ELSEVIER

Journal of Pure and Applied Algebra 151 (2000) 107–133

JOURNAL OF PURE AND APPLIED ALGEBRA

Monoids determined by a homogenous linear diophantine equation and the half-factorial property

Scott T. Chapman[a,*,1], Ulrich Krause[b], Eberhard Oeljeklaus[b]

[a] *Department of Mathematics, Trinity University, 715 Stadium Drive, San Antonio, TX 78212-7200, USA*

[b] *Universität Bremen, Fachbereich Mathematik/Informatik, D-28334 Bremen, Germany*

Received 5 May 1998; received in revised form 11 February 1999
Communicated by A.V. Geramita

Abstract

We study additive submonoids $\boldsymbol{M}$ of $\mathbb{N}^n$ consisting of the solutions of a homogeneous linear diophantine equation with integer coefficients. Surprisingly, not very much is known about the structure of $\boldsymbol{M}$. $\boldsymbol{M}$ is a Krull monoid which, however, cannot be realized as a multiplicative monoid of a Krull domain. The concepts of divisor theory and divisor class group, nevertheless, do apply and we use them to characterize the factoriality of $\boldsymbol{M}$ in terms of the coefficients of the diophantine equation. In this paper, we concentrate on the more difficult question of finding conditions under which $\boldsymbol{M}$ is half-factorial. Since the famous Carlitz criterion of class number at most two breaks down for the Krull monoid $\boldsymbol{M}$, we develop some new sufficient and/or necessary conditions for the half-factoriality of $\boldsymbol{M}$. Among others, we present a geometric criterion for $\boldsymbol{M}$ to be half-factorial and an inequality condition on the coefficients of the diophantine equation assuring the half-factoriality of $\boldsymbol{M}$.

MSC: Primary 11D04; 11A51; secondary 13A05; 20M14

Consider an integral domain D which is *atomic* in the sense that each nonzero nonunit of D can be factored into a finite product of irreducible elements. A principle question in number theory, as well as in commutative algebra, is the question of when D

* Corresponding author. Tel.: +1-210-999-8245; fax: +1-210-999-8264.
E-mail address: schapman@trinity.edu (S.T. Chapman).

[1] The first author gratefully acknowledges support under grants from the Deutscher Akademischer Austausch Dienst and the Trinity University Faculty Development Committee.

0022-4049/00/$ - see front matter
PII: S0022-4049(99)00062-6

is a *unique factorization domain* (UFD), or a *factorial domain* (i.e., an integral domain in which the factorization of a given element into irreducible elements is unique up to units and the ordering of factors). In the case where D is the ring of all integers in a finite algebraic extension of the rationals, D is factorial if and only if the class group has order one. Moreover, if D is not factorial, then the class group in some way is thought to measure the deviation from unique factorization. This idea can be traced back to Kummer and Dedekind and was substantiated by Carlitz who proved in 1960 (see [4]) for the case of algebraic integers that the class group has order less or equal to two if and only if all factorizations of a given element into irreducible elements have equal length.

Today such domains are called half-factorial. More precisely, an atomic integral domain D is called a *half-factorial domain* (HFD) if whenever $x_1,\dots,x_n$ and $y_1,\dots,y_m$ are irreducible elements of D with $x_1\dots x_n = y_1\dots y_m$ then $n = m$. For investigating divisibility, factoriality, and half-factoriality, Krull domains are of particular interest within the realm of atomic integral domains (See [2,5,6,9,10]). Moreover, it has been recognized over the years that many results for domains concerning divisibility properties depend only on the multiplicative structure of the domain. Actually, being a Krull domain is a property depending only on the multiplicative monoid of the domain [14]. Thus, it is reasonable to investigate divisibility and factorization properties for atomic monoids and especially for *Krull monoids* as defined in Section 1 (this point of view is put forward forcefully in the recent monograph [13]). To give an example, the above-mentioned result by Carlitz on rings of algebraic integers carries over to Krull monoids for which the class group is finite and each nontrivial class contains at least one prime divisor (see Section 1 for definitions). That is, for such a Krull monoid the class group has order less than or equal to two if and only if the monoid is half-factorial [15].

Whereas the multiplicative monoid of a Krull domain is a Krull monoid, the latter category is much richer and shows new phenomena. There are many Krull monoids which cannot be realized as the multiplicative monoid of a domain (see Proposition 1.2). Among those are the Krull monoids we are concentrating on in the present paper, namely *monoids determined by a homogeneous linear Diophantine equation*. To denote such monoids, we use the notation

$$\boldsymbol{M}(a_1,\dots,a_n) = \left\{ (r_1,\dots,r_n) \in \mathbb{N}^n \;\middle|\; \sum_{j=1}^{n} r_j a_j = 0 \right\},$$

where $a_1,\dots,a_n \in \mathbb{Z}$ and the semigroup operation is given by (componentwise) addition (here $\mathbb{Z}$ is the set of (rational) integers and $\mathbb{N}$ the set of nonnegative integers). These monoids are not only interesting as a class of Krull monoids not captured by multiplicative monoids of Krull domains, but they are themselves fascinating objects with several interesting applications. Whereas it is simple to determine the solution set of a linear Diophantine equation in integers, it is surprisingly difficult to determine the solution set of such an equation in *nonnegative* integers. Remarkably, not very much is

known about the solution monoids $\boldsymbol{M}(a_1,\ldots,a_n)$. Stanley [17] contains an elaborated theory on nonnegative integral solutions of linear Diophantine equations dealing with combinatorial questions (e.g., the number of magic squares). An early example of a monoid $\boldsymbol{M}(a_1,\ldots,a_n)$ in connection with commutative algebra can be found in [11]. A fundamental fact about the (additive) monoid $\boldsymbol{M}(a_1,\ldots,a_n)$ is that by a theorem of Dickson [8] (sometimes also called Gordan's Lemma, see [17]) it is generated by its finitely many irreducible elements. This fact, however, does not help very much to compute all solutions or to determine the structure of the solution set.

In general, the monoid $\boldsymbol{M}(a_1,\ldots,a_n)$ may be factorial, half-factorial, or neither. Concentrating on the structure of the solution monoid in the present paper, we provide necessary and sufficient conditions on the coefficients $a_1,\ldots,a_n$ for the monoid to be factorial by computing the class group (Theorem 1.3 and Corollary 1.4). With regard to half-factoriality, the traditional link between class group and half-factoriality as in the above mentioned extension of Carlitz' result to Krull monoids breaks down for the Krull monoids $\boldsymbol{M}(a_1,\ldots,a_n)$ since there are not enough prime divisors. Though a monoid $\boldsymbol{M}(a_1,\ldots,a_n)$ with a class group of order less than or equal to two is always half-factorial, the reverse implication is not true. Indeed, half-factoriality can be obtained for every class number (see the remark following Corollary 2.5). Therefore, in the present paper we develop other criteria for half-factoriality and concentrate on solution monoids with finite class groups. As a general result, we obtain that such a monoid is half-factorial if and only if each irreducible element is in a unique manner given as a *convex combination* over the rational number of primary elements (Proposition 2.1). Factoriality corresponds to the particular case where the convex combination is taken of one element only. Again, half-factoriality appears as an appealing extension of the concept of factoriality. Since primary elements are easy to compute (Proposition 1.2) the knowledge of factoriality or half-factoriality for a solution monoid opens the way to compute irreducible solutions and, hence, arbitrary solutions. To check half-factoriality directly from the coefficients $a_1,\ldots,a_n$ of the monoid seems, in contrast to the case of factoriality, to be a hard task. Beside settling some particular cases, we derive a general inequality involving the coefficients which assures half-factoriality (Theorem 4.1). The proof for this result, though elementary in nature, is quite lengthy and proceeds by reducing the problem to certain special monoids.

The authors acknowledge the useful suggestions made by an anonymous referee on an earlier draft of the paper.

1. Definitions and basic results

Let $\boldsymbol{S}$ be a commutative and cancellative multiplicative monoid. For simplicity we assume the group of units to consist of 1 only. We denote the quotient group of $\boldsymbol{S}$ by $\boldsymbol{Q}(\boldsymbol{S})$ and the set of irreducible elements of $\boldsymbol{S}$ by $\mathscr{I}(\boldsymbol{S})$. Let $\leq$ be the divisibility relation (or quasi-ordering) on $\boldsymbol{S}$ induced by the following: $x \leq y$ in $\boldsymbol{Q}(\boldsymbol{S})$ if and only if $xz = y$ for some $z \in \boldsymbol{S}$. An irreducible $x \in \boldsymbol{S}$ is *prime* whenever $x \leq yz$ implies

$x \le y$ or $x \le z$ and it is *primary* whenever $x \le yz$ implies $x \le y$ or $x \le z^k$ for some k. Next we sketch the construction of a divisor theory for $\boldsymbol{S}$ (cf. [12,14,15]). Let $\mathscr{F}$ be a nonempty family of homomorphisms $f \not\equiv 0$ of $\boldsymbol{Q}(\boldsymbol{S})$ into $\mathbb{Z}$ such that for each $x \in \boldsymbol{Q}(\boldsymbol{S})$ the set

$$\mathscr{F}(x) = \{f \in \mathscr{F} \mid f(x) \neq 0\}$$

is finite. An element of $\mathscr{F}$ is called a *state* on $\boldsymbol{S}$. If the monoid $\boldsymbol{S}$ is *defined by* $\mathscr{F}$ (i.e., $\boldsymbol{S} = \{x \in \boldsymbol{Q}(\boldsymbol{S}) | f(x) \ge 0 \ \forall f \in \mathscr{F}\}$), then $\boldsymbol{S}$ is a *Krull monoid*. A state f on $\boldsymbol{S}$ is *essential* if for any $x,\ y \in \boldsymbol{Q}(\boldsymbol{S})$ there exists $z \in \boldsymbol{Q}(\boldsymbol{S})$ such that $x \leqq z,\ y \leqq z$ and $f(z) = \max\{f(x), f(y)\}$. Let $\boldsymbol{I}$ denote the set of essential states f which are *normalized* (i.e., $f(\boldsymbol{Q}(\boldsymbol{S})) = \mathbb{Z}$). Consider the map

$$\varphi : \boldsymbol{S} \to \mathbb{N}^{(\boldsymbol{I})},$$

defined by

$$\varphi(x)(f) = f(x),$$

where $\mathbb{N} = \{0, 1, 2, \ldots,\}$ and $\mathbb{N}^{(\boldsymbol{I})}$ is the direct sum of $|\boldsymbol{I}|$ copies of $\mathbb{N}$. For a Krull monoid $\boldsymbol{S}$ this map satisfies the following two properties:

1. for all $x,\ y \in \boldsymbol{S},\ x \leqq y$ if and only if $\varphi(x) \le \varphi(y)$ (here $\le$ denotes the pointwise ordering),

2. each element of $\mathbb{N}^{(\boldsymbol{I})}$ is the minimum of finitely many elements for the set $\varphi(\boldsymbol{S})$.

As described above, the essential states of a Krull monoid yield a *divisor theory* for $\boldsymbol{S}$ (see [12,14]). The factor monoid

$$\mathbb{N}^{(\boldsymbol{I})}/\varphi(\boldsymbol{S}) \cong \mathbb{Z}^{(\boldsymbol{I})}/\varphi(\boldsymbol{Q}(\boldsymbol{S})),$$

where φ is extended in the obvious way to $\boldsymbol{Q}(\boldsymbol{S})$, is a group known as the *divisor class group of* $\boldsymbol{S}$ and denoted $\mathrm{Cl}(\boldsymbol{S})$. The unit vectors e_i in $\mathbb{N}^{(\boldsymbol{I})}$ (i.e., $e_i(j) = \delta_{ij}$) are the *prime divisors*. Let $[x]$ denote the class in $\mathrm{Cl}(\boldsymbol{S})$ generated by $x \in \mathbb{Z}^{(\boldsymbol{I})}$. In this respect, some well-known *facts* are (cf. [14]):

1. An integral domain D is a Krull domain if and only if $D^* = D \setminus \{0\}$ is a Krull monoid.

2. If D is a Krull domain then the divisor class group of the Krull monoid D^* is merely the divisor class group of D.

3. A monoid $\boldsymbol{S}$ is a *factorial monoid* (i.e., each element of $\boldsymbol{S}$ is a unique product of irreducible elements) if and only if it is a Krull monoid with trivial divisor class group.

