Primary ideals of finitely generated commutative cancellative monoids

J.C. Rosales *, J.I. García-García

Departamento de Álgebra, Universidad de Granada, E-18071 Granada, Spain

Received 7 March 2000; accepted 8 March 2001
Submitted by J. Dias da Silva

Abstract

We give a characterization of primary ideals of finitely generated commutative monoids and in the case of finitely generated cancellative monoids we give an algorithmic method for deciding if an ideal is primary or not. Finally we give some properties of primary elements of a cancellative monoid and an algorithmic method for determining the primary elements of a finitely generated cancellative monoid. © 2001 Elsevier Science Inc. All rights reserved.

Keywords: Semigroup; Ideal; Primary element

0. Introduction

All semigroups appearing in this paper are commutative. For this reason in the sequel we will omit this adjective. We denote by \( \mathbb{Z} \) and \( \mathbb{N} \) the set of integers and the set of nonnegative integers, respectively.

The works [2,4] start to develop a theory which studies ideals of semigroups. This theory is similar to the theory of Ideals of Commutative Rings. For this reason many of the definitions and theorems in Commutative Algebra have their analogues in the theory of Ideals of Semigroups (see [1]) and this is why the concept of primary ideal plays an important role in the theory of Ideals of Semigroup. More recently, the problem of factorization in domains has been translated, in a more general setting, to the

* This paper was supported by the project DGES PB96-1424.
* Corresponding author. Tel.: +34-58-242863; fax: +34-58-243289.
E-mail addresses: jrosales@ugr.es (J. Rosales), jigg@ugr.es (J.I. García-García).
problem of factorization in monoids (see [3,6,8,10]). For this reason new interesting concepts appear. One of them is the concept of primary element of a monoid.

Every finitely generated cancellative monoid is isomorphic to a monoid of the form \( \mathbb{N}^p/\sim_M \) with \( M \) a subgroup of \( \mathbb{Z}^p \) and \( \sim_M \) a congruence on \( \mathbb{N}^p \) defined by \( a \sim_M b \) if \( a - b \in M \). In this paper, our goal is to give the following two algorithms:

(1) An algorithm to determine if an ideal of \( \mathbb{N}^p/\sim_M \) is primary.
(2) An algorithm to compute the set of primary elements of \( \mathbb{N}^p/\sim_M \).

The first of these two algorithms is essentially based on two results: an algorithmic characterization of the primary ideals of \( \mathbb{N}^p \) and an algorithm for computing the primitive elements of a congruence of the form \( \sim_M \). The calculations of the primitive elements of \( \sim_M \) have already been studied in [12] and they are based on finding the nonnegative elements of a subgroup of \( \mathbb{Z}^n \). To solve this problem we can use some methods which can be found in [5,12,13]. The concept of Archimedean component was introduced by Tamura and Kimura in [15]. This concept plays an important role in Algorithm (2). To obtain this algorithm we need to compute from a system of generators of \( \sim_M \) the Archimedean components of \( \mathbb{N}^p/\sim_M \) (we can do that using an algorithm presented in [12]). Once we have computed these sets, this algorithm uses Algorithm (1) and it returns the set of primary elements of \( \mathbb{N}^p/\sim_M \).

The contents of this paper are organized as follows. In Section 1 we prove that primary ideals of finitely generated monoids are quotients of primary ideals of \( (\mathbb{N}^k, +) \) for some positive integer \( k \) and we characterize the primary ideals of \( \mathbb{N}^k \). In Section 2 we give Algorithm (1), and Algorithm (2) is described in Section 3.

1. Primary ideals of a finitely generated monoid

An ideal of a monoid \((S, +)\) is a nonempty subset \(I\) of \(S\) fulfilling that for all \(x \in I\) and for all \(s \in S\) the element \(x + s \in I\). An ideal \(I\) is a primary ideal if it fulfills that for all \(x, y \in S\) with \(x + y \in I\) and \(x \not\in I\), there exists \(k \in \mathbb{N}\setminus\{0\}\) such that \(ky \in I\).

Let \((S, +)\) be the monoid generated by \(\{s_1, \ldots, s_p\}\), \(\varphi : \mathbb{N}^p \to S\) the monoid epimorphism defined by \(\varphi(a_1, \ldots, a_p) = a_1s_1 + \cdots + a_ps_p\) and \(R\) the kernel congruence of \(\varphi\), which is defined by \(xRy\) if \(\varphi(x) = \varphi(y)\). It is known that \(S\) is isomorphic to the quotient monoid \(\mathbb{N}^p/R\). In this section, our aim is to describe primary ideals of \(\mathbb{N}^p/R\). With this purpose we introduce the following result (see [7]).

**Lemma 1.** Let \(I\) be an ideal of a finitely generated monoid \((S, +)\). There exists a finite subset \(B\) of \(S\) such that \(I = B + S = \{b + s \mid b \in B, \ s \in S\}\).

In the rest of this section we will assume that \(R\) is a congruence on \(\mathbb{N}^p\), \(I\) an ideal of \(\mathbb{N}^p/R\) and \(E(I) = \{x \in \mathbb{N}^p \mid [x] \in I\}\), where \([x]\) denotes the \(R\)-class of \(\mathbb{N}^p\) containing \(x\).
The following two results can be easily deduced. They can be found in [8, Proposition 6.9].

