THE SET OF DISTANCES IN KRULL MONOIDS

ALFRED GEROLDINGER AND PINGZHI YUAN*

ABSTRACT. Let H be a Krull monoid with class group G and suppose that every class contains a prime divisor. The set of distances $\Delta(H)$ of H is the set of all $d \in \mathbb{N}$ with the following property: there are irreducible elements $u_1, \ldots, u_k, v_1, \ldots, v_{k+d}$ such that $u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_{k+d}$, but $u_1 \cdot \ldots \cdot u_k$ cannot be written as a product of l irreducible elements for any l with $k < l < k+d$. We show that $\Delta(H)$ is an interval.

1. Introduction and Main Result

Let H be a Krull monoid with class group G. Examples of such monoids are the non-zero elements of a Krull or Dedekind domain (further examples will be discussed in Section 2). Then every non-unit of H has a factorization as a finite product of atoms, (or irreducible elements), and all these factorizations are unique (in other words, H is factorial) if and only if G is trivial. In case of a non-trivial class group, the non-uniqueness of factorizations is described by arithmetical invariants, such as sets of lengths, sets of distances, catenary and tame degrees. We recall some of these concepts.

Let $L = \{l_1, \ldots, l_k\}$ be a finite non-empty subset of the positive integers with $l_1 < \ldots < l_k$. Then $\Delta(L) = \{l_2 - l_1, \ldots, l_k - l_{k-1}\}$ is called the set of distances of L, and L is said to be an interval if it is an arithmetical progression with difference 1, or equivalently if $\Delta(L) \subset \{1\}$. If a non-unit $a \in H$ has a factorization $a = u_1 \cdot \ldots \cdot u_k$ into atoms $u_1, \ldots, u_k$, then k is called the length of the factorization, and the set $\mathsf{L}(a)$ of all possible k is called the set of lengths of a. An easy observation shows that in the Krull case, all sets of lengths are finite. The set of distances $\Delta(H)$ is the union of all sets $\Delta\big(\mathsf{L}(a)\big)$ over all non-units $a \in H$. In other words, $\Delta(H)$ is the set of all $d \in \mathbb{N}$ such that there are atoms $u_1, \ldots, u_k, v_1, \ldots, v_{k+d}$ with $u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_{k+d}$, and $u_1 \cdot \ldots \cdot u_k$ has no factorization of length l for any l with $k < l < k+d$.

Now suppose that every class of G contains a prime divisor (rings of integers in algebraic number fields have this property), and to simplify the discussion, suppose for the moment that $3 \le |G| < \infty$. Then the set of distances $\Delta(H)$ is finite, non-empty, and the system of sets of lengths has a well-described structure which is known to be best possible ([12, Section 4.7], [17]). The assumption that every class of G contains a prime divisor has a strong impact on the factorizations in H. Unions of sets of lengths are intervals ([8], [10, Theorem 3.1.3]), and if the set of classes of prime divisors of some element $a \in H$ form a subgroup of G, then the set of lengths $\mathsf{L}(a)$ is an interval ([12, Theorem 7.6.9]). The structure of a crucial subset of $\Delta(H)$ was studied in [5, 16].

In the present paper we show that $\Delta(H)$ is an interval. We formulate our main result, where $\mathsf{D}(G)$ denotes the Davenport constant of the group G (see Section 2).

2010 *Mathematics Subject Classification.* 13A05, 20M13, 11B50.

Key words and phrases. non-unique factorizations, set of distances, Krull monoids.

*The corresponding author. This work was supported by the Austrian Science Fund FWF (Projects W1230-N13 and P21576-N18), and by the National Science Fund NSF of China (Project Number 10971072).

Theorem 1.1. *Let H be a Krull monoid with class group G and suppose that every class contains a prime divisor. Then $\Delta(H)$ is an interval. More precisely, we have the following.*

1. *If $|G| \le 2$, then $\Delta(H) = \emptyset$.*
2. *Suppose that G is finite with $|G| \ge 3$, say $G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$ with $1 < n_1 \mid \ldots \mid n_r$. Then $\Delta(H)$ is a finite non-empty interval with $\min \Delta(H) = 1$, and if $\lfloor \frac{1}{2}\mathsf D(G) + 1 \rfloor \le \max\{n_r, 1 + \sum_{i=1}^r \lfloor \frac{n_i}{2} \rfloor\}$, then $\Delta(H) = [1, \mathsf c(H) - 2]$, where $\mathsf c(H)$ is the catenary degree of H.*
3. *If G is infinite, then $\Delta(H) = \mathbb N$.*

