Pacific Journal of Mathematics

ON DIOPHANTINE MONOIDS AND THEIR CLASS GROUPS

Scott T. Chapman, Ulrich Krause, and Eberhard Oeljeklaus

Volume 207 No. 1 November 2002

PACIFIC JOURNAL OF MATHEMATICS
Vol. 207, No. 1, 2002

ON DIOPHANTINE MONOIDS AND THEIR CLASS GROUPS

Scott T. Chapman, Ulrich Krause, and Eberhard Oeljeklaus

A Diophantine monoid S is a monoid which consists of the set of solutions in nonnegative integers to a system of linear Diophantine equations. Given a Diophantine monoid S, we explore its algebraic properties in terms of its defining integer matrix A. If $d_r(S)$ and $d_c(S)$ denote respectively the minimal number of rows and minimal number of columns of a defining matrix A for S, then we prove in Section 3 that $d_r(S) = \operatorname{rank} \mathrm{Cl}(S)$ and $d_c(S) = \operatorname{rank} \mathrm{Cl}(S) + \operatorname{rank} Q(S)$ where $\mathrm{Cl}(S)$ represents the divisor class group of S and $Q(S)$ the quotient group of S. The proof relies on the characteristic properties of the so-called essential states of S, which are developed in Section 2. We close in Section 4 by offering a characterization of factorial Diophantine monoids and an algorithm which determines if a Diophantine monoid is half-factorial.

1. Introduction.

Because of their applications in commutative algebra, algebraic geometry, combinatorics, number theory, and computational algebra, the study of commutative cancellative monoids has recently increased in popularity (see for example [**14**]). Let $\mathbb{Z}$ and $\mathbb{N}$ represent the integers and the nonnegative integers respectively. For $1 \leq m, n$ in $\mathbb{N}$ and $A \in \mathbb{Z}^{m \times n}$ set

$$M_A = \mathbb{N}^n \cap \{x \in \mathbb{Z}^n \mid Ax = 0\}. \tag{1}$$

We will refer to M_A as a *Diophantine monoid* and to A as a matrix which *determines* M_A. Admitting the possibility that $m = 0$, we set $M_A = \mathbb{N}^n$ if $m = 0$. The special case of a Diophantine monoid M_A for $A \in \mathbb{Z}^{1 \times n}$ (i.e., one single homogeneous linear Diophantine equation) has been studied in [**2**], where it was shown that the divisor class group of M_A (denoted $\mathrm{Cl}\,(M_A)$) in this case must be cyclic [**2**, Theorem 1.3].

It is natural to consider the question of whether a Diophantine monoid M_A given by a matrix $A \in \mathbb{Z}^{m \times n}$ can be described (up to isomorphy) by another matrix with less rows or less columns. For a Diophantine monoid S, let $d_r(S)$ and $d_c(S)$ denote respectively the minimal number of rows and minimal number of columns of a matrix A with $S \simeq M_A$. One has that

$d_c(S) = d_r(S) + \operatorname{rank} Q(S)$ where $Q(S)$ is the quotient group of S. In this paper, we prove for a monoid which is root-closed and finitely generated that $d_r(S) = \operatorname{rank} \mathrm{Cl}\,(S)$ and hence $d_c(S) = \operatorname{rank} \mathrm{Cl}\,(S) + \operatorname{rank} Q(S)$ (Theorem 3.8). Furthermore, this theorem also shows that for such an S there exists an $A \in \mathbb{Z}^{m\times n}$ with $m = d_r(S)$, $n = d_c(S)$ and $S \simeq M_A$.

More precisely, we divide our work into three additional sections. After a very brief review of Krull monoids, we focus our considerations in Section 2 on the so-called essential states of these monoids and provide in Lemma 2.3 and Proposition 2.4 their characteristic properties. Using these properties, we obtain the above mentioned result (Theorem 3.8) from our crucial Theorem 3.1 together with Lemma 3.5. Theorem 3.1 demonstrates that any Krull monoid with finitely many essential states must be isomorphic to a Diophantine monoid and describes the structure of the representing matrix as well as the structure of the class group. As a consequence, we obtain in Corollary 3.3 various equivalent characterizations of the above Krull monoids or, equivalently, Krull monoids with finitely generated divisor class group and finitely many prime divisors. For some results related to Corollary 3.3, the interested reader can consult [**7**, Theorem 5], [**8**, Lemma 3], [**10**, Proposition 2], and [**13**, Corollary 1]. We note that Lemma 3.5 yields a description of the class group of a Diophantine monoid S purely in terms of linear algebra. In Section 4, we present some examples to illustrate the results of Sections 2 and 3 and also obtain in Proposition 4.1 a characterization of when M_A is factorial (recall that M_A is factorial if any nonzero element has a representation $\alpha_1 + \cdots + \alpha_k$ by irreducible elements α_i which is unique up to ordering). We close by presenting an algorithm, which when teamed with known algorithms for computing the set of minimal nonnegative solutions to M_A, will compute the class group of M_A and determine if M_A is half-factorial (recall that M_A is half-factorial if whenever $\alpha_1,\ \alpha_2, \ldots, \alpha_k$ and $\beta_1,\ \beta_2, \ldots, \beta_l$ are irreducible elements of M_A with $\alpha_1 + \cdots + \alpha_k = \beta_1 + \cdots + \beta_l$, then $k = l$).

Although the literature concerning the algebraic structure of the monoids M_A is not extensive, we take interest in this topic partly because of the rich mathematical history behind the study of Diophantine equations. It is easy to determine the solution set of a system of linear Diophantine equations over the integers, but this is not the case for determining the set of solutions over the *nonnegative* integers. While a modern treatment of the combinatorial aspects of this subject can be found in the works of Stanley (see [**15**] and [**16**] for example), attempts to determine the set of "irreducible solutions" of M_A can be traced back almost 100 years to a paper of Elliott [**4**], where the author produces generating functions to determine these solutions. Another early attempt at producing this set of minimal solutions can be found in [**5**]. The development of modern algorithms connected with these solutions has become a popular topic of research in computational algebra (see [**3**] and [**14**]).

2. Essential states.

Let S be a commutative cancellative monoid (i.e., a subsemigroup of an abelian group written additively with $0 \in S$). Throughout this paper we assume that $S \neq \{0\}$. If $\{0\}$ is the only subgroup of S, then S is called *reduced*. Let

$$Q(S) := \{x - y \,|\, x, y \in S\}$$

be the group generated by S. A homomorphism $\pi : Q(S) \to \mathbb{Z}$ is called a *state* of S if $\pi(S) \subseteq \mathbb{N}$. The monoid S is a *Krull monoid* if there exists, for some set K, a monomorphism

$$\varphi : Q(S) \to \mathbb{Z}^{(K)} \quad \text{(direct sum)}$$

such that

$$\varphi(S) = \mathbb{N}^{(K)} \cap \varphi(Q(S)) = \mathbb{N}^{(K)} \cap Q(\varphi(S)).$$

As a consequence of our definition, a Krull monoid is always reduced.

For $j \in K$ let $p_j : \mathbb{Z}^{(K)} \to \mathbb{Z}$ be the surjection onto the j-th component, $p_j((x_k)_{k\in K}) = x_j$, and

$$\pi_j : Q(S) \to \mathbb{Z}, \quad \pi_j = p_j \circ \varphi.$$

Then

$$(*) \qquad S = \{x \in Q(S) \,|\, \pi_j(x) \geq 0 \ \text{ for all } \ j \in K\}$$

where $(\pi_j)_{j\in K}$ is a family of states of S with $\pi_j(x) = 0$ for almost all $j \in K$ and any fixed $x \in Q(S)$. We may assume that $\pi_j \neq 0$ for all $j \in K$.

Example 2.1. For every $A \in \mathbb{Z}^{m\times n}$ the *Diophantine monoid*

$$M_A = \{x \in \mathbb{N}^n \,|\, Ax = 0\} \subseteq \mathbb{Z}^n$$

is a Krull monoid. With $K = \{1, 2, \ldots, n\}$ and $\varphi : Q(M_A) \to \mathbb{Z}^n$ the canonical embedding, we have

$$M_A = \{(x_1, \ldots, x_n) \in Q(M_A) \,|\, \pi_j(x) = x_j \geq 0 \text{ for } j \in K\}.$$

When a Krull monoid S is given in the form $(*)$, it is natural to ask for minimal subsets $E \subseteq K$ with the property that

$$S = \{x \in Q(S) \,|\, \pi_i(x) \geq 0 \text{ for all } i \in E\}.$$

Such subsets exist and can be described by the so-called essential states of S.

Definition 2.2. A nonzero state π of S is called *essential*, if for every $x, y \in Q(S)$ with $\pi(x) \geq \pi(y)$ there exists $z \in Q(S)$ with

$$\pi(z) = \pi(x),\ z - x \in S \text{ and } z - y \in S.$$

The essential states can be characterized as follows:

Lemma 2.3. *Let S be a Krull monoid and $(\pi_j)_{j\in J}$ the family of all nonzero states of S. For every $i \in J$ the following statements are equivalent:*

i) *π_i is essential.*
ii) *For every $j \in J$ with $\pi_j \notin \mathbb{Q}\pi_i$ there exists $x \in S$ such that $\pi_i(x) = 0$ and $\pi_j(x) > 0$.*
iii) *$S \cap \operatorname{Ker}\pi_i$ is a maximal element in the set $\{S \cap \operatorname{Ker}\pi_j \mid j \in J\}$ with respect to set inclusion.*
iv) *If $j \in J$ and $(S \cap \operatorname{Ker}\pi_i) \subseteq (S \cap \operatorname{Ker}\pi_j)$ then $\pi_j = \alpha\pi_i$ for some $\alpha \in \mathbb{Q}, \alpha > 0$.*

In particular, the family of essential states of S is not empty.

