On the Number of Factorizations of an Element in an Atomic Monoid

Scott T. Chapman  
Trinity University, schapman@trinity.edu

Juan Ignacio García-García

Pedro A. García Sánchez

José Carlos Rosales

Follow this and additional works at: http://digitalcommons.trinity.edu/math_faculty

Part of the Mathematics Commons

Repository Citation

This Article is brought to you for free and open access by the Mathematics Department at Digital Commons @ Trinity. It has been accepted for inclusion in Mathematics Faculty Research by an authorized administrator of Digital Commons @ Trinity. For more information, please contact jcostanz@trinity.edu.
On the number of factorizations of an element
in an atomic monoid

S.T. Chapman, a, *, 1 J.I. García-García, b
P.A. García-Sánchez, b and J.C. Rosales b

a Trinity University, Department of Mathematics, 715 Stadium Drive,
San Antonio, TX 78212-7200, USA
b Departamento de Álgebra, Universidad de Granada, E-18071 Granada, Espagne

Received 20 November 2001; accepted 15 January 2002

Abstract

Let S be a reduced commutative cancellative atomic monoid. If s is a nonzero element
of S, then we explore problems related to the computation of η(s), which represents the
number of distinct irreducible factorizations of s ∈ S. In particular, if S is a saturated
submonoid of \( \mathbb{N}^d \), then we provide an algorithm for computing the positive integer r(s)
for which

\[
0 < \lim_{n \to \infty} \frac{\eta(s^n)}{n^{r(s)-1}} < \infty.
\]

We further show that r(s) is constant on the Archimedean components of S. We apply the
algorithm to show how to compute

\[
\lim_{n \to \infty} \frac{\eta(s^n)}{n^{r(s)-1}}
\]

and also consider various stability conditions studied earlier for Krull monoids with finite
divisor class group.

© 2002 Elsevier Science (USA). All rights reserved.
1. Introduction

The study of factorization properties of a commutative cancellative monoid has been an active area of research in the recent mathematical literature. In this paper, we continue an investigation begun in the papers [1,2,8] concerning the number of different factorizations of an element into a product of irreducible elements. In a multiplicative monoid $S$, if we set $a \simeq b$ if and only if $a|b$ and $b|a$, then the factor monoid $S/\simeq$ is called the reduction of $S$. By the results of [7] or [15], the study of the factorization properties of a commutative cancellative monoid $S$ is equivalent to the study of the same properties in $S/\simeq$. Thus, throughout the remainder of this paper, we assume that all monoids are commutative, cancellative, and reduced.

If $(S, \cdot)$ is such a monoid with minimal system of generators $\{s_1, \ldots, s_p\}$, then it is well known that $S$ is atomic (i.e., every nonzero element of $S$ can be written as a product of irreducible elements of $S$) and that the set of atoms (or irreducible elements) of $S$ is $A(S) = \{s_1, \ldots, s_p\}$. For a given $s \in S$ denote by

- $\eta(s)$ the number of factorizations of $s$ into irreducibles,
- $R(s) = \{(k_1, \ldots, k_p) \in \mathbb{N}^p \mid s_1^{k_1} \cdots s_p^{k_p} = s^k$ for some $k \in \mathbb{N} \setminus \{0\}\},$ and
- $r(s)$ the dimension of $L_\mathbb{Q}(R(s))$, the $\mathbb{Q}$-vector space spanned by $R(s)$.

From [8] we deduce the following result.

**Theorem 1.1.** Let $S$ be a finitely generated reduced cancellative commutative monoid and let $s \in S$. There exists a rational positive constant $A(s) \in \mathbb{Q}$ such that

$$\eta(s^n) = A(s)n^{r(s)-1} + O\left(n^{r(s)-2}\right).$$

Suppose $S$ is a monoid satisfying the hypothesis of Theorem 1.1 and $s \in S \setminus \{0\}$. We break the results of this paper into three sections. After this introduction, Section 2 gives an upper bound for $r(s)$ in terms of a presentation of the monoid $S$. We further show that the function $r$ is constant on the Archimedean components of $S$. Section 3 contains the principal goal of this work, an algorithm to compute $r(s)$ from a presentation of $S$ when $S$ is a saturated submonoid of $\mathbb{N}^d$. In Section 4, we consider the limit

$$\overline{\eta}(s) = \lim_{n \to \infty} \frac{\eta(s^n)}{n^{r(s)-1}}.$$ 

In [1] and [2] this limit is used to characterize Dedekind domains and Block Monoids with particular finite class groups. In view of Theorem 1.1, $\overline{\eta}(s)$ is exactly the constant $A(s)$, and we will show how, given the results in Section 3, the formula given in [9] for $A(s)$ can be used to compute this value. We close with a brief discussion of stability properties examined for more specific structures in [2] and [1].
2. Bounds on $r(s)$ and Archimedean components

Let $(S, \cdot)$ be a finitely generated reduced cancellative commutative monoid. As we pointed out above, $S$ is then atomic and $S = \langle A(S) \rangle$. If $A(S) = \{s_1, \ldots, s_p\}$, then we can define the map

$$\varphi : \mathbb{N}^p \to S, \quad \varphi(a_1, \ldots, a_p) = s_1^{a_1} \cdots s_p^{a_p},$$

which is usually known as the factorization homomorphism of $S$. In [14, Chapter 1] it is shown that $\ker(\varphi) = \{(a, b) \in \mathbb{N}^p \times \mathbb{N}^p \mid \varphi(a) = \varphi(b)\} = \sim_M$, where $M$ is a subgroup of $\mathbb{Z}^p$ such that $M \cap \mathbb{N}^p = \{0\}$ and $\sim_M$ is the congruence on $\mathbb{N}^p$ defined by $a \sim_M b$ if $a - b \in M$. Hence, $S$ is isomorphic to the monoid $(\mathbb{N}^p / \sim_M, +)$ (see [14, Chapter 3] for a complete description of the equations of $M$ in terms of the generators of $S$). Thus, for studying factorization problems on $S$, we can restrict ourselves to the study of factorization problems on $\mathbb{N}^p / \sim_M$ with $M \cap \mathbb{N}^p = \{0\}$, where we will use additive notation. For $x \in \mathbb{N}^p$, $[x]_{\sim_M}$ denotes the $\sim_M$-class of $x$. Observe that $\eta([x]_{\sim_M}) = \#([x]_{\sim_M})$ and that $[x]_{\sim_M} = (x + M) \cap \mathbb{N}^p$. Actually, for a given $s \in S$, the set $\varphi^{-1}(s)$ contains the coefficients of all the factorizations of $s$ in terms of $s_1, \ldots, s_p$. Moreover, for every $x \in \varphi^{-1}(s)$, $[x]_{\sim_M} = \varphi^{-1}(s)$. In this setting,

$$R(s) = R([x]_{\sim_M}) = \bigcup_{n \in \mathbb{N}} [nx]_{\sim_M}.$$

**Lemma 2.1.** Let $x \in \mathbb{N}^p \setminus \{0\}$ and $M$ be a subgroup of $\mathbb{Z}^p$ such that $M \cap \mathbb{N}^p = \{0\}$. Take $m_1, \ldots, m_t \in M$. The following conditions are equivalent.