Let G be as in 2., so $G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$ and set $\mathsf D^*(G) = 1 + \sum_{i=1}^r (n_i - 1)$. Then $\mathsf D^*(G) \le \mathsf D(G)$, and equality holds for p-groups, groups of rank at most two, and others (see [10] for an overview). In all these groups the above inequality involving $\mathsf D(G)$ is satisfied. The very definitions show that $\Delta(H) \subset [1, \mathsf c(H) - 2]$, and the standing conjecture is that $\max \Delta(H) = \mathsf c(H) - 2$. Only recently, this conjecture has been verified under the above assumption on the Davenport constant ([11, Corollary 4.1]).

In Section 2 we introduce the required concepts and tools. The proof of Theorem 1.1 will be given in Section 3. After the proof we discuss several examples indicating that the fact that $\Delta(H)$ is an interval is a very special feature of the Krull monoids under consideration.

2. Preliminaries

Our notation and terminology are consistent with [12]. We denote by $\mathbb N$ the set of positive integers, and for $a, b \in \mathbb Z$, we denote by $[a, b] = \{x \in \mathbb Z \mid a \le x \le b\}$ the discrete, finite interval between a and b. By a monoid we mean a commutative semigroup with identity which satisfies the cancellation laws. If H is a monoid, then $\mathcal A(H)$ denotes the set of atoms (or irreducible elements) of H. A monoid F is called free (with basis $P \subset F$), and we write $F = \mathcal F(P)$, if every $a \in F$ has a unique representation of the form

$$a = \prod_{p \in P} p^{\mathsf v_p(a)} \quad \text{with} \quad \mathsf v_p(a) \in \mathbb N_0 \quad \text{and} \quad \mathsf v_p(a) = 0 \quad \text{for almost all} \quad p \in P\,.$$

A monoid H is said to be a *Krull monoid* if it satisfies one of the following two equivalent conditions (see [12, Theorem 2.4.8]).

(a) H is v-noetherian and completely integrally closed.
(b) There exists a monoid homomorphism $\varphi \colon H \to F = \mathcal F(P)$ into a free monoid F such that $a \,|\, b$ in H if and only if $\varphi(a) \,|\, \varphi(b)$ in F.

Condition (a) shows that the multiplicative monoid of non-zero elements of a noetherian domain is Krull if and only if the domain is integrally closed. Rings of integers, holomorphy rings in algebraic function fields, and regular congruence monoids in these domains are Krull monoids with finite class group such that every class contains a prime divisor ([12, Section 2.11 and Examples 7.4.2]). Monoid domains and power series domains that are Krull are discussed in [15, 4]. For the role of Krull monoids in module theory, we refer the reader to [6, 7].

Most aspects of the arithmetic of a Krull monoid can be studied in the associated block monoid (this is the monoid of zero-sum sequences over its class group). Let G be an additively written abelian group. An element $S = g_1 \cdot \ldots \cdot g_l \in \mathcal F(G)$ is called a sequence over G, $\sigma(S) = g_1 + \ldots + g_l$ is called its sum, and $|S| = l$ its length. The monoid

$$\mathcal B(G) = \{S \in \mathcal F(G) \mid \sigma(S) = 0\}$$

is the monoid of zero-sum sequences over G, and since the embedding $\varphi \colon \mathcal B(G) \hookrightarrow \mathcal F(G)$ satisfies Condition (b), $\mathcal B(G)$ is a Krull monoid. As usual, we set $\mathcal A(G) = \mathcal A\big(\mathcal B(G)\big)$ and $\Delta(G) = \Delta\big(\mathcal B(G)\big)$. Note that the atoms of $\mathcal B(G)$ are precisely the minimal zero-sum sequences over G, and

$$\mathsf D(G) = \sup\{|U| \mid U \in \mathcal A(G)\} \in \mathbb N \cup \{\infty\}$$

is the *Davenport constant* of G. The next lemma states that sets of distances in a Krull monoid can be studied in the associated monoid of zero-sum sequences over its class group. Its proof can be found in [12, Theorem 3.4.10].

Lemma 2.1. *Let H be a Krull monoid with class group G and suppose that every class contains a prime divisor. Then $\Delta(H) = \Delta(G)$.*

3. Proof of the Main Result

In this section, we give the proof of Theorem 1.1, and provide some examples showing that in general sets of distances need not be intervals.