**Lemma 2.** Let $I$ be an ideal of $\mathbb{N}^P/R$. The set $E(I)$ is an ideal of $\mathbb{N}^P$.

Using this fact we obtain the following property.

**Proposition 3.** An ideal $I$ is a primary ideal of $\mathbb{N}^P/R$ if and only if $E(I)$ is a primary ideal of $\mathbb{N}^P$.

The following proposition characterizes primary ideals of $\mathbb{N}^P$. For every $i \in \{1, \ldots, p\}$, $e_i$ denotes the element of $\mathbb{N}^P$ having all its coordinates equal to zero except the $i$th which is equal to one.

Denote by $\leq$ the order on $\mathbb{N}^P$ defined by $(a_1, \ldots, a_p) \leq (b_1, \ldots, b_p)$ if $a_i \leq b_i$ for all $i \in \{1, \ldots, p\}$. By Dickson’s Lemma (see [12]), if $A$ is a subset of $\mathbb{N}^P$, then $\text{Minimals}_{\leq}(A)$, the set of minimal elements of $A$ with respect to $\leq$, is finite. Observe that if $J$ is an ideal of $\mathbb{N}^P$, then $J = \text{Minimals}_{\leq}(J) + \mathbb{N}^P$.

**Proposition 4.** Let $J$ be an ideal of $\mathbb{N}^P$. The following statements are equivalent:
1. $J$ is a primary ideal of $\mathbb{N}^P$,
2. if $(x_1, \ldots, x_p) \in \text{Minimals}_{\leq}(J)$ and $x_i \neq 0$, then $te_i \in \text{Minimals}_{\leq}(J)$ for some $t \in \mathbb{N}\setminus\{0\}$.

**Proof.** (1) $\Rightarrow$ (2): Let $x = (x_1, \ldots, x_p) \in \text{Minimals}_{\leq}(J)$ and $x_i \neq 0$. Then $x - e_i, e_j \in \mathbb{N}^P$, $(x - e_i) + e_j \in J$ and $x - e_j \not\in J$. Using that $J$ is a primary ideal, we deduce that there exists $t \in \mathbb{N}\setminus\{0\}$ such that $te_i \in J$. Let $k = \min\{t \in \mathbb{N}\setminus\{0\} | te_i \in J\}$. This leads to $ke_i \in \text{Minimals}_{\leq}(J)$, since if $y \in J$ and $y \leq ke_i$ then $y = [0, \ldots, 0]$ and so $y \preceq x$ in $J$, contradicting the fact that $x$ is minimal in $J$.

(2) $\Rightarrow$ (1): Let $x, y \in \mathbb{N}^P$ such that $x + y \in J$ and $x \not\in J$. Since $x + y \in J$, we have that $x + y = m + z$ for some $m \in \text{Minimals}_{\leq}(J)$ and some $z \in \mathbb{N}^P$. Furthermore, since $J$ is an ideal, $x \not\in J$ and $m \in J$, we have $m \not\preceq x$ and on the other hand $m < x + y$. Thus there exists $i \in \{1, \ldots, p\}$ such that $m_i > x_i$ and $m_i < x_i + y_i$. Hence $y_i > m_i - x_i > 0$ and so $y_i - e_i \geq 0$. Therefore $y - e_i \in \mathbb{N}^P$. By hypothesis there exists $t \in \mathbb{N}\setminus\{0\}$ such that $te_i \in \text{Minimals}_{\leq}(J) \subseteq J$. Finally, since $y - e_i \in \mathbb{N}^P$, we obtain $ty = t(y - e_i) + te_i \in J$. $\square$

We finish this section describing a method to determine whether an ideal $I$ of $\mathbb{N}^P/R$ is primary. If $I$ is an ideal of $\mathbb{N}^P/R$, then there exist $m_1, \ldots, m_q \in \mathbb{N}^P$ such that

$$I = \{[m_1], \ldots, [m_q]\} + \mathbb{N}^P/R.$$

Thus we obtain

$$E(I) = \{x \in \mathbb{N}^P \mid xR(m_i + s) \text{ for some } i \in \{1, \ldots, q\} \text{ and some } s \in \mathbb{N}^P\}.$$
So, if we compute the set $\text{Minimals}_{\leq}(E(I))$ from $m_1, \ldots, m_q$ and from a system of generators of $R$, then using Proposition 4 we can decide if $E(I)$ is a primary ideal of $\mathbb{N}^p$. Finally, Proposition 3 tell us if $I$ is primary. Observe that the set $\text{Minimals}_{\leq}(E(I))$ can be computed using Algorithm 16 of [14].

In the next section we show that in the case of $\mathbb{N}^p/R$ being a cancellative monoid ($[a] + [c] = [b] + [c]$ implies $[a] = [b]$) we can obtain an algorithmic method for deciding whether an ideal is primary or not.

