Hilbert Bases in Integer Programming

A subset $C \subseteq \mathbb{R}^n$ is called a *cone*, if for all $x \in C$ and all $\lambda \geq 0$ we have $\lambda x \in C$. A cone $C \subseteq \mathbb{R}^n$ is called *pointed* if there exists a vector $a \in \mathbb{R}^n$ such that $a^T x > 0$ for all $x \in C \setminus \{0\}$.

In this section we shall only consider convex cones[1]. We say that a set $H \subseteq C$ generates the convex cone C, and denote it by $C = cone(H)$, if C is the set of nonnegative linear combinations of the vectors of H, i.e., if

$$C \;=\; \left\{ \sum_{h \in H} \lambda_h h \;\middle|\; (\lambda_h \mid h \in H) \in \mathbb{R}_+^{|H|} \right\}. \tag{1}$$

Given a convex cone C, its *polar* C^* is defined as

$$C^* = \left\{ y \in \mathbb{R}^n \mid y^T x \geq 0,\ x \in C \right\}.$$

It is easy to see that $(C^*)^* = C$, and if $C^* = cone(H^*)$, then

$$C = \left\{ x \in \mathbb{R}^n \mid a^T x \geq 0,\ a \in H^* \right\}. \tag{2}$$

We say that a convex cone $C \subseteq \mathbb{R}^n$ is *rational*, if there exists a set $H \subseteq \mathbb{Q}^n$ such that $C = cone(H)$, and C is said to be *finitely generated* if $C = cone(H)$ for a finite set H. The elements $h \in H$ are called *generators* of $C = cone(H)$. We say that C is a *polyhedral cone*, if C^* is finitely generated, which can be seen equivalent with the fact that C itself is finitely generated (see e.g., Farkas (1898), Minkowski (1896), Weyl (1935)). Every finitely generated rational convex cone C has unique minimal sets $G, F^* \subseteq \mathbb{Q}^n$ such that $C = cone(G)$ and $C^* = cone(F^*)$. The vectors in G are called the *extremal directions* of C, while the inequalities $a^T x \geq 0$ for $a \in F^*$ are called the *facets* of C.[2]

A set $H \subseteq \mathbb{R}^n$ is called a *Hilbert basis* of the cone $C = cone(H)$ (see e.g., Giles and Pulleyblank, 1979), if all integral vectors in $cone(H)$ can be represented as a nonnegative integral combination of the vectors of H, i.e.,

$$cone(H) \cap \mathbb{Z}^n \;=\; \left\{ \sum_{h \in H} \lambda_h h \;\middle|\; (\lambda_h \mid h \in H) \in \mathbb{Z}_+^{|H|} \right\}.$$

[1] Aren't all cones convex? Can you show a cone which is not pointed?

[2] Can you find examples for finitely generated rational cones C which have exponentially more extremal directions than facets?

In this section we shall be interested in integral Hilbert bases, i.e., when $H \subseteq \mathbb{Z}^n$.

The first natural question to ask is about the existence of a finite Hilbert basis for every finitely generated rational cone. Essentially this was shown by Gordan (1873) (cf. Hilbert 1890). Moreover, if the cone is pointed then Corput (1937) showed that it has a unique minimal Hilbert basis.

Theorem 1 (Gordan 1873) *If C is a rational polyhedral cone, then $C = cone(H)$ for a finite Hilbert basis H.*

Proof. Let $G \subseteq \mathbb{Q}^n$ be the set of extremal directions of C (i.e., $C = cone(G)$). Since by multiplying the vectors in G by nonnegative integers does not change the fact that G generates C, we can assume that $G \subseteq \mathbb{Z}^n$. Let us then consider the set

$$H = \left\{ \sum_{g \in G} \lambda_g g \in \mathbb{Z}^n \;\middle|\; 0 \leq \lambda_g \leq 1,\ g \in G \right\}. \tag{3}$$

