7 Integer programming in fixed dimension

The exposition of this chapter follows Bertsimas and Weismantel's book [3, §§6.5–6].

7.1 Maximum volume inscribed ellipsoid

In this chapter, we describe Lenstra's (1983) algorithm for integer programming, which runs in polynomial time if the dimension (the number of variables) is fixed. Besides basis reduction and other lattice techniques we learned in the previous chapter, an important piece of the algorithm is to be able to squeeze a polytope between two ellipsoids whose sizes do not differ too much (to **approximate** the polytope by an ellipsoid). The existence of such ellipsoids goes back to John (1948).

An **ellipsoid** $E(d, D)$ is the set $\{x \in \mathbb{R}^n : (x-d)^T D^{-2}(x-d) \le 1\}$, where $D \in \mathbb{R}^{n\times n}$ is a symmetric positive definite matrix and D^{-2} is the inverse of $D^2 = DD$. The ellipsoid $E(d, D)$ is the image of the **unit ball** $B(\mathbf{0}, 1) = \{x \in \mathbb{R}^n : \|x\| \le 1\}$ under the affine transformation $x \mapsto Dx + d$.

Definition 7.1 The **maximum volume inscribed ellipsoid problem** is for an input matrix $A \in \mathbb{Z}^{m\times n}$ and a vector $b \in \mathbb{Z}^m$ such that $P = \{x \in \mathbb{R}^n : Ax \le b\}$ is full-dimensional and bounded, to find a matrix D and a vector d such that the ellipsoid $E(d, D)$ is contained in P and has maximum volume among all ellipsoids contained in P.

Theorem 7.2 *There is a polynomial-time algorithm for the maximum volume inscribed ellipsoid problem.*

Proof. The volume of $E(d, D)$ is proportional to $\det D$. Hence maximizing the volume of an inscribed ellipsoid is equivalent to computing

$$\begin{aligned} M &:= \max\{\log\det D : E(d,D) \subseteq P\} \\ &= \max\Big\{\log\det D : \max\left\{a_i^T x : (x-d)^T D^{-2}(x-d) \le 1\right\} \le b_i \text{ for } i = 1,\dots,m\Big\}, \end{aligned} \tag{7.1}$$

where a_i is the transpose of the ith row of A.

Exercise 7.1 Show that $\max\{a_i^T x : (x-d)^T D^{-2}(x-d) \le 1\}$ is attained by

$$x^* = d + \frac{D^2 a_i}{\sqrt{a_i^T D^2 a_i}}.$$

Therefore

$$\begin{aligned} M &= \max\left\{\log\det D : a_i^T d + \sqrt{a_i^T D^2 a_i} \le b_i,\ i = 1,\dots,m\right\} \\ &= \max\left\{\log\det D : a_i^T D^2 a_i - b_i^2 + 2b_i(a_i^T d) - (a_i^T d)^2 \le 0,\ i = 1,\dots,m\right\}. \end{aligned} \tag{7.2}$$

Problem (7.2) can be solved in polynomial time by interior-point methods. For details see, for instance, [5, §8.4]. ∎

Proposition 7.3 *If* $E = \{x : (x-d)^T D^{-2}(x-d) \le 1\}$ *is the maximum volume inscribed ellipsoid in* $P = \{x : Ax \le b\}$*, found by the above algorithm, then*

$$P \subseteq E' = \{x : (x-d)^T D^{-2}(x-d) \le n^2\}.$$

Proof. Let a_i be the transpose of the ith row of A ($i = 1, \dots, m$). The Karush-Kuhn-Tucker (KKT) conditions for (7.2) are:

$$D^{-1} = \sum_{i=1}^{m} \lambda_i (D a_i a_i^T + a_i a_i^T D) \tag{7.3}$$

$$\sum_{i=1}^{m} \lambda_i (a_i b_i - a_i^T d a_i) = 0 \tag{7.4}$$

$$\|Da_i\| \le b_i - a_i^T d \quad \text{for } i = 1, \dots, m \tag{7.5}$$

$$\lambda_i \left(a_i^T D^2 a_i - b_i^2 + 2b_i(a_i^T d) - (a_i^T d)^2\right) = 0 \quad \text{for } i = 1, \dots, m \tag{7.6}$$