2. An algorithmic method for determining whether an ideal of a finitely generated cancellative monoid is a primary ideal

Let $R$ be a congruence on $\mathbb{N}^p$. Denote by $M_R = \{a - b \mid (a, b) \in R\}$. Clearly $M_R$ is a subgroup of $\mathbb{Z}^p$. Conversely, if $M$ is a subgroup of $\mathbb{Z}^p$, then the binary relation defined on $\mathbb{N}^p$ by $\sim_M = \{(a, b) \in \mathbb{N}^p \times \mathbb{N}^p \mid a - b \in M\}$ is a congruence. It is known (see for instance [11] or [12]) that the monoid $\mathbb{N}^p/R$ is cancellative if and only if $R = \sim_{M_R}$. Hence every finitely generated cancellative monoids is isomorphic to a monoid of the form $\mathbb{N}^p/\sim_M$ with $M$ a subgroup of $\mathbb{Z}^p$. Our goal in this section is to give an algorithmic method for determining from $M$ whether an ideal $I$ of $\mathbb{N}^p/\sim_M$ is a primary ideal. This algorithm will allow us to decide from $\{m_1, \ldots, m_q\} \subseteq \mathbb{N}^p$ and a basis of $M$, if the ideal $I = \{[m_1], \ldots, [m_q]\} + \mathbb{N}^p/\sim_M$ is primary.

The following lemma can be easily proved.

**Lemma 5.** Let $I = \{[m_1], \ldots, [m_q]\} + \mathbb{N}^p/\sim_M$ and $I_j = \{[m_j]\} + \mathbb{N}^p/\sim_M$ for $j = 1, \ldots, q$. The following conditions are satisfied.

1. $I_j$ is an ideal of $\mathbb{N}^p/\sim_M$ for all $j \in \{1, \ldots, q\}$.
2. $I = I_1 \cup \cdots \cup I_q$.
3. $E(I) = E(I_1) \cup \cdots \cup E(I_q)$.
4. $\text{Minimals}_{\leq}(E(I)) \subseteq \text{Minimals}_{\leq}(E(I_1)) \cup \cdots \cup \text{Minimals}_{\leq}(E(I_q))$.

We now focus our attention on finding an algorithmic method for determining the set $\text{Minimals}_{\leq}(E(I_i))$. To this end we introduce the concept of irreducible element of a congruence. An element $(a, b)$ of a congruence $R$ on $\mathbb{N}^p$ is **irreducible** if it cannot be expressed as $(a, b) = (a_1, b_1) + (a_2, b_2)$ with $(a_1, b_1), (a_2, b_2) \in R \setminus \{(0, 0)\}$. Denote by $\mathcal{I}_R$ the set of irreducible elements of $R$. Note that $R$ is a submonoid of $\mathbb{N}^p \times \mathbb{N}^p$ because $(0, 0) \in R$ and if $(a, b), (c, d) \in R$, then $(a + c, b + d) \in R$. Thus $\mathcal{I}_R$ is a minimal system of generators of the monoid $R$. The most interesting properties of $\mathcal{I}_{\sim_M}$ are: it is finite, since $M$ is a subgroup of $\mathbb{Z}^p$, and there exists an algorithmic method to compute it [12] from a basis of $M$. In fact, by Corollary 8.8 in [12] we get an algorithm for computing the primitive elements of $\sim_M$, using now Proposition 8.4 in [12] we can easily obtain the irreducible elements of $\mathbb{N}^p/\sim_M$. Now, assume that $\mathcal{I}_{\sim_M} = \{(\alpha_1, \beta_1), \ldots, (\alpha_t, \beta_t)\}$. We will show how to compute $\text{Minimals}_{\leq}(E(I_i))$ from $\mathcal{I}_{\sim_M}$.
Lemma 6. Let

$$\mathcal{B}_i = \{ (a_1, \ldots, a_t) \in \mathbb{N}^t \mid a_1 \beta_1 + \cdots + a_t \beta_t = m_i + s \text{ for some } s \in \mathbb{N}^p \}.$$ 

If \( x \in \text{Minimals} \leq (\mathcal{E}(I_i)) \), then there exists \((a_1, \ldots, a_t) \in \text{Minimals} \leq (\mathcal{B}_i)\) such that \( x = a_1 \alpha_1 + \cdots + a_t \alpha_t \).

Proof. If \( x \in \text{Minimals} \leq (\mathcal{E}(I_i)) \), then \([x] \in I_i = \{[m_i]\} + \mathbb{N}^p/\sim_M\). Hence there exists \( s \in \mathbb{N}^p \) such that \( x \sim_M (m_i + s) \). Applying the fact that \( \mathcal{A}_M \) is a system of generators of \( \sim_M \) as a monoid, we deduce that there exists \((a_1, \ldots, a_t) \in \mathbb{N}^t \) such that \( (x, m_i + s) = a_1(\alpha_1, \beta_1) + \cdots + a_t(\alpha_t, \beta_t) \), whence \( x = a_1 \alpha_1 + \cdots + a_t \alpha_t \). Assume that \((a_1, \ldots, a_t) \notin \text{Minimals} \leq (\mathcal{B}_i)\). In this case there exists \((b_1, \ldots, b_t) < (a_1, \ldots, a_t)\) such that \( b_1 \beta_1 + \cdots + b_t \beta_t = m_i + u \) for some \( u \in \mathbb{N}^p \). Let \( y = b_1 \alpha_1 + \cdots + b_t \alpha_t \). Then \( y \in \mathcal{E}(I_i) \) and \( y < x \) which contradicts the minimality of \( x \). \( \square \)

Thus the problem of determining if an ideal is primary is reduced to compute the set \( \text{Minimals} \leq (\mathcal{B}_i) \) because from this set, applying Lemma 6, it can be determined the set \( \text{Minimals} \leq (\mathcal{E}(I_i)) \).