A monoid $\boldsymbol{S}$ is *half-factorial* if whenever $x_1, \ldots, x_n,\ y_1, \ldots, y_m$ are irreducible elements of $\boldsymbol{S}$ with $x_1, \ldots, x_n = y_1 \ldots y_m$ then $n = m$.

In the following, we will be concerned with additive submonoids $\boldsymbol{M}$ of $\mathbb{N}^n$. The two factoriality properties then may be rephrased as follows. $\boldsymbol{M}$ is half-factorial (resp. factorial) if whenever $x_1, \ldots, x_k$ are pairwise different irreducible elements of $\boldsymbol{M}$ with $\sum_{i=1}^k n_i x_i = 0,\ n_i \in \mathbb{Z}$, then $\sum_{i=1}^k n_i = 0$ (resp. $n_i = 0$ for all i). With respect

to the additive monoids

$$\boldsymbol{M} = \boldsymbol{M}(a_1,\ldots,a_n) = \left\{ (r_1,\ldots,r_n) \in \mathbb{N}^n \,\middle|\, \sum_{j=1}^{n} r_j a_j = 0 \right\} \text{ for } n \geq 2$$

where $a_1,\ldots,a_n \in \mathbb{Z}$ and addition is componentwise, we will assume throughout without loss of generality that $a_i \neq 0$ for all i, not all a_i are of equal sign and $\gcd(a_1,\ldots,a_n)=1$. If $x=(x_1,\ldots,x_n) \in \boldsymbol{Q}(\boldsymbol{M}(a_1,\ldots,a_n))$ and $\pi_i(x)=x_i$ is the ith projection of $\boldsymbol{Q}(\boldsymbol{M})$ into $\mathbb{Z}$ then

$$\boldsymbol{M}(a_1,\ldots,a_n) = \{x \in \boldsymbol{Q}(\boldsymbol{M}) | \pi_i(x) \geq 0 \ \forall i \in \{1,\ldots,n\}\}$$

and $\boldsymbol{M}(a_1,\ldots,a_n)$ is an additive Krull monoid defined by the projections $\{\pi_i\}_{i=1}^n$. We will later find the following lemma quite useful.

Lemma 1.1. (i) *The projection π_i of $\boldsymbol{M}(a_1,\ldots,a_n)$ is not essential if and only if $n \geq 3$ and $a_i a_j < 0$ for all $j \neq i$.*

(ii) *The mapping $\alpha : \boldsymbol{M}(a_1,\ldots,a_n) \to \boldsymbol{M}(a_1',\ldots,a_n')$ defined by $(r_1,\ldots,r_n) \mapsto (\frac{r_1}{c_1},\ldots,\frac{r_n}{c_n})$ where*

$$c_i = \gcd\{a_j\}_{j\neq i} \quad \text{and} \quad a_j' = \frac{a_j}{\prod\limits_{i\neq j} c_i} \quad \text{for } 1 \leq i,j \leq n$$

is a monoid isomorphism.

(iii) *Up to the above isomorphism of the solution monoid we may assume that the equation $a_1 r_1 + \cdots + a_n r_n = 0$ is normalized (i.e., $c_i = \gcd\{a_j\}_{j\neq i} = 1$ for all $1 \leq i \leq n$). The projections π_i for a normalized equation are all normalized.*

Proof. (i) The statement follows from [15, p. 682, Example 2].

(ii) As already remarked, we may assume $\gcd\{a_1,\ldots,a_n\}=1$. This implies $\gcd\{c_i,c_k\}=1$ for $i \neq k$ and hence $\prod_{i\neq j} c_i | a_j$ for all j. For $(r_1,\ldots,r_n) \in \boldsymbol{M}(a_1,\ldots,a_n)$ we must have that $c_i | a_i r_i$ which together with $c_i | a_j$ for $i \neq j$ implies that $c_i | r_i$. Because of $a_1 r_1 + \cdots + a_n r_n = \prod_{i=1}^n c_i (a_1'(r_1/c_1) + \cdots + a_n'(r_n/c_n))$ the mapping $\alpha : \boldsymbol{M}(a_1,\ldots,a_n) \to M(a_1',\ldots,a_n')$ is well defined. Obviously, α is bijective and a monoid homomorphism.

(iii) For the coefficients a_j' defined in (ii) we have $gcd\{a_j'\}_{j\neq i} | \gcd\{a_j/c_i\}_{j\neq i}$ and $\gcd\{a_j'\}_{j\neq i} = 1$ by definition of c_i. Let $a_1 r_1 + \cdots + a_n r_n = 0$ be normalized and π_i the ith projection of $\boldsymbol{Q}(\boldsymbol{M}) = \boldsymbol{Q}(\boldsymbol{M}(a_1,\ldots,a_n))$ into $\mathbb{Z}$. Now, $c_i = \gcd\{a_j\}_{j\neq i} = 1$ implies that $\sum_{j\neq i} a_j x_j = 1$ with $x_j \in \mathbb{Z}$. Hence, for $x_i \in \mathbb{Z}$ arbitrary we have that $\sum_{j\neq i} a_j(-a_i x_j x_i) + a_i x_i = 0$. That is, $\pi_i(L) = \mathbb{Z}$ where L is the set of solutions $(y_1,\ldots,y_n)$ of $a_1 y_1 + \cdots + a_n y_n = 0$ with $y_i \in \mathbb{Z}$. We show that $L = \boldsymbol{Q}(\boldsymbol{M})$. Obviously, $\boldsymbol{Q}(\boldsymbol{M}) \subset L$. By general assumptions, the sets $I_+ = \{i \,|\, 1 \leq i \leq n, a_i > 0\}$ and $I_- = \{j \,|\, 1 \leq j \leq n, a_j < 0\}$ are non-empty and $I_+ \cup I_- = \{1,\ldots,n\}$. By $\bar{x}_i = -\sum_{j\in I_-} a_j$ for all $i \in I_+$ and $\bar{x}_j = \sum_{i\in I_+} a_i$ for all $j \in I_-$ a particular solution $\sum_{i=1}^n a_i \bar{x}_i = 0$ is defined with strictly positive integer components. For $y \in L$ there

exist some $k \in \mathbb{N}$ such that $k\bar{x} + y \in \boldsymbol{M}(a_1, \ldots, a_n)$ and hence, $y = (k\bar{x} + y) - k\bar{x} \in \boldsymbol{Q}(\boldsymbol{M})$. □

By the above lemma, for every projection π_i of the solution monoid $\boldsymbol{M}(a_1, \ldots, a_m)$ the state $(1/c_i)\pi_i$ is normalized. For $m = 2$ both projections have to be essential and the solution monoid turns out to be isomorphic to $\mathbb{N}$ for all possible choices of the coefficients. Therefore, we may assume $m \geq 3$ in what follows. Consider the case that there is exactly one positive coefficient or exactly one negative coefficient. Without loss of generality, suppose $a_i < 0$ for exactly one $i \in \{1, \ldots, m\}$. Then, by the lemma, the essential projections are the π_j for $j \neq i$. If the above case does not apply, then there must be at least two positive coefficients and at least two negative coefficients in which case all projections are essential by the lemma. Thus, for $m \geq 3$ there are just two cases possible.

Case 1: The solution is of the form

$$\boldsymbol{M}(a_1, \ldots, a_n; b) = \left\{ (r_1, \ldots, r_{n+1}) \in \mathbb{N}^{n+1} \;\middle|\; \sum_{j=1}^{n} r_j a_j = r_{n+1} b \right\},$$

where $a_1, \ldots, a_n, b \in \mathbb{N}_+ := \mathbb{N} \setminus \{0\}$ and $n \geq 2$ (for simplicity we use the same labelling for the a_i). The essential normalized states in this case are given by $(1/c_i)\pi_i$ for $1 \leq i \leq n$.

Case 2: The solution monoid is of the form

$$\boldsymbol{M}(a_1, \ldots, a_n; b_1, \ldots, b_k) = \left\{ (r_1, \ldots, r_{n+k}) \in \mathbb{N}^{n+k} \;\middle|\; \sum_{j=1}^{n} r_j a_j = \sum_{i=1}^{k} r_{n+i} b_i \right\},$$

where $a_1, \ldots, a_n, b_1, \ldots, b_k \in \mathbb{N}_+$ and $n \geq 2$, $k \geq 2$ (the labelling of the a_i not changed). The essential normalized states in this case are given by $(1/c_i)\pi_i$ for $1 \leq i \leq n + k$.

Below we will see that monoids behave quite differently in these two cases (see Theorem 1.3). The monoids $\boldsymbol{M}(a_1, \ldots, a_m)$ show distinctive features among Krull monoids as the following proposition indicates.

Proposition 1.2. 1. $\mathrm{Cl}(\boldsymbol{M}(a_1, \ldots, a_n))$ *has only finitely many divisor classes containing prime divisors. Moreover, each class containing a prime divisor contains finitely many.*

2. $\boldsymbol{M}(a_1, \ldots, a_n)$ *is not realizable as the multiplicative monoid* D^* *of a Krull domain* D.

3. $\boldsymbol{M}(a_1, \ldots, a_n)$ *contains finitely many irreducible elements.*

4. *In* $\boldsymbol{M}(a_1, \ldots, a_n)$ *the primary elements are precisely the elements* q *for which* $\varphi(q) = ke_i$, $k = \mathrm{ord}[e_i] < \infty$ *for some* i. *In the particular case of* $\boldsymbol{M}(a_1, \ldots, a_m; b)$, *the primary elements are given by*

$$q = \frac{b}{\gcd(a_i, b)} \bar{e}_i + \frac{a_i}{\gcd(a_i, b)} \bar{e}_{m+1} \quad \text{for } i = 1, 2, \ldots, m,$$

the $\bar{e}_i$ *being the unit vectors in* $\mathbb{Z}^{m+1}$.

5. *If an element of* $\boldsymbol{M}(a_1,\dots,a_n)$ *is a sum of primary elements, then these primary elements are uniquely defined.*

Proof. Statement 1 follows directly from the definition of the divisor class group and statement 3 from a well-known theorem of Dickson [8, Theorem 9.18]. Assertion 2 follows from a fundamental result of Skula [16] for Krull domains. Namely, if D is a Krull domain with divisor class group G and P is the set of prime divisors of D^* then for every finite subset $E \subseteq P$ we have

$$G = \langle \{[p] \mid p \in P \setminus E\} \rangle$$

(see [1, Lemma 3.3]). Hence a Krull domain D has either a divisor class which contains infinitely many prime divisors, or infinitely many divisor classes which contain prime divisors. This yields assertion 2.