$$\lambda_i \ge 0 \quad \text{for } i = 1, \dots, m \tag{7.7}$$

First let us assume that the optimum is the unit ball $B(\mathbf{0}, 1)$, that is, that $D = I$ and $d = \mathbf{0}$. Then $b > \mathbf{0}$, so we may moreover assume that $b = \mathbf{1}$. The KKT conditions become:

$$I = \sum_{i=1}^{m} \lambda_i a_i a_i^T \tag{7.8}$$

$$\sum_{i=1}^{m} \lambda_i a_i = 0 \tag{7.9}$$

$$\lambda_i(\|a_i\| - 1) = 0 \quad \text{for } i = 1, \dots, m \tag{7.10}$$

$$\|a_i\| \le 1 \quad \text{for } i = 1, \dots, m \tag{7.11}$$

$$\lambda_i \ge 0 \quad \text{for } i = 1, \dots, m \tag{7.12}$$

Comparing the traces of both sides in (7.8), we get that

$$\sum_{i=1}^{m} \lambda_i = n.$$

Now let $x \in P$; we want to prove that $x \in B(\mathbf{0}, n)$, that is, $\|x\| \le n$. Let $\|x\| = r$. Then $-r \le a_i^T x \le 1$ for all i with $\lambda_i \ne 0$, and so

$$\begin{aligned} 0 &\le \sum_{i=1}^{m} \lambda_i (1 - a_i^T x)(r + a_i^T x) \\ &= r \cdot \sum_{i=1}^{m} \lambda_i + (1-r) \sum_{i=1}^{m} \lambda_i a_i^T x - \sum_{i=1}^{m} (a_i^T x)^2 \\ &= rn - r^2. \end{aligned}$$

Hence $\|x\| = r \le n$.

If the optimum ellipsoid is not the unit ball, consider the (invertible) affine transformation $\phi : x \mapsto D^{-1}x - d$ and let $P' = \phi[P]$. Then $B(\mathbf{0}, 1) \subseteq P' \subseteq B(\mathbf{0}, n)$ and therefore

$$E = \phi^{-1}[B(\mathbf{0}, 1)] \subseteq P = \phi^{-1}[P'] \subseteq E' = \phi^{-1}[B(\mathbf{0}, n)].$$

∎

7.2 Lenstra's algorithm

We want to solve the **feasibility problem** of integer programming, that is, given a rational polyhedron $P = \{x \in \mathbb{R}^n : Ax \le b\}$ to decide whether $P \cap \mathbb{Z}^n = \emptyset$.

Algorithm 7.1 (Reduction of dimension)

Input: $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$ such that $P = \{x \in \mathbb{R}^n : Ax \le b\}$ is full-dimensional and bounded.

Output: A feasible $y \in P \cap \mathbb{Z}^n$, or a series of feasibility problems given by polytopes $(P_k : k \in K)$ of dimension $n - 1$.

1. Apply the algorithm of Theorem 7.2 to find D, d such that

$$E = \{x : (x - d)^T D^{-2}(x - d) \le 1/n^2\} \subseteq P \subseteq E' = \{x : (x - d)^T D^{-2}(x - d) \le 1\}.$$

2. Set $P' := \{x \in \mathbb{R}^n : ADx \le b\}$; $p := D^{-1}d$.

3. Let $L := L(D^{-1})$ be the lattice generated by the columns of D^{-1}. Compute a reduced basis $B = \{b_1, \dots, b_n\}$ of L; rearrange so that $\|b_n\|$ is maximum.

