Charles University in Prague
Faculty of Mathematics and Physics

MASTER THESIS

Marek Scholle

Semigroups of lattice points

Department of Algebra

Supervisor of the master thesis:
prof. RNDr. Tomáš Kepka, DrSc.

Study programme: Mathematics
Specialization: Mathematical structures

Prague 2012

First and foremost, I would like to thank my parents for their consistent support throughout the long time of my studies. I thank to prof. Tomáš Kepka for giving me the opportunity to work under his guidance.

I declare that I carried out this master thesis independently, and only with the cited sources, literature and other professional sources.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Coll., the Copyright Act, as amended, in particular the fact that the Charles University in Prague has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 paragraph 1 of the Copyright Act.

In Prague date ________________

Marek Scholle

Název práce: Pologrupy mřížových bodů
Autor: Marek Scholle
Katedra: Katedra algebry
Vedoucí diplomové práce: prof. RNDr. Tomáš Kepka, DrSc., Katedra algebry

Abstrakt: V práci se zabýváme podpologrupami $(\mathbb{N}_0^m, +)$, speciální diskuse je posléze věnována případům $m = 1$, $m = 2$ a $m = 3$. Dokážeme, že podpologrupa $\mathbb{N}_0^m$ je konečně generovaná, právě když jí generovaný kužel je konečně generovaný, ekvivalentně polyhedrální, a popisujeme základní topologické vlastnosti takovýchto kuželů. Na příkladech dokládáme, že podmínky zaručující konečnou generovanost v $\mathbb{N}_0^2$ nelze snadno přenést do vyšších dimenzí. Definujeme Hilbertovu bázi a s ní související pojem Carathéodoryho ranku a kromě základních vlastností dokážeme, že Carathéodoryho rank podpologrupy $\mathbb{N}_0^m$, $m = 1, 2, 3$, je menší nebo roven m. Zvláštní pozornost věnujeme pologrupám obsahujícím netriviální podpologrupu „odčítacích“ prvků.

Klíčová slova: pologrupa, konečně generovaný, mřížový bod, kužel, polyhedrální, díra, odčítací prvek, Hilbertova báze, Carathéodoryho rank

Title: Semigroups of lattice points
Author: Marek Scholle
Department: Department of algebra
Supervisor: prof. RNDr. Tomáš Kepka, DrSc., Department of algebra

Abstract: The thesis deals with subsemigroups of $(\mathbb{N}_0^m, +)$, a special discussion is later devoted to the cases $m = 1$, $m = 2$ and $m = 3$. We prove that a subsemigroup of $\mathbb{N}_0^m$ is finitely generated if and only if its generated cone is finitely generated (equivalently polyhedral) and we describe basic topological properties of such cones. We give a few examples illustrating that conditions sufficient for finite generation in $\mathbb{N}_0^2$ can not be easily transferred to higher dimensions. We define the Hilbert basis and the related notion of Carathéodory's rank. Besides their basic properties we prove that Carathédory's rank of a subsemigroup of $\mathbb{N}_0^m$, $m = 1, 2, 3$, is less than or equal to m. A particular attention is devoted to the subsemigroups containing non-trivial subsemigroups of “subtractive” elements.

Keywords: semigroup, finitely generated, lattice point, cone, polyhedral, hole, subtractive element, Hilbert basis, Carathéodory's rank

Contents

Preface

The aim of this thesis is to compile a relevant material on subsemigroups of $\mathbb{N}_0^m$ and extend the materials which originated in my supervisor's research on parasemifields. One of the goals was to describe some of the basic properties of subtractive elements and answer the question whether finitely generated semigroups have some special topological properties (mainly in the cases $m = 2$ and $m = 3$). The following problems arise from [Jež12]:

Question 1: If a semigroup A of $\mathbb{N}_0^m$ possesses a subtractive element (later: $\mathcal{E}(A)$ is non-trivial), is necessarily finitely generated? The problem was solved in [Jež12] for $m = 2$ using very simple and non-general methods. The case $m = 2$ turns to be a special case of original Theorem 3.17. Combining Lemma 2.10 and Example 4.12 shows that the theorem can not be simply extended (but is still far from being conclusive). As far as I know, no one paid deeper attention to the subsemigroup $\mathcal{E}(A)$; only the most trivial properties are introduced in [Kep09]. Thus 2.9(iv), 2.10, 3.10–3.17 and 4.12 can be treated as an original material.

Question 2: Do finitely generated semigroups have some special topological properties? It is known that semigroups are finitely generated if its cones are finitely generated. (The motivation of other authors differs from ours, hence the terminology is not same. Moreover, none of them works with topology in $\mathbb{Q}^m$.) According to my opinion, there is no "really independent" way (in dimension ≥ 3) to describe finitely generated semigroups, cf. Example 4.13. There are only tests detecting some of non-finitely generated ones.

The motivation for study of subsemigroups of $\mathbb{N}_0^m$ goes to recent Prague research on parasemifields. A classical result, occasionally attributed to Kaplansky, states that every field finitely generated as a ring is finite; the non-commutative analogy is at present far from being solved, but there is also an analogy in parasemifields generated as semirings. (A commutative semiring is an algebraic structure with two associative commutative binary operations called addition and multiplication such that the multiplication distributes over the addition. A parasemifield is a non-trivial commutative semiring whose multiplicative semigroup is a group.) There are many examples of additively idempotent commutative parasemifields, which are finitely generated as semirings. One may ask whether *every* parasemifield finitely generated as a semiring is additively idempotent. In [Jež12] there is given an affirmative answer in the 2-generated case; the procedure relies on transferring the problem to subsemigroups of $\mathbb{N}_0^m$ with special properties. The method is further developed in [Kal09] and [Jež10].

* * *

I have compiled in Chapter 1 some basic facts needed later. The proofs are mainly standard (I used [Kep09], [Bar02] and [Mat02], some statements and proofs are mine). The proofs of Lemma 1.16 and Theorem 1.17 were adapted from [Sch86].

Chapter 2 is a brief introduction to subsemigroups of $\mathbb{N}_0^m$. Most of material were taken from [Kep09] except the part dealing with Hilbert basis. Its definition and Proposition 2.4 were taken from [Seb90]. My own are 2.5, 2.6, 2.9(iv) and 2.16.

In Chapter 3 we are concerned with the notion of pure semigroups, Carathéodory's rank and holes in semigroups. Parts 3.6 and 3.7 are taken from [Seb90] and [Br98], Lemma 3.8 is mine (other authors generally do not care about semigroups which are not finitely generated). Most of ideas presented in 3.18 appear in [He09].

In Chapter 4 we discuss special cases $m = 1$, $m = 2$ and $m = 3$. Lemma 4.1 was adapted from [Kep09], the parts 4.9 and 4.10 from [Seb90] (with slight changes). The notion of the slope and the border rays was adapted from [Kep09] and originated in [Jež12]. Theorem 4.14 and its very interesting proof was presented by András Sebő in [Seb90]. Although I present only a compilation of his ideas, I believe that the readability and accuracy is superior to the original (there are some minor errors in [Seb90] and many details are left to reader). Moreover, the final conclusion is simplified using the (original) trivial observation 2.5(ii), maybe overseen by Sebő. Propositions 4.3 and 4.7 and Examples 4.11–4.13 are original. Proposition 4.15 belongs with its nature rather to third chapter than fourth; the reason why I have placed it before the proof of 4.14 is that the proofs of 4.15 and 4.16 share important ideas.

1. Preliminaries

We shall use the following notation throughout the thesis:

$\mathbb{Z}$, $\mathbb{N}$, $\mathbb{N}_0$	...	the set of all/all positive/all non-negative integers,
$\mathbb{Q}$, $\mathbb{R}$	...	the ordered field of rational/real numbers,
$\mathbb{Q}^+$, $\mathbb{R}^+$	...	the set of all positive rational/real numbers,
$\mathbb{Q}_0^+$, $\mathbb{R}_0^+$	...	the set of all non-negative rational/real numbers,
$\mathbb{T}$	...	the field $\mathbb{Q}$ or $\mathbb{R}$,
m	...	an arbitrary positive integer,
$k \times t$	...	$k \in \mathbb{N}_0$, $t \in \mathbb{T}$, an abbreviation for $\underbrace{t + t + \cdots + t}_{k\text{-times}}$,
A	...	a subset of $\mathbb{T}^m$, often an additive subsemigroup of $(\mathbb{T}^m, +)$,
$\mathrm{Lin}(A)$	...	the linear hull of A in the vector space $\mathbb{T}^m/\mathbb{T}$,
$\dim A$	...	the dimension of a linear subspace A of $\mathbb{T}^m/\mathbb{T}$,
$\operatorname{rank} A$	...	the dimension of the linear hull of A in the vector space $\mathbb{T}^m/\mathbb{T}$.

The theory introduced in this chapter can be developed simultaneously in rational and real spaces, thus we work with "$\mathbb{T}$", which is either $\mathbb{Q}$ or $\mathbb{R}$. Occasionally we use the usually ordered set $\mathbb{T} \cup \{-\infty, \infty\}$ obtained by adjoining two improper elements $-\infty$ and ∞ to $\mathbb{T}$ (i.e. $-\infty < t < \infty$ for all $t \in \mathbb{T}$).

The set $\mathbb{T}^m$ of all ordered m-tuples of elements of $\mathbb{T}$ is regarded as a vector space over $\mathbb{T}$; sometimes we refer to the elements of $\mathbb{T}^m$ as *points*. The elements of $\mathbb{Z}^m$ are called *integer points*. We do not distinguish elements of $\mathbb{T}^k \times \mathbb{T}^\ell$ and $\mathbb{T}^{k+\ell}$, where $k, \ell \in \mathbb{N}$.

Let $A, B \subseteq \mathbb{T}^m$, $a_0 \in \mathbb{T}^m$ and $q \in \mathbb{T}$. We write $A + B$ resp. qA for the set $\{a + b \mid a \in A, b \in B\}$ resp. $\{qa \mid a \in A\}$ and define $-A = (-1)A$, $A - B = A + (-B)$, $a_0 + A = \{a_0\} + A$, $A - a_0 = (-a_0) + A$ and $A/q = (1/q)A$ in the case $q \neq 0$.

A set A is called *convex* if $qa + (1-q)b \in A$ for arbitrary $a, b \in A$ and every $q \in \mathbb{T}_0^+$, $q \leq 1$. A set A is a *convex cone* (*cone* for short) if $qa + rb \in A$ for all $a, b \in A$ and any $q, r \in \mathbb{T}_0^+$.

Let $n \in \mathbb{N}$ and $a_1, a_2, \ldots, a_n \in \mathbb{T}^m$. Moreover, let $q_1, q_2, \ldots, q_n \in \mathbb{T}_0^+$ be arbitrary resp. such that $\sum_{i=1}^n q_i = 1$. The sum $q_1 a_1 + q_2 a_2 + \cdots + q_n a_n$ is called a *conic combination* resp. a *convex combination* of the points $a_1, a_2, \ldots, a_n$.

1.1 Definition. Let $A \subseteq \mathbb{T}^m$. The *convex hull of the set* A, denoted by $\mathrm{conv}(A)$, is the set of all convex combinations from A and the *conic hull of the set* A, denoted by $\mathrm{cone}(A)$, is the set of all conic combinations from A. Thus

$$\mathrm{cone}(A) = \Big\{ \sum_{i=1}^n q_i a_i \;\Big|\; n \in \mathbb{N},\, a_i \in A,\, q_i \in \mathbb{T}_0^+ \Big\},$$

$$\mathrm{conv}(A) = \Big\{ \sum_{i=1}^n q_i a_i \;\Big|\; n \in \mathbb{N},\, a_i \in A,\, q_i \in \mathbb{T}_0^+,\, \sum_{i=1}^n q_i = 1 \Big\}.$$

Let A be a cone. We say that A is a *finitely generated cone* if there exist $a_1, \ldots, a_n \in A$, $n \in \mathbb{N}_0$, such that $A = \operatorname{cone}(\{a_1, \ldots, a_n\})$. In this case the points $a_1, \ldots, a_n$ are called the *generators of the cone* A (thus the cone $\emptyset$ is generated by $\emptyset$).

1.2 Proposition. *Let A and B be convex (conic) subsets of $\mathbb{T}^m$. Then $-A$, $A + B$ and $A - B$ are convex (conic) sets. The intersection of a non-empty system of convex (conic) subsets of $\mathbb{T}^m$ is a convex (conic) set.*

1.3 Lemma. *Let $A \subseteq \mathbb{T}^m$. Then*

- (i) $A \subseteq \operatorname{conv}(A)$;
- (ii) $\operatorname{conv}(\operatorname{conv}(A)) = \operatorname{conv}(A)$;
- (iii) *if* $A \subseteq (\mathbb{T}_0^+)^m$, *then* $\operatorname{conv}(A) \subseteq (\mathbb{T}_0^+)^m$ *and moreover,* $0 \in \operatorname{conv}(A)$ *if and only if* $0 \in A$;
- (iv) *if* $A \subseteq (\mathbb{T}^+)^m$, *then* $\operatorname{conv}(A) \subseteq (\mathbb{T}^+)^m$ *and* $0 \notin A$.

Proof of (ii). Take an a in $\operatorname{conv}(\operatorname{conv}(A))$ and write $a = \sum_{i=1}^n q_i a_i$, where $n \in \mathbb{N}$, $a_i \in \operatorname{conv}(A)$ and $q_i \in \mathbb{T}_0^+$, $\sum_{i=1}^n q_i = 1$. Express every a_i as $a_i = \sum_{j=1}^{k_i} q_{ij} a_{ij}$, where $k_i \in \mathbb{N}$, $a_{ij} \in A$ and $q_{ij} \in \mathbb{T}_0^+$, $\sum_{j=1}^{k_i} q_{ij} = 1$. There is no loss of generality in assuming $k_1 = k_2 = \cdots = k_n = k \in \mathbb{N}$. We have $a = \sum_{i=1}^n \sum_{j=1}^k q_i q_{ij}\, a_{ij}$ and

$$\sum_{i=1}^n \sum_{j=1}^k q_i q_{ij} = \sum_{i=1}^n q_i \sum_{j=1}^k q_{ij} = \sum_{i=1}^n q_i = 1,$$

thus $a \in \operatorname{conv}(A)$. Hence $\operatorname{conv}(\operatorname{conv}(A)) \subseteq \operatorname{conv}(A)$; the rest follows from (i). ∎

1.4 Lemma. *Let $A \subseteq \mathbb{T}^m$. Then*

- (i) $A \subseteq \operatorname{conv}(A) \subseteq \operatorname{cone}(A) = \operatorname{conv}(B)$, *where* $B = \{qa \mid a \in A,\ q \in \mathbb{T}_0^+\}$;
- (ii) *if* $A \neq \emptyset$, *then* $0 \in \operatorname{cone}(A)$;
- (iii) $\operatorname{cone}(\operatorname{cone}(A)) = \operatorname{conv}(\operatorname{cone}(A)) = \operatorname{cone}(\operatorname{conv}(A)) = \operatorname{cone}(A)$;
- (iv) *if* $A \subseteq (\mathbb{T}_0^+)^m$, *then* $\operatorname{cone}(A) \subseteq (\mathbb{T}_0^+)^m$;
- (v) $\operatorname{cone}(A) = A$ *if and only if* $\operatorname{conv}(A) = A$ *and* $qA \subseteq A$ *for every* $q \in \mathbb{T}_0^+$.

It easily follows from 1.3 and 1.4 that the convex hull resp. conic hull of A is the smallest set containing A and closed under the operation of convex combination resp. conic combination. Hence $\operatorname{conv}(A)$ is the smallest convex superset of A and $\operatorname{cone}(A)$ is the smallest convex cone containing A.

1.5 Lemma (Carathéodory's theorem for convex sets)**.**
Let n be a positive integer, $q_1, \ldots, q_n \in \mathbb{T}_0^+$, $\sum_{i=1}^n q_i = 1$, and $a_1, \ldots, a_n \in \mathbb{T}^m$. Let $a = \sum_{i=1}^n q_i a_i$. Then there exist $\ell \in \mathbb{N}$, $\ell \leq m + 1$, $r_1, \ldots, r_\ell \in \mathbb{T}_0^+$, $\sum_{k=1}^{\ell} r_k = 1$, and pairwise distinct indices $i_1, \ldots, i_\ell \in \{1, \ldots, n\}$ such that $a = \sum_{k=1}^{\ell} r_k a_{i_k}$. In other words: a is a convex combination of at most $m + 1$ points from the set $\{a_1, \ldots, a_n\}$.

Proof. It suffices to prove this property: If $n \geq m+2$, then a can be written as a convex combination of $n - 1$ points from the set $\{a_1, \ldots, a_n\}$. Thus suppose that $n \geq m + 2$, the points $a_1, \ldots, a_n$ are pairwise different and $q_1, \ldots, q_n \in \mathbb{T}^+$ (if $q_i = 0$ for some i, this property is trivial).

There are $s_1, \dots, s_{n-1} \in \mathbb{T}$ such that $\sum_{i=1}^{n-1} s_i(a_i - a_n) = 0$ and $s_{i_0} \neq 0$ for some i_0 (the vectors $a_i - a_n$ are linearly dependent in $\mathbb{T}^m$). Set $s_n = -(s_1 + \cdots + s_{n-1})$. Then $\sum_{i=1}^n s_i a_i = 0$ and $\sum_{i=1}^n s_i = 0$. Hence the set $J = \{j \in \{1, \dots, n\} \mid s_j > 0\}$ is non-empty and there is a $j_0 \in J$ such that $q_{j_0}/s_{j_0} \leq q_j/s_j$ for all $j \in J$. Write $t = q_{j_0}/s_{j_0} \in \mathbb{T}^+$ and set $r_i = q_i - ts_i$ for every $i = 1, \dots, n$. We have $r_i \in \mathbb{T}_0^+$, $r_{j_0} = 0$ and $\sum_{i=1}^n r_i = \sum_{i=1}^n q_i - t \sum_{i=1}^n s_i = 1$. Furthermore,

$$\sum_{i=1,\, i \neq j_0}^{n} r_i a_i = \sum_{i=1}^{n} r_i a_i = \sum_{i=1}^{n} q_i a_i - t \sum_{i=1}^{n} s_i a_i = a - 0 = a.$$

Thus a is a convex combination of $n-1$ points from the set $\{a_1, \dots, a_n\}$. ∎

1.6 Lemma (Carathéodory's theorem for cones)**.**
Let n be a positive integer, $q_1, \dots, q_n \in \mathbb{T}_0^+$ and $a_1, \dots, a_n \in \mathbb{T}^m$. Let $a = \sum_{i=1}^n q_i a_i$. Then there is an $L \subseteq \{1, 2, \dots, n\}$ such that the set $\{a_\ell \mid \ell \in L\}$ is linearly independent (thus $|L| \leq m$) and $a = \sum_{\ell \in L} r_\ell a_\ell$ for some $r_\ell \in \mathbb{T}_0^+$, $\ell \in L$. In other words: a is a conic combination of linearly independent vectors from the set $\{a_1, \dots, a_n\}$.

Proof. We may assume that $a \neq 0$. Take an $L \subseteq \{1, 2, \dots, n\}$ such that $a \in \operatorname{cone}(\{a_\ell \mid \ell \in L\})$ and $|L|$ is smallest possible. There exist $r_\ell \in \mathbb{T}^+$, $\ell \in L$, such that $a = \sum_{\ell \in L} r_\ell a_\ell$. Aiming for a contradiction, suppose the set $\{a_\ell \mid \ell \in L\}$ is not linearly independent. Then we can find $s_\ell \in \mathbb{T}$, $\ell \in L$, such that $\sum_{\ell \in L} s_\ell a_\ell = 0$ and at least one s_ℓ is positive. Set $J = \{\ell \in L \mid s_\ell > 0\} \neq \emptyset$ and denote by j_0 an element of J with $t = r_{j_0}/s_{j_0} \leq r_j/s_j$ for all $j \in J$. For every $\ell \in L$ set $r'_\ell = r_\ell - ts_\ell$; note that $r'_\ell \geq 0$ and $r'_{j_0} = 0$. Moreover,

$$\sum_{\ell \in L \setminus \{j_0\}} r'_\ell a_\ell = \sum_{\ell \in L} r'_\ell a_\ell = \sum_{\ell \in L} (r_\ell - ts_\ell) a_\ell = \sum_{\ell \in L} r_\ell a_\ell - t \sum_{\ell \in L} s_\ell a_\ell = a - 0 = a.$$

Therefore $a \in \operatorname{cone}(\{a_\ell \mid \ell \in L \setminus \{j_0\}\})$, which contradicts the minimality of $|L|$. ∎

1.7 Remark. Suppose that $a = \sum_{i=1}^{\ell} r_i a_i$, where $\ell \in \mathbb{N}$, $r_i \in \mathbb{T}^+$ and $0 \neq a_i \in (\mathbb{T}_0^+)^m$ for all $i \in \{1, \dots, \ell\}$, and suppose the set $\{a_i \mid i = 1, \dots, \ell\}$ is not linearly independent. Then there exist $s_i \in \mathbb{T}$, $i = 1, \dots, \ell$, not all zero, such that $\sum_{i=1}^{\ell} s_i a_i = 0$ and $\sum_{i=1}^{\ell} s_i \geq 0$. Since a_i's are nonzero, at least one s_i is positive and at least one s_i is negative. Let $J = \{j \in \{1, \dots, \ell\} \mid s_j < 0\} \neq \emptyset$ and let $j_0 \in J$ be such that $-r_j/s_j \leq -r_{j_0}/s_{j_0} = t \in \mathbb{T}^+$ for all $j \in J$. Consider the representation $a = \sum_{i=1}^{\ell} (r_i + ts_i) a_i$. We have $r_i + ts_i \geq 0$ for all i, since $r_j + ts_j \geq 0$ for all $j \in J$, and $r_{j_0} + ts_{j_0} = 0$. Moreover, $\sum_{i=1}^{\ell} (r_i + ts_i) = \sum_{i=1}^{\ell} r_i + t \sum_{i=1}^{n} s_i \geq \sum_{i=1}^{n} r_i$.