To prove 4, suppose $\varphi(q) = ke_i$ with $k = \operatorname{ord}[e_i] < \infty$ (with respect to the class group). We need q to be irreducible. If $q \le x + y$ for $x, y \in \boldsymbol{M}(a_1,\dots,a_n)$ and $q \not\le x$, then $ke_i = \varphi(q) \le \varphi(x) + \varphi(y)$ and $ke_i = \varphi(q) \not\le \varphi(x)$. Therefore, $e_i \le \varphi(y)$ and $\varphi(q) = ke_i \le \varphi(ky)$, which implies $q \le ky$. Conversely, suppose q is primary and let $\varphi(q) = \sum_{i\in I} q_i e_i$ with I finite and $q_i \ge 1$. By the definition of a divisor theory, there exist for each $i \in I$ elements $x_{ij} \in \boldsymbol{M}(a_1,\dots,a_n)$ such that $e_i = \min\{\varphi(x_{ij}) \mid j \in I_i\}$ with I_i finite ("min" here is taken componentwise). It follows that $\varphi(q) \le c \sum_{i\in I} e_i \le c \sum_{i\in I} \varphi(x_{ij(i)})$ for some $c \ge 1$ and $j(i)$ taken arbitrarily from I_i. This implies $q \le c \sum_{i\in I} x_{ij(i)}$ for all $j(i) \in I_i$. Since q is primary, it follows inductively that there exist $i_0 \in I$ and integers $k_j \ge 1$ such that $q \le k_j x_{i_0 j}$ for all $j \in I_{i_0}$. For $k' = \max_j k_j$, therefore, we have that

$$\varphi(q) \le k' \min\{\varphi(x_{i_0 j}) \mid j \in I_{i_0}\} = k' e_{i_0}.$$

That is, $\varphi(q) = ke_{i_0}$ for some $k \le k'$ and, because q is irreducible, we must have $\operatorname{ord}[e_{i_0}] = k < +\infty$.

Concerning the particular monoid $\boldsymbol{M}(a_1,\dots,a_m;b)$, let q be primary. Thus $\varphi(q) = ke_i$ with $k = \operatorname{ord}[e_i] < \infty$. The element $x = b/\gcd(a_i,b)\bar{e}_i + a_i/\gcd(a_i,b)\bar{e}_{m+1}$ is in $\boldsymbol{M}(a_1,\dots,a_n;b)$ and it is obviously irreducible. By the definition of φ, $\varphi(x) = le_i$ for some $l \in \mathbb{N}$ and $k = \operatorname{ord}[e_i]$ implies $k \le l$. Hence, $\varphi(q) \le \varphi(x)$ and the irreducibility of x implies $q = x$.

Finally, concerning assertion 5, suppose $\sum_{i\in I} q_i = \sum_{j\in J} p_j$ for primary elements q_i, p_j. By applying φ and using property 4 above we obtain a bijection $\alpha : I \to J$ such that $q_i = p_{\alpha(i)}$ for all $i \in I$. □

We now compute the divisor class groups of the $\boldsymbol{M}(a_1,\dots,a_n)$, separately for the two possible cases mentioned above.

Theorem 1.3. 1. *Consider the monoid* $\boldsymbol{M}(a_1,\dots,a_n;b)$, $n \ge 2$, *as in case one above where* $c_i = \gcd(b \cup \{a_j\}_{j\ne i})$ *and* $c = \prod_{i=1}^n c_i$. *Then*

$$\operatorname{Cl}(\boldsymbol{M}(a_1,\dots,a_n;b)) = \mathbb{Z}_{b/c}.$$

2. *Consider the monoid* $\boldsymbol{M}(a_1,\ldots,a_n;b_1,\ldots,b_k)$, $n \geq 2$ *and* $k \geq 2$, *as in case two above. Then*

$$\mathrm{Cl}(\boldsymbol{M}(a_1,\ldots,a_n;b_1,\ldots,b_k)) = \mathbb{Z}.$$

Proof. For a monoid $\boldsymbol{M} = \boldsymbol{M}(a_1,\ldots,a_n)$ of general type by Lemma 2.1, we have an isomorphism $\alpha : \boldsymbol{M} \to \boldsymbol{M}'$ where $\boldsymbol{M}' = \boldsymbol{M}(a_1',\ldots,a_n')$ is the normalized monoid. For φ and φ' defining the divisor theory of $\boldsymbol{M}$ and $\boldsymbol{M}'$ respectively, we have from the definition of α that $\varphi = \varphi' \circ \alpha$. Therefore, the two class groups $\mathrm{Cl}(\boldsymbol{M})$ and $\mathrm{Cl}(\boldsymbol{M}')$ are isomorphic and it suffices to consider a normalized monoid.

To prove assertion 1, we may assume that $\boldsymbol{M} = \boldsymbol{M}(a_1,\ldots,a_n;b)$ is normalized, that is $c_i = 1$ for $1 \leq i \leq n$ and $c = 1$. Choose integers $y_1,\ldots,y_n$ such that $a_1y_1 + \cdots + a_ny_n = 1$. The order of $(y_1,\ldots,y_n)$ in $\mathrm{Cl}(\boldsymbol{M})$ is clearly b. Choose for each i a number $t_i \in \mathbb{N}$ such that $k_i = a_i + bt_i > 0$. Then for all i, $e_i - k_i(y_1,\ldots,y_n)$ is a solution of the normalized equation in integers and hence, $k_i[(y_1,\ldots,y_n)] = [e_i]$ for all $1 \leq i \leq n$. Thus, $\mathrm{Cl}(\boldsymbol{M})$ is cyclic of order b.

Concerning assertion 2, we also reduce to the case of a normalized monoid, $\boldsymbol{M} = \boldsymbol{M}(a_1,\ldots,a_n;b_1,\ldots,b_k)$. Let $t = n + k$ and $f : \mathbb{Z}^t \to \mathbb{Z}$,

$$f(x_1,\ldots,x_t) = a_1x_1 + \cdots + a_nx_n - b_1x_{n+1} - \cdots - b_kx_{n+k}.$$

Because the greatest common divisor of the a_i and b_j is 1, f must be surjective and hence,

$$\mathbb{Z}^t/\ker f \cong \operatorname{im} f = \mathbb{Z}.$$

Obviously, $\boldsymbol{Q}(\boldsymbol{M}) = \ker f$. Since all projections of $\boldsymbol{M}$ are essential, φ must be the identity and we obtain

$$\mathrm{Cl}(\boldsymbol{M}) = \mathbb{Z}^t/\varphi(\boldsymbol{Q}(\boldsymbol{M})) = \mathbb{Z}^t/\ker f \cong \mathbb{Z}. \qquad \square$$

Corollary 1.4. *For monoids of the type* $\boldsymbol{M} = \boldsymbol{M}(a_1,\ldots,a_m)$, $m \geq 3$, *the following statements are equivalent*:

(i) $\boldsymbol{M}$ *is factorial.*

(ii) $\boldsymbol{M}$ *is of the form* $\boldsymbol{M} = \boldsymbol{M}(a_1,\ldots,a_n;b)$ *and* $b = c = \prod_{i=1}^n c_i$.

(iii) $\boldsymbol{M}$ *is of the form* $\boldsymbol{M} = \boldsymbol{M}(a_1,\ldots,a_n;b)$ *and each element of* $\boldsymbol{M}$ *is a sum of primary elements.*

(iv) $\boldsymbol{M}$ *is isomorphic to* $\mathbb{N}^n$ *under addition with* $n = m - 1$.

Proof. By Theorem 1.3 and the general fact 3, statements (i) and (ii) are equivalent. (ii) $\Rightarrow$ (iii): Since by Theorem 1.3 $\mathrm{Cl}(\boldsymbol{M})$ must be trivial, we have that ord $[e_i] = 1$ for $1 \leq i \leq n$. By Proposition 1.2(4), the primary elements q_i of $\boldsymbol{M}$ are given by $\varphi(q_i) = e_i$ for all i. If $x \in \boldsymbol{M}$ then $\varphi(x) = \sum_{i=1}^n x_ie_i = \sum_{i=1}^n x_i\varphi(q_i) = \varphi(\sum_{i=1}^n x_iq_i)$ with $x_i \in \mathbb{N}$ and hence, $x = \sum_{i=1}^n x_iq_i$.

(iii) $\Rightarrow$ (iv): The isomorphism follows by using the unique representation by primary elements from Proposition 1.2(5).

(iv) $\Rightarrow$ (i): The irreducible elements in the additive monoid $\mathbb{N}^n$ are the $e_i, 1 \le i \le n$, the representation by which is unique. □

As the corollary indicates, primary elements play an important role (in [17] the so-called "completely fundamental" elements are considered, which turn out to be equivalent to primary elements). According to the corollary, if there are plenty of primary elements in the sense that they generate the monoid, then the monoid must be factorial. Whereas in general primary elements need not be prime elements, this holds in factorial monoids. There exist simple monoids which do not have primary elements at all. For example, by Theorem 1.3, in conjunction with Proposition 1.2(4), the monoids $\boldsymbol{M}(a_1,\dots,a_n;b_1,\dots,b_k)$ (note that $n,k \ge 2$) cannot possess primary elements. As we shall see later, half-factorial monoids of type $\boldsymbol{M}(a_1,\dots,a_n;b)$ can be characterized by the property that there are enough primary elements in the sense that they generate the monoids in a convex manner.

As is the case with a Krull domain, the divisor class group can be used to compute the complete set of irreducible elements of $\boldsymbol{M}(a_1,\dots,a_n)$. Let G be an abelian group. A nonempty sequence $\{g_1,\dots,g_r\}$ of not necessarily distinct nonzero elements of G is called a *minimal-zero sequence* if $g_1 + \cdots + g_r = 0$ and no proper subsequence of $\{g_1,\dots,g_r\}$ sums to zero. By [9, Proposition 1], the irreducible elements of $\boldsymbol{M}(a_1,\dots,a_n)$ are in correspondence with the minimal-zero sequences of $\mathrm{Cl}(\boldsymbol{M}(a_1,\dots,a_n))$ consisting of the divisor classes containing a prime divisor.

The following examples illustrate some of our definitions and results.

Example 1.5. 1. Nonnegative solutions of linear Diophantine equations play a role in various parts of algebra. The following equation we take from [11] to illustrate our general principles. The equation $2x_1 + 5x_2 = 3x_3$ is already in normalized form and for the solution monoid $\boldsymbol{M} = \boldsymbol{M}(2,5;3)$ it follows $\mathrm{Cl}(\boldsymbol{M}) = \mathbb{Z}_3$ by Theorem 1.3, implying that $\boldsymbol{M}$ cannot be factorial. According to Proposition 1.2 there are two primary elements $q_1 = 3\bar{e}_1 + 2\bar{e}_3 = (3,0,2)$ and $q_2 = 3\bar{e}_2 + 5\bar{e}_3 = (0,3,5)$ corresponding to $\mathrm{ord}\,[e_1] = \mathrm{ord}\,[e_2] = 3$. The minimal zero-sequences, beside $3[e_1] = 3[e_2] = 0$ are $[e_1] + 2[e_2] = 0$ and $2[e_1] + [e_2] = 0$. Thus, there are two more irreducible elements, $x = (1,2,4)$ and $y = (2,1,3)$, neither of which is primary. The latter can be represented in a convex manner by $3x = q_1 + 2q_2$, $3y = 2q_1 + q_2$. Thus, by this representation the number of irreducible summands neither increases nor decreases and we conclude that $\boldsymbol{M}$ must be half-factorial. The above representations also imply that $\boldsymbol{M}$ has no prime element because $q_1 \le 3x$, $q_2 \le 3y$ but neither $q_1 \le x$ nor $q_2 \le y$.

If we slightly change the given equation to $x_1 + 5x_2 = 3x_3$, then the solution monoid $\boldsymbol{M}(1,5;3)$ is no longer half-factorial. By the same method as before, we obtain as the irreducible elements $q_1 = (3,0,1)$, $q_2 = (0,3,5)$, $x = (1,1,2)$ where q_1, q_2 are primary but not prime and x is not primary. $\boldsymbol{M}(1,5;3)$ is not half-factorial because of the relationship $3x = q_1 + q_2$.