1. The vectors $m_1, \ldots, m_t$ are $\mathbb{Q}$-linearly independent.
2. The vectors $x, x + m_1, \ldots, x + m_t$ are $\mathbb{Q}$-linearly independent.

**Proof.** (1) $\Rightarrow$ (2). Assume that $z_0 x + z_1 (x + m_1) + \cdots + z_t (x + m_t) = 0$ with $z_0, \ldots, z_t \in \mathbb{Z}$. Then $(z_0 + \cdots + z_t)x = (-z_1) m_1 + \cdots + (-z_t) m_t$. Since $M \cap \mathbb{N}^p = \{0\}$, we obtain that $z_0 + \cdots + z_t = 0$, whence $(-z_1) m_1 + \cdots + (-z_t) m_t = 0$. Since $\{m_1, \ldots, m_t\}$ are $\mathbb{Q}$-linearly independent, we conclude that $z_1 = \cdots = z_t = 0$, which leads to $z_0 = 0$.

(2) $\Rightarrow$ (1). Assume that $m_1, \ldots, m_t$ are not linearly independent. We can assume without loss of generality that there exist $q_1, \ldots, q_t \in \mathbb{Q}$ such that $m_t = q_1 m_1 + \cdots + q_{t-1} m_{t-1}$. Then

$$q_1(x + m_1) + \cdots + q_{t-1}(x + m_{t-1}) - (q_1 + \cdots + q_{t-1} - 1)x = x + m_t,$$

which contradicts the fact that $x, x + m_1, \ldots, x + m_t$ are linearly independent. □

**Proposition 2.2.** Let $M$ be a subgroup of $\mathbb{Z}^p$ such that $M \cap \mathbb{N}^p = \{0\}$. Then

1. for every $x \in \mathbb{N}^p$, $r([x]_{\sim_M}) \leq \operatorname{rank}(M) + 1$,
(2) \( r([1, \ldots, 1]_{\sim_M}) = \text{rank}(M) + 1. \)

**Proof.** (1) Let \( \{a_1, \ldots, a_t\} \subseteq \mathbb{N}^P \) be a basis of \( L_{\mathbb{Q}}(R([x]_{\sim_M})). \) From the definition of \( R([x]_{\sim_M}) \), we deduce that there exist \( k_1, \ldots, k_t \in \mathbb{N} \setminus \{0\} \) such that \( a_1 \in [k_1x]_{\sim_M}, \ldots, a_t \in [k_tx]_{\sim_M}. \) If \( m = k_1 \cdots k_t, \) then \( \frac{m}{k_1}a_1, \ldots, \frac{m}{k_t}a_t \in [mx]_{\sim_M}. \) Furthermore, these elements are linearly independent and by Lemma 2.1, the same holds for \( \frac{m}{k_2}a_2 - \frac{m}{k_1}a_1, \ldots, \frac{m}{k_t}a_t - \frac{m}{k_1}a_1 \in M. \) Hence \( t - 1 \leq \text{rank}(M). \)

(2) Let \( t = \text{rank}(M) \) and let \( \{m_1, \ldots, m_t\} \) be a basis of \( M. \) Clearly there exists \( n \in \mathbb{N} \setminus \{0\} \) such that \( n(1, \ldots, 1) + m_1, \ldots, n(1, \ldots, 1) + m_t \in \mathbb{N}^P. \) Moreover, using again Lemma 2.1, we have that the elements \( n(1, \ldots, 1), n(1, \ldots, 1) + m_1, \ldots, n(1, \ldots, 1) + m_t \) are linearly independent. Since these elements belong to \( [n(1, \ldots, 1)]_{\sim_M}, \) they all belong to \( R([x]_{\sim_M}), \) whence \( r([1, \ldots, 1]_{\sim_M}) \geq t + 1. \) Using (1) we now conclude that \( r(\cdot) = t + 1 = \text{rank}(M) + 1. \) \( \square \)

We see next how the map \( r \) behaves on the Archimedean components of a monoid. This behavior will allow us in a practical manner to compute \( r. \) On a commutative monoid \( (S, \cdot) \) define the following binary relation: \( a \sim b \) if there exist \( n, m \in \mathbb{N} \setminus \{0\} \) and \( x, y \in S \) such that \( a^n = xb \) and \( b^m = ya. \) In [16] it is shown that \( \sim \) is a congruence on \( S. \) The \( \sim \)-classes are called the Archimedean components of \( S. \) We will now show that \( r(x) = r(y) \) whenever \( x \sim y \) (of course assuming the hypothesis of Theorem 1.1). We begin with a lemma which follows directly from the definitions of \( r \) and \( \eta. \)

**Lemma 2.3.** Let \( (S, \cdot) \) be a finitely generated reduced cancellative commutative monoid and take \( s \in S \setminus \{1\}. \) Then

(1) \( r(s) = r(s^k) \) for all \( k \in \mathbb{N} \setminus \{0\}, \)
(2) \( \eta(s) \leq \eta(ss') \) for all \( s' \in S. \)

**Proposition 2.4.** Let \( (S, \cdot) \) be a finitely generated reduced cancellative commutative monoid. Take \( x, y, z \in S \) and \( k \in \mathbb{N} \setminus \{0\} \) such that \( x^k = yz. \) Then \( r(y) \leq r(x). \)

**Proof.** By Lemma 2.3, we have that \( \eta(y^n) \leq \eta(y^n z^n) \) for all \( n \in \mathbb{N}. \) Applying Theorem 1, we obtain that \( r(y) \leq r(yz) = r(x^k). \) Again using Lemma 2.3 we obtain \( r(y) \leq r(x). \) \( \square \)

As a consequence of this result we obtain the following.
Corollary 2.5. Let \((S, \cdot)\) be a finitely generated reduced cancellative commutative monoid. If \(x, y \in S \setminus \{1\}\) are such that \(xN y\), then \(r(x) = r(y)\).

