ON MINIMAL DISTANCES IN KRULL MONOIDS WITH INFINITE CLASS GROUP

S. T. CHAPMAN, W. A. SCHMID, AND W. W. SMITH

ABSTRACT. Let H be a Krull monoid with infinite class group such that each divisor class contains a prime divisor. It is shown that for every positive integer n, there exists a divisor closed submonoid S of H such that $\min \Delta(S) = n$.

1. Introduction and main result

Let H be an *atomic* monoid, i.e., each non-invertible element is a finite product of irreducible elements. Factorizations into irreducible elements, opposed to factorizations into primes, are not necessarily unique. For a non-invertible element $a \in H$ the *set of lengths* $\mathsf{L}_H(a)$ is the set of all positive integers n such that $a = u_1 \ldots u_n$ with irreducible elements $u_i \in H$. If $a \in H$ is invertible, then $\mathsf{L}_H(a) = \{0\}$. The investigation of sets of lengths is a main subject in non-unique factorization theory.

A central aim of non-unique factorization theory is to classify the phenomena of non-uniqueness of factorizations occurring for different (types of) monoids and domains (see the recent monograph [12] and the proceedings [1, 5] for a comprehensive presentation of the subject). It has its origins in algebraic number theory, in the investigation of the multiplicative arithmetic of rings of integers of algebraic number fields, and has been initiated in the 1960s by the work of L. Carlitz, W. Narkiewizc and others (see [18, Chapter 9]). Subsequently, factorizations in more general integral domains have been investigated (see, e.g., [2]). Meanwhile, many investigations in non-unique factorization theory are done in a purely multiplicative framework. Krull monoids are the multiplicative analogues of Krull domains, in particular the multiplicative monoid of a Dedekind or Krull domain is a Krull monoid (see [15, 14, 12] for details on Krull monoids). The notion Krull monoid

2000 *Mathematics Subject Classification.* 20K01, 13F05, 11R27.

Key words and phrases. Delta set, Krull monoid, infinite abelian group.

W. A. Schmid is supported by the FWF (Project number P18779-N13).

also covers other monoids of interest. The monoids formed by the isomorphy classes of certain modules under direct-sum decomposition are Krull monoids (see, e.g., [8, 16]). Moreover, the monoids of zero-sum sequences over subsets of abelian groups are Krull monoids, and conversely many questions regarding factorizations in Krull monoids can be transferred to questions regarding zero-sum sequences over subsets of their class groups (see Section 2 for details). This links the investigation of factorizations in Krull monoids to problems in additive group theory (see, e.g., [10]).

In order to understand the structure of sets of lengths, one considers the successive distances appearing in them. For a set of non-negative integers $L = \{l_1, l_2, \dots\}$ with $l_i < l_{i+1}$, let $\Delta(L) = \{l_2 - l_1, l_3 - l_2, \dots\}$ denote the *set of successive distances* of L and let $\Delta(H) = \bigcup_{a \in H} \Delta(\mathsf{L}_H(a))$ denote the *set of distances* of H. Of particular interest is the minimum of the set of distances and, more generally, the minima of the sets of distances of divisor-closed submonoids of H (a submonoid $S \subset H$ is called *divisor-closed*, if for $a \in S$ and $b \in H$, $b \mid_H a$ implies $b \in S$). More specifically, one is interested in the following subset of $\Delta(H)$:

$$\Delta^*(H) = \{\min \Delta(S) \colon S \subset H \text{ divisor-closed submonoid, } \Delta(S) \neq \emptyset\}.$$

These quantities were investigated in the papers [9, 13, 19, 3, 4]; also see [12, Chapters 4 and 6] for results and applications. Here we focus on the investigation of $\Delta^*(H)$ for Krull monoids with infinite class group. Specifically, the aim of this note is to prove the following result.

Theorem 1.1. *Let H be a Krull monoid with infinite class group such that each class contains a prime divisor. Then $\Delta^*(H)$ is equal to the set of positive integers.*

Examples of Krull monoids fulfilling the conditions of this result include certain monoids of isomorphy classes of modules (see, e.g., [16, Theorem 6.3]) and higher-dimensional finitely generated algebras over infinite fields (see [17] and [12, Example 7.4.2] for further examples).

The proof of this result is split into several cases, according to the type of the class group, which we address individually in several auxiliary results (see Section 3). Partial results on this problem, which we use in our proof, are given in [12, Proposition 6.8.2], where it is proved under the condition that the class group is not a torsion group or its p-rank is infinite for some prime p.