2. Consider the equation $2x_1 + 3x_2 + 4x_3 = 6x_4$. Since $c_1 = c_3 = 1$, $c_2 = 2$, and $c = 2$, normalization yields $x_1 + 3x_2 + 2x_3 = 3x_4$. The class group for both equations is $\mathbb{Z}_3$, hence $\boldsymbol{M} = \boldsymbol{M}(1,3,1;3)$ is not factorial. Proceeding as in Example 1, we obtain for $\boldsymbol{M}$ as primary elements $q_1 = (3,0,0,1)$, $q_2 = (0,1,0,1)$, $q_3 = (0,0,3,1)$ corresponding to $3[e_1] = 3[e_3] = 0$ and $[e_2] = 0$. This shows that q_2 is a prime element. Beside the above, the only minimal zero-sequences are $[e_1] + 2[e_3] = 0$ and $2[e_1] + [e_3] = 0$ which yield the irreducible elements $x = (1,0,2,1)$ and $y = (2,0,1,1)$. Furthermore, $3x = q_1 + 2q_3$ and $3y = 2q_1 + q_3$ which shows that q_1 and q_3 are not prime and that $\boldsymbol{M}$ and, hence, $\boldsymbol{M}(2,3,4;6)$ are half-factorial. Thus $\boldsymbol{M}$ has five irreducible elements consisting of one prime element, two primary elements which are not prime and two irreducible elements which are not primary.

Although the class groups in the two examples are isomorphic and both have some relations in common, the monoids in the two examples are not isomorphic (e.g., the former contains a prime but the latter does not).

For the remainder of this paper, we focus on the problem of determining when the monoid $\boldsymbol{M}(a_1,\ldots,a_n;b)$ is half-factorial. While there is a characterization of such half-factorial monoids in terms of the cross numbers of the minimal zero-sequences (see [15] or [5] for an analysis), we focus on conditions involving the coefficients $a_1,\ldots,a_n,b$. The problem of determining when the monoid $\boldsymbol{M}(a_1,\ldots,a_n;b_1,\ldots,b_k)$ is half-factorial is closely related to the work done in [2,3]. While we leave investigation of this problem to future work, we provide an example which helped motivate our current research.

Example 1.6. In [15, Example 2], the authors argue that the monoid $\boldsymbol{M}(5,2;5)$ is factorial, the monoid $\boldsymbol{M}(1,1,2)$ is half-factorial and provide the monoid $\boldsymbol{M}(1,1;1,1)$ as an example of a monoid where all projections are essential. The monoid $\boldsymbol{M}(1,1;1,1)$ is also half-factorial. This can be seen using elementary linear algebra as follows. Using a matrix argument, it is easy to show that the only irreducible elements of $\boldsymbol{M}(1,1;1,1)$ are $u_1 = (1,0,1,0)$, $u_2 = (1,0,0,1)$, $u_3 = (0,1,1,0)$ and $u_4 = (0,1,0,1)$. If

$$x_1u_1 + x_2u_2 + x_3u_3 + x_4u_4 = y_1u_1 + y_2u_2 + y_3u_3 + y_4u_4,$$

then $x_1 + x_2 = y_1 + y_2$ and $x_3 + x_4 = y_3 + y_4$ and thus $x_1 + x_2 + x_3 + x_4 = y_1 + y_2 + y_3 + y_4$. This result can also be seen using the divisor class group. Since $[e_1] - [e_2] = 0$ and $[e_3] - [e_4] = 0$ in the class group, we have that $\boldsymbol{M}(1,1;1,1)$ is a Krull monoid with divisor class group $\mathbb{Z}$ such that all the prime divisors of $\boldsymbol{M}(1,1;1,1)$ are contained in the divisor classes 1 and -1. The argument offered in [7, Theorem 4.1] for a Dedekind domain with class group $\mathbb{Z}$ easily extends to any Krull monoid with divisor class group $\mathbb{Z}$ and yields that $\boldsymbol{M}(1,1;1,1)$ is half-factorial. This class group argument can be extended to show that if $\boldsymbol{S}$ is of the form $\boldsymbol{M}(\pm1,\ldots,\pm1;\pm1,\ldots,\pm1)$, then $\boldsymbol{S}$ is half-factorial.

2. The monoids $M := M(a_1, \ldots, a_n; b)$

We want to characterize the half-factorial monoids of the form

$$\boldsymbol{M} := \boldsymbol{M}(a_1, \ldots, a_n; b) := \left\{ (r_1, \ldots, r_{n+1}) \in \mathbb{N}^{n+1} \;\middle|\; \sum_{j=1}^{n} r_j a_j = r_{n+1} b \right\},$$

in terms of their coefficients $a_1, \ldots, a_n, b \in \mathbb{N}_+$. Although we do not have a complete solution for this problem, we will present conditions on the coefficients which are sufficient and others which are necessary for half-factoriality.

Let the monoid $\boldsymbol{M} = \boldsymbol{M}(a_1, \ldots, a_n; b)$ be given, normalized according to Lemma 1.1 (i.e., $\gcd\{b \cup \{a_j\}_{j \neq i}\} = 1$ for $i = 1, \ldots, n$ and $\gcd\{a_j \mid 1 \leq j \leq n\} = 1$) and let $a_j = \alpha_j d_j$, $b = \beta_j d_j$, $d_j = \gcd a_j, b \in \mathbb{N}$, $1 \leq j \leq n$. Let $e_1 := (1, 0, \ldots, 0), \ldots, e_{n+1} := (0, \ldots, 0, 1)$ be the unit vectors in $\mathbb{Q}^{n+1}$.

It can be immediately checked that the primary elements of $\boldsymbol{M}$ are the n linear independent vectors $q_i = \beta_i e_i + \alpha_i e_{n+1}$, $1 \leq i \leq n$ (cf. also Proposition 1.2). Every element $x \in \boldsymbol{M}$ has a unique representation $x = \sum_{i=1}^{n} r_i q_i$ with $r_i \in \mathbb{Q}$, $r_i \geq 0$, for each $x \in \boldsymbol{M}$, and the rational number $z(x) := \sum_{i=1}^{n} r_i$ is the value of the so-called *Zaks–Skula function* at x (cf. [15,16]). There is a minimal positive number $m(x) \in \mathbb{N}$ such that $m(x)x$ splits completely into primary elements (i.e., $m(x)x = \sum_{i=1}^{n} m_i q_i$, $m_i \in \mathbb{N}$). The number $z(m(x)x) = m(x)z(x)$ equals the number of primary elements which are involved in the above representation of $m(x)x$. Hence, $z(x)$ measures the splitting of x into primary elements.

The following proposition provides a simple *geometrical* criterion for the half-factoriality of $\boldsymbol{M}$, namely that $\boldsymbol{M}$ is half-factorial if and only if the set $I(\boldsymbol{M})$ of irreducible elements is flat in the sense that it is contained in the $(n-1)$-dimensional simplex

$$Simpl(\boldsymbol{M}) = \{x \in \boldsymbol{M} \mid z(x) = 1\}$$

of convex combinations over $\mathbb{Q}$ of the primary elements. This is equivalent to $I(\boldsymbol{M})$ being contained in a two-codimensional affine subspace of $\mathbb{Q}^{n+1}$.

Proposition 2.1. *The following statements for the monoid* $\boldsymbol{M} = \boldsymbol{M}(a_1, \ldots, a_n; b)$ *are equivalent*:

(i) $\boldsymbol{M}$ *is half-factorial.*
(ii) $I(\boldsymbol{M}) = \boldsymbol{M} \cap Simpl(\boldsymbol{M})$
(iii) *The Zaks–Skula function is identically* 1 *on* $I(\boldsymbol{M})$.
(iv) *Every element* $(r_1, \ldots, r_{n+1}) \in I(\boldsymbol{M})$ *satisfies the equation* $\sum_{j=1}^{n} r_j d_j = b$.

Proof. (i) $\Rightarrow$ (ii): If $\boldsymbol{M}$ is half-factorial and $x \in I(\boldsymbol{M})$ then $m(x)x = \sum_{i=1}^{n} m_i q_i$ with $m(x) = z(m(x)x) = m(x)z(x)$. Therefore, $x \in Simpl(\boldsymbol{M})$. Note that $I(\boldsymbol{M}) \subset \boldsymbol{M} \cap Simpl(\boldsymbol{M})$ implies $I(\boldsymbol{M}) = \boldsymbol{M} \cap Simpl(\boldsymbol{M})$.

(ii) $\Rightarrow$ (iii): Trivial.

(iii) $\Rightarrow$ (iv): For $x=(r_1,\dots,r_{n+1})\in \boldsymbol{M}$ we have

$$x=\sum_{i=1}^{n+1} r_i e_i=\sum_{j=1}^{n}\frac{r_j}{\beta_j}q_j+\left(r_{n+1}-\sum_{j=1}^{n}\frac{r_j\alpha_j}{\beta_j}\right)e_{n+1}=\sum_{j=1}^{n}\frac{r_j}{\beta_j}q_j.$$

For $x\in I(\boldsymbol{M})$ equation $z(x)=1$ implies $b=bz(x)=z(bx)=\sum_{j=1}^{n} br_j/\beta_j=\sum_{j=1}^{n} r_j d_j$.

(iv) $\Rightarrow$ (i): Let

$$x=(s_1,\dots,s_{n+1})=\sum_{k=1}^{t} x_k$$

be a sum of t elements $x_1,\dots,x_t\in I(\boldsymbol{M})$. From (iv) it follows that $t=1/b\sum_{j=1}^{n} s_j d_j$. Hence $\boldsymbol{M}$ is half-factorial. □

Remarks. 1. The proof of the proposition shows in particular that the Zaks–Skula function, which is defined for arbitrary Krull monoids with a torsion class group, can be explicitly calculated in the case of a monoid $\boldsymbol{M}(a_1,\dots,a_n;b)$ as $z(x)=1/b\sum_{j=1}^{n} s_j d_j$ for $x=(s_1,\dots,s_{n+1})$.

2. It is not difficult to see that $b=\operatorname{lcm}\{m(x)\mid x\in I(\boldsymbol{M})\}$. Thus, b is an upper bound for the possible values of $m(x)$ for $x\in I(\boldsymbol{M})$. Also, from a general result on Krull monoids [15, Theorem 1] it follows that $z(x)$ for $x\in I(\boldsymbol{M})$ is bounded from above by the so-called cross number $k(\mathrm{Cl}(\boldsymbol{M}))$ of the class group. A fortiori we have that $\sum_{i=1}^{n} x_i d_i\le b\ k(\mathrm{Cl}(\boldsymbol{M}))$ for all $x\in I(\boldsymbol{M})$.

We illustrate Proposition 2.1 by returning to Example 1.5.

Example 2.2. For $\boldsymbol{M}(2,5;3)$ the primary elements are $q_1=(3,0,2)$ and $q_2=(0,3,5)$. Since $m(x)|b$ by Remark 3 above, for the non-primary irreducible elements $x=(1,2,4)$ and $y=(2,1,3)$ we must have $m(x)=m(y)=3$. Indeed, $3x=q_1+2q_2$ and $3y=2q_1+q_2$ and hence, all irreducible elements are contained in the one-dimensional simplex in $\mathbb{Q}^3$ spanned by q_1 and q_2. The affine subspace is given by $x_1+x_2=3$ and also contains all irreducible elements. Concerning the slight variation $\boldsymbol{M}(1,5;3)$, the irreducible elements are $q_1=(3,0,1)$, $q_2=(0,3,5)$ and $x=(1,1,2)$, where q_1,q_2 are primary and x is not. Again, $m(x)=3$ and $3x=q_1+q_2$. Thus, x is not contained in the simplex spanned by q_1 and q_2. The affine subspace is the same as before containing q_1 and q_2 but not x.

The following corollary presents a necessary condition for half-factoriality of a monoid $\boldsymbol{M}=\boldsymbol{M}(a_1,\dots,a_n;b)$ in terms of its coefficients.

Corollary 2.3. *Let $\boldsymbol{M}=\boldsymbol{M}(a_1,\dots,a_n;b)$ be half-factorial and $d_j=\gcd\{a_j,b\}$, $1\le j\le n$. Then*

(1) $\sum_{j=1}^{n} r_j d_j\in b\mathbb{N}$ *for every* $(r_1,\dots,r_{n+1})\in\boldsymbol{M}$,

(2) $a_i d_j-a_j d_i\in b\mathbb{Z}$ *for all* $i,j\in\{1,\dots,n\}$.