Proof. Note that for any finite subset $I \subseteq J$, there exists $x \in S$ with $\pi_i(x) > 0$ for all $i \in I$.

Statements ii) and iv) are obviously equivalent. We begin by showing that i) $\Rightarrow$ iii). Assume that i) holds and that, for some $j \in J$,

$$(S \cap \operatorname{Ker}\pi_i) \subsetneqq (S \cap \operatorname{Ker}\pi_j).$$

Choose $y \in (S \cap \operatorname{Ker}\pi_j) \setminus \operatorname{Ker}\pi_i$ and $x \in S$ with $\pi_j(x) > 0$. Then

$$u := \pi_i(y)x - \pi_i(x)y \in \operatorname{Ker}\pi_i.$$

Condition i) yields an element $z \in Q(S)$ with

$$\pi_i(z) = \pi_i(\pi_i(y)x) = \pi_i(\pi_i(x)y),$$

$$z - \pi_i(y)x \in S \cap \operatorname{Ker}\pi_i \subseteq \operatorname{Ker}\pi_j$$

and

$$z - \pi_i(x)y \in S \cap \operatorname{Ker}\pi_i \subseteq \operatorname{Ker}\pi_j.$$

In particular, $\pi_j(z - \pi_i(y)x) = \pi_j(z - \pi_i(x)y) = 0$. But this gives

$$0 = \pi_j(z - \pi_i(x)y) = \pi_j(z) - \pi_i(x)\pi_j(y) = \pi_j(z),$$

and the contradiction

$$0 = \pi_j(z - \pi_i(y)x) = \pi_j(z) - \pi_i(y)\pi_j(x) = -\pi_i(y) \cdot \pi_j(x) < 0.$$

For the rest of the proof, let $K \subseteq J$ be a subset of J with the property that

$$S = \{x \in Q(S) \mid \pi_j(x) \geq 0 \text{ for all } j \in K\}$$

where $\pi_j(x) = 0$ for almost all $j \in K$ and any fixed $x \in Q(S)$. The representation $(*)$ shows that such subsets K exist.

For iii) $\Rightarrow$ iv), we fix $i \in J$ and assume that iii) is true for π_i. Moreover we fix $j \in J$ and assume that $S \cap \operatorname{Ker}\pi_i \subseteq S \cap \operatorname{Ker}\pi_j$. Define $L := K \cup \{i, j\}$.

From iii) we know that

$$\begin{aligned} L_0 :&= \{k \in L \,|\, (S \cap \text{ Ker } \pi_i) \subseteq \text{ Ker } \pi_k\} \\ &= \{k \in L \,|\, S \cap \text{ Ker } \pi_i = S \cap \text{ Ker } \pi_k\}. \end{aligned}$$

We choose some $v \in S$ with $\pi_i(v) > 0$. Then $\pi_j(v) > 0$ by our assumption and $\alpha = \frac{\pi_j(v)}{\pi_i(v)} > 0$. Let $w \in S$ be arbitrary. If $\pi_i(w) = 0$, then $\pi_j(w) = 0$ and $\pi_i(w) = \alpha\pi_j(w)$. Assume that $\pi_i(w) > 0$. Then

$$i \in L_0' := \{k \in L_0 \,|\, \pi_k(w) \neq 0\}.$$

Since L_0' is finite, we can define $m = \prod_{k \in L_0'} \pi_k(w)$ and

$$\lambda = \text{ max } \{r \in \mathbb{N} \,|\, r \geq 1, \, \pi_k(mv - rw) \geq 0 \text{ for all } k \in L_0\}.$$

For some $k_1 \in L_0'$ the equality

$$\pi_{k_1}(mv - \lambda w) = 0$$

holds. For every $k \in L_2 := \{k \in L \backslash L_0 \,|\, \pi_k(mv - \lambda w) \neq 0\}$ we choose $x_k \in S \cap \text{ Ker } \pi_i$ with

$$\pi_k(x_k) > \max\{0, \pi_k(\lambda w - mv)\}.$$

Since L_2 is finite (and possibly empty), the element $x := \sum_{\mu \in L_2} x_\mu$ is well-defined and $x \in S \cap \text{ Ker } \pi_i \subseteq \text{ Ker } \pi_j$.

In the next step, we show that $u = x + mv - \lambda w \in S$ (i.e., that $\pi_k(u) \geq 0$ for all $k \in L$). We have already seen that for $k \in L_0$ we have

$$\pi_k(u) = \pi_k(x) + \pi_k(mv - \lambda w) \geq \pi_k(mv - \lambda w) \geq 0.$$

For $k \in L_2$ we get

$$\pi_k(u) = \pi_k(x) + \pi_k(mv - \lambda w) \geq \pi_k(x_k) + \pi_k(mv - \lambda w) \geq 0,$$

and finally for $k \in L \backslash (L_0 \cup L_2) = (L \backslash L_0) \backslash L_2$ we have that

$$\pi_k(u) = \pi_k(x) \geq 0.$$

Therefore $u \in S$, and it follows for the above chosen $k_1 \in L_0'$ with $\pi_{k_1}(mv - \lambda w) = 0$ that

$$\pi_{k_1}(u) = \pi_{k_1}(x) + \pi_{k_1}(mv - \lambda w) = \pi_{k_1}(x) = 0,$$

since $x \in S \cap \text{ Ker } \pi_i = S \cap \text{ Ker } \pi_{k_1}$. In particular, $u \in S \cap \text{ Ker } \pi_i \subseteq \text{ Ker } \pi_j$. This gives

$$\pi_j(u) = 0 = \pi_i(u) = \pi_i(mv - \lambda w) = \pi_j(mv - \lambda w).$$

Hence

$$\lambda\pi_j(w) = \pi_j(mv), \; \lambda\pi_i(w) = \pi_i(mv)$$

and

$$\pi_j(w) = \frac{1}{\lambda}\pi_j(mv) = \frac{\pi_j(mv)}{\pi_i(mv)}\pi_i(w) = \frac{\pi_j(v)}{\pi_i(v)}\pi_i(w) = \alpha\pi_i(w).$$

Since $w \in S$ was chosen arbitrarily, it follows that $\pi_j = \alpha\pi_i$.

For iv) $\Rightarrow$ i), assume that $x, y \in Q(S)$ are given with $\pi_i(x) \geq \pi_i(y)$. As above, we define

$$L := K \cup \{i, j\}, L_0 := \{k \in L \,|\, (S \cap \text{ Ker } \pi_i) \subseteq \text{ Ker } \pi_k\}, L_1 := L \backslash L_0,$$

and $L_2 := \{k \in L_1 \,|\, \pi_k(x - y) \neq 0\}$. Note that L_2 is a finite set. By iv) we know that

$$\pi_k = \alpha_k \pi_i, \quad \text{for all} \quad k \in L_0 \text{ where } 0 < \alpha_k \in \mathbb{Q}.$$

For every $k \in L_1$ there exists $x_k \in S \cap \text{Ker } \pi_i$ with

$$\pi_k(x - y) + \pi_k(x_k) \geq 0.$$

Defining $z = x + \sum_{\mu \in L_2} x_\mu$, we get

$$z - x = \sum_{\mu \in L_2} x_\mu \in S.$$

We prove that $z - y \in S$ by showing that $\pi_k(z - y) \geq 0$ for all $k \in L$.

If $k \in L_2$, then

$$\begin{aligned} \pi_k(z - y) &= \pi_k \left(x - y + \sum_{\mu \in L_2} x_\mu \right) = \pi_k(x - y) + \sum_{\mu \in L_2} \pi_k(x_\mu) \\ &= \pi_k(x - y) + \pi_k(x_k) + \sum_{\mu \in L_2 \backslash \{k\}} \pi_k(x_\mu) \geq 0. \end{aligned}$$

For $k \in L_0$ we get

$$\pi_k(z - y) = \pi_k(x - y) = \alpha_k \pi_i(x - y) \geq 0.$$

Finally, for $k \in L_1 \backslash L_2$ we have

$$\pi_k(z - y) = \pi_k \left(\sum_{\mu \in L_2} x_\mu \right) \geq 0.$$

□

Again, let the Krull monoid S be given in the form $(*)$. Thus,

$$S = \{x \in Q(S) \,|\, \pi_j(x) \geq 0 \text{ for all } j \in K\}$$

where $(\pi_j)_{j \in K}$ is a family of nonzero states of S such that $\pi_j(x) = 0$ for almost all $j \in K$ and any fixed $x \in Q(S)$.