Suppose \( m_i = (m_{i_1}, \ldots, m_{i_p}) \) and \( \beta_k = (\beta_{k_1}, \ldots, \beta_{kp}) \). For every \( j \in \{1, \ldots, p\} \) define

$$\mathcal{B}_{ij} = \{ (a_1, \ldots, a_t) \in \mathbb{N}^t \mid a_1 \beta_{1j} + \cdots + a_t \beta_{tj} = m_{ij} + s \text{ for some } s \in \mathbb{N} \}.$$ 

Clearly the sets \( \mathcal{B}_{ij} \) are ideals of \( \mathbb{N}^t \) and \( \mathcal{B}_i = \mathcal{B}_{i_1} \cap \cdots \cap \mathcal{B}_{i_p} \).

The following lemma shows a way to determine \( \text{Minimals} \leq (\mathcal{B}_i) \) from \( \text{Minimals} \leq (\mathcal{B}_{ij}) \). For every pair of elements

- \( a = (a_1, \ldots, a_t), b = (b_1, \ldots, b_t) \in \mathbb{N}^t \)

set

$$a \lor b = (\text{maximum}\{a_1, b_1\}, \ldots, \text{maximum}\{a_t, b_t\}) .$$

Lemma 7. Let \( A = \{x_1, \ldots, x_r\} + \mathbb{N}^t \) and \( B = \{y_1, \ldots, y_s\} + \mathbb{N}^t \) be ideals of \( \mathbb{N}^t \). Then

$$A \cap B = \{x_1 \lor y_1, \ldots, x_1 \lor y_s, x_2 \lor y_1, \ldots, x_2 \lor y_s, \ldots, x_r \lor y_1, \ldots, x_r \lor y_s\} + \mathbb{N}^p.$$ 

Proof. If \( a \in A \cap B \), then \( a \in A \) and \( a \in B \). Thus there exist \( x_i \) and \( y_j \) such that \( a \geq x_i \) and \( a \geq y_j \). Hence \( a \geq x_i \lor y_j \).

Conversely, if \( a \geq x_i \lor y_j \), then \( a \geq x_i \) and \( a \geq y_j \) and therefore \( a \in A \cap B \). \( \square \)

In order to solve our problem we only need to know \( \text{Minimals} \leq (\mathcal{B}_{ij}) \). But this set can be easily computed using the following result.
Let $\mathbb{Q}$ be the set of rational numbers and for all $x \in \mathbb{Q}$ denote by $\lceil x \rceil$ the element \(\text{Minimum}\{t \in \mathbb{Z} \mid x \leq t\}\).

**Lemma 8.** Let $n_1, \ldots, n_t, n \in \mathbb{N}$ and
\[
A = \{ (a_1, \ldots, a_t) \in \mathbb{N}^t \mid a_1 n_1 + \cdots + a_t n_t = n + s \text{ for some } s \in \mathbb{N} \}.
\]
If $(a_1, \ldots, a_t) \in \text{Minimals}_{\leq}(A)$, then one of the following conditions is fulfilled.
(1) If $n_j = 0$, then $a_j = 0$.
(2) If $n_j \neq 0$, then $a_j \leq \lceil n/n_j \rceil$.

**Proof.** (1) It follows from the fact that if $n_j = 0$ and $(a_1, \ldots, a_t) \in A$, then
\[
a_1 n_1 + \cdots + a_t n_t = a_1 n_1 + \cdots + a_{j-1} n_{j-1} + a_j 0 + a_{j+1} n_{j+1} + \cdots + a_t n_t
\]
and therefore $(a_1, \ldots, a_{j-1}, 0, a_{j+1}, \ldots, a_t) \in A$.
(2) We only have to take into account that if $(a_1, \ldots, a_t) \in A$ and $a_j > \lceil n/n_j \rceil$, then
\[
(a_1, \ldots, a_{j-1}, a_j - 1, a_{j+1}, \ldots, a_t) \in A.
\]

Using all the exposed in this section we give the following algorithm which determines if the ideal $I = \{ [m_1], \ldots, [m_q] \} + \mathbb{N}_p / \sim_M$ with $m_1 = (m_{11}, \ldots, m_{1p}), \ldots, m_q = (m_{q1}, \ldots, m_{qp})$ is a primary ideal of $\mathbb{N}_p / \sim_M$.

**Algorithm 9.**

**Input:** The set $m_1, \ldots, m_q$ and a basis of $M$.

**Output:** If $I = \{ [m_1], \ldots, [m_q] \} + \mathbb{N}_p / \sim_M$ is a primary ideal of $\mathbb{N}_p / \sim_M$, then return “True”, and “False” otherwise.