Proof. Statement (1) follows directly from Proposition 2.1. For (2), take $m \in \mathbb{N}$ with $mb - a_j \in \mathbb{N}$ for $1 \le j \le n$. Then

$$a_i mb = a_i(mb - a_j) + a_i a_j \text{ for all } i, j \in \{1, \dots, n\}.$$

Therefore by (1),

$$(mb - a_j)d_i + a_i d_j = mb + (a_i d_j - a_j d_i) \in b\mathbb{N}.$$

To shorten notation we call $\boldsymbol{M} = \boldsymbol{M}(a_1, \dots, a_n; b)$ a *regular* monoid if

$$b | (a_i d_j - a_j d_i) \quad \text{for all } i, j \in \{1, \dots, n\} \text{ and } d_j := \gcd\{a_j, b\}.$$

Hence, Corollary 2.3 implies that a half-factorial monoid of the form $\boldsymbol{M} = \boldsymbol{M}(a_1, \dots, a_n; b)$ is regular. With further regard to the half-factorial property, we may restrict the class of monoids to be considered even further by using the following lemma.

Lemma 2.4. *A regular monoid $\boldsymbol{M} = \boldsymbol{M}(a_1, \dots, a_n; b)$ is isomorphic to the monoid $\tilde{\boldsymbol{S}} = \boldsymbol{M}(d_1, \dots, d_n; b)$ with $d_j = \gcd(a_j, b) \in \mathbb{N}$, $1 \le j \le n$. The morphism*

$$\varphi : \boldsymbol{M} \to \tilde{\boldsymbol{S}},\ \varphi(r_1, \dots, r_{n+1}) := \left(r_1, \dots, r_n, \frac{1}{b} \sum_{j=1}^{n} r_j d_j \right)$$

is bijective and $\varphi^{-1}(s_1, \dots, s_{n+1}) = (s_1, \dots, s_n, \frac{1}{b} \sum s_j a_i)$.

Proof. It suffices to show for all $(r_1, \dots, r_{n+1}) \in \mathbb{N}^{n+1}$ that

$$\frac{1}{b} \sum_{j=1}^{n} r_j d_j \in \mathbb{N} \Leftrightarrow \frac{1}{b} \sum r_j a_j \in \mathbb{N}.$$

Let $a_j = \alpha_j d_j$, $b = \beta_j d_j$, and $k_{ij} := (a_i d_j - a_j d_i)/b \in \mathbb{N}$ for $1 \le i, j \le n$. Note that $b = \operatorname{lcm}(\beta_1, \dots, \beta_n)$ because of our assumption $\gcd(d_1, \dots, d_n) = 1$. For $(r_1, \dots, r_{n+1}) \in \mathbb{N}^{n+1}$ and every $i \in \{1, 2, \dots, n\}$ we have

$$\begin{aligned} \sum_{j=1}^{n} r_j a_j &= \sum_{j=1}^{n} r_j \left(\frac{a_i d_j - k_{ij} b}{d_i} \right) = \frac{a_i}{d_i} \sum_{j=1}^{n} r_j d_j - \frac{b}{d_i} \sum_{j=1}^{n} r_j k_{ij} \\ &= \alpha_i \sum_{j=1}^{n} r_j d_j - \beta_i \cdot \sum_{j=1}^{n} r_j k_{ij}. \end{aligned}$$

If $\sum_{j=1}^{n} r_j d_j \in b\mathbb{N}$, then $\beta_i | \sum_{j=1}^{n} r_j a_j$ for $1 \le i \le n$ and therefore $\sum_{j=1}^{n} r_j a_j \in b\mathbb{N}$. If $\sum_{j=1}^{n} r_j a_j \in b\mathbb{N}$, then $\beta_i | \sum_{j=1}^{n} r_j d_j$ for $1 \le i \le n$, since $\gcd(\alpha_i, \beta_i) = 1$. Hence $\sum_{j=1}^{n} r_j d_j \in b\mathbb{N}$. □

The following simple result shows that it is easy to characterize half-factorial monoids of the form $\boldsymbol{M}(a_1, a_2; b)$.

Corollary 2.5. *A monoid $\boldsymbol{M} = \boldsymbol{M}(a_1, a_2; b)$ is half-factorial if and only if it is regular.*

Proof. The assertion ($\Rightarrow$) follows directly from the definition of regular and Corollary 2.3. For ($\Leftarrow$), we may assume that $\boldsymbol{M} = \boldsymbol{M}(a_1, a_2; b)$ is already given in normalized form (i.e., $\gcd\{a_i, b\} = 1$ for $1 \le i \le 2$). By Lemma 2.4, $\boldsymbol{M}$ is isomorphic to $\tilde{\boldsymbol{S}} = \boldsymbol{M}(1, 1; b)$. Since $I(\tilde{\boldsymbol{S}}) = \{(k, b-k, 1) \mid 0 \le k \le b\}$, the monoid $\tilde{\boldsymbol{S}}$ is obviously half-factorial. □

As a consequence, we obtain that half-factoriality is not closely linked with the class group in the following sense. For any natural number $b \ge 3$ the monoid $\boldsymbol{M}(b-1, b+1; b)$ is not regular, hence not half-factorial. But it has the same class group, namely $\mathbb{Z}_b$, as the half-factorial monoid $\boldsymbol{M}(1, 1; b)$.

With respect to the question of half-factoriality of $\boldsymbol{M} := \boldsymbol{M}(a_1, \ldots, a_n; b)$, we may assume that $d_j = \gcd\{a_j, b\} < b$ for $1 \le j \le n$. If $d_k = b$, $a_k = \alpha b$ for some $k \in \{1, \ldots, n\}$, then

$$\phi : \boldsymbol{M}(a_1, \ldots, a_n; b) \to \mathbb{N} \times \boldsymbol{M}(a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n; b),$$

defined by

$$\phi(r_1, \ldots, r_{n+1}) := (r_k, r_1, \ldots, r_{k-1}, r_{k+1}, \ldots, r_n, r_{n+1} - \alpha r_k),$$

is an isomorphism of semigroups. In particular, $\boldsymbol{M}(a_1, \ldots, a_n; b)$ is half-factorial if and only if $\boldsymbol{M}(a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n; b)$ is half-factorial. We call the number

$$k := \#\{d_j \mid 1 \le j \le n, d_j < b\}$$

the *length* of the monoid $\boldsymbol{M}(a_1, \ldots, a_n; b)$. By a permutation of the coefficients of $\boldsymbol{M} := \boldsymbol{M}(a_1, \ldots, a_n; b)$ we can always arrange a situation where

$$1 \le d_1 < d_2 < \cdots < d_k < b, \text{ and } \{d_i \mid 1 \le i \le k\} = \{d_j \mid 1 \le j \le n\} \setminus \{b\}.$$

In this situation, we call the monoid $\boldsymbol{S} = \boldsymbol{M}(d_1, \ldots, d_k; b)$ the $=$ *special reduction* of $\boldsymbol{M} = \boldsymbol{M}(a_1, \ldots, a_n; b)$. Note that $\boldsymbol{S}$ is uniquely determined by $\boldsymbol{M}$. To decide whether a (regular) monoid is half-factorial it suffices to study its special reduction.

Proposition 2.6. *The following statements about a regular monoid* $\boldsymbol{M} = \boldsymbol{M}(a_1, \ldots, a_n; b)$ *are equivalent*:

(i) $\boldsymbol{M}$ *is half-factorial* (*resp. factorial*).

(ii) *The special reduction* $\boldsymbol{S} = \boldsymbol{M}(d_1, \ldots, d_k; b)$ *of* $\boldsymbol{M}$ *is half-factorial* (*resp. factorial*).

For the proof of this proposition we need the following auxiliary statement.

Lemma 2.7. *Let* T *be an abelian semigroup and* $\varphi : T \to \mathbb{N}$ *a semigroup morphism. The semigroup*

$$H := \{(n, z) \mid n \in \mathbb{N}, z \in T, \varphi(z) \ge n\}$$

is half-factorial (*resp. factorial*) *if and only if* T *is half-factorial* (*resp. factorial*).

Proof. For $1 \le j \le t$, let $y_j = (n_j, z_j) \in H$ be irreducible elements, with $\sum_{j=1}^{t} m_j y_j = 0$ and $m_j \in \mathbb{Z}$. In particular, note that $\sum_{j=1}^{t} m_j z_j = 0$. The elements z_j are irreducible in T since otherwise a decomposition $z_j = u + w$, $u, w \in T$, $u \neq z_j \neq w$, would lead to $n_j \le \varphi(z_j) = \varphi(u) + \varphi(w)$ and to $\alpha, \beta \in \mathbb{N}$ with $\alpha \le \varphi(u)$, $\beta \le \varphi(w)$, $\alpha + \beta = n_j$. In particular $y_j = (n_j, z_j) = (\alpha, u) + (\beta, w)$ would be reducible, contrary to our assumption.

If T is half-factorial then $\sum_{j=1}^{t} m_j z_j = 0$ implies $\sum_{j=1}^{t} m_j = 0$. If T is not half-factorial and $\sum_{j=1}^{t} m_j z_j = 0$ for some irreducible elements $z_j \in T$, $\sum_{j=1}^{t} m_j \neq 0$, then $(0, z_j) \in H$ is irreducible, $1 \le j \le t$, and $\sum_{j=1}^{t} m_j (0, z_j) = 0$. If T is factorial then $\sum_{j=1}^{t} m_j z_j = 0$ implies $m_j = 0$ for $1 \le j \le t$. If T is not factorial and $\sum_{j=1}^{t} m_j z_j = 0$ for some irreducible elements $z_j \in T$, $m_1 \neq 0$, then $(0, z_j) \in H$ is irreducible, $1 \le j \le t$, and $\sum_{j=1}^{t} m_j (0, z_j) = 0$. □

Proof of Proposition 2.6. We give the proof for the statement about half-factoriality; the proof for the factoriality statement is completely analogous. The monoids $\boldsymbol{M}$ and $\tilde{\boldsymbol{S}} = \boldsymbol{M}(d_1, \ldots, d_n; b)$ are isomorphic (Lemma 2.4). Moreover they have the same special reduction $\boldsymbol{S} = \boldsymbol{S}(d_1, \ldots, d_k; b)$. Therefore it suffices to show that $\boldsymbol{S}$ is half-factorial if and only if $\tilde{\boldsymbol{S}}$ is half-factorial. This we prove by induction on $n \ge k$. By the above remarks, we may assume that $d_j < b$ for $1 \le j \le n$. Assuming that $n \ge k + 1$ we choose $j_0 \in \{1, \ldots, k\}$ with $d_n = d_{j_0}$. Define $T := \boldsymbol{M}(d_1, \ldots, d_{n-1}; b)$ and $\varphi : T \to \mathbb{N}$, $\varphi(s_1, \ldots, s_{n-1}, s_n) := s_{j_0}$. Then

$$H := \{(t, z) \in \mathbb{N} \times T, \varphi(z) \ge t\}$$

is a semigroup and is isomorphic to $\tilde{\boldsymbol{S}}$ via

$$\phi : \tilde{\boldsymbol{S}} \to H, \phi(r_1, \ldots, r_{n+1}) := (r_n, r_1, \ldots, r_{j_0 - 1}, r_{j_0} + r_n, r_{j_0 + 1}, \ldots, r_{n-1}, r_{n+1})$$

with

$$\phi^{-1}(m, s_1, \ldots, s_n) = (s_1, \ldots, s_{j_0 - 1}, s_{j_0} - m, s_{j_0 + 1}, s_{n-1}, m, s_n).$$

This implies, together with Lemma 2.7:

$$T \text{ half factorial} \Leftrightarrow H \text{ half-factorial} \Leftrightarrow \tilde{\boldsymbol{S}} \text{ half-factorial}.$$

Note that $\boldsymbol{S} = \boldsymbol{M}(d_1, \ldots, d_k; b)$ is also the reduction of T. The induction step finishes the proof. □