In [14, Chapter 13] there is a procedure for computing the Archimedean components of a monoid of the form \(\mathbb{N}^p/\sim_M\) once we are given the subgroup \(M\). Hence, if we want to compute the image of the map \(r: \mathbb{N}^p/\sim_M \setminus \{0\}\) \(\rightarrow \mathbb{N}\), then we only have to choose an element \([x_i]_\sim_M\) from each of the Archimedean components of \(\mathbb{N}^p/\sim_M\) different from the one containing \([0]_\sim_M\) and compute \(r([x_i]_\sim_M)\) (there are at most \(2^p\) Archimedean components in \(\mathbb{N}^p/\sim_M\)). In the next section, we will show how to compute \(r([x]_\sim_M)\) from \(x\) and \(M\).

Example 2.6. Let \(S\) be a numerical monoid (i.e., the submonoid of \((\mathbb{N}, +)\) minimally generated by \(\{n_1, \ldots, n_k\}\)). Then \(S\) has two Archimedean components: \([0]\) and \(S \setminus \{0\}\). Moreover \(S \cong \mathbb{N}^k/\sim_M\), with \(M = \{(x_1, \ldots, x_k) \in \mathbb{Z}^k | n_1 x_1 + \cdots + n_k x_k = 0\}\) (see Proposition 3.1 in [14]). Since \(\text{rank}(M) = k - 1\), Proposition 2.2 and Corollary 2.5 state that \(r(s) = k\) for all \(s \in S \setminus \{0\}\). Hence the only values of \(r\) are 0 and \(k\), which means that we may encounter atomic monoids with big "gaps" in the image of \(r\).

3. An algorithm for computing \(r(s)\)

For \(a = (a_1, \ldots, a_p) \in \mathbb{N}^p\), set \(\text{supp}(a) = \{i | a_i \neq 0\}\). If \(X\) is a subset of \(\mathbb{N}^p\), take \(\text{supp}(X)\) to be \(\bigcup_{x \in X} \text{supp}(x)\). For every \(i \in \{1, \ldots, p\}\) denote by \(e_i\) the element in \(\mathbb{N}^p\) all of whose coordinates are zero except the \(i\)th which is equal to one.

Lemma 3.1. Let \(x \in \mathbb{N}^p \setminus \{0\}\) and let \(M\) be a subgroup of \(\mathbb{Z}^p\) such that \(M \cap \mathbb{N}^p = \{0\}\). Assume without loss of generality that \(\text{supp}(R([x]_\sim_M)) = \{1, \ldots, q\}\). Then \(r([x]_\sim_M) = r([e_1 + \cdots + e_q]_\sim_M)\).

Proof. Since \(\text{supp}(x) \subseteq \{1, \ldots, q\}\), there exist \(k \in \mathbb{N} \setminus \{0\}\) and \(y \in \mathbb{N}^p\) such that \(k(e_1 + \cdots + e_q) = x + y\). By Proposition 2.4, this implies that \(r([x]_\sim_M) \leq r([e_1 + \cdots + e_q]_\sim_M)\).

Since \(\{1, \ldots, q\} \subseteq \text{supp}(R([x]_\sim_M))\), there exist \(y_1, \ldots, y_q \in \mathbb{N}^p\) and \(k_1, \ldots, k_q \in \mathbb{N} \setminus \{0\}\) such that \([e_i]_\sim_M + [y_i]_\sim_M = [k_i x]_\sim_M\) for all \(i \in \{1, \ldots, q\}\). This implies that \([e_1 + \cdots + e_q]_\sim_M + [y_1 + \cdots + y_q]_\sim_M = [(k_1 + \cdots + k_q)x]_\sim_M\).

Using once again Proposition 2.4, we obtain \(r([e_1 + \cdots + e_q]_\sim_M) \leq r([x]_\sim_M)\). Define on \(\mathbb{N}^q\) the congruence \(\tau\) by
\[(x_1, \ldots, x_q) \tau (y_1, \ldots, y_q) \quad \text{if} \quad (x_1, \ldots, x_q, 0, \ldots, 0) \sim_M (y_1, \ldots, y_q, 0, \ldots, 0).\]

Since \(\mathbb{N}^p / \sim_M\) is cancellative and reduced, it follows that \(\mathbb{N}^q / \tau\) is also cancellative and reduced (note that \(\tau\) is the restriction of \(\sim_M\) to the first \(q\)-coordinates). Thus there exists a subgroup \(M'\) of \(\mathbb{Z}^q\) such that \(\tau = \sim_{M'}\). Moreover, once we know the defining equations of \(M\),

\[
\begin{align*}
\alpha_{11}x_1 + \cdots + \alpha_{1p}x_p &\equiv 0 \pmod{\delta_1}, \\
\vdots & \\
\alpha_{k1}x_1 + \cdots + \alpha_{kp}x_p &\equiv 0 \pmod{\delta_k}, \\
\alpha_{(k+1)1}x_1 + \cdots + \alpha_{(k+1)p}x_p &= 0, \\
\vdots & \\
\alpha_{n1}x_1 + \cdots + \alpha_{np}x_p &= 0,
\end{align*}
\]

the equations of \(M'\) are just

\[
\begin{align*}
\alpha_{11}x_1 + \cdots + \alpha_{1q}x_q &\equiv 0 \pmod{\delta_1}, \\
\vdots & \\
\alpha_{k1}x_1 + \cdots + \alpha_{kq}x_q &\equiv 0 \pmod{\delta_k}, \\
\alpha_{(k+1)1}x_1 + \cdots + \alpha_{(k+1)q}x_q &= 0, \\
\vdots & \\
\alpha_{n1}x_1 + \cdots + \alpha_{nq}x_q &= 0.
\end{align*}
\]

**Proposition 3.2.** Let \(x, M,\) and \(M'\) be as above. Then \(r([x]_{\sim_M}) = \text{rank}(M') + 1.\)

**Proof.** Let \(n \in \mathbb{N} \setminus \{0\}\). Define

\[f : [n(1, \ldots, 1)]_{\sim_{M'}} \to [n(e_1 + \cdots + e_q)]_{\sim_M}\]

by

\[f(y_1, \ldots, y_q) = (y_1, \ldots, y_q, 0, \ldots, 0).\]