Proposition 2.4. *For every $\emptyset \neq I \subseteq K$ the following statements are equivalent:*

i) $S = \{x \in Q(S) \,|\, \pi_i(x) \geq 0$ *for all* $i \in I\}$.

ii) *If π is an essential state of S, then there exists $i \in I$ and $\alpha \in \mathbb{Q}, \alpha > 0$, such that*

$$\pi = \alpha\pi_i.$$

Proof. i) $\Longrightarrow$ ii) Let π be an essential state of S. It suffices to show that $\pi \in \mathbb{Q}\pi_i$ for some $i \in I$. Let $i_0 \in I$ and $v, w \in S$ with $\pi(v) > 0, \pi_{i_0}(w) > 0$ and define $u := v + w$. Then $\pi(u) > 0$ and

$$i_0 \in I_1 := \{i \in I \mid \pi_i(u) > 0\}, \quad |I_1| < \infty.$$

We claim that $\pi \in \mathbb{Q}\pi_i$ for some $i \in I_1$. Assume the contrary. Then $\pi_i \notin \mathbb{Q}\pi$ and we apply Lemma 2.3 ii) to get for every $i \in I_1$ an element $x_i \in S$ with $\pi(x_i) = 0$ and $\pi_i(x_i) > 0$. With $x := \sum_{i \in I_1} x_i \in S$ it follows that $\pi(x) = 0$ and for every $i \in I_1$

$$\pi_i(x) = \pi_i(x_i) + \sum_{j \in I_1 \setminus \{i\}} \pi_i(x_j) > 0.$$

Let $i_1 \in I_1$ with

$$\frac{\pi_{i_1}(x)}{\pi_{i_1}(u)} = \min \left\{ \frac{\pi_i(x)}{\pi_i(u)} \;\middle|\; i \in I_1 \right\}$$

and $z := \pi_{i_1}(u)x - \pi_{i_1}(x)u$. From i) we get $z \in S$, since

$$\pi_i(z) = \pi_{i_1}(u)\pi_i(x) - \pi_{i_1}(x)\pi_i(u) \geq 0 \text{ for } i \in I_1,$$

and

$$\pi_i(z) = \pi_{i_1}(u)\pi_i(x) \geq 0 \text{ for } i \in I \setminus I_1.$$

But $\pi(z) = -\pi_{i_1}(x)\pi(u) < 0$, a contradiction to the fact that $\pi(S) \subseteq \mathbb{N}$.

ii)$\Longrightarrow$ i) Let

$$N := \{w \in Q(S) \mid \pi_i(w) \geq 0 \text{ for all } i \in I\}.$$

For $y \in N$ we consider the finite set $K(y) := \{j \in K \mid \pi_j(y) < 0\}$ and prove that $|K(y)| = 0$ (i.e., that $A := \{y \in N \mid |K(y)| \geq 1\} = \varnothing$). Assume the contrary and choose $y \in A$ such that $|K(y)|$ is minimal. Let $j_0 \in K$ such that π_{j_0} is an essential state of S. From ii) we know that $j_0 \notin K(y)$. For every $j \in \{j_0\} \cup K(y)$ there exists $x_j \in S$ with $\pi_j(x_j) > 0$. Thus $x := \sum_{j \in \{j_0\} \cup K(y)} x_j \in S$ and $\pi_j(x) > 0$ for every $j \in \{j_0\} \cup K(y)$. Let $j_1 \in K(y)$ such that

$$0 > \frac{\pi_{j_1}(y)}{\pi_{j_1}(x)} = \max \left\{ \frac{\pi_j(y)}{\pi_j(x)} \;\middle|\; j \in K(y) \right\}.$$

We define $z := \pi_{j_1}(x)y - \pi_{j_1}(y)x$. Since $\pi_{j_1}(y) < 0$ it follows for every $j \in K \setminus K(y)$ that

$$\pi_j(z) = \pi_{j_1}(x)\pi_j(y) - \pi_{j_1}(y)\pi_j(x) \geq -\pi_{j_1}(y)\pi_j(x) \geq 0.$$

In particular, $z \in N$ since $I \subseteq K \backslash K(y)$, and $K(z) \subseteq K(y)$. Moreover $|K(z)| < |K(y)|$ because $j_1 \notin K(z)$. From the minimality of $|K(y)|$ we conclude $|K(z)| = 0$ (i.e., $z \in S$). Since

$$\pi_{j_0}(z) = \pi_{j_1}(x)\pi_{j_0}(y) - \pi_{j_1}(y)\pi_{j_0}(x) \geq -\pi_{j_1}(y)\pi_{j_0}(x) > 0$$

it follows that

$$z \in (S \cap \text{ Ker } \pi_{j_1}) \not\subseteq (S \cap \text{ Ker } \pi_{j_0}).$$

But, by Lemma 2.3 iii), there has to be an essential state π of S with

$$(S \cap \text{ Ker } \pi_{j_1}) \subseteq (S \cap \text{ Ker } \pi).$$

Since π_{j_0} was already arbitrarily chosen, this contradiction finishes the proof. □

We call a state π of S a *normal* state, if $\pi(Q(S)) = \mathbb{Z}$. For every nonzero state $\pi : Q(S) \to \mathbb{Z}$, the image $\pi(Q(S))$ is a nonzero ideal $d\mathbb{Z}$ of $\mathbb{Z}$ where $d \in \mathbb{N}, d \geq 1$, and $\pi_{\text{nor}} := \frac{1}{d}\pi$ is normal. Let K_N denote the set of all normal states of a given Krull monoid S. From Proposition 2.4 we obtain the following.

Corollary 2.5. *There is a unique minimal subset $I(S) \subseteq K_N$ such that*

$$S = \{x \in Q(S) \mid \pi(x) \geq 0 \quad \textit{for all } \pi \in I(S)\}.$$

The set $I(S)$ consists exactly of the essential normal states of S. Moreover $\pi(x) = 0$ for almost all $\pi \in I(S)$ and any fixed $x \in Q(S)$.

Proof. Let L be a set of nonzero states of S such

$$S = \{x \in Q(S) \,|\, \pi(x) \geq 0 \text{ for all } \pi \in L\}$$

and $\pi(x) = 0$ for almost all $\pi \in L$ and any fixed $x \in Q(S)$. Define $\widetilde{L} := \{\pi_{\text{nor}} \,|\, \pi \in L\}$. Obviously $S = \{x \in Q(S) \,|\, \pi_{\text{nor}}(x) \geq 0 \text{ for all } \pi \in L\}$, and the set $I(S)$ of normal essential states of S is a subset of $\widetilde{L}$ by Proposition 2.4. In particular $\pi(x) = 0$ for almost all $\pi \in I(S)$ and any fixed $x \in Q(S)$. Now we may again apply Proposition 2.4 and conclude that $S = \{x \in Q(S) \,|\, \pi(x) \geq 0 \text{ for all } \pi \in I(S)\}$. □

We consider the form

$$S = \{x \in Q(S) | \pi(x) \geq 0 \quad \text{for all } \pi \in I(S)\}$$

as the (uniquely determined) *normal representation* of the Krull monoid S. It gives rise to a *divisor theory*

$$\varphi : Q(S) \to \mathbb{Z}^{(I(S))}, \qquad \text{(direct sum)}$$
$$\varphi(x) := (\pi(x))_{\pi \in I(S)},$$

with Ker $\varphi = S \cap (-S) = \{0\}$, which maps $Q(S)$ onto a free subgroup of $\mathbb{Z}^{(I(S))}$ such that

$$\varphi(S) = \mathbb{N}^{(I(S))} \cap \varphi(Q(S)) = \mathbb{N}^{(I(S))} \cap Q(\varphi(S)).$$

The quotient group

$$\mathrm{Cl}\,(S) := \mathbb{Z}^{(I(S))}/\varphi(Q(S))$$

is the *divisor class group* of S. It is a direct consequence of the construction that isomorphic Krull monoids have isomorphic divisor class groups.

Now suppose that $A \in \mathbb{Z}^{m\times n}$ and S is isomorphic to the Diophantine monoid

$$M_A = \{x \in \mathbb{N}^n \mid Ax = 0\}.$$

For $1 \le i \le n$ let $p_i : \mathbb{Z}^n \to \mathbb{Z}$, with $p_i(x_1, \dots, x_n) = x_i$, denote the natural surjection. The restriction maps $\pi_i = p_i|Q(M_A)$ from $Q(M_A)$ into $\mathbb{Z}$ are states of M_A. We call them the *canonical projections* of $Q(M_A)$. Note that a relation $\pi_i = \pi_j$ does not imply $i = j$. Moreover, for $1 \le i \le n$ we define $c_i = \gcd\,(x_i \mid x = (x_1, \dots, x_n) \in M_A) \in \mathbb{N}$ where $c_i = 0$ if and only if $x_i = \pi_i(x) = 0$ for all $x \in M_A$. We call the product $w(M_A) = \prod_{i=1}^{n} c_i$ the *weight* of the monoid M_A. If $n \ge 2$ and $c_i = 0$, then M_A is canonically isomorphic to the monoid $M_{\widetilde{A}} \subseteq \mathbb{N}^{n-1}$, where $\widetilde{A} \in \mathbb{Z}^{m\times(n-1)}$ is given by canceling the i-th column of A. Therefore it suffices to study the situation $w(M_A) \ne 0$. All canonical projections $\pi_i, 1 \le i \le n$, are normal if and only if $w(M_A) = 1$. In this case, every normal essential state of M_A is a canonical projection (as follows immediately from Corollary 2.5), hence there are at most n essential states of M_A. In general, not all normal canonical projections of $Q(M_A)$ are essential states of M_A. Let

$$I(M_A) := \{i \mid 1 \le i \le n,\ \pi_i \text{ is an essential state of } M_A\}$$

and note that the following statements are equivalent:

i) $w(M_A) \ne 0$,
ii) there exist elements $x = (x_1, \dots, x_n) \in M_A$ with $x_i > 0$ for $1 \le i \le n$.

