbol{y}'\boldsymbol{Ax} \in \mathcal{Z}$ 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

- 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 $\boldsymbol{B}^{-1}\boldsymbol{b} \notin \mathcal{Z}^m$.
- $$\boldsymbol{x} \in S \iff \boldsymbol{x} = \boldsymbol{x}^0 + \boldsymbol{y} : \ \boldsymbol{A}\boldsymbol{y} = \boldsymbol{0}, \ -\boldsymbol{x}^0 \leq \boldsymbol{y}.$$

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