COLLOQUIUM MATHEMATICUM

VOL. 78 1998 NO. 2

A STRUCTURE THEOREM FOR SETS OF LENGTHS

BY

ALFRED GEROLDINGER (GRAZ)

1. Introduction. Let R be a noetherian domain. Then every non-zero element $a \in R$ has a factorization $a = u_1 \ldots u_k$ into irreducible elements of R. The number of factors, k, is called the length of the factorization, and the set of lengths $L(a)$ is defined as the set of all possible k. Sets of lengths play a central role in factorization theory of integral domains (cf. the survey articles in [An]). If all sets $L(a)$ consist of exactly one element, then the domain is called half-factorial. By definition, factorial domains are half-factorial. Suppose that R is not half-factorial. Since R is noetherian, all sets of lengths are finite. However, for every $N \in \mathbb{N}_+$ there exists some $a \in R$ such that $\#L(a) \geq N$. If R is a ring of integers in a number field, then even equality holds (observed by J. Śliwa 1982 in [Sl]) and the sets $L(a)$ have a well-defined structure: in essence they are unions of arithmetical progressions (proved in [Ge1], 1988). In the meantime this result was extended to more general monoids and domains (cf. [Ge3] and the literature cited there).

In this paper we present a new approach to a Structure Theorem for Sets of Lengths, which unifies, strengthens and extends all hitherto known results. This is made possible by extracting its combinatorial kernel. In Section 2 we start with a result from additive number theory, which will be used to derive a Structure Theorem for Sets of Lengths in a very general setting (Theorem 3.2). All therein described phenomena appear already in rings of algebraic integers (Realization Theorem 3.5).

Theorem 3.2 will be applied to arithmetically relevant monoids and the associated integral domains including certain weakly Krull domains, in particular orders in global fields (Theorems 8.3 and 9.3). The significance of the assumptions in the Structure Theorem may be seen in Theorem 8.5, which provides simple Krull monoids not satisfying the assertion of the Structure Theorem.

All this needs a lot of monoid-theoretical preparations, done in Sections 4 to 7. Along the way we introduce new and generalize well-known concepts from factorization theory. Apart from being used for the Structure Theorem

1991 *Mathematics Subject Classification*: 11R27, 13F05.

these concepts seem to be of their own interest (cf. Theorem 7.4). Notations and terminology are consistent with those in the survey articles [Ch-Ge], [HK2] by Chapman, Halter-Koch and myself in [An].

2. A combinatorial result on sumsets. In this section we study finite subsets of the integers. Let $\mathbb{N}$ denote the non-negative integers and $\mathbb{N}_+$ the positive integers. For convenience we set $\min\emptyset = \max\emptyset = 0$. For a set X let $\mathbb{P}_{\mathrm{fin}}(X)$ denote the set of all finite subsets of X. If $a, b \in \mathbb{Z}$, then $[a,b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$ is the closed interval and $(a,b]$, $[a,b)$, (a,b) have their usual meaning. For a finite subset $L = \{a_1, \ldots, a_k\} \subseteq \mathbb{Z}$ with $a_1 < \ldots < a_k$, we call

$$\Delta(L) = \{a_i - a_{i-1} \mid 2 \le i \le k\} \subseteq \mathbb{N}_+$$

the *set of differences* of L; by definition, $\Delta(L) = \emptyset$ if and only if $\#L \le 1$. Furthermore, L is an *arithmetical progression with difference* d if and only if $\Delta(L) = \{d\}$. For a family $\mathcal{L}$ of finite subsets of $\mathbb{Z}$ we set

$$\Delta(\mathcal{L}) = \bigcup_{L \in \mathcal{L}} \Delta(L) \subseteq \mathbb{N}_+.$$

For a subset $L' \subseteq \mathbb{Z}$,

$$L + L' = \{a + b \mid a \in L,\ b \in L'\}$$

denotes the *sumset of* L *and* L'. For every $b \in \mathbb{Z}$ we set

$$L + b = b + L = L + \{b\}.$$

We are mainly interested in the inner structure of finite subsets of $\mathbb{Z}$ and give the following definition.

Definition 2.1. A finite subset $L \subseteq \mathbb{Z}$ is called an

1. *arithmetical multiprogression* (of period $(\delta_1, \ldots, \delta_\mu)$ with $0 = \delta_0 < \delta_1 < \ldots < \delta_\mu = d$, distance $d \in \mathbb{N}_+$ and period length $\mu \in \mathbb{N}_+$) if

$$L = \{m + \delta_0 + k_0 d, m + \delta_1 + k_1 d, \ldots, m + \delta_{\mu-1} + k_{\mu-1} d \mid k_i \in \mathbb{N} \text{ such that } m + \delta_i + k_i d \le \max L \text{ for } 0 \le i \le \mu - 1\}$$

where $m = \min L$,

2. *almost arithmetical* (*multi*)*progression* (of given period) bounded by $M \in \mathbb{N}_+$ if $L = L_1 \cup L^* \cup L_2$ where L^* is an arithmetical (multi)progression, $\max L_1 < \min L^*$, $\max L^* < \min L_2$ and $\#L_i \le M$ for every $1 \le i \le 2$.

If L is an arithmetical multiprogression with period $(\delta_1, \ldots, \delta_\mu)$, then L is the union of μ arithmetical progressions with difference $d = \delta_\mu$, and $\Delta(L) = \{\delta_i - \delta_{i-1} \mid 1 \le i \le \mu\}$ where $\delta_0 = 0$.

Next we define the key invariant for our investigations of finite sets of integers. For every $d \in \mathbb{N}_+$ set

$$\kappa_d(L) = \max\{\#(L \cap (m, m+d]) \mid m \in L\}.$$

Clearly,

$$\kappa_d(L) \le \frac{d}{\min \Delta(L)}.$$

We now present the main result of this section. Its proof will be done in a series of lemmata.

PROPOSITION 2.2. *Let $L \subseteq \mathbb{Z}$ be a finite set, $d \in \mathbb{N}_+$ and $\kappa = \kappa_d(L)$. Suppose there are sets $L_1, L_2 \subseteq \mathbb{Z}$ with $L_1 + L_2 \subseteq L$, $\min(L_1+L_2) = \min L$, $\max(L_1 + L_2) = \max L$, $\min \Delta(L_2) + \max \Delta(L_2) \le d$ and $L_1 = \{a, a+\delta_1, \ldots, a+\delta_\kappa\}$ where $0 = \delta_0 < \ldots < \delta_\kappa \le d$. Then $L = L_1 + L_2$ and L is an arithmetical multiprogression of period $(\delta_1, \ldots, \delta_\mu)$ for some $\mu \in \{1, \ldots, \kappa\}$. Furthermore, if $\Delta(L_2) \ne \emptyset$, then $\delta_\mu \in \Delta(L_2)$.*

LEMMA 2.3. *$L = L_1 + L_2$.*

Proof. Let $c \in L$ be given. We have to show that $c \in L_1 + L_2$. Set $L_2 = \{b_1, \ldots, b_k\}$ with $b_1 < \ldots < b_k$. Then $b_1 + a = \min(L_1 + L_2) = \min L \le c$. If $b_1 + a = c$, we are done. Otherwise, let $i \in \{1, \ldots, k\}$ be maximal with $b_i + a < c$. If $i = k$, then

$$b_i + a + d \ge b_i + a + \delta_\kappa = \max(L_1 + L_2) = \max L \ge c.$$

Let $i < k$; since $b_{i+1} - b_i \le \max \Delta(L_2) \le d$ and by the maximality of i, it follows that

$$b_i + a + d \ge b_{i+1} + a \ge c.$$

Hence, in both cases we have

$$\{c, b_i + a + \delta_1, \ldots, b_i + a + \delta_\kappa\} \subseteq L \cap (b_i + a, b_i + a + d].$$

Since

$$\#(L \cap (b_i + a, b_i + a + d]) \le \kappa_d(L) = \kappa,$$

we infer that

$$c \in \{b_i + a + \delta_1, \ldots, b_i + a + \delta_\kappa\} \subseteq L_1 + L_2. \ \blacksquare$$

LEMMA 2.4. *Let $b, b+\delta \in L_2$ with $0 < \delta \le d$. Then $\delta \in \{\delta_1, \ldots, \delta_\kappa\}$. In particular, $\Delta(L_2) \subseteq \{\delta_1, \ldots, \delta_\kappa\}$.*

Proof. Since $\max \Delta(L_2) \le d$, the second statement is an immediate consequence of the first. Since

$$\{b + a + \delta_1, \ldots, b + a + \delta_\kappa, b + a + \delta\} \subseteq L \cap (b + a, b + a + d]$$

and since

$$\#(L \cap (b + a, b + a + d]) \le \kappa,$$

it follows that $b + a + \delta \in \{b + a + \delta_i \mid 1 \le i \le \kappa\}$, whence $\delta \in \{\delta_1, \ldots, \delta_\kappa\}$. $\blacksquare$

LEMMA 2.5. *Suppose $\delta_\mu \in \Delta(L_2)$ for some $\mu \in \{1,\ldots,\kappa\}$. Then $\delta_{\mu k+j} = k\delta_\mu + \delta_j$ for all $0 \le j < \mu$ and all $k \ge 0$ with $\mu k + j \le \kappa$.*

Proof. Suppose that $b, b+\delta_\mu \in L_2$. Then

$$\begin{aligned}&\{a+(b+\delta_\mu), a+\delta_1+(b+\delta_\mu), \ldots, a+\delta_\kappa+(b+\delta_\mu)\} \cup \\ &\{a+\delta_\mu+b, a+\delta_\mu+(\delta_{\mu+1}-\delta_\mu)+b, \ldots, a+\delta_\mu+(\delta_\kappa-\delta_\mu)+b\} \\ \subseteq\ & L \cap [a+b+\delta_\mu, a+b+\delta_\mu+d].\end{aligned}$$

Since $\kappa = \kappa_d(L)$, it follows that

$$(*) \qquad \{\delta_i - \delta_\mu \mid \mu+1 \le i \le \kappa\} \subseteq \{\delta_1, \ldots, \delta_\kappa\}.$$

Now we shall prove that $\delta_\kappa - \delta_\mu < \delta_{\kappa-\mu+1}$. Assume to the contrary that $\delta_\mu + \delta_{\kappa-\mu+1} \le \delta_\kappa$. Then $b+a+\delta_1, \ldots, b+a+\delta_\mu$, $b+\delta_\mu+a+\delta_1, \ldots, b+\delta_\mu+a+\delta_{\kappa-\mu+1}$ are $\kappa+1$ pairwise distinct elements lying in $L \cap (b+a, b+a+d]$, a contradiction. Therefore, $\delta_\kappa - \delta_\mu < \delta_{\kappa-\mu+1}$ and hence $(*)$ gives

$$\{\delta_i - \delta_\mu \mid \mu+1 \le i \le \kappa\} \subseteq \{\delta_1, \ldots, \delta_{\kappa-\mu}\},$$

which implies

$$(**) \qquad \delta_{\mu+j} = \delta_\mu + \delta_j$$

for all $1 \le j \le \kappa - \mu$.