Moreover, we establish a result on $\Delta^*(H)$ for Krull monoids with finite class group as well, which complements known results (see Theorem 4.1). Our main tool is a recent result, obtained in [4], that allows

us to determine the minimal distance of certain Krull monoids with cyclic class group (see the discussion preceding Proposition 3.1).

2. Preliminaries

Our notation is consistent with [12]. For convenience we recall some key notions. We denote by $\mathbb{Z}$ the set of integers and by $\mathbb{N}$ and $\mathbb{N}_0$ the set of positive and non-negative integers, respectively; by $\mathbb{P} \subset \mathbb{N}$ the set of prime numbers and, for $a \in \mathbb{N}_0$, by $\mathbb{N}_{\ge a}$ the set of integers of size at least a. Let $(G, +)$ be an abelian group. A family $\{e_i \colon i \in I\}$ of elements of G is called *independent* if, for $m_i \in \mathbb{Z}$ and almost all 0, $\sum_{i \in I} m_i e_i = 0$ implies $m_i e_i = 0$ for each $i \in I$. By $\mathsf{r}_0(G)$ and $\mathsf{r}_p(G)$ for $p \in \mathbb{P}$ we denote the *torsionfree rank* and the *p-rank* of G, respectively. Furthermore, we denote by $\mathsf{r}(G) = \mathsf{r}_0(G) + \sup_{p \in \mathbb{P}} \mathsf{r}_p(G)$ the *rank* of G and by $\mathsf{r}^*(G) = \mathsf{r}_0(G) + \sum_{p \in \mathbb{P}} \mathsf{r}_p(G)$ the *total rank* of G. Moreover, let $\exp(G) = \sup\{\mathrm{ord}(g) \colon g \in G\} \in \mathbb{N} \cup \{\infty\}$ denote the *exponent* of G. We call G *bounded* if its exponent is finite.

Let $G_0 \subset G$ be a subset. We denote the (multiplicatively written) free abelian monoid over G_0 by $\mathcal{F}(G_0)$. An element $S \in \mathcal{F}(G_0)$ is called a *sequence* over G_0 and by definition $S = \prod_{g \in G_0} g^{v_g}$ with $v_g \in \mathbb{N}_0$ and almost all v_g equal to 0. The sequence S is called a *zero-sum sequence* if its *sum* $\sigma(S) = \sum_{g \in G_0} v_g g$ is equal to $0 \in G$. The set $\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \colon \sigma(S) = 0\}$ is a submonoid of $\mathcal{F}(G_0)$ and is called the *block monoid* over G_0. As mentioned in the Introduction, block monoids are Krull monoids and in particular atomic; their irreducible elements are the minimal zero-sum sequences over G_0, which we denote by $\mathcal{A}(G_0)$. Conversely, block monoids are a crucial tool in the investigation of Krull monoids (see [12, Chapter 3]); in particular, the following holds true (see [12, Proposition 4.3.13]).

Lemma 2.1. *Let H be a Krull monoid with class group G and let $G_P \subset G$ denote the subset of classes containing prime divisors. Then*

$$\Delta^*(H) = \Delta^*(\mathcal{B}(G_P)) = \{\min \Delta(\mathcal{B}(G_0)) \colon G_0 \subset G_P,\ \Delta(\mathcal{B}(G_0)) \neq \emptyset\}.$$

We will frequently make use of the fact, which is a direct consequence of the second equality in the above lemma, that if G' is isomorphic to a subgroup of G, then $\Delta^*(\mathcal{B}(G')) \subset \Delta^*(\mathcal{B}(G))$. For convenience we write $\Delta(G_0)$ and $\Delta^*(G)$ instead of $\Delta(\mathcal{B}(G_0))$ and $\Delta^*(\mathcal{B}(G))$, respectively.

We make use of the following well known arithmetical functions. For $n \in \mathbb{N}$ let $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ denote Euler's totient function, let $\lambda(n) = \exp((\mathbb{Z}/n\mathbb{Z})^\times)$ denote Carmichael's function, and let $\omega(n) = |\{p \in \mathbb{P} \colon p \mid n\}|$. If the modulus is clear from context, we write $\overline{m}$

for $m + n\mathbb{Z}$. All intervals are intervals of integers (i.e., for $a, b \in \mathbb{Z}$, $[a, b] = \{z \in \mathbb{Z} \colon a \le z \le b\}$).

3. Proof of Theorem 1.1

An important tool in our investigation is the following result in the special case $G_0 = \{\overline{1}, \overline{a}\}$ in $\mathbb{Z}/n\mathbb{Z}$. It is merely a special case of [4, Theorem 2.1] where the $\min \Delta(G_0)$ is described in terms of the continued fraction of n/a . For convenience we include an alternate proof of this special case.