If \((y_1, \ldots, y_q) \sim_{M'} n(1, \ldots, 1),\) then

\[(y_1, \ldots, y_q, 0, \ldots, 0) \sim_M n(e_1 + \cdots + e_q),\]

which means that \(f\) is well defined. Clearly \(f\) is injective. We see next that it is also surjective. If \((y_1, \ldots, y_p) \sim_M n(e_1 + \cdots + e_q),\) then \(y_{q+1} = \cdots = y_p = 0,\) because otherwise we could deduce that \(\text{supp}(R([x]_{\sim_M})) \neq \{1, \ldots, q\}\). Hence \(f(y_1, \ldots, y_q) = (y_1, \ldots, y_p).\) This implies that \(f\) is bijective and therefore
Applying now Theorem 1.1, we obtain that
\[ r([1, \ldots, 1]_M) = r([e_1 + \cdots + e_q]_M) . \]

Finally, Proposition 2.2 and Lemma 3.1 assert that \( r([x]_M) = \text{rank}(M') + 1 \).

In view of the preceding results, for computing \( r([x]_M) \) it suffices to determine \( \text{supp}(R([x]_M)) \). This is the step we accomplish next.

The congruence \( \sim_M \) is itself a submonoid of \( \mathbb{N}^p \times \mathbb{N}^p \) that is generated by its set of minimal nonzero elements, which turns out to be \( A(\sim_M) \). There is an algorithm for computing this set from the equations of \( M \) (see [14, Chapter 8]).

**Proposition 3.3.** Let \( M \) be a subgroup of \( \mathbb{Z}^p \) such that \( M \cap \mathbb{N}^p = \{0\} \) and let \( x \in \mathbb{N}^p \). Then
\[
\text{supp}(R([x]_M)) = \bigcup_{(a, b) \in A(\sim_M), \text{supp}(a) \subseteq \text{supp}(x)} \text{supp}(b) .
\]

**Proof.** Let \( (a, b) \in A(\sim_M) \) such that \( \text{supp}(a) \subseteq \text{supp}(x) \). Then there exists \( n \in \mathbb{N} \setminus \{0\} \) such that \( nx - a \in \mathbb{N}^p \), whence \( nx - a + b \sim_M nx \). This implies that \( \text{supp}(b) \subseteq \text{supp}(R([x]_M)) \).

For the other inclusion, take \( (y_1, \ldots, y_p) \in R([x]_M) \). Then \( (y_1, \ldots, y_p) \sim_M nx \) for some \( n \in \mathbb{N}^p \setminus \{0\} \). Hence
\[
(nx, (y_1, \ldots, y_p)) = \sum_{i=1}^{k} (a_i, b_i),
\]
for some \( (a_i, b_i) \in A(\sim_M) \) (this set generates \( \sim_M \) as a monoid). For every \( i \in \{1, \ldots, k\} \),
\[
\text{supp}(a_i) \subseteq \text{supp}(nx) = \text{supp}(x) \quad \text{and} \\
\text{supp}(y_1, \ldots, y_p) \subseteq \bigcup_{i=1}^{k} \text{supp}(b_i). \]

For a given \( s \in S \), \( \text{supp}(R(s)) = \{i_1, \ldots, i_r\} \) implies that the irreducibles appearing in the factorizations of the powers of \( s \) are actually \( s_{i_1}, \ldots, s_{i_r} \).

We illustrate these results with an example.
Example 3.4. Let \( S = \langle (2, 4, 1), (0, 1, 2), (3, 6, 1) \rangle \subseteq \mathbb{N}^2 \times \mathbb{Z}/3\mathbb{Z} \). The semigroup is thus cancellative. By [14, Proposition 3.1], \( S \) is isomorphic to \( \mathbb{N}^3 / \sim_M \), where \( M \) is the subgroup of \( \mathbb{Z}^3 \) with defining equations

\[
\begin{align*}
2x + 3z &= 0, \\
4x + y + 6z &= 0, \\
x + 2y + z &\equiv 0 \pmod{3}
\end{align*}
\]

(the columns of the equations of \( M \) are just the generators of \( S \)). Clearly \( M \cap \mathbb{N}^3 = \{0\} \) and consequently \( S \) is reduced. Take \( g = 3(2, 4, 1) − 2(3, 6, 1) = (0, 0, 1) \) which is in the quotient group of \( S \) (the group generated by \( S \) in \( \mathbb{Z}^2 \times \mathbb{Z}/3\mathbb{Z} \)) and is not in \( S \). Notice that \( 3g = (0, 0, 0) \in S \), whence \( S \) is not root-closed, which in particular means that \( S \) is not a Krull monoid.

Applying the results obtained in [14, Chapter 8] we get that

\[
\mathcal{A}(\sim_M) = \{(9e_1, 6e_3), (6e_3, 9e_1), (e_1, e_1), (e_2, e_2), (e_3, e_3)\}
\]

(this in particular means that \( \{[e_1]_{\sim_M}, [e_2]_{\sim_M}, [e_3]_{\sim_M}\} \) is a minimal system of generators for \( S \); otherwise we would find an element of the form \((e_i, b) \) in \( \mathcal{A}(\sim_M) \) with \( i \notin \text{supp}(b) \)).

We compute \( r([e_1]_{\sim_M}) \). By Proposition 3.3 we deduce that

\[
\text{supp}(R([e_1]_{\sim_M})) = \{1, 3\}.
\]

Hence \( M' \) is the subgroup of \( \mathbb{Z}^2 \) with defining equations

\[
\begin{align*}
2x + 3z &= 0, \\
4x + 6z &= 0, \\
x + z &\equiv 0 \pmod{3}.
\end{align*}
\]

Clearly \( \text{rank}(M') = 1 \) and therefore \( r([e_1]_{\sim_M}) = 2 \).