1.8 Proposition. *Let n be a positive integer, $a_1, \dots, a_n \in (\mathbb{T}_0^+)^m$ be nonzero and $a \in \operatorname{cone}(\{a_1, \dots, a_n\})$. Among all possible representations of a in the form $\sum_{i=1}^n q_i a_i$, where $q_i \in \mathbb{T}_0^+$, there is one with $\sum_{i=1}^n q_i$ maximal. Furthermore, it can be chosen in such way that the set $\{a_i \mid i \in \{1, \dots, n\},\ q_i \neq 0\}$ is linearly independent.*

Proof. Since there are only finitely many linearly independent subsets of $\{a_1, \dots, a_n\}$, it is enough to prove that if we are given a representation $a = \sum_{i=1}^n q_i a_i$, where $q_i \in \mathbb{T}_0^+$, then there exists a representation $a = \sum_{i=1}^{n} r_i a_i$, where $r_i \in \mathbb{T}_0^+$, such that the set $\{a_i \mid i \in \{1,\dots,n\},\ r_i \neq 0\}$ is linearly independent and $\sum_{i=1}^{n} r_i \geq \sum_{i=1}^{n} q_i$. Such representation can be obtained by iterating the step described in the previous remark. ∎

Lemma 1.5 and Lemma 1.6 can be reformulated as follows:

1.9 Proposition. *Let $A \subseteq \mathbb{T}^m$. Then*

$$\operatorname{conv}(A) = \bigcup\bigl\{\operatorname{conv}(B) \bigm| B \subseteq A,\ |B| \leq m+1\bigr\}$$

and

$$\operatorname{cone}(A) = \bigcup\bigl\{\operatorname{cone}(C) \bigm| C \subseteq A,\ |C| \leq m\bigr\}.$$

(Compare with Definition 1.1, later with Lemmas 3.5 and *3.6.)*

1.10 Note. When needed, we use the notation $\operatorname{cone}_{\mathbb{Q}}(-)$ and $\operatorname{conv}_{\mathbb{R}}(-)$ for $\operatorname{cone}(-)$ and $\operatorname{conv}(-)$ if $\mathbb{T}$ is the field $\mathbb{Q}$ and $\mathbb{R}$ respectively. Let $A \subseteq \mathbb{Q}^m$. We prove that $\operatorname{cone}_{\mathbb{Q}}(A)$ is the set of all rational points in $\operatorname{cone}_{\mathbb{R}}(A)$ (similarly we have $\operatorname{conv}_{\mathbb{Q}}(A) = \operatorname{cone}_{\mathbb{R}}(A) \cap \mathbb{Q}^m$). The inclusion $\operatorname{cone}_{\mathbb{Q}}(A) \subseteq \operatorname{cone}_{\mathbb{R}}(A) \cap \mathbb{Q}^m$ is trivial. Conversely, suppose that $a = \sum_{i=1}^{\ell} r_\ell a_\ell \in \mathbb{Q}^m$, where $r_i \in \mathbb{R}_0^+$, $1 \leq i \leq \ell$, and that the set $\{a_1,\dots,a_\ell\} \subseteq A$ is linearly independent in the vector space $\mathbb{R}^m/\mathbb{R}$ (c.f. Lemma 1.6). In other words, the real system of linear equations corresponding to the matrix

$$\left(\begin{array}{cccc|c} a_1^1 & a_2^1 & \cdots & a_\ell^1 & a^1 \\ a_1^2 & a_2^2 & \cdots & a_\ell^2 & a^2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1^m & a_2^m & \cdots & a_\ell^m & a^m \end{array}\right)$$

(upper indices denote components in $\mathbb{Q}^m$) has the unique solution $(r_1,\dots,r_\ell) \in \mathbb{R}^\ell$. It follows from the Gaussian elimination that this solution is rational, hence $a \in \operatorname{cone}_{\mathbb{Q}}(A)$.

1.11 Norm and topology on $\mathbb{T}^m$. From now on, $\|\cdot\|$ denotes the "Manhattan" norm on $\mathbb{T}^m$, i.e. $\|a\| = |q_1| + |q_2| + \cdots + |q_m|$ for $a = (q_1, q_2, \dots, q_m) \in \mathbb{T}^m$. The norm $\|\cdot\|$ gives rise to a metric on $\mathbb{T}^m$; the distance of $a, b \in \mathbb{T}^m$ is defined to be $\|a - b\|$. We denote by $B(a, r)$ the open ball of radius $r \in \mathbb{R}^+$ centered at $a \in \mathbb{T}^m$, i.e. $B(a,r) = \{b \in \mathbb{T}^m \mid \|b - a\| < r\}$. We speak about open and closed sets in the usual way. Let $A \subseteq \mathbb{T}^m$. *The interior of* A is the open set $\operatorname{int}(A) = \{a \in A \mid \exists \varepsilon \in \mathbb{R}^+\colon B(a,\varepsilon) \subseteq A\}$; $\operatorname{int}(A)$ is the union of all open subsets of A. *The closure of* A is the closed set $\operatorname{cl}(A) = \{a \in \mathbb{T}^m \mid \forall \varepsilon \in \mathbb{R}^+\colon B(a,\varepsilon) \cap A \neq \emptyset\}$; $\operatorname{cl}(A)$ is the intersection of all closed supersets of A. *The boundary of* A is the closed set $\partial A = \{a \in \mathbb{T}^m \mid \forall \varepsilon \in \mathbb{R}^+\colon B(a,\varepsilon) \cap A \neq \emptyset$ and $B(a,\varepsilon) \cap (\mathbb{T}^m \setminus A) \neq \emptyset\} = \operatorname{cl}(A) \setminus \operatorname{int}(A)$.

1.12 Lemma. *Let $A \subseteq \mathbb{T}^m$ be a cone. Then the sets* $\operatorname{int}(A) \cup \{0\}$ *and* $\operatorname{cl}(A)$ *are cones.*

Proof. We first prove that $\operatorname{int}(A) \cup \{0\}$ is a cone. Let $a_1, a_2 \in \operatorname{int}(A)$ and let $\varepsilon \in \mathbb{R}^+$ be such that $B(a_i, \varepsilon) \subseteq A$ for $i = 1, 2$. Take arbitrary $r_1, r_2 \in \mathbb{T}_0^+$ and set $a = r_1 a_1 + r_2 a_2$. If $r_1 = r_2 = 0$, then $a = 0$. If $r_1 = 0$ and $r_2 \neq 0$, then $a = r_2 a_2$ and $B(a, r_2\varepsilon) \subseteq A$, hence

$a \in \operatorname{int}(A)$. The symmetric case $r_1 \neq 0$ and $r_2 = 0$ gives the same result. Assume now that r_1 and r_2 are both nonzero and take an arbitrary $b \in \mathbb{T}^m$ with $\|b\| < \min(r_1\varepsilon, r_2\varepsilon)$. We have $a + b = r_1(a_1 + b/(2r_1)) + r_2(a_2 + b/(2r_2))$. Since $(a_i + b/(2r_i)) \in B(a_i, \varepsilon) \subseteq A$ for $i = 1, 2$, we have $a + b \in A$ and consequently $a \in \operatorname{int}(A)$.

Now we prove that $\operatorname{cl}(A)$ is a cone. We may assume that $A \neq \emptyset$, thus $0 \in A$. Let $a_1, a_2 \in \operatorname{cl}(A)$ and $r_1, r_2 \in \mathbb{T}_0^+$. Set $a = r_1a_1 + r_2a_2$ and take an arbitrary $\varepsilon \in \mathbb{R}^+$. The task is to find $a' \in B(a, \varepsilon) \cap A$. If $r_1 = r_2 = 0$, then $a = 0$ and we may set $a' = 0$. If $r_1 = 0$ and $r_2 \neq 0$, find $a_2' \in B(a_2, \varepsilon/r_2) \cap A$ and we have $a' = r_2a_2' \in B(a, \varepsilon) \cap A$. The symmetric case is analogous. If r_1 and r_2 are both nonzero, find $a_1' \in B(a_1, \varepsilon/(2r_1)) \cap A$ and $a_2' \in B(a_2, \varepsilon/(2r_2)) \cap A$ and set $a' = r_1a_1' + r_2a_2' \in A$. We have $\|a - a'\| = \|r_1(a_1 - a_1') + r_2(a_2 - a_2')\| \leq r_1\|a_1 - a_1'\| + r_2\|a_2 - a_2'\| < r_1\varepsilon/(2r_1) + r_2\varepsilon/(2r_2) = \varepsilon$. ∎

1.13 Proposition. *Let $a_0, a_1, \dots, a_m \in \mathbb{T}^m$ be such that the vectors $a_1 - a_0, \dots, a_m - a_0$ are linearly independent in $\mathbb{T}^m/\mathbb{T}$ and let $q_0, q_1, \dots, q_m \in \mathbb{T}^+$ be such that $\sum_{i=0}^m q_i = 1$. Then $a = \sum_{i=0}^m q_ia_i \in \operatorname{int}(\operatorname{conv}(\{a_0, \dots, a_m\}))$.*

Proof. Let $\{\pi_j \mid j = 1, \dots, m\}$ be the dual basis corresponding to the basis $\{a_j - a_0 \mid j = 1, \dots, m\}$ of $\mathbb{T}^m$ and let $\pi_0 = -\sum_{j=1}^m \pi_j$. Thus we have $c = \sum_{i=0}^m \pi_i(c)\, a_i$ for every $c \in \mathbb{T}^m$.

Let $\{e_j \mid j = 1, \dots, m\}$ be the canonical basis of $\mathbb{T}^m$ and let $\varepsilon \in \mathbb{R}^+$ be such that $\varepsilon|\pi_i(e_j)| < q_i/m$ for all $i \in \{0, \dots, m\}$ and $j \in \{1, \dots, m\}$.

Take an arbitrary $b = (r_1, \dots, r_m) \in \mathbb{T}^m$ with $\|b\| < \varepsilon$. We have

$$b = \sum_{j=1}^m r_je_j = \sum_{j=1}^m r_j \sum_{i=0}^m \pi_i(e_j)\, a_i = \sum_{i=0}^m \sum_{j=1}^m \Big(r_j\pi_i(e_j)\Big)a_i.$$

For $i = 0, \dots, m$ set $s_i = \sum_{j=1}^m r_j\pi_i(e_j)$ (note that $\sum_{i=0}^m s_i = \sum_{i=0}^m \sum_{j=1}^m r_j\pi_i(e_j) = \sum_{j=1}^m r_j\big(\sum_{i=0}^m \pi_i(e_j)\big) = 0$). Since $|r_j| < \varepsilon$ for $j = 1, \dots, m$, we have

$$|s_i| \leq \sum_{j=1}^m |r_j|\,|\pi_i(e_j)| < \sum_{j=1}^m \varepsilon|\pi_i(e_j)| < m \cdot q_i/m = q_i,$$

hence $q_i + s_i > 0$. It is $\sum_{i=0}^m (q_i + s_i) = 1 + 0 = 1$ and finally

$$a + b = \sum_{i=0}^m q_ia_i + \sum_{i=0}^m s_ia_i = \sum_{i=0}^m (q_i + s_i)a_i \in \operatorname{conv}(\{a_0, \dots, a_m\}).$$

Thus we have $B(a, \varepsilon) \subseteq \operatorname{conv}(\{a_0, \dots, a_m\})$ and $a \in \operatorname{int}(\operatorname{conv}(\{a_0, \dots, a_m\}))$. ∎

1.14 Corollary. *Let $A \subseteq (\mathbb{T}_0^+)^m$ be a cone containing m linearly independent points $a_1, \dots, a_m$. Then $B = \operatorname{int}(A) \cup \{0\} \supsetneq \{0\}$ is a cone with $\partial B = \{0\}$.*

Proof. We have $\emptyset \neq \big\{\sum_{i=1}^m q_ia_i \mid q_i \in \mathbb{T}^+, \sum_{i=1}^m q_i = 1\big\} \subseteq \operatorname{int}(A)$ by the proposition above. The rest follows from Lemma 1.12. ∎

In what follows, $\langle \cdot, \cdot \rangle$ denotes the inner product on $\mathbb{T}^m$. A linear subspace V of $\mathbb{T}^m$ of dimension $m-1$ is called a *vector hyperplane*, a set in the form $a + V$, where $a \in \mathbb{T}^m$, is called *an (affine) hyperplane*. It is well-known that vector hyperplanes are zero sets of non-trivial linear functionals and that a set $H \subseteq \mathbb{T}^m$ is a hyperplane if and only if there exist a nonzero vector $w \in \mathbb{T}^m$ and $\mu \in \mathbb{T}$ such that $H = \{x \in \mathbb{T}^m \mid \langle w, x\rangle = \mu\}$.

Let $H = \{\langle w, x\rangle = \mu\}$, where $0 \neq w \in \mathbb{T}^m$ and $\mu \in \mathbb{T}$, be a hyperplane. The sets $H_0^+ = \{\langle w, x\rangle \geq \mu\}$ and $H_0^- = \{\langle w, x\rangle \leq \mu\}$ are called the *closed half-spaces* and the sets $H^+ = \{\langle w, x\rangle > \mu\}$ and $H^- = \{\langle w, x\rangle < \mu\}$ are called the *open half-spaces*, the set H is called the *determining hyperplane* in this context. By a *half-space* we always mean a closed half-space.

1.15 Lemma. *Closed half-spaces are closed sets and open half-spaces are open sets. A determining hyperplane is a boundary of a closed resp. open half-space, hence it is a closed set.*

Proof. Let $H = \{\langle w, x\rangle = \mu\}$, H_0^+, H_0^- and H^+, H^- be as above. Since $H_0^- = \mathbb{T}^m \setminus H^+$, it suffices to prove that H^+ is an open set. Without loss of generality we may assume that $\mu = 0$. Take an $x \in H^+$ ($\langle w, x\rangle > 0$) and define $\varepsilon = \langle w, x\rangle / \|w\| \in \mathbb{R}^+$. Let $b \in \mathbb{T}^m$ be such that $\|b\| < \varepsilon$. We have $\langle w, x+b\rangle = \langle w, x\rangle + \langle w, b\rangle$ and $|\langle w, b\rangle| \leq \|w\| \cdot \|b\| < \langle w, x\rangle$ (this is *not* the Cauchy-Schwarz inequality), thus $\langle w, x+b\rangle > 0$ and $x + b \in H^+$. The statement concerning a determining hyperplane is obvious. ∎

We order $\mathbb{T}^m$ by setting $a \leq b$ if and only if $b - a \in (\mathbb{T}_0^+)^m$ (and we write $a < b$ if $a \leq b$ and $a \neq b$). This order is stable both under addition and under multiplication by non-negative scalar $q \in \mathbb{T}_0^+$.

We say that a cone A is *polyhedral* if $A = \{x \in \mathbb{T}^m \mid Wx^{\mathrm{T}} \leq 0\}$ for some matrix $W \in \mathbb{T}^{n \times m}$ (it should be clear that such set is a *non-empty* cone; A is considered to be $\mathbb{T}^m$ in the case $n = 0$). Let $w_1, \dots, w_n \in \mathbb{T}^m$ be the row vectors of W. Then $\langle w_i, x\rangle \leq 0$ for all $x \in A$ and $i = 1, \dots, n$, hence

$$A = \bigcap_{i=1}^{n} \{x \in \mathbb{T}^m \mid \langle w_i, x\rangle \leq 0\}$$

and a cone is polyhedral if and only if it is the intersection of a finite system of half-spaces in the form $\{\langle w, x\rangle \leq 0\}$, $0 \neq w \in \mathbb{T}^m$. It follows that the intersection of a finite system of polyhedral cones is a polyhedral cone.

Note that a vector hyperplane $H = \{\langle w, x\rangle = 0\}$ is a polyhedral cone $\{\langle w, x\rangle \leq 0\} \cap \{\langle -w, x\rangle \leq 0\}$. Thus every proper linear subspace of $\mathbb{T}^m$ is a polyhedral cone, since it is the intersection of a finite number of vector hyperplanes.

The following famous lemma says that if $b \in \mathbb{T}^m$ do not lie within a cone generated by points $a_1, \dots, a_n$, then there exists a hyperplane "separating" the cone and the point b.

1.16 Lemma (Fundamental theorem of linear inequalities)**.**
Let $a_1, \dots, a_n$, $n \in \mathbb{N}$, and b be elements of $\mathbb{T}^m$ and let d be the dimension of the linear hull of $\{a_1, \dots, a_n, b\}$. Then

(i) *either $b \in \operatorname{cone}(\{a_1, \dots, a_n\})$,*

(ii) *or there exists a hyperplane* $\{x \in \mathbb{T}^m \mid \langle w, x\rangle = 0\}$, $0 \neq w \in \mathbb{T}^m$, *containing* $d-1$ *linearly independent vectors from* $\{a_1, \ldots, a_n\}$ *such that* $\langle w, b\rangle < 0$ *and* $\langle w, a_i\rangle \geq 0$ *for* $i = 1, \ldots, n$.

Proof. Note that (i) and (ii) can not be both true, otherwise we would have $b = \sum_{\ell=1}^{n} q_\ell a_\ell$ for some $q_\ell \in \mathbb{T}_0^+$ and $0 > \langle w, b\rangle = \sum_{\ell=1}^{n} q_\ell \langle w, a_\ell\rangle \geq 0$. We first assume that $a_1, \ldots, a_n$ span $\mathbb{T}^m$. Let $D = \{a_{i_1}, \ldots, a_{i_m}\} \subseteq \{a_1, \ldots, a_n\}$ be a set of linearly independent vectors. Consider the following iterative algorithm:

Algorithm.

(I) Find $q_{i_1}, \ldots, q_{i_m} \in \mathbb{T}$ such that $b = \sum_{k=1}^{m} q_{i_k} a_{i_k}$. If all q_{i_k}'s are non-negative, we are in case (i) and the algorithm terminates.

(II) Let $j = \min\{i_k \mid k \in \{1, \ldots, m\},\ q_{i_k} < 0\}$ and let $w \in \mathbb{T}$, $w \neq 0$, be such that $\mathrm{Lin}(D \setminus \{a_j\})$ is the half-space $\{\langle w, x\rangle = 0\}$ and $\langle w, a_j\rangle = 1$. It follows that $\langle w, b\rangle = \langle w, q_j a_j\rangle = q_j < 0$.

(III) If $\langle w, a_\ell\rangle \geq 0$ for all $\ell \in \{1, \ldots, n\}$, we are in case (ii) and the algorithm terminates.

(IV) Let $j' = \min\{\ell \in \{1, \ldots, n\} \mid \langle w, a_\ell\rangle < 0\}$. Replace a_j by $a_{j'}$ in D (i.e. $D \leftarrow (D \setminus \{a_j\}) \cup \{a'_j\}$) and go to step (I).