Proof of Theorem 1.1. If $|G| \le 2$, then H is half-factorial by [12, Corollary 3.4.12], and thus $\Delta(H) = \emptyset$. Suppose that G is infinite. Then by a Theorem of Kainrath, every finite set $L \subset \mathbb{N}_{\ge 2}$ is a set of lengths in H (see [14] or [12, Theorem 7.4.1]). This implies that $\mathbb{N} \subset \Delta(H) \subset \mathbb{N}$.

Now we suppose that G is finite with $|G| \ge 3$. Then $\Delta(G)$ is finite by [12, Corollary 3.4.13], and if the condition on the Davenport constant $\mathsf{D}(G)$ holds, then $\max \Delta(H) = \mathsf{c}(H) - 2$ by [11, Corollary 4.1]. By Lemma 2.1, we have $\Delta(H) = \Delta(G)$, and thus it remains to prove that $\Delta(G)$ is an interval with $\min \Delta(G) = 1$.

We start with two simple observations. If $U = g_1 \cdot \ldots \cdot g_l \in \mathcal{A}(G)$ with $|U| = l \ge 2$, then $g_1^{-1} g_2^{-1} (g_1 + g_2) U = (g_1 + g_2) g_3 \cdot \ldots \cdot g_l \in \mathcal{A}(G)$ too. Conversely, if $U' = (g_1 + g_2) g_3 \cdot \ldots \cdot g_l \in \mathcal{A}(G)$ with $|U'| = l \ge 2$, then $g_1 g_2 (g_1 + g_2)^{-1} U'$ is either an atom or a product of precisely two atoms.

Now we define a function $f \colon \Delta(G) \to \mathbb{N}$ as follows. If $d \in \Delta(G)$, then there are $k, l \in \mathbb{N}$ and $U_1, \ldots, U_k$, $V_1, \ldots, V_l \in \mathcal{A}(G)$ such that

$$U_1 \cdot \ldots \cdot U_k = V_1 \cdot \ldots \cdot V_l \,,$$

where $l - k = d$, and $U_1 \cdot \ldots \cdot U_k$ has no factorization of length in $[k+1, l-1]$. Let $f(d)$ be defined as the minimum over all $|U_1 \cdot \ldots \cdot U_k|$ where $U_1, \ldots, U_k$ stem from such a configuration. We continue with the following assertion.

A. For every $d \in [1, \max \Delta(G)]$, the interval $[d, \max \Delta(G)] \subset \Delta(G)$ and the function $f \mid [d, \max \Delta(G)] \colon [d, \max \Delta(G)] \to \mathbb{N}$ is strictly increasing.

Clearly, **A** implies that $\Delta(G) = [1, \max \Delta(G)]$ is an interval with $\min \Delta(G) = 1$.

Proof of **A**. We proceed by induction on d. Obviously, the assertion holds for $d = \max \Delta(G)$. Now suppose that the assertion holds for some $d \in [2, \max \Delta(G)]$. We have to show that it holds for $d-1$. To do so, we start with a configuration as in the definition of $f(d)$. Thus, let $U_1, \ldots, U_k, V_1, \ldots, V_l \in \mathcal{A}(G)$ such that

$$U_1 \cdot \ldots \cdot U_k = V_1 \cdot \ldots \cdot V_l \,,$$

where $l - k = d$, $U_1 \cdot \ldots \cdot U_k$ has no factorization of length in $[k+1, l-1]$, and $f(d) = |U_1 \cdot \ldots \cdot U_k|$. For every $i \in [1, l]$, we set $V_i = U_{1,i} \cdot \ldots \cdot U_{k,i}$ with $U_{1,i}, \ldots, U_{k,i} \in \mathcal{F}(G)$ such that

$$U_j = U_{j,1} \cdot \ldots \cdot U_{j,l} \quad \text{for all} \quad j \in [1, k] \,.$$