Finally, we verify the assertion of the lemma by induction on k. Clearly, it holds true for $k = 0$. Suppose $k \ge 1$ and pass from $k-1$ to k using $(**)$:

$$\begin{aligned}\delta_{\mu k+j} &= \delta_{\mu(k-1)+\mu+j} = \delta_\mu + \delta_{\mu(k-1)+j} \\ &= \delta_\mu + (k-1)\delta_\mu + \delta_j = k\delta_\mu + \delta_j. \ \blacksquare\end{aligned}$$

Proof of Proposition 2.2. Lemma 2.3 states that $L = L_1 + L_2$, and it remains to verify that L is an arithmetical multiprogression. Set $L_2 = \{b_1, \ldots, b_k\}$ with $b_1 < \ldots < b_k$. If $k = 1$, then $L = b_1 + L_1$ and the assertion holds with $\mu = \kappa$. Suppose $k \ge 2$; then $\Delta(L_2) \ne \emptyset$ and hence by Lemma 2.4 we have $\min \Delta(L_2) = \delta_\mu$ for some $\mu \in \{1, \ldots, \kappa\}$. For $1 \le r \le k$ set

$$L^{(r)} = \{b_i + a + \delta_j \mid 1 \le i \le r,\ 0 \le j \le \kappa\}.$$

Then $L^{(k)} = L_1 + L_2 = L$ and hence it is sufficient to verify that

$$\begin{aligned}L^{(r)} = \{m + k_0\delta_\mu, m+\delta_1+k_1\delta_\mu, \ldots, m+\delta_{\mu-1}+k_{\mu-1}\delta_\mu \mid k_i \in \mathbb{N} \text{ such that} \\ m+\delta_i+k_i\delta_\mu \le \max L^{(r)} \text{ for every } 0 \le i \le \mu-1\}\end{aligned}$$

with $m = a + b_1$. We proceed by induction on r.

Using Lemma 2.5 we infer that

$$\begin{aligned}
L^{(1)} &= \{b_1 + a + \delta_i \mid 0 \le i \le \kappa\} \\
&= \{b_1 + a + k\delta_\mu + \delta_j \mid 0 \le j \le \mu - 1,\ k \ge 0 \text{ with } \mu k + j \le \kappa\} \\
&= \{m + k_0\delta_\mu, m + \delta_1 + k_1\delta_\mu, \ldots, m + \delta_{\mu-1} + k_\mu\delta_\mu \mid k_i \ge 0 \text{ such that} \\
&\qquad\qquad m + \delta_i + k_i\delta_\mu \le m + \delta_\kappa = \max L^{(1)}\}.
\end{aligned}$$

Let $r \ge 2$ and suppose the assertion is true for $r - 1$. We have

$$\begin{aligned}
L^{(r)} &= L^{(r-1)} \cup \{b_r + a + \delta_i \mid 0 \le i \le \kappa\} \\
&= \{m + k_0\delta_\mu, m + \delta_1 + k_1\delta_\mu, \ldots, m + \delta_{\mu-1} + k_{\mu-1}\delta_\mu \mid k_i \ge 0 \text{ such that} \\
&\qquad\qquad m + \delta_i + k_i\delta_\mu \le \max L^{(r-1)} = b_{r-1} + a + \delta_\kappa\} \\
&\quad \cup \{b_r + a + k_0\delta_\mu, \ldots, b_r + a + \delta_{\mu-1} + k_{\mu-1}\delta_\mu \mid k_i \ge 0 \text{ such that} \\
&\qquad\qquad b_r + a + \delta_i + k_i\delta_\mu \le b_r + a + \delta_\kappa = \max L^{(r)}\}.
\end{aligned}$$

Therefore, it is sufficient to show that, for every $0 \le i \le \mu - 1, c_i = b_r + a + \delta_i \in L^{(r-1)}$. Let $i \in \{0, \ldots, \mu - 1\}$. Since $d \ge \max \Delta(L_2) + \min \Delta(L_2)$ and $\delta_i < \delta_\mu = \min \Delta(L_2)$ it follows that

$$b_r - b_{r-1} + \delta_i \le \max \Delta(L_2) + \delta_i < d,$$

whence

$$c_i = b_{r-1} + a + (b_r - b_{r-1} + \delta_i) \in L \cap (b_{r-1} + a, b_{r-1} + a + d].$$

On the other hand, we have

$$\begin{aligned}
\{b_{r-1} + a + \delta_1, \ldots, b_{r-1} + a + \delta_\kappa\} &\subseteq L^{(r-1)} \cap (b_{r-1} + a, b_{r-1} + a + d] \\
&\subseteq L \cap (b_{r-1} + a, b_{r-1} + a + d].
\end{aligned}$$

Because $\#(L \cap (b_{r-1} + a, b_{r-1} + a + d]) \le \kappa$, the three sets are equal, which implies that $c_i \in L^{(r-1)}$. ∎

3. A structure theorem for sets of lengths. Throughout this paper, monoids are assumed to be commutative and cancellative. If not stated otherwise, we shall use multiplicative notation. Let H be a monoid. Then $H^\times$ denotes the group of invertible elements, and H is called *reduced* if $H^\times = \{1\}$. The monoid $H_{\mathrm{red}} = H/H^\times$ is the associated reduced monoid of H. The irreducible elements of H are called *atoms* and $\mathcal{A}(H)$ is the set of atoms. For a subset $H' \subseteq H$ we denote by $[H']$ the submonoid of H generated by H', and we say that $H' \subseteq H$ is *divisor closed* if $a \in H$, $b \in H'$ and $a \mid b$ implies that $a \in H'$. The monoid H is called *atomic* if $H = [\mathcal{A}(H) \cup H^\times]$.

Suppose that H is atomic and let $a \in H$. If $a = u_1 \ldots u_k$ with $u_1, \ldots, u_k \in \mathcal{A}(H)$, we say that k is the *length* of the factorization. The set $L(a) \subseteq \mathbb{N}$ of all possible k is called the *set of lengths* of a. If $a \in H^\times$, then set $L(a) = \{0\}$, and $L(a)=\{1\}$ if $a\in\mathcal{A}(H)$. Define

$$\mathcal{L}(H)=\{L(a)\mid a\in H\}$$

as the *system of sets of lengths*. H is called a *BF-monoid* (bounded factorization monoid) if all $L\in\mathcal{L}(H)$ are finite and in this case we set

$$\Delta(H)=\Delta(\mathcal{L}(H))\subseteq\mathbb{N}_+.$$

Let H be a BF-monoid with finite, non-empty set of differences $\Delta(H)$. Let $r\ge 1$ and $\mathbf{d}=(d_1,\ldots,d_r)\in\Delta(H)^r$; set

$$\begin{aligned}\Phi_{\mathbf{d}}(H)=\{a\in H\mid{}&\text{there exist } m_0,\ldots,m_r \text{ with } m_i-m_{i-1}=d_i\\ &\text{for } 1\le i\le r \text{ such that } \{m_0,\ldots,m_r\}\subseteq L(a)\}.\end{aligned}$$

Clearly, $\Phi_{\mathbf{d}}(H)$ is an ideal in H.

For $a\in\Phi_{\mathbf{d}}(H)$ let $\varphi_{\mathbf{d}}(a)\in\mathbb{N}$ be defined as the minimum of all $N\in\mathbb{N}$ such that there exists some $a^*\in\Phi_{\mathbf{d}}(H)$ with $a=a^*b$ satisfying

$$\max L(a^*b)-\min L(a^*)-\max L(b)\le N$$

and

$$\min L(b)+\max L(a^*)-\min L(a^*b)\le N.$$

Further, set

$$\varphi_{\mathbf{d}}(H)=\sup\{\varphi_{\mathbf{d}}(a)\mid a\in\Phi_{\mathbf{d}}(H)\}\in\mathbb{N}\cup\{\infty\}$$

and

$$\varphi(H)=\max\left\{\varphi_{\mathbf{d}}(H)\;\middle|\;\mathbf{d}\in\Delta(H)^r,\ 1\le r\le 2\frac{\max\Delta(H)}{\min\Delta(H)}\right\}.$$

LEMMA 3.1. *Let H be an atomic monoid and $S\subseteq H$ a divisor closed submonoid.*

1. *$\mathcal{A}(S)=S\cap\mathcal{A}(H)$ and S is atomic. For every $a\in S$, $L_H(a)=L_S(a)$, $\Delta(S)\subseteq\Delta(H)$ and if H is a BF-monoid, then so is S.*
2. *$\varphi(S)\le\varphi(H)$.*

Proof. 1. Obvious.