We claim that H is a finite[3] integral Hilbert basis of C. Clearly, $G \subseteq \mathbb{Z}^n$, and it is finite. It is also easy to see that $G \subseteq H$, since for all $g \in G$ we can represent g as in (3), by choosing $\lambda_g = 1$, and $\lambda_{g'} = 0$ for all $g \neq g' \in G$. Thus, $C = cone(H)$ follows. Let us now consider an arbitrary integer vector $b \in C \cap \mathbb{Z}^n$. Since $C = cone(G)$ we have nonnegative coefficients $\beta_g \geq 0$, $g \in G$ such that

$$b = \sum_{g \in G} \beta_g g,$$

which we can re-write as

$$b \;=\; \sum_{g \in G} \lfloor \beta_g \rfloor g \;+\; \sum_{g \in G} (\beta_g - \lfloor \beta_g \rfloor) g.$$

Here the for second summation we have $d = \sum_{g \in G} (\beta_g - \lfloor \beta_g \rfloor) g \in H$, i.e., d itself is an integer vector belonging to H, by (3), while the first summation is a nonnegative integral combination of the vectors of $G \subseteq H$. Thus, the above equality is a nonnegative integral combination of some vectors from H (namely, of $G \cup \{d\} \subseteq H$, proving that H is indeed a Hilbert basis of C. $\square$

[3] WHY?

Theorem 2 (Corput 1937) *If C is a pointed rational polyhedral cone, then $C = cone(H^*)$ for a unique minimal Hilbert basis H^*.*

Proof. Since C is pointed, we have $a^T x > 0$ for all $x \in C$ for some $a \in \mathbb{R}^n$. Let us introduce the notation $Z = (C \cap \mathbb{Z}^n) \setminus \{0\}$, and consider the set

$$H^* = \{u \in Z \mid \nexists v, w \in Z : u = v + w\}.$$

Note that we did not exclude $v = w$!

It is easy to see that $H^* \subseteq H$ for every Hilbert basis H of C. We can prove this by contradiction. Assume that there exists a Hilbert basis H of cone C such that $H^* \not\subseteq H$. Let us choose $u \in H^* \setminus H$. Since $u \in H^* \subseteq Z \subseteq C$ and H is a Hilbert basis of C, u can be represented as nonnegative integer combination of the vectors of H:

$$u \;=\; \sum_{h \in H} \lambda_h \cdot h,$$

where $\lambda_h \in \mathbb{Z}_+$ for all $h \in H$. Since $u \notin H$, we must have

$$\sum_{h \in H} \lambda_h \;\geq\; 2.$$

Choose $h^* \in H$ such that $\lambda_{h^*} > 0$, and define

$$v \;=\; \lambda_{h^*} \cdot h^* + \sum_{\substack{h \in H \\ h \neq h^*}} \lambda_h \cdot h \quad \text{and} \quad w = h^*.$$

Then we have $v, w \in Z$ and $u = v + w$, contradicting $u \in H^*$.

We claim next that H^* itself is a Hilbert basis, which then will complete the proof of the theorem. To see this claim, assume indirectly that H^* is not a Hilbert basis of C, i.e., that there are some vectors in Z which cannot be represented as a nonnegative integral combination of the vectors of H^*. Let us choose such a vector $u \in Z$ for which $a^T u$ is minimal[4] Since u is not generated by H^*, in particular $u \notin H^*$, and hence we have integral vectors $v, w \in Z$ such that $u = v + w$ by the definition of H^*. Since $v \neq 0$ and $w \neq 0$, we must have $a^T v > 0$ and $a^T w > 0$, and hence $\max\{a^T v, a^T w\} < a^T u$ is implied. Therefore, by the choice of u we must have both v and w generated

[4]Why is there a vector $u \in Z$, not generated by H^* for which $a^T u$ is minimal?

as nonnegative integral combinations of the vectors of H^*, but then so is $u = v + w$, a contradiction, proving the claim, and finishing our proof. □

Though the above prove that a Hilbert basis is always finite, it may be of very large cardinality. Try to construct two vectors $a, b \in \mathbb{Z}^2$, for which the unique minimal Hilbert basis of the generated cone $C = cone(\{a, b\})$ is exponentially large in the size of these two vectors.