In some special settings there are alternative ways for computing \( r(s) \) without computing \( \mathcal{A}(\sim_M) \). These methods could be cumbersome in some cases. One of special interest in factorization theory is explained next. Let \( S \) be a submonoid of \( \mathbb{N}^d \) for some positive integer \( d \). For a given subset \( A \) of \( \mathbb{N}^d \) write \( \mathcal{Q}(A) \) for the subgroup of \( \mathbb{Z}^d \) generated by \( A \). The monoid \( S \) is saturated if \( \mathcal{Q}(S) \cap \mathbb{N}^d = S \) (this kind of monoid has been widely studied in the literature, and is sometimes called a full affine semigroup; see for instance [10,13]). It is well known that every finitely generated reduced Krull monoid is isomorphic to a saturated submonoid of \( \mathbb{N}^d \) for some positive integer \( d \) (see for instance [3]). Since \( S \) is reduced and cancellative, it is atomic. The set \( \mathcal{A}(S) \) coincides with the set of minimal elements of \( S \setminus \{0\} = (\mathcal{Q}(S) \cap \mathbb{N}^d) \setminus \{0\} \) with respect to the usual partial order on \( \mathbb{N}^d \), which by Dickson’s lemma is finite.

Lemma 3.5. Let \( S \) be a saturated submonoid of \( \mathbb{N}^d \) and let \( \{s_1, \ldots, s_p\} \) be its set of atoms. Take \( s \in S \). Then

\[
\text{supp}(R(s)) = \{i \in \{1, \ldots, p\} \mid \text{supp}(s_i) \subseteq \text{supp}(s)\}.
\]
Proof. Let \( i \in \text{supp}(R(s)) \). Then there exists \((k_1, \ldots, k_p) \in R(s)\) such that \(k_i \neq 0\). This implies that \(ks = k_1s_1 + \cdots + k_ps_p\) for some nonnegative integer \(k\), and as \(k_i \neq 0\), this yields \(\text{supp}(s_i) \subseteq \text{supp}(s)\).

Now assume that \(\text{supp}(s_i) \subseteq \text{supp}(s)\) for some \(i \in \{1, \ldots, p\}\). Then we can find \(k \in \mathbb{N} \setminus \{0\}\) such that \(ks - s_i \in \mathbb{N}^d\). Since \(ks - s_i \in \mathbb{Q}(S)\) and \(S\) is saturated, we get that \(ks - s_i \in S\). Thus there exists \(k_1, \ldots, k_p \in S\) such that \(ks - s_i = k_1s_1 + \cdots + k_ps_p\). Hence
\[
(k_1, \ldots, k_{i-1}, k_i + 1, k_{i+1}, \ldots, k_p) \in R(s)
\]

and \(k_i + 1 \neq 0\), which implies that \(i \in \text{supp}(R(s))\).

Proposition 3.6. Let \(S\) be a saturated submonoid of \(\mathbb{N}^d\) and let \(s \in S \setminus \{0\}\). Set
\[
I(s) = \{a \in A(S) \mid \text{supp}(a) \subseteq \text{supp}(s)\}.
\]
Then
\[
r(s) = \#I(s) - \text{rank}(\mathbb{Q}(\langle I(s) \rangle)) + 1.
\]

Proof. Assume that \(A(S) = \{s_1, \ldots, s_p\}\) and \(I(s) = \{s_{i_1}, \ldots, s_{i_t}\}\). As we pointed out above, the factorization homomorphism
\[
\varphi : \mathbb{N}^p \to S, \quad \varphi(a_1, \ldots, a_p) = \sum_{i=1}^p a_is_i,
\]
yields an isomorphism between \(S\) and \(\mathbb{N}^p/\sim_M\), where \(M\) is the subgroup of \(\mathbb{Z}^p\) with defining equations
\[
(s_1 \cdots s_p) \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = 0,
\]
such that the coordinates of \(s_i \in \mathbb{N}^d\) are written in columns (this makes \(d\) linear equations; see [12] or [14, Chapter 3]). By Lemma 3.5, we know that \(\text{supp}(R(s)) = \{i_1, \ldots, i_t\}\). Using Proposition 3.2, and taking into account that \(\text{supp}(R(s)) = \text{supp}(R([x]_{\sim_M}))\) for every \(x \in \varphi^{-1}(s)\), we obtain that \(r(s) = \text{rank}(M') + 1\), where \(M'\) is the subgroup of \(\mathbb{Z}^t\) with defining equations
\[
(s_{i_1} \cdots s_{i_t}) \begin{pmatrix} x_1 \\ \vdots \\ x_t \end{pmatrix} = 0.
\]
Notice that \(\text{rank}(M') = t - \text{rank}(\mathbb{Q}(\{s_{i_1}, \ldots, s_{i_t}\}))\), which concludes the proof.

Example 3.7. While Proposition 3.6 is not a direct generalization of [2, Proposition 6] or [1, Proposition 1.3], it can be used to compute values of \(r(s)\) for a wider class of monoids than either of these two cited results. For instance,
Proposition 3.6 can be used to compute values of $r(s)$ in Krull monoids with torsion free divisor class group. In particular, let $S$ be the Diophantine monoid defined by the equation $x_1 + x_2 = x_3 + x_4$ (i.e., $S = \{(x_1, x_2, x_3, x_4) \in \mathbb{N}^4 | x_1 + x_2 = x_3 + x_4\}$). Every Diophantine monoid is a Krull monoid (see [5]) and by [4, Theorem 1.3], the divisor class group of $S$ is $\mathbb{Z}$. Now, $A(S) = \{(1, 0, 0, 1), (1, 0, 1, 0), (0, 1, 0, 1), (0, 1, 1, 0)\}$ and hence for $s \neq 0$ in $S$ we have that $\text{rank}(Q(\langle I(s) \rangle)) = \text{supp}(s) - 1$. Thus by Proposition 3.6,

$$r(s) = \begin{cases} 1 & \text{if } \text{supp}(s) = 2 \text{ or } 3, \\ 2 & \text{if } \text{supp}(s) = 4. \end{cases}$$

4. Some applications and examples

4.1. The computation of $A(s)$

Recall that $\overline{\eta}(s) = \lim_{n \to \infty} (\eta(s^n)/n^{r(s)-1})$ and by Theorem 1.1 we get $\overline{\eta}(s) = A(s)$. If $r(s) = 1$, then the corresponding $M'$ computed for $s$ as explained in the preceding section is trivial (its rank is zero). Hence, the irreducibles appearing in the factorizations of the collective powers of $s$ are not “related.” This in particular means that there is actually a unique factorization for each of these elements and thus $\overline{\eta}(s) = 1 = A(s)$.