2. It is sufficient to show that $\varphi_{\mathbf{d}}(S)\le\varphi_{\mathbf{d}}(H)$ for every $\mathbf{d}\in\Delta(S)^r$ with

$$1\le r\le 2\frac{\max\Delta(S)}{\min\Delta(S)}\le 2\frac{\max\Delta(H)}{\min\Delta(H)}.$$

Fix such a $\mathbf{d}$. Since $\Phi_{\mathbf{d}}(S)=\Phi_{\mathbf{d}}(H)\cap S$, it follows from the very definition that $\varphi_{\mathbf{d}}(S)\le\varphi_{\mathbf{d}}(H)$. ∎

THEOREM 3.2 (Structure Theorem for Sets of Lengths). *Let H be a BF-monoid with finite, non-empty set $\Delta(H)$ and with $\varphi(H)<\infty$. Let $a\in H$.*

1. *The set of lengths $L(a)$ is an almost arithmetical multiprogression of some distance $\delta\in\Delta(H)$ bounded by $\varphi(H)$.*

2. *If $L(a)$ contains an arithmetical progression with difference* $\min \Delta(H)$ *and of length* $2\frac{\max \Delta(H)}{\min \Delta(H)}$, *then the sets of lengths of multiples of a are almost arithmetical progressions with difference* $\min \Delta(H)$ *bounded by* $\varphi(H)$.

3. *There exists some* $\psi(a) \in \mathbb{N}_+$ *such that for all* $b \in H$ *with* $a^{\psi(a)} \mid b \mid a^k$ *for some* $k \ge \psi(a)$ *the sets* $L(b)$ *are almost arithmetical progressions with the same difference* $\delta \in \Delta(H)$ *bounded by* $\varphi(H)$.

Proof. 1. Define $d = 2\max \Delta(H)$, $\kappa = \kappa_d(L(a))$ and let $\{m, m+\delta_1, \ldots, m+\delta_\kappa\} \subseteq L(a)$ with $0 = \delta_0 < \delta_1 < \ldots < \delta_\kappa \le d$. By definition of κ it follows that $d_i = \delta_i - \delta_{i-1} \in \Delta(H)$ for every $1 \le i \le \kappa$. Set $\mathbf{d} = (d_1, \ldots, d_\kappa) \in \Delta(H)^\kappa$ and recall that $\kappa \le \frac{1}{\min \Delta(L(a))} d \le \frac{1}{\min \Delta(H)} d$. Choose $a^* \in \Phi_{\mathbf{d}}(H)$ with $a = a^* b$ for some $b \in H$ such that

$$\max L(a) - \min L(a^*) - \max L(b) \le \varphi(H)$$

and

$$\min L(b) + \max L(a^*) - \min L(a) \le \varphi(H).$$

Set $L_2 = L(b)$; obviously, there is some $n \in \mathbb{N}_+$ such that

$$L_1 = \{n, n+\delta_1, \ldots, n+\delta_\kappa\} \subseteq L(a^*).$$

If $\Delta(L_2) = \emptyset$, then $L = L_2 + \{n, n+\delta_1\}$ is an arithmetical progression with difference $\delta_1 \in \Delta(H)$. Suppose $\Delta(L_2) \ne \emptyset$ and define

$$L = L(a) \cap [\min(L_1 + L_2), \max(L_1 + L_2)].$$

Then $L_1 + L_2 \subseteq L$, $\min L = \min(L_1 + L_2)$, $\max L = \max(L_1 + L_2)$ and $\kappa_d(L) = \kappa_d(L(a))$. Therefore, by Proposition 2.2, $L = L_1 + L_2$ is an arithmetical multiprogression of period $(\delta_1, \ldots, \delta_\mu)$ and distance $\delta_\mu \in \Delta(L_2) \subseteq \Delta(H)$ for some $1 \le \mu \le \kappa$. In both cases we infer that

$$\max L(a) - \max L \le \max L(a) - \min L_1 - \max L(b) \le \varphi(H)$$

and

$$\min L - \min L(a) = \min L_1 + \min L(b) - \min L(a) \le \varphi(H).$$

2. If $L(a)$ contains such an arithmetical progression, then the same is true for $L(ab)$ for every $b \in H$. Hence it is sufficient to prove the assertion for $L(a)$. Using the above notations the assumption gives $\delta_i = i \min \Delta(H)$ for $1 \le i \le \kappa$. Hence $L(a)$ is an almost arithmetical multiprogression of distance $\delta_\mu = \mu \min \Delta(H)$ and period $(\delta_1, \ldots, \delta_\mu)$, i.e., it is an almost arithmetical progression with difference $\min \Delta(H)$.

3. Clearly, $S = \{b \in H \mid b \text{ divides some power of } a\}$ is a divisor closed submonoid of H. Lemma 3.1 implies that S is a BF-monoid with $\Delta(S) \subseteq \Delta(H), \varphi(S) \le \varphi(H)$ and $L_S(b) = L_H(b)$ for every $b \in S$. Therefore, we may study factorizations of elements of S in S instead of H and apply part 2 of the Theorem for the monoid S. Obviously, $\min \Delta(S) = \min \Delta(\{L(a^n) \mid n \in$

$\mathbb{N}_+\}$). If $\Delta(S) = \emptyset$, nothing has to be proved. So, suppose $\min \Delta(L(a^k)) = \min \Delta(S) = \delta$, and set $\psi(a) = 2k\frac{\max \Delta(S)}{\min \Delta(S)}$. Then $L(a^{\psi(a)})$ contains an arithmetical progression with difference δ and length $2\frac{\max \Delta(S)}{\min \Delta(S)}$. Thus, part 2 implies the assertion. ∎

In Section 8 we are going to discuss how this abstract Structure Theorem can be applied to monoids of arithmetical relevance. These will include Krull monoids with finite divisor class group, such as rings of integers in algebraic number fields. Apart from factorial monoids the arithmetic of such Krull monoids is best understood and is considered to be simplest.

Our next aim in this section is to prove a Realization Theorem. We show that for every period and every $M \in \mathbb{N}_+$ there exists a Krull monoid with finite class group G which has arbitrarily long sets of lengths being almost arithmetical multiprogressions of given period and with bound not less than M.

It is sufficient to prove such a result for the classical block monoid $\mathcal{B}(G)$ which was introduced by W. Narkiewicz in [Na1]. We use standard notations (cf. [HK2; Section 5]). In particular, we have $\mathcal{B}(G) \subseteq \mathcal{F}(G)$, where $\mathcal{F}(G)$ is the free abelian monoid with basis G, and we write $\mathcal{L}(G)$ instead of $\mathcal{L}(\mathcal{B}(G))$.

LEMMA 3.3. *Let $a_1, a_2 \in \mathbb{N}_+$ with* $\gcd(a_1, a_2) = d$ *and $k \in \mathbb{N}_+$ with $k \ge a_1$. Then*

$$\begin{aligned} L &= \{m_1a_1 + m_2a_2 \mid 0 \le m_1, m_2 \le k\} \\ &= \{x_1, \ldots, x_\alpha, y, y+d, \ldots, y+ld, z_1, \ldots, z_\beta\} \end{aligned}$$

where $0 = x_1 < \ldots < x_\alpha$, $z_1 < \ldots < z_\beta$, $y - x_\alpha \ge 2d$, $z_1 - (y+ld) \ge 2d$ *and* $\alpha = \beta = (a_1/d - 1)(a_2/d - 1)/2$.

Proof. Obviously, it is sufficient to consider the case $d = 1$.

Set $A = \{a_1, a_2\}$ and consider the linear form $f = a_1X_1 + a_2X_2$. Then the *Frobenius number* $g(A)$ is defined as the largest integer $g \in \mathbb{N}_+$ which is not represented by f. Let $n(A)$ denote the number of positive integers which are not represented by f. It is well known that

$$g(A) = (a_1 - 1)(a_2 - 1) - 1 \quad \text{and} \quad n(A) = \frac{g(A) + 1}{2}$$

(cf. [Sc; p. 435]). Therefore, if we set

$$\{m_1a_1 + m_2a_2 \mid m_1, m_2 \in \mathbb{N}\} = \{0 = x_1, x_2, \ldots, x_\alpha, y, y+1, y+2, \ldots\}$$

with $x_1 < \ldots < x_\alpha$, $y - x_\alpha \ge 2$, then $g(A) = y - 1$, $n(A) = y - 1 - (\alpha - 1)$, whence $\alpha = y - n(A) = (g(A) + 1)/2$. In other words, $\alpha - 1$ is the number of positive integers below $g(A) + 1$ which are represented by f.

Obviously, $k \geq a_1$ implies that $y = g(A) + 1 \in L$ and we may set

$$L = \{0 = x_1, \ldots, x_\alpha, y, y+1, \ldots, y+l, z_1, \ldots, z_\beta\}$$

with $z_1 < \ldots < z_\beta$ and $z_1 - (y+l) \geq 2$. Since

$$\begin{aligned} L &= \{(k-m_1)a_1 + (k-m_2)a_2 \mid 0 \leq m_1, m_2 \leq k\} \\ &= ka_1 + ka_2 - \{m_1a_1 + m_2a_2 \mid 0 \leq m_1, m_2 \leq k\} \\ &= z_\beta - L = \{0, z_\beta - z_{\beta-1}, \ldots, z_\beta - z_1, z_\beta - (y+l), \ldots\} \end{aligned}$$

and

$$z_\beta - (y+l) - (z_\beta - z_1) = z_1 - (y+l) \geq 2,$$

it follows that $x_\alpha = z_\beta - z_1$, whence $\alpha = \beta$. ■

The following result was achieved by F. Kainrath in [Ka].

PROPOSITION 3.4. 1. *Let G be an infinite abelian group. Then every $L \subseteq \mathbb{N}_+ \setminus \{1\}$ lies in $\mathcal{L}(G)$. Thus, $\mathcal{L}(G) = \mathbb{P}_{\mathrm{fin}}(\mathbb{N}_+ \setminus \{1\}) \cup \{\{0\}, \{1\}\}$.*

2. *For every finite set $L \subseteq \mathbb{N}_+ \setminus \{1\}$ there exists some $N \in \mathbb{N}_+$ such that $L \in \mathcal{L}(G)$ for every cyclic group G with $\#G \geq N$.*

Proof. 1. See Theorem 1 in [Ka].