1. Compute $\mathfrak{S}_M = \{ (\alpha_1, \beta_1), \ldots, (\alpha_t, \beta_t) \}$ (see Corollary 8.8 in [12]).
2. For every $i \in \{1, \ldots, q\}$ and every $j \in \{1, \ldots, p\}$ compute the set $\text{Minimals}_{\leq}(\mathfrak{B}_{ij})$, where
\[
\mathfrak{B}_{ij} = \{ (a_1, \ldots, a_t) \in \mathbb{N}^t \mid a_1 \beta_{1j} + \cdots + a_t \beta_{tj} \geq m_{ij} \}
\]
(in this step we use Lemma 8).
3. For every $i \in \{1, \ldots, q\}$ compute $\text{Minimals}_{\leq}(\mathfrak{B}_i)$, where
\[
\mathfrak{B}_i = \mathfrak{B}_{i1} \cap \cdots \cap \mathfrak{B}_{ip}
\]
(use Lemma 7).
4. Compute $\text{Minimals}_{\leq}(\mathfrak{B})$, where $\mathfrak{B} = \mathfrak{B}_1 \cup \cdots \cup \mathfrak{B}_q$.
5. Compute $\text{Minimals}_{\leq}(\mathfrak{A})$, where
\[
\mathfrak{A} = \{ a_1 \alpha_1 + \cdots + a_t \alpha_t \mid (a_1, \ldots, a_t) \in \text{Minimals}_{\leq}(\mathfrak{B}) \}
\]
6. Check if $\text{Minimals}_{\leq}(\mathfrak{A}) + \mathbb{N}_p$ is a primary ideal of $\mathbb{N}_p$ (in this step we use Proposition 4).
7. If $\text{Minimals}_{\leq}(\mathfrak{A}) + \mathbb{N}_p$ is a primary ideal of $\mathbb{N}_p$, then return “True”, otherwise return “False”.

We finish this section giving the following example.

**Example 10.** Let

\[ M = \left\{ (x_1, x_2, x_3) \in \mathbb{Z}^3 \mid \begin{array}{c} x_1 + x_2 + x_3 = 0 \\ x_1 - x_2 - x_3 = 0 \end{array} \right\}, \]

\[ m_1 = (1, 2, 1) \text{ and } m_2 = (2, 0, 1). \text{ We apply the above algorithm for determining if } 
I = \langle m_1 \rangle, \langle m_2 \rangle + \mathbb{N}^3/\sim \text{ is a primary ideal of } \mathbb{N}^3/\sim \text{ or not.} \]

**Step 1.** Applying the results of [12] we obtain

\[ \mathfrak{Z}_{\sim} = \{(e_1, e_1), (e_2, e_2), (e_3, e_3), (e_3, e_2), (e_2, e_3)\}, \]

where \( e_1 = (1, 0, 0), e_2 = (0, 1, 0) \) and \( e_3 = (0, 0, 1) \). Thus, we get

\[ \alpha_1 = e_1, \quad \alpha_2 = e_2, \quad \alpha_3 = e_3, \quad \alpha_4 = e_3, \quad \alpha_5 = e_2, \]
\[ \beta_1 = e_1, \quad \beta_2 = e_2, \quad \beta_3 = e_3, \quad \beta_4 = e_2, \quad \beta_5 = e_3. \]

**Step 2.**

\[ \mathfrak{B}_{11} = \{(a_1, a_2, a_3, a_4, a_5) \in \mathbb{N}^5 \mid a_1 + a_2 + a_3 + a_4 + a_5 \geq 1\}, \]
\[ \mathfrak{B}_{12} = \{(a_1, a_2, a_3, a_4, a_5) \in \mathbb{N}^5 \mid a_1 + a_2 + a_3 + a_4 \geq 2\}, \]
\[ \mathfrak{B}_{13} = \{(a_1, a_2, a_3, a_4, a_5) \in \mathbb{N}^5 \mid a_1 + a_2 + a_3 + a_4 + a_5 \geq 1\}, \]
\[ \mathfrak{B}_{21} = \{(a_1, a_2, a_3, a_4, a_5) \in \mathbb{N}^5 \mid a_1 + a_2 + a_3 \geq 2\}, \]
\[ \mathfrak{B}_{22} = \{(a_1, a_2, a_3, a_4, a_5) \in \mathbb{N}^5 \mid a_1 + a_2 + a_3 + a_4 + a_5 \geq 0\}, \]
\[ \mathfrak{B}_{23} = \{(a_1, a_2, a_3, a_4, a_5) \in \mathbb{N}^5 \mid a_1 + a_2 + a_3 + a_4 \geq 1\}. \]

Thus we have:

\[ \text{Minimals}_< (\mathfrak{B}_{11}) = \{(1, 0, 0, 0, 0)\}, \]
\[ \text{Minimals}_< (\mathfrak{B}_{12}) = \{(0, 2, 0, 0, 0), (0, 1, 0, 1, 0), (0, 0, 0, 2, 0)\}, \]
\[ \text{Minimals}_< (\mathfrak{B}_{13}) = \{(0, 0, 1, 0, 0), (0, 0, 0, 0, 1)\}, \]
\[ \text{Minimals}_< (\mathfrak{B}_{21}) = \{(2, 0, 0, 0)\}, \]
\[ \text{Minimals}_< (\mathfrak{B}_{22}) = \{(0, 0, 0, 0)\}, \]
\[ \text{Minimals}_< (\mathfrak{B}_{23}) = \{(0, 0, 1, 0, 0), (0, 0, 0, 0, 1)\}. \]

**Step 3.** First we compute the set Minimals_<(\mathfrak{B}_1), where

\[ \mathfrak{B}_1 = \mathfrak{B}_{11} \cap \mathfrak{B}_{12} \cap \mathfrak{B}_{13}. \]

\[ \mathfrak{B}_{11} \cap \mathfrak{B}_{12} = \{(1, 0, 0, 0, 0) \cup (0, 2, 0, 0, 0), \]
\[ (1, 0, 0, 0, 0) \cup (0, 1, 0, 1, 0), \]
\[ (1, 0, 0, 0, 0) \cup (0, 0, 0, 2, 0)\} + \mathbb{N}^5 \]
\[ = \{(1, 2, 0, 0, 0), (1, 1, 0, 1, 0), (1, 0, 0, 2, 0)\} + \mathbb{N}^5. \]

\[ (\mathfrak{B}_{11} \cap \mathfrak{B}_{12}) \cap \mathfrak{B}_{13} = \{(0, 0, 1, 0, 0) \cup (1, 2, 0, 0, 0), (0, 0, 1, 0, 0) \]
\[ \cup (1, 1, 0, 1, 0), (0, 0, 1, 0, 0) \]
\[ \cup (1, 0, 0, 2, 0), (0, 0, 0, 0, 1) \]. \]
We now compute the set \( \text{Minimals} \leq B \) \( \subseteq \mathbb{N}^5 \).