3. Special reductions

As we have seen in the last section, every half-factorial monoid $\boldsymbol{M} = \boldsymbol{M}(a_1, \ldots, a_n; b)$ has to be regular, and a regular monoid $\boldsymbol{M} = \boldsymbol{M}(a_1, \ldots, a_n; b)$ is half-factorial if and only if its special reduction is half-factorial. Since it is much easier to deal with the special reduction of a monoid $\boldsymbol{M}$ than with $\boldsymbol{M}$ itself, we fix again the following setting:

Let $d_1,\dots,d_k,b$ be finitely many integers with $\gcd(d_1,\dots,d_k)=1$ and

$$1 \le d_1 < \cdots < d_k < b = \beta \cdot \operatorname{lcm}(d_1,\dots,d_k) \quad \text{for some } \beta \in \mathbb{N}_+.$$

The monoid

$$\boldsymbol{S} := \boldsymbol{S}(d_1,\dots,d_k;b) := \left\{ (r_1,\dots,r_{k+1}) \in \mathbb{N}^{k+1} \;\middle|\; \sum_{i=1}^{k} r_i d_i = r_{k+1} b \right\}$$

is of length k and equals its special reduction. Therefore we call $\boldsymbol{S}$ a *special monoid.* $\boldsymbol{S}$ is an additive subsemigroup of $\mathbb{N}^{k+1}$ and we are interested in criteria on $d_1,\dots,d_k,b$ so that $\boldsymbol{S}$ is half-factorial. Factoriality for such monoids is easy to check since a special monoid $\boldsymbol{S}$ is factorial if and only if $b=\prod_{i=1}^{k} c_i$ where $c_i=\gcd\{d_j\}_{j\neq i}$. As an elementary calculation shows, the latter condition is equivalent to $b^{k-1}=\prod_{i=1}^{k} d_i$. Thus, a given special monoid $S=S(d_1,\dots,d_k;b)$ is factorial if and only if $\prod_{i=1}^{k} d_i = b^{k-1}$. This means that a regular monoid $\boldsymbol{M}=\boldsymbol{M}(a_1,\dots,a_n;b)$, given in normalized form, is factorial if and only if it has length $k=1$ and its special reduction equals $\boldsymbol{S}=\boldsymbol{S}(1;1)$.

It is much more difficult to characterize half-factorial special monoids. We start with a few elementary facts for a special monoid $\boldsymbol{S}=\boldsymbol{S}(d_1,\dots,d_k;b)$.

Elementary Facts:

(1) If $(r_1,\dots,r_k,m) \in \boldsymbol{S}$ is irreducible then $m=1$ or $r_i d_i < b$ for $1 \le i \le k$. In particular $m \le \max\{1,k-1\}$.

(2) From (1) and Proposition 2.1(iv), it follows immediately that $\boldsymbol{S}$ is half-factorial for $k \le 2$. This implies that every regular monoid $\boldsymbol{M}=\boldsymbol{M}(a_1,\dots,a_n;b)$ of length k is half-factorial. In particular every regular monoid $\boldsymbol{M}=\boldsymbol{M}(a_1,\dots,a_n;pq)$ with prime numbers p and q is half-factorial.

(3) If $\boldsymbol{S}(d_1,\dots,d_k;b)$ is half-factorial then $\boldsymbol{S}(d_1,\dots,d_k;rb)$ is half-factorial for every $r \in \mathbb{N}_+$.

(4) The monoid $\boldsymbol{S}=\boldsymbol{S}(1,d_2,d_3;b)$ is half-factorial. To see this, let $(r_1,r_2,r_3,m) \in \boldsymbol{S}$ be irreducible and assume that $m=2$. Then

$$r_1 + r_2 d_2 = 2b - r_3 d_3 > b$$

and

$$0 < r_1' := r_1 + r_2 d_2 - b = r_1 - (b - r_2 d_2) < r_1.$$

It follows that

$$(r_1',0,r_3,1) \in \boldsymbol{S}, \quad (r_1 - r_1', r_2, 0, 1) \in \boldsymbol{S}$$

and

$$(r_1,r_2,r_3,m) = (r_1,r_2,r_3,2) = (r_1',0,r_3,1) + (r_1 - r_1', r_2, 0, 1),$$

contrary to the irreducibility of (r_1,r_2,r_3,m). Therefore $m=1$.

(5) Let $\boldsymbol{S}=\boldsymbol{S}(d_1,\dots,d_k;b)$ be a special monoid with $k \ge 3$. If there exists $i_0 \in I := \{1,\dots,k\}$ with the property

$$q := \gcd(d_i,d_j) = \gcd(d_1,\dots,d_{i_0-1},d_{i_0+1},\dots,d_k)$$

for all $i,j \in J := I \setminus \{i_0\}$, $i \neq j$, then $\boldsymbol{S}$ is half-factorial if and only if

$$\boldsymbol{S}_q := \boldsymbol{S}\left(\frac{d_1}{q}, \ldots, \frac{d_{i_0-1}}{q}, d_{i_0}, \frac{d_{i_0+1}}{q}, \ldots, \frac{d_k}{q}; \frac{b}{q}\right)$$

is half-factorial. Note that the assumption is always true for $k=3$. A proof of statement (5) is given by the remark that

$$\boldsymbol{S} \to \boldsymbol{S}_q,$$

defined by

$$(r_1, \ldots, r_k, m) \mapsto \left(r_1, \ldots, r_{i_0-1}, \frac{r_{i_0}}{q}, r_{i_0+1}, \ldots, r_k, m\right),$$

is an isomorphism between $\boldsymbol{S}$ and $\boldsymbol{S}_q$.

We shall see later (Corollary 4.4 to Theorem 4.1) that $S(d_1,d_2,d_3;b)$ is always half-factorial. But for $k \geq 3$ there is a standard procedure of constructing special monoids $S(1,d_1,\ldots,d_k;b)$ which are not half-factorial.

Proposition 3.1. *Let $q_1 > q_2 > \cdots > q_k \geq 2$ be finitely many natural numbers with $\gcd(q_i,q_j) = 1$ for $1 \leq i < j \leq k$ and $a := \sum_{i=1}^k 1/q_i \geq 1$. Define $b := \prod_{i=1}^k q_i$ and $d_i := b/q_i, 1 \leq i \leq k$. The special monoid $M = M(1,d_1,\ldots,d_k;b)$ is not half-factorial and contains an irreducible element of the form $(1,t_1,\ldots,t_k,m)$ with $m > a$.*

Proof. Let

$$A := \{(r_1,\ldots,r_k) \in \mathbb{N}^k \mid 0 \leq r_i \leq q_i - 1,\ 1 \leq i \leq k\}$$

and define

$$\phi : A \to \mathbb{Z}/b\mathbb{Z},\ \phi(r_1,\ldots,r_k) := \sum_{i=1}^k r_i d_i \bmod b.$$

By our assumptions it is immediate that ϕ is injective, hence bijective. Take $(t_1,\ldots,t_k) \in A$ with $\sum_{i=1}^k t_i d_i \equiv -1 \bmod b$. Then $1 + \sum_{i=1}^k t_i d_i = mb$ for some $m \in \mathbb{N}$ and $x := (1,t_1,\ldots,t_k,m) \in M$. Note that $t_i \geq 1$ for $1 \leq i \leq k$ since $t_i = 0$ would lead to the contradiction $q_i | 1$.

We claim that x is irreducible in M and that $m > a$, thereby proving the proposition.

Assume that $x = y + z$, $y,z \in M$. Then y (or z) is of the form $y = (0,r_1,\ldots,r_k,r)$ $0 \leq r_i \leq q_i - 1$, $1 \leq i \leq k$. But $q_i | r_i d_i$ and therefore $q_i | r_i$, since $\gcd(q_i,d_i) = 1$. It follows that $r_i = 0$ and $y = 0$. We have

$$m = \frac{1}{b}\left(1 + \sum_{i=1}^k t_i d_i\right) = \frac{1}{b}\left(1 + b\sum_{i=1}^k \frac{t_i}{q_i}\right)$$

$$= \frac{1}{b} + \sum_{i=1}^k \frac{t_i}{q_i} \geq \frac{1}{b} + \sum_{i=1}^k \frac{1}{q_i} > a. \qquad \square$$

For $k = 3$ and $q_1 = 5$, $q_2 = 3$, $q_3 = 2$, we obtain the special monoid $S = S(1, 6, 10, 15; 30)$ which contains the irreducible element $(1, 4, 2, 1, 2)$.

A special monoid $\boldsymbol{S}(d_1, \ldots, d_k; b)$ is half-factorial if the principal ideals $\mathbb{Z}d_i \subset \mathbb{Z}$ form a descending chain $\mathbb{Z}d_1 \supset \mathbb{Z}d_2 \supset \cdots \supset \mathbb{Z}d_k$ in $\mathbb{Z}$.

Proposition 3.2. *Let $\boldsymbol{M} = \boldsymbol{M}(a_1, \ldots, a_n; b)$ be a regular monoid with special reduction $\boldsymbol{S} = \boldsymbol{S}(d_1, \ldots, d_k; b)$. If $d_i | d_j$ for $1 \leq i, j \leq k$, then $\boldsymbol{M}$ is half-factorial. In particular this is the case if $b = p^m$ for some prime number p* and $m \in \mathbb{N}$.

Proof. We proceed by induction on b and may therefore assume that $d_1 = 1$. If $d_i = \gamma_i d_2$, $2 \leq i \leq k$, then $1 = \gamma_2 < \gamma_3 < \cdots < \gamma_k$; moreover $\gamma_i | \gamma_j$ for $2 \leq i, j \leq k$. Let $(r_1, \ldots, r_k, m) \in \boldsymbol{S}$ be irreducible,

$$r_1 + \sum_{i=2}^{k} r_i d_i = mb = r_1 + \left(\sum_{i=2}^{k} r_i \gamma_i \right) d_2.$$

It follows that $r_1 = a d_2$ for some $a \in \boldsymbol{N}$ and

$$\left(a + r_2, r_3, \ldots, r_k, m \frac{b}{d_2} \right) \in \boldsymbol{S} \left(1, \gamma_2, \ldots, \gamma_k; \frac{b}{d_2} \right) = \tilde{\boldsymbol{S}}.$$

By induction, $\tilde{\boldsymbol{S}}$ is half-factorial, so there are natural numbers $\tilde{r}_1 \leq a + r_2$, $r_3' \leq r_3, \ldots, r_k' \leq r_k$ with

$$\tilde{r}_1 + \sum_{i=3}^{k} r_i' \gamma_i = \frac{b}{d_2}.$$

Then

$$\tilde{r}_1 d_2 + \sum_{i=3}^{k} r_i' d_i = b$$

with $\tilde{r}_1 d_2 \leq r_1 + r_2 d_2$. Choosing $r_1', r_2' \in \mathbb{N}$ with $r_1' \leq r_1$, $r_2' \leq r_2$ and $\tilde{r}_1 d_2 = r_1' + r_2' d_2$, we finally obtain $(r_1', r_2', \ldots, r_k', 1) = (r_1, r_2, \ldots, r_k, m)$. □

4. Sufficient conditions for half-factoriality

A monoid $\boldsymbol{M} = \boldsymbol{M}(a_1, \ldots, a_n; b)$ is half-factorial if b is sufficiently large compared to the divisors $d_i = \gcd\{a_i, b\}$, $1 \leq i \leq n$. The following theorem makes this idea more precise.

Theorem 4.1. *Let $\boldsymbol{M} = \boldsymbol{M}(a_1, \ldots, a_n; b)$ be a regular monoid with special reduction $\boldsymbol{S} = \boldsymbol{S}(d_1, \ldots, d_k; b)$. $\boldsymbol{M}$ is half-factorial if*

$$(*) \quad \max \left\{ d_{k-1} \sum_{i=2}^{k} d_i, d_k \sum_{i=1}^{k-1} d_i \right\} < b + \sum_{i=1}^{k} d_i.$$

The following two lemmata serve as main tools for the proof of the theorem. We fix a special monoid $\boldsymbol{S} = \boldsymbol{S}(d_1, \ldots, d_k; b)$ and assume that $k \geq 3$ and that $d_1 > 1$ if $k = 3$ (cf. Elementary Facts (2) and (4) in Section 3). Moreover, we fix an element $(r_1, \ldots, r_k, m) \in \boldsymbol{S}$ with $m \geq 2$.