2. This is a consequence of part 1 in the case $G = \mathbb{Z}$. For details see [Ka; part 2 of the proof of the Theorem]. ■

THEOREM 3.5 (A Realization Theorem). *Let $\mu \in \mathbb{N}_+$, $(\delta_1, \ldots, \delta_\mu) \in \mathbb{N}^\mu$ with $0 = \delta_0 < \delta_1 < \ldots < \delta_\mu = d$ and $M \in \mathbb{N}$. Then there exists a finite abelian group G having the following property: for every sufficiently large $k \in \mathbb{N}_+$ there is some $L_k \in \mathcal{L}(G)$ with $\#L_k \geq k$ such that*

$$\begin{aligned} L_k = \{x_1, \ldots, x_\alpha, \quad & y, \quad \ldots, \quad y + \delta_{\mu-1}, \\ & y+d, \ \ldots, \ y + \delta_{\mu-1} + d, \\ & \vdots \\ & y + ld, \ldots, y + \delta_{\mu-1} + ld, z_1, \ldots, z_\beta\}, \end{aligned}$$

where $x_1 < \ldots < x_\alpha$, $z_1 < \ldots < z_\beta$, $y - x_\alpha \geq 2d - \delta_{\mu-1}$, $z_1 - (y + ld + \delta_{\mu-1}) \geq 2d - \delta_{\mu-1}$ and $M \leq \alpha, \beta \leq \mu M$, i.e., L_k is an almost arithmetical multiprogression of given period $(\delta_1, \ldots, \delta_\mu)$ bounded by μM but not by $(M-1)$.

Proof. 1. We prove the assertion in the case $\mu = 1$. Suppose $M \geq 1$. There are integers $n_1 \geq n_2 \geq 4$ such that

$$M = \frac{1}{2}\left(\frac{n_1 - 2}{d} - 1\right)\left(\frac{n_2 - 2}{d} - 1\right)$$

and $d = \gcd(n_1 - 2, n_2 - 2)$ (e.g. choose $n_1 = (2M+1)d + 2$ and $n_2 = 2d + 2$). For $1 \leq i \leq 2$ let $g_i \in C_{n_i}$ with $\mathrm{ord}(g_i) = n_i$, $B_i = (-g_i)^{n_i} g_i^{n_i}$ and obviously

$$L(B_i^k) = \{2k, 2k + (n_i - 2), \ldots, 2k + k(n_i - 2)\}$$

for every $k \ge 1$. Set $G' = C_{n_1} \oplus C_{n_2}$ and $A_k = B_1^k B_2^k$. Then $L'_k = L(A_k) \in \mathcal{B}(G')$ and

$$L'_k = L(B_1^k) + L(B_2^k) = 4k + \{m_1(n_1 - 2) + m_2(n_2 - 2) \mid 0 \le m_1, m_2 \le k\}.$$

By Lemma 3.3 it follows that, for sufficiently large k,

$$-4k + L'_k = \{u_1, \ldots, u_r, v, \ldots, v + ld, w_1, \ldots, w_r\}$$

with $0 = u_1 < \ldots < u_r$, $w_1 < \ldots < w_r$, $v - u_r \ge 2d$, $w_1 - (v + ld) \ge 2d$, $r = M$ and $\# L'_k \ge k$.

If $M = 0$, set $n_1 = d + 2$, $G' = C_{n_1}$, B_1 as above and $A'_k = B_1^k$. Then $L'_k = L(A'_k)$ has the required form.

2. Suppose $\mu \ge 2$. By Proposition 3.4 there is some $n_3 \in \mathbb{N}_+$ and a block $B_3 \in \mathcal{B}(C_{n_3})$ such that

$$L(B_3) = \{2, 2 + \delta_1, \ldots, 2 + \delta_{\mu-1}\}.$$

Define $G = G' \oplus C_{n_3}$ and $L_k = L(A_k B_3)$. Then $L_k = L(A_k) + L(B_3)$ and

$$-(4k + 2) + L_k = L^{(1)} \mathbin{\dot\cup} L^{(2)} \mathbin{\dot\cup} L^{(3)}$$

where

$$\begin{aligned} L^{(1)} &= \{u_i + \delta_j \mid 1 \le i \le r,\ 0 \le j \le \mu - 1\}, \\ L^{(2)} &= \{v + \mathrm{id} + \delta_j \mid 0 \le i \le l,\ 0 \le j \le \mu - 1\}, \\ L^{(3)} &= \{w_i + \delta_j \mid 1 \le i \le r,\ 0 \le j \le \mu - 1\}. \end{aligned}$$

Write L_k as in the formulation of the theorem and define

$$x_\alpha = (4k + 2) + \max L^{(1)}, \quad y = (4k + 2) + v, \\ z_1 = (4k + 2) + \min L^{(3)}.$$

Then

$$M = r \le \# L^{(1)} = \alpha \le \mu M, \quad M = r \le \# L^{(3)} = \beta \le \mu M, \\ y - x_\alpha = v - \max L^{(1)} = v - (u_r + \delta_{\mu-1}) \ge 2d - \delta_{\mu-1}$$

and

$$\begin{aligned} z_1 - (y + ld + \delta_{\mu-1}) &= \min L^{(3)} - (v + ld + \delta_{\mu-1}) \\ &= w_1 - (v + ld) - \delta_{\mu-1} \ge 2d - \delta_{\mu-1}. \ \blacksquare \end{aligned}$$

REMARKS. Let G be the group in Theorem 3.5.

1. Admitting weaker bounds for α and β we may choose G to be either cyclic or a p-group for any given prime p.

2. Let H be a Krull monoid with class group G such that each class contains a prime divisor. Then by [Ge1; Proposition 1] we have $\mathcal{L}(H) = \mathcal{L}(G)$, whence the above result holds for H.

3. Class field theory shows that there exists a cyclic algebraic number field K with ring of integers $\mathfrak{o}_K$ whose ideal class group contains G (cf.

[Wa; Corollary 3.9]). Thus $\mathcal{L}(G) \subseteq \mathcal{L}(\mathfrak{o}_K)$ and the above sets L_k stem from algebraic integers $a_k \in \mathfrak{o}_K$.

4. Tamely generated subsets. We introduce the notion of tamely generated subsets. BF-monoids H with finite sets $\Delta(H)$ and for which the sets $\Phi_{\mathbf{d}}(H)$ are tamely generated satisfy $\varphi(H) < \infty$ and thus the Structure Theorem for Sets of Lengths holds (Proposition 4.8). This will be the key result for applying the abstract Theorem 3.2 to concrete monoids (cf. Section 8). We start with some monoid-theoretical preparations.

For a set P let $\mathcal{F}(P)$ denote the free abelian monoid with basis P. Every element $a \in \mathcal{F}(P)$ will be written in the form

$$a = \prod_{p \in P} p^{n_p} \in \mathcal{F}(P)$$

with $n_p = v_p(a) \in \mathbb{N}$ and $n_p = 0$ for all but finitely many $p \in P$. We set $\sigma(a) = \sum_{p \in P} v_p(a) \in \mathbb{N}$.

Let H be an atomic monoid. The free abelian monoid

$$\mathcal{Z}(H) = \mathcal{F}(\mathcal{A}(H_{\mathrm{red}}))$$

with basis $\mathcal{A}(H_{\mathrm{red}})$ is called the *factorization monoid* of H. Let $\pi = \pi_H : \mathcal{Z}(H) \to H_{\mathrm{red}}$ denote the canonical homomorphism. Since H is atomic, π is surjective. For an element $a \in H$ the elements of

$$\mathcal{Z}_H(a) = \mathcal{Z}(a) = \pi^{-1}(aH^{\times}) \subseteq \mathcal{Z}(H)$$

are called *factorizations* of a. H is said to be an *FF-monoid* (finite factorization monoid) if for every $a \in H$ the set $\mathcal{Z}(a)$ is finite. The distance function $d : \mathcal{Z}(H) \times \mathcal{Z}(H) \to \mathbb{N}$ is defined by

$$d(z, z') = \max\left\{\sigma\left(\frac{z}{\gcd(z, z')}\right), \sigma\left(\frac{z'}{\gcd(z, z')}\right)\right\} \in \mathbb{N}$$

for two factorizations $z, z' \in \mathcal{Z}(H)$. It has all expected properties of a distance function (cf. [Ge3; Lemma 3.1]). In particular, we shall use the fact that

$$|\sigma(z) - \sigma(z')| \le d(z, z')$$

for every $z, z' \in \mathcal{Z}(H)$.

DEFINITION 4.1. Let H be an atomic monoid and $H' \subseteq H$ a subset.

1. The *tame degree* $t_H(H', X)$ of H' with respect to a set $X \subseteq \mathcal{Z}(H)$ is the minimum of all $N \in \mathbb{N} \cup \{\infty\}$ having the following property: if $a \in H'$, $z \in \mathcal{Z}(a)$ and $x \in X$ is a factorization of a divisor of a, then there exists a factorization $z' \in \mathcal{Z}(a)$ with $x \mid z'$ (in $\mathcal{Z}(H)$) and $d(z, z') \le N$.

2. We say that H' is *locally tame* if $t_H(H', \mathcal{Z}(a)) < \infty$ for all $a \in H$; H' is called *tame* if the *tame degree*

$$t(H') = t_H(H', \mathcal{A}(H_{\mathrm{red}})) < \infty.$$

The concept of tameness of factorizations was already used successfully in [Ge3, Ge4]. However, in this paper we have strengthened the notion of local tameness. It coincides with the old one for FF-monoids; furthermore, tame FF-monoids are locally tame. This can be easily seen by the following (trivial) lemma, which will be used without further mention.

LEMMA 4.2. *Let H be a reduced atomic monoid.*

1. *For every $H' \subseteq H$ and $X \subseteq \mathcal{Z}(H)$ we have*

$$t_H(H', X) = \sup\{t_H(H', x) \mid x \in X\} \le \sup\{\sup L_H(a) \mid a \in H'\}.$$

2. *If $H' \subseteq H$ is divisor closed and $x_1, \ldots, x_r \in \mathcal{Z}(H)$, then*

$$t\Big(H', \prod_{i=1}^{r} x_i\Big) \le \sum_{i=1}^{r} t(H', x_i).$$

3. *Suppose $H = H_1 \times H_2$, $M \in \mathbb{N}_+$, $H' = \{a = a_1a_2 \in H \mid \max L_{H_2}(a_2) \le M\}$ and $X \subseteq \mathcal{Z}(H_1)$ finite. If H is a locally tame monoid, then $t_H(H', X\mathcal{Z}(H_2)) < \infty$.*

Proof. Parts 1 and 2 follow immediately from the definition.