Note that $f(d) = |U_1 \cdot \ldots \cdot U_k| = |V_1 \cdot \ldots \cdot V_l| \ge 2l = 2k + 2d$. Thus, after renumbering if necessary, we may suppose that $|U_1| \ge 3$, $|U_{1,1}| \ge 1$ and $|U_{1,2}| \ge 1$. Moreover, say $g_1 \,|\, U_{1,1}$ and $g_2 \,|\, U_{1,2}$ with $g_1, g_2 \in G$. Clearly,

$$U_1' = (g_1 + g_2) g_1^{-1} g_2^{-1} U_1 \quad \text{and} \quad V_1' = (g_1 + g_2) g_1^{-1} g_2^{-1} V_1 V_2$$

are zero-sum sequences, $U_1' \in \mathcal{A}(G)$, and

$$U_1' U_2 \cdot \ldots \cdot U_k = V_1' V_3 \cdot \ldots \cdot V_l \,.$$

First, we assert that $U_1'U_2 \cdot \ldots \cdot U_k$ has no factorization of length in $[k+1, l-2]$. Indeed, assume to the contrary that

$$U_1'U_2 \cdot \ldots \cdot U_k = W_1 \cdot \ldots \cdot W_t \,,$$

where $t \in [k+1, l-2]$, $W_1, \ldots, W_t \in \mathcal{A}(G)$ and $(g_1+g_2) \,|\, W_1$. Since $(g_1+g_2)^{-1}g_1g_2W_1$ is either an atom or a product of two atoms, $U_1 \cdot \ldots \cdot U_k$ would have a factorization of length in $[k+1, l-1]$, a contradiction.

Now we assume to the contrary that $U_1'U_2 \cdot \ldots \cdot U_k$ has no factorization of length $l-1$. Then there exists a $t \ge l$ such that $U_1'U_2 \cdot \ldots \cdot U_k$ has a factorization of length t, but no factorization of length in $[k+1, t-1]$. Therefore, $t-k \in \Delta(G)$, $t-k \ge l-k = d$, and

$$f(t-k) \le |U_1'U_2 \cdot \ldots \cdot U_k| = |U_1 \cdot \ldots \cdot U_k| - 1 = f(d) - 1 \,,$$

a contradiction to the induction hypothesis that f is strictly increasing on $[d, \max \Delta(G)]$.

Thus $U_1'U_2 \cdot \ldots \cdot U_k$ has a factorization of length $l-1$ which implies that $l-1-k = d-1 \in \Delta(G)$ and $f(d-1) \le |U_1'U_2 \cdot \ldots \cdot U_k| < |U_1 \cdot \ldots \cdot U_k| = f(d)$. □

Remarks 3.1. On the one side, the set of distances (also called the delta set in the literature) of an atomic monoid H cannot be an arbitrary subset of the positive integers. For example, we always have that $\gcd \Delta(H) = \min \Delta(H)$ ([12, Proposition 1.4.4]). But on the other side, even for nice classes of monoids the fact that $\Delta(H)$ is an interval whose maximum equals $\mathsf{c}(H) - 2$ is a very special feature of the Krull monoids under consideration. We briefly outline this by several examples.

1. A straightforward observation shows that $2 + \sup \Delta(H) \le \mathsf{c}(H)$ whenever H is non-factorial ([12, Theorem 1.6.3]). A list of examples for which this inequality is strict can be found in [11, page 146].

2. Sets of distances have been studied in detail for congruence monoids and numerical monoids. In particular, it was demonstrated that sets of distances of such monoids need not be intervals (see for example [1, 2]).

3. Suppose that H is a Krull monoid whose class group G is a finite cyclic group of odd order $|G| = n = 2m+1 \ge 7$, and suppose that $G_0 = \{g, mg, -g\} \subset G$ is the set of classes containing prime divisors. We outline that $\Delta(H) = \Delta(G_0)$ is not an interval (by Claborn's Realization Theorem, there are Dedekind domains having such a distribution of prime divisors, see [12, Theorem 3.7.8]). We have

$$\mathcal{A}(G_0) = \{g^n, (-g)^n, g(-g), (mg)^n, g(mg)^2, g^{n-m}(mg), (mg)(-g)^m\} \,.$$

Then $g^n(-g)^n = \big(g(-g)\big)^n$ and $g^n(mg)^n = \big(g(mg)^2\big)^m \big(g^{n-m}(mg)\big)$ show that $n-2, m-1 \in \Delta(G_0)$. Since $\max \Delta(G_0) \le \mathsf{c}(G_0) - 2 \le \mathsf{D}(G_0) - 2 = n-2$, it follows that $\max \Delta(G_0) = n-2 = \mathsf{c}(G_0) - 2$. Furthermore, we get that $1 = \gcd(n-2, m-1) = \gcd \Delta(G_0) \in \Delta(G_0)$. It is easy to check that $n-3 \notin \Delta(G_0)$, and hence $\Delta(H) = \Delta(G_0)$ is not an interval.

