ON DELTA SETS AND THEIR REALIZABLE SUBSETS IN KRULL MONOIDS WITH CYCLIC CLASS GROUPS

SCOTT T. CHAPMAN*, FELIX GOTTI*, AND ROBERTO PELAYO*

ABSTRACT. Let \( M \) be a commutative cancellative monoid. The set \( \Delta(M) \), which consists of all positive integers which are distances between consecutive irreducible factorization lengths of elements in \( M \), is a widely studied object in the theory of nonunique factorizations. If \( M \) is a Krull monoid with divisor class group \( \mathbb{Z}_n \), then it is well-known that \( \Delta(M) \subseteq \{1, 2, \ldots, n-2\} \). Moreover, equality holds for this containment when each divisor class of \( \mathbb{Z}_n \) contains a prime divisor from \( M \). In this note, we consider the question of determining which subsets of \( \{1, 2, \ldots, n-2\} \) occur as the delta set of an individual element from \( M \). We first prove for \( x \in M \) that if \( n-2 \in \Delta(x) \), then \( \Delta(x) = \{n-2\} \) (i.e., not all subsets of \( \{1, 2, \ldots, n-2\} \) can be realized as delta sets of individual elements). We close by proving an Archimedean-type property for delta sets from Krull monoids with cyclic divisor class group: for every natural number \( m \), there exist a natural number \( n \) and Krull monoid \( M \) with divisor class group \( \mathbb{Z}_n \) such that \( M \) has an element \( x \) with \(|\Delta(x)| \geq m\).

1. Introduction

The arithmetic of Krull monoids is a well-studied area in the theory of nonunique factorizations. The interested reader can find a good summary of their known arithmetic properties in the monograph [12, Chapter 6]. We focus here on Theorem 6.7.1 of [12], where the authors show that

\[ \Delta(M) = \{1, 2, \ldots, n-2\} \]

for \( M \) a Krull monoid with divisor class group \( \mathbb{Z}_n \) where each divisor class of \( \mathbb{Z}_n \) contains a prime divisor of \( M \). Here \( \Delta(M) \) represents the set of all positive integers which are distances between consecutive irreducible factorization lengths of elements in \( M \). We ask in this note a question related to the above equality that is seemingly unasked in the literature. Which subsets \( T \subseteq \{1, 2, \ldots, n-2\} \) are realized as the delta set of an individual element in \( M \) (i.e., for which \( T \) does there exist an \( x \in M \) such that \( T = \Delta(x) \))? Based on the structure theorem for sets of lengths in Krull monoids with finite divisor class group (see [12, Chapter 4]), it is reasonable to assume that not all subsets of \( \{1, 2, \ldots, n-2\} \) will be realized. We verify this in Theorem 3.3 by showing for \( x \in M \) that if \( n-2 \in \Delta(x) \), then \( \Delta(x) = \{n-2\} \). We constrast this in Theorem 3.6 by showing that we can construct delta sets of arbitrarily large size (i.e., for any \( m \in \mathbb{N} \) there exist a natural number \( n \) and Krull monoid \( M \) with divisor class group \( \mathbb{Z}_n \) such that \( M \) has an element \( x \) with \(|\Delta(x)| \geq m\)).
2. Definitions and Background

We open with some basic definitions from the theory of nonunique factorizations. For a commutative cancellative monoid $M$, let $\mathcal{A}(M)$ represent the irreducible elements of $M$ and $M^\times$ its set of units. We provide here an informal description of factorizations and associated notions. From a more formal point of view, factorizations can be considered as elements in the factorization monoid which is defined as the free abelian monoid with basis $M$. Two irreducible factorizations are equivalent if there is a permutation of atoms carrying one factorization to the other. We denote by $Z(x)$ the set of all irreducible factorizations of $x$. If $z \in Z(x)$, then let $|z|$ denote the number of atoms in the factorization $z$ of $x$. We call $|z|$ the length of $z$. Now, let $x \in M \setminus M^\times$ with irreducible factorizations

$$z = \alpha_1 \cdots \alpha_l \beta_1 \cdots \beta_s$$

and

$$z' = \alpha_1 \cdots \alpha_l \gamma_1 \cdots \gamma_u$$

where for each $1 \leq i \leq s$ and $1 \leq j \leq u$, $\beta_i \neq \gamma_j$. Define