Lemma 4.2. *If condition* $(*)$ *of Theorem* 4.1 *is true, then*

$$i_0 := \max\{i \in \{2, \ldots, k\} | r_i \geq d_{k-1}\},$$

$$i_1 := \max\{i \in \{1, \ldots, i_0 - 1\} | r_i \geq d_{i_0}\}$$

exist.

Proof. Since

$$\begin{aligned} r_1 d_1 + (d_{k-1} - 1) \sum_{i=2}^{k} d_i &\leq \left(\frac{b}{d_1} - 1\right) d_1 + (d_{k-1} - 1) \sum_{i=2}^{k} d_i \\ &= b + d_{k-1} \sum_{i=2}^{k} d_i - \sum_{i=1}^{k} d_i < 2b \leq mb, \end{aligned}$$

it follows that i_0 exists. For $i_0 \leq k - 1$ we get

$$\begin{aligned} &(d_{i_0} - 1) \sum_{i=1}^{i_0 - 1} d_i + r_{i_0} d_{i_0} + (d_{k-1} - 1) \sum_{i=i_0+1}^{k} d_i \\ &\quad \leq (d_{k-1} - 1) \sum_{\substack{i=1 \\ i \neq i_0}}^{k} d_i + \left(\frac{b}{d_{i_0}} - 1\right) d_{i_0} \\ &\quad \leq (d_{k-1} - 1) \sum_{i=2}^{k} d_i + b - d_{i_0} \leq d_{k-1} \sum_{i=2}^{k} d_i - \sum_{i=1}^{k} d_i + b < mb \end{aligned}$$

and for $i_0 = k$,

$$\begin{aligned} (d_k - 1) \sum_{i=1}^{k-1} d_i + r_k d_k &\leq (d_k - 1) \sum_{i=1}^{k-1} d_i + \left(\frac{b}{d_k} - 1\right) d_k \\ &= d_k \sum_{i=1}^{k-1} d_i - \sum_{i=1}^{k} d_i + b < mb. \end{aligned}$$

Therefore i_1 also exists. □

We define $q := \gcd(d_{i_0}, d_{i_1}) \in \mathbb{N}$ and $\gamma_i, \delta_i \in \mathbb{N}$ with $r_i = \gamma_i q + \delta_i$, $0 \leq \delta_i < q$, $1 \leq i \leq k$.

Lemma 4.3. *The following inequalities hold if* $(*)$ *is true.*

(α) *If* $i_0 \geq 3$, *then* $d_{k-1}d_{i_0} + \sum_{i=i_0+1}^{k} r_i d_i < b$.

(β) *If* $i_0 = 2$, *then* $(d_{k-1} - 2)d_2 + \sum_{i=3}^{k} r_i d_i < b$.

(γ) $(\frac{d_{i_0}}{q} - 1)d_{i_1} + \sum_{i=1}^{k} \delta_i d_i < (m-1)b + \delta_{i_1} d_{i_1} + \delta_{i_0} d_{i_0}$.

Proof. (α) We assume at first that $k = i_0 \geq 3$. Then

$$d_{k-1}d_k + d_k \sum_{i=1}^{k-2} d_i = d_k \sum_{i=1}^{k-1} d_i < b + \sum_{i=1}^{k} d_i$$

and

$$d_{k-1}d_k < b + (1 - d_k) \sum_{i=1}^{k-2} d_i + d_{k-1} + d_k.$$

We have to show that

$$(d_k - 1) \sum_{i=1}^{k-2} d_i \geq d_{k-1} + d_k.$$

If $k \geq 4$ or $d_1 \geq 3$ then $\sum_{i=1}^{k-2} d_i \geq 3$ and

$$(d_k - 1) \sum_{i=1}^{k-2} d_i \geq 3(d_k - 1) = 2d_k - 1 + (d_k - 2) \geq 2d_k - 1$$
$$= (d_k - 1) + d_k \geq d_{k-1} + d_k.$$

If $k = 3$ and $d_1 = 2$ we know by $(*)$ that

$$d_2 d_3 + d_2^2 < b + d_1 + d_2 + d_3 = b + 2 + d_2 + d_3,$$
$$d_2 d_3 + 2d_3 < b + d_1 + d_2 + d_3 = b + 2 + d_2 + d_3.$$

We need to show that $d_2^2 \geq 2 + d_2 + d_3$ or $d_3 \geq 2 + d_2$. Assume that $d_3 = 1 + d_2$. Note that $d_2 \geq 3$. Therefore

$$4 \leq (d_2 - 1)^2 = d_2^2 - 2d_2 + 1.$$

In particular, $d_2^2 \geq 2d_2 + 3 = 2 + d_2 + (d_2 + 1) = 2 + d_2 + d_3$ as desired. This proves (α) in the case that $i_0 = k$.

Now we assume that $k - 1 \geq i_0 \geq 3$. We get

$$d_{k-1}d_{i_0} + \sum_{i=i_0+1}^{k} r_i d_i \leq d_{k-1}d_{i_0} + (d_{k-1} - 1) \sum_{i=i_0+1}^{k} d_i$$
$$= d_{k-1} \sum_{i=i_0}^{k} d_i - \sum_{i=i_0+1}^{k} d_i,$$

and hence

$$d_{k-1}d_{i_0} + \sum_{i=i_0+1}^{k} r_i d_i < b + \sum_{i=1}^{k} d_i - \sum_{i=2}^{i_0-1} d_i d_{k-1} - \sum_{i=i_0+1}^{k} d_i$$
$$= b + \sum_{i=1}^{i_0} d_i - d_{k-1} \sum_{i=2}^{i_0-1} d_i.$$

It suffices to show that

$$(d_{k-1} - 1) \sum_{i=2}^{i_0-1} d_i \geq d_1 + d_{i_0}.$$

We have

$$(d_{k-1} - 1) \sum_{i=2}^{i_0-1} d_i \geq (d_{k-1} - 1) d_2 \geq 2(d_{k-1} - 1)$$

and

$$2(d_{k-1} - 1) \geq d_1 + d_{k-1} \geq d_1 + d_{i_0}$$

since $d_{k-1} \geq d_3 \geq 2 + d_1$. The proof of (α) is finished.

(β) Assume that $i_0 = 2$. We have

$$(d_{k-1} - 2)d_2 + \sum_{i=3}^{k} r_i d_i \leq (d_{k-1} - 2)d_2 + (d_{k-1} - 1) \sum_{i=3}^{k} d_i$$
$$= d_{k-1} \sum_{i=2}^{k} d_i - d_2 - \sum_{i=2}^{k} d_i < b + \sum_{i=1}^{k} d_i - d_2 - \sum_{i=2}^{k} d_i$$
$$= b + d_1 - d_2 < b.$$

(γ) We have

$$\left(\frac{d_{i_0}}{q} - 1\right) d_{i_1} + \sum_{i=1}^{k} \delta_i d_i$$
$$\leq \left(\frac{d_{i_0}}{q} - 1\right) d_{i_1} + (q-1) \sum_{\substack{i=1 \\ i \neq i_0, i \neq i_1}}^{k} d_i + \delta_{i_1} d_{i_1} + \delta_{i_0} d_{i_0}.$$

Hence, it suffices to show that

$$\left(\frac{d_{i_0}}{q} - 1\right) d_{i_1} + (q-1) \sum_{\substack{i=1 \\ i \neq i_0, i \neq i_1}}^{k} d_i < (m-1)b.$$

This is true for $q = 1$ since

$$(d_{i_0} - 1)d_{i_1} < r_{i_1} d_{i_1} < b \leq (m-1)b.$$

Assume now that $q \geq 2$. Then

$$\left(\frac{d_{i_0}}{q} - 1\right) d_{i_1} + (q-1) \sum_{\substack{i=1 \\ i \neq i_0, i \neq i_1}}^{k} d_i \leq \left(\frac{d_{i_0}}{2} - 1\right) d_{i_1} + (d_{i_1} - 1) \sum_{\substack{i=1 \\ i \neq i_0, i \neq i_1}}^{k} d_i$$

$$= d_{i_1} \sum_{\substack{i=1 \\ i \neq i_0, i \neq i_1}}^{k} d_i - \frac{d_{i_1} d_{i_0}}{2} - \sum_{\substack{i=1 \\ i \neq i_0}}^{k} d_i \leq d_{k-1} \sum_{i=2}^{k} d_i - \sum_{\substack{i=1 \\ i \neq i_0}}^{k} d_i - \frac{d_{i_1} d_{i_0}}{2}$$

$$< b + \sum_{i=1}^{k} d_i - \sum_{\substack{i=1 \\ i \neq i_0}}^{k} d_i - \frac{d_{i_1} d_{i_0}}{2} = b + d_{i_0} - \frac{d_{i_1} d_{i_0}}{2}$$

$$= b + d_{i_0}\left(1 - \frac{d_{i_1}}{2}\right) \leq b \leq (m-1)b,$$

since $d_{i_1} \geq q \geq 2$. □

Proof of Theorem 4.1. Assume that $\boldsymbol{S} = \boldsymbol{S}(d_1, \ldots, d_k; b)$ is not half-factorial and that $(r_1, \ldots, r_k, m) \in \boldsymbol{S}$ is irreducible with $m \geq 2$. We know already that this implies $k \geq 3$ and $d_1 > 1$ if $k = 3$. Our assumption will lead to a contradiction. Let $i_0, i_1, q, \gamma_i, \delta_i$ be defined as above. We distinguish the cases $i_0 \geq 3$ and $i_0 = 2$.

(a) $i_0 \geq 3$: By statement (α) of Lemma 4.3 we have

$$(m-1)b = mb - b < mb - \left(d_{k-1} d_{i_0} + \sum_{i=i_0+1}^{k} r_i d_i\right)$$

$$= \sum_{i=1}^{k} r_i d_i - \left(d_{k-1} d_{i_0} + \sum_{i=i_0+1}^{k} r_i d_i\right)$$

$$= r_{i_1} d_{i_1} + (r_{i_0} - d_{k-1}) d_{i_0} + \sum_{\substack{i=1 \\ i \neq i_1}}^{i_0-1} r_i d_i$$

$$= r_{i_1} d_{i_1} + (r_{i_0} - d_{k-1}) d_{i_0} + \sum_{\substack{i=1 \\ i \neq i_1}}^{i_0-1} (\gamma_i q + \delta_i) d_i$$

$$\leq r_{i_1} d_{i_1} + (r_{i_0} - d_{k-1}) d_{i_0} + q \sum_{\substack{i=1 \\ i \neq i_1}}^{i_0-1} (\gamma_i q + \delta_i) d_i + \sum_{i=i_0+1}^{k} \delta_i d_i$$

$$= r_{i_1} d_{i_1} + (r_{i_0} - d_{k-1}) d_{i_0} + q \sum_{\substack{i=1 \\ i \neq i_1}}^{i_0-1} \gamma_i d_i + \sum_{\substack{i=1 \\ i \neq i_0, i \neq i_1}}^{k} \delta_i d_i = x$$

and by statement (γ) of Lemma 4.3:

$$x > (m-1)b > \left(\frac{d_{i_0}}{q} - 1\right) d_{i_1} + \sum_{\substack{i=1 \\ i\neq i_0, i\neq i_1}}^{k} \delta_i d_i.$$

Remember that $r_{i_1} > d_{i_0}/q - 1$ and that $r_{i_0} - d_{k-1} \geq 0$. The two inequalities show that we can find

$$r'_{i_1} \in \mathbb{N}, \quad r_{i_1} \geq r'_{i_1} \geq \frac{d_{i_0}}{q} - 1, \quad r'_{i_0} \in \mathbb{N}, \ r'_{i_0} \leq r_{i_0} - d_{k-1},$$
$$\gamma'_i \in \mathbb{N}, \quad \gamma'_i \leq \gamma_i, \quad 1 \leq i \leq i_0 - 1, \ i \neq i_1$$

such that

$$(m-1)b \geq y := r'_{i_1} d_{i_1} + r'_{i_0} d_{i_0} + q \sum_{\substack{i=1 \\ i\neq i_1}}^{i_0-1} \gamma'_i d_i + \sum_{\substack{i=1 \\ i\neq i_0, i\neq i_1}}^{k} \delta_i d_i > (m-1)b - q d_{i_0}.$$

Since q divides d_{i_1} and d_{i_0} it follows that q divides

$$\sum_{\substack{i=1 \\ i\neq i_0, i\neq i_1}}^{k} \delta_i d_i = mb - r_{i_0} d_{i_0} - r_{i_1} d_{i_1} - q \sum_{\substack{i=1 \\ i\neq i_0, i\neq i_1}}^{k} \gamma_i d_i.$$

In particular, q divides x, y and $\alpha := (m-1)b - y < q d_{i_0}$. Note that $\alpha > 0$ since $\alpha = 0$ would contradict our assumption that $(r_1, \ldots, r_k, m)$ is irreducible.