Now assume that $x \in \mathbb{N}^p \setminus \{0\}$, $M$ is a subgroup of $\mathbb{Z}^p$ such that $M \cap \mathbb{N}^p = \{0\}$ and $r([x]_{M'}) = 2$. From the results obtained in the last section, we can also assume that $\text{supp}(R([x]_{M'})) = \{1, \ldots, p\}$ (otherwise we would use $\mathbb{N}^q/\sim_{M'}$) and thus $\text{rank}(M) = 1$. Hence, there exists $m \in \mathbb{Z}^p$ such that $M = \{zm \mid z \in \mathbb{Z}\}$. Let $m^+$ and $m^-$ be elements of $\mathbb{N}^p$ such that $m = m^+ - m^-$ and $\text{supp}(m^+) \cap \text{supp}(m^-) = \emptyset$ (these elements are necessarily unique).

**Lemma 4.1.** Under the above hypothesis, if $a \in \mathbb{N}^p \setminus \{0\}$, then

$$[a]_{M'} = \{-k^+(a)m + a, \ldots, a, \ldots, a + k^-(a)m\},$$

where

$$k^+(a) = \max \{k \in \mathbb{N} \mid a - km \in \mathbb{N}^p\} \quad \text{and}$$

$$k^-(a) = \max \{k \in \mathbb{N} \mid a - km \in \mathbb{N}^p\}$$

(notice that $k^+(a)$ and $k^-(a)$ are both finite since $M \cap \mathbb{N}^p = \{0\}$).

**Proof.** Clearly $\{-k^+(a)m + a, \ldots, a, \ldots, a + k^-(a)m\} \subseteq [a]_{M'}$, since $a - (a - lm) \in M$. For the other inclusion, note that $[a]_{M'} = (a + M) \cap \mathbb{N}^p$ and that $\text{supp}(m^+) \cap \text{supp}(m^-) = \emptyset$. □
From this result, we deduce that \( \eta([x]_\sim_M) = k^+(x) + k^-(x) + 1 \). The integers \( k^+(x) \) and \( k^-(x) \) can be easily computed. For a given element \( a \in \mathbb{N}^p \), denote by \( a_i \) its \( i \)th coordinate. Then

\[
k^+(x) = \left\lfloor \min \left\{ \frac{x_i}{m_i^+} \mid i \in \text{supp}(m^+) \right\} \right\rfloor,
\]

and

\[
k^-(x) = \left\lfloor \min \left\{ \frac{x_i}{m_i^-} \mid i \in \text{supp}(m^-) \right\} \right\rfloor,
\]

where \( \lfloor \alpha \rfloor \) denotes the integer part of the rational number \( \alpha \).

With these facts, it is straightforward to prove the following result.

**Proposition 4.2.** Under the above hypothesis,

\[
\tilde{\eta}([x]_\sim_M) = \min \left\{ \frac{x_i}{m_i^+} \mid i \in \text{supp}(m^+) \right\} + \min \left\{ \frac{x_i}{m_i^-} \mid i \in \text{supp}(m^-) \right\}.
\]

**Example 4.3.** Let \( S \) be the Diophantine monoid given by the equation \( x + 2y - 3z = 0 \), that is, \( S = \{(x, y, z) \in \mathbb{N}^3 \mid x + 2y - 3z = 0\} \). The monoid \( S \) is minimally generated by \( \{(3, 0, 1), (0, 3, 2), (1, 1, 1)\} \), its set of irreducible elements. By [14, Proposition 3.1], \( S \) is isomorphic to \( \mathbb{N}^3 / \sim_M \), where \( M \) has defining equations

\[
M \equiv \left\{ \begin{array}{l}
3x_1 + x_3 = 0, \\
3x_2 + x_3 = 0, \\
x_1 + 2x_2 + x_3 = 0,
\end{array} \right. \quad \Rightarrow \left\{ \begin{array}{l}
3x_1 + x_3 = 0, \\
3x_2 + x_3 = 0,
\end{array} \right.
\]

whence \( \text{rank}(M) = 1 \) and

\[
\text{r}((4, 4, 4)) = \text{r}([(e_1 + e_2 + e_3]_\sim_M)) = 1 + 1 = 2
\]

(the formula given in Proposition 3.6 yields \( 3 - 2 + 1 = 2 \)). The subgroup \( M \) is generated by \( m = (1, 1, -3) \) which implies that \( m^+ = (1, 1, 0) \) and \( m^- = (0, 0, 3) \). Using the formula given in Proposition 4.2, we obtain \( \tilde{\eta}((4, 4, 4)) = 4 + 4/3 = 16/3 \).

If one wants to compute \( A(s) \) for an element such that \( \text{r}(s) > 2 \), then one can use the formula given in [9] extracted from [11, Chapter VI, Section 2, Theorem 2]. An explanation of this formula follows. Let \( a \in \mathbb{N}^p \) and \( M \) be a subgroup of \( \mathbb{Z}^p \) such that \( M \cap \mathbb{N}^p = \{0\} \). As above, we can assume that \( \text{supp}(R([a]_\sim_M)) = \{1, \ldots, p\} \). Then \( \text{r}([a]_\sim_M) = \text{rank}(M) + 1 \). Let \( s = \text{rank}(M) = \text{r}([a]_\sim_M) - 1 \) and \( \{m_1, \ldots, m_s\} \) be a basis of \( M \). Set

\[
F(M) = \left\{ t_1m_1 + \cdots + t_sm_s \mid 0 \leq t_i < 1 \text{ for all } i \right\}.
\]

\( F(M) \) is called a fundamental domain for \( M \). Let

\[
P_a = \left\{ x \in \mathbb{L}_\mathbb{R}(M) \mid x \geq -a \right\} = \left\{ y \in a + \mathbb{L}_\mathbb{R}(M) \mid y \geq 0 \right\},
\]
where \((x_1, \ldots, x_p) \geq (y_1, \ldots, y_p)\) if \(x_i \geq y_i\) for all \(i\) and \(L_\mathbb{R}(M)\) is the \(\mathbb{R}\)-vector space spanned by \(M\) (that is, the subspace of \(\mathbb{R}^p\) generated by \(\{m_1, \ldots, m_s\}\)). Then

\[
A([a]_\sim_M) = \frac{\text{vol}(P_a)}{\text{vol}(F(M))},
\]

where \(\text{vol}(\cdot)\) is the volume computed in \(L_\mathbb{R}(M)\). One can in fact use this formula for \(r(s) = 2\), but it turns out that the formula given in Proposition 4.2 is much easier to use and compute. These volumes are computed in the following manner (the formulas can be found in any elementary differential geometry textbook). The vector space \(L_\mathbb{R}(M)\) can be parametrized by

\[
X(t_1, \ldots, t_s) = \sum_{i=1}^{s} t_i m_i.
\]