$$\gcd(z, z') = \alpha_1 \cdots \alpha_l$$

and

$$d(z, z') = \max\{s, u\}$$

to be the distance between $z$ and $z'$. The basic properties of this distance function can be found in [12, Proposition 1.2.5]. An $N$-chain of factorizations from $z$ to $z'$ is a sequence $z_0, \ldots, z_k$ such that each $z_i$ is a factorization of $z$, $z_0 = z$, $z_k = z'$, and $d(z_i, z_{i+1}) \leq N$ for all $i$. The catenary degree of $x$, denoted $c(x)$, is the minimal $N \in \mathbb{N} \cup \{\infty\}$ such that for any two factorizations $z, z'$ of $x$, there is an $N$-chain from $z$ to $z'$. The catenary degree of $M$, denoted by $c(M)$, is defined by

$$c(M) = \sup\{c(x) \mid x \in M \setminus M^\times\}.$$  

A review of the known facts concerning the catenary degree can be found in [12, Chapter 3]. An algorithm which computes the catenary degree of a finitely generated monoid can be found in [5] and a more specific version for numerical monoids in [6].

We shift from considering particular factorizations to analyzing their lengths. For $x \in M \setminus M^\times$, we define

$$\mathcal{L}(x) = \{n \mid \text{there are } \alpha_1, \ldots, \alpha_n \in \mathcal{A}(M) \text{ with } x = \alpha_1 \cdots \alpha_n\}.$$  

We refer to $\mathcal{L}(x)$ as the set of lengths of $x$ in $M$. Further, set

$$\mathcal{L}(M) = \{\mathcal{L}(x) : x \in M \setminus M^\times\},$$  

which we refer to as the set of lengths of $M$. The interested reader can find many recent advances concerning sets of lengths in [10], [14], and [15]. Given $x \in M \setminus M^\times$, write its length set in the form

$$\mathcal{L}(x) = \{n_1, n_2, \ldots, n_k\}$$  

where $n_i < n_{i+1}$ for $1 \leq i \leq k - 1$. The delta set of $x$ is defined by $\Delta(x) = \{n_i - n_{i-1} \mid 2 \leq i \leq k\}$ and the delta set of $M$ by

$$\Delta(M) = \bigcup_{x \in M \setminus M^\times} \Delta(x).$$
REALIZABLE SUBSETS IN $\Delta(B(Z_n))$ 3

A monoid $M$ is called a Krull monoid if there is an injective monoid homomorphism $\varphi : M \to D$ where $D$ is a free abelian monoid and $\varphi$ satisfies the following two conditions:

1. if $a, b \in M$ and $\varphi(a) | \varphi(b)$ in $D$, then $a | b$ in $M$,
2. for every $\alpha \in D$ there exists $a_1, \ldots, a_n \in M$ with $\alpha = \gcd{\varphi(a_1), \ldots, \varphi(a_n)}$.

The basis elements of $D$ are called the prime divisors of $M$. The above properties guarantee that $\text{Cl}(M) = D/\varphi(M)$ is an abelian group, which we call the divisor class group of $M$ (see [12, Section 2.3]). Note that since any Krull monoid is isomorphic to a submonoid of a free abelian monoid, a Krull monoid is commutative, cancellative, and atomic. The class of Krull monoids contains many well-studied types of monoids, such as the multiplicative monoid of a ring of algebraic integers (see [1]).

Let $G$ be an abelian group and $\mathcal{F}(G)$ the free abelian monoid on $G$. The elements of $\mathcal{F}(G)$, which we write in the form $X = g_1 \cdots g_l = \prod_{g \in G} g^{v_g(X)}$, are called sequences over $G$. The exponent $v_g(X)$ is the multiplicity of $g$ in $X$. The length of $X$ is defined as $|X| = l = \sum_{g \in G} v_g(X)$ (note that as $\mathcal{F}(G)$ and $Z(x)$ are both free abelian monoids, there is really no redundancy in this notation). For every $I \subset [1, l]$, the sequence $Y = \prod_{i \in I} g_i$ is called a subsequence of $X$. The subsequences are precisely the divisors of $X$ in the free abelian monoid $\mathcal{F}(G)$. The submonoid

$$B(G) = \{ \prod_{g \in G} g^{v_g} \in \mathcal{F}(G) \mid \sum_{g \in G} v_g g = 0 \}$$

is known as the block monoid on $G$ and its elements are referred to as zero-sum sequences or blocks over $G$ ([12, Section 2.5] is a good general reference on block monoids). If $S$ is a subset of $G$, then the submonoid

$$B(G, S) = \{ \prod_{g \in G} g^{v_g} \in B(G) \mid v_g = 0 \text{ if } g \notin S \}$$

of $B(G)$ is called the restriction of $B(G)$ to $S$. Block monoids are important examples of Krull monoids and their true relevance in the theory of nonunique factorizations lies in the following result.