Lemma 2.6. *Let M_A be a Diophantine monoid with $A \in \mathbb{Z}^{m\times n}$ and $w(M_A) \ne 0$. The following statements are true:*

i) *$Q(M_A) = \{x \in \mathbb{Z}^n | Ax = 0\}$, and there exists a linearly independent system of vectors $v_1, v_2, \dots v_{n-r} \in M_A$, where $r = \mathrm{rank}\, A$.*
ii) *Let c_i be defined as above and $D := \mathrm{diag}\,(c_1, \dots, c_n) \in \mathbb{Z}^{n\times n}$. The map $M_{AD} \to M_A$, defined by $y \mapsto Dy$, is an isomorphism of monoids and $w(M_{AD}) = 1$.*
iii) *There are at most n normal essential states of M_A.*

Proof. i): The assumption $w(M_A) \neq 0$ yields an element $x = (x_1, \ldots, x_n) \in M_A$ with $x_i > 0$ for $1 \leq i \leq n$. Obviously $Q(M_A) \subseteq G = \{u \in \mathbb{Z}^n | Au = 0\}$. If $y \in G$ then $z = kx - y \in \mathbb{N}^n \cap G = M_A$ for $k \in \mathbb{N}$ sufficiently big, hence $y = kx - z \in Q(M_A)$ and $Q(M_A) = G$. Let $r = \operatorname{rank} A$ and $w_1, \ldots, w_{n-r}$ be a basis of the $\mathbb{Q}$-vector space $W = \{z \in \mathbb{Q}^n \,|Az = 0\}$. We may assume that $w_j \in \mathbb{Z}^n$ for $1 \leq j \leq n-r$. Let $m_0 \in \mathbb{N}$ with $m_0 x + w_j \in M_A, 1 \leq j \leq n-r$. Since the family $(kx + w_j \,|1 \leq j \leq n-r)$ is linearly independent for all but at most one $k \in \mathbb{N}$, we are done.

We leave the verification of statements ii) and iii) to the reader. □

3. The representation of Krull monoids by matrices.

In this section, we show that any Krull monoid S with a finite number e of essential states must be isomorphic to a Diophantine monoid. We describe the structure of the corresponding matrix and show in principle its computation, as well as the computation of the divisor class group of S. For the class group $\operatorname{Cl}(S)$ defined in the previous section, we have the short exact sequence

$$0 \longrightarrow Q(S) \xrightarrow{\varphi} \mathbb{Z}^{(I)} \xrightarrow{\rho} \operatorname{Cl}(S) \longrightarrow 0$$

where $I = I(S)$ indexes the set of all normalized essential states of S and where ρ denotes the canonical epimorphism. To obtain the desired description of S by a matrix, we will use a particular basis for the $\mathbb{Z}$-module $\mathbb{Z}^{(I)}$. For an arbitrary $\mathbb{Z}$-module M, let *rank* M denote the minimal number of generators of M and *free rank* M the maximal length of a free family in M. Of course, if M is a free module, then the rank and the free rank of M coincide and are equal to the cardinality of a $\mathbb{Z}$-basis of M (since $M = \{0\}$ is generated by the empty set, one has rank $\{0\}$ = free rank $\{0\} = 0$).

Theorem 3.1. *For a (reduced) Krull monoid S, the number e of essential states is finite if and only if the* rank *r of $Q(S)$, the* free rank *h of $\operatorname{Cl}(S)$, and the* rank *k of the torsion group of $\operatorname{Cl}(S)$ are all finite. In this case, the following statements apply.*

i) *There exist natural numbers $\alpha_1, \ldots, \alpha_k \geq 2$ with $\alpha_{i+1} \mid \alpha_i$ for $1 \leq i \leq k-1$ such that*

$$\operatorname{Cl}(S) \simeq \mathbb{Z}_{\alpha_1} \oplus \cdots \oplus \mathbb{Z}_{\alpha_k} \oplus \mathbb{Z}^h$$

and $h + r = e$.

ii) *S is isomorphic to a Diophantine monoid M_A with $A \in \mathbb{Z}^{m \times n}$ for $m = k + h$ and $n = k + e$ (if $h = k = 0$, then $m = 0$ and $M_A = \mathbb{N}^e$).*

iii) *The matrix A has a block structure*

$$A = \begin{array}{|c|c|}\hline A_{11} & A_{12} \\ \hline A_{21} & 0 \\ \hline \end{array}$$

where $A_{11} \in \mathbb{N}^{k\times e}$ *with entries of the* i*-th row in* $\{0, 1, \dots, \alpha_i - 1\}$, $A_{12} = -\mathrm{diag}(\alpha_1, \dots, \alpha_k) \in \mathbb{N}^{k\times k}$ *and* $A_{21} \in \mathbb{N}^{h\times e}$ *contains in each row at least two strictly positive and two strictly negative entries.*

Proof. $M = \varphi(Q(S))$ is a submodule of the free module $\mathbb{Z}^{(I)}$ and therefore free. If $e = |I|$ is finite then rank M is finite and, hence, r is finite. By its definition as the quotient of $\mathbb{Z}^{(I)}$ and M, the class group is finitely generated and h and k are finite. Conversely, if r, h and k are finite then

$$k + h = \ \mathrm{rank}\, \mathrm{Cl}\,(S) \geq \ \mathrm{rank}\, \mathbb{Z}^{(I)} - \ \mathrm{rank}\, \varphi(Q(S))$$

and hence $e \leq k + h + r$ is finite.

Step I. In a first step, we analyze certain submodules of $\mathbb{Z}^{(I)}$ for an arbitrary index set I. Let $(b_i)_{i\in I}$ be a basis of the free module $\mathbb{Z}^{(I)}$. For a given set $\{\alpha_j \mid j \in J\} \subseteq \mathbb{N}\backslash\{0\}$, $\emptyset \neq J \subseteq I$, let M be the free submodule with basis $(\alpha_j b_j)_{j\in J}$. Consider the epimorphism $\psi\colon \mathbb{Z}^{(I)} \longrightarrow \bigoplus_{i\in J'} \mathbb{Z}_{\alpha_i} \bigoplus \mathbb{Z}^{(I\backslash J)}$ for $J' = \{j \in J \mid \alpha_j \neq 1\}$ defined by

$$\psi\left(\sum_{i\in I} r_i b_i\right) = \sum_{i\in J'} (r_i \mod \alpha_i) b_i + \sum_{i\in I\backslash J} r_i b_i.$$

Obviously, $\mathrm{Ker}\, \psi = M$ and, hence,

$$\mathbb{Z}^{(I)}/M \simeq \bigoplus_{i\in J'} \mathbb{Z}_{\alpha_i} \bigoplus \mathbb{Z}^{(I\backslash J)}. \tag{2}$$

To describe M by a matrix, let $(u_i)_{i\in I}$ be the standard basis of $\mathbb{Z}^{(I)}$ and $u_j = \sum_{i\in I} c_{ij} b_i$, $c_{ij} \in \mathbb{Z}$ for $i, j \in I$. Define a block matrix

(3)

$$A = \begin{array}{c|c|c} & I & J' \\ \hline J' & A_{11} & A_{12} \\ \hline I\backslash J & A_{21} & 0 \\ \hline \end{array}$$

where the blocks in the above diagram are given as follows:

A_{11}: For $i \in J'$, $j \in I$, let $a_{ij} \in \{0, 1, \ldots, \alpha_i - 1\}$ be the residue of $c_{ij} \mod \alpha_i$.
A_{12}: For $i, j \in J'$, let $a_{ij} = -\alpha_i \delta_{ij}$.
A_{21}: For $i \in I \backslash J$, $j \in I$, let $a_{ij} = c_{ij}$.

Note that A_{21} cannot have a zero-row. Namely, $c_{i_0 j} = 0$ for $i_0 \in I \backslash J$ and all $j \in I$ would imply $u_j = \sum_{i \neq i_0} c_{ij} b_i$ for all $j \in I$, which contradicts the freeness of $(b_i)_{i \in I}$.

For $N_A := \left\{ (x, y) \in \mathbb{Z}^{(I)} \times \mathbb{Z}^{(J')} \mid A \begin{bmatrix} x \\ y \end{bmatrix} = 0 \right\}$ and $\pi \colon \mathbb{Z}^{(I)} \times \mathbb{Z}^{(J')} \longrightarrow \mathbb{Z}^{(I)}$, defined by $\pi(x, y) = x$, we shall show that $\pi \colon N_A \longrightarrow M$ is an isomorphism of $\mathbb{Z}$-modules.

For $x \in \mathbb{Z}^{(I)}$ we have that

$$x = \sum_j x_j u_j = \sum_j x_j \sum_i c_{ij} b_i = \sum_i \left(\sum_j c_{ij} x_j \right) b_i.$$

Therefore, $x \in M$ if and only if

$$\alpha_i \Big| \sum_j c_{ij} x_j \text{ for } i \in J' \text{ and } \sum_j c_{ij} x_j = 0 \text{ for } i \in I \backslash J,$$

which is equivalent to

$$(4) \quad \sum_{j \in I} a_{ij} x_j = \alpha_i y_i \text{ with } y_i \in \mathbb{Z} \text{ for } i \in J' \text{ and } \sum_{j \in I} a_{ij} x_j = 0 \text{ for } i \in I \backslash J.$$

According to the definition of A, this means that $x \in M$ if and only if $(x, y) \in N_A$ for some $y \in \mathbb{Z}^{(J')}$. Thus, $\pi \colon N_A \longrightarrow M$ is a well-defined epimorphism. π is injective because by (4) $y = (y_i)_{i \in J'}$ is uniquely determined by $x = (x_j)_{j \in I}$. This shows that $\pi \colon N_A \longrightarrow M$ is an isomorphism.

Step II. Consider now a (reduced) Krull monoid S for which $I = I(S) = \{1, \ldots, e\}$ is finite and let $M = \varphi(Q(S)) \subseteq \mathbb{Z}^{(I)}$. Since $\mathbb{Z}^{(I)}$ is finitely generated, by the elementary divisor theorem (see [**9**]) there exist a basis $(b_i)_{i \in I}$ of $\mathbb{Z}^{(I)}$ and numbers $\alpha_j \in \mathbb{N} \backslash \{0\}$ for $1 \leq j \leq r \leq e$ with $\alpha_j \neq 1$ for $1 \leq j \leq k \leq r$ and $\alpha_{j+1} \mid \alpha_j$ for $1 \leq j \leq k - 1$ such that $(\alpha_j b_j)_{1 \leq j \leq r}$ is a basis of M ($k = 0$ admitted). Obviously, $r = \operatorname{rank} \varphi(Q(S)) = \operatorname{rank} Q(S)$. Setting $J = \{1, \ldots, r\}$ and $J' = \{1, \ldots, k\}$, from (2) in Step I, we obtain for $M = \varphi(Q(S))$ that $\operatorname{Cl}(S) = \mathbb{Z}^{(I)} / M \simeq \bigoplus_{i=1}^{k} \mathbb{Z}_{\alpha_i} \bigoplus \mathbb{Z}^{I \backslash J}$.