4. We end with some more positive examples. Indeed, the set of distances $\Delta(H)$ equals $\mathbb{N}$ in each of the following cases:

- H is a semiring of polynomials with non-negative coefficients taken from a domain D with $\mathbb{Z} \subset D \subset \mathbb{R}$: [3].
- H is a Krull monoid with infinite class group G, and the set of classes $G_0 \subset G$ containing prime divisors has the property that, for a positive integer h, the h-fold sumset of G_0 equals G: [13].
- H is the set of non-zero integer-valued polynomials. Indeed, S. Frisch [9] proved that every finite set $L \subset N_{\ge 2}$ can be realized as a set of lengths of some polynomial $f \in \text{Int}(\mathbb{Z})$, and hence $\Delta\big(\text{Int}(\mathbb{Z})\big) = \mathbb{N}$.

Acknowledgements. We thank the referees for their useful suggestions.

References

[1] P. Baginski, S.T. Chapman, and G.J. Schaeffer, *On the delta set of a singular arithmetical congruence monoid*, J. Théor. Nombres Bordx **20** (2008), 45 – 59.

[2] C. Bowles, S.T. Chapman, N. Kaplan, and D. Reiser, *On delta sets of numerical monoids*, J. Algebra Appl. **5** (2006), 695 – 718.

[3] P. Cesarz, S.T. Chapman, S. McAdam, and G.J. Schaeffer, *Elastic properties of some semirings defined by positive systems*, Commutative Algebra and its Applications (B. Olberding and I. Swanson, eds.), deGruyter, 2009, pp. 89 – 101.

[4] Gyu-Whan Chang, *Every divisor class of Krull monoid domains contains a prime ideal*, J. Algebra **336** (2011), 370 – 377.

[5] S.T. Chapman, W.A. Schmid, and W.W. Smith, *On minimal distances in Krull monoids with infinite class group*, Bull. Lond. Math. Soc. **40** (2008), 613 – 618.

[6] A. Facchini, *Krull monoids and their application in module theory*, Algebras, Rings and their Representations (A. Facchini, K. Fuller, C. M. Ringel, and C. Santa-Clara, eds.), World Scientific, 2006, pp. 53 – 71.

[7] 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 (J.W. Brewer, S. Glaz, W. Heinzer, and B. Olberding, eds.), Springer, 2006, pp. 153 – 168.

[8] M. Freeze and A. Geroldinger, *Unions of sets of lengths*, Funct. Approximatio, Comment. Math. **39** (2008), 149 – 162.

[9] S. Frisch, *A construction of integer-valued polynomials with prescribed sets of lengths of factorizations*, manuscript.

[10] A. Geroldinger, *Additive group theory and non-unique factorizations*, Combinatorial Number Theory and Additive Group Theory (A. Geroldinger and I. Ruzsa, eds.), Advanced Courses in Mathematics CRM Barcelona, Birkhäuser, 2009, pp. 1 – 86.

[11] A. Geroldinger, D.J. Grynkiewicz, and W.A. Schmid, *The catenary degree of Krull monoids I*, J. Théor. Nombres Bordx. **23** (2011), 137 – 169.

[12] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.

[13] W. Hassler, *Factorization properties of Krull monoids with infinite class group*, Colloq. Math. **92** (2002), 229 – 242.

[14] F. Kainrath, *Factorization in Krull monoids with infinite class group*, Colloq. Math. **80** (1999), 23 – 30.

[15] H. Kim and Y. S. Park, *Krull domains of generalized power series*, J. Algebra **237** (2001), 292 – 301.

[16] A. Plagne and W.A. Schmid, *On congruence half-factorial Dedekind domains with cyclic class group*, manuscript.

[17] W.A. Schmid, *A realization theorem for sets of lengths*, J. Number Theory **129** (2009), 990 – 999.

Institut für Mathematik und Wissenschaftliches Rechnen, Karl–Franzens–Universität Graz, Heinrichstrasse 36, 8010 Graz, Austria

E-mail address: `alfred.geroldinger@uni-graz.at`

School of Mathematics, South China Normal University, Guangzhou 510631, P.R. China

E-mail address: `mcsypz@mail.sysu.edu.cn`