**Proposition 2.1.** [12, Theorem 3.4.10.3] Let $M$ be a Krull monoid with divisor class group $G$ and set $S$ of divisor classes of $G$ which contain prime divisors. Then

$$\mathcal{L}(M) = \mathcal{L}(B(G, S)).$$

Hence, to understand the arithmetic of lengths of irreducible factorizations in a Krull monoid, one merely needs to understand the factorization theory of block monoids. Thus, while we state our results in the context of general Krull monoids, Proposition 2.1 allows us to write the proofs using block monoids.

For our purposes, there are two arithmetic properties of the block monoid $B(Z_n)$ which we will later use:

1. $c(B(Z_n)) = n$ [12, Theorem 6.4.7],
Example 2.3. We illustrate some aspects of the last definition with several examples.

(1) Let $M$ be any Krull monoid $M$ with $\Delta(M) = \{c\}$ for $c \in \mathbb{N}$. Clearly any element $x \in M$ with $| \mathcal{L}(x) | > 1$ yields $\Delta(x) = \{c\}$ and hence every subset of $\Delta(M)$ is realizable. A large class of Dedekind domains (whose multiplicative monoids are Krull) with such delta sets are constructed in [8]. Another example of such a monoid, is a primitive numerical monoid whose minimal generating set forms an arithmetic sequence (see [3, Theorem 3.9]).

(2) Let $G$ be any infinite abelian group and $S$ any finite nonempty subset of $\{2, 3, 4, \ldots\}$. By a well-known theorem of Kainrath [13], there is a block $B \in \mathcal{B}(G)$ with $\mathcal{L}(B) = S$. From this, it easily follows that $\Delta(B(G)) = \mathbb{N}$. Moreover, it also easily follows that any finite subset $T$ of $\mathbb{N}$ is realizable in $\Delta(B(G))$.

(3) In general, there are commutative cancellative monoids $M$ with unrealizable subsets of $\Delta(M)$. For our initial example, we again appeal to numerical monoids. Let $S$ be the monoid of positive integers under addition generated by 4, 6, and 15 (i.e., $S = \langle 4, 6, 15 \rangle$). By [3, Example 2.5], $\Delta(S) = \{1, 2, 3\}$. By [7, Theorem 1], the sequence of sets $\{\Delta(n)\}_{n \in S}$ is eventually periodic, and hence using the periodic bound in that Theorem allows one to check for all realizable subsets of $\{1, 2, 3\}$ in finite time. Using programming from the GAP numericalsgps package [9], one can verify that $\{1\}, \{1, 2\}$, and $\{1, 3\}$ are the only realizable subsets of $\Delta(S)$.

(4) There are three generated numerical monoids that behave differently from the two types discussed above. For instance, let $S$ be the numerical monoid generated by 7, 10, and 12 (i.e., $S = \langle 7, 10, 12 \rangle$). By [3, Example 2.5], $\Delta(S) = \{1, 2\}$. Again, using the GAP programming [9], we have that $\Delta(34) = \{1\}$, $\Delta(42) = \{2\}$, and $\Delta(56) = \{1, 2\}$. Thus, all nonempty subsets of $\Delta(S)$ are realizable.

(5) By [11, Corollary 2.3.5], for each $1 \leq i \leq n - 2$, the set $\{i\}$ is realizable in $\Delta(B(\mathbb{Z}_n))$.

(6) Suppose $G$ is an abelian group and $S_1 \subseteq S_2$ subsets of $G$. By the properties of the block monoid, if $B \in \mathcal{B}(G, S_1)$, then $\mathcal{L}(B)$ is equal in both $\mathcal{B}(G, S_1)$ and $\mathcal{B}(G, S_2)$. Thus, if $T$ is realizable in $\Delta(B(G, S_1))$, then $T$ is realizable in $\Delta(B(G, S_2))$. Elementary examples show that this relationship does not work conversely.

Our eventual goal is to show that in contrast to $\mathcal{B}(G)$ where $G$ is infinite abelian, not all subsets of $\Delta(B(\mathbb{Z}_n))$ are realizable.

3. Main Results

Now we state three number theory results that we shall use later in the proof of Lemma 3.2. We leave the proofs to the reader.

Lemma 3.1. Let $a, b$, and $n$ be positive integers.

(1) If $\gcd(n, a) = 1$, then for every integer $x$, the set

$$S = \{x, x + a, x + 2a, \ldots, x + (n - 1)a\}$$

Thus $\Delta(B(\mathbb{Z}_n)) = \{1, 2, \ldots, n - 2\}$. We will be interested in the following types of subsets of $\Delta(M)$.

