Прилози, Одд. мат. тех. науки, МАНУ, XVIII, 1–2 (1997), с. 59–66
Contributions, Sec. Math. Tech. Sci., MANU, XVIII, 1–2 (1997), p. 59–66
ISSN 0351–3246
UDC: 514.742/75
512.533.7

INTEGRAL HILBERT BASES AND SUBSEMIGROUPS OF N^n

Magdalena Hadži-Kosta Josifovska

A b s t r a c t: In this paper we make a connection between the Hilbert bases and the polyhedral cones of N^n using subsemigroups of N^n.

Key words: Hilbert basis, Integral Hilbert basis, Subsemigroup of N^n, full subsemigroup

1. *Preliminaries*

In this section we recall the basic definitions and results used in the next section.

Further in this paper, $N = \{0, 1, \ldots, n, \ldots\}$ is the set of natural numbers and zero, that is, the set of nonnegative integers, and R is the set of real numbers. The symbol R^n denotes the n-dimensional Euclidean space. The elements of R^n are called n-dimensional vectors over R.

A vector or matrix is called **rational (integral**, respectively) if all its entries are rationals (integers, respectively).

A nonempty set C of points in Euclidean space is called a (convex) **cone** if $\lambda x + \mu y \in C$ for any $x, y \in C$ and $\lambda, \mu \geq 0$.

The cone generated by the set X of vectors $x_1, \ldots, x_m$ $(X = \{x_1, \ldots, x_m\})$ is the set

$$cone(X) := \{\lambda_1 x_1 + \ldots + \lambda_m x_m \mid \lambda_1, \ldots, \lambda_m \geq 0\} = cone\{x_1, \ldots, x_m\}, \quad (1.1)$$

i.e. it is the smallest convex cone containing $x_1, \ldots, x_m$. A cone defined in this way is called **finitely generated cone** by $x_1, \ldots, x_m$.

A cone C is **polyhedral** if

$$C = \{x \mid Ax \leq 0\} \quad (1.2)$$

for a matrix A, i.e. if C is the intersection of finitely many linear half-spaces. Here a **linear half-space** is a set of the form $\{x \mid ax \leq 0\}$ for some nonzero row vector a.

A finite set of vectors $a_1, \ldots, a_t$ is a **Hilbert basis** if each integral vector b in $cone\{a_1, \ldots, a_t\}$ is a nonnegative integral combination of $a_1, \ldots, a_t$.

Integral Hilbert basis is a Hilbert basis consisting of integral vectors only.

A **subsemigroup** of N^n generated by $H = \{a_1, \ldots, a_t\} \subseteq N^n$ denoted by $< H >$ is:

$$< H > := \left\{ \sum_{i=1}^{t} \alpha_i a_i \mid \alpha_i \in \mathbf{N} \right\}. \quad (1.3)$$

A subsemigroup $G \subseteq \mathbf{N}^n$ is called **full subsemigroup** if

$$G := N^n \cap C; \text{ for a } cone\ C \text{ in } \boldsymbol{R}^n. \quad (1.4)$$

2. *The Connection between Hilbert Bases and Subsemigroups of* N^n

Theorem 2.1. $H = \{a_1, \ldots, a_t\} \subseteq N^n$ is an integral Hilbert basis iff the subsemigroup $< H >$ of N^n generated by H, is full subsemigroup.

Proof. Directly from the definitions of $< H >$ and $cone(H)$, it follows that $< H > \subseteq cone(H)$.

Let H be an integral Hilbert basis. Then according to the definition of integral Hilbert basis, each $x \in N^n \cap cone(H)$ can be represented as: $x = \sum_{a \in H} \alpha_a a$, $\alpha_a \in N$. This implies (using (1.3)) that $x \in < H >$, i.e. $N^n \cap cone(H) \subseteq < H >$. Since $< H > \subseteq cone(H)$ and $< H > \subseteq N^n$ it follows that $< H > \subseteq N^n \cap cone(H)$. Therefore $< H > = N^n \cap cone(H)$, i.e. $< H >$ is full subsemigroup.