It follows that k is the rank of the torsion group of $\operatorname{Cl}(S)$ and that $e - r = |I \backslash J|$ is the free rank of $\operatorname{Cl}(S)$. This proves Part i) of Theorem 3.1.

Further, for the matrix A defined by (3) in Step I, we have that $\pi \colon N_A \longrightarrow M$ is an isomorphism. Hence the equations in (4) show that $\pi(x, y) \in \mathbb{N}^I$ implies $(x, y) \in \mathbb{N}^I \times \mathbb{N}^{J'}$. Since S is a Krull monoid it follows that

$\varphi(S) = \mathbb{N}^I \cap \varphi(Q(S)) = \mathbb{N}^I \cap M$. Combining these facts, we obtain for $M_A := (\mathbb{N}^I \times \mathbb{N}^{J'}) \cap N_A$ that $S \xrightarrow{\varphi} \mathbb{N}^I \cap M \xrightarrow{\pi^{-1}} M_A$. Since φ and π^{-1} are monoid isomorphisms, we have that S is isomorphic to the Diophantine monoid M_A.

Also, by (3) of Step I, the matrix A is a block matrix where $A_{11} \in \mathbb{Z}^{k\times e}$ with entries $a_{ij} \in \{0, 1, \dots, \alpha_i - 1\}$, $A_{12} = -\mathrm{diag}(\alpha_1, \dots, \alpha_k) \in \mathbb{N}^{k\times k}$ and $A_{21} \in \mathbb{Z}^{h\times e}$. In particular, $A \in \mathbb{Z}^{m\times n}$ with $m = k + h$, $n = k + e$. This proves Part ii) and the first part of iii) of Theorem 3.1.

It remains to show the statement about A_{21} in iii). Pick $i \in I\backslash J$ and let $I_+ = \{j \in I \mid a_{ij} > 0\}$ and $I_- = \{k \in I \mid a_{ik} < 0\}$. Since by Step I the submatrix A_{21} cannot have a zero-row, we must have that I_+ or I_- is nonempty. We shall show in fact that both I_+ and I_- must be nonempty. Suppose that $j_1 \in I_+$. Since $J \neq \emptyset$ and $i \in I\backslash J$ imply $|I| \geq 2$, there exists $j_2 \in I$, $j_2 \neq j_1$. Let $(\pi_j)_{j\in I}$ be the set of normalized essential states of S. By the isomorphism of S and M_A proved above, one has $x \in \mathbb{N}^I$ with $\sum_{j\in I} a_{ij}x_j = 0$ for $x_j = \pi_j(s)$ with $j \in I$ and $s \in S$. Since π_{j_2} is essential, there exists by Lemma 2.3 an $s \in S$ with $\pi_{j_2}(s) = 0$ and $\pi_{j_1}(s) > 0$. Therefore, there must be some $j \in I$ with $a_{ij} < 0$. Thus, $I_+ \neq \emptyset$ implies $I_- \neq \emptyset$. Similarly, $I_- \neq \emptyset$ implies $I_+ \neq \emptyset$. Therefore, there exist $j_1 \in I_+$ and $k_1 \in I_-$. Suppose now $I_+ = \{j_1\}$. Since π_{j_1} is essential, by Lemma 2.3 there exists $s \in S$ with $\pi_{j_1}(s) = 0$ and $\pi_{k_1}(s) > 0$. But then, for $x = (\pi_j(s))_j$, we obtain $0 = -a_{ij_1}x_{j_1} = \sum_{j\neq j_1} a_{ij}x_j < 0$, which is a contradiction.

Thus we must have that $|I_+| \geq 2$. Similarly, $|I_-| \geq 2$. This proves the statement about A_{21} in Part iii) of Theorem 3.1. □

Remarks 3.2.

1. The Diophantine monoid M_A in Theorem 3.1 ii) consists of two different kinds of equations. The first k equations are of type 1 and the remaining h equations are of type 2 in the sense of [**2**, Theorem 1.3]. The latter type does not occur if and only if $h = 0$, or, equivalently, $r = e$ which for $e \leq 3$ must happen by Theorem 3.1 iii).
2. Concerning Krull monoids S with infinitely many essential states, Step I in the proof of Theorem 3.1 can be used provided the module $M = \varphi(Q(S))$ meets the assumptions made there. In general, a submodule M of $\mathbb{Z}^{(I)}$ does not satisfy these assumptions as the following simple example shows. Let $I = \mathbb{N}$, $(u_i)_{i\in\mathbb{N}}$ the standard basis of $\mathbb{Z}^{(\mathbb{N})}$, $\mathbb{Q} = \{q_i\}_{i\in\mathbb{N}}$ and $\tau\colon \mathbb{Z}^{(\mathbb{N})} \longrightarrow \mathbb{Q}$ be the $\mathbb{Z}$-homomorphism defined by $\tau(u_i) = q_i$ for all $i \in \mathbb{N}$. If the submodule $M = \mathrm{Ker}\,\tau$ of $\mathbb{Z}^{(\mathbb{N})}$ would satisfy the assumptions of Step I, then by (2) $\mathbb{Q} \simeq \mathbb{Z}^{(\mathbb{N})}/M$ should be isomorphic to a direct sum of copies of $\mathbb{Z}$ and $\mathbb{Z}_\alpha$ (which is not the case). If, however, for I infinite $\mathrm{Cl}\,(S)$ is finitely generated, then one

can argue that S is isomorphic to a monoid M_A where the number of rows of A is rank $\mathrm{Cl}\,(S)$ and the "number" of columns of A is given by the cardinality of I augmented by a finite set. Similarly, if $\mathrm{Cl}\,(S)$ is free, then S is isomorphic to a monoid M_A with $|I \backslash J|$ equations in $|I|$ unknowns.

From Theorem 3.1 we obtain the following characterization of Diophantine monoids.

Corollary 3.3. *For a reduced monoid S the following statements are equivalent:*

i) *S is a Krull monoid with finitely many essential states.*
ii) *S is isomorphic to a Diophantine monoid.*
iii) *S is isomorphic to a monoid $W \cap \mathbb{N}^n$ for a vector subspace W of $\mathbb{Q}^n$ and some $n \geq 1$.*
iv) *S is isomorphic to a full and expanded submonoid T of $\mathbb{N}^n$ (i.e., $x, y \in T,\ y - x \in \mathbb{N}^n$ imply $y - x \in T$, and $kz \in T$ for $k \geq 1,\ z \in \mathbb{N}^n$, implies $z \in T$).*
v) *S is root-closed and finitely generated.*

Proof. i) $\Rightarrow$ ii) follows directly from Theorem 3.1. Obviously, ii) $\Rightarrow$ iii). Since $T = W \cap \mathbb{N}^n$ is full and expanded, iii) $\Rightarrow$ iv). From iv) it follows by Dickson's Lemma (see [**14**, Theorem 5.1]) that T, and hence S, is finitely generated. Since T is expanded, S must be root-closed (i.e., $kz \in S$ for $k \geq 1,\ z \in Q(S)$ implies $z \in S$). This yields iv) $\Rightarrow$ v). Finally, v) $\Rightarrow$ i) follows from a well-known theorem of Halter-Koch [**7**, Theorem 5] and the main result in [**13**], by which a root-closed and finitely generated monoid is a Krull monoid described by finitely many states. □

Remarks 3.4.

1. In [**13**, Corollary 1] a description of the class group is given by employing terminology and methods from convex analysis. Using results from [**13**], in [**10**, Proposition 2] it is shown that a monoid S satisfying $Q(S) = \mathbb{Z}^n$ is isomorphic to the monoid of nonnegative solutions of a homogeneous system of integral linear equations if and only if S is a Krull monoid which holds if any only if S is finitely generated and root-closed. The method used in the proof of Theorem 3.1 is direct and does not involve convex analysis. Moreover, Theorem 3.1 describes the representing matrix $A \in \mathbb{Z}^{m \times n}$ in terms of the class group and the number of essential states of S. This yields in particular that $m = \ \mathrm{rank}\,\mathrm{Cl}\,(S)$.
2. Corollary 3.3 applies in particular to additive submonoids S of $\mathbb{N}^n$. For this case it has been shown in [**8**, Lemma 3] that S is the set of solutions in the nonnegative integers of a system of homogeneous linear equations with rational coefficients if and only if $S = W \cap \mathbb{N}^n$

for a vector subspace W of $\mathbb{Q}^n$ or, equivalently, S is full and expanded. An additive submonoid S of $\mathbb{N}^n$ is called a full affine semigroup if $S = M \cap \mathbb{N}^n$ for a subgroup M of $\mathbb{Z}^n$ or, equivalently, $S = Q(S) \cap \mathbb{N}^n$ (see [**14**, Chapter 7] for more about these semigroups). Obviously, such a semigroup is root-closed, but it need not be expanded as the example $S = 2\mathbb{N}$ shows. Furthermore, such a semigroup is a Krull monoid with finitely many essential states. From Corollary 3.3 one concludes that an arbitrary reduced monoid is a Krull monoid with finitely many essential states if and only if it is isomorphic to a full affine semigroup.