Definition 2.2. Let $M$ be a commutative cancellative monoid and suppose $T$ is a nonempty subset of $\Delta(M)$. We call $T$ realizable in $\Delta(M)$ if there is an element $x \in M$ with $\Delta(x) = T$.
is a complete set of residues modulo n.

(2) If n is an odd such that n divides \(a + b\) and \(\gcd(n, a) = \gcd(n, b) = 1\), then

\[
S = \{0, a, 2a, \ldots, \frac{n-1}{2}a, b, 2b, \ldots, \frac{n-1}{2}b\}
\]

is a complete set of residues modulo n.

(3) If n is an even such that n divides \(a + b\) and \(\gcd(n, a) = \gcd(n, b) = 1\), then

\[
S = \{0, a, 2a, \ldots, \frac{n}{2}a, b, 2b, \ldots, \frac{n}{2}b\}
\]

is a complete set of residues modulo n.

Our next lemma will be vital in the proof of Theorem 3.3.

Lemma 3.2. Let \(u \in \mathcal{B}(\mathbb{Z}_n)\) where \(n > 2\), \(a \in \mathbb{N}\), and \(z, z' \in \mathcal{Z}(u)\) such that \(\gcd(n, a) = 1\) and

\[
z = ([a]^n)^r([−a]^n)^sB([a][−a])^q
\]

where \(r, s > 0\) and \(B\) is the product of atoms which are not in the set \([a]^n, [−a]^n, [a][−a]\).

If \(|z'|−|z|= n − 2\) and there are no irreducible factorizations of \(u\) having length between \(|z|\) and \(|z'|\), then \(B\) is the empty sequence.

Proof. Assume, by way of contradiction, that \(A\) is an atom of \(\mathcal{B}(\mathbb{Z}_n)\) contained in \(B\). Suppose that the sequence \(A\) contains distinct divisors of the form \([x], [y]\), and \([w]\) for \(x, y, w \in \mathbb{Z}_n\). If \(n\) is odd, by the Pigeonhole Principle and Lemma 3.1 (2), two of the three divisors \([−x], [−y]\), and \([−w]\) are in either \(C = \{[a], [a]^2, \ldots, [a]^{\frac{n-1}{2}}\}\) or \(D = \{[b], [b]^2, \ldots, [b]^{\frac{n-1}{2}}\}\). Suppose without loss of generality that \([−x], [−y] \in C\). Let \(1 ≤ e < f ≤ \frac{n-1}{2}\) such that \([−x] = [a]^e\) and \([−y] = [a]^f\). Then \([a]^nA\) contains the atoms \([x][a]^e\) and \([y][a]^f\). Since \(e + f < n\), \([a]^nA\) must contain a third atom. But this is a contradiction because this way of factoring \([a]^nA\) gives an intermediate length between \(|z|\) and \(|z'|\) (note that by [12, Theorem 5.1.10], \(|A| < n\) and hence \(|[a]^nA| < 2n\)). If \(n\) is even we can apply a similar argument using Lemma 3.1 (3) instead of Lemma 3.1 (2) to get the same contradiction.

Suppose now that \(A\) contains at most two divisors of the form \([x]\) and \([y]\) for \(x, y \in \mathbb{Z}_n\). Then we have that \(A = [x]^t\) for \(t \in \mathbb{N}\), \(A = [x][y]\), or \(A \) contains \([x]^2[y]\). We proceed to analyze these cases one at a time.

Case 1. Suppose that \(A = [x]^t\) where \(t\) is a positive integer. If \(n\) is even and \([x] = [\frac{n}{2}]\), then we have that \(t = 2\) and so

\[
[a]^nA[−a]^n = ([a]\frac{n}{2})([a]\frac{n}{2})([−a]\frac{n}{2})([−a]\frac{n}{2})([a][−a])\frac{n}{2}.
\]

The above irreducible factorization of \([a]^nA[−a]^n\) gives a factorization of \(u\) with an intermediate length because \(3 < \frac{n}{2} + 2 < 3 + (n - 2)\) when \(n > 2\). Therefore, let us assume without loss of generality that \([x] \neq \frac{n}{2}\). Take \(k\) such that \(0 ≤ k < n\) and \(n\) divides \(x + ka\). Notice that \(k \notin \{1, n - 1\}\) because \(A\) is different from both \([−a]^n\) and \([a]^n\). Then we have that \(2 ≤ k ≤ n - 2\). Also we can assume without loss of generality that \(k ≤ \frac{n}{2}\), otherwise we can interchange the roles of \(-a\) and \(a\) and choose \(n - k\) instead of \(k\). Note that \([x] \neq \frac{n}{2}\) implies that \(t > 2\). Now we can see that

\[
[a]^nA[−a]^n = ([a]^k[x]^2([a]^{n-k}[x])A'.
\]