4. Apply the Gram-Schmidt orthogonalization to B to get $B^* = \{b_1^*, \dots, b_n^*\}$.

5. Apply the approximate closest vector algorithm (Theorem 6.11) to get $y \in L$, the approximate closest vector to p.

6. If $y \in P'$, then $Dy \in P \cap \mathbb{Z}^n$; return Dy and stop.

   Otherwise set

$$c^* := \frac{b_n^*}{\|b_n^*\|^2}, \tag{7.13}$$

$$B := \begin{pmatrix} b_1 & b_2 & \dots & b_n \end{pmatrix}, \tag{7.14}$$

$$K := \left\{ \lfloor c^{*T}p - \|c^*\| \rfloor, \dots, \lceil c^{*T}p + \|c^*\| \rceil \right\}, \tag{7.15}$$

$$P_k := \left\{ z \in \mathbb{R}^{n-1} : ADB\left(\begin{smallmatrix} z \\ k \end{smallmatrix}\right) \le b \right\} \qquad \text{for } k \in K, \tag{7.16}$$

   and return the polytopes $(P_k : k \in K)$.

Lemma 7.4 *If $y \notin P'$ in Step 6., then*

$$\max\{c^{*T}x : x \in P' \cap L\} - \min\{c^{*T}x : x \in P' \cap L\} \le n^{3/2} \cdot 2^{n(n-1)/4}.$$

Proof. The algorithm of Theorem 6.11 finds a vector $y \in L$ such that

$$p - y = \sum_{i=1}^{n} \mu_i b_i^*$$

with each $|\mu_i| \le \frac{1}{2}$ (see (6.17)).

If $B(p, r) = \{x \in \mathbb{R}^n : \|x - p\| \le r\}$, then

$$B(p, 1/n) \subseteq P' \subseteq B(p, 1) \tag{7.17}$$

because $E \subseteq P \subseteq E'$. As $y \notin P'$, we have $\|y - p\| > 1/n$. Therefore

$$\begin{aligned} \frac{1}{n} < \|y - p\| &\le \sqrt{\frac{1}{4} \sum_{i=1}^{n} \|b_i^*\|^2} \\ &\le \frac{1}{2} \sqrt{\sum_{i=1}^{n} \|b_i\|^2} && \text{by Lemma 6.5(a)} \\ &\le \frac{1}{2} \sqrt{n}\, \|b_n\| && \text{by maximality of } \|b_n\|. \end{aligned} \tag{7.18}$$

By Theorem 6.8(d),

$$\begin{aligned} \alpha(B) = \|b_1\| \cdots \|b_n\| &\le 2^{n(n-1)/4} \det L \\ &= 2^{n(n-1)/4} \|b_1^*\| \cdots \|b_n^*\| \\ &\le 2^{n(n-1)/4} \|b_1\| \cdots \|b_{n-1}\| \, \|b_n^*\| . \end{aligned}$$

Hence

$$\frac{\|b_n\|}{2^{n(n-1)/4}} \le \|b_n^*\| \le \|b_n\| .$$

By definition $\|c^*\| = \frac{1}{\|b_n^*\|}$, and from (7.17) we obtain:

$$\begin{aligned} \max\{c^{*T}x : x \in P' \cap L\} &- \min\{c^{*T}x : x \in P' \cap L\} \\ &\le \max\{c^{*T}x : x \in B(p,1)\} - \min\{c^{*T}x : x \in B(p,1)\} \\ &\le c^{*T}\left(p + \frac{c^*}{\|c^*\|}\right) - c^{*T}\left(p - \frac{c^*}{\|c^*\|}\right) \\ &= 2\,\|c^*\| = \frac{2}{\|b_n^*\|} \le \frac{2 \cdot 2^{n(n-1)/4}}{\|b_n\|} \le n\sqrt{n}\, 2^{n(n-1)/4}; \end{aligned}$$

the last inequality follows from (7.18) and for finding the max and min we reuse Exercise 7.1. ∎

Lemma 7.5 *The polytopes P_k defined in* (7.16) *have the property that $P \cap \mathbb{Z}^n = \emptyset$ if and only if $P_k \cap \mathbb{Z}^{n-1} = \emptyset$ for all $k \in K$.*