Conversely, let $< H >$ be full, i.e. $< H > = N^n \cap C$, for a cone C in R^n. Since $H \subseteq C$ it follows that $cone(H) \subseteq C$. Let $b \in cone(H) \cap N^n \subseteq C \cap N^n = < H >$. Then $b = \sum_{a \in H} \alpha_a a, \alpha_a \in N$, i.e. b is a nonnegative integral combination of vectors in H. So H is an integral Hilbert basis. ■

Theorem 2.2. Let $H = \{h_1, \ldots, h_t\}$. Then there is a unique minimal subset $K \subseteq H$, with $< K > = < H >$.

Proof. For a finite set X let $| X |$ denote the number of elements in X. So, $| H | = t$. We define a subset $K(H) \subseteq H$ by:

$$K(H) := \{a \mid a \in < H >, a \neq \sum_{i=1}^{t} \gamma_i h_i, \sum_{i=1}^{t} \gamma_i \geq 2; a \neq 0\}. \qquad (2.1)$$

Step 1. Proof that $< K(H) > = < H >$.

We will prove this by mathematical induction on t.

First let $t = 1$, i.e. $H = \{h\}$. According to (1.3), $< H > = \{nh \mid n \in N\}$. Then (2.1) implies that $K(H) = \{a \mid a \in < H >, \ a \neq \gamma h, \ \gamma \geq 2; \ a \neq 0\} = \{a \mid a = mh; \ m \in N; \ a \neq \gamma h; \ \gamma \geq 2; \ a \neq 0\} = \{a \mid a = h\} = H$. The last equation, $K(H) = H$, implies $< H > = < K(H) >$.

Let us suppose that $< K(H) > = < H >$ for sets H with k elements, for $k \leq t - 1$, i.e. if $| H | \leq t - 1$, then $< H > = < K(H) >$.

Now let H be a set of t different elements, i.e. $| H | = t$.

If $K(H) = H$, then $< H > = < K(H) >$.

Let $K(H) \neq H$, which means that there is $h \in H$ and $h \notin K(H)$. Without loss of generality, let $h = h_1$ and therefore $h_1 \in H \subseteq < H >$ and $h_1 \notin K(H)$. So:

$$h_1 = \sum_{i=1}^{t} \beta_i h_i; \quad h_1 \neq 0; \quad \sum_{i=1}^{t} \beta_i \geq 2,$$

i.e.

$$h_1 = \beta_1 h_1 + \sum_{i=2}^{t} \beta_i h_i; \beta_i \in N,$$

i.e.

$$(1-\beta_1)h_1 = \sum_{i=2}^{t} \beta_i h_i.$$

If $\beta_1 = 1$, then for each i, $\beta_i = 0$, i.e. $\sum_{i=1}^{t} \beta_i = 1$, which contradicts the assumption that $\sum_{i=1}^{t} \beta_i \geq 2$. For $\beta_1 \geq 2, (1-\beta_1)h_1 \notin N^n$ and $\sum_{i=2}^{t} \beta_i h_i \in N^n$, which contradicts the fact that $(1-\beta_1)h_1 = \sum_{i=2}^{t} \beta_i h_i$.

The above discussion implies that $\beta_1 = 0$, and so:

$$h_1 = \sum_{i=2}^{t} \beta_i h_i; \quad \sum_{i=2}^{t} \beta_i \geq 2. \tag{2.2}$$

Now, let $H' := H \setminus \{h_1\} = \{h_2, \ldots, h_t\}$. Then $|H'| = t-1$ and $H' \subseteq H$. Since $h_1 = \sum_{i=2}^{t} \beta_i h_i$, $\sum_{i=2}^{t} \beta_i \geq 2$, it follows that $h_1 \in <H'>$. So, $<H> \subseteq <H'>$, and since $H' \subseteq H$ it follows that $<H> = <H'>$. Let:

$$K(H') := \{a \mid a \in <H'>, a \neq \sum_{i=2}^{t} \gamma_i h_i; \quad \sum_{i=2}^{t} \gamma_i \geq 2, a \neq 0\}. \tag{2.3}$$

The inductive assumption implies that:

$$<K(H')> = <H'> = <H>. \tag{2.4}$$

Next, we shall prove that $K(H') = K(H)$.

If $a \notin K(H')$, (2.3) implies that $a = 0$ or $a = \sum_{i=2}^{t} \gamma_i h_i; \quad \sum_{i=2}^{t} \gamma_i \geq 2$.

If $a = 0$, (2.1) implies that $a \notin K(H)$.