where \(1 ≤ |A'| ≤ 2n - 3 - k ≤ 2n - 5\). Therefore, \(A'\) contains at least one atom and can be factored as the product of at most \(n - 3\) atoms. Hence the above irreducible factorization of \([a]^nA[−a]^n\) gives an irreducible factorization of \(u\) of length strictly between \(|z|\) and \(|z'|\).
Case 2. Suppose that $A = [x][y] = [x][-x]$. Then $n$ divides $x + ka$ for some $0 \leq k < n$. Notice $k \neq 0$ because $n$ does not divide $x$. Also notice that if $k \in \{1, n-1\}$, then $A = [-a][a]$; but it contradicts the fact that $A$ is an atom of $B$. Therefore, $2 \leq k < n - 1$. Assume without loss of generality that $k \leq \frac{n}{2}$, otherwise we can interchange the roles of $-a$ and $a$ and choose $n - k$ instead of $k$. Now note that

$$[a]^n A[-a]^n = ([a]^k[x])/([-a]^k[-x])/([a][-a])^{n-k}.$$  

This irreducible factorization of $[a]^n A[-a]^n$ gives an irreducible factorization of $u$ with length strictly in between $|z|$ and $|z'|$ because $2 \leq k \leq \frac{n}{2}$ implies that $n - 2 \geq n - k \geq \frac{n}{2} > 1$ when $n > 2$.

Case 3. Let us assume that $A = [x]^2[y]A'$. By Lemma 3.1 (1), there exists an integer $k$ such that $0 \leq k \leq n - 1$ which satisfies $x + ka \equiv 0 \pmod{n}$. Since $A$ is an atom, we have that $n$ does not divide $x$. Therefore $k \geq 1$. We have also that $x + (n - k)(-a) \equiv 0 \pmod{n}$. Consequently, we can assume without loss of generality that $k \leq \frac{n}{2}$; otherwise we can change the roles of $a$ and $-a$ and take $n - k$ instead of $k$. Since $1 \leq k \leq \frac{n}{2}$ and $n$ divides $x + ka$, the element $[a]^k[x]$ of $B(\mathbb{Z}_n)$ is an atom. Notice now that

$$[a]^n A = ([a]^k[x])^2([a]^{n-2k}[y]A') = ([a]^k[x])^2 A'',$$

where $A'' = [a]^{n-2k}[y]A'$. Since $A''$ contains at least one $[y]$, any irreducible factorization of $A''$ gives an irreducible factorization of $u$ with length greater than $|z|$. Notice that $|A''| \leq 2n - 2k - 2$. If we prove that any irreducible factorization of $A''$ has length strictly less than $n - 2$ we are done (note that we only need one factorization of $A''$ with length less than $n - 2$). We will analyze the two subcases, first when $x \not\equiv -a \pmod{n}$ and then when $x \equiv -a \pmod{n}$.

If $x \not\equiv -a \pmod{n}$, we have that $n$ does not divide $x + a$. Therefore, $k > 1$, and so $|A''| \leq 2n - 6$. This implies that any irreducible factorization of $A''$ has length at most $n - 3$. Hence we have an irreducible factorization of $u$ with length strictly in between $|z|$ and $|z'|$.

On the other hand, if $x \equiv -a \pmod{n}$, we have that $[x] = [-a]$. In this case $A = [-a]^p[y]^q$ where $p \geq 2$. Since $[x] \neq [y]$, we get that $y \not\equiv -a \pmod{n}$. Also $y \neq a \pmod{n}$, otherwise $A$ would not be an atom. Notice that if $q \geq 2$, we are in a situation that is similar to the previous subcase because $y \not\equiv a \pmod{n}$ and $y \not\equiv -a \pmod{n}$. Therefore, we can assume without loss of generality that $q = 1$, and so $A = [-a]^p[y]$. Note that $p < n - 1$, otherwise we would have $[y] = [-a] = [x]$. In this case, we observe that

$$[a]^n A[-a]^n = (-a)^n([a]^{n-p}[y])([-a])^p$$

gives an irreducible factorization of $u$ with length strictly between $|z|$ and $|z'|$. \hfill \Box

Lemma 3.2 leads us to our first main result.

**Theorem 3.3.** Let $n \geq 3$ be a natural number and let $M$ be a Krull monoid with divisor class group $\mathbb{Z}_n$. If $x \in M$ and $n - 2 \in \Delta(x)$, then $\Delta(x) = \{n - 2\}$.