There are $s, t \in \mathbb{N}$, $0 \leq t \leq d_{i_0}/q - 1$ with $\alpha = s d_{i_0} - t d_{i_1}$. In particular,

$$(r'_{i_1} - t) d_{i_1} + (r'_{i_0} + s) d_{i_0} + \sum_{\substack{i=1 \\ i\neq i_1}}^{i_0-1} (\gamma'_i q + \delta_i) d_i + \sum_{i=i_0+1}^{k} \delta_i d_i = (m-1)b.$$

It remains to show that $r'_{i_1} - t \geq 0$ and $r'_{i_0} + s \leq r_{i_0}$. Whereas the first inequality is trivial, we will verify the second inequality. From

$$q d_{i_0} > \alpha = s d_{i_0} - t d_{i_1} \geq s d_{i_0} - \left(\frac{d_{i_0}}{q} - 1\right) d_{i_1} = d_{i_0} \left(s - \frac{d_{i_1}}{q}\right) + d_{i_1},$$

we have

$$s - \frac{d_{i_1}}{q} + \frac{d_{i_1}}{d_{i_0}} < q \quad \text{or} \quad s < q + \frac{d_{i_1}}{q} - \frac{d_{i_1}}{d_{i_0}}.$$

Since $s \in \mathbb{N}$ and $d_{i_1}/q \in \mathbb{N}$ it follows that

$$s \leq q + \frac{d_{i_1}}{q} - 1.$$

Then

$$r'_{i_0} + s \leq r_{i_0} - d_{k-1} + q - 1 + \frac{d_{i_1}}{q}$$

and, since $d_{i_1} \leq d_{k-1}$, it suffices to show that

$$d_{i_1} + 1 \geq q + \frac{d_{i_1}}{q}.$$

But this is equivalent to

$$d_{i_1}\left(1-\frac{1}{q}\right)\geq q-1.$$

Division by q leads to

$$\frac{d_{i_1}}{q}\left(1-\frac{1}{q}\right)\geq 1-\frac{1}{q}.$$

This is true for $q=1$. If $q\geq 2$, this is equivalent to $d_{i_1}/q\geq 1$, which is true because $d_{i_1}/q\in\mathbb{N}^+$. This finishes the proof for $i_0\geq 3$.

(b) $i_0=2$: Using Lemma 4.3, statement (β), we get in the same manner as above that

$$\begin{aligned} &r_1d_1+(r_2+2-d_{k-1})d_2+\sum_{i=3}^{k}\delta_i d_i>(m-1)b\\ &\left(\frac{d_2}{q}-1\right)d_1+\sum_{i=3}^{k}\delta_i d_i<(m-1)b. \end{aligned}\tag{$**$}$$

There are $r_1',r_2'\in\mathbb{N}$ with $r_1\geq r_1'\geq \frac{d_2}{q}-1$, $r_2'\leq r_2+2-d_{k-1}$, such that

$$r_1'd_1+r_2'd_2+\sum_{i=3}^{k}\delta_i d_i=(m-1)b-\alpha,$$

where $0<\alpha<d_2$ and $q|\alpha$. Let $s,t\in\mathbb{N}$, $0\leq t\leq d_2/q-1$, with $\alpha=sd_2-td_1$. As above, it remains to show that

$$r_2'+s\leq r_2.$$

An easy calculation yields $s\leq d_1/q$. Then

$$r_2'+s\leq r_2+2-d_{k-1}+\frac{d_1}{q}$$

and it suffices to show that

$$d_{k-1}\geq\frac{d_1}{q}+2$$

or

$$d_{k-1}-1\geq\frac{d_1}{q}+1.$$

If $d_{k-1}\geq 2+d_1$ (e.g., if $k\geq 4$), it follows that

$$d_{k-1}-1\geq d_1+1\geq\frac{d_1}{q}+1.$$

For $k=3$ and $d_{k-1}=d_2=1+d_1\geq 3$ we have $q=1$ and $r_1=r_{i_1}\geq d_{i_0}=d_2=d_1+1>d_1$. The inequalities $(**)$ yield

$$\begin{aligned} &r_1d_1+(r_2+1-d_1)(d_1+1)>b,\\ &d_1^2<b. \end{aligned}$$

In this special case, using the relation $r_1 > d_1$, we can find $r_1', r_2' \in \mathbb{N}$ with

$$2 \le d_1 \le r_1' < r_1$$

and $r_2' \le r_2 + 1 - d_1 \le r_2$, such that

$$b > y := r_1' d_1 + r_2'(d_1 + 1) > b - d_1.$$

Again let $s, t \in \mathbb{N}$, $0 \le t \le d_1$, with $\alpha := b - y = s(d_1 + 1) - td_1 \le d_1 - 1$. Finally it suffices to show that

$$s \le d_1 - 1,$$

since this implies $r_2' + s \le r_2 + 1 - d_1 + s \le r_2$. The inequality

$$d_1 - 1 \ge \alpha = s(d_1 + 1) - td_1 \ge s(d_1 + 1) - d_1^2$$

yields

$$s \le \frac{d_1^2 + d_1 - 1}{d_1 + 1} = d_1 - \frac{1}{d_1 + 1}.$$

Hence $s \le d_1 - 1$ since $s \in \mathbb{N}$. This completes the proof of the theorem. □

Finally we note the following consequence of Theorem 4.1.

Corollary 4.4. *Let* $\boldsymbol{M} = \boldsymbol{M}(a_1, \ldots, a_n; b)$ *be a regular monoid of length* k. *If* $\gcd\{d_i, d_j\} = 1$ *for* $1 \le i < j \le k$ *or if* $k \le 3$ *then* M *is half-factorial.*

Proof. Assume that $\gcd\{d_i, d_j\} = 1$ for $1 \le i < j \le k$. By elementary facts (2), (3) and (4) of Section 4 we may assume $k \ge 3$, $d_1 \ge 2$ if $k = 3$, and

$$b = \prod_{i=1}^{k} d_i.$$

It suffices to show that

$$(\alpha) \quad d_{k-1} \sum_{i=2}^{k} d_i \le \prod_{i=1}^{k} d_i,$$

$$(\beta) \quad d_k \sum_{i=1}^{k-1} d_i \le \prod_{i=1}^{k} d_i.$$

For (α),

(i) $k \ge 5$:

$$d_2 + \cdots + d_k \le (k-1)d_k \le (k-2)(k-3)d_k \le d_{k-2}d_{k-3}d_k,$$

(ii) $k = 4$:

$$d_2 + d_3 + d_4 \leq 3d_4 \leq d_2 d_4 \text{ if } d_2 \geq 3.$$

For $d_2 = 2$ we have $d_4 \geq 2 + d_3$ since $\gcd(d_4, 2) = \gcd(d_3, 2) = 1$ and therefore

$$d_2 + d_3 + d_4 = (2 + d_3) + d_4 \leq 2d_4 = d_2 d_4.$$

(iii) $k = 3, d_1 \geq 2$:

$$d_2 + d_3 \leq 2d_3 \leq d_1 d_3.$$

For (β),

(i) $k \geq 5$:

$$d_1 + \cdots + d_{k-1} \leq (k-1)d_{k-1} \leq (k-3)(k-2)d_{k-1} \leq d_{k-3}d_{k-2}d_{k-1}.$$

(ii) $k = 4$:

$$d_1 + d_2 + d_3 \leq 3d_3 \leq d_2 d_3 \text{ if } d_2 \geq 3.$$

If $d_2 = 2$, then $d_1 + d_2 + d_3 = 3 + d_3 \leq d_3 + d_3 = 2d_3 = d_2 d_3$.

(iii) $k = 3, d_1 \geq 2$:

$$d_1 + d_2 \leq 2d_2 \leq d_1 d_2.$$

This completes the proof of the first statement.

Assume that $k = 3$. By Elementary Fact (5) of Section 3, we may assume that $\gcd(d_i, d_j) = 1$ for $1 \leq i < j \leq 3$. Then the first statement of the corollary applies. □

References

[1] D.D. Anderson, S. Chapman, F. Halter-Koch, M. Zafrullah, Criteria for unique factorization in integral domains, J. Pure Applied Algebra 127 (1998), 205–218.
[2] D.F. Anderson, S.T. Chapman, W.W. Smith, Some factorization properties of Krull domains with infinite cyclic divisor class group, J. Pure Appl. Algebra 96 (1994) 97–112.
[3] D.F. Anderson, S.T. Chapman, W.W. Smith, On Krull half-factorial domains with infinite cyclic divisor class group, Houston J. Math. 20 (1994) 561–570.
[4] L. Carlitz, A characterization of algebraic number fields with class number two, Proc. Amer. Math. Soc. 11 (1960) 391–392.
[5] S.T. Chapman, A. Geroldinger, Krull domains and monoids, their sets of lengths and associated combinatorial problems, Lecture Notes in Pure and Applied Mathematics, vol. 189, chapter 3, Marcel Dekker, New York, 1997, pp. 73–112.
[6] S.T. Chapman, W.W. Smith, Factorization in Dedekind domains with finite class group, Israel J. Math 71 (1990) 65–95.
[7] S.T. Chapman, W.W. Smith, On the HFD, CHFD and k-HFD properties in Dedekind domains, Commun. Algebra 20 (1992) 1955–1987.
[8] A.H. Clifford, G.B. Preston, The Algebraic Theory of Semigroups, vol. II, Amer. Math. Soc., Providence, RI, 1967.
[9] A. Geroldinger, Über nicht-eindeutige Zerlegungen in irreduzible Elemente, Math. Z. 197 (1988) 505–529.
[10] A. Geroldinger, Systeme von Längenmengen, Abh. Math. Sem. Univ. Hamburg 60 (1990) 115–130.
[11] J.H. Grace, A. Young, The Algebra of Invariants, Cambridge University Press, Cambridge, 1903

[12] F. Halter-Koch, Halbgruppen mit Divisorentheorie, Expo. Math. 8 (1990) 27–66.
[13] F. Halter-Koch, Ideal Systems, An Introduction to Multiplicative Ideal Theory, Marcel Dekker, New York, 1998.
[14] U. Krause, On monoids of finite real character, Proc. Amer. Math. Soc. 105 (1989) 546–554.
[15] U. Krause, C. Zahlten, Arithmetic in Krull monoids and the cross number of divisor class groups, Mitt. Math. Ges. Hamburg 12 (1991) 681–696.
[16] L. Skula, Divisorentheorie einer Halbgruppe, Math. Z. 114 (1970) 113–120.
[17] R. Stanley, Combinatorics and Commutative Algebra, Birkhäuser, Boston, 1983.