3. Since X is finite, there is a finite set $B \subseteq H$ such that $X \subseteq \bigcup_{b\in B} \mathcal{Z}(b)$. Let $a = a_1a_2 \in H'$ and $z = xy \in X\mathcal{Z}(H_2)$. Then by parts 1 and 2 we have

$$\begin{aligned} t_H(a, z) &= t_{H_1}(a_1, x) + t_{H_2}(a_2, y) \\ &\le t_{H_1}(a_1, X) + M \le \max\{t_{H_1}(a_1, \mathcal{Z}(b)) \mid b \in B\} + M < \infty, \end{aligned}$$

which implies the assertion. ∎

Let H be a monoid. We say that H satisfies the *ACCP* (ascending chain condition for principal ideals) if every ascending chain of principal ideals becomes stationary (equivalently, every non-empty set of principal ideals contains a maximal element with respect to inclusion). Let $E \subseteq I \subseteq H$ be subsets. If $I \subseteq EH$, then E is called a *generating system* of I. E is said to be a *minimal generating system* of I if no proper subset is a generating system. If E is a generating system of I, then it is also a generating system of IH. We say that I is *finitely generated* if it has a finite generating system.

LEMMA 4.3. *Let H be a monoid and $I \subseteq H$ a subset.*

1. *For a subset $E \subseteq I$ whose elements are pairwise non-associated, the following conditions are equivalent*:

   (a) *$\{eH \mid e \in E\}$ is the set of maximal elements of $\{aH \mid a \in I\}$ with respect to inclusion.*

(b) *E is a minimal generating system of I.*

2. *If E and E' are minimal generating systems of I, then $EH^\times = E'H^\times$.*

3. *If H satisfies the ACCP, then every generating system of I contains a minimal generating system.*

Proof. 1. Straightforward.

2. In a minimal generating system elements are pairwise non-associated. Therefore, 1 implies that $\{eH \mid e \in E\} = \{e'H \mid e' \in E'\}$, whence the assertion follows.

3. Let $E \subseteq I$ be a generating system of I. It is sufficient to find a minimal generating system for E. Since H satisfies ACCP, the set $\{eH \mid e \in H\}$ contains maximal elements which implies the assertion by 1. ∎

Definition 4.5. Let H be an atomic monoid and $I \subseteq H$ a subset. A generating system $E \subseteq I$ is said to be

(a) *of bounded length* if $\sup\{\sup L(e) \mid e \in E\} < \infty$.

(b) *tame in H*, or a *tame generating system* (for I and with bound $N \in \mathbb{N}$), if for every $a \in I$ there exists some $e \in E$ dividing a such that $t_H(a, \mathcal{Z}(e)) \le N$.

We say that I is *tamely generated* if it has a tame generating system.

Lemma 4.6. *Let H be an atomic monoid and $I \subseteq H$ a subset.*

1. *$I \subseteq H$ is tamely generated if and only if $I_{\mathrm{red}} \subseteq H_{\mathrm{red}}$ is tamely generated.*

2. *Let $E' \subseteq E \subseteq I$ be two generating systems. If E is a tame generating system, then so is E'.*

3. *If H satisfies the ACCP and IH is tamely generated, then so is I.*

Proof. 1. This follows immediately from the definition.

2. Suppose that E is a tame generating system for I with bound $N \in \mathbb{N}_+$. Let $a \in H$; then there is some $e \in E$ dividing a such that $t(a, \mathcal{Z}(e)) \le N$. Since E' is a generating system, there is some $e' \in E'$ dividing e. Therefore, we infer that $e' \mid e \mid a$ and clearly

$$t(a, \mathcal{Z}(e')) \le t(a, \mathcal{Z}(e)) \le N.$$

3. By part 1 we may suppose that H is reduced. Let E be a tame generating system for IH. By Lemma 4.3.2, IH has a unique minimal generating system E^* and by 4.3.3 it follows that $E^* \subseteq E$ and $E^* \subseteq I$. From part 2 we infer that E^* is a tame generating system for IH and hence for I. ∎

Proposition 4.7. *Let H be a locally tame monoid.*

1. *Every finitely generated subset is tamely generated.*

2. *If H is finitely generated, then every subset is tamely generated.*

3. *If H is tame, then every generating system of bounded length is tame.*

Proof. 1. Let $I \subseteq H$ be generated by a finite set $E \subseteq I$. Then for every $a \in I$ there is some $a^* \in E$ dividing a such that

$$t(a, \mathcal{Z}(a^*)) \le t(H, \mathcal{Z}(a^*)) \le \max\{t(H, \mathcal{Z}(e)) \mid e \in E\} < \infty,$$

since H is locally tame.

2. Finitely generated monoids satisfy the ACCP and every ideal is finitely generated (cf. [Gi; Theorems 5.1 and 7.8]). Hence, by Lemma 4.6 it is sufficient to consider ideals instead of arbitrary subsets and thus 1 implies the assertion.

3. Let $I \subseteq H$ be a subset, $E \subseteq I$ a generating system, $a \in I$ and $e \in E$ dividing a. Then, by Lemma 4.2.2,

$$\begin{aligned} t(a, \mathcal{Z}(e)) &\le t(H, \mathcal{Z}(e)) \\ &\le \sup\{\sup L(e) \mid e \in E\} \cdot \sup\{t(H, u) \mid u \in \mathcal{A}(H_{\mathrm{red}})\} \\ &= \sup\{\sup L(e) \mid e \in E\} \cdot t(H). \ \blacksquare \end{aligned}$$

Our interest in tamely generated subsets is motivated by the following result.

PROPOSITION 4.8. *Let H be a BF-monoid with finite, non-empty set $\Delta(H)$. If for every $1 \le r \le 2\frac{\max \Delta(H)}{\min \Delta(H)}$ and every $\mathbf{d} \in \Delta(H)^r$ the set $\Phi_{\mathbf{d}}(H)$ is tamely generated, then $\varphi(H) < \infty$. Thus the Structure Theorem for Sets of Lengths holds.*

Proof. Let $1 \le r \le 2\frac{\max \Delta(H)}{\min \Delta(H)}$ and $\mathbf{d} \in \Delta(H)^r$. Suppose that $\Phi_{\mathbf{d}}(H)$ is tamely generated with bound $N \in \mathbb{N}_+$, i.e., there exists a generating system $E \subseteq \Phi_{\mathbf{d}}(H)$ such that for every $a \in H$ there is some $a^* \in E$ with $a^* \mid a$ and $t(a, \mathcal{Z}(a^*)) \le N$.

Let $a \in H$; we show that for every divisor a^* of a with $a = a^* b$ the following two assertions hold:

(i) $\max L(a) - \min L(a^*) - \max L(b) \le t(a, \mathcal{Z}(a^*))$,
(ii) $\min L(b) + \max L(a^*) - \min L(a) \le t(a, \mathcal{Z}(a^*))$.

Hence by the very definition of $\varphi_{\mathbf{d}}(a)$ it follows that $\varphi_{\mathbf{d}}(a) \le N$. Therefore, we have $\varphi_{\mathbf{d}}(H) \le N$ and hence $\varphi(H) < \infty$. It remains to prove (i) and (ii).

(i) Choose some $z \in \mathcal{Z}(a)$ with $\sigma(z) = \max L(a)$ and some $u \in \mathcal{Z}(a^*)$ with $\sigma(u) = \min L(a^*)$. Then there exists a factorization $z' = uw \in \mathcal{Z}(a)$ with $d(z, z') \le t(a, u)$. Hence,

$$\begin{aligned} \max L(a) - \min L(a^*) - \max L(b) &\le \sigma(z) - \sigma(u) - \sigma(w) = \sigma(z) - \sigma(z') \\ &\le d(z, z') \le t(a, u) \le t(a, \mathcal{Z}(a^*)). \end{aligned}$$

(ii) Choose some $z \in \mathcal{Z}(a)$ with $\sigma(z) = \min L(a)$ and some $v \in \mathcal{Z}(a^*)$ with $\sigma(v) = \max L(a^*)$. Similarly to (i), there exists a factorization $z' =$

$vw \in \mathcal{Z}(a)$ with $d(z,z') \le t(a,v)$, which implies that

$$\begin{aligned}\min L(b) + \max L(a^*) - \min L(a) &\le \sigma(w) + \sigma(v) - \sigma(z) = \sigma(z') - \sigma(z) \\ &\le d(z,z') \le t(a,v) \le t(a, \mathcal{Z}(a^*)). \ \blacksquare\end{aligned}$$

5. Strongly primary monoids. Inspired by N. Bourbaki (cf. p. 298 of [Bo]) we define strongly primary ideals in monoids and introduce a new class of monoids, called strongly primary monoids. The main examples we have in mind stem from ring theory. They will be discussed in Lemmata 9.1 and 9.2.

Let D be a monoid. A submonoid $H \subseteq D$ is said to be *saturated* if $a, b \in H$ and $a \mid b$ in D implies that $a \mid b$ in H. Therefore, $H \subseteq D$ is saturated if and only if $H_{\rm red} \subseteq D_{\rm red}$ is saturated. The factor group G of the quotient groups of D and H is called the *class group* of $H \subseteq D$. Class groups will be written additively. For $a \in D$ we denote by $[a] \in G$ the class of a; obviously, we have $[a] = 0 \in G$ if and only if $a \in H$. Suppose that D is reduced. For an element $x = \prod_{i=1}^r u_i \in \mathcal{Z}_D(a) \subseteq \mathcal{Z}(D)$ with $u_1, \ldots, u_r \in \mathcal{A}(D)$ we set $[x] = \prod_{i=1}^r [u_i] \in \mathcal{F}(G)$. Clearly, we have $a \in H$ if and only if $[x] \in \mathcal{B}(G)$.

Primary ideals and monoids were studied in [Ge5]. We repeat their definition and point out their relationship with strongly primary ideals and monoids.

Definition 5.1. Let H be a monoid with $H \ne H^\times$ and let $\mathfrak{m} = H \setminus H^\times$ denote the unique maximal ideal.