Then

\[
\text{vol}(F(M)) = \int_{F(M)} \text{d}A = \int_{0}^{1} \cdots \int_{0}^{1} \sqrt{G} \, dt_1 \cdots dt_s,
\]

where

\[
G = \det \left( \frac{\partial X}{\partial t_i} \cdot \frac{\partial X}{\partial t_j} \right)_{i, j \in \{1, \ldots, s\}} = \det (m_i \cdot m_j)_{i, j \in \{1, \ldots, s\}}
\]

\((x \cdot y\) represents the dot product of \(x\) and \(y\)) and

\[
\text{vol}(P_a) = \int_{P_a} \text{d}A = \int_{t_i \in R} \sqrt{G} \, dt_1 \cdots dt_s,
\]

where \(R\) is the region in \(\mathbb{R}^s\) determined by the \(p\) inequalities \(\sum_{i=1}^{s} t_i m_i \geq -a\).

Let us illustrate this with an example.

**Example 4.4.** Let \(S\) be the submonoid of \(\mathbb{N}\) generated by \(\{3, 4, 5\}\). We already know by Example 2.6 that \(r(s) = 3\) for all \(s \in S \setminus \{0\}\). By [14, Proposition 3.1], \(S\) is isomorphic to \(\mathbb{N}^3 / \sim_M\) with \(M\) given by the equation \(3x_1 + 4x_2 + 5x_3 = 0\). Let \(a = (1, 1, 0)\). Then

\[
 r([1, 1, 0]_\sim_M) = r(3 + 4) = r(7) = 3
\]

and \(\text{supp}(R([1, 1, 0]_\sim_M)) = \{1, 2, 3\}\). A basis for \(M\) is \(\{(4, -3, 0), (5, -5, 1)\}\). In this setting,

\[
X(t_1, t_2) = t_1(4, -3, 0) + t_2(5, -5, 1).
\]

Hence

\[
\text{vol}(F(M)) = \int_{F(M)} \text{d}A = \int_{0}^{1} \int_{0}^{1} \sqrt{\det \begin{bmatrix} 25 & 35 \\ 35 & 51 \end{bmatrix}} \, dt_1 \, dt_2 = 5\sqrt{2}.
\]
The inequality \( t_1(4, -3, 0) + t_2(5, -5, 1) \geq -(1, 1, 0) \) yields \( 4t_1 + 5t_2 \geq -1, -3t_1 - 5t_2 \geq -1 \) and \( t_2 \geq 0 \). Using this,

\[
\text{vol}(P_a) = \int_{P_a} dA = 5 \sqrt{2} \left( \int_{-1/4}^{1} \int_{(1-3t_1)/5}^{(1-3t_1)/5} dt_1 dt_2 + \int_{-1/4}^{(1-3t_1)/5} \int_{0}^{1/3} dt_1 dt_2 \right)
\]

whence \( A(7) = 49/120 \).

### 4.2. A-stability and ia-stability

Let \( S \) be a finitely generated reduced cancellative commutative monoid. An element \( x \in S \setminus \{0\} \) is asymptotically stable (a-stable for short) if \( r(x) \leq 2 \). We say that \( S \) itself is a-stable if \( r(x) \leq 2 \) for all \( x \in S \), and \( S \) is irreducibly asymptotically stable (ia-stable for short) if \( r(x) \leq 2 \) for all \( x \in A(S) \). Observe that from a presentation of \( S \) (in fact it suffices to know \( M \) for which \( S \) is isomorphic to \( \mathbb{N}^p/\sim_M \)) one can determine the a-stable elements of \( S \). If an element is a-stable, then by Corollary 2.5 the whole Archimedean component containing it is formed by a-stable elements of \( S \). In this way, it is also easy to decide whether the monoid \( S \) is a-stable or ia-stable. From Proposition 2.2 one obtains the following consequence.

**Corollary 4.5.** Let \( M \) be a subgroup of \( \mathbb{Z}^p \) such that \( M \cap \mathbb{N}^p = \{0\} \). Then \( \mathbb{N}^p/\sim_M \) is a-stable if and only if \( \text{rank}(M) \in \{0, 1\} \).

**Proof.** Note that if \( \text{rank}(M) \in \{0, 1\} \), then by Proposition 2.2, every element \( [x] \sim_M \) in \( \mathbb{N}^p/\sim_p \) satisfies \( r([x] \sim_M) \leq 1 + 1 = 2 \) and thus \( \mathbb{N}^p/\sim_M \) is a-stable.

If \( \text{rank}(M) \geq 2 \), then by Proposition 2.2, \( r([(1, \ldots, 1)] \sim_M) \geq 3 \), whence \( \mathbb{N}^p/\sim_M \) is not a-stable, since \( [(1, \ldots, 1)] \sim_M \) is not a-stable. \( \square \)

In view of Example 2.6, a numerical semigroup is ia-stable if and only if it is a-stable and this occurs if and only if it is minimally generated by less than three elements (that is, its embedding dimension is less than or equal to two).

It may happen that \( \mathbb{N}^p/\sim_M \) is ia-stable but not a-stable, as the following example shows.

**Example 4.6.** Let \( M \) be the subgroup of \( \mathbb{N}^{2n} \) with defining equations

\[
x_1 + x_2 = 0, \\
x_3 + x_4 = 0, \\
\vdots \\
x_{2n-1} + x_{2n} = 0.
\]
By Proposition 2.2, $r([1, \ldots, 1]_M) = n + 1$, since $\text{rank}(M) = n$. Therefore $\mathbb{N}^{2n} / \sim_M$ is not a-stable for $n \geq 2$.