\[
\begin{align*}
\text{Minimals} & \leq B = \{(1, 2, 1, 0, 0), (1, 1, 1, 1, 0), (1, 0, 1, 2, 0), \\
& \quad (1, 2, 0, 0, 1), (1, 1, 0, 1, 1), (1, 0, 0, 2, 1)\} + \mathbb{N}^5.
\end{align*}
\]

Hence,

\[
\text{Minimals}_\leq (B_1) = \{(1, 2, 1, 0, 0), (1, 1, 1, 1, 0), \\
& \quad (1, 0, 1, 2, 0), (1, 2, 0, 0, 1), \\
& \quad (1, 1, 0, 1, 1), (1, 0, 0, 2, 1)\}.
\]

We now compute the set \( \text{Minimals}_\leq (B_2) \), where

\[
B_2 = B_{21} \cap B_{22} \cap B_{23}.
\]

Using again the same reasoning we have that

\[
\text{Minimals}_\leq (B_2) = \{(2, 0, 1, 0, 0), (2, 0, 0, 0, 1)\}.
\]

**Step 4.** We compute the set \( \text{Minimals}_\leq (B) \), where \( B = B_1 \cup B_2 \). Then

\[
\text{Minimals}_\leq (B) = \{(1, 2, 1, 0, 0), (1, 1, 1, 1, 0), (1, 0, 1, 2, 0), \\
& \quad (1, 2, 0, 0, 1), (1, 1, 0, 1, 1), (1, 0, 0, 2, 1), \\
& \quad (2, 0, 1, 0, 0), (2, 0, 0, 0, 1)\}.
\]

**Step 5.** First, we compute the set \( \mathfrak{A} \):

\[
\begin{align*}
\mathfrak{A} & = \{e_1 + 2e_2 + e_3, e_1 + e_2 + e_3 + e_3, e_1 + e_3 + 2e_3, e_1 + 2e_2 + e_2, \\
& \quad e_1 + e_2 + e_3 + e_2, e_1 + 2e_2 + e_2, 2e_1 + e_3, 2e_1 + e_2\} \\
& = \{(1, 2, 1), (1, 1, 2), (1, 0, 3), (1, 3, 0), (1, 2, 1), (1, 1, 2), \\
& \quad (2, 0, 1), (2, 1, 0)\}.
\end{align*}
\]

Hence,

\[
\text{Minimals}_\leq (\mathfrak{A}) = \{(1, 2, 1), (1, 1, 2), (1, 0, 3), (1, 3, 0), (2, 0, 1), (2, 1, 0)\}.
\]

**Step 6.** Applying Proposition 4, we easily deduce that \( \text{Minimals}_\leq (\mathfrak{A}) + \mathbb{N}^3 \) is not a primary ideal of \( \mathbb{N}^3 \).

**Step 7.** The algorithm returns “False” and therefore \( I \) is not a primary ideal of \( \mathbb{N}^3 / \sim_M \).
3. Primary elements of a cancellative monoid

Let \((S, +)\) be a monoid and \(\mathcal{U}(S) = \{x \in S \mid x + y = 0 \text{ for some } y \in S\}\) its group of units. An element \(a \in S\setminus\mathcal{U}(S)\) is a primary element of \(S\) if \(\{a\} + S\) is a primary ideal of \(S\). In this section, our aim is to show how the elements of this kind are distributed in a cancellative monoid. The principal results used for this purpose were given by Tamura and Kimura [15] (see also [12]). If \((S, +)\) is a monoid, then we have a binary relation \(\mathcal{N}\) defined by \(a \mathcal{N} b\) if there exist \(k_1, k_2 \in \mathbb{N}\setminus\{0\}\) and \(s_1, s_2 \in S\) such that \(k_1a = b + s_1\) and \(k_2b = a + s_2\). Then \(\mathcal{N}\) is a congruence on \(S\) and the quotient monoid \(S/\mathcal{N}\) is a semilattice (it is a semigroup with only idempotent elements) and every \(\mathcal{N}\)-class is a subsemigroup of \(S\). These \(\mathcal{N}\)-classes are known as the Archimedean components of \(S\) and we will denote them by \([a]\). Since \(S/\mathcal{N}\) is a semilattice, the binary relation \(\leq\) defined on \(S/\mathcal{N}\) by \([a]\) \(\leq\) \([b]\) if \([a] + [b] = [b]\) is an order relation (it satisfies reflexive, antisymmetric and transitive laws). Furthermore, \(\mathcal{U}(S) = [0] = \text{Minimum}_{\leq}(S/\mathcal{N})\).

It is known that if \((S, +)\) is a cancellative monoid, then this monoid is contained in a group and therefore we can write \(x - y\) when \(x, y \in S\).