By Theorem 3.1 Part ii), we know how to describe an arbitrary Krull monoid S having a finite number of essential states by a particular matrix adapted to S. The following Lemma addresses, conversely, a Krull monoid given by an arbitrary matrix. For a matrix A, let $\operatorname{im} A$ denote the image of the mapping induced by A.

Lemma 3.5. *Let $S \simeq M_A$ with $A \in \mathbb{Z}^{m\times n}$, $m \geq 1, n \geq 1$ and weight $w(M_A) = 1$. Arrange A such that the first e canonical projections are exactly the normal essential states of M_A and let $A = [A'A'']$ where $A' \in \mathbb{Z}^{m\times e}$, $A'' \in \mathbb{Z}^{m\times(n-e)}$. The following statements hold:*

i) $\operatorname{Cl}(S) \simeq \operatorname{im} A'/(\operatorname{im} A' \cap \operatorname{im} A'')$.
ii) $n = \operatorname{rank} A + \operatorname{rank} Q(S) = \operatorname{rank} A'' + e$.
iii) $\operatorname{rank} A' - \operatorname{rank}(\operatorname{im} A' \cap \operatorname{im} A'') = \text{free rank } \operatorname{Cl}(S) \leq \operatorname{rank} \operatorname{Cl}(S) \leq \operatorname{rank} A'$.
iv) $\operatorname{rank} \operatorname{Cl}(S) \leq m$ *and* $\operatorname{rank} \operatorname{Cl}(S) + \operatorname{rank} Q(S) \leq n$.

In particular, if $A' = A$, then one has $\operatorname{Cl}(S) \simeq \mathbb{Z}^k$, $k = \operatorname{rank} A$ and $\operatorname{rank} \operatorname{Cl}(S) + \operatorname{rank} Q(S) = n$.

Proof. It can be assumed that $S = M_A$. By assumption the divisor theory $\varphi\colon Q(S) \longrightarrow \mathbb{Z} = EA$ is given by $\varphi(y_1, \ldots, y_n) = (y_1, \ldots, y_e)$. From Lemma 2.6 it follows that $Q(S) = \operatorname{Ker} A$.

i) Consider $f\colon \operatorname{im} A' \longrightarrow \operatorname{Cl}(S)$ defined by $A'x \longmapsto x + \varphi\big(Q(S)\big)$ for $x \in \mathbb{Z}^e$. The mapping f is well-defined. For, if $A'x = 0$, then $y = \begin{bmatrix} x \\ 0 \end{bmatrix} \in Q(S)$ and, hence, $x = \varphi(y) \in \varphi\big(Q(S)\big)$. Obviously, f is surjective. Furthermore, if $A'x \in \operatorname{Ker} f$ then $x \in \varphi\big(Q(S)\big)$ and $A'x + A''y = 0$ for some $y \in \mathbb{Z}^{n-e}$. This shows $\operatorname{Ker} f \subseteq \operatorname{im} A' \cap \operatorname{im} A''$. Conversely, if $A'x \in \operatorname{im} A''$, then $A'x + A''y = 0$ for some $y \in \mathbb{Z}^{n-e}$ and $x = \varphi\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) \in \varphi\big(Q(S)\big)$. This shows $\operatorname{im} A' \cap \operatorname{im} A'' \subseteq \operatorname{Ker} f$. Thus, $\operatorname{Ker} f = \operatorname{im} A' \cap \operatorname{im} A''$ and we have the short exact sequence

$$0 \longrightarrow \operatorname{im} A' \cap \operatorname{im} A'' \xrightarrow{i} \operatorname{im} A' \xrightarrow{f} \operatorname{Cl}(S) \longrightarrow 0,$$

where i denotes the embedding. Therefore, $\mathrm{Cl}\,(S) \simeq \mathrm{im}\,A'/(\mathrm{im}\,A' \cap \mathrm{im}\,A'')$.

ii) Obviously, $n = \mathrm{rank\,im}\,A + \mathrm{rank\,Ker}A$. Since $\mathrm{Ker}A = Q(S)$ it follows that $n = \mathrm{rank}\,A + \mathrm{rank}\,Q(S)$. Also, $n - e = \mathrm{rank\,im}\,A'' + \mathrm{rank\,Ker}A''$. We show that $\mathrm{Ker}A'' = 0$ which proves ii). If $z \in \mathrm{Ker}A''$, then $y, -y \in \mathrm{Ker}A$ for $y = \begin{bmatrix} 0 \\ z \end{bmatrix}$. It follows that $y, -y \in Q(M_A)$ and $\pi_i(-y) = \pi_i(y) \in \mathbb{N}$ for every $i \in I = \{1, 2, \ldots, e\}$. Since $\pi_i,\ i \in I$ are the essential projections of M_A, we obtain that $y, -y \in M_A$. Since $M_A \subseteq \mathbb{N}^n$ we must have that $y = 0$ and, hence, $z = 0$.

iii) Follows directly from i).

iv) From iii) we have that

$$\mathrm{rank}\,\mathrm{Cl}\,(S) \leq \mathrm{rank}\,A' \leq \min\{m,\ \mathrm{rank}\,A\}$$

and using ii) we obtain

$$\mathrm{rank}\,\mathrm{Cl}\,(S) + \mathrm{rank}\,Q(S) \leq \mathrm{rank}\,A + \mathrm{rank}\,Q(S) = n.$$

The result for $A' = A$ follows immediately since in this case the proof for i) shows that $\mathrm{Ker}f = \{0\}$. □

Concerning the representation of a monoid by a matrix, it is a natural question to ask for a matrix with a minimal number of rows and columns, respectively.

Definition 3.6. For a monoid S the *row degree of* S is defined by

$$d_r(S) = \min\{m \in \mathbb{N} \mid S \simeq M_A \text{ for } A \in \mathbb{Z}^{m \times n}\}$$

and the *column degree of* S is defined by

$$d_c(S) = \min\{n \in \mathbb{N}\backslash\{0\} \mid S \simeq M_A \text{ for } A \in \mathbb{Z}^{m \times n}\}.$$

Remark 3.7. Since we defined for $A \in \mathbb{Z}^{m \times n}$ that $M_A = \mathbb{N}^n$ if $m = 0$, it follows that $d_r(S) = 0$ if and only if $S \simeq \mathbb{N}^n$ for some n. Also, for $S \simeq \mathbb{N}^n$ it follows from Lemma 3.5 ii) that $d_c(S) = n$.

From Theorem 3.1 together with Lemma 3.5, we obtain the theorem announced in the Introduction.

Theorem 3.8. *For a reduced monoid S which is root-closed and finitely generated the following holds:*

i) *Row degree and column degree of S are finite and*

$$d_r(S) = \mathrm{rank}\,\mathrm{Cl}\,(S),\ d_c(S) = \mathrm{rank}\,\mathrm{Cl}\,(S) + \mathrm{rank}\,Q(S).$$

ii) *There exists a matrix $A \in \mathbb{Z}^{m \times n}$ with $m = d_r(S)$ and $n = d_c(S)$ such that S is isomorphic to the Diophantine monoid M_A.*

Proof. By Corollary 3.3, S is a Krull monoid with finitely many essential states.

i) By Theorem 3.1, $d_r(S) \leq \operatorname{rank} \mathrm{Cl}\,(S) < \infty$ and $d_c(S) \leq \operatorname{rank} \mathrm{Cl}\,(S) + \operatorname{rank} Q(S) < \infty$. Suppose $S \simeq M_A$ for $A \in \mathbb{Z}^{m\times n}$. We may assume that $w(M_A) \neq 0$ and, by Lemma 2.6, that $S \simeq M_{AD}$ with $w(M_{AD}) = 1$. From Lemma 3.5 iv) we obtain $\operatorname{rank} \mathrm{Cl}\,(S) \leq m$ and $\operatorname{rank} \mathrm{Cl}\,(S) + \operatorname{rank} Q(S) \leq n$. This proves i).
ii) Follows immediately from i) and Theorem 3.1.

□

4. Some consequences and examples.

The results of the previous section can be used to check if a Diophantine monoid is factorial or half-factorial.

Proposition 4.1. *Let $S \simeq M_A$ and $A = [A'A'']$ be given as in Lemma* 3.5.

i) *S is factorial if and only if each column of A' is in the column space of A''.*
ii) *If any two columns of A' not in the column space of A'' have their difference in the column space of A'', then S is half-factorial.*

Proof. It is well-known that any Krull monoid S is factorial if and only if $\mathrm{Cl}\,(S) = \{0\}$ and that S is half-factorial if $\mathrm{Cl}\,(S) \simeq \mathbb{Z}_2$ (cf. [**12**, Proposition 2]).

i) By Lemma 3.5, $\mathrm{Cl}\,(S) = \{0\}$ if and only if $\operatorname{im} A' \subseteq \operatorname{im} A''$. Therefore, S is factorial if and only if each column of A' is in the $\mathbb{Z}$-span of the columns of A''.
ii) If all columns of A' are in $\operatorname{im} A''$ then by i) S is factorial and, a fortiori, half-factorial. Suppose there is a column A'_{i_0} of A' which is not in $\operatorname{im} A''$. By assumption, for any column $A'_i \notin \operatorname{im} A''$ it holds that $A'_i - A'_{i_0} \in \operatorname{im} A''$. Therefore, for each column A'_i of A' either $A'_i \in \operatorname{im} A''$ or $A'_i \in A'_{i_0} + \operatorname{im} A''$. Lemma 3.5 implies that $\mathrm{Cl}\,(S) \simeq \mathbb{Z}_2$ and, hence, S is half-factorial.