The set $A(\sim_M)$ is equal to
\[
\{(e_1, e_1), \ldots, (e_{2n}, e_{2n}), (e_1, e_2), (e_3, e_4), \ldots, (e_{2n-1}, e_{2n}),
(e_2, e_1), (e_4, e_3), \ldots, (e_{2n-1}, e_{2n})\}.
\]

Using Proposition 3.3, we get that
\[
\text{supp}(R([e_{2k-1}]_M)) = \text{supp}(R([e_{2k}]_M)) = \{2k - 1, 2k\}
\]
for all $k \in \{1, \ldots, n\}$ and the corresponding $M'$ for each of these supports is of rank one (one equation in dimension two). Hence
\[
r([e_{2k-1}]_M) = r([e_{2k}]_M) = 1 + 1 = 2
\]
for all $k \in \{1, \ldots, n\}$, which means that $\mathbb{N}^{2n} / \sim_M$ is ia-stable. One possible interpretation of this example is that ia-stability has nothing to do with the rank of $M$, while a-stability depends strongly on it.

Observe also that if we take $x_k = \sum_{i=1}^k e_{2k-1}$, $k \in \{1, \ldots, n\}$, then
\[
\text{supp}(R([x_k]_M)) = \{e_1, e_2, \ldots, e_{2k}\}
\]
and its corresponding $M'$ has rank $k$, which means that $r([x_k]_M) = k + 1$. Thus the image of $r$ for this monoid is $\{0, 2, 3, \ldots, n + 1\}$.

We can use Proposition 3.6 in order to study a-stability on saturated submonoids of $\mathbb{N}^d$.

**Proposition 4.7.** Let $S$ be a saturated submonoid of $\mathbb{N}^d$. For a given $s \in S$, set $MI(s)$ to be the set of elements in $I(s)$ with minimal support (with respect to set inclusion in the set of all supports of elements in $A(S)$). If $\#I(s) - \#MI(s) \geq 2$, then $s$ is not a-stable.

**Proof.** In [6] it is shown that if $a \in A(S)$ is not of minimal support, then $a = \sum_{i=1}^r \lambda_i a_i$ with $\lambda_i \in (0, 1) \cap \mathbb{Q}$ and $a_i$ elements of $A(S)$ with minimal support. If there is an element $a$ in $I(s)$ that is not of minimal support, then it can be written as a combination of elements $a_1, \ldots, a_r$ with minimal support in $A(S)$. Since the support of these elements must be contained in the support of $a$, it follows that $\text{supp}(a_i) \subseteq \text{supp}(s)$ for all $i \in \{1, \ldots, r\}$, whence $a_i \in MI(s)$ for all $i$. Notice that if this is the case, then
\[
\text{rank}(Q(\{a, a_1, \ldots, a_r\})) = \text{rank}(Q(\{a_1, \ldots, a_r\})).
\]
Using this, we obtain that $\text{rank}(Q(I(s))) = \text{rank}(Q(MI(s)))$. By Proposition 3.6, it follows that
\[
r(s) = \#I(s) - \text{rank}(Q(MI(s))) + 1 \geq \#I(s) - \#MI(s) + 1 \geq 2 + 1 = 3.
\]
Therefore $s$ is not a-stable. \[\square\]
Lemma 4.8. Let $S$ be a saturated submonoid of $\mathbb{N}^d$ and let $s_1, s_2 \in \mathcal{A}(S)$ such that $\text{supp}(s_1) = \text{supp}(s_2) = I$. Then there exists $s_3 \in \mathcal{A}(S)$ whose support is properly contained in $I$.

Proof. Let $s_1 = (x_1, \ldots, x_d)$ and $s_2 = (y_1, \ldots, y_d)$. Take $i \in I$ such that $y_i/x_i = \max\{y_j/x_j \mid j \in I\}$. Then $y_i x_j - x_i y_j \geq 0$ for all $j \in I$, which means that $y_i s_1 - x_i s_2 \in \mathbb{N}^d$. Since $S$ is saturated, we get that $y_i s_1 - x_i s_2 \in S$. The element $y_i s_1 - x_i s_2 \neq 0$, because otherwise we have $y_i/x_i = y_j/x_j$ for all $j \in I$. This would lead to $s_1 = \lambda s_2$ for some $\lambda \in \mathbb{Q} \setminus \{0\}$, which is impossible since $s_1, s_2 \in \mathbb{N}^d$ are incomparable elements with respect to $\leq$. Hence, there must be an atom $s_3$ of $S$ such that $s_3 \leq y_i s_1 - x_i s_2$ (recall that $\mathcal{A}(S) = \text{Minimals}_{\leq}^\mathcal{A}(S \setminus \{0\})$). This implies that $i \in I \setminus \text{supp}(s_3)$ and $\text{supp}(s_3) \subset I$. \hfill $\square$

Corollary 4.9. Let $S$ be a saturated submonoid of $\mathbb{N}^d$ and let $s \in S$. If $s$ is of minimal support among the elements in $S$, then $s$ is a-stable.

Proof. Since $s$ is of minimal support, by Lemma 4.8, $I(s) = \{a\}$, for some $a \in \mathcal{A}(S)$. Using now Proposition 3.6 we obtain that $r(s) = 1 - 1 + 1 = 1$, whence $s$ is a-stable. \hfill $\square$

Example 4.10. The a-stability and ia-stability properties are examined in [1, Theorem 3.5] and [2, Proposition 8 and Theorem 9] for certain Krull monoids with torsion divisor class groups. As with our earlier comments in Section 3 concerning the computation of $r(s)$, the results of this section can be applied to a wider class of monoids than those listed above. For instance, let $S$ be the Diophantine monoid defined by the equation $x_1 + x_2 + x_3 = x_4 + x_5$. By [4, Theorem 1.3], the divisor class group of $S$ is $\mathbb{Z}$. It is easy to see that this monoid is not a-stable by Corollary 4.5. In this example,

$$\mathcal{A}(S) = \{(1, 0, 0, 1, 0), (1, 0, 0, 0, 1), (0, 1, 0, 1, 0), (0, 1, 0, 0, 1), (0, 0, 1, 0, 1), (0, 0, 1, 1, 0)\}$$

and hence every irreducible is of minimal support amongst the elements of $S$. Thus, $r(s) = 1 - 1 + 1$ for every $s \in \mathcal{A}(S)$ and $S$ is ia-stable (this is actually Corollary 4.9). Notice that the largest value of $r(s)$ in $S$ is achieved by the Archimedean component of $(2, 2, 2, 3, 3)$, where $r(2, 2, 2, 3, 3) = 6 - 4 + 1 = 3$ by Proposition 3.6. Moreover, in this example Proposition 4.7 does not detect that $(2, 2, 2, 3, 3)$ is not a-stable.

References