**Lemma 11.** If \((S, +)\) is a cancellative monoid and \(a\) is a primary element of \(S\), then \([a]\) \(\in\) Minimals\(_{\leq}(S/\mathcal{N}\setminus\{[0]\})\).

**Proof.** Let \([b]\) \(\in\) \(S/\mathcal{N}\setminus\{[0]\}\) such that \([b]\) \(\leq\) \([a]\). Since \([b]\) \(\leq\) \([a]\), we have that \([a + b]\) = \([a]\) + \([b]\) = \([a]\), whence \((a + b)\mathcal{N} a\). Therefore we can assert that there exist \(k \in \mathbb{N}\setminus\{0\}\) and \(s \in S\) such that \(ka = a + b + s\). If for all \(t \in \mathbb{N}\) we have \(s - ta \in S\), then \(s - (k - 1)a = s' \in S\) and \(ka = a + b + (k - 1)a + s'\). Thus we deduce that \(b + s' = 0\), which contradicts with \([b]\) \(\neq\) \([0]\) = \(\mathcal{U}(S)\). Hence there exist \(t \in \mathbb{N}\) and \(c \notin \{a\} + S\) such that \(s = ta + c\) and consequently we have that \((k - t - 1)a = b + c\) with \(c \notin \{a\} + S\). Since \(k - t - 1 > 0\), otherwise \(b \in \mathcal{U}(S)\), we obtain that \(b + c \in \{a\} + S\). Using now the fact that \(\{a\} + S\) is a primary ideal we deduce that there exists \(\overline{k} \in \mathbb{N}\setminus\{0\}\) such that \(\overline{k}b \in \{a\} + S\). This means that \(\overline{k}b = a + \overline{s}\) for some \(\overline{s} \in S\). Finally, as \(ka = b + (a + s)\), we conclude that \(a\mathcal{N} b\), whence \([a]\) = \([b]\). \(\square\)

The following two results can be easily deduced. They can also be found in Proposition 1.2 of [9].

**Lemma 12.** Let \((S, +)\) be a cancellative monoid and \(a, b \in S\) be two primary elements such that \(a\mathcal{N} b\). Then the element \(a + b\) is a primary element of \(S\).

**Lemma 13.** Let \((S, +)\) be a cancellative monoid, \(a \in S\setminus\mathcal{U}(S)\), \(b \in S\) such that \(a + b\) is a primary element. Then \(a\) is a primary element of \(S\).
Lemma 14. Let \((S, +)\) be a cancellative monoid, \(a\) be a primary element and \(b \in S\) such that \(aN(b)\). Then \(b\) is a primary element of \(S\).

Proof. By hypotheses there exist \(k \in \mathbb{N}\setminus\{0\}\) and \(c \in S\) such that \(ka = b + c\). Since \(a\) is primary, applying Lemma 12 we obtain that \(ka\) is primary element. Hence \(b + c\) is primary and \(b \not\in \mathcal{U}(S)\) (note that \(b \in [[a]] \neq \mathcal{U}(S)\)). Finally, using Lemma 13 we conclude that \(b\) is a primary element. \(\square\)

The following theorem summarizes all the results given so far in this section.

Theorem 15. Let \((S, +)\) be a cancellative monoid and \(\mathcal{P}(S)\) be the set of primary elements of \(S\). Then there exists a family \(\{C_i \mid i \in \Delta\}\) of elements of \(\text{Minimals}_{\leq}(S/\mathcal{N} \setminus \{[[0]]\})\) such that \(\mathcal{P}(S) = \bigcup_{i \in \Delta} C_i\).

We finish this section describing an algorithm for computing the set of primary elements of a finitely generated cancellative monoid.

Let \(M\) be a subgroup of \(\mathbb{Z}^p\) and \(S = \mathbb{N}^p/\sim_M\) (recall the definition of \(\sim_M\) given in Section 2). In [12] an algorithm for computing a system of generators of the congruence \(\sim_M\) is given (note that Proposition 8.3 in [12] assures that the primitive elements of \(\sim_M\) generate \(\sim_M\) as a congruence). In [12] it also appears an algorithm for calculating the Archimedean components of \(S\) from a system of generators of \(\sim_M\) and it is proved that the number of Archimedean components of \(\mathbb{N}^p/\sim_M\) is less than or equal to \(2^p\).

Let \(C\) be an Archimedean component of \(S = \mathbb{N}^p/\sim_M\). Let

\[
\text{Supp}(C) = \{i_1, \ldots, i_r\}
= \left\{ i \in \{1, \ldots, p\} \mid \text{there exists } (x_1, \ldots, x_p) \in \mathbb{N}^p, \right. \\
\left. x_i \neq 0, [(x_1, \ldots, x_p)] \in C \right\}
\]

and

\[
I_C = \left\{ (x_1, \ldots, x_r) \in \mathbb{N}^r \mid [x_1 e_{i_1} + \cdots + x_r e_{i_r}] \in C \right\}
\]

where \(e_i\) is the \(p\)-tuple with all its coordinates equal to zero except the \(i\)th which is equal to one. In this setting, \(I_C\) is an ideal of \(\mathbb{N}^r\) and

\[
C = \left\{ [x_1 e_{i_1} + \cdots + x_r e_{i_r}] \mid (x_1, \ldots, x_r) \in I_C \right\}.
\]