Suppose, contrary to our claim, that the algorithm does not terminate. In what follows, we use Greek letters to indicate the steps and the variable values in the ζ-th iteration, $\zeta \in \mathbb{N}$. Since there are only finitely many possible choices for D, one must have $D_\alpha = D_\beta$ for some $\alpha < \beta$. Let $r \in \{1, \ldots, n\}$ be the highest index for which a_r has been removed at step (IV) from one of the sets $D_\alpha, D_{\alpha+1}, \ldots, D_\beta$, say from D_γ (i.e. $r = j_\gamma$). Since $D_\alpha = D_\beta$, there exists a δ between α and β such that a_r was added to D_δ in step $(\mathrm{IV})_\delta$ (i.e. $r = j'_\delta$). Hence

$$(*) \qquad D_\gamma \cap \{a_{r+1}, \ldots, a_n\} = D_\delta \cap \{a_{r+1}, \ldots, a_n\}$$

Let $D_\gamma = \{a_{i_1}, \ldots, a_{i_m}\}$ and let $q_{i_k} \in \mathbb{T}$ be such that $b = \sum_{k=1}^{m} q_{i_k} a_{i_k}$ (as in $(\mathrm{I})_\gamma$). For every $k \in \{1, \ldots, m\}$ it is:

$$\left.\begin{array}{l} \text{if } i_k < r, \text{ then } q_{i_k} \geq 0 \text{ by } (\mathrm{II})_\gamma \text{ and } \langle w_\delta, a_{i_k}\rangle \geq 0 \text{ by } (\mathrm{IV})_\delta \\ \text{if } i_k = r, \text{ then } q_{i_k} < 0 \text{ by } (\mathrm{II})_\gamma \text{ and } \langle w_\delta, a_{i_k}\rangle < 0 \text{ by } (\mathrm{IV})_\delta \\ \text{if } i_k > r, \text{ then } \langle w_\delta, a_{i_k}\rangle = 0 \text{ by } (*) \text{ and } (\mathrm{II})_\gamma \end{array}\right\} \ q_{i_k}\langle w_\delta, a_{i_k}\rangle \geq 0.$$

Consequently, we have

$$\langle w_\delta, b\rangle = \sum_{k=1}^{m} \langle w_\delta, q_{i_k} a_{i_k}\rangle = \sum_{k=1}^{m} q_{i_k} \langle w_\delta, a_{i_k}\rangle \geq 0,$$

a contradiction with $(\mathrm{II})_\delta$.

If the points $a_1, \ldots, a_n$ do not span $\mathbb{T}^m$ and $b \notin \mathrm{cone}(\{a_1, \ldots, a_n\})$, then we can find linearly independent vectors $a'_1, \ldots, a'_k \in \mathbb{T}^m$ such that $b \notin \mathrm{cone}(\{a_1, \ldots, a_n, a'_1, \ldots, a'_k\})$, $\mathrm{Lin}(\{a_1, \ldots, a_n\}) \cap \mathrm{Lin}(\{a'_1, \ldots, a'_k\}) = \{0\}$ and the points $a_1, \ldots, a_n, a'_1, \ldots, a'_k$ span $\mathbb{T}^m$. Applying the previous part gives an appropriate half-space. ∎

The lemma above allows us to prove the following aesthetically pleasing theorem, which is geometrically evident in dimension 3.

1.17 Theorem (Weyl-Minkowski)**.** *Let $A \subseteq \mathbb{T}^m$ be a non-empty cone. Then A is finitely generated if and only if it is polyhedral.*

Proof. If $A = \mathbb{T}^m$, then A is both polyhedral and finitely generated, since it is the intersection of the empty system of half-spaces and $A = \operatorname{cone}(\{\pm e_1, \ldots, \pm e_m\})$, where $\{e_1, \ldots, e_m\}$ is the canonical basis of $\mathbb{T}^m$. Thus we may assume $A \subsetneq \mathbb{T}^m$.

We first prove the direct implication. Let $a_1, \ldots, a_n \in \mathbb{T}^m$ be such that $A = \operatorname{cone}(\{a_1, \ldots, a_n\})$. We shall show that A is polyhedral. First assume that $a_1, \ldots, a_n$ span $\mathbb{T}^m$ and consider the finite system $\mathcal{H}$ of all half-spaces $H_0^- = \{\langle w, x\rangle \leq 0\}$ such that $a_1, \ldots, a_n \in H_0^-$ and $H = \{\langle w, x\rangle = 0\}$ is spanned by $m-1$ linearly independent vectors from $\{a_1, \ldots, a_n\}$. Lemma 1.16 gives $(b \in \mathbb{T}^m \setminus A) \Rightarrow ((\exists H_0^- \in \mathcal{H})(b \notin H_0^-))$, equivalently $((\forall H_0^- \in \mathcal{H})(b \in H_0^-)) \Rightarrow (b \in A)$. In other words, $A \supseteq \bigcap \mathcal{H}$. Since $A \subseteq H_0^-$ for all $H_0^- \in \mathcal{H}$, we also have $A \subseteq \bigcap \mathcal{H}$. It follows that $A = \bigcap \mathcal{H}$ and A is a polyhedral cone.

If the points $a_1, \ldots, a_n$ do not span $\mathbb{T}^m$, we can find linearly independent vectors $a'_1, \ldots, a'_k \in \mathbb{T}^m$ such that $\operatorname{Lin}(\{a_1, \ldots, a_n\}) \cap \operatorname{Lin}(\{a'_1, \ldots, a'_k\}) = \{0\}$ and $a_1, \ldots, a_n$, $a'_1, \ldots, a'_k$ span $\mathbb{T}^m$. The cone generated by points $a_1, \ldots, a_n$ and $a'_1, \ldots, a'_k$ is polyhedral by the previous part and its intersection with $\operatorname{Lin}(\{a_1, \ldots, a_n\})$ is exactly A. Again, the cone A is polyhedral.

Now assume that A is a polyhedral cone given as the intersection of n half-spaces $\{\langle w_i, x\rangle \leq 0\}$, where $0 \neq w_i \in \mathbb{T}^m$ for $i = 1, \ldots, n$. We have proved above that the cone generated by $w_1, \ldots, w_n$ is polyhedral. Let $b_1, \ldots, b_p \in \mathbb{T}^m$ be such that $\operatorname{cone}(\{w_1, \ldots, w_n\}) = \{x \in \mathbb{T}^m \mid \langle b_1, x\rangle \leq 0, \ldots, \langle b_p, x\rangle \leq 0\}$ and let B be the cone generated by $b_1, \ldots, b_p$. The proof is completed by showing that $A = B$. Take an arbitrary $b = \sum_{j=1}^p q_j b_j \in B$, where $q_j \in \mathbb{T}_0^+$, and an $i \in \{1, \ldots, n\}$. We have $\langle w_i, b\rangle = \sum_{j=1}^p q_j \langle w_i, b_j\rangle \leq 0$, since $\langle w_i, b_j\rangle \leq 0$ for all $i = 1, \ldots, n$ and $j = 1, \ldots, p$ (so were taken $b_1, \ldots, b_p$). Thus $B \subseteq A$. On the contrary, assume that there exists a point $a \in A \setminus B$. Then there exists by Lemma 1.16 a nonzero $w \in \mathbb{T}^m$ such that $\langle w, b_j\rangle \leq 0$ for $j = 1, \ldots, p$ and $\langle w, a\rangle > 0$. We have $w \in \operatorname{cone}(\{w_1, \ldots, w_n\})$, hence $w = \sum_{i=1}^n r_i w_i$, where $r_i \in \mathbb{T}_0^+$. Consequently, $\langle w, a\rangle = \sum_{i=1}^n r_i \langle w_i, a\rangle \leq 0$, a contradiction with the choice of w. ∎

1.18 Corollary. *If A is a finitely generated cone, then A is a closed set. The intersection of a finite system of finitely generated cones is a finitely generated cone.*

Proof. We may assume $\emptyset \neq A \subsetneq \mathbb{T}^m$. The cone A is the intersection of a finite number of half-spaces, each of them is closed and therefore A is closed. The rest is clear. ∎

1.19 Proposition. *Let V be a linear subspace of $\mathbb{T}^m$. Then $V \cap (\mathbb{T}_0^+)^m$ is a finitely generated cone.*

Proof. The set $(\mathbb{T}_0^+)^m$ is the cone generated by the canonical basis of $\mathbb{T}^m$, hence both V and $(\mathbb{T}_0^+)^m$ are polyhedral cones. The rest follows from Corollary 1.18. ∎

1.20 Proposition. *Let $m \geq 2$ and let $A \subseteq \mathbb{T}^m$ be a finitely generated cone. Let $\ell = \{a + tv \mid t \in \mathbb{T}\}$, $a, v \in \mathbb{T}^m$, $v \neq 0$, be a line in $\mathbb{T}^m$. Then there are $t_1, t_2 \in \mathbb{T} \cup \{-\infty, \infty\}$ such that $\ell \cap A = \{a + tv \mid t \in \mathbb{T}, t_1 \leq t \leq t_2\}$.*

Proof. If H_0^- is an arbitrary half-space, then either $\ell \subseteq H_0^-$ and $\ell \cap H_0^- = \{a+tv \mid t \in \mathbb{T}\}$ or there is a $t_1 \in \mathbb{T}$ such that either $\ell \cap H_0^- = \{a+tv \mid t \in \mathbb{T},\, t_1 \le t\}$ or $\ell \cap H_0^- = \{a+tv \mid t \in \mathbb{T},\, t \le t_1\}$. We have $A = \bigcap \mathcal{H}$ for a suitable finite system $\mathcal{H}$ of half-spaces. Our claim then follows directly from the equality $\ell \cap A = \bigcap\{\ell \cap H_0^- \mid H_0^- \in \mathcal{H}\}$. ∎

1.21 Proposition. *Let $m \ge 2$. If $A \subseteq (\mathbb{T}_0^+)^m$ is a finitely generated cone, then ∂A generates A. If $B \subseteq (\mathbb{T}_0^+)^m$, $B \supsetneq \{0\}$, is a cone with $\partial B = \{0\}$, then B is not finitely generated (cf. Corollary 1.14).*

Proof. We may suppose that $\mathrm{int}(A) \neq \emptyset$, otherwise the statement is trivial. Take an $a \in \mathrm{int}(A)$ and consider the line $\ell = \{\gamma(t) \mid t \in \mathbb{T}\}$, where $\gamma(t) = a + t(1,-1,0,\dots,0)$ ($m-2$ zeros), $t \in \mathbb{T}$. The set $I = \{t \in \mathbb{T} \mid \gamma(t) \in A\} \subseteq \mathbb{T}$ is bounded, since $\ell \cap (\mathbb{T}_0^+)^m$ is so, hence $I = \{t \in \mathbb{T} \mid t_1 \le t \le t_2\}$ for some $t_1, t_2 \in \mathbb{T}$, $t_1 < 0 < t_2$ (see the previous proposition); obviously the points $\gamma(t_1)$ and $\gamma(t_2)$ lie at the boundary of A and $a = \gamma(0)$ is a convex combination of $\gamma(t_1)$ and $\gamma(t_2)$. It follows that $\mathrm{int}(A) \subseteq \mathrm{conv}(\partial A) \subseteq \mathrm{cone}(\partial A)$. ∎

1.22 Proposition. *Let $a_1, \dots, a_m \in (\mathbb{T}_0^+)^m$ be linearly independent. Then the number of integer points in $P = \big\{\sum_{i=1}^m q_i a_i \mid q_i \in \mathbb{T}_0^+,\, q_i < 1\big\}$ is equal to $|\det(a_1,\dots,a_m)|$.*

Sketch of proof. We can assume $\mathbb{T} = \mathbb{R}$ (see Note 1.10). Define $A = \{a_1, \dots, a_m\}$. The sets $\big\{\sum_{i=1}^m k_i a_i + P \mid k_i \in \mathbb{N}_0\big\}$ form a partition of the set $(\mathbb{R}_0^+)^m$. Take an $n \in \mathbb{N}$ (and think of n as a "large" number). The number of integer points in $\{0,1,\dots,n\}^m$ is $(n+1)^m = n^m + o(n^{m-1})$ and equals

$$\big(\mathrm{vol}([0,n]^m)/\mathrm{vol}(P)\big) \cdot |P \cap \mathbb{N}_0^m| + o(n^{m-1}) = \\ = \big(n^m/|\det(a_1,\dots,a_m)|\big) \cdot |P \cap \mathbb{N}_0^m| + o(n^{m-1}).$$

Thus $|P \cap \mathbb{N}_0^m|/|\det(a_1,\dots,a_m)| = 1 + o(n^{-1})$ and the statement follows. ∎

1.23 Convention. In the following chapters we will use all defined notions as if they were defined for $\mathbb{T} = \mathbb{Q}$.

2. Subsemigroups of $\mathbb{N}_0^m$

We recall that a *semigroup* is a universal algebra with one binary operation, which is associative. All semigroups mentioned in this thesis are treated as subsemigroups of $(\mathbb{Q}^m, +)$, the *additive semigroup* of the vector space $\mathbb{Q}^m$.

2.1 Definition. Let B be a non-empty subset of $\mathbb{Q}^m$. We define $\mathrm{Sg}(B)$ to be the smallest subsemigroup of $\mathbb{Q}^m$ containing B (the intersection of all semigroups containing B), evidentally

$$\mathrm{Sg}(B) = \Big\{ \sum_{i=1}^{n} k_i b_i \;\Big|\; n \in \mathbb{N},\, k_i \in \mathbb{N} \text{ and } b_i \in B \text{ for } i = 1, \ldots, n \Big\}.$$

Let A be a subsemigroup of $\mathbb{Q}^m$. A non-empty set $B \subseteq A$ is a *generating set of* A if $\mathrm{Sg}(B) = A$ and A is *finitely generated* if there is a finite generating set of A.

2.2 Lemma. *Let A be a subsemigroup of $\mathbb{Q}^m$ generated by a non-empty set $B \subseteq \mathbb{Q}^m$. Then* $\mathrm{cone}(A) = \mathrm{cone}(B)$.

Proof. Since $B \subseteq A$, we have $\mathrm{cone}(B) \subseteq \mathrm{cone}(A)$. On the other hand, $\mathrm{cone}(B)$ is a subsemigroup of $\mathbb{Q}^m$ containing A. Therefore $\mathrm{cone}(A) \subseteq \mathrm{cone}(\mathrm{cone}(B)) = \mathrm{cone}(B)$. ∎

2.3 Lemma. *Let A be a subsemigroup of $\mathbb{Q}^m$. Then*

(i) *for every $a \in \mathrm{cone}(A)$, $a \neq 0$, there is a $k \in \mathbb{N}$ such that $ka \in A$;*

(ii) *either $0 \notin A$ and $\mathrm{cone}(A) = \{0\} \cup \bigcup_{k \in \mathbb{N}} A/k$ or $0 \in A$ and $\mathrm{cone}(A) = \bigcup_{k \in \mathbb{N}} A/k$;*

(iii) $\mathrm{cone}(A) = \{0\} \cup \bigcup_{k \in \mathbb{N}} \mathrm{conv}(A)/k$.

Proof. Let a be an arbitrary element of $\mathrm{cone}(A)$, i.e. $a = \sum_{i=1}^{n} q_i a_i$, $q_i \in \mathbb{Q}_0^+$, $a_i \in A$. Find $k \in \mathbb{N}$ such that all rational numbers kq_i are integers. Then $ka = \sum_{i=1}^{n} kq_i a_i \in A$. Parts (ii) and (iii) follow immediately from (i). ∎

2.4 Proposition. *Let A be a subsemigroup of $\mathbb{N}_0^m$. Then A possesses the smallest generating set (with respect to inclusion); it is the set*

$$B = \{ b \in A \mid b \neq c + d \textit{ for all nonzero } c, d \in A \}.$$

Proof. It is easily seen that B is a subset of every generating set. To prove $\mathrm{Sg}(B) = A$, we proceed by induction on $\|\cdot\|$. If $a \in A$ is such that $\|a\| = 0$, then $a = 0 \in B \subseteq A$. Assume that all elements of A with $\|\cdot\|$ smaller then $k \geq 1$ lie within $\mathrm{Sg}(B)$ and take an arbitrary $a \in A$ with $\|a\| = k$ (if exists). Either $a \in B$ or a can be written as $c + d$, where $c, d \in A$ are both nonzero. In the latter case we have $\|c\| < \|a\|$ and $\|d\| < \|a\|$, which implies $c, d \in \mathrm{Sg}(B)$ and consequently $a \in \mathrm{Sg}(B)$. ∎

We shall refer to the smallest generating set of A described in the previous proposition as *the (Hilbert) basis of* A and we shall denote it by $\mathrm{Hb}(A)$. Note that the semigroup $\mathbb{Q}_0^+$ does not possess any smallest generating set since $\mathbb{Q}_0^+ = \mathrm{Sg}(\{q \in \mathbb{Q}_0^+ \mid q \leq r\})$ for every $r \in \mathbb{Q}^+$. The following lemma is an immediate consequence of the previous proposition.

2.5 Lemma. *Let* A *and* $B \supseteq A$ *be subsemigroups of* $\mathbb{N}_0^m$. *Then*

(i) $0 \in \mathrm{Hb}(A)$ *if and only if* $0 \in A$;

(ii) *if* $a \in A \cap \mathrm{Hb}(B)$, *then* $a \in \mathrm{Hb}(A)$ *(equivalently* $A \cap \mathrm{Hb}(B) \subseteq \mathrm{Hb}(A)$*).*

2.6 Lemma. *Let* A *be a subsemigroup of* $\mathbb{N}_0^p$ *and* B *be a subsemigroup of* $\mathbb{N}_0^q$, *where* $p, q \in \mathbb{N}$. *Then* $A \times B$ *is a subsemigroup of* $\mathbb{N}_0^{p+q}$ *and*

if $0 \notin A$ *and* $0 \notin B$, *then* $\mathrm{Hb}(A \times B) = (\mathrm{Hb}(A) \times B) \cup (A \times \mathrm{Hb}(B))$;
if $0 \in A$ *and* $0 \notin B$, *then* $\mathrm{Hb}(A \times B) = A \times \mathrm{Hb}(B)$;
if $0 \notin A$ *and* $0 \in B$, *then* $\mathrm{Hb}(A \times B) = \mathrm{Hb}(A) \times B$;
if $0 = 0_A \in A$ *and* $0 = 0_B \in B$, *then* $\mathrm{Hb}(A \times B) = (\{0_A\} \times \mathrm{Hb}(B)) \cup (\mathrm{Hb}(A) \times \{0_B\})$.

Proof. Clearly $A \times B$ is a subsemigroup of $\mathbb{N}_0^{p+q}$. Here we give the proof only for the first, possibly the least obvious case $0 \notin A$ and $0 \notin B$. The inclusion $\mathrm{Hb}(A \times B) \supseteq (\mathrm{Hb}(A) \times B) \cup (A \times \mathrm{Hb}(B))$ follows from the description given in Proposition 2.4. To prove the converse inclusion, assume that $(a, b) \in \mathrm{Hb}(A \times B)$ and $(a, b) \notin A \times \mathrm{Hb}(B)$, which means that $b = b_1 + b_2$ for some $b_1, b_2 \in B$. But this implies $a \neq a_1 + a_2$ for *all* $a_1, a_2 \in A$, for otherwise we would have $(a_1, b_1) + (a_2, b_2) = (a, b)$, a contradiction with $(a, b) \in \mathrm{Hb}(A \times B)$. Thus $a \in \mathrm{Hb}(A)$. In the same manner we see that $(a, b) \in \mathrm{Hb}(A \times B) \setminus (\mathrm{Hb}(A) \times B)$ implies $(a, b) \in A \times \mathrm{Hb}(B)$. ∎

2.7 Definition. Let A be a subsemigroup of $\mathbb{N}_0^m$. We denote by $\mathcal{E}(A)$ the set of all elements $a \in A$ such that $b - a \in A$ whenever $b \in A$ and $b - a \in \mathbb{N}_0^m$. It is easily verified that

$$\mathcal{E}(A) = \{a \in A \mid A = \mathbb{N}_0^m \cap (A - a)\} = \{a \in A \mid A + a = (\mathbb{N}_0^m + a) \cap A\}.$$

2.8 Lemma. *Let* A *be a subsemigroup of* $\mathbb{N}_0^m$. *Then* $0 \in A \Leftrightarrow 0 \in \mathcal{E}(A) \Leftrightarrow \mathcal{E}(A) \neq \emptyset$. *Either* $0 \notin A$ *and* $\mathcal{E}(A) = \emptyset$ *or* $0 \in \mathcal{E}(A) \subseteq A$ *and* $\mathcal{E}(A)$ *is a subsemigroup of* A.

Proof. Implications $0 \in A \Rightarrow 0 \in \mathcal{E}(A) \Rightarrow \mathcal{E}(A) \neq \emptyset$ are trivial. If $a \in \mathcal{E}(A)$, then by the definition of $\mathcal{E}(A)$ we have $a - a = 0 \in A$. If $\mathcal{E}(A)$ is non-empty and $a, b \in \mathcal{E}(A)$, then $A + (a + b) = (A + a) + b = ((\mathbb{N}_0^m + a) \cap A) + b = (\mathbb{N}_0^m + a + b) \cap (A + b) = (\mathbb{N}_0^m + a + b) \cap (\mathbb{N}_0^m + b) \cap A = (\mathbb{N}_0^m + a + b) \cap A$. Consequently, $a + b \in \mathcal{E}(A)$ and $\mathcal{E}(A)$ is a subsemigroup of A. ∎

2.9 Lemma. *Let* A *be a subsemigroup of* $\mathbb{N}_0^m$ *containing* 0. *Then*

(i) *if* $a, b \in \mathcal{E}(A)$ *are such that* $b - a \in \mathbb{N}_0^m$, *then* $b - a \in \mathcal{E}(A)$;

(ii) $(\mathcal{E}(A) - \mathcal{E}(A)) \cap \mathbb{N}_0^m = \mathcal{E}(A)$;

(iii) $\mathcal{E}(\mathcal{E}(A)) = \mathcal{E}(A)$;

(iv) $\mathrm{Hb}(\mathcal{E}(A)) = \mathrm{Hb}(A) \cap \mathcal{E}(A)$.