**Proof.** By Proposition 2.1, we need only prove the Theorem for $B(\mathbb{Z}_n, S)$ where $S$ is the set of divisor classes in $\mathbb{Z}_n$ which contain prime divisors. By our comment in Example 2.3 (6), it suffices to prove our theorem for $S = \mathbb{Z}_n$ (i.e., for $B(\mathbb{Z}_n)$).

Let $z, z' \in Z(x)$ such that $|z'| - |z| = n - 2$ and there are no irreducible factorizations of $x$ with length between $|z|$ and $|z'|$. We shall prove that there exists $[a] \in \mathbb{Z}_n$ such that $z$ contains the atoms $[a]^n$ and $[-a]^n$. By a previous observation, we know that the catenary degree of $B(\mathbb{Z}_n)$ is $n$. Therefore, $\kappa(x) \leq n$ and so there exists an $n$-chain $z = z_0, z_1, \ldots, z_k = z'$
of irreducible factorizations of \( x \) from \( z \) to \( z' \). We have also, by [12, Lemma 1.6.2], that 
\[ |z_{i+1} - z_j| \leq d(z, z_{i+1}) - 2 \leq n - 2. \]
Let \( j \) be the least index such that \( |z_{j+1}| > |z| \). Then we have that \( |z_j| = |z| \) and \( |z_{j+1}| = |z'| \) because there are no irreducible factorizations of \( x \) with length between \( |z| \) and \( |z'| \) and also because \( |z_{i+1} - z_j| \leq n - 2 \). It follows that
\[ d(z_j, z_{j+1}) \geq ||z_{j+1} - z_j|| + 2 = n. \]
Therefore, by redefining, if necessary, \( z \) and \( z' \) as \( z_j \) and \( z_{j+1} \) respectively, we can assume that \( d(z, z') = n \).

Let \( d \) be the greatest common divisor of \( z \) and \( z' \), and define \( w \) and \( w' \) such that \( z = dw \) and \( z' = dw' \). Notice that \( \frac{|w'|}{|w|} = \frac{|z'|}{|z|} = n - 2 \). Since \( \max\{|w|, |w'|\} = d(z, z') = n \), we have that \( |w'| = n \) and \( |w| = 2 \). Since \( |z'| = |z| \), it follows that \( |w'| = |w| \). It is well known that \( y \in A(B(Z_n)) \) implies that \( y \leq n \) and \( y = n \) if and only if \( y = [b]^n \) for some \( 1 \leq b < n \) (again by [12, Theorem 5.1.10]). Since \( w \) consists of only two atoms, \( |w| \leq 2n \). So, \( |w'| \) is also less than or equal to \( 2n \). Since \( w' \) contains exactly \( n \) atoms, each atom has to have length \( 2 \). Then \( |w| = 2n \) and so \( w = [a]^n[b]^n \). Since \( w' \) contains an atom of length \( 2 \), we get that \( [b] = [-a] \), and so \( z = [a]^n[-a]^n d \).

Now we write \( z \) as \( ([a]^n)^r([-a]^n)^s B([a][-a])^q \) where \( B \) does not have any atom of the form \( [a]^n \), \( [-a]^n \), or \( [a][-a] \). Now since there are no irreducible factorizations of \( x \) having length between \( z \) and \( z' \), by Lemma 3.2, we get that \( B \) must be empty. Hence \( z = ([a]^n)^r([-a]^n)^s([a][-a])^q \). Note that the only atoms we can generate with the length one divisors \([a]\) and \([-a]\) are the atoms \([a]^n\), \([-a]^n\), and \([a][-a]\). Therefore, any other irreducible factorization \( v \) of \( x \) is of the form \( ([a]^n)^r'([-a]^n)^s'([a][-a])^q' \). Since the set of length \( 1 \) divisors is the same for any two irreducible factorizations of \( x \), we have that
\[
\begin{align*}
nr + q &= nr' + q' \\
ns + q &= ns' + q'.
\end{align*}
\]
From (1) and (2), we can deduce that \( r - r' = s - s' \) and \( q' - q = n(r - r') \). Consequently,
\[ |z| - |v| = (r - r') + (s - s') + (q - q') = (n - 2)(r - r). \]
Notice also that we can get all the lengths between \( |z| \) and \( |v| \) that are multiples of \( n - 2 \) by changing a finite number of times the two atoms \([a]^n\) and \([b]^n\) by \( n \) atoms of the form \([a][-a]\). Therefore, \( L(x) = \{c, +c + (n - 2), \ldots, c + k(n - 2)\} \) for certain natural numbers \( c \) and \( k \). Hence \( \Delta(x) = \{n - 2\} \). □

As an immediate consequence of Theorem 3.3, we have the following result.