If $a \neq 0$, then $a = 0 \cdot h_1 + \sum_{i=2}^{t} \gamma_i h_i = \sum_{i=1}^{t} \gamma_i h_i$; $\gamma_1 = 0$ and therefore

$$\sum_{i=1}^{t} \gamma_i = 0 + \sum_{i=2}^{t} \gamma_i \geq 2.$$

This implies that $a \notin K(H)$.

This shows that $K(H) \subseteq K(H')$.

Conversely, if $a \notin K(H)$, it follows that $a = 0$ or $a = \sum_{i=1}^{t} \gamma_i h_i$; $\sum_{i=1}^{t} \gamma_i \geq 2$.

If $a = 0$, by (2.3) $a \notin K(H')$.

If $a \neq 0$, then $a = \sum_{i=1}^{t} \gamma_i h_i$; $\sum_{i=1}^{t} \gamma_i \geq 2$, i.e.

$$a = \gamma_1 h_1 + \sum_{i=2}^{t} \gamma_i h_i = \gamma_1 \sum_{i=2}^{t} \beta_i h_i + \sum_{i=2}^{t} \gamma_i h_i = \sum_{i=2}^{t} (\gamma_1 \beta_i + \gamma_i) h_i;$$

where

$$\sum_{i=2}^{t} (\gamma_i \beta_i + \gamma_i) = \gamma_i \sum_{i=2}^{t} \beta_i + \sum_{i=2}^{t} \gamma_i \geq \gamma_i + \sum_{i=2}^{t} \gamma_i = \sum_{i=1}^{t} \gamma_i \geq 2,$$

which implies that $a \notin K(H')$.

Thus, we have shown that $K(H') \subseteq K(H)$.

Hence, $K(H') = K(H)$ and so, $< K(H') > = < K(H) >$. This, together with (2.4) implies that $< K(H) > = < H >$.

Step 2. Proof that $K(H)$ is a **minimal** subset of H, among the subsets L of H satisfying $< L > = < H >$.

Let us assume that there is a proper subset T of $K(H)$, such that $< T > = < K(H) > = < H >$. Since $T \subseteq K(H)$, it follows that there is $h \in K(H)$ and $h \notin T$.

Without loss of generality let $K(H) = \{h_1, \ldots, h_s\} \subseteq H$ and

$$T = \{h_1, \ldots, h_m\} \subseteq K(H),$$

for $m < s$. Then $h_s \in K(H)$ and $h_s \notin T$.

If $h_s \in <T>$, then $h_s = \sum_{i=1}^{m} \gamma_i h_i$, $\gamma_i \in N$, and therefore:

(a) If $\sum_{i=1}^{m} \gamma_i = 0$ then $\gamma_i = 0, (i = 1,\ldots,m)$ and $h_s = 0$, which contradicts the assumption that $h_s \in K(H)$.

(b) If $\sum_{i=1}^{m} \gamma_i = 1$, without loss of generality let $\gamma_1 = 1$. Then $\gamma_i = 0$ for $i \geq 2$ and so $h_s = h_1$. This is also a contradiction since $h_s \notin T$.

(c) If $\sum_{i=1}^{m} \gamma_i \geq 2$, then $h_s = \sum_{i=1}^{m} \gamma_i h_i + \sum_{i=m+1}^{t} \gamma_i h_i$, for $\gamma_i = 0$, $m+1 \leq i \leq t$, i.e. $h_s = \sum_{i=1}^{t} \gamma_i h_i$, $\sum_{i=1}^{t} \gamma_i \geq 2$. This implies that $h_s \notin K(H)$, which contradicts the assumption that $h_s \in K(H)$.

So, $<T> = <K(H)>$ and $T \subseteq H$, imply that $T = K(H)$.

Step 3. Proof that $K(H)$ is the **unique** minimal subset of H with $<K(H)> = <H>$.

Let us suppose, that $T \subseteq H$ is a minimal subset, with $<T> = <H>$. This implies that for each proper subset $M \subseteq T$, $<M> \neq <H>$. We shall show that $T = K(H)$.

Let $T = \{h_1,\ldots,h_m\}$, $m \leq t$ and let $a \in <T> = <H>$, with $a \notin T$. Then it follows that $a = \sum_{i=1}^{m} \gamma_i h_i$; $\gamma_i \in N$ and therefore:

(a) If $\sum_{i=1}^{m} \gamma_i = 0$ then $a = 0$, and thus $a \notin K(H)$ according to (2.1).