In [12] it is shown how the set

\[
\text{Supp}(C) \mid C \text{ is an Archimedean component of } S
\]

can be computed from a system of generators of \(\sim_M\). Using this method and Theorem 15 we can determine \(\mathcal{P}(S)\), the set of primary elements of \(S\). Firstly, observe that from [12] it is deduced that if \(C_1, C_2 \in S/\mathcal{N}\), then \(C_1 \leq C_2\) if and only if
Supp(C₁) ⊆ Supp(C₂) (recall the definition of ≤ given at the beginning of this section). Thus we can determine the set Minimals_{≤}(S/Δ \{[[0]]\}) (recall that by Theorem 15 we know that all primary elements of S belong to some of these Archimedean components). Assume that we have computed the set Minimals_{≤}(S/Δ \{[[0]]\}) = \{C₁, \ldots, Cₗ\}. Now we take \( m₁ \in C₁, \ldots, mₗ \in Cₗ \) (note that if Supp(C) = \{e₁, \ldots, eₗ\}, then \([e₁ + \cdots + eₗ] \in C\)). Now with Algorithm 9 we can determine which ideals of the set \([m₁] + S, \ldots, [mₗ] + S\) are primary ideals. Assume that these primary ideals are \([m₁₁] + S, \ldots, [mₗₖ] + S\). Then, using the definition of primary element and Theorem 15, we have that \( P(S) = C₁₁ \cup \cdots \cup Cₗₖ \).

We now illustrate computing the set of primary elements of a monoid.

Example 16. Let M be the subgroup of \( \mathbb{Z}^6 \) generated by

\[
\{(2, 5, -3, -2, 0, 0), (0, 0, 0, 2, -8)\}
\]

and \( S \equiv \mathbb{N}^6 / \sim_M \). The defining equations of M are

\[
\begin{align*}
x₁ &= 0 \pmod{2}, \\
x₁ - x₂ + x₃ &= 0, \\
x₁ + x₄ &= 0, \\
5x₁ - 2x₂ &= 0, \\
4x₅ + x₆ &= 0.
\end{align*}
\]

First, we compute the set Minimals_{≤}(S/Δ \{[[0]]\}) and we obtain:

\[
\begin{align*}
C₁ &= \{(x₁, 0, 0, 0, 0, 0) \mid x₁ \geq 1\}, \\
C₂ &= \{(0, x₂, 0, 0, 0, 0) \mid x₂ \geq 1\}, \\
C₃ &= \{(0, 0, x₃, 0, 0, 0) \mid x₃ \geq 1\}, \\
C₄ &= \{(0, 0, 0, x₄, 0, 0) \mid x₄ \geq 1\}, \\
C₅ &= \{(0, 0, 0, x₅, x₆) \mid x₅ \geq 1 \text{ or } x₆ \geq 1\}.
\end{align*}
\]

By Lemma 11, if an element \( a \in S \) is primary, then there exists \( i \in \{1, 2, 3, 4, 5\} \) such that \( a \in Cᵢ \). We also have that if \( a \in Cᵢ \) is a primary element, then \( Cᵢ \subseteq P(S) \). We take now the elements \( x₁ = [(1, 0, 0, 0, 0, 0)], x₂ = [(0, 1, 0, 0, 0, 0)], x₃ = [(0, 0, 1, 0, 0, 0)], x₄ = [(0, 0, 0, 1, 0, 0), x₅ = [(0, 0, 0, 0, 1, 0), x₆ = [(0, 0, 0, 0, 1, 0)] \) which belong to \( C₁, C₂, C₃, C₄ \) and \( C₅ \), respectively. Using Algorithm 9 for checking if the ideal generated by each one of these elements is primary, we obtain Table 1. The first column is the column of the elements \( xᵢ \). In the second column are shown the sets of minimals of the ideals \( E(xᵢ + S) \) with \( i \in \{1, 2, 3, 4, 5\} \). The third answers whether the element \( xᵢ \) is a primary element (YES) or not (NO). Thus we obtain \( P(S) = C₅ \).
Table 1

<table>
<thead>
<tr>
<th>$x_i$</th>
<th>Minimals $\subseteq (E(x_i + S))$</th>
<th>Is $x_i$ primary?</th>
</tr>
</thead>
<tbody>
<tr>
<td>[(1, 0, 0, 0, 0, 0)]</td>
<td>{(1, 0, 0, 0, 0, 0), (0, 0, 3, 2, 0, 0)}</td>
<td>NO</td>
</tr>
<tr>
<td>[(0, 1, 0, 0, 0, 0)]</td>
<td>{(0, 1, 0, 0, 0, 0), (0, 0, 3, 2, 0, 0)}</td>
<td>NO</td>
</tr>
<tr>
<td>[(0, 0, 1, 0, 0, 0)]</td>
<td>{(0, 0, 1, 0, 0, 0), (2, 5, 0, 0, 0, 0)}</td>
<td>NO</td>
</tr>
<tr>
<td>[(0, 0, 0, 1, 0, 0)]</td>
<td>{(0, 0, 0, 1, 0, 0), (2, 5, 0, 0, 0, 0)}</td>
<td>NO</td>
</tr>
<tr>
<td>[(0, 0, 0, 0, 1, 0)]</td>
<td>{(0, 0, 0, 0, 1, 0), (0, 0, 0, 0, 0, 8)}</td>
<td>YES</td>
</tr>
</tbody>
</table>

Acknowledgement

We would like to thank the referee for his comments and suggestions.

References