Proof. Every $x^* \in P' \cap L$ can be written as

$$x^* = \sum_{i=1}^{n-1} z_i b_i + k b_n \quad \text{for some } z_i, k \in \mathbb{Z}.$$

That is, $x^* = B\binom{z}{k}$, where B has columns $b_1, \ldots, b_n$. Now $c^* = b_n^* / \|b_n^*\|^2$, hence c^* is orthogonal to all b_i for $1 \le i \le n-1$ and $c^{*T} b_n = 1$. Thus $c^{*T} x^* = k$ is integral.

Moreover,

$$c^{*T} x^* \in \big[\min\{c^{*T} x : x \in P' \cap L\}, \max\{c^{*T} x : x \in P' \cap L\}\big] \subseteq [c^{*T} p - \|c^*\|, c^{*T} p + \|c^*\|],$$

hence $c^{*T} x^* \in K$.

Therefore

$$\begin{aligned} \text{some } x \in P \cap \mathbb{Z} &\iff x^* = D^{-1} x \in P' \cap L \\ &\iff ADx^* \le b,\ x^* = B\tbinom{z}{k} \text{ for some } z \in \mathbb{Z}^{n-1},\ k \in K \\ &\iff ADB\tbinom{z}{k} \le b \\ &\iff z \in P_k \cap \mathbb{Z}^{n-1} \text{ for some } k \in K. \end{aligned}$$

So $P \cap \mathbb{Z} \ne \emptyset$ if and only if $P_k \cap \mathbb{Z}^{n-1} \ne \emptyset$ for some $k \in K$. ∎

Theorem 7.6 (Lenstra (1983)) *Let $n \in \mathbb{N}$ be fixed. Then there exists an algorithm that for given $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$, decides whether $\{x \in \mathbb{Z}^n : Ax \le b\} = \emptyset$ in time polynomial in the encoding size of A and b.*

Proof. Here we present a proof for the case when P is full-dimensional and bounded. If P is not full-dimensional, the ellipsoid method for LP can be used to reduce the dimension. If P is not bounded, one may consider the intersection of P with a suitable box whose size depends on the encoding size of the input (using ideas of Theorem 4.3).

Assuming that P is full-dimensional and bounded, we apply Algorithm 7.1. If $y \in P \cap \mathbb{Z}^n$ is found, then $P \cap \mathbb{Z}^n \ne \emptyset$. Otherwise we run Algorithm 7.1 on the $(n-1)$-dimensional problems $\{ADB\binom{z}{k} \le b\} \cap \mathbb{Z}^n$ for all $k \in K$.

All we need to check is that ADB is integral. Because $L(D^{-1}) = L(B)$, by Theorem 2.10 the matrices D^{-1} and B have the same Hermite normal form. So there exists a unimodular matrix $U \in \mathbb{Z}^{n \times n}$ such that $D^{-1} U = B$. Therefore $ADB = ADD^{-1} U = AU \in \mathbb{Z}^{m \times n}$ because A is integral.

By Lemma 7.4, the size of K is bounded by a constant (since n is fixed). The input for the $(n-1)$-dimensional subproblems is produced by a polynomial algorithm, hence of polynomial size with respect to the size of our input. Thus our algorithm consists in a constant number of applications of a polynomial algorithm, and therefore it is polynomial as well. ∎

Corollary 7.7 *Let $n \in \mathbb{N}$ be fixed. Then there exists a polynomial algorithm to solve the IP $\max\{c^T x : Ax \le b,\ x \in \mathbb{Z}^n\}$, where $A \in \mathbb{Z}^{m \times n}$.*

Proof. From Theorem 4.3 it follows that the size of the optimum is polynomially bounded in terms of the size of the input. Hence it can be found by binary search, using the feasibility algorithm. To work out the details is an exercise. ∎

Note. Careful examination of the algorithms reveals that they work in polynomial time also for rational input.