Let us associate to a set of vectors $H = \{h_1, ..., h_m\} \subseteq \mathbb{R}^n$ a matrix $A_H \in \mathbb{R}^{n \times m}$, the columns of which are the vectors of H, in the listed order. Try to prove the following claim:

Lemma 1 *If $H \subseteq \mathbb{Z}^n$ contains a set of n linearly independent vectors, then it is a Hilbert basis if and only if A_H is a unimodular matrix.* □

Analogues of Carathéodory's theorem

Theorem 1 suggests that Hilbert bases play a similar role in integer programming as extremal directions of a cone (or vertices of a polytope) in linear programming. A powerful property behind the efficiency of linear programming is Carathéodory's theorem, claiming that every vector in a convex cone $C = Cone(G) \subseteq \mathbb{R}^n$ can be represented as a nonnegative linear combination of at most n vectors of G (no matter how large the set G is!).

Theorem 3 (Carathéodory 1911) *If $C = Cone(G) \subseteq \mathbb{R}^n$, and $x \in C$, then $x \in cone(I)$ for some linearly independent subset $I \subseteq G$.* □

It is just natural to ask, what is the integer analogue of this theorem. Let us denote by $c^I(H, x)$ the minimum number of nonzero coefficients in a nonnegative integral combination of the vectors of H representing $x \in Z = cone(H) \cap \mathbb{Z}^n$, and let $c^I(H) = \max_{x \in Z} c^I(H, x)$.

Theorem 4 (Cook, Fonlupt, and Schrijver 1986) *If $H \subseteq \mathbb{Z}^n$ is a Hilbert basis, then $c^I(H) \leq 2n - 1$.*

Proof. To prove the statement, it is enough to show that $c^I(H,x) \leq 2n-1$ for all $x \in Z = cone(H) \cap \mathbb{Z}^n$. For this let us fix a vector $x \in Z$, and let λ_h^*, $h \in H$ denote an optimal basic solution to the linear programming problem

$$\max \left\{ \sum_{h \in H} \lambda_h \;\middle|\; x = \sum_{h \in H} \lambda_h h,\ \lambda_h \geq 0 \text{ for all } h \in H \right\}.$$

Let us note that by the basic theorem of linear programming, at most n nonzeros are among the λ_h^*, $h \in H$ values. Let us denote by $B \subseteq H$ the set corresponding to the nonzeros, i.e., we have $\lambda_h^* = 0$ for $h \notin B$, and $|B| \leq n$. Let us next consider the vector $y = x - \sum_{h \in B} \lfloor \lambda_h^* \rfloor h$. Since we have $y = \sum_{h \in B} (\lambda_h^* - \lfloor \lambda_h^* \rfloor) h$ as a nonnegative linear combination of some vectors of H, we have $y \in cone(H)$. Furthermore, $y \in \mathbb{Z}^n$ by its definition, and hence we have $y \in Z$, implying that

$$y \;=\; \sum_{h \in H} \alpha_h h$$

for some nonnegative integers α_h, $h \in H$, because H is a Hilbert basis. Let $N = \{h \in H \mid \alpha_h \neq 0\}$. Then we have

$$x = \sum_{h \in B} \lfloor \lambda_h^* \rfloor h \;+\; \sum_{h \in N} \alpha_h h \tag{4}$$

as a nonnegative linear (and also integral) combination of some of the vectors of H. Then, by the optimal choice of λ_h^*, $h \in H$, we must have

$$\sum_{h \in B} \lfloor \lambda_h^* \rfloor \;+\; \sum_{h \in N} \alpha_h \;\leq\; \sum_{h \in H} \lambda_h^*$$

implying that $\sum_{h \in N} \alpha_h < n$, from which $|B \cup N| \leq 2n-1$ follows. This proves that (4) involves at most $2n-1$ of the vectors of H, i.e., that $c^I(H,x) \leq 2n-1$. □

The above bound on $c^I(H)$ has been slightly improved to $2n-2$, but the true value of this parameter is still open.

Analogues of Helly's theorem

Another powerful result behind the efficiency of linear programming is Helly's theorem, which provide us with a simple certificate, whenever a system of inequalities is inconsistent (regardless the size of the system). Helly (1912) is a statement about the nonemptyness of the intersection of convex sets. Here we recall it for the special case involving half spaces.