□

Remark 4.2. Neither the condition given in ii) nor the condition $\mathrm{Cl}\,(S) \simeq \mathbb{Z}_2$ are necessary for half-factoriality. This is so even for $m = 1$; see [**2**] for various sufficient or necessary conditions of half-factoriality in this particular case.

In [**2**, Theorem 1.3], the current authors found a formula for computing the class group of a Diophantine monoid given by just one equation. The results of Section 3 yield a simpler proof of this formula, as well as an additional characterization of such monoids.

Proposition 4.3.

i) *A monoid S is isomorphic to a nonfactorial Diophantine monoid given by just one equation if and only if S is reduced, root-closed, and finitely generated with* $\operatorname{rank} \mathrm{Cl}(S) = 1$.

ii) *Let $S = M_A$ with $A = [a_1 a_2 \dots a_n] \in \mathbb{Z}^{1\times n}$ and, without restriction, $a_i \neq 0$ for all i, not all a_i of equal sign and* $\gcd(a_1, \dots, a_n) = 1$. *There are exactly two possible cases:*

   a) $\mathrm{Cl}(S) \simeq \mathbb{Z}_\alpha$ *with* $\alpha \in \mathbb{N}$. *This case occurs if and only if all a_i except one, say a_n, are of equal sign. Thus we have $\alpha = \frac{|a_n|}{c}$, where $c = \prod_{i=1}^{n-1} c_i$ and $0 < c_i = \gcd(|a_j| \mid j \neq i)$ for $1 \le i \le n$.*

   b) $\mathrm{Cl}(S) \simeq \mathbb{Z}$. *This case occurs if and only if there are at least two a_i with positive sign and at least two a_i with negative sign.*

Proof. The proof of i) follows directly from Theorem 3.8. For ii), let $\widetilde{a_j} = \frac{a_j}{d_j}$ with $d_j = \prod_{i\neq j} c_i$. For $\widetilde{A} = [\widetilde{a_1} \dots \widetilde{a_n}]$ the mapping $\psi\colon M_A \longrightarrow M_{\widetilde{A}}$, $\psi_i(x_1, \dots, x_n) = \frac{x_i}{c_i}$ is a monoid isomorphism. Hence $\mathrm{Cl}(M_A) \simeq \mathrm{Cl}(M_{\widetilde{A}})$. Furthermore, $w(M_{\widetilde{A}}) = 1$. Thus, we can assume that $c_i = 1$ for all i, $c = 1$ and $w(M_A) = 1$.

a) Let $a_i > 0$ for $1 \le i \le n-1$ and $a_n < 0$. Then $A = [A'A'']$ with $A' = [a_1 \dots a_{n-1}]$ and $A'' = a_n = -\alpha$. Since $c_n = 1$, we have that $1 \in \operatorname{im} A'$ and, hence, $\operatorname{im} A' = \mathbb{Z}$. Obviously, $\operatorname{im} A'' = \alpha\mathbb{Z}$ and from Lemma 3.5 i) we obtain $\mathrm{Cl}(M_A) \simeq \mathbb{Z}_\alpha$.

b) From the assumption in b), all projections must be essential and hence, $A = A'$. From $\gcd(a_1, \dots, a_n) = 1$ it follows that $\operatorname{im} A' = \mathbb{Z}$ and Lemma 3.5 yields $\mathrm{Cl}(M_A) \simeq \mathbb{Z}$.

□

The following example illustrates the concept of row degree and column degree, respectively and the statements made in Theorem 3.8.

Example 4.4. Consider the Diophantine monoid

$$S = \{x \in \mathbb{N}^5 \mid x_1 + x_2 = x_4 + x_5,\ x_2 + x_5 = x_3 + x_4\}.$$

Obviously, $S = M_A$ for $A = \begin{bmatrix} 1 & 1 & 0 & -1 & -1 \\ 0 & 1 & -1 & -1 & 1 \end{bmatrix} \in \mathbb{Z}^{2\times 5}$. All canonical projections are normal and by Lemma 2.3 the projections π_1 to π_4 are essential while π_5 is not. We have $w(M_A) = 1$ and $A = [A'A'']$ with $A' = \begin{bmatrix} 1 & 1 & 0 & -1 \\ 0 & 1 & -1 & -1 \end{bmatrix}$ and $A'' = \begin{bmatrix} -1 \\ 1 \end{bmatrix}$. It follows that $\operatorname{im} A' = \mathbb{Z} \oplus \mathbb{Z}$, $\operatorname{im} A'' = \mathbb{Z} \begin{bmatrix} -1 \\ +1 \end{bmatrix}$, and, by Lemma 3.5 i), $\operatorname{Cl}(M_A) \simeq \mathbb{Z}$. Since $\operatorname{rank} Q(M_A) = 3$, it follows from Theorem 3.8 i) that $d_r(S) = 1$ and $d_c(S) = 1 + 3 = 4$. By Theorem 3.8 ii) there exists a matrix $B \in \mathbb{Z}^{1\times 4}$ such that M_A is isomorphic to the Diophantine monoid M_B given by the smaller matrix B. Indeed, one can reduce the given system of two equations to just one equation as follows. Eliminating $x_5 = x_1 + x_2 - x_4$ yields $x_2 + (x_1 + x_2 - x_4) = x_3 + x_4$. That is $x_1 + 2x_2 - x_3 - 2x_4 = 0$. One has to make sure, however, that for any solution in $\mathbb{N}$ of the latter equation, it automatically holds that $x_5 = x_1 + x_2 - x_4 \geq 0$. This is obvious in case of $x_2 \geq x_4$. If $x_2 \leq x_4$, then one obtains $x_1 + x_2 - x_4 \geq x_1 + 2(x_2 - x_4) = x_3 \geq 0$.

By Theorem 3.8, one can easily check if a given Diophantine monoid can be described by a smaller matrix without actually carrying out the elimination procedure as in the above example. This latter process might be quite difficult in general.

The following example also illustrates Theorem 3.8, and essentially covers all class group possibilities of rank 2. In contrast to Example 4.4, here there is no possible smaller description of the given monoids.

Example 4.5. Let G be a finitely generated abelian group of rank 2. We show how to construct a Diophantine monoid S defined by 2 equations such that $\operatorname{Cl}(S) \simeq G$. There are three cases to consider.

(a) Suppose $G \simeq \mathbb{Z}_n \oplus \mathbb{Z}_{kn}$ for positive integers $n > 1$ and $k \geq 1$. Let

$$S = \{x \in \mathbb{N}^5 \mid x_1 + x_3 = nx_4,\ x_2 + x_3 = knx_5\}.$$

Obviously, $S = M_A$ for $A = \begin{bmatrix} 1 & 0 & 1 & -n & 0 \\ 0 & 1 & 1 & 0 & -kn \end{bmatrix} \in \mathbb{Z}^{2\times 5}$. It is easy to check that all canonical projections are normal and, using Lemma 2.3, that the projections π_1, π_2, π_3 are essential while π_4, π_5 are not. Thus, $w(M_A) = 1$ and $A = [A'\, A'']$ with $A' = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ and $A'' = \begin{bmatrix} -n & 0 \\ 0 & -kn \end{bmatrix}$. It follows

that $\operatorname{im} A' = \mathbb{Z} \oplus \mathbb{Z}$ and $\operatorname{im} A'' = n\mathbb{Z} \oplus kn\mathbb{Z}$. Therefore, by Lemma 3.5 i), $\operatorname{Cl}(S) \simeq (\mathbb{Z} \oplus \mathbb{Z})/(n\mathbb{Z} \oplus kn\mathbb{Z}) \simeq \mathbb{Z}_n \oplus \mathbb{Z}_{kn}$. Since $\operatorname{rank} Q(S) = 3$, by Theorem 3.8 we have that $d_r(S) = 2$ and $d_c(M) = 2+3 = 5$. Therefore, the Diophantine monoid S can neither be described by one equation alone, nor by less than five variables.

(b) Suppose $G \simeq \mathbb{Z} \oplus \mathbb{Z}_n$ for some positive integer $n > 1$. Let

$$S = \{x \in \mathbb{N}^6 \mid x_1 + x_2 - x_3 - x_4 = 0,\ x_1 + x_3 + x_5 = nx_6\}.$$

Clearly, $S = M_A$ for $A = \begin{bmatrix} 1 & 1 & -1 & -1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & -n \end{bmatrix} \in \mathbb{Z}^{2\times 6}$. As in (a), $w(M_A) = 1$, the projections $\pi_1, \pi_2, \pi_3, \pi_4$ and π_5 are essential and π_6 is not essential. Hence, if $A' = \begin{bmatrix} 1 & 1 & -1 & -1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$ and $A'' = \begin{bmatrix} 0 \\ -n \end{bmatrix}$, then $\operatorname{im} A' = \mathbb{Z} \oplus \mathbb{Z}$ and $\operatorname{im} A'' = n\mathbb{Z}$. Thus, $\operatorname{Cl}(S) \simeq (\mathbb{Z} \oplus \mathbb{Z})/n\mathbb{Z} \simeq \mathbb{Z} \oplus \mathbb{Z}_n$. Since $\operatorname{rank} Q(S) = 4$, we have that $d_r(S) = 2$ and $d_c(M) = 2 + 4 = 6$.

(c) Suppose that $G \simeq \mathbb{Z} \oplus \mathbb{Z}$. Let

$$S = \{x \in \mathbb{N}^6 \mid x_1 + x_3 - x_4 - x_6 = 0,\ x_2 + x_3 - x_5 - x_6 = 0\}.$$

Clearly, $S = M_A$ for $A = \begin{bmatrix} 1 & 0 & 1 & -1 & 0 & -1 \\ 0 & 1 & 1 & 0 & -1 & -1 \end{bmatrix} \in \mathbb{Z}^{2\times 6}$. As above, $w(M_A) = 1$, but here all projections are essential. Thus, $A' = A$ and Lemma 3.5 yields $\operatorname{Cl}(S) \simeq \mathbb{Z}^2$. Since $\operatorname{rank} Q(S) = 4$, we have that $d_r(S) = 2$ and $d_c(M) = 2 + 4 = 6$.