**Corollary 3.4.** Let \( M \) be a Krull monoid with divisor class group \( Z_n \). If \( T \) is a nonempty subset of \( \{1, 2, \ldots, n - 2\} \) with \( n - 2 \in T \) but \( T \neq \{n - 2\} \), then \( T \) is not realizable in \( \Delta(M) \).

**Example 3.5.** We use the last two results to determine all the realizable sets of \( \Delta(B(Z_5)) \).
Since \( \Delta(B(Z_5)) = \{1, 2, 3\} \), Theorem 3.3 implies that the only possible realizable sets are \( \{1\}, \{2\}, \{3\}, \) and \( \{1, 2\} \). The singleton sets are guaranteed by Example 2.3 (5). Let \( B = [1]^8[2][4]^5 \). We claim that \( \Delta(B) = \{1, 2\} \). If \( A \) is an atom containing \([2]\) in an irreducible factorization of \( B \), we have that \( A = [2][1]^3 \) or \( A = [2][4]^2 \). Since \( L([1]^5[4]^3) = \{2, 5\} \), we have irreducible factorizations of \( B \) with length 3 and 6 when \( A = [2][1]^3 \). Observe also that having \( A = [2][4]^2 \) determines uniquely the irreducible factorization of \( B \) given by \( z = ([2][4]^2)([1][4]^3([1]^1)) \). Therefore, \( L(B) = \{3, 5, 6\} \) and so \( \Delta(B) = \{1, 2\} \). Hence, \( \{1\}, \{2\}, \{3\}, \) and \( \{1, 2\} \) is the complete set of realizable sets of \( \Delta(B(Z_5)) \).
Our results to this point have produced delta sets in $B(\mathbb{Z}_n)$ of relatively small size. However, we now prove that we can have realizable sets of large size providing we choose an adequate $n$.

**Theorem 3.6.** For every $K \in \mathbb{N}$ there exist a natural number $n$, a Krull monoid $M$ with divisor class group $\mathbb{Z}_n$, and $x \in M$ such that $|\Delta(x)| \geq K$.

**Proof.** Let $m = K + 1$. Choose a natural number $b_1 > 2m$ and define $b_2, \ldots, b_m$ recursively by $b_{i+1} = 2(\sum_{i=1}^{k} b_i) + 2m$ if $k > 0$. Choose a natural number $n$ such that $n > \sigma = \sum_{i=1}^{m} b_i$ and set $M = B(\mathbb{Z}_n)$.

Define

$$S' = \left\{ \sum_{i=1}^{n} b_i : 1 \leq t_1 < t_2 < \cdots < t_a \text{ where } a \leq m \right\}.$$

Take two elements $s, s' \in S'$. If $s > s' = \sum b_i$, then there exists a summand $b_i$ of $s$ that is not a summand of $s'$. Among all such summands, let $b_j$ be the largest. Since $s > s'$, it follows from the definition of $\{b_1, \ldots, b_m\}$ that $j > t_i$ and we have that

$$s - s' \geq b_j - \sum_{i=1}^{j-1} b_i \geq \sum_{i=1}^{j-1} b_i + 2m > 2m.$$

By a symmetric argument, we have that if $s' > s$ then $s' - s > 2m$. Therefore, any two distinct elements in $S'$ differ by at least $2m$.

Now we arrange the elements of $S'$ in increasing order, say $S' = \{s_1, s_2, \ldots, s_r\}$ and define $S_i = [s_i - m, s_i + m]$. Also define $S$ as the union of all the $S_i$.

Consider now the element $x = [1]^{n-\sigma}[b_1][b_2] \cdots [b_m][n-1]^n$ (recall that $\sigma = b_1 + \cdots + b_m < n$). We shall prove that any irreducible factorization $z \in Z(x)$ satisfies $n - |z| \in S$. Then, for any $S_i$, we shall find $z_i \in Z(x)$ such that $n - |z_i| \in S_i$. Finally, we shall use these two pieces of information to find $m$ distinct elements in $\Delta(x)$.

Let $z \in Z(x)$ and $[b_{t_1}], [b_{t_2}], \ldots, [b_{t_u}]$ be the divisors of $x$ having at least one divisor $[1]$ in their respective atoms with regard to the irreducible factorization $z$. Let $[b_{q_1}], [b_{q_2}], \ldots, [b_{q_v}]$ be the rest of the $[b_i]$’s. Since $1 < b_i < n - 1$, any atom containing the divisor $[b_i]$ cannot contain both the length 1 divisors $[1]$ and $[n-1]$ but must contain one of them. It is not hard to see that we can write $z$ as

$$CD([1][n-1])^{n-\sum b_{q_i}}$$

where $D = ([b_{q_1}][n-1]^{b_{q_1}}) \cdots ([b_{q_v}][n-1]^{b_{q_v}})$ and $C$ is comprised of all the atoms containing a divisor $[b_{t_i}]$ for some $t_i$. Since $u + v = m$, $CD$ contains at most $m$ atoms with respect to the irreducible factorization $z$. Therefore, $n - \sum b_{q_i} < |z| \leq n - \sum b_{q_i} + m$, that is

$$\sum b_{q_i} - m \leq n - |z| < \sum b_{q_i}.$$

It follows that $n - |z| \in S$.