Theorem 5 (Helly 1912) *If the polyhedral set* $K = \{x \in \mathbb{R}^n \mid a_i^T x \leq b_i,\ i = 1, ..., m\}$ *is empty, then there exists a subset* $I \subseteq \{1, 2, ..., m\}$ *of the indices with* $|I| \leq n + 1$ *such that* $K_I = \{x \in \mathbb{R}^n \mid a_i^T x \leq b_i,\ i \in I\}$ *is also empty.* □

It is natural to ask that how many of the inequalities we need to prove that $K \cap \mathbb{Z}^n = \emptyset$? For a set of linear inequalities $\mathcal{A} = \{a_i^T x \leq b_i \mid i = 1, ..., m\}$ let us denote by $h(\mathcal{A})$ the minimum number of inequalities from $\mathcal{A}$ which do not have a feasible integral solution (if $\mathcal{A}$ has a feasible integral solution, let us define $h(\mathcal{A}) = +\infty$). Let us further define $h(n) = \max h(\mathcal{A})$, where the maximum is taken over all system of linear inequalities $\mathcal{A}$ involving n variables. Helly's theorem shows that if we disregard integrality in the above definitions, then $h(n) \leq n+1$, and actually equality here can be shown easily.

For the integral case, let us consider first an example. Let us introduce the notation $\bar{x} = 1 - x$ for a real $x \in \mathbb{R}$, let $\bar{x} = (\bar{x}_1, ..., \bar{x}_n)$ for a vector $x = (x_1, ..., x_n) \in \mathbb{R}^n$, and let $\mathbb{B}^n = \{0, 1\}^n$. Let us then consider the system of linear inequalities

$$\mathcal{A}_{\mathbb{B}^n} = \left\{ a^T x + \bar{a}^T \bar{x} \leq n - 1 \mid a \in \mathbb{B}^n \right\}.$$

Let us note that this system, consisting of 2^n inequalities in n variables, has no feasible integral solutions. To see this, let us consider an arbitrary integer vector $x \in \mathbb{Z}^n$, and denote by

$$P = \{j \mid x_j \geq 1\} \quad \text{and} \quad \bar{P} = \{j \mid x_j \leq 0\}.$$

Then we have $|P| + |\bar{P}| = n$ since x is integral. Note also that we have $\bar{x}_j \geq 1$ for all $j \in \bar{P}$. Let us then consdier the binary vector a defined by

$$a_j = \begin{cases} 1 & \text{if } j \in P, \\ 0 & \text{if } j \in \bar{P}. \end{cases}$$

Then we have

$$a^T x \geq |P| \quad \text{and} \quad \bar{a}^T \bar{x} \geq |\bar{P}|,$$

implying

$$a^T x + \bar{a}^T \bar{x} \ \geq \ n.$$

Let us also note that the above system has some non-integer feasible solutions. For instance $x = (\frac{1}{2}, ..., \frac{1}{2})$ is feasible whenever $n \geq 2$.

However, if we delete any of the inequalities, e.g., the inequality corresponding to vector $a \in \mathbb{B}^n$, then $x = a$ will be a feasible integer solution for $\mathcal{A}_{\mathbb{B}^n \setminus \{a\}}$[5]. This example shows that we have $h(n) \geq 2^n$, indicating clearly that proving inconsistency of systems of inequalities over integer variables can be substantially harder to verify than in the continuous case.

Doignon (1973) (cf. Bell (1977) and Scarf (1977)) showed that in fact we have the equality $h(n) = 2^n$.

Theorem 6 (Doignon 1973; Bell 1977; Scarf 1977) *If the system of linear inequalities $\mathcal{A} = \{a_i^T x \leq b_i \mid i = 1, ..., m\}$ has no feasible integral solution, then there exists a subset $I \subseteq \{1, ..., m\}$ of cardinality $|I| \leq 2^n$ for which the subsystem $\mathcal{A}_I = \{a_i^T x \leq b_i \mid i \in I\}$ has no integral feasible solution, either.*

This theorem implies that $h(n) \leq 2^n$, which together with the above example shows that $h(n) = 2^n$.

Proof. We can assume without any loss of generality that $\mathcal{A}$ is minimal with respect to infeasibility, i.e., that by deleting any of the inequalities from $\mathcal{A}$, the rest has an integral feasible solution. In which case the theorem is equivalent with showing that $m \leq 2^n$.