To close Section 4, we present an algorithm which reflects the techniques developed in Sections 2 and 3. The method is based on having the complete set of minimal solutions over the nonnegative integers of the system $Ax = 0$. An algorithm for that computation, by García-Sánchez and Rosales, can be found in [**14**, Section 3, p. 80]. Before proceeding, we will require one additional result. Let M be a finitely generated submonoid of $(\mathbb{N}^n, +)$ and $u_1, \ldots, u_t$ the irreducible elements of M. Let V and W be the $\mathbb{Q}$-vector spaces generated by $u_1, \ldots, u_t$ and $u_2 - u_1, \ldots, u_t - u_1$ respectively. Then $\dim V - \dim W \leq 1$ and $V = W$ if and only if $u_1 \in W$.

Lemma 4.6. *Let M, V and W be as above. The following statements are equivalent:*

i) *M is half factorial*
ii) $\dim V = 1 + \dim W$.

Proof. For i) $\Rightarrow$ ii), assume that $u_1 = \sum_{j=2}^{t} \alpha_j(u_j - u_1) \in W$ with each $\alpha_j \in \mathbb{Q}$. Then $k_1 u_1 = \sum_{j=2}^{t} k_j(u_j - u_1)$ for suitable $k_1, \ldots, k_t \in \mathbb{Z}$, $k_1 \neq 0$. Since $(k_1 + \sum_{j=2}^{t} k_j)u_1 - \sum_{j=2}^{t} k_j u_j = 0$, the monoid M is not half factorial.

For ii) $\Rightarrow$ i), let $r_1, \ldots, r_t \in \mathbb{Z}$ with

$$\sum_{j=1}^{t} r_j u_j = 0 = \sum_{j=2}^{t} r_j (u_j - u_1) + \left(\sum_{j=1}^{t} r_j \right) u_1.$$

Since $u_1 \notin W$ it follows that $\sum_{j=1}^{t} r_j = 0$. □

Algorithm 4.7. Assume that $A \in \mathbb{Z}^{m \times n}$. The following algorithm calculates the class group of M_A and determines whether or not M_A is half-factorial. Suppose that $(u_\tau | 1 \le \tau \le t) \neq \emptyset$ is the family of all irreducible elements of the monoid M_A. Let $C := (u_{i\tau}) \in \mathbb{N}^{n \times t}$ be the matrix with column vectors u_τ and row vectors $v_i := (u_{i\tau}) \in \mathbb{N}^{1 \times t}, 1 \le i \le n$. Let $C_1 := (u_{i\tau} - u_{i1}) \in \mathbb{Z}^{n \times t}$. By Lemma 4.6, M_A is not half factorial if and only if $\operatorname{im}_{\mathbb{Z}} C = \operatorname{im}_{\mathbb{Z}} C_1$. The calculation of the class group proceeds as follows.

I) Reduction of the system. Let $v_i := (u_{i\tau}) \in \mathbb{N}^{1 \times t}, 1 \le i \le n$, be the i-th row vector of the matrix C.

Step 1): For all $i \in \{1, \ldots, n\}$, if $v_i = 0$, then cancel the i-th row of C.

Step 2): For all $i, j \in \{1, \ldots, n\}$ with $i < j$, if $\lambda v_i = v_j$ for some $\lambda \in \mathbb{Q}$, then cancel the j-th row of C.

After these canceling steps, we denote the new matrix again with C. Then $C \in \mathbb{Z}^{\widetilde{n} \times t}$ for some $\widetilde{n} \le n$.

Step 3): For all $j \in \{1, \ldots, \widetilde{n}\}$, calculate $c_j := \gcd(u_{j\tau} | 1 \le \tau \le t) \in \mathbb{N}$ and replace the row vector v_j of C by $\frac{1}{c_j} v_j$.

II) Determining the essential states.

Step 4): For every $i \in \{1, \ldots, \widetilde{n}\}$, define $J_i := \{\tau \in \{1, \ldots, t\} | u_{i\tau} = 0\}$. If $J_i \neq \emptyset$, calculate the sums

$$v_j^{(i)} := \sum_{\tau \in J_i} u_{j\tau}$$

for all $j \in \{1, \ldots, \widetilde{n}\}, j \neq i$. Define

$$I := \{i \in \{1, \ldots, \widetilde{n}\} | \, J_i \neq \emptyset, \, v_j^{(i)} \neq 0 \text{ for all } j \in \{1, \ldots, \widetilde{n}\}, j \neq i\}$$

and $e := |I|$. The projections π_i, $i \in I$, are exactly the essential states of M.

III) The final calculation.

Step 5): Let $\widetilde{C} \in \mathbb{N}^{e \times t}$ be the matrix with the row vectors $v_i, i \in I$. Transform $\widetilde{C}$ into its Smith normal form, using e.g., the algorithm given in [**14**].

From the Smith normal form one gets $k := \operatorname{rank} \widetilde{C}$ and $r \geq 0$ elementary divisors $\alpha_i \geq 2$ of $\widetilde{C}$ with $\alpha_{i+1} | \alpha_i$ for $1 \leq i \leq r-1$ if $r \geq 2$. Then

$$\operatorname{Cl}(M) = \mathbb{Z}^{e-k} \oplus \mathbb{Z}/\alpha_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/\alpha_r\mathbb{Z}.$$

Acknowledgment. The authors would like to acknowledge many useful suggestions made by an anonymous referee on an earlier draft of the paper.

References

[1] S. Chapman and A. Geroldinger, *Krull domains and monoids, their sets of lengths, and associated combinatorial problems*, Lecture Notes in Pure and Applied Mathematics, Marcel Dekker, **189** (1997), 73-112, MR 98g:13017, Zbl 0897.13001.

[2] S. Chapman, U. Krause and E. Oeljeklaus, *Monoids determined by a homogeneous linear Diophantine equation and the half-factorial property*, J. Pure Appl. Algebra, **151** (2000), 107-133, MR 2001g:11034.

[3] E. Contejean and H. Devie, *An efficient incremental algorithm for solving systems of linear Diophantine equations*, Inform. and Comput., **113** (1994), 143-172, MR 96a:11151, Zbl 0809.11015.

[4] E.B. Elliott, *On linear homogenous Diophantine equations*, Quart. J. Pure Appl. Math., **34** (1903), 348-377.

[5] J.H. Grace and A. Young, *The Algebra of Invariants*, Cambridge University Press, Cambridge, 1903.

[6] F. Halter-Koch, *Halbgruppen mit divisorentheorie*, Exposition Math., **8** (1990), 27-66, MR 91c:20091, Zbl 0698.20054.

[7] ———, *The integral closure of a finitely generated monoid and the Frobenius problem in higher dimensions*, in 'Semigroups: Algebraic Theory and Applications to Formal Languages and Codes' (eds. C. Bonzini et al.), World Scientific 1993, 86-93, CMP 1 647 172, Zbl 0818.20079.

[8] M. Hochster, *Ring of invariants of tori, Cohen-Macauley rings generated by monomials, and polytopes*, Ann. of Math., II Ser., **96** (1972), 318-337, MR 46 #3511, Zbl 0237.14019.

[9] N. Jacobson, *The Theory of Rings*, Mathematical Surveys II, AMS, Providence, 1943, MR 5,31f, Zbl 0060.07302.

[10] F. Kainrath and G. Lettl, *Geometric notes on monoids*, Semigroup Forum, **61** (2000), 298-302, CMP 1 832 189, Zbl 0964.20037.

[11] U. Krause, *On monoids of finite real character*, Proc. Amer. Math. Soc., **105** (1989), 546-554, MR 89i:20102, Zbl 0692.20058.

[12] U. Krause and C. Zahlten, *Arithmetic in Krull monoids and the cross number of divisor class groups*, Mitt. Math. Ges. Hamburg, **12** (1991), 681-696, MR 93b:11142, Zbl 0756.20010.

[13] G. Lettl, *Subsemigroups of finitely generated groups with divisor-theory*, Monatsh. Math., **106** (1988), 205-210, MR 89m:20078, Zbl 0671.20059.

[14] J.C. Rosales and P.A. García-Sánchez, *Finitely Generated Commutative Monoids*, Nova Scientific Publishers, 1999, MR 2000d:20074, Zbl 0966.20028.

[15] R. Stanley, *Linear Diophantine equations and local cohomology*, Inv. Math., **68** (1982), 175-193, MR 83m:10017, Zbl 0516.10009.

[16] ———, *Combinatorics and Commutative Algebra*, Birkhäuser, Boston, 1983, MR 85b:05002, Zbl 0537.13009.

Received September 25, 2000 and revised November 9, 2001. Part of this work was completed while the first author was on an Academic Leave granted by the Trinity University Faculty Development Committee. Part of this work was completed while the second author was visiting Trinity University during the fall of 1999 as the Eva and O.R. Mitchell Visiting Distinguished Professor of Mathematics.

Trinity University
Department of Mathematics
715 Stadium Drive
San Antonio, Texas 78212-7200
E-mail address: schapman@trinity.edu

Universität Bremen
Fachberich Mathematik/Informatik
DW-2800 Bremen, Germany
E-mail address: krause@math.uni-bremen.de

Universität Bremen
Fachberich Mathematik/Informatik
DW-2800 Bremen, Germany
E-mail address: oel@math.uni-bremen.de