Proposition 3.1. *Let a, n and k be in $\mathbb{N}$ such that $1 \le k < a < n$ where $n \equiv k \pmod a$ and $a \equiv 1 \pmod k$. Let $G_0 = \{\overline{1}, \overline{a}\} \subset \mathbb{Z}/n\mathbb{Z}$. Then $\min \Delta(G_0) = \frac{a-1}{k}$.*

To prove this result we recall the definition of the *g-norm* of a zero-sum sequence (see [7, Definition 1] or [12, Definition 6.8.4]) and its relation to the problem of determining the minimal distance of Krull monoids (see [11, Proposition 7] or [12, Lemma 6.8.5]). Let $G = \langle g \rangle$ be a cyclic group of order n. For $S = \prod_{i=1}^{\ell}(n_i g) \in \mathcal{F}(G)$ with $n_i \in [1, n]$ let

$$||S||_g = \frac{n_1 + \cdots + n_\ell}{n}.$$

Note that $||S||_g$ is an integer if and only if B is a zero-sum sequence.

Lemma 3.2. *Let $G = \langle g \rangle$ be a cyclic group of order n. Let $G_0 \subset G$ such that $\Delta(G_0) \ne \emptyset$. Then $\min \Delta(G_0) = \gcd\{||U||_g - 1 \colon U \in \mathcal{A}(G_0)\}$.*

Proof. See [12, Lemma 6.8.5]. □

Proof of Proposition 3.1. We set $m = \frac{n-k}{a}$ and $d = \frac{a-1}{k}$. We have

$$\mathcal{A}(G_0) = \{\overline{a}^{\ell}\overline{1}^{n-\ell a} \colon \ell \in [0, m]\} \cup \{\overline{a}^{m+\ell(dm+1)}\overline{1}^{k-\ell} \colon \ell \in [1, k]\}$$

(see [6] for a detailed argument). Since $||\overline{a}^{\ell}\overline{1}^{n-\ell a}||_{\overline{1}} = 1$ for each $\ell \in [0, m]$ and $||\overline{a}^{m+\ell(dm+1)}\overline{1}^{k-\ell}||_{\overline{1}} = 1 + d\ell$ for each $\ell \in [1, k]$ the claim follows by Lemma 3.2. □

Proposition 3.3. *Let $p \in \mathbb{P}$ and $d, k \in \mathbb{N}$. If $k \ge \lambda(dp + 1) + 1$, then $d \in \Delta^*(\mathbb{Z}/p^k\mathbb{Z})$.*

Proof. Since $\gcd(p, dp + 1) = 1$, we have $p^{\lambda(dp+1)} \equiv 1 \pmod{dp + 1}$. Thus, $p^{\lambda(dp+1)+1} \equiv p \pmod{dp + 1}$ and $pd + 1 \equiv 1 \pmod p$. Consequently, by Proposition 3.1, $\frac{(dp+1)-1}{p} = d \in \Delta^*(\mathbb{Z}/p^{\lambda(dp+1)+1}\mathbb{Z})$. If $k \ge \lambda(dp+1)+1$, then $\Delta^*(\mathbb{Z}/p^{\lambda(dp+1)+1}\mathbb{Z}) \subset \Delta^*(\mathbb{Z}/p^k\mathbb{Z})$ and the result follows. □

Remark 3.4. If $d \not\equiv -1 \pmod p$, then Proposition 3.3 can be modified in the following way. If $p \in \mathbb{P}$, $d, k \in \mathbb{N}$, $k \ge \lambda(d+1)$, and $d \not\equiv -1 \pmod p$, then $d \in \Delta^*(\mathbb{Z}/p^k\mathbb{Z})$ (since $d \not\equiv -1 \pmod p$, we have $\gcd(d+1, p) = 1$ and $p^{\lambda(d+1)} \equiv 1 \pmod{d+1}$; the claim follows by Proposition 3.1 with $n = p^{\lambda(d+1)}$ and $a = d+1$).

Proposition 3.5. *Let $P \subset \mathbb{P}$ and $G = \oplus_{p\in P}\mathbb{Z}/p\mathbb{Z}$. Furthermore, let $b \in \mathbb{N}_{\ge 2}$ such that*

$$\varphi(b)(\lambda(b) - 1) + \omega(b) < |P|. \tag{1}$$

Then $b - 1 \in \Delta^*(G)$.