Now we shall show that for each $S_i$ there exists $z_i \in Z(x)$ such that $n - |z_i| \in S_i$. Let $\{r_1, r_2, \ldots, r_w\}$, where $1 \leq w \leq m$, be the subset of $\{1, 2, \ldots, m\}$ satisfying $r_1 < r_2 < \cdots < r_w$ and $s_i = \sum b_{r_i} \in S_i$. We can then combine the atoms $[b_{r_1}][n-1]^{b_{r_1}}$ and $n - \sum b_{r_i}$ copies of $[1][n-1]$ to get

$$x = B([b_{r_1}][n-1]^{b_{r_1}}) \cdots ([b_{r_w}][n-1]^{b_{r_w}})([1][n-1])^{n-\sum b_{r_i}}.$$

(3)
Notice that $B$ cannot contain $[n - 1]$ as a length 1 divisor because the $n$ length 1 divisors $[n - 1]$ of $x$ were already used. So any irreducible decomposition of $B$ has at most $m - w$ atoms. Therefore, once we fix an irreducible factorization for $B$ in (3), we get an irreducible factorization $z_i \in Z(x)$ such that $n - |z_i| \in S_i$.

We now construct $K$ distinct elements of $\Delta(x)$. For $1 \leq k \leq m$ there exists a natural number $j_k$ such that $s_{j_k} = b_1 + \cdots + b_k$. Since $b_1 \cdots b_k \geq \sum_{i=1}^{k} b_i$, we have that $s_{j_k+1} = b_{k+1}$. By the result proved in the previous paragraph, we can take two irreducible factorizations of $x$, say $z_1$ and $z_2$, such that $|z_1| \in S_{j_k}$ and $|z_2| \in S_{j_k+1}$. We can choose $z_1$ and $z_2$ such that there is no $z' \in Z(x)$ satisfying $|z_1| < |z'| < |z_2|$. Since $|z_1| \in S_{j_k}$ and $|z_2| \in S_{j_k+1}$, we have that $|z_1| = s_{j_k} + d_1$ and $|z_2| = s_{j_k+1} + d_2$ where $-m \leq d_1, d_2 \leq m$. Since

$$|z_2| - |z_1| = (b_{k+1} + d_2) - \left(\sum_{i=1}^{k} b_i + d_1\right) = \sum_{i=1}^{k} b_i + (2m + d_2 - d_1)$$

and

$$0 \leq 2m + d_2 - d_1 \leq 4m < 2b_1 + 2m \leq b_{k+1}$$

the following is true:

$$\sum_{i=1}^{k} b_i \leq |z_2| - |z_1| < \sum_{i=1}^{k+1} b_i.$$

Since there is no irreducible factorizations for $x$ having length strictly in between $|z_1|$ and $|z_2|$, we have that $|z_2| - |z_1| \in \Delta(x)$. Therefore, for any $1 \leq k \leq m - 1$ there is an element of $d_k \in \Delta(x)$ such that

$$\sum_{i=1}^{k} b_i \leq d_k < \sum_{i=1}^{k+1} b_i.$$

Hence we can conclude that $|\Delta(x)| \geq m - 1 = K$. \hfill \square

The results of this paper suggest that a full classification of the realizable subsets of $\Delta(B(\mathbb{Z}_n))$ is likely an arduous task. However, related questions may be of equal interest. For instance, if $G$ is an abelian group, then set

$$\Lambda(G) = \max\{|\Delta(B)| : B \in B(G)\}.$$

For $n \geq 13$ we have shown that $\Lambda(\mathbb{Z}_n) \leq n - 3$. Finding reasonable lower and upper bounds for $\Lambda(\mathbb{Z}_n)$ would be challenging, as programming this problem, even for small values of $n$, is difficult.

References


Sam Houston State University, Department of Mathematics, Box 2206, Huntsville, TX 77341
E-mail address: scott.chapman@shsu.edu

University of Florida, Department of Mathematics, Gainesville, FL 32611, USA
E-mail address: felixgotti@ufl.edu

University of Hawai‘i at Hilo, Mathematics Department, Hilo, HI 96720
E-mail address: robertop@hawaii.edu