Proof. (i) For $a, b \in \mathcal{E}(A)$, $b - a \in \mathbb{N}_0^m$, we have $A + (b - a) = (A + b) - a = (\mathbb{N}_0^m + b - a) \cap (A - a) = (\mathbb{N}_0^m + b - a) \cap ((A - a) \cap \mathbb{N}_0^m) = (\mathbb{N}_0^m + b - a) \cap A$, hence $b - a \in \mathcal{E}(A)$. Assertions (ii) and (iii) follow immediately from (i). Now we prove (iv). Suppose, contrary to $\mathrm{Hb}(\mathcal{E}(A)) \subseteq \mathrm{Hb}(A)$, that there is an $a \in \mathrm{Hb}(\mathcal{E}(A)) \setminus \mathrm{Hb}(A)$. It is $a = c + d$ for some nonzero $c, d \in A$. If $b \in A$ and $b - (a - c) \in \mathbb{N}_0^m$, then $b - (a - c) = (b + c) - a \in A$, since $b+c \in A$, hence $d = a-c \in \mathcal{E}(A)$. Part (i) gives $c = a-d \in \mathcal{E}(A)$, a contradiction with $a = c+d \in \mathrm{Hb}(\mathcal{E}(A))$. The inclusion $\mathrm{Hb}(\mathcal{E}(A)) \supseteq \mathrm{Hb}(A) \cap \mathcal{E}(A)$ follows from Lemma 2.5(ii). ∎

2.10 Lemma. *Let A and B be as in Lemma 2.6. Then $\mathcal{E}(A \times B) = \mathcal{E}(A) \times \mathcal{E}(B)$.*

Proof. We may assume that $0 \notin A$ and $0 \notin B$; since otherwise the statement is trivial (Lemma 2.8). It is obvious that $\mathcal{E}(A) \times \mathcal{E}(B) \subseteq \mathcal{E}(A \times B)$. Take an arbitrary $(a, b) \in \mathcal{E}(A \times B)$. We have $(c, b) - (a, b) = (c - a, 0) \in A \times B$ whenever $c \in A$ and $c - a \in \mathbb{N}_0^p$, hence $a \in \mathcal{E}(A)$. Similarly $b \in \mathcal{E}(B)$ and consequently $(a, b) \in \mathcal{E}(A) \times \mathcal{E}(b)$. ∎

2.11 Order of $\mathbb{N}_0^m$. The order $\leq$ of $\mathbb{Q}^m$ (defined at page 8) induces in natural way an order of $\mathbb{N}_0^m$ (i.e. if $a, b \in \mathbb{N}_0^m$, then $a \leq b$ if and only if $b - a \in \mathbb{N}_0^m$). Clearly there are infinite ascending chains and no descending ones in $(\mathbb{N}_0^m, \leq)$; the set $\{b \in \mathbb{N}_0^m \mid b \leq a\}$ is finite for every $a \in \mathbb{N}_0^m$. For $m \geq 2$ there is no finite upper bound of antichain cardinality, since for $m = 2$ and $n \in \mathbb{N}_0$ the set $A_2 = \{(0, n), (1, n-1), \ldots, (n, 0)\}$ is an antichain in $\mathbb{N}_0^2$, for $m > 2$ the set $A_2 \times \{(0, 0, \ldots, 0)\}$ ($m - 2$ zeros) is an antichain in $\mathbb{N}_0^m$. However, the following theorem asserts there are only finite antichains.

2.12 Theorem. *There is no infinite set of pairwise incomparable m-tuples in $\mathbb{N}_0^m$.*

Proof. We proceed by induction on m. In the set $\mathbb{N}_0$ there are no incomparable elements. Assume the statement is true for all positive integers $\leq m$ and let A be a set of pairwise incomparable elements of $\mathbb{N}_0^{m+1}$. For every $k \in \mathbb{N}_0$ put

$$B_k = \{b \in \mathbb{N}_0^m \mid \text{there exists an } a \in A \text{ such that } a \leq (b, k)\}.$$

Clearly $B_0 \subseteq B_1 \subseteq B_2 \subseteq \cdots$ and all B_k's are upper sets in $(\mathbb{N}_0^m, \leq)$; the set $B = \bigcup_{k<\omega} B_k$ is then also an upper set. Denote by C_k resp. C the set of all minimal elements of B_k resp. B; the sets C_k, $k \in \mathbb{N}$, and C are antichains in $\mathbb{N}_0^m$ and therefore finite by induction assumption. Thus there is a $k_0 \in \mathbb{N}_0$ such that $C \subseteq B_{k_0}$ and consequently $B_{k_0} = B_{k_0+1} = \cdots = B$ and $C_{k_0} = C_{k_0+1} = \cdots = C$. For every $a = (b_1, k_1) \in A$, $b_1 \in \mathbb{N}_0^m$, $k_1 \in \mathbb{N}_0$, we have $b_1 \in B_{k_1} \subseteq B = B_{k_0}$, hence $a_1 \leq (b_1, k_0)$ for some $a_1 \in A$. If $k_0 \leq k_1$, then $a_1 \leq a$, thus $a_1 = a$ (A is an antichain) and $k_0 = k_1$. Thus we have $k_1 \leq k_0$ anyway. Since $b_1 \in B_{k_1}$, there is a $c_1 \in C_{k_1}$ with $c_1 \leq b_1$ and $(c_1, k_1) \leq a$. By the definition of B_{k_1} we can find $a' \in A$ such that $a' \leq (c_1, k_1) \leq a = (b_1, k_1)$. Hence $a' = a$ and $b_1 = c_1$.

Recapitulate what we have just shown: for arbitrarily chosen $a = (b_1, k_1) \in A$ we have got $a = (c_1, k_1)$, where $k_1 \leq k_0$ and c_1 is a minimal element of B_{k_1}. Therefore $A \subseteq \bigcup_{k<\omega}(C_k \times \{0, \ldots, k_0\}) = \bigcup_{k \leq k_0}(C_k \times \{0, \ldots, k_0\})$, which is a finite set. ∎

2.13 Corollary. *If A is an upper set in $\mathbb{N}_0^m$, then there are $a_1, \ldots, a_n \in A$, $n \in \mathbb{N}_0$, such that $A = \bigcup_{i=1}^n \{a \in \mathbb{N}_0^m \mid a \geq a_n\}$.*

Proof. The set of all minimal elements of A is an antichain in $\mathbb{N}_0^m$, thus finite. ∎

2.14 Proposition. *Let A_1 be a non-empty finite subset of $\mathbb{N}_0^m$ and A be a subsemigroup of $\mathbb{N}_0^m$ such that $A_1 \subseteq A \subseteq \mathrm{cone}(A_1)$. Then A is a finitely generated semigroup.*

Proof. Let

$$A_1 = \{a_1, \ldots, a_n\},\ n \in \mathbb{N}, \quad \text{and} \quad B = \Big\{\sum_{i=1}^{n} q_i a_i \ \Big|\ q_i \in \mathbb{Q}_0^+,\ q_i < 1\Big\} \cap \mathbb{N}_0^m.$$

We have $A_1 \subseteq A \subseteq \operatorname{cone}(A_1) \cap \mathbb{N}_0^m$ and obviously B is finite. Let a be an arbitrary element of A. Then $a = \sum_{i=1}^{n} r_i a_i$, where $r_i = \ell_i + s_i \in \mathbb{Q}_0^+$, $\ell_i \in \mathbb{N}_0$ and $s_i \in \mathbb{Q}_0^+$, $s_i < 1$. Let $b_1 = \sum_{i=1}^{n} s_i a_i$. We have $a = b_1 + \sum_{i=1}^{n} \ell_i a_i$, where $b_1 \in B$ and $(\ell_1, \ldots, \ell_n) \in \mathbb{N}_0^m$. For every $b \in B$ set

$$N_b = \Big\{(k_1, \ldots, k_n) \in \mathbb{N}_0^n \ \Big|\ b + \sum_{i=1}^{n} k_i a_i \in A\Big\}.$$

The set N_b is an upper set; denote by M_b the set of all its minimal elements. By Theorem 2.12, the set M_b is finite and therefore $\bigcup_{b \in B} M_b$ is finite. Moreover, every $a \in A$ can be expressed as $a = b + \sum_{i=1}^{n} k_i a_i + \sum_{i=1}^{n} k_i' a_i$, where $b \in B$, $(k_1, \ldots, k_n) \in M_b$ and $(k_1', \ldots, k_n') \in \mathbb{N}_0^n$. Hence A is generated by

$$\{a_1, \ldots, a_n\} \cup \bigcup_{b \in B} \Big\{b + \sum_{i=1}^{n} k_i a_i \ \Big|\ (k_1, \ldots, k_n) \in M_b\Big\},$$

which is a finite set. ∎

2.15 Theorem. *Let A be a subsemigroup of $\mathbb{N}_0^m$. Then A is a finitely generated semigroup if and only if $\operatorname{cone}(A)$ is a finitely generated cone.*

Proof. Let $a_1, \ldots, a_n$ be generators of $\operatorname{cone}(A)$. There are $k_1, \ldots, k_n \in \mathbb{N}$ such that the set $A_1 = \{k_1 a_1, \ldots, k_n a_n\}$ is a subset of A (Lemma 2.3) and generates $\operatorname{cone}(A)$. According to the previous lemma, the semigroup A is finitely generated. Conversely, if A is generated by its finite subset B, then B also generates $\operatorname{cone}(A)$ as a cone (Lemma 2.2). ∎

2.16 Remark. Let A be a subsemigroup of $\mathbb{N}_0^m$ with $\operatorname{Hb}(A) = \{0, a_1, \ldots, a_n\}$, where $0, a_1, \ldots, a_n$ are supposed to be pairwise different. Define the equivalence $\sim$ on $\mathbb{N}_0^n$ by setting $(q_1, \ldots, q_n) \sim (r_1, \ldots, r_n)$ if and only if $\sum_{i=1}^{n} q_i a_i = \sum_{i=1}^{n} r_i a_i$. It is easily verified that the set $\mathbb{N}_0^n/\!\sim$ with the binary operation $\oplus$ defined as $[q]_\sim \oplus [r]_\sim = [q+r]_\sim$, $q, r \in \mathbb{N}_0^n$, is a semigroup isomorphic to A via the mapping $(q_1, \ldots, q_n) \mapsto \sum_{i=1}^{n} q_i a_i$. Since $q < r$ implies $[q]_\sim \neq [r]_\sim$, the elements of $\mathbb{N}_0^n/\!\sim$ are antichains in $\mathbb{N}_0^n$ and therefore finite sets (Theorem 2.12).

3. Pure subsemigroups of $\mathbb{N}_0^m$

This chapter is devoted to the study of semigroups with the property given in the following definition:

3.1 Definition. A subsemigroup A of $\mathbb{N}_0^m$ is said to be *pure* if for every $a \in \mathbb{N}_0^m$ and every $n \in \mathbb{N}$ we have $a \in A$ whenever $na \in A$.

3.2 Lemma. *Let A be a subsemigroup of $\mathbb{N}_0^m$. The following conditions are equivalent:*

- (i) *the semigroup A is pure;*
- (ii) *if $a = (a_1, \dots, a_m) \in A$, then $a/r \in A$, where $r = \gcd(a_1, \dots, a_m)$;*
- (iii) *$nA = A \cap n\mathbb{N}_0^m$ for every $n \in \mathbb{N}$;*
- (iv) *if $a \in \mathbb{N}_0^m$ and $q \in \mathbb{Q}^+$ are such that $qa \in A$, then $a \in A$;*
- (v) *if $n \in \mathbb{N}$, $a_1, \dots, a_n \in A$ and $q_1, \dots, q_n \in \mathbb{Q}^+$ are such that $a = \sum_{i=1}^n q_i a_i \in \mathbb{N}_0^m$, then $a \in A$;*
- (vi) *$A \cup \{0\} = \operatorname{cone}(A) \cap \mathbb{N}_0^m$.*

Proof. It is easy to check that the equivalences (i) $\Leftrightarrow$ (ii), (i) $\Leftrightarrow$ (iii) and (v) $\Leftrightarrow$ (vi) hold. Let us prove (i) $\Rightarrow$ (v). Let A be a pure semigroup and let $a = \sum_{i=1}^n q_i a_i \in \mathbb{N}_0^m$ be as in (v). There is an $s \in \mathbb{N}$ such that $sq_i \in \mathbb{N}$ for every $i = 1, \dots, n$. Then $sa = \sum_{i=1}^n sq_i a_i \in A$ and consequently we have $a \in A$. The implications (vi) $\Rightarrow$ (iv) and (iv) $\Rightarrow$ (i) are trivial. ∎

3.3 Lemma. *Let B be a non-empty subset of $\mathbb{N}_0^m$. Then*

$$\operatorname{Sg}^{\mathrm{P}}(B) = \Big(\bigcup_{n \in \mathbb{N}} \operatorname{Sg}(B)/n \Big) \cap \mathbb{N}_0^m$$

is the smallest pure semigroup containing B.

Proof. If the intersection of an arbitrary system of pure subsemigroups of $\mathbb{N}_0^m$ is non-empty, it is a pure subsemigroup, hence the smallest pure semigroup containing B exists; denote it by A. We have $\operatorname{Sg}(B) \subseteq A$ and $(A/n) \cap \mathbb{N}_0^m \subseteq A$ for all $n \in \mathbb{N}$, hence $\operatorname{Sg}^{\mathrm{P}}(B) \subseteq A$ and we only need to show that $\operatorname{Sg}^{\mathrm{P}}(B)$ is a pure semigroup. But it is easily verified that $\big\{\bigcup_{n\in\mathbb{N}} \operatorname{Sg}(B)/n\big\} \cup \{0\} = \operatorname{cone}(B)$, which completes the proof. ∎

3.4 Corollary. *If B is a non-empty subset of $\mathbb{N}_0^m$, then $\operatorname{cone}(\operatorname{Sg}(B)) = \operatorname{cone}(\operatorname{Sg}^{\mathrm{P}}(B))$. A subsemigroup A of $\mathbb{N}_0^m$ is finitely generated if and only if $\operatorname{Sg}^{\mathrm{P}}(A)$ is finitely generated.*

Proof. The statement follows easily from the lemma above and Theorem 2.15. ∎

3.5 Lemma. *Let A be a pure subsemigroup of $\mathbb{N}_0^m$. Then*

$$A = \bigcup \big\{ \operatorname{Sg}^{\mathrm{P}}(B) \bigm| B \subseteq A,\ |B| \le m \big\}.$$

Proof. Let $a \in A$. We have $a \in \operatorname{cone}(A)$ and Carathéodory's theorem 1.6 enables us to write $a = \sum_{i=1}^m q_i a_i$, where $q_i \in \mathbb{Q}_0^+$ and $a_i \in A$. We have $a \in \operatorname{cone}(B) \cap \mathbb{N}_0^m$ for $B = \{a_1, \dots, a_m\}$. Using Lemma 3.2(v), we obtain $a \in \operatorname{Sg}^{\mathrm{P}}(B)$. ∎

3.6 Proposition. *Let A be a pure subsemigroup of $\mathbb{N}_0^m$, B be its Hilbert basis and $C \subseteq \mathbb{N}_0^m$ be some set of generators of $\operatorname{cone}(A)$. Then*

$$B \subseteq P \cup C, \quad \text{where} \quad P = \Big\{ \sum_{i=1}^{k} q_i c_i \;\Big|\; k \in \mathbb{N}_0,\, c_i \in C,\, q_i \in \mathbb{Q}_0^+,\, q_i < 1 \Big\} \cap \mathbb{N}_0^m.$$

Every $a \in A$ can be written as $k_1 b_1 + \dots + k_n b_n$, where $1 \le n \le 2m-1$, $k_1, \dots, k_n \in \mathbb{N}$ and $b_1, \dots, b_n \in B$. In other words,

$$A = \bigcup \big\{ \operatorname{Sg}(B') \;\big|\; B' \subseteq B,\, |B'| \le 2m-1 \big\}.$$

Proof. Take an arbitrary $a \in A$ and express it as $\sum_{i=1}^k r_i c_i$, where $r_i \in \mathbb{Q}_0^+$ and $c_i \in C$. We have $a = \sum_{i=1}^k \lfloor r_i \rfloor c_i + \sum_{i=1}^k (r_i - \lfloor r_i \rfloor) c_i$. The second sum is an element of P, hence $\operatorname{Sg}(C \cup P) = A$ and consequently $B \subseteq C \cup P$.

Let $a \in A$, $a \ne 0$, and let $B_a = \{b_1, \dots, b_p\}$, where $p \in \mathbb{N}$, be the set of all nonzero $b \in B$ such that $b \le a$ (we assume that $b_1, \dots, b_p$ are pairwise different). Obviously $a \in \operatorname{Sg}(B_a)$. Choose $q_i \in \mathbb{Q}_0^+$, $i = 1, \dots, p$, such that $a = \sum_{i=1}^p q_i b_i$, the set $\{b_i \mid i \in \{1, \dots, p\},\, q_i \ne 0\}$ is linearly independent and $\sum_{i=1}^p q_i$ is maximal possible (see Proposition 1.8). Note that at most m of q_i's are nonzero. Set

$$a_0 = \sum_{i=1}^p q_i b_i - \sum_{i=1}^p \lfloor q_i \rfloor b_i.$$

We have $a_0 \in \operatorname{cone}(B_a) \cap \mathbb{N}_0^m$, hence $a_0 \in A$. Moreover, since $a_0 \le a$, it is $a_0 \in \operatorname{Sg}(B_a)$ and thus there are $\kappa_1, \dots, \kappa_p \in \mathbb{N}_0$ such that $a_0 = \sum_{i=1}^p \kappa_i b_i$. Clearly,

$$(*) \qquad a = \sum_{i=1}^p \kappa_i b_i + \sum_{i=1}^p \lfloor q_i \rfloor b_i,$$

which implies $\sum_{i=1}^p \kappa_i \le m-1$. (This is a bit tricky: if it was $\sum_{i=1}^p \kappa_i \ge m$, then $\sum_{i=1}^p (\kappa_i + \lfloor q_i \rfloor) \ge m + \sum_{i=1}^p \lfloor q_i \rfloor > \sum_{i=1}^p q_i$, since there are at most m nonzeros among q_i's. This would contradict our choice of q_i's.) It follows that there are at most $m-1$ nonzeros among numbers $\kappa_1, \dots, \kappa_p$. Removing zero terms from $(*)$ now establishes the desired representation of a. ∎

3.7 Carathéodory's rank and ICP. The second part of the previous proposition relates with the notion of the *Carathéodory's rank $CR(A)$ of subsemigroup A of $\mathbb{N}_0^m$*, defined as

$$CR(A) = \sup_{a \in A} \min \big\{ n \in \mathbb{N} \;\big|\; \text{there are } k_i \in \mathbb{N} \text{ and } b_i \in \operatorname{Hb}(A),\ i = 1, \dots, n, \text{ such that } a = k_1 b_1 + \dots + k_n b_n \big\} \in \mathbb{N} \cup \{\infty\}.$$

(In the existing literature, $CR(A)$ is defined only if A is pure and finitely generated. Then it suffices to write 'min' instead of 'sup'.) Note that if A is finitely generated, then $CR(A) < \infty$.

Proposition 3.6 states that $CR(A) \le 2m-1$ for pure semigroups. (The best known bound $CR(A) \le 2m-2$ was obtained by Sebő in [Seb90].)

A subsemigroup A of $\mathbb{N}_0^m$ has a property known as *integral Carathéodory's property* (ICP for short) if $CR(A) \le m$ (compare with Carathéodory's theorem for cones 1.6). It was conjectured by Sebő ([Seb90]) that A satisfies ICP whenever A is pure and finitely generated. For $m \ge 6$, this was disproved in [Br98] by constructing pure subsemigroups A of $\mathbb{N}_0^m$ with $CR(A) \ge \lfloor 7m/6 \rfloor$. These counterexamples arise from one concrete counterexample in $\mathbb{N}_0^6$, which is a pure semigroup $A = \mathrm{Sg}^{\mathrm{P}}(\{b_1, \dots, b_{10}\})$ with $CR(A) = 7$, where

$$\begin{aligned} b_1 &= (0,1,0,0,0,0), & b_6 &= (1,0,2,1,1,2),\\ b_2 &= (0,0,1,0,0,0), & b_7 &= (1,2,0,2,1,1),\\ b_3 &= (0,0,0,1,0,0), & b_8 &= (1,1,2,0,2,1),\\ b_4 &= (0,0,0,0,1,0), & b_9 &= (1,1,1,2,0,2),\\ b_5 &= (0,0,0,0,0,1), & b_{10} &= (1,2,1,1,2,0). \end{aligned}$$

All pure subsemigroups of $\mathbb{N}_0^m$, $m = 1,2,3$, satisfy ICP (see the first paragraph of Chapter 4, Proposition 4.10 and Theorem 4.14), the situation in dimensions $m = 4$ and $m = 5$ is still an open problem.