Proof. For $\overline{r} \in (\mathbb{Z}/b\mathbb{Z})^\times$, let $P_{\overline{r}} = P \cap \overline{r}$. We note that if $p \in P \setminus \bigcup_{\overline{r}\in(\mathbb{Z}/b\mathbb{Z})^\times} P_{\overline{r}}$, then $p \mid b$. Thus, $|P| \le \omega(b) + \sum_{\overline{r}\in(\mathbb{Z}/b\mathbb{Z})^\times} |P_{\overline{r}}|$ and there exists some $\overline{r'} \in (\mathbb{Z}/b\mathbb{Z})^\times$ such that $|P_{\overline{r'}}| \ge \frac{|P|-\omega(b)}{\varphi(b)} > \lambda(b) - 1$. Let $p_1, \ldots, p_{\lambda(b)} \in P_{\overline{r'}}$ be distinct and $n = \prod_{i=1}^{\lambda(b)} p_i$. Since $p_i \in \overline{r'}$ for each i, we have $n \in \overline{r'}^{\lambda(b)} = 1 + b\mathbb{Z}$. Thus, by Proposition 3.1, $b - 1 \in \Delta^*(\mathbb{Z}/n\mathbb{Z})$. Since $\Delta^*(\mathbb{Z}/n\mathbb{Z}) \subset \Delta^*(G)$, the claim follows. □

The following two results are known (cf. [12, Proposition 6.8.2]), for convenience we include (a sketch of) the proofs.

Lemma 3.6. $\Delta^*(\mathbb{Z}) = \mathbb{N}$.

Proof. Let $d \in \mathbb{N}$ and let $G_d = \{1, (d+1), -1, -(d+1)\} \subset \mathbb{Z}$. Then $\Delta(G_d) = \{d\}$. □

Lemma 3.7. *Let G be an abelian torsion group. If $d \in \mathbb{N}$ and $d < \mathsf{r}(G)$, then $d \in \Delta^*(G)$.*

Proof. Since $d < \mathsf{r}(G)$, there exists some $p \in \mathbb{P}$ and independent elements $e_1, \ldots, e_{d+1}$ such that $\mathrm{ord}(e_i) = p$. Let $e_0 = \sum_{i=1}^{d+1} e_i$ and $G_0 = \{e_i \colon i \in [0, d+1]\}$. Then $\Delta(G_0) = \{d\}$ (see [12, Proposition 6.8.1] for a detailed argument). □

Now, we combine these results to prove Theorem 1.1.

Proof of Theorem 1.1. Let G be the class group of H. By Lemma 2.1 it suffices to show that $\Delta^*(G) = \mathbb{N}$. If G is not a torsion group, then it has a subgroup isomorphic to $\mathbb{Z}$ and the claim follows by Lemma 3.6. Thus, we suppose that G is a torsion group. If G is bounded, then its rank has to be infinite. In this case the claim follows by Lemma 3.7. Thus, we suppose that G is not bounded. Therefore, at least one of the following conditions has to hold:

- There exists an infinite subset $P \subset \mathbb{P}$ such that for each $p \in P$ there is some $g_p \in G$ with $\mathrm{ord}(g_p) = p$.

- There exists some $p \in \mathbb{P}$ such that for each $k \in \mathbb{N}$ there exists some $g_k \in G$ with $\mathrm{ord}(g_k) = p^k$.

If the latter holds true, the claim follows by Proposition 3.3. If the former holds true, the claim follows by Proposition 3.5, since (1) trivially holds for each b. □

4. Finite class groups

The methods used in the proof of Theorem 1.1 can be used to obtain information on $\Delta^*(H)$ for Krull monoids with finite class group as well. For an overview of results on this problem see [12, Section 6.8]. In particular, it might be interesting to contrast the second part of the following result with a result of W. D. Gao and A. Geroldinger [9] (also see [12, Proposition 6.8.7]) asserting that $\Delta^*(H) \subset [1, \mathsf{r}^*(G) - 1]$ if $\mathsf{r}^*(G) \ge (\exp(G) - 1) + \frac{1}{2}(\exp(G) - 1)^2(\exp(G) - 2)$.

Theorem 4.1. *Let H be a Krull monoid with finite class group G such that each class contains a prime divisor.*

(1) $[1, \lceil \sqrt{\omega(\exp(G))} \rceil - 1] \subset \Delta^*(H)$.
(2) $[1, \lceil \sqrt[3]{\mathsf{r}^*(G)} \rceil - 1] \subset \Delta^*(H)$.

Proof. Let $n = \exp(G)$.

(1) The group $\mathbb{Z}/n\mathbb{Z}$ has a subgroup isomorphic to $\oplus_{p \in P} \mathbb{Z}/p\mathbb{Z}$ where $P \subset \mathbb{P}$ and $|P| = \omega(n)$. Since, for $d \in \mathbb{N}$,

$$\varphi(d+1)(\lambda(d+1) - 1) + \omega(d+1) \le d(d-1) + d = d^2,$$

the claim follows by Proposition 3.5 and Lemma 2.1.