1. The monoid H is said to be

(i) *primary* if for every $a, b \in H \setminus H^\times$ we have $a \mid b^n$ for some $n \in \mathbb{N}_+$;

(ii) *strongly primary* if H is atomic and for every $a \in H \setminus H^\times$ there exists some $\mathcal{M}_H(a) = \mathcal{M}(a) \in \mathbb{N}_+$ such that $a \mid b$ for every $b \in H$ with $\sup L(b) \ge \mathcal{M}(a)$;

(iii) *finitely primary* (of exponent $\alpha \in \mathbb{N}_+$) if H is a submonoid of a factorial monoid F with s pairwise non-associated prime elements $p_1, \ldots, p_s$,

$$H \subseteq F = [p_1, \ldots, p_s] \times F^\times,$$

such that the following two conditions are satisfied:

(a) $(p_1 \ldots p_s)^\alpha F \subseteq H$,

(b) if $\varepsilon p_1^{\alpha_1} \ldots p_s^{\alpha_s} \in H$ (where $\varepsilon \in F^\times$ and $\alpha_i \in \mathbb{N}$) then either $\alpha_1 = \ldots = \alpha_s = 0, \varepsilon \in H^\times$ or $\alpha_1 \ge 1, \ldots, \alpha_s \ge 1$.

2. An ideal $I \subseteq H$ is said to be

(i) *primary* if $a, b \in H$, $ab \in I$ and $a \notin I$ implies that $b^n \in I$ for some $n \in \mathbb{N}_+$,

(ii) *strongly primary* if there exists some $k \in \mathbb{N}_+$ such that $\mathfrak{m}^k \subseteq I$.

LEMMA 5.2. 1. *For an atomic monoid H with $\emptyset \neq \mathfrak{m} = H \setminus H^\times$ the following conditions are equivalent*:

(a) *H is strongly primary.*
(b) *Every proper ideal is strongly primary.*
(c) *Every proper principal ideal is strongly primary.*

2. *A strongly primary ideal is primary. In particular*, *a strongly primary monoid is primary.*

3. *A saturated atomic submonoid of a strongly primary monoid is strongly primary.*

4. *A monoid is strongly primary if and only if its associated reduced monoid is strongly primary.*

Proof. 1. (a)$\Rightarrow$(b). Let $I \subseteq H$ be an ideal with $I \neq H$. Choose some $a \in I$. Then there exists some $\mathcal{M}(a) \in \mathbb{N}_+$ such that $a \mid b$ for every $b \in H$ with $\sup L(b) \geq \mathcal{M}(a)$. This implies that $\mathfrak{m}^{\mathcal{M}(a)} \subseteq aH \subseteq I$.

(b)$\Rightarrow$(c). Obvious.

(c)$\Rightarrow$(a). Let $a \in H \setminus H^\times$. Then there exists some $k \in \mathbb{N}_+$ such that $\mathfrak{m}^k \subseteq aH$. Set $\mathcal{M}(a) = k$ and take some arbitrary $b \in H$ with $\sup L(b) \geq k$. Then $b \in \mathfrak{m}^k \subseteq aH$, whence $a \mid b$.

2. Let $I \subseteq H$ be a strongly primary ideal and $a, b \in H$ with $ab \in I$ and $a \notin I$. Then there is some $k \in \mathbb{N}_+$ such that $\mathfrak{m}^k \subseteq I \subseteq \mathfrak{m}$. Assume to the contrary that $b \notin \mathfrak{m}$; then $b \in H^\times$ and $a = (ab)b^{-1} \in I$, a contradiction. Thus $b \in \mathfrak{m}$ and $b^k \in \mathfrak{m}^k \subseteq I$, whence I is primary. The second assertion follows from part 1 and from Lemma 1 in [Ge5].

3. Let D be a strongly primary monoid and $H \subseteq D$ a saturated atomic submonoid. Let $a, b \in H$ such that $a \nmid b$ in H. Then $a \nmid b$ in D and hence

$$\sup L_H(b) \leq \sup L_D(b) < \mathcal{M}_D(a).$$

Therefore H is strongly primary with $\mathcal{M}_H(a) = \mathcal{M}_D(a)$.

4. Obvious. ∎

LEMMA 5.3. *Every finitely primary monoid is a locally tame*, *strongly primary BF-monoid.*

Proof. Let

$$H \subseteq F = [p_1, \ldots, p_s] \times F^\times$$

be a finitely primary monoid of exponent $\alpha \in \mathbb{N}_+$ and let all notations be as in the previous definition. Without restriction we assume that H is reduced. By [Ge5; Proposition 6] it is a BF-monoid.

To show that H is strongly primary, let $a, b \in H \setminus H^\times$ be given with $a \nmid b$. Hence there is some $i \in \{1, \ldots, s\}$ such that

$$\begin{aligned}\max L(b) &\le \min\{v_{p_j}(b) \mid 1 \le j \le s\} \le v_{p_i}(b) \\ &< v_{p_i}(a) + \alpha \le \max\{v_{p_j}(a) \mid 1 \le j \le s\} + \alpha =: \mathcal{M}(a).\end{aligned}$$

To show that H is locally tame, we choose some $a \in H$ and have to find an upper bound for $t(H, \mathcal{Z}(a))$. Let $b \in H$ with $a \mid b$, $z = u_1 \ldots u_r \in \mathcal{Z}(b)$ and $x \in \mathcal{Z}(a)$. Then

$$\sigma(x) \le \max L(a) \le \max\{v_{p_j}(a) \mid 1 \le j \le s\} = \mathcal{M}(a) - \alpha$$

and a divides $u_1 \ldots u_m$ for some $m \le \mathcal{M}(a)$. Set $u_1 \ldots u_m = ac$. If $s \ge 2$, then by [Ge5; Lemma 6], c has a factorization $y \in \mathcal{Z}(c)$ with $\sigma(y) \le 2\alpha$. If $s = 1$, then every atom $w \in H$ satisfies $v_{p_1}(w) \le 2\alpha - 1$; thus c has a factorization $y \in \mathcal{Z}(c)$ with

$$\sigma(y) \le v_{p_1}(u_1 \ldots u_m a^{-1}) \le m(2\alpha - 1) - (\mathcal{M}(a) - \alpha) \le \mathcal{M}(a)(2\alpha - 2) + \alpha.$$

Setting

$$z' = xyu_{m+1} \ldots u_r \in \mathcal{Z}(a)$$

we obtain

$$d(z, z') \le \max\{m, \sigma(x) + \sigma(y)\} \le \mathcal{M}(a)(2\alpha - 1) + 1,$$

whence $t(H, \mathcal{Z}(a)) \le \mathcal{M}(a)(2\alpha - 1) + 1$. ∎

PROPOSITION 5.4. *In a locally tame, strongly primary monoid every subset has a tame generating system of bounded length.*

Proof. Let H be a locally tame, strongly primary monoid and $I \subseteq H$ a subset. Fix some $a^* \in I$ and choose an arbitrary $b \in I$. If $a^* \nmid b$, then

$$t(b, \mathcal{Z}(b)) \le \max L(b) < \mathcal{M}(a^*).$$

If a^* divides b, then $t(b, \mathcal{Z}(a^*)) \le t(H, \mathcal{Z}(a^*))$. Hence I is tamely generated by $E = \{a^*\} \cup \{b \in I \mid a^* \nmid b\}$. ∎

LEMMA 5.5. *Let $H \subseteq D = D_1 \times D_2$ be a saturated atomic submonoid of an atomic monoid D with class group G, finite set $G_1 = \{[u] \in G \mid u \in \mathcal{A}(D)\}$ and $M \in \mathbb{N}_+$. Then $D_{2,M} = \{c \in D_2 \mid \max L_D(c) \le M\}$ allows a finite partition, say $D_{2,M} = \bigcup_{i=1}^{\varphi} C_i$, with the following property: if $a = bc \in H$ with $b \in D_1$, $c \in D_{2,M}$ and if $c' \in D_{2,M}$ is in the same class C_i as c, then $bc' \in H$ and $L_H(a) = L_H(bc')$.*

Proof. Without restriction we may suppose that H and D are reduced.

1. For every $a \in D$ and every $z \in \mathcal{Z}_D(a)$ we study product decompositions

$$(*) \qquad z = \prod_{\lambda=1}^{k} v_\lambda \prod_{\lambda=1}^{l} w_\lambda$$

where all v_λ are irreducible in H and no w_λ is divisible by an irreducible element of H. Such a decomposition gives rise to the following tuple:

$$(**) \quad (k, \{\{[x] \in \mathcal{F}(G_1) \mid x \in \mathcal{Z}_D(w_1)\}, \ldots, \{[x] \in \mathcal{F}(G_1) \mid x \in \mathcal{Z}_D(w_l)\}\}).$$

For $a \in D$ let $T(a)$ denote the set of all tuples $(**)$ arising from product decompositions $(*)$.

2. We show that for all $b \in D_1$ and $c \in D_2$ with $bc \in H$ the set $L_H(bc)$ just depends on $T(b)$ and $T(c)$. Hence, in particular, $L_H(bc) = L_H(bc')$ for all $b \in D_1$ and $c, c' \in D_2$ with $T(c) = T(c')$ and $bc, bc' \in H$.

Let $b \in D_1$ and $c \in D_2$ be such that $bc \in H$. Then $L_H(bc)$ is the set of all $k + k' + l$ for which there exist tuples

$$(k, \{X_1, \ldots, X_l\}) \in T(b) \quad \text{and} \quad (k', \{X_1', \ldots, X_l'\}) \in T(c)$$

where $X_i, X_i' \subseteq \mathcal{F}(G_1)$, having the following property: there is a permutation $\sigma \in \mathfrak{S}_l$ such that for all $1 \le i \le l$, all $S \in X_i$ and all $S' \in X_{\sigma(i)}$, the sequence SS' is an irreducible block in $\mathcal{B}(G_1)$.