Introduce $I = \{1, 2, ..., m\}$, and for subsets $J \subseteq I$ let $\mathcal{A}_J = \{a_i^T x \leq b_i \mid i \in J\}$. Then, our assumption implies that for every index $k \in I$ we have an integral vector $x^k \in \mathbb{Z}^n$ for which

$$a_i x^k \leq b_i \quad \text{holds for all} \quad i \in I \setminus \{k\}.$$

Let $Z = \mathbb{Z}^n \cap conv\,(\{x^i | i \in I\})$, $Z_k = \{z \in Z \mid a_k^T z > b_k\}$, and define

[5]WHY?

$$\max \beta_1 + \cdots + \beta_m$$

$$\beta_j \ \geq \ \min_{z \in Z_j} a_j^T z \tag{5a}$$

$$\{x \in \mathbb{R}^n \mid a_i^T x < \beta_i, \ i \in I\} \cap Z = \emptyset \tag{5b}$$

Note that Z is finite, $Z_k \neq \emptyset$ by our assumptions, and $\beta_i > b_i$ for $i \in I$[6]. It follows then that such β_i, $i \in I$ exist, since (a) the set of $\beta = (\beta_1, ..., \beta_m)$ vectors satisfying (5a)-(5b) is nonempty (e.g., take equalities in (5a)), (b) bounded (since $\beta_i \leq a_i^T x^i$ for $i \in I$), and (c) closed (since the negation of (5b): "$\exists z \in Z$ for which $\beta_i > a_i^T z$ holds for all $i \in I$" defines an open set)[7].

Consequently[8], there are vectors $y^i \in Z$, $i \in I$ such that

$$a_j^T y^j = \beta_j \quad \text{and} \quad a_i^T y^j < \beta_i \quad \text{holds for all} \quad i \neq j, \ i, j \in I. \tag{6}$$

Assume now indirectly that we have $m > 2^n$. Then, we must have a pair of indices $i \neq j$, $i, j \in I$ for which the integral vectors y^i and y^j have the same parity componentwise, i.e., for which $z = \frac{1}{2}(y^i + y_j)$ is also an integral vector. Since in this case $z \in Z$, and $a_i^T z < \beta_i$ would hold for all $i \in I$ by (6), we get a contradiction with (5b), proving that our indirect assumption is false, i.e. that the claim of the theorem is true. □

Given a system $\mathcal{A}_I = \{a_i^T x \leq b_i, \ i \in I\}$ of linear inequalities in n variables, a vector $c \in \mathbb{R}^n$ and a subset $J \subseteq I$, let us define

$$\nu(J) = \max\{c^T x \mid a_i^T x \leq b_i, \ i \in J, \ \ x \in \mathbb{Z}^n\}.$$

The following corollary of the above theorem was proved by Scarf (1977) (cf. Todd (1977)).

Corollary 1 *If $\nu(I)$ is finite, then*

$$\nu(I) \quad = \quad \nu(J) \tag{7}$$

for some subset $J \subseteq I$ with $|J| \leq 2^n - 1$.

[6]WHY?
[7]WHY, WHY, and WHY???
[8]WHY?

Proof. Clearly, $\nu(J) \geq \nu(I)$ for all subsets $J \subseteq I$, thus it is enough to show that there exists a subset $J \subseteq I$ of size $|J| \leq 2^n - 1$ for which we have $\nu(J) \leq \nu(I)$.

Since $\nu(I)$ is finite, the system $\mathcal{A}_I \cup \{c^T x \geq \nu(I) + \frac{1}{t}\}$ has no feasible integral solution, for every integer $t \in \mathbb{Z}$. Therefore, by Theorem 6 it has a subsystem of size at most 2^n, which still does not have an integral feasible solution. Since $\mathcal{A}$ is feasible over $\mathbb{Z}^n$, the last inequality must belong to such an infeasible subsystem, i.e., for every $t \in \mathbb{Z}$ we have a subset $J_t \subseteq I$ such that $\mathcal{A}_{J_t} \cup \{c^T x \geq \nu(I) + \frac{1}{t}\}$ does not have a feasible integral solution, and $|J_t| \leq 2^n - 1$. Since I has only finitely many subsets, for one of them, say for J of size $|J| \leq 2^n - 1$, we must have $J = J_t$ for infinitely many values $t \in \mathbb{Z}$, i.e., for which $\mathcal{A}_J \cup \{c^T x > \nu(I)\}$ has no feasible integral solution, implying $\nu(J) \leq \nu(I)$, and hence completing the proof of (7). $\square$