(2) We note that $\mathsf{r}^*(G) \le \mathsf{r}(G)\omega(n)$. Thus, $\mathsf{r}(G) \ge \mathsf{r}^*(G)^{1/3}$ or $\omega(n) \ge \mathsf{r}^*(G)^{2/3}$. Now, the claim follows by Lemma 3.7 and part (1) above, respectively, and Lemma 2.1. □

References

[1] D. D. Anderson, editor, *Factorization in integral domains* (Marcel Dekker Inc., New York, 1997).
[2] D. D. Anderson, D. F. Anderson, and M. Zafrullah, 'Factorization in integral domains', *J. Pure Appl. Algebra* 69 (1990) 1–19.
[3] C. Bowles, S. T. Chapman, N. Kaplan, and D. Reiser, 'On delta sets of numerical monoids', *J. Algebra Appl.* 5 (2006) 695–718.
[4] S. Chang, S. T. Chapman, and W. W. Smith, 'On minimum delta set values in block monoids over cyclic groups', *Ramanujan J.* 14 (2007) 155–171.

[5] S. T. Chapman, editor, *Arithmetical properties of commutative rings and monoids* (Chapman & Hall/CRC, Boca Raton, FL, 2005).

[6] S. T. Chapman and W. W. Smith, 'On factorization in block monoids formed by $\{\overline{1}, \overline{a}\}$ in $\mathbb{Z}_n$', *Proc. Edinb. Math. Soc. (2)* 46 (2003) 257–267.

[7] S. T. Chapman and W. W. Smith, 'A characterization of minimal zero-sequences of index one in finite cyclic groups', *Integers* 5 (2005) A27, 5 pp. (electronic).

[8] A. Facchini, W. Hassler, L. Klingler, and R. Wiegand, 'Direct-sum decompositions over one-dimensional Cohen-Macaulay local rings', *Multiplicative ideal theory in commutative algebra*, A tribute to the work of Robert Gilmer (eds. J. W. Brewer, S. Glaz, W. J. Heinzer, and B. M. Olberding, Springer, New York, 2006), pp. 153–168.

[9] W. Gao and A. Geroldinger, 'Systems of sets of lengths. II', *Abh. Math. Sem. Univ. Hamburg* 70 (2000) 31–49.

[10] W. Gao and A. Geroldinger, 'On a property of minimal zero-sum sequences and restricted sumsets', *Bull. London Math. Soc.* 37 (2005) 321–334.

[11] A. Geroldinger, 'On nonunique factorizations into irreducible elements. II', *Number theory, Vol. II (Budapest, 1987)* (eds. K. Győry and G. Halász), Colloq. Math. Soc. János Bolyai 51 (North-Holland, Amsterdam, 1990), pp. 723–757.

[12] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory* (Chapman & Hall/CRC, Boca Raton, FL, 2006).

[13] A. Geroldinger and Y. O. Hamidoune, 'Zero-sumfree sequences in cyclic groups and some arithmetical application', *J. Théor. Nombres Bordeaux* 14 (2002) 221–239.

[14] P. A. Grillet, *Commutative semigroups* (Kluwer Academic Publishers, Dordrecht, 2001).

[15] F. Halter-Koch, *Ideal systems* (Marcel Dekker Inc., New York, 1998).

[16] W. Hassler, R. Karr, L. Klingler, and R. Wiegand, 'Big indecomposable modules and direct-sum relations', *Illinois J. Math.* 51 (2007) 99–122.

[17] F. Kainrath, 'The distribution of prime divisors in finitely generated domains', *Manuscripta Math.* 100 (1999) 203–212.

[18] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers, third edition* (Springer, Berlin, 2004).

[19] W. A. Schmid, 'Differences in sets of lengths of Krull monoids with finite class group', *J. Théor. Nombres Bordeaux* 17 (2005) 323–345.

Trinity University, Department of Mathematics, One Trinity Place, San Antonio, TX 78212-7200, USA
E-mail address: schapman@trinity.edu

Institut für Mathematik und Wissenschaftliches Rechnen, Karl-Franzens-Universität Graz, Heinrichstrasse 36, 8010 Graz, Austria
E-mail address: wolfgang.schmid@uni-graz.at

The University of North Carolina at Chapel Hill, Department of Mathematics, Phillips Hall, Chapel Hill, NC 27599, USA
E-mail address: wwsmith@email.unc.edu