3.8 Lemma. *Let n be the smallest positive integer such that $CR(B) \le n$ for every finitely generated pure subsemigroup B of $\mathbb{N}_0^m$. Then every pure subsemigroup A of $\mathbb{N}_0^m$ satisfies $CR(A) \le n$.*

Proof. First note that such an n exists and is $\le 2m-1$ (Proposition 3.6). Take an arbitrary $a \in A$ and denote by C the set $\{b \in A \mid b \le a\}$. The semigroup $B = \mathrm{Sg}^{\mathrm{P}}(C)$ contains a and is finitely generated, hence $a = k_1 b_1 + \dots + k_p b_p$, where $1 \le p \le n$ and $k_i \in \mathbb{N}$ and $b_i \in \mathrm{Hb}(B)$ for $i = 1, \dots, p$. Fix an $i \in \{1, \dots, n\}$. It follows from Proposition 2.4 that $b_i \in C$ is *not* a sum of two nonzero elements of C, thus also $b_i \in \mathrm{Hb}(A)$ (use 2.4 again). Consequently, we have $CR(A) \le n$. ∎

There is a natural question whether there is an $m \in \mathbb{N}$ and a subsemigroup A of $\mathbb{N}_0^m$ with $CR(A) = \infty$. (It is clear that such semigroup would be neither pure nor finitely generated.) We anticipate that the answer is 'yes' as we shall see in Example 4.11 (where $m = 2$).

3.9 Lemma. *Let A be a pure subsemigroup of $\mathbb{N}_0^m$ containing 0. Then $\mathcal{E}(A)$ is a pure subsemigroup of $\mathbb{N}_0^m$.*

Proof. We proved in Lemma 2.8 that $\mathcal{E}(A)$ is a subsemigroup of $\mathbb{N}_0^m$. Let $a \in \mathbb{N}_0^m$ and $n \in \mathbb{N}$ be such that $na \in \mathcal{E}(A)$. The semigroup A is pure and thus $a \in A$. If $b \in A$ is such that $b - a \in \mathbb{N}_0^m$, then $n(b-a) \in \mathbb{N}_0^m$ and consequently $n(b-a) \in A$, since $na \in \mathcal{E}(A)$. Using the fact that A is pure we get $b - a \in A$, which implies $a \in \mathcal{E}(A)$. ∎

3.10 Proposition. *Let A be a pure subsemigroup of $\mathbb{N}_0^m$ containing 0. Then there exists a $b \in A \setminus \{0\}$ such that $a - b \in A$ whenever $a \in A$ and $a - b \in \mathbb{N}_0^m$ if and only* *if there exists a* $b' \in \text{cone}(A) \setminus \{0\}$ *such that* $a' - b' \in \text{cone}(A)$ *whenever* $a' \in \text{cone}(A)$ *and* $a' - b' \in (\mathbb{Q}_0^+)^m$.

Proof. The statement is trivial if $A = \{0\}$, therefore assume $A \neq \{0\}$. To prove the direct implication, set $b' = b \in \text{cone}(A) \setminus \{0\}$ and take an arbitrary $a' \in \text{cone}(A)$ with $a' - b \in (\mathbb{Q}_0^+)^m$. There exists $k \in \mathbb{N}$ such that $ka' \in A$. We have $ka' - kb = k(a' - b) \in \mathbb{N}_0^m$ and thus $ka' - kb \in A$. Hence it is $a' - b \in \text{cone}(A)$. To prove the converse implication, find $k \in \mathbb{N}$ with $kb' \in \mathbb{N}_0^m$ and set $b = kb' \in A$. For every $a \in A$ with $a - b \in \mathbb{N}_0^m$ we have $a/k \in \text{cone}(A)$ and $(a - b)/k = a/k - b' \in (\mathbb{Q}_0^+)^m$. Therefore $(a - b)/k \in \text{cone}(A)$ and $a - b \in \text{cone}(A) \cap \mathbb{N}_0^m$, which implies $a - b \in A$. ∎

3.11 Lemma. *Let* A *be a pure subsemigroup of* $\mathbb{N}_0^m$ *containing* 0 *and let* $b \in (\mathbb{Q}_0^+)^m$. *Then* $b \in \text{cone}(\mathcal{E}(A))$ *if and only if* $(\mathbb{Q}b + \mathbb{Q}_0^+(a - b)) \cap (\mathbb{Q}_0^+)^m \subseteq \text{cone}(A)$ *for all* $a \in \text{cone}(A)$.

Proof. It is obvious that it suffices to prove the assertion for "$b \in \mathcal{E}(A)$" and "all $a \in A$". Assume that $b \in \mathcal{E}(A)$ and let $a \in A$, $r \in \mathbb{Q}$ and $s \in \mathbb{Q}_0^+$ be such that $c = rb + s(a - b) \in (\mathbb{Q}_0^+)^m$. There is a $k \in \mathbb{N}$ such that $r' = kr \in \mathbb{Z}$ and $s' = ks \in \mathbb{N}_0$. We have $kc = r'b + s'(a - b) = s'a - (s' - r')b \in \mathbb{N}_0^m$. Either $s' - r' \leq 0$ and $-(s' - r')b \in A$ or $s' - r' > 0$ and $(s' - r')b \in \mathcal{E}(A)$. In both cases we get $kc \in A$, hence $c \in \text{cone}(A)$. Now we prove the converse implication. Let $b \in \mathbb{N}_0^m$ and let $a \in A$ be such that $a - b \in \mathbb{N}_0^m$. Then we have $a - b = 0b + 1(a - b) \in \text{cone}(A)$ and consequently $a - b \in A$. ∎

3.12 Corollary. *Let* A *be a pure subsemigroup of* $\mathbb{N}_0^m$ *containing* 0. *Then either* $A = \mathbb{N}_0^m$ *or* $\mathcal{E}(A) \subseteq \partial(\text{cone}(A))$.

Proof. Suppose that there exists a $b \in \mathcal{E}(A) \cap \text{int}(\text{cone}(A))$ and fix an $\varepsilon \in \mathbb{Q}^+$ such that $B(b, \varepsilon) \subseteq \text{cone}(A)$. Let $a \in \mathbb{N}_0^m$, $a \neq b$. We have $a = b + \frac{1}{r}(b + r(a - b) - b)$, where $r = \varepsilon/(2\|a - b\|) \in \mathbb{Q}^+$. It is $\|b + r(a - b) - b\| = r\|a - b\| < \varepsilon$, thus $b + r(a - b) \in B(a, \varepsilon) \subseteq \text{cone}(A)$. Lemma 3.11 (applied on $a^* = b + r(a - b)$, $b^* = b$) gives $a \in A$ and consequently $A = \mathbb{N}_0^m$. ∎

3.13 Proposition. *Let* A *be a pure subsemigroup of* $\mathbb{N}_0^m$ *containing* 0. *Then we have* $\text{cone}(\mathcal{E}(A)) = \text{Lin}(\mathcal{E}(A)) \cap (\mathbb{Q}_0^+)^m$ *and* $\mathcal{E}(A)$ *is a finitely generated semigroup.*

Proof. We first prove that $(\mathbb{Q}a + \mathbb{Q}b) \cap (\mathbb{Q}_0^+)^m \subseteq \text{cone}(\mathcal{E}(A))$ for all $a, b \in \mathcal{E}(A)$. By Lemma 3.11 applied on $\mathcal{E}(A)$ we have

$$(\mathbb{Q}b + \mathbb{Q}_0^+(a - b)) \cap (\mathbb{Q}_0^+)^m \subseteq \text{cone}(\mathcal{E}(A)),$$
$$(\mathbb{Q}a + \mathbb{Q}_0^+(b - a)) \cap (\mathbb{Q}_0^+)^m \subseteq \text{cone}(\mathcal{E}(A)).$$

It is easily verified that the union of the sets on the left sides is $(\mathbb{Q}a + \mathbb{Q}b) \cap (\mathbb{Q}_0^+)^m$, hence it is a subset of $\text{cone}(\mathcal{E}(A))$.

Let $b_1, \dots, b_n \in \mathcal{E}(A)$ and $r_1, \dots, r_n \in \mathbb{Q}$ be such that $\sum_{i=1}^n r_i b_i \in (\mathbb{Q}_0^+)^m$. We may assume that $r_1 \geq r_2 \geq \cdots \geq r_n$. We prove by induction that $\sum_{i=1}^k r_i b_i \in \text{cone}(\mathcal{E}(A))$ for $k = 1, \dots, n$. The claim is obvious for $k = 1$. Assume that $c = \sum_{i=1}^k r_i b_i \in \text{cone}(\mathcal{E}(A))$ for some k such that $1 \leq k < n$. We can find an $\ell \in \mathbb{N}$ such that $\ell c \in \mathcal{E}(A)$. Then $\ell c + \ell r_{k+1} b_{k+1} \in (\mathbb{Q}\ell c + \mathbb{Q}\ell b_k) \cap (\mathbb{Q}_0^+)^m$ and consequently $c + r_{k+1} b_{k+1} \in \text{cone}(\mathcal{E}(A))$.

It follows that $\mathrm{cone}(\mathcal{E}(A)) = (\mathbb{Q}_0^+)^m \cap V$, where $V = \mathrm{Lin}(\mathcal{E}(A))$. The cone generated by $\mathcal{E}(A)$ is finitely generated by Lemma 1.19, thus $\mathcal{E}(A)$ is a finitely generated semigroup. ∎

3.14 Proposition. *Let A be a subsemigroup of $\mathbb{N}_0^m$ containing 0. Then*

(i) $\mathrm{Sg}^{\mathrm{p}}(\mathcal{E}(A)) \subseteq \mathcal{E}(\mathrm{Sg}^{\mathrm{p}}(A))$;

(ii) *if A is pure, then* $\mathrm{Sg}^{\mathrm{p}}(\mathcal{E}(A)) = \mathcal{E}(\mathrm{Sg}^{\mathrm{p}}(A))$;

(iii) *the semigroup $\mathcal{E}(A)$ is finitely generated.*

Proof. (i) Let $b \in \mathrm{Sg}^{\mathrm{p}}(\mathcal{E}(A))$ and take an arbitrary $a \in \mathrm{Sg}^{\mathrm{p}}(A)$ with $a-b \in \mathbb{N}_0^m$. There are $k, \ell \in \mathbb{N}$ such that $kb \in \mathcal{E}(A)$ and $\ell a \in A$. We have $k\ell(a-b) = k(\ell a) - \ell(kb) \in \mathbb{N}_0^m$, hence $k\ell(a-b) \in A$ and $a - b \in \mathrm{Sg}^{\mathrm{p}}(A)$. Thus $b \in \mathcal{E}(\mathrm{Sg}^{\mathrm{p}}(A))$ and (i) is proved.

(ii) This is obvious, since if A is pure, then $\mathrm{Sg}^{\mathrm{p}}(\mathcal{E}(A)) = \mathcal{E}(A)$ and $\mathrm{Sg}^{\mathrm{p}}(A) = A$.

(iii) Apply (i) on $\mathcal{E}(A)$ to obtain $\mathrm{Sg}^{\mathrm{p}}(\mathcal{E}(\mathcal{E}(A))) = \mathrm{Sg}^{\mathrm{p}}(\mathcal{E}(A)) \subseteq \mathcal{E}(\mathrm{Sg}^{\mathrm{p}}(\mathcal{E}(A)))$. Obviously the converse inclusion also holds, hence $\mathrm{Sg}^{\mathrm{p}}(\mathcal{E}(A)) = \mathcal{E}(\mathrm{Sg}^{\mathrm{p}}(\mathcal{E}(A)))$. On the right side there is a finitely generated semigroup (see the previous proposition), hence $\mathrm{Sg}^{\mathrm{p}}(\mathcal{E}(A))$ and $\mathcal{E}(A)$ are finitely generated. ∎

3.15 Remark. We can not write '=' in part (i) of the previous proposition, since for the subsemigroup $A = \mathbb{N}\setminus\{1\}$ of $\mathbb{N}_0$ we have $\mathrm{Sg}^{\mathrm{p}}(\mathcal{E}(A)) = \mathrm{Sg}^{\mathrm{p}}(\{0\}) = \{0\}$ and $\mathcal{E}(\mathrm{Sg}^{\mathrm{p}}(A)) = \mathcal{E}(\mathbb{N}_0) = \mathbb{N}_0$.

3.16 Lemma. *Let $M = \{e_1, \dots, e_m\}$ be the canonical basis of $\mathbb{Q}^m$ and let A be a pure subsemigroup of $\mathbb{N}_0^m$ such that $0 \in A$ and $\mathrm{rank}\, A = m$. Then $\mathcal{E}(A) \neq \mathrm{cone}(M \setminus \{e_i\}) \cap \mathbb{N}_0^m = \mathrm{Sg}(\{0\} \cup (M \setminus \{e_i\}))$ for every $i = 1, \dots, m$ (c.f. Proposition 3.13). If $\mathrm{rank}\,\mathcal{E}(A) = m-1$, then there is a $b \in \mathcal{E}(A) \cap \mathbb{N}^m$.*

Proof. On the contrary, suppose that $\mathcal{E}(A) = \mathrm{cone}(M \setminus \{e_i\}) \cap \mathbb{N}_0^m$ for some i in $\{1, \dots, m\}$. Since $\mathrm{rank}\, A > \mathrm{rank}\,\mathcal{E}(A)$, there is an $a = (a_1, \dots, a_m) \in A$ with $a_i \neq 0$. It is $(a_1, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_m) \in \mathcal{E}(A)$, thus $(0, \dots, 0, a_i, 0, \dots, 0) \in A$ and consequently $e_i \in A$ (A is pure). It follows $A \supseteq \mathrm{Sg}(\mathcal{E}(A) \cup \{e_i\}) = \mathbb{N}_0^m$ and $A = \mathcal{E}(A) = \mathbb{N}_0^m$, a contradiction.

If $\mathrm{rank}\,\mathcal{E}(A) = m-1$, then there are by the previous part $b_1, \dots, b_m \in \mathcal{E}(A)$ such that the i-th coordinate of b_i is nonzero and we may set $b = b_1 + \cdots + b_m$. ∎

3.17 Theorem. *Let A be a pure subsemigroup of $\mathbb{N}_0^m$ containing 0 and let $V = \mathrm{Lin}(\mathcal{E}(A))$. Then*

(i) *if $\dim V = m$, then $A = \mathbb{N}_0^m$;*

(ii) *if $\dim V = m-1$, then $A = \mathcal{E}(A)$ or A is the set of integer points with nonnegative coordinates in a half-space determined by V.*

If one of these cases takes place, then A is finitely generated.

Proof. If $\dim V = m$, then $A = \mathbb{N}_0^m$ by Proposition 3.13 and obviously A is finitely generated. If $\dim V = m-1$ and $\dim \mathrm{Lin}(A) = m-1$, then we have $A \subseteq \mathcal{E}(A)$ by 3.13, hence $A = \mathcal{E}(A)$ is a finitely generated semigroup.

Suppose now that $\dim V = m-1$ and $\dim \mathrm{Lin}(A) = m$. Let $w \in \mathbb{Q}^m$ be such that $V = \{\langle w, x\rangle = 0\}$ and let $a \in A \setminus \mathcal{E}(A)$. Without loss of generality we may assume that

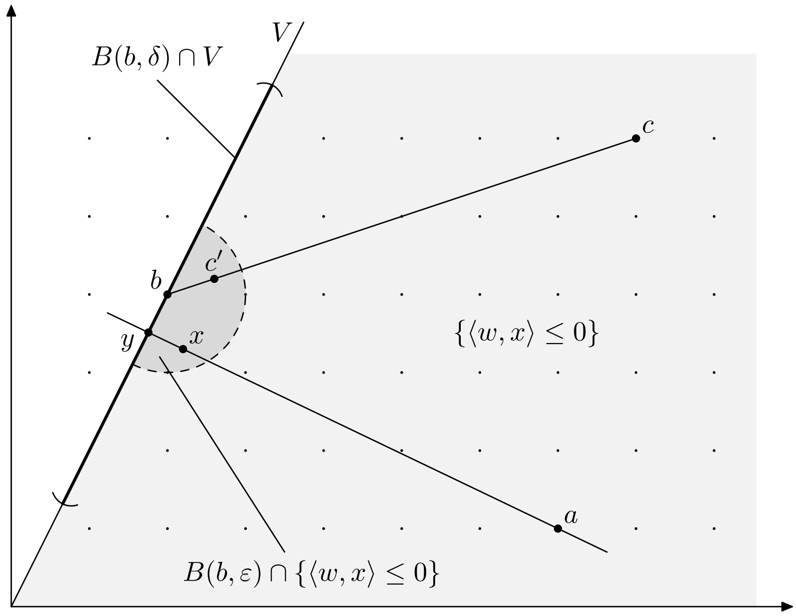

Fig. 1: to the proof of Theorem 3.17

$\langle w,a\rangle < 0$. There is a nonzero $b \in \mathcal{E}(A)$ and $\delta \in \mathbb{Q}^+$ such that $B(b,\delta)\cap V \subseteq \operatorname{cone}(\mathcal{E}(A))$ (use Lemma 3.16). Our first goal is to prove that there exists an $\varepsilon \in \mathbb{Q}^+$ such that $B(b,\varepsilon)\cap\{\langle w,x\rangle \le 0\} \subseteq \operatorname{cone}(A)$ (see Fig. 1). Choose an $\varepsilon \in \mathbb{Q}^+$, $\varepsilon < \delta/3$, with this property:

$$x \in B(b,\varepsilon) \implies \left(x-a \notin V \quad\text{and}\quad \left|\frac{\langle w,a\rangle}{\langle w,a-x\rangle} - 1\right| < \min\left\{\frac{1}{100}, \frac{\delta}{3\|a-b\|}\right\}\right)$$

(note that $|\langle w,a-x\rangle - \langle w,a\rangle| = |\langle w,-x\rangle| = |\langle w,b-x\rangle| \le \|w\|\cdot\|b-x\| < \varepsilon\|w\|$; the $\frac{1}{100}$ ensures that $\frac{3}{2}\langle w,a\rangle < \langle w,a-x\rangle < \frac{1}{2}\langle w,a\rangle$).

Fix an $x \in B(b,\varepsilon)\cap\{\langle w,x\rangle \le 0\}$. If $x \in V$, then we have $x \in \operatorname{cone}(\mathcal{E}(A))$, since $\varepsilon < \delta$. From now on suppose $\langle w,x\rangle < 0$. The line given parametrically by the point a and the direction vector $x-a$ intersects V in some point $y = a + t(x-a)$, where $t \in \mathbb{Q}$ is uniquely determined. We have $\langle w,y\rangle = 0$, hence

$$\langle w, a+t(x-a)\rangle = 0, \quad t\cdot\langle w,x-a\rangle = -\langle w,a\rangle \quad\text{and}\quad t = \frac{\langle w,a\rangle}{\langle w,a-x\rangle}\,.$$

Since $0 > \frac{1}{2}\langle w,a\rangle > \langle w,a-x\rangle = \langle w,a\rangle - \langle w,x\rangle > \langle w,a\rangle$, we have $t > 1$. The point x can be written as $sy + (1-s)a$, where $0 < s = 1/t < 1$. Thus x is a convex combination of the points a and y and we have $x \in \operatorname{cone}(A)$ after showing $y \in B(b,\delta)$. It is

$$\begin{aligned}\|y-b\| \le \|y-x\| + \|x-b\| = \|(t-1)(x-a)\| + \|x-b\| \le \\ (t-1)\cdot\big(\|x-b\| + \|b-a\|\big) + \|x-b\| = (t-1)\cdot\|b-a\| + t\,\|x-b\|.\end{aligned}$$

We have $(t-1)\cdot\|b-a\| < \delta/3$ and $t\|x-b\| < 2\|x-b\| < 2\delta/3$. Thus $y \in B(b,\delta)$ and $x \in \operatorname{cone}(A)$.

We recall that in the preceding paragraph, we got an $\varepsilon \in \mathbb{Q}^+$ such that $B(b,\varepsilon)\cap\{\langle w,x\rangle \le 0\} \subseteq \operatorname{cone}(A)$. Now take an arbitrary point $c \in (\mathbb{Q}_0^+)^m$ with $\langle w,c\rangle < 0$.