(b) If $\sum_{i=1}^{m} \gamma_i = 1$, then without loss of generality let $\gamma_1 = 1$. Then $\gamma_i = 0$ for $i \geq 2$ and so $a = \gamma_1 h_1 = h_1 \in T$. This is also a contradiction since $a \notin T$.

(c) If $\sum_{i=1}^{m} \gamma_i \geq 2$, then $a = \sum_{s=1}^{t} \gamma_s h_s$, where in the case $m < t$, $\gamma_j = 0$ for $m+1 \leq j \leq t$, and $\sum_{s=1}^{t} \gamma_s = \sum_{i=1}^{m} \gamma_i + \sum_{j=m+1}^{t} \gamma_j \geq 2 + 0 = 2$, which implies that $a \notin K(H)$.

Thus, we have shown that $K(H) \subseteq T$. Since T is a minimal subset of H with $<T>=<H>$ and since $<K(H)>=<H>$, it follows that $K(H)=T$. ■

Theorem 2.3. Let G be a finitely generated subsemigroup of N^n. Then there is a unique minimal subset K of G, such that $<K>=G$.

Proof. It is enough to show that the set $K(H)$ definied in Theorem 2.2, does not depend on the set of generators H. So, let H_1 and H_2 be two finite generating sets for G, i.e. $<H_1>=<H_2>=G$. Let $H=H_1 \cup H_2$. Then H is also a generating set for G, i.e. $<H>=G$. Theorem 2.2 implies that $<K(H_1)>=<K(H_2)>=<K(H)>=G$. Then, since $H_i \subseteq H, i=1,2$ and $K(H)$ is the unique minimal subset of H with $<K(H)>=<H>=G$, it follows that $K(H_1)=K(H_2)=K(H)$. ■

As a result of Theorems 2.1 and 2.2 we obtain as a Corollary the well-known existence of unique minimal integral Hilbert basis for a given integral Hilbert basis [5] (T.16.4).

Corollary 2.4. If $H \subseteq N^n$ is an integral Hilbert basis, then there is a unique subset $K \subseteq H$, such that K is a minimal integral Hilbert basis.

Proof. If $H \subseteq N^n$ is an integral Hilbert basis, according to Theorem 2.1 it follows that the subsemigroup $<H>$ of N^n generated by H, is full subsemigroup, and by Theorem 2.2 it follows that there is a unique minimal subset $K \subseteq H$ with $<H>=<K>$. Therefore, the subsemigroup $<K>$ is full. Now, Theorem 2.1 implies that K is an integral Hilbert basis, and Theorem 2.2 implies that K is a unique minimal integral Hilbert basis for H. ■

REFERENCES

[1] Bachem A.: *The theorem of Minkowski for polyhedral monoids and aggregated linear diophantine systems*, in: Optimization and Operations Research (Proceedings of a Workshop held at the University of Bonn, 1977), Lecture Notes in Economics and Mathematical Systems 157, Springer, Berlin, p.p. 1–13 (1978).

[2] Димовски Д.: *Адитивни полугрупи на цели броеви*, МАНУ, Скопје, Прилози, **IX**, 2, (1977).

[3] Jeroslow R. G.: *Some basis theorems for integral monoids*, Mathematics of Operations Research, 3, 145–154 (1978).

[4] Meyer R. R.: *On the existence of optimal solutions to integer and mixed-integer programming problems*, Mathematical Programming, 7, 223–235 (1974).

[5] Schrijver A.: *Theory of linear and integer programming*, John Wiley&Sons, Ltd., Chichester, 1986.

Р е з и м е

ИНТЕГРАЛНИ ХИЛБЕРТОВИ БАЗИ И ПОТПОЛУГРУПИ ОД N^n

Во овој труд е разгледана врската меѓу Хилбертовите бази и многуставните конуси во N^n со помош на потполугрупи од N^n. Основен резултат е:

Теорема 2.3. Секоја конечно генерирана потполугрупа од N^n има (еднозначно определена) база, т.е. најмало генераторно множество.

Magdalena Hadži-Kosta Josifovska

Technical faculty,
97000 Bitola, Republic of Macedonia