3. To verify that $\mathcal{T} = \{T(c) \mid c \in D_{2,M}\}$ is finite, let $c \in D_{2,M}$ be given and consider a tuple of the form $(**)$ in $T(c)$. Clearly,

$$k + l \le \max L_D(c) \le M$$

and, for $1 \le i \le l$,

$$\#\{[x] \in \mathcal{F}(G_1) \mid x \in \mathcal{Z}_D(w_i)\} \le (\#G_1 - 1)^{\mathcal{D}(G_1)-1}.$$

Hence $\mathcal{T}$ is finite, say $\mathcal{T} = \{T_1, \ldots, T_\varphi\}$. Then, for $1 \le i \le \varphi$ we set

$$C_i = \{c \in D_{2,M} \mid T(c) = T_i\}$$

to obtain the required partition. ■

PROPOSITION 5.6. *Let $H \subseteq D \times D'$ be a saturated atomic submonoid of the atomic monoid $D \times D'$ with class group G, finite set $G_1 = \{[u] \in G \mid u \in \mathcal{A}(D \times D')\}$ and suppose that D is a finite product of locally tame, strongly primary BF-monoids. Then every subset $I \subseteq D$ of the form*

$$I = \{a \in D \mid ab \in H \text{ and } L_H(ab) \in P\},$$

where $b \in D'$ and $P \subseteq \mathbb{P}_{\text{fin}}(\mathbb{N}_+)$, has a generating system of bounded length, which is tame in D.

Proof. Suppose $D = \prod_{\nu \in \Omega} D_\nu$ where every D_ν is a locally tame, strongly primary BF-monoid. We proceed by induction on $\#\Omega$. If $\#\Omega = 1$, the assertion follows from Proposition 5.4. Suppose $\#\Omega \ge 2$ and let b, P and I be as above. Choose some $a^* \in I$ and set $M = \sum_{\nu \in \Omega} \mathcal{M}(a_\nu^*)$ and $M' = M + \max L_{D'}(b)$.

Consider a partition $\Omega = \Omega_1 \dot\cup \Omega_2$ with $\emptyset \neq \Omega_1 \neq \Omega$ and set $D_i = \prod_{\nu\in\Omega_i} D_\nu$ for $1 \le i \le 2$. Let

$$(D_2 \times D')_{M'} = \{w \in D_2 \times D' \mid \max L(w) \le M'\} = \bigcup_{j=1}^{\varphi} C_j$$

where the partition into the C_j's has the properties of Lemma 5.5. Let $1 \le j \le \varphi$; choose some $c_j \in C_j$ and define

$$I_j = \{a \in D_1 \mid ac_j \in H \text{ and } L_H(ac_j) \in P\} \subseteq D_1.$$

By induction hypothesis we infer that I_j has a tame generating system $E_j \subseteq I_j$ with bound N_j and with $\sup\{\sup L_D(e) \mid e \in E_j\} = K_j$. Let N resp. K denote the maximum over all N_j resp. K_j and all partitions $\Omega = \Omega_1 \dot\cup \Omega_2$ with $\emptyset \neq \Omega_1 \neq \Omega$.

Let $a \in I$; we have to find some $a' \in I$ which divides a such that $t_D(a, \mathcal{Z}(a'))$ and $\max L_D(a')$ are universally bounded. To begin with, set $\Omega_1 = \{\nu \in \Omega \mid \max L(a_\nu) \ge \mathcal{M}(a_\nu^*)\}$, $\Omega_2 = \Omega \setminus \Omega_1$ and $D_i = \prod_{\nu\in\Omega_i} D_\nu$ for $1 \le i \le 2$.

If $\Omega_1 = \Omega$, then $a_\nu^* \,|\, a_\nu$ for all $\nu \in \Omega$ and hence $a^* \,|\, a$. In this case we set $a' = a^*$; obviously, $t_D(a, \mathcal{Z}(a^*)) \le t_D(D, \mathcal{Z}(a^*))$ and $\max L_D(a^*)$ are bounded in a^*.

If $\Omega_1 = \emptyset$, we set $a' = a$ and infer that

$$t_D(a, \mathcal{Z}(a')) \le \max L_D(a) = \sum_{\nu\in\Omega} \max L_{D_\nu}(a_\nu) < \sum_{\nu\in\Omega} \mathcal{M}(a_\nu^*) = M.$$

From now on suppose that $\emptyset \neq \Omega_1 \neq \Omega$ and set $a = a_1 a_2$ with $a_i \in D_i$ for $1 \le i \le 2$. Then

$$\max L_{D_2}(a_2) = \sum_{\nu\in\Omega_2} \max L_{D_\nu}(a_\nu) < \sum_{\nu\in\Omega_2} \mathcal{M}(a_\nu^*) \le M$$

and hence

$$\max L_{D_2\times D'}(a_2 b) \le M'.$$

Let

$$(D_2 \times D')_{M'} = \bigcup_{j=1}^{\varphi} C_j$$

be as above and suppose that $a_2 b$ and c_j are in the same class C_j for some $j \in \{1, \ldots, \varphi\}$. Since $ab = a_1 a_2 b \in H$ and $L_H(ab) \in P$, it follows that $a_1 c_j \in H$ and $L_H(a_1 c_j) \in P$, i.e., $a_1 \in I_j$. Therefore, there exists some $\widehat{a} \in E_j$ dividing a_1 such that $t_{D_1}(a_1, \mathcal{Z}(\widehat{a})) \le N$. Now, we define

$$a' = \widehat{a} a_2 \in D_1 \times D_2 = D.$$

Clearly, a' divides a in D,

$$\max L_D(a') = \max L_{D_1}(\widehat{a}) + \max L_{D_2}(a_2) \le K + M$$

and

$$t_D(a,\mathcal{Z}(a')) = t_{D_1}(a_1,\mathcal{Z}(\widehat{a})) + t_{D_2}(a_2,\mathcal{Z}(a_2)) \le N + \max L_{D_2}(a_2) \le N + M.$$

In order to show that $a' \in I$ we have to verify that $a'b \in H$ and $L_H(a'b) \in P$. Since $\widehat{a} \in I_j$, it follows that $\widehat{a}c_j \in H$ and $L_H(\widehat{a}c_j) \in P$. This implies that $\widehat{a}a_2b \in H$ and $L_H(\widehat{a}a_2b) = L_H(\widehat{a}c_j) \in P$, i.e., $a' = \widehat{a}a_2 \in I$. ∎

6. Strictly saturated submonoids. Let H, D be atomic monoids and $H \subseteq D$ a saturated submonoid with class group G. Set $G_1 = \{[u] \in G \mid u \in \mathcal{A}(D)\}$. Then *Davenport's constant* $\mathcal{D}(G_1)$ is defined as

$$\mathcal{D}(G_1) = \sup\{\sigma(U) \mid U \in \mathcal{B}(G_1) \text{ is irreducible}\} \in \mathbb{N} \cup \{\infty\}.$$

In [Ge3; Lemma 4.4] it was shown that $\mathcal{D}(G_1)$ is the minimum of all $N \in \mathbb{N} \cup \{\infty\}$ satisfying the following property: for all $u_1, \ldots, u_n \in \mathcal{A}(D)$ with $\prod_{i=1}^n u_i \in H$ there exists a subset $\emptyset \ne J \subseteq \{1, \ldots, n\}$ with $\# J \le N$ such that $\prod_{j\in J} u_j \in H$.

For $k \in \mathbb{N}_+$ we set

$$\mu_k(H) = \sup\{\sup L \mid \min L \le k,\ L \in \mathcal{L}(H)\} \in \mathbb{N}_+ \cup \{\infty\}.$$

Then for the elasticity

$$\varrho(H) = \sup\left\{\frac{\sup L}{\min L} \;\middle|\; L \in \mathcal{L}(H)\right\} \in \mathbb{N}_+ \cup \{\infty\}$$

we have $\mu_k(H) \le k\varrho(H)$ for every $k \in \mathbb{N}_+$ (cf. [Ch-Ge; Section 2.2a]).

Let $H \subseteq D$ be saturated with $\mathcal{D}(G_1) < \infty$. Then $\mu_k(D) < \infty$ for all $k \in \mathbb{N}_+$ (resp. $\varrho(D) < \infty$) implies that $\mu_k(H) < \infty$ for all $k \in \mathbb{N}_+$ (resp. $\varrho(H) < \infty$) (cf. [G-L; Theorem 1]). However, there are arithmetical finiteness properties which do not carry over from D to H (see [Ge2; Proposition 6.5] for an example where D has finite catenary degree but H does not). We introduce the concept of strictly saturated submonoids $H \subseteq D$, which makes it possible to carry over arithmetical properties as local tameness or the finiteness of the catenary degree from D to H (see Theorems 7.4 and 7.5).

DEFINITION 6.1. Let D be an atomic monoid, $H \subseteq D$ a saturated submonoid with class group G and $G_1 = \{[u] \in G \mid u \in \mathcal{A}(D)\}$.

1. Let $\varrho(H, D)$ denote the minimum of all $N \in \mathbb{N} \cup \{\infty\}$ having the following property: for all $a \in H$ having a factorization $y \in \mathcal{Z}_D(a)$ with $[y] \in \mathcal{B}(G)$ irreducible, there exists a factorization $y^* \in \mathcal{Z}_H(a)$ with $\sigma(y^*) \le N$.

2. We say that $H \subseteq D$ is *strictly saturated* if H is atomic, $\mathcal{D}(G_1) < \infty$ and $\varrho(H, D) < \infty$.