On the line segment between c and b there exists a point $c' \in B(b, \varepsilon)$, $c' \neq b$. Hence $c = b + r(c' - b)$ for some $r \in \mathbb{Q}^+$ and $c \in \operatorname{cone}(A)$ by Lemma 3.11. Therefore we have $A \supseteq \{\langle w, x\rangle \leq 0\} \cap (\mathbb{Q}_0^+)^m$. Striving for a contradiction, assume there exists a $d \in A$ with $\langle w, d\rangle > 0$. Then, by symmetry considerations, we see that $A \supseteq \{\langle w, x\rangle \geq 0\} \cap (\mathbb{Q}_0^+)^m$ and thus $\operatorname{cone}(A) = (\mathbb{Q}_0^+)^m$, which implies $A = \mathbb{N}_0^m = \mathcal{E}(A)$, a contradiction with $\dim V = m - 1$.

We proved that $\operatorname{cone}(A) = \{\langle w, x\rangle \leq 0\} \cap (\mathbb{Q}_0^+)^m$, thus A is a finitely generated semigroup of non-negative integer points in one of half-spaces determined by V (it is obvious that $\{\langle w, x\rangle \leq 0\} \cap (\mathbb{Q}_0^+)^m$ is a polyhedral cone and thus finitely generated by Theorem 1.17). ∎

3.18 Holes in subsemigroups of $\mathbb{N}_0^m$. Let A be a subsemigroup of $\mathbb{N}_0^m$. We say that $h \in \operatorname{Sg}^{\mathrm{p}}(A)$ is a *hole* in A if $h \notin A$ and a hole f is *fundamental* if there is no hole h such that $f - h \in A$. Let H resp. F be the set of all holes resp. fundamental holes in A. It follows that $\operatorname{Sg}^{\mathrm{p}}(A) = A \cup \bigcup\{f + A \mid f \in F\}$.

Suppose that A is finitely generated, $\operatorname{Hb}(A) = \{0, a_1, a_2, \ldots, a_n\}$, where $n \in \mathbb{N}$ and $0, a_1, \ldots, a_n$ are pairwise distinct, and that $C \subseteq A$ is some finite set of generators of $\operatorname{cone}(A)$. We have $F \subseteq \{\sum_{i=1}^k q_i c_i \mid k \in \mathbb{N}_0,\ c_i \in C,\ q_i \in \mathbb{Q}_0^+,\ q_i < 1\}$. Indeed, if $q_1, \ldots, q_k \in \mathbb{Q}_0^+$, then $\sum_{i=1}^k q_i c_i \in A$ whenever $\sum_{i=1}^k (q_i - \lfloor q_i \rfloor) c_i \in A$. It follows that the set F is finite. Let $f \in F$. The set

$$M = \Big\{(q_1, \ldots, q_n) \in \mathbb{N}_0^n \;\Big|\; f + \sum_{i=1}^n q_i a_i \in A\Big\}$$

is an upper set, hence there are pairwise different $m_1, \ldots, m_p \in \mathbb{N}_0^n$, where $p \in \mathbb{N}_0$, such that $M = \bigcup_{i=1}^p \{m \in \mathbb{N}_0^n \mid m \geq m_i\}$ (Corollary 2.13) and

$$(f + F) \cap H = \Big\{f + \sum_{i=1}^n q_i a_i \;\Big|\; (q_1, \ldots, q_n) \ngeq m_i \text{ for every } i \in \{1, \ldots, p\}\Big\}.$$

Determining $m_1, \ldots, m_p$ directly seems to be computationally difficult ([He09]), but it is possible give an alternative finite description of M. There are software packages (e.g. [4ti2]) that give the finite set $M'_{\min}$ of all minimal elements of the set

$$M' = \Big\{(q_1, \ldots, q_n, r_1, \ldots, r_n) \in \mathbb{N}_0^{2n} \;\Big|\; f + \sum_{i=1}^n q_i a_i = \sum_{i=1}^n r_i a_i\Big\}$$

Then it is obvious that $\{m_1, \ldots, m_p\}$ is the set of all minimal elements of $\{q \in \mathbb{N}_0^n \mid$ there exists $r \in \mathbb{N}_0^n$ such that $(q, r) \in M'_{\min}\}$.

3.19 Example. We use the same notation as above. Let A be the subsemigroup of $\mathbb{N}_0^2$ generated by $(0,0)$, $a_1 = (2,1)$, $a_2 = (1,2)$ and $a_3 = (4,4)$ (see Fig. 2). Evidently $\operatorname{Hb}(A) = \{0, a_1, a_2, a_3\}$ (hence $n = 3$), one of valid choices of C is $C = \{a_1, a_2\}$ and $F = \{(1,1), (2,2)\}$. Let $f = (1,1) \in F$. We have $M' = \{(q_1, q_2, q_3, r_1, r_2, r_3) \in \mathbb{N}_0^6 \mid q_1 a_1 + q_2 a_2 + q_3 a_3 - r_1 a_1 - r_2 a_2 - r_3 a_3 = -f\}$, hence

$$M' = \{x \in \mathbb{N}_0^6 \mid W x^{\mathrm{T}} \leq (-1, -1, 1, 1)^{\mathrm{T}}\}, \quad \text{where } W = \begin{pmatrix} 2 & 1 & 4 & -2 & -1 & -4 \\ 1 & 2 & 4 & -1 & -2 & -4 \\ -2 & -1 & -4 & 2 & 1 & 4 \\ -1 & -2 & -4 & 1 & 2 & 4 \end{pmatrix}.$$

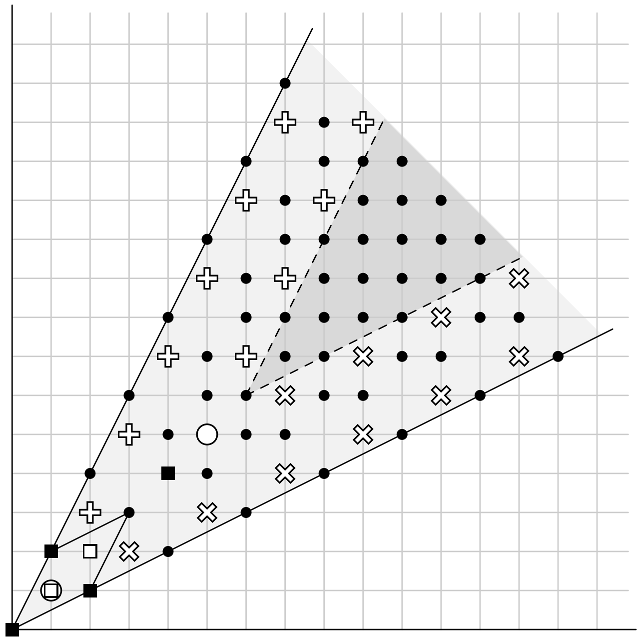

Fig. 2: $A = \{\blacksquare\} \cup \{\bullet\}$, $\mathrm{Hb}(A) = \{\blacksquare\}$, $F = \{\square\}$, $H_1 = \{\bigcirc\}$, $H_2 = \{$✖$\}$ and $H_3 = \{$✚$\}$

The minimal solutions are $(0,0,2,3,3,0)$ and $(1,1,0,0,0,1)$ (the author used [4ti2]*, program `zsolve`), hence $M = \{(q_1,q_2,q_3) \in \mathbb{N}_0^3 \mid (q_1,q_2,q_3) \geq (0,0,2)$ or $(q_1,q_2,q_3) \geq (1,1,0)\}$. Thus the holes in $f + A$ fall into one of the sets $H_i = \{f + q_1a_1 + q_2a_2 + q_3a_3 \mid (q_1,q_2,q_3) \in Q_i\}$, $i = 1,2,3$, where

$$Q_1 = \{(0,0,0),(0,0,1)\}, \quad Q_2 = \{(n,0,0),(n,0,1) \mid n \in \mathbb{N}\}$$
$$\text{and} \quad Q_3 = \{(0,n,0),(0,n,1) \mid n \in \mathbb{N}\}.$$

Similarly the holes in $f' + A = (2,2) + A$ fall into one of the sets $H'_i = \{f' + q_1a_1 + q_2a_2 + q_3a_3 \mid (q_1,q_2,q_3) \in Q'_i\}$, $i = 1,2,3$, (with the exception of the hole $(5,5)$ belonging both to H'_2 and H'_3,) where

$$Q'_1 = \{(0,0,0)\}, \quad Q'_2 = \{(n,0,0),(n,1,0) \mid n \in \mathbb{N}\}$$
$$\text{and} \quad Q'_3 = \{(0,n,0),(1,n,0) \mid n \in \mathbb{N}\}.$$

There are no holes in A in the region $(6,6) + \mathrm{cone}(A)$ (see Fig. 2), since

$$A \cap ((6,6) + \mathrm{cone}(A)) \supseteq ((6,6) + A) \cup ((7,7) + A) \cup ((8,8) + A) =$$
$$(6,6) + (A \cup (f + A) \cup (f' + A)) = (6,6) + \mathrm{Sg^p}(A).$$

---

* PROJECT.mat:

```
 4  6
 2  1  4 -2 -1 -4
 1  2  4 -1 -2 -4
-2 -1 -4  2  1  4
-1 -2 -4  1  2  4
```

PROJECT.rel:

```
1 4
< < < <
```

PROJECT.rhs:

```
 1  4
-1 -1 1 1
```

PROJECT.sign: → PROJECT.zinhom:

```
1 6
1 1 1 1 1 1
```

```
2 6
0 0 2 3 3 0
1 1 0 0 0 1
```

4. Subsemigroups of $\mathbb{N}_0^1$, $\mathbb{N}_0^2$ and $\mathbb{N}_0^3$

In this chapter we examine some properties of subsemigroups of $\mathbb{N}_0$, $\mathbb{N}_0^2$ and $\mathbb{N}_0^3$.

(I) Subsemigroups of $\mathbb{N}_0$. The situation in dimension 1 is in fact quite simple. The only non-empty cones in $\mathbb{Q}_0^+$ are $\{0\}$ and $\mathbb{Q}_0^+$, hence the only pure subsemigroups of $\mathbb{N}_0$ are $\{0\} = \mathrm{Sg}(\{0\})$, $\mathbb{N} = \mathrm{Sg}(\{1\})$ and $\mathbb{N}_0 = \mathrm{Sg}(\{0,1\})$ (see Lemma 3.2(vi)). It follows from Corollary 3.4 that *all* subsemigroups of $\mathbb{N}_0$ are finitely generated.

4.1 Lemma. *Let $A \neq \{0\}$ be a subsemigroup of $\mathbb{N}_0$. Then*

(i) *there is the maximal number $r \in \mathbb{N}$ such that there is a subsemigroup A_1 of $\mathbb{N}_0$ with $A = rA_1$;*

(ii) *if r and A_1 are as in (i), then there is the smallest $s \in \mathbb{N}_0$ such that $s + \mathbb{N}_0 \subseteq A_1$;*

(iii) *if $\mathcal{E}(A) \supsetneq \{0\}$, then $A = r\mathbb{N}_0$ for the $r \in \mathbb{N}$ from (i).*

Proof. Since $A \neq \{0\}$, there exists $\gcd(A) \in \mathbb{N}$, which is evidentally the r from (i); a semigroup A_1 is uniquely determined as $A_1 = A/r$ and we have $\gcd(A_1) = 1$. Define

$$m = \min\{m' \in \mathbb{N} \mid \text{there exists an } n' \in A_1 \cup \{0\} \text{ such that } m' + n' \in A_1\}$$

and fix some $n \in A_1 \cup \{0\}$ with $m + n \in A_1$. Let $m_1 \in \mathbb{N}$ and $n_1 \in A_1 \cup \{0\}$ be such that $m_1 + n_1 \in A_1$. We have $m_1 = km + \ell$, where $k, \ell \in \mathbb{N}_0$, $\ell < m$, and both $km + kn + n_1 = k(m+n) + n_1$ and $km + kn + n_1 + \ell = m_1 + n_1 + kn$ are in A_1. Using the minimal property of m, we observe that $\ell < m$ must be zero and thus m divides m_1. In particular, the number m divides every element of A_1 (we could choose $m_1 = n_1 \in A_1 \cap \mathbb{N}$) and therefore $m = 1$ (recall $\gcd(A_1) = 1$).

We have $n \in A_1 \cup \{0\}$ and $n + 1 \in A_1$. If $n = 0$, then either $A_1 = \mathbb{N}_0$ and $s = 0$ or $A_1 = \mathbb{N}$ and $s = 1$. Suppose now that $0 \neq n$ (thus n and $n+1$ are both in A_1). For $r_1, r_2 \in \mathbb{N}_0$, $r_1 \geq n$, $0 \leq r_2 < n$, we have $r_1 n + r_2 = (r_1 - r_2)n + r_2(n+1) \in A_1$ and we observe that $n^2 + \mathbb{N}_0 \subseteq A_1$. The existence of the s from (ii) is now obvious.

Assume that there is a $b \in \mathcal{E}(A)$, $b \neq 0$. It is easily seen that $b' = b/r \in \mathcal{E}(A_1)$. Since $A_1 \supseteq s + \mathbb{N}_0$, we have $A_1 \supseteq ((s + \mathbb{N}_0) - \mathbb{N}_0 b') \cap \mathbb{N}_0 = \mathbb{N}_0$, hence $A_1 = \mathbb{N}_0$ and the proof is complete. ∎

The Carathéodory's rank of a subsemigroup of $\mathbb{N}_0$ is always finite, but as we shall see in Proposition 4.3, it may be arbitrarily large.

4.2 Lemma. *Let n be a non-negative integer and $a_0, a_1, \dots, a_n \in \{0, 2^0, 2^1, \dots, 2^n\}$ be such that the sum $a_0 + a_1 + \dots + a_n$ equals $2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1$. Then $\{a_0, a_1, \dots, a_n\} = \{2^0, 2^1, \dots, 2^n\}$.*

Proof. We proceed by induction on n. The case $n = 0$ is trivial. Suppose the assertion is true for some $n \geq 0$ and let the sum of $a_0, \dots, a_{n+1} \in \{0, 2^0, 2^1, \dots, 2^{n+1}\}$ be $2^{n+2} - 1$. Among $a_0, \dots, a_{n+1}$ there are an odd number of ones; without loss of generality we may assume that $a_0 = a_1 = \cdots = a_{2k} = 1$, where $k \in \mathbb{N}_0$, and $a_i \neq 1$ for $2k+1 \leq i \leq n+1$. We have

$$\begin{aligned}(2k+1) \times 1 + a_{2k+1} + \cdots + a_{n+1} &= 2^{n+2} - 1,\\ k \times 0 + k \times 1 + \frac{a_{2k+1}}{2} + \cdots + \frac{a_{n+1}}{2} &= \frac{2^{n+2}-2}{2} = 2^{n+1} - 1.\end{aligned}$$

On the left side there are $n+1$ summands from the set $\{0, 2^0, 2^1, \ldots, 2^n\}$ and the induction assumption gives $k = 0$ and $\{a_{2k+1}/2, \ldots, a_{n+1}/2\} = \{2^0, 2^1, \ldots, 2^n\}$. Hence the numbers $a_0, a_1, \ldots, a_{n+1}$ are up to order the numbers $2^0, 2^1, \ldots, 2^{n+1}$. ∎

4.3 Proposition. *Let n and N be positive integers such that*

$$N > \max\{(n-3) \cdot 2^{n-1} + 1, 2^n - 2 - n\}$$

(this means that $N \in \mathbb{N}$ is arbitrary if $n \in \{1,2\}$, $N > 3$ if $n = 3$, $N > 10$ if $n = 4$ and $N > (n-3) \cdot 2^{n-1} + 1$ for $n \geq 5$). Let

$$A_1 = \{N + 2^i \mid i = 0, \ldots, n-1\} \quad \textit{and} \quad A = \mathrm{Sg}(A_1).$$

Then A_1 is the Hilbert basis of A and $CR(A) = n$.

Proof. It is easily verified that $N + 2^0 < N + 2^1 < \cdots < N + 2^{n-1} < 2(N + 2^0)$, thus we have $\mathrm{Hb}(A) = A_1$. Let $b = \sum_{a \in A_1} a = nN + 2^n - 1$ and assume that $b = a_0 + \cdots + a_k$ for some $k \in \mathbb{N}$ and some (not necessarily pairwise different) $a_i \in A_1$, $0 \leq i \leq k$. The numbers n and N are so chosen that

$$(n-1)(N + 2^{n-1}) < nN + 2^n - 1 < (n+1)(N + 2^0),$$

hence k must be equal to $n - 1$. We have

$$(a_0 - N) + (a_1 - N) + \cdots + (a_{n-1} - N) = b - nN = 2^n - 1$$

and $a_i - N \in \{2^0, 2^1, \ldots, 2^{n-1}\}$ for $i = 0, \ldots, n-1$. By the lemma above we have $\{a_0 - N, a_1 - N, \ldots, a_{n-1} - N\} = \{2^0, 2^1, \ldots, 2^{n-1}\}$. It follows that $\{a_0, \ldots, a_n\} = A_1$ and therefore $CR(A) = n$. ∎

(II) Subsemigroups of $\mathbb{N}_0^2$. The situation in dimension 2 is well describable because of a simple structure of cones in $(\mathbb{Q}_0^+)^2$. To shorten notation, we write $\mathbb{P}$ instead of $(\mathbb{Q}_0^+)^2 \setminus \{0\}$. Let $a = (a_1, a_2) \in \mathbb{P}$. The *slope* of the point a is defined as $\sigma(a) = a_2/a_1$ if $a_1 > 0$ and $\sigma(a) = \infty$ if $a_1 = 0$; the range of the slope function is the usually ordered set $\mathbb{Q}_0^+ \cup \{\infty\}$. We define a relation $\trianglelefteq$ on $\mathbb{P}$ by setting $a \trianglelefteq b$ if and only if $\sigma(a) \leq \sigma(b)$ and we write $a \triangleleft b$ if $\sigma(a) < \sigma(b)$.

4.4 Lemma. *The relation $\trianglelefteq$ has the following properties:*

(i) *it is a quasi-ordering on $\mathbb{P}$ (i.e. $\trianglelefteq$ is both reflexive and transitive);*
(ii) *if $a = (a_1, a_2) \in \mathbb{P}$ and $b = (b_1, b_2) \in \mathbb{P}$, then $a \trianglelefteq b$ if and only if $a_1 b_2 \geq a_2 b_1$ and $a \triangleleft b$ if and only if $a_1 b_2 > a_2 b_1$;*

(iii) *if $a, b \in \mathbb{P}$, then $a \trianglelefteq b \trianglelefteq a$ if and only if $\mathbb{Q}_0^+ a = \mathbb{Q}_0^+ b$;*
(iv) *if $a, b \in \mathbb{P}$ are such that $\sigma(a) \neq \sigma(b)$, then either $a \triangleleft b$ or $b \triangleleft a$.*

Proof. The assertions follow immediately from the definitions above. ∎

4.5 Lemma. *Let $a = (a_1, a_2)$ and $b = (b_1, b_2)$ be points in $\mathbb{P}$ such that $a \trianglelefteq b$. Then*

$$\operatorname{cone}(\{a, b\}) = \mathbb{Q}_0^+ a + \mathbb{Q}_0^+ b = \{0\} \cup \{c \in \mathbb{P} \mid a \trianglelefteq c \trianglelefteq b\}.$$

Proof. The first equality follows from the definition of cone(−). If $\sigma(a) = \sigma(b)$, then $\mathbb{Q}_0^+ a = \mathbb{Q}_0^+ b$ and the statement is trivial. Assume that $\sigma(a) < \sigma(b)$. It is easy to verify that for every $c = qa + rs$, where $q, r \in \mathbb{Q}_0^+$, the slope $\sigma(c)$ lies between $\sigma(a)$ and $\sigma(b)$. On the other hand, take a $c = (c_1, c_2) \in \mathbb{P}$ such that $a \triangleleft c \triangleleft b$. This means that $a_1 b_2 - a_2 b_1 > 0$, $b_2 c_1 - b_1 c_2 > 0$ and $a_1 c_2 - a_2 c_1 > 0$, hence

$$(c_1, c_2) = \frac{b_2 c_1 - b_1 c_2}{a_1 b_2 - a_2 b_1} (a_1, a_2) + \frac{a_1 c_2 - a_2 c_1}{a_1 b_2 - a_2 b_1} (b_1, b_2) \in \mathbb{Q}_0^+ a + \mathbb{Q}_0^+ b. \qquad \square$$

4.6 Definition. A set $R = \mathbb{Q}_0^+ a$, where $a \in \mathbb{P}$, is called a *ray*; the *slope* $\sigma(R)$ of R is defined as the common slope of its nonzero points. Let A be a cone in $(\mathbb{Q}_0^+)^2$. We say that a ray $R \subseteq A$ is a *border ray* of A if either $\sigma(R') \geq \sigma(R)$ for all rays $R' \subseteq A$ or $\sigma(R') \leq \sigma(R)$ for all rays $R' \subseteq A$. A ray R is called a *lower* border ray in the former case and an *upper* border ray in the latter one.

4.7 Proposition. *Let A^* be a subsemigroup of $\mathbb{N}_0^2$ and $A = \operatorname{cone}(A^*)$. Then*

(i) *A is finitely generated if and only if there are $a, b \in A$ such that $A = \operatorname{cone}(\{a, b\})$;*
(i*) *A^* is a finitely generated semigroup if and only if there are $a, b \in A^*$ such that $\operatorname{Sg}^{\mathrm{P}}(A^*) = \operatorname{Sg}^{\mathrm{P}}(\{a, b\})$;*
(ii) *∂A is the union of $\{0\}$ and the border rays of A;*
(iii) *if $A \supsetneq \{0\}$, then A resp. A^* is finitely generated if and only if A has both the lower and the upper border ray;*
(iv) *A resp. A^* is finitely generated if and only if A is a closed set in $\mathbb{Q}^2$ and $\operatorname{cone}_{\mathbb{R}}(A)$ is a closed set in $\mathbb{R}^2$ ($\operatorname{cone}_{\mathbb{R}}(A)$ being the same as in Note 1.10);*
(v) *A is finitely generated if and only if $A = \operatorname{cone}(\partial A)$;*
(v*) *A^* is finitely generated if and only if $\operatorname{cone}(A^*) = \operatorname{cone}(\partial \operatorname{cone}(A^*))$;*
(vi) *A is finitely generated if and only if for every line $\ell = \{a + qv \mid q \in \mathbb{Q}\}$, $a, v \in \mathbb{Q}^2$, $v \neq 0$, there are $q_1, q_2 \in \mathbb{Q} \cup \{-\infty, \infty\}$ such that $\ell \cap A = \{a + qv \mid q \in \mathbb{Q}, q_1 \leq q \leq q_2\}$.*

Sketch of proof. The statement is obvious if $A = \{0\}$ or if A is a ray, thus we may suppose to the rest of the proof that $\operatorname{rank} A = 2$. Ad (i): If $A = \operatorname{cone}(\{a_1, \ldots, a_n\})$ for some $a_1, \ldots, a_n \in \mathbb{P}$, then $A = \operatorname{cone}(\{a_i, a_j\})$, where $i, j \in \{1, \ldots, n\}$ are such that $a_i \trianglelefteq a_k \trianglelefteq a_j$ for all $k \in \{1, \ldots, n\}$. Ad (ii): Obviously $0 \in \partial A$ and it an easy exercise to prove that border rays lie within ∂A and every nonzero point $a \in \partial A$ determines a border ray $\mathbb{Q}_0^+ a$. Ad (iii): If A is finitely generated, then $A = \operatorname{cone}(\{a, b\})$ for some $a, b \in \mathbb{P}$, $a \triangleleft b$, and $\mathbb{Q}_0^+ a$ and $\mathbb{Q}_0^+ b$ are the lower and the upper ray respectively, and vice versa. Ad (iv): It is clear that if $A = \mathrm{cone}(\{a_1, \dots, a_n\})$, then $\mathrm{cone}_{\mathbb{R}}(A) = \mathrm{cone}_{\mathbb{R}}(\{a_1, \dots, a_n\})$ and the direct implication follows from Corollary 1.18. To prove the converse implication, we should observe that both the infimum and the supremum of the set $\Sigma = \{\sigma(a) \mid a \in A\} \subseteq \mathbb{Q}_0^+ \cup \{\infty\}$ exist in $\mathbb{R}_0^+ \cup \{\infty\}$; denote them α and β respectively. If $\alpha \notin \mathbb{Q}_0^+$ or $\beta \notin \mathbb{Q}^+ \cup \{\infty\}$, then $\mathrm{cone}_{\mathbb{R}}(A)$ is not closed set in $\mathbb{R}^2$ and A is not finitely generated. If $\alpha \in \mathbb{Q}_0^+ \setminus \Sigma$ or $\beta \in (\mathbb{Q}^+ \cup \{\infty\}) \setminus \Sigma$, then $\mathrm{cone}(A)$ is not closed in $\mathbb{Q}^2$ and A is not finitely generated. If $\alpha, \beta \in \Sigma$, then A has both the lower and the upper border ray and is finitely generated by (iii). Ad (v): This should be clear. Ad (vi): The direct implication follows from Proposition 1.20. On the other hand, take the line $(0,1) + (1,-1)q$, $q \in \mathbb{Q}$. The points $(0,1) + (1,-1)q_1$ and $(0,1) + (1,-1)q_2$ are then the points a and b from part (i). ∎

4.8 Proposition. *Let A be a pure subsemigroup of $\mathbb{N}_0^2$ such that $\mathcal{E}(A) \supsetneq \{0\}$. Then A is finitely generated and there is an $e \in \mathcal{E}(A)$ such that $A = \mathbb{N}_0 e$ or $A = \{a \in \mathbb{N}_0^2 \mid (1,0) \trianglelefteq a \trianglelefteq e\}$ or $A = \{a \in \mathbb{N}_0^2 \mid e \trianglelefteq a \trianglelefteq (0,1)\}$ or $A = \mathcal{E}(A) = \mathbb{N}_0^2$.*

Proof. We apply Theorem 3.17. If $\mathrm{rank}\,\mathcal{E}(A) = 2$, then $A = \mathbb{N}_0^2$. If $\mathrm{rank}\,\mathcal{E}(A) = 1$, then $\mathcal{E}(A)$ is equal to $\mathrm{cone}(\{e\}) \cap \mathbb{N}_0^2$ for some $e \in \mathcal{E}(A)$ (see Proposition 3.13) and there exists an $e = (e_1, e_2) \in \mathcal{E}(A)$ such that $\mathcal{E}(A) = \mathbb{N}_0 e$. Either $A = \mathcal{E}(A)$ or $A = A_1 = \{a \in \mathbb{N}_0^2 \mid \langle a, (-e_2, e_1)\rangle \le 0\}$ or $A = A_2 = \{a \in \mathbb{N}_0^2 \mid \langle a, (-e_2, e_1)\rangle \ge 0\}$. But it is not difficult to prove that $A_1 = \{a \in \mathbb{N}_0^2 \mid (1,0) \trianglelefteq a \trianglelefteq e\}$ and $A_2 = A = \{a \in \mathbb{N}_0^2 \mid e \trianglelefteq a \trianglelefteq (0,1)\}$. ∎

4.9 Lemma. *Let A be a finitely generated pure subsemigroup of $\mathbb{N}_0^2$ and let $n \in \mathbb{N}$ and points $a_1, \dots, a_n \in \mathbb{P}$, $a_1 \vartriangleleft \cdots \vartriangleleft a_n$, be such that $B = \{0, a_1, \dots, a_n\} = \mathrm{Hb}(A)$. Then $B \setminus \{a_1\}$ is the basis of $\mathrm{Sg}^{\mathrm{P}}(B \setminus \{a_1\})$ and $B \setminus \{a_n\}$ is the basis of $\mathrm{Sg}^{\mathrm{P}}(B \setminus \{a_n\})$.*

Proof. We may suppose $n \ge 3$, otherwise is the statement trivial, and we show (due to symmetric reasons) only the part concerning $\mathrm{Sg}^{\mathrm{P}}(B \setminus \{a_1\})$. Write $B' = B \setminus \{a_1\}$. We know from Proposition 3.6 that $\mathrm{Sg}^{\mathrm{P}}(B')$ is generated by $B' \cup P$, where $P = \big\{qa_2 + ra_n \mid q, r \in \mathbb{Q}_0^+,\ q, r < 1\big\} \cap \mathbb{N}_0^2 \subseteq \mathrm{cone}(A)$, thus it is enough to verify that $P \subseteq \mathrm{Sg}(B')$ (the rest then follows from Lemma 2.5, since $\mathrm{Hb}(\mathrm{Sg}^{\mathrm{P}}(B')) \supseteq \mathrm{Hb}(A) \cap \mathrm{Sg}^{\mathrm{P}}(B') \supseteq B'$).

We prove that if $a = \sum_{i=1}^{n} k_i a_i \in P$, $k_i \in \mathbb{N}_0$, then necessarily $k_1 = 0$. Suppose on the contrary that $k_1 \ge 1$ in such representation. Since $a_i \in \mathrm{cone}(\{a_1, a_n\})$ for every $i = 2, \dots, n-1$ and $a_1 \vartriangleleft a_n$, every a_i, $i = 2, \dots, n-1$, can be uniquely written as $qa_1 + ra_n$, where $q, r \in \mathbb{Q}_0^+$, $q, r < 1$. (We used Proposition 3.6 again; the set $\{a_1, a_n\}$ generates $\mathrm{cone}(A)$.) Substituting this into $a = \sum_{i=1}^{n} k_i a_i$ gives $a = \alpha_1 a_1 + \alpha_2 a_n$, where $\alpha_1, \alpha_2 \in \mathbb{Q}_0^+$, $\alpha_1 \ge k_1 \ge 1$.

We have $a_2 = \beta_1 a_1 + \beta_2 a_n$ for some $\beta_1, \beta_2 \in \mathbb{Q}_0^+$, $\beta_1, \beta_2 < 1$, and also $a = \gamma_1 a_2 + \gamma_2 a_n$, where $\gamma_1, \gamma_2 \in \mathbb{Q}_0^+$, $\gamma_1, \gamma_2 < 1$ ($a \in P$). Combining all together, we get

$$\alpha_1 a_1 + \alpha_2 a_n = a = \gamma_1(\beta_1 a_1 + \beta_2 a_n) + \gamma_2 a_n = \gamma_1\beta_1 a_1 + (\gamma_1\beta_2 + \gamma_2)a_n.$$

But a_1 and a_n are linearly independent, thus $\alpha_1 \ge 1$ should be equal to $\gamma_1\beta_1 < 1$, a contradiction. ∎

4.10 Proposition. *Let A be a pure subsemigroup of $\mathbb{N}_0^2$. Then $CR(A) \le 2$ and if $a, b \in \mathrm{Hb}(A) \cap \mathbb{P}$, $a \lhd b$, are such that there is no $c \in \mathrm{Hb}(A) \cap \mathbb{P}$ with $a \lhd c \lhd b$, then* $\det(a, b) = 1$.

Proof. We may that suppose $\operatorname{rank} A = 2$, since $\operatorname{rank} A \le 1$ implies $CR(A) = 1$. First assume that A is finitely generated and $\mathrm{Hb}(A) = \{0, a_1, \dots, a_n\}$, where $n \ge 2$ and $a_1 \lhd \dots \lhd a_n$. Let $a \in A \setminus \bigcup_{i=1}^n \mathbb{N}_0 a_i$. We have $a_i \lhd a \lhd a_{i+1}$ for some $i \in \{1, \dots, n-1\}$. Repeated application of Lemma 4.9 shows that the Hilbert basis of $\mathrm{Sg}^{\mathrm{P}}(\{0, a_i, a_{i+1}\})$ is $\{0, a_i, a_{i+1}\}$, thus $a = ka_i + \ell a_{i+1}$ for some $k, \ell \in \mathbb{N}$. It follows that $CR(A) = 2$.

Suppose that $\det(a_j, a_{j+1}) \ge 2$ for some j ($\det(a_j, a_{j+1})$ is an integer). It follows from Proposition 1.22 that there exists a nonzero $b = qa_j + ra_{j+1} \in \mathbb{N}_0^2$, $q, r \in \mathbb{Q}_0^+$, $q, r < 1$. Since $b \ne a_j$, $b \ne a_{j+1}$ and $b < a_j + a_{j+1}$, the point b do not lie within $\mathrm{Sg}(\{0, a_j, a_{j+1}\})$, a contradiction with $\{0, a_j, a_{j+1}\} = \mathrm{Hb}(\mathrm{cone}(\{a_j, a_{j+1}\}) \cap \mathbb{N}_0^2)$.

Now assume that A is not finitely generated. The statement about Carathéodory's rank follows from Lemma 3.8. Write $A' = \{d \in A \mid d \le a + b\}$. We have $\mathrm{Hb}(\mathrm{Sg}^{\mathrm{P}}(A')) = \mathrm{Hb}(A) \cap A'$ (use Proposition 2.4) and therefore $\det(a, b) = 1$ by the previous part applied on $\mathrm{Sg}(A')$. ∎

The section about subsemigroups of $\mathbb{N}_0^2$ is concluded by the promised example of subsemigroup with the infinite Carathéodory's rank.

4.11 Example. Let A be a subsemigroup of $\mathbb{N}_0^2$ generated by $A_0 = \{a_0, a_1, \dots\}$, where $a_n = (2^n, 2^n - 1)$, $n \in \mathbb{N}_0$. It is easily seen that $a_0 < a_1 < \cdots$ and $a_0 \lhd a_1 \lhd \cdots$, hence $a_{n+1} \notin \mathrm{cone}(\{a_0, \dots, a_n\}) = \mathrm{cone}(\{a_0, a_n\})$ and we have $\mathrm{Hb}(A) = A_0$. For every $n \in \mathbb{N}_0$ set

$$b_n = \sum_{i=0}^{n} a_i = (2^{n+1} - 1, 2^{n+1} - n - 2) \in \mathrm{Sg}(\{a_0, \dots, a_n\}).$$

We shall prove that $b_n = 1 \cdot a_0 + \cdots + 1 \cdot a_n$ is the unique representation of b in the form $k_0 a_0 + \cdots + k_n a_n$, where $k_i \in \mathbb{N}_0$ (note that $b_n < a_{n+1}$). We have

$$k_0 \times 2^0 + k_1 \times 2^1 + \cdots + k_n \times 2^n = 2^{n+1} - 1,$$
$$k_0 \times (2^0 - 1) + k_1 \times (2^1 - 1) + \cdots + k_n \times (2^n - 1) = 2^{n+1} - n - 2,$$

hence $\sum_{i=0}^n k_i = n + 1$ and Lemma 4.2 gives $k_0 = k_1 = \cdots = k_n = 1$. Consequently, A is an example of a semigroup with $CR(A) = \infty$.

(III) Subsemigroups of $\mathbb{N}_0^3$. If we are striving for an example of a pure subsemigroup A of $\mathbb{N}_0^m$ with $\dim \mathrm{Lin}(A) = m$, $|\mathrm{Hb}(A)| = \omega$ and $\mathcal{E}(A) \supsetneq \{0\}$, we have to start our search with $m = 3$ and $\operatorname{rank} \mathcal{E}(A) = 1$ (see Theorem 3.17).

4.12 Example. Let α be an irrational number, $0 < \alpha < 1$, and let $C = \mathrm{cone}_{\mathbb{R}}\{(1,0,0), (1,0,\alpha), (0,1,0), (0,1,1-\alpha)\} \subseteq (\mathbb{R}_0^+)^3$. Then $A = C \cap \mathbb{N}_0^3$ is a pure subsemigroup of $\mathbb{N}_0^3$ which is not finitely generated and $\mathcal{E}(A) = \mathbb{N}_0(1,1,1)$. (Similarly $A \times \mathbb{N}_0^p$, $p \in \mathbb{N}$, is a pure subsemigroup of $\mathbb{N}_0^{3+p}$ which is not finitely generated and $\mathcal{E}(A) = (\mathbb{N}_0(1,1,1)) \times \mathbb{N}_0^2$.)

Proof. It it not difficult to observe that $C = \{x \in (\mathbb{R}_0^+)^3 \mid \langle w, x \rangle \le 0\}$, where $w = (-\alpha, \alpha - 1, 1)$, and therefore A is a pure subsemigroup of $\mathbb{N}_0^3$. It is easily seen that A is

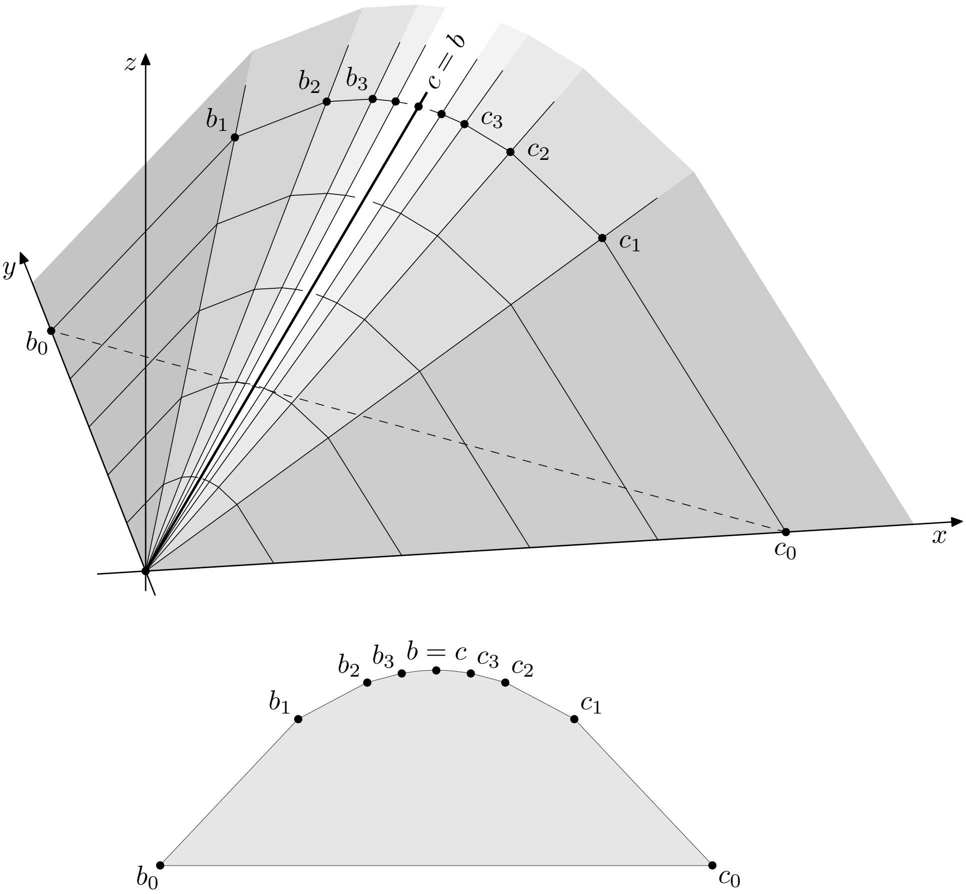

Fig. 3: The cone $A = \operatorname{cone}(B \cup C)$ viewed in $\mathbb{R}^3$ (z-axis scaled $5\times$) and $\operatorname{conv}(B \cup C)$ viewed in the hyperplane generated by the points b_0, c_0 and $b = c$ (z-axis scaled $3\times$).

not finitely generated. Indeed, if $C \cap (\mathbb{Q}_0^+)^3$ was a finitely generated cone in $\mathbb{Q}^3$, then $\big(C \cap (\mathbb{Q}_0^+)^3\big) \cap \big(\mathbb{Q}_0^+ \times \{0\} \times \mathbb{Q}_0^+\big) = \operatorname{cone}_{\mathbb{R}}\{(1,0,0),(1,0,\alpha)\} \cap (\mathbb{Q}_0^+)^3$ would be finitely generated (Corollary 1.18). But $\operatorname{cone}_{\mathbb{R}}(\{(1,0),(1,\alpha)\}) \cap (\mathbb{Q}_0^+)^2$ is not finitely generated in $\mathbb{Q}^2$ (by Section (II)), hence $C \cap (\mathbb{Q}_0^+)^3$ is not finitely generated in $\mathbb{Q}^3$.

If $a \in A$ and $a - (1,1,1) \in \mathbb{N}_0^3$, then $\langle w, a - (1,1,1)\rangle = \langle w, a\rangle - \langle w, (1,1,1)\rangle = \langle w, a\rangle - 0 \le 0$, hence $a - (1,1,1) \in C \cap \mathbb{N}_0^3 = A$. Consequently, $(1,1,1) \in \mathcal{E}(A)$ and $\mathcal{E}(A) \supseteq \mathbb{N}_0(1,1,1)$. Since A is not finitely generated, the dimension of $\operatorname{Lin}(\mathcal{E}(A))$ can not be 2 or 3 and thus $\mathcal{E}(A)$ *equals* $\mathbb{N}_0(1,1,1)$. ∎

4.13 Example. For every $n \in \mathbb{N}_0$ define (Fig. 3)

$$\begin{aligned} b_n &= (\Gamma_n, 2 - \Gamma_n, \Delta_n) \in (\mathbb{Q}_0^+)^3, \\ c_n &= (2 - \Gamma_n, \Gamma_n, \Delta_n) \in (\mathbb{Q}_0^+)^3, \end{aligned} \quad \text{where } \Gamma_n = \sum_{i=1}^{n} 1/2^i \text{ and } \Delta_n = \sum_{i=1}^{n} 1/4^i.$$

Let $b = \lim_{n\to\infty} b_n = (1,1,1/3) = \lim_{n\to\infty} c_n = c$, $B = \{b_n \mid n \in \mathbb{N}_0\} \cup \{b\}$ and $C = \{c_n \mid n \in \mathbb{N}_0\} \cup \{c\}$. Let $A = A_{\mathbb{Q}} = \operatorname{cone}(B \cup C)$, $A_{\mathbb{R}} = \operatorname{cone}_{\mathbb{R}}(B \cup C)$ and $A^* = A \cap \mathbb{N}_0^3$. Let $p \in \mathbb{N}_0$ and $\mathbb{T} \in \{\mathbb{Q}, \mathbb{R}\}$. Then

(i) $A_{\mathbb{T}} \times (\mathbb{T}_0^+)^p$ is not a finitely generated cone in $(\mathbb{T}_0^+)^{3+p}$;

(i*) $A^* \times \mathbb{N}_0^p$ is a pure subsemigroup of $\mathbb{N}_0^{3+p}$, which is not finitely generated, and $\operatorname{rank}(A^* \times \mathbb{N}_0^p) = 3 + p$;

(ii) $\partial(A_{\mathbb{T}} \times (\mathbb{T}_0^+)^p) = \Big(((\mathbb{T}_0^+)^2 \times \{0\}) \cup \bigcup_{n=0}^{\infty} \operatorname{cone}_{\mathbb{T}}(\{b_n, b_{n+1}\}) \cup \bigcup_{n=0}^{\infty} \operatorname{cone}_{\mathbb{T}}(\{c_n, c_{n+1}\}) \cup \mathbb{T}_0^+ b\Big) \times (\mathbb{T}_0^+)^p$ (the boundary being taken in $\mathbb{T}^{3+p}$);

(iii) $A_{\mathbb{T}} \times (\mathbb{T}_0^+)^p$ is a closed set in $\mathbb{T}^{3+p}$;

(iv) if $\ell = \{a + tv \mid t \in \mathbb{T}\}$, where $a, v \in \mathbb{T}^{3+p}$, $v \neq 0$, is a line in $\mathbb{T}^{3+p}$, then there are $t_1, t_2 \in \mathbb{T} \cup \{-\infty, \infty\}$ such that $\ell \cap (A_{\mathbb{T}} \times (\mathbb{T}_0^+)^p) = \{a + tv \mid t \in \mathbb{T},\ t_1 \leq t \leq t_2\}$;

(v) $A_{\mathbb{T}} \times (\mathbb{T}_0^+)^p = \operatorname{cone}_{\mathbb{T}}\big(\partial(A_{\mathbb{T}} \times (\mathbb{T}_0^+)^p)\big)$ (the boundary being taken in $\mathbb{T}^{3+p}$).

(Compare with Proposition 4.7, part (iii) with Corollary 1.18, part (iv) with Proposition 1.20 and part (v) with Proposition 1.21.)

Sketch of proof. It suffices to prove these assertions only for $p = 0$ and moreover, we can assume $\mathbb{T} = \mathbb{Q}$, since the arguments for $\mathbb{T} = \mathbb{R}$ and $\mathbb{T} = \mathbb{Q}$ are the same. The whole example relies on the fact that b_n and c_n are so chosen that $b_n \notin \operatorname{cone}((B \cup C) \setminus \{b_n\})$, $c_n \notin \operatorname{cone}((B \cup C) \setminus \{c_n\})$ and $b \notin \operatorname{cone}((B \cup C) \setminus \{b\})$. ∎

The rest of the thesis is devoted to the proof of the following theorem:

4.14 Theorem. *Let A be a pure subsemigroup of $\mathbb{N}_0^3$. Then $CR(A) = 3$.*

The proof is divided into a sequence of assertions (the final conclusion is at page 32). To shorten notation, we write $P(A)$, where $A \subseteq \mathbb{Q}^m$, for the set $\big\{\sum_{i=1}^n q_i a_i \mid n \in \mathbb{N}_0, q_i \in \mathbb{Q}_0^+, q_i < 1, a_i \in A\big\}$.

4.15 Proposition. *Let A be a pure subsemigroup of $\mathbb{N}_0^m$ and suppose that $\operatorname{Hb}(A) = \{0, a_1, \dots, a_n\}$, where $n \in \mathbb{N}$ and $a_1, \dots, a_n$ are nonzero and pairwise different. Let $a \in A$. Then there are $q_1, \dots, q_n \in \mathbb{Q}_0^+$ such that*

(i) $a = \sum_{i=1}^n q_i a_i$ and $\sum_{i=1}^n q_i$ is maximal possible (in sense of Proposition 1.8); let $i_1 < \cdots < i_s$ be all indices i such that $q_i > 0$,

(ii) the set $\{a_{i_1}, \dots, a_{i_s}\}$ is linearly independent and

(iii) $1 < \sum_{i=1}^s r_i < s-1 \leq m-1$ for every $p = r_1 a_{i_1} + \cdots + r_s a_{i_s} \in P(\{a_1, \dots, a_s\}) \cap \mathbb{N}_0^m$, $p \neq 0$, where $r_i \in \mathbb{Q}_0^+$, $r_i < 1$.

In other words, for every $a \in A$ there exists a linearly independent subset of $\operatorname{Hb}(A)$ for which (i) and (iii) hold.

Proof. We first find $q_1, \dots, q_n \in \mathbb{Q}_0^+$ satisfying (i) and (ii) as in Proposition 1.8. Without loss of generality we may assume $\{i_1, \dots, i_s\} = \{1, \dots, s\}$. Suppose now that there is an $h \in \operatorname{Hb}(A) \cap \operatorname{conv}(\{a_1, \dots, a_s\})$, $h \notin \{0, a_1, \dots, a_s\}$, and write $h = \sum_{i=1}^s q_i' a_i$, $q_i \in \mathbb{Q}_0^+$, $\sum_{i=1}^s q_i = 1$. Then

$$a = \varepsilon h + \sum_{i=1}^{s} (q_i - \varepsilon q_i') a_i, \quad \text{where } \varepsilon = \min\{q_i / q_i' \mid i \in \{1, \dots, s\},\ q_i' \neq 0\} \in \mathbb{Q}^+.$$

We have $q_i - \varepsilon q_i' \geq 0$ and $q_{i_0} - \varepsilon q_{i_0}' = 0$ for an i_0 for which $\varepsilon = q_{i_0} / q_{i_0}'$. Moreover, it holds $\varepsilon + \sum_{i=1}^s (q_i - \varepsilon q_i') = \sum_{i=1}^s q_i$ and the set $\{h, a_1, \dots, a_s\} \setminus \{a_{i_0}\}$ is linearly independent (the linear dependence of this set would imply the linear dependence of $\{a_1, \dots, a_s\}$). Thus we are allowed to *additionally suppose that $a_1, \dots, a_s$ are so chosen that* $\operatorname{conv}(\{a_1, \dots, a_s\}) \cap \mathbb{N}_0^m = \{a_1, \dots, a_s\}$.

Let $p = \sum_{i=1}^{s} r_i a_i \neq 0$ be as in (iii) and suppose on the contrary that $\sum_{i=1}^{s} r_i \leq 1$. Since $p \in A$, we have $p = \sum_{\ell=1}^{n} k_\ell a_\ell$ for some $k_\ell \in \mathbb{N}_0$ (not all zero). It is

$$a = \varepsilon p + \sum_{i=1}^{s} (q_i - \varepsilon r_i) a_i, \quad \text{where } \varepsilon \in \mathbb{Q}^+ \text{ is such that } q_i - \varepsilon r_i > 0,$$

thus $a = \sum_{\ell=1}^{n} \varepsilon k_\ell a_\ell + \sum_{i=1}^{s} (q_i - \varepsilon r_i) a_i$ and $\sum_{\ell=1}^{n} \varepsilon k_\ell + \sum_{i=1}^{s} (q_i - \varepsilon r_i) \geq \sum_{i=1}^{s} q_i$. The maximal property of $q_1, \dots, q_s$ (see (i)) implies that the equality occurs. This is possible only if $\sum_{i=1}^{s} r_i = 1$ and exactly one of k_ℓ's is equal to 1 and the others are zero. In other words, $p \in \operatorname{Hb}(A) \cap \operatorname{conv}(\{a_1, \dots, a_s\})$ and consequently $p \in \{a_1, \dots, a_s\}$, a contradiction with $p \in P(\{a_1, \dots, a_s\})$.

Thus we have $\sum_{i=1}^{s} r_i > 1$. If $r_i = 0$ for some i, then obviously $\sum_{i=1}^{s} r_i < s - 1$. Otherwise $p' = \sum_{i=1}^{s} (1 - r_i) a_i \neq 0$ is as in (iii) and we can proceed as above to obtain $\sum_{i=1}^{s} (1 - r_i) > 1$, which is equivalent to $\sum_{i=1}^{s} r_i < s - 1$. ∎

4.16 Lemma. *Let A be a pure subsemigroup of $\mathbb{N}_0^3$ and $\operatorname{Hb}(A) = \{0, a_1, \dots, a_n\}$, where $n \in \mathbb{N}$ and $a_1, \dots, a_n$ are nonzero and pairwise different. Let $a \in A$. Then*

(i) *there exists an $s \in \{1, 2, 3\}$ and $a_1, \dots, a_s \in \operatorname{Hb}(A)$ such that $\{a_1, \dots, a_s\}$ is linearly independent, $P(\{a_1, \dots, a_s\}) \cap \mathbb{N}_0^3 \subseteq \operatorname{Hb}(A)$ and $a \in \operatorname{cone}(\{a_1, \dots, a_s\})$.*

Suppose that $s = 3$ in (i) and without loss of generality that $\Delta = \det(a_1, a_2, a_3) > 0$. Then

(ii) *there is a $p = \sum_{i=1}^{3} r_i a_i \in P(\{a_1, a_2, a_3\}) \cap \mathbb{N}_0^3$, where $r_i \in \mathbb{Q}_0^+$ and $r_i < 1$, such that $\Delta(r_1 + r_2 + r_3) = \Delta + 1$ (Cramer's rule gives $r_1 = \det(p, a_2, a_3)/\Delta$, $r_2 = \det(a_1, p, a_3)/\Delta$ and $r_3 = \det(a_1, a_2, p)/\Delta$).*

Proof. (i) We may suppose $a \neq 0$. Let $a_1, \dots, a_s$, $1 \leq s \leq 3$, be the vectors from part (ii) of the previous proposition (again assume $\{i_1, i_2, \dots, i_s\} = \{1, \dots, s\}$). Suppose there is a $p \in (P(\{a_1, \dots, a_s\}) \cap \mathbb{N}_0^3) \setminus \operatorname{Hb}(A)$. We have $p = \sum_{i=1}^{s} r_i a_i$, where $r_i \in \mathbb{Q}_0^+$, $r_i < 1$, $\sum_{i=1}^{s} r_i < 2$ (4.15(iii)), and also $p = \sum_{\ell=1}^{n} k_\ell a_\ell$ for some $k_\ell \in \mathbb{N}_0$. Since $p \notin \operatorname{Hb}(A)$ is nonzero, it is $\sum_{\ell=1}^{n} k_\ell \geq 2$. Now we have similarly as above

$$a = \varepsilon p + \sum_{i=1}^{s} (q_i - \varepsilon r_i) a_i, \quad \text{where } \varepsilon \in \mathbb{Q}^+ \text{ is such that } q_i - \varepsilon r_i > 0,$$

thus $a = \sum_{\ell=1}^{n} \varepsilon k_\ell a_\ell + \sum_{i=1}^{s} (q_i - \varepsilon r_i) a_i$ and $\sum_{\ell=1}^{n} \varepsilon k_\ell + \sum_{i=1}^{s} (q_i - \varepsilon r_i) > \sum_{i=1}^{s} q_i$, a contradiction with 4.15(i).

(ii) We know from Proposition 1.22 that $P = P(\{a_1, a_2, a_3\})$ contains exactly $\Delta - 1$ nonzero integer points. Every $a \in \operatorname{cone}(\{a_1, a_2, a_3\}) \cap \mathbb{N}_0^3$ can be uniquely written in the form $\frac{1}{\Delta} \sum_{i=1}^{3} k_i a_i$, where $k_i \in \mathbb{N}_0$ (use Cramer's rule); define $\Omega(a) = k_1 + k_2 + k_3$. Part (i) of this lemma immediately gives $\Delta < \Omega(a) < 2\Delta$ for $0 \neq a \in P \cap \mathbb{N}_0^3$ (see 4.15(iii)). Thus Ω is a function assigning to each of $\Delta - 1$ nonzero integer points in P

one of $\Delta - 1$ values $\Delta + 1, \ldots, 2\Delta - 1$ and the proof is completed by showing that Ω is one-to-one on $P \cap \mathbb{N}_0^3$.

Let p_1 and p_2 be nonzero integer points in P such that $\Omega(p_1) = \Omega(p_2)$. Suppose moreover that $p_1 = \sum_{i=1}^3 q_i a_i$ and $p_2 = \sum_{i=1}^3 r_i a_i$, where $r_i, q_i \in \mathbb{Q}_0^+$, $0 \leq q_1 < 1$ and $0 < r_i < 1$, and define $p_2' = \sum_{i=1}^3 (1 - r_i) a_i \in P \cap \mathbb{N}_0^3$. We have $\Omega(p_1 + p_2') = \Omega(p_1 + a_1 + a_2 + a_3 - p_2) = \Omega(p_1) + 3 - \Omega(p_2) = 3$, thus $\sum_{i=1}^3 (q_i + (1 - r_i)) = 3$. It follows that $\sum_{i=1}^3 \{q_i + (1 - r_i)\} \in \mathbb{N}_0$, where $\{\cdot\}$ denotes the fractional part. The point $p = \sum_{i=1}^3 \{q_i + (1 - r_i)\} a_i$ is an integer point in P and $\Omega(p) \in \Delta \mathbb{N}_0$, thus $\Omega(p) = 0$ (recall: possible nonzero values are $\Delta + 1, \ldots, 2\Delta - 1$) and consequently $q_i = 1 - r_i$ for $i = 1, 2, 3$ and $p_1 = p_2$. If $p_2 = r_{i_1} a_{i_1} + r_{i_2} a_{i_2}$, where $i_1, i_2 \in \{1, 2, 3\}$, $i_1 \neq i_2$ and $r_{i_1}, r_{i_2} \in \mathbb{Q}^+$, define $p_2' = (1 - r_{i_1}) a_{i_1} + (1 - r_{i_2}) a_{i_2}$ and proceed similarly. ∎

Proof of Theorem 4.14. We may suppose that $0 \in A$ and that A is finitely generated (Lemma 3.8). Take an arbitrary $a \in A$, $a \neq 0$, and apply Lemma 4.16. If $s = 1$, then $a = k a_1$ for some $k \in \mathbb{N}$. If $s = 2$, then there are $k_1, k_2 \in \mathbb{N}_0$ such that $a_3 = a - k_1 a_1 - k_2 a_2 \in P(\{a_1, a_2\})$. The point a_3 lies in $\mathrm{Hb}(A)$ and $a = k_1 a_1 + k_2 a_2 + a_3$. The interesting case is $s = 3$: let $p = \sum_{i=1}^3 r_i a_i$ and Δ be as in 4.16(ii). If $r_i = 0$ for some i, we proceed similarly as in the case $s = 2$; thus assume $r_1, r_2, r_3 \in \mathbb{Q}^+$. The Hilbert basis of the semigroup $A' = \mathrm{Sg}^{\mathrm{p}}(\{a_1, a_2, a_3\}) \subseteq A$ equals $(P(\{a_1, a_2, a_3\}) \cap \mathbb{N}_0^3) \cup \{a_1, a_2, a_3\} \subseteq \mathrm{Hb}(A)$ (use 2.5 and 3.6). It is obvious that

$$(*) \quad \Big(P(\{a_1, a_2, p\}) \cup P(\{a_2, a_3, p\}) \cup P(\{a_3, a_1, p\}) \Big) \cap \mathbb{N}_0^3 \supseteq \mathrm{Hb}(A') \setminus \{a_1, a_2, a_3, p\}$$

and that $\{a_1, a_2, p\}$, $\{a_2, a_3, p\}$ and $\{a_3, a_1, p\}$ are linearly independent sets. At least the point 0 lies in the union on the left side, thus counting integer points gives

$$\det(a_1, a_2, p) + \det(p, a_2, a_3) + \det(a_1, p, a_3) - 2 \geq \Delta - 1$$

But the equality occurs here due to 4.16(ii). Consequently, we must have the equality in $(*)$ and the sets $P(\{a_1, a_2, p\}) \setminus \{0\}$, $P(\{a_2, a_3, p\}) \setminus \{0\}$ and $P(\{a_3, a_1, p\}) \setminus \{0\}$ must form a partition of $\mathrm{Hb}(A') \setminus \{0, a_1, a_2, a_3, p\}$. The point a lies in at least one of the sets $\mathrm{cone}(\{a_1, a_2, p\})$, $\mathrm{cone}(\{a_2, a_3, p\})$ and $\mathrm{cone}(\{a_3, a_1, p\})$. Suppose for symmetric reasons that $a \in \mathrm{cone}(\{a_1, a_2, p\})$ and put $A'' = \mathrm{Sg}^{\mathrm{p}}(\{a_1, a_2, p\})$. It follows from Proposition 3.6 that $\mathrm{Hb}(A'') \subseteq (P(\{a_1, a_2, p\}) \cap \mathbb{N}_0^3) \cup \{a_1, a_2, p\} \subsetneq \mathrm{Hb}(A')$ (in fact, the equality occurs due to 2.5). Thus we have reduced the proof of $CR(A) = 3$ to the proof of $CR(A'') = 3$, where A'' is pure, finitely generated and $\mathrm{Hb}(A'') \subsetneq \mathrm{Hb}(A') \subseteq \mathrm{Hb}(A)$. Theorem 4.14 then follows recursively. ∎

Bibliography

[4ti2] 4ti2 team. *4ti2—A software package for algebraic, geometric and combinatorial problems on linear spaces*. Available at http://www.4ti2.de.

[Bar02] Barvinok, A. *A course in convexity*. Graduate Studies in Mathematics, vol. 54. American Mathematical Society, 2002.

[Br99] Bruns, W. Diskrete Kegel und der Satz von Carathéodory. In: *Wege der Wissenschaft*. Universitätsverlag Rasch, Osnabrück, 1999, 361–371. Used english version 'Discrete cones and Carathéodory's theorem' available at author's website http://www.home.uni-osnabrueck.de/wbruns.

[Br98] Bruns, W., Gubeladze, J., Henk, M., Martin, A., Weismantel, R. A counterexample to an integer analogue of Carathéodory's theorem. *Journal für die reine und angewandte Mathematik*. **1999**(510), 179–185.

[He09] Hemmecke, R., Takemura, A., Yoshida, R. Computing holes in semigroups and its applications to transportation problems. *Contributions to Discrete Mathematics*. North America, **4**(1) (2009). Available at http://cdm.ucalgary.ca/cdm/index.php/cdm/article/view/149.

[Jež12] Ježek, J., Kala, V., Kepka, T. Finitely generated algebraic structures with various divisibility conditions. *Forum Mathematicum*. **24**(2) (2012), 379–397.

[Jež10] Ježek, J., Kepka, T. Finitely generated commutative division semirings. *Acta Univ. Carolin. Math. Phys.* **51**(1) (2010), 3–27.

[Kal09] Kala, V., Kepka, T., Korbelář, M. Notes on commutative parasemifields. *Comment. Math. Univ. Carolin.* **50**(4) (2009), 521–533.

[Kal10] Kala, V., Kepka, T. Commutative parasemifields finitely generated as semirings. *Acta Univ. Carolin. Math. Phys.* **51**(1) (2010), 49–56.

[Kep09] Kepka, T. *Notes on subsemigroups of* $\mathbb{N}_0^m(+)$. Handwritten notes.

[Mat02] Matoušek, J. *Lectures on discrete geometry*. Graduate Texts in Mathematics, vol. 212. Springer, 2002.

[Sch86] Schrijver, A. *Theory of linear and integer programming*. Wiley, 1986.

[Seb90] Sebő, A. Hilbert bases, Carathéodory's theorem and combinatorial optimization. In: *Proceedings of the 1st Integer Programming and Combinatorial Optimization Conference*. University of Waterloo Press, Waterloo, Canada, 1990, 431–456.

[Hig98] Higham, N. *Handbook of writing for the mathematical sciences.* Miscellaneous Titles in Applied Mathematics Series. SIAM, 1998.

[Trz95] Trzeciak, J. *Writing mathematical papers in English: a practical guide.* European Mathematical Society, 1995.