Let D be a reduced atomic monoid and $H \subseteq D$ a strictly saturated submonoid. For every factorization $x = \prod_{i=1}^{r} u_i \in \mathcal{Z}(H)$ with $u_i \in \mathcal{A}(H)$ we call

$$Z_D(x) = \Big\{ \prod_{i=1}^{r} y_i \;\Big|\; y_i \in \mathcal{Z}_D(u_i) \Big\} \subseteq \mathcal{Z}(D)$$

the set of *factorizations induced by* x. For $X \subseteq \mathcal{Z}(H)$ we set

$$Z_D(X) = \bigcup_{x \in X} Z_D(x) \subseteq \mathcal{Z}(D).$$

For every $a \in H$ and every $y \in \mathcal{Z}_D(a)$ with $[y] \in \mathcal{B}(G)$ irreducible we fix a factorization $y^* \in \mathcal{Z}_H(a)$ with $\sigma(y^*) \le \varrho(H, D)$. For $a \in H$ and $y \in \mathcal{Z}_D(a)$ we set

$$Z_H(y) = \Big\{ \prod_{i=1}^{r} y_i^* \;\Big|\; y = \prod_{i=1}^{r} y_i \text{ with } 1 \ne y_i \in \mathcal{Z}(D) \text{ such that } [y_i] \in \mathcal{B}(G) \text{ is irreducible} \Big\} \subseteq \mathcal{Z}_H(a).$$

LEMMA 6.2. *Let D be a reduced atomic monoid and $H \subseteq D$ a strictly saturated submonoid with class group G and $G_1 = \{[u] \in G \mid u \in \mathcal{A}(D)\}$. Then for every $a \in H$ the following holds*:

1. $\mathcal{Z}_H(a) = \bigcup_{y \in \mathcal{Z}_D(a)} Z_H(y)$.
2. *For every $x \in \mathcal{Z}_H(a)$ and every $y \in Z_D(x)$ we have*
$$\sigma(x) \le \sigma(y) \le \sigma(x)\mathcal{D}(G_1).$$
3. *For every $y \in \mathcal{Z}_D(a)$ and every $x \in Z_H(y) \subseteq \mathcal{Z}_H(a)$ we have*
$$\sigma(x) \le \sigma(y)\varrho(H, D) \le \sigma(x)\mathcal{D}(G_1)\varrho(H, D).$$
4. *For every $y, y' \in \mathcal{Z}_D(a)$ there exist $x \in Z_H(y)$ and $x' \in Z_H(y')$ such that*
$$d(x, x') \le (\mathcal{D}(G_1) + d(y, y'))\varrho(H, D).$$

Proof. 1. Let $x = \prod_{i=1}^{r} u_i \in \mathcal{Z}_H(a)$ be given with $u_i \in \mathcal{A}(H)$. For every $1 \le i \le r$ choose some $y_i \in \mathcal{Z}_D(u_i)$; then $[y_i]$ is irreducible in $\mathcal{B}(G)$ and $y_i^* \in \mathcal{Z}_H(u_i) = \{u_i\}$, whence $y_i^* = u_i$. Since $y = \prod_{i=1}^{r} y_i \in \mathcal{Z}_D(a)$, it follows that

$$x = \prod_{i=1}^{r} u_i = \prod_{i=1}^{r} y_i^* \in Z_H(y).$$

The other inclusion is clear by definition.

2. By the very definition of $Z_D(x)$ we have $\sigma(x) \le \sigma(y)$. The inequality $\sigma(y) \le \sigma(x)\mathcal{D}(G_1)$ follows from the definition of $\mathcal{D}(G_1)$.

3. Let $y = \prod_{i=1}^{r} y_i \in \mathcal{Z}_D(a)$ with $1 \neq y_i \in \mathcal{Z}(D), [y_i] \in \mathcal{B}(G)$ irreducible and $x = \prod_{i=1}^{r} y_i^* \in Z_H(y)$. Then

$$r \leq \sigma(x) = \sum_{i=1}^{r} \sigma(y_i^*) \leq r\varrho(H,D) \quad \text{and} \quad r \leq \sigma(y) = \sum_{i=1}^{r} \sigma(y_i) \leq r\mathcal{D}(G_1),$$

which implies the assertion.

4. Suppose

$$y = y_1 y_2 \quad \text{and} \quad y' = y_1 y_2'$$

with $y_1, y_2, y_2' \in \mathcal{Z}(D)$ such that $d(y,y') = \max\{\sigma(y_2), \sigma(y_2')\}$. There exists some $y_0 \in \mathcal{Z}(D)$ with $y_0 \mid y_1$ and $\sigma(y_0) \leq \mathcal{D}(G_1)$ such that $y_0 y_2$ and $y_0 y_2'$ are factorizations of some element $b \in H$. Choose factorizations $x_1 \in Z_H(y_1 y_0^{-1}), x_2 \in Z_H(y_0 y_2)$ and $x_2' \in Z_H(y_0 y_2')$. Then $x = x_1 x_2 \in Z_H(y) \subseteq \mathcal{Z}_H(a)$ and $x' = x_1 x_2' \in Z_H(y')$. Using statement 3 we infer that

$$d(x,x') \leq \max\{\sigma(x_2), \sigma(x_2')\} \leq (\mathcal{D}(G_1) + d(y,y'))\varrho(H,D). \ \blacksquare$$

Proposition 6.3. *Let $H \subseteq D$ be a saturated submonoid of a reduced atomic BF-monoid D with class group $G, G_1 = \{[u] \in G \mid u \in \mathcal{A}(D)\}$ and $\mathcal{D}(G_1) < \infty$.*

1. *$\varrho(H,D) \leq \mu_{\mathcal{D}(G_1)}(D) \leq \mathcal{D}(G_1)\varrho(D)$. In particular, $H \subseteq D$ is strictly saturated if D is factorial* (*i.e., H is a Krull monoid*).

2. *If D is a coproduct of finitely primary monoids having some common exponent $\alpha \in \mathbb{N}_+$ and* $\exp(G) < \infty$, *then $H \subseteq D$ is strictly saturated.*

Proof. 1. Let $a \in H$ and $y \in \mathcal{Z}_D(a)$ be such that $[y] \in \mathcal{B}(G)$ is irreducible. Then $\sigma(y) \leq \mathcal{D}(G_1)$ and hence $\max L_D(a) \leq \mu_{\mathcal{D}(G_1)}(D)$. Since $\max L_H(a) \leq \max L_D(a)$ we infer that $\varrho(H,D) \leq \mu_{\mathcal{D}(G_1)}(D)$. The second inequality follows from the observation at the beginning of this section.

2. By [HK4; Theorem 3], H is a BF-monoid, whence atomic. Thus it remains to show that $\varrho(H,D) < \infty$. Suppose $D = \coprod_{\nu \in \Omega} D_\nu$ where each D_ν is finitely primary of exponent $\alpha \in \mathbb{N}_+$ and set $\beta = \alpha\exp(G)$. Let $a \in H$ and $z \in \mathcal{Z}_D(a)$ be such that $[z] \in \mathcal{B}(G)$ is irreducible. Then there is a subset $I \subseteq \Omega$ such that $a = \prod_{i \in I} a_i$ with $1 \neq a_i \in D_i$ and $z = \prod_{i \in I} z_i$ with $z_i \in \mathcal{Z}_{D_i}(a_i)$. Obviously,

$$\#I \leq \sum_{i \in I} \sigma(z_i) = \sigma(z) \leq \mathcal{D}(G_1).$$

Let $i \in I$; suppose

$$D_i \subseteq F_i = [p_{i,1}, \ldots, p_{i,s_i}] \times F_i^\times$$

and

$$a_i = \varepsilon_i \prod_{j=1}^{s_i} p_{i,j}^{k_{i,j}}$$

with $\varepsilon_i \in F_i^\times$. Set

$$I_1 = \{i \in I \mid k_{i,j} \ge 2\beta + \alpha \text{ for all } 1 \le \nu \le s_i\}$$

and let $i \in I_1$. For $j \in \{1, \ldots, s_i\}$ let $k_{i,j} = 2\beta l_{i,j} + \alpha + r_{i,j}$ with $0 \le r_{i,j} < 2\beta$. Set

$$b_i = \Big(\prod_{j=1}^{s_i} p_{i,j}^{2l_{i,j}}\Big)^\beta \quad \text{and} \quad c_i = \Big(\varepsilon_i \prod_{j=1}^{s_i} p_{i,j}^{\alpha + r_{i,j}}\Big);$$

then $b_i \in H$, $c_i \in D_i$ and $a_i = b_i c_i$. For $i \in I \setminus I_1$ set $c_i = a_i$. Next set

$$b = \prod_{i \in I_1} b_i \quad \text{and} \quad c = \prod_{i \in I} c_i.$$

Obviously, we have $a = bc$ with $b \in H$ and $c \in D$, whence $c \in H$ since $H \subseteq D$ is saturated.

We choose some $y \in \mathcal{Z}_H(c)$ and obtain

$$\begin{aligned}\sigma(y) &\le \max L_H(c) \le \max L_D(c) \\ &= \sum_{i \in I} \max L_{D_i}(c_i) \le \sum_{i \in I} (2\beta + \alpha) \le \sigma(z)(2\beta + \alpha).\end{aligned}$$

Let $i \in I_1$; we have to find a suitable factorization $x_i \in \mathcal{Z}_H(b_i)$. If $s_i = 1$, we choose any $x_i \in \mathcal{Z}_H(b_i)$ and infer that

$$\sigma(x_i) \le \max L_H(b_i) \le \max L_{D_i}(a_i) \le \sigma(z_i)\varrho(D_i) < \infty$$

since D_i has finite elasticity (cf. [HK2; Proposition 4.1]). Suppose $s_i \ge 2$; set

$$b_{i,1} = \Big(p_{i,1} \prod_{j=2}^{s_i} p_{i,j}^{2l_{i,j}-1}\Big)^\beta \quad \text{and} \quad b_{i,2} = \Big(p_{i,1}^{2l_{i,1}-1} \prod_{j=2}^{s_i} p_{i,j}\Big)^\beta.$$

Then $b_{i,1}, b_{i,2} \in H$ and $b_i = b_{i,1} b_{i,2}$. For $1 \le j \le 2$ we choose a factorization $x_{i,j} \in \mathcal{Z}_H(b_{i,j})$, infer that

$$\sigma(x_{i,j}) \le \max L_H(b_{i,j}) \le \max L_D(b_{i,j}) \le \beta$$

and set $x_i = x_{i,1} x_{i,2} \in \mathcal{Z}_H(b_i)$. Then $x = \prod_{i \in I_1} x_i \in \mathcal{Z}_H(b)$ and

$$\sigma(x) = \sum_{i \in I_1} \sigma(x_i) \le \sum_{i \in I_1} \sigma(z_i)(\varrho + 2\beta) \le \sigma(z)(\varrho + 2\beta)$$

where $\varrho = \max\{\varrho(D_i) \mid i \in I_1 \text{ with } s_i = 1\}$.

Summing up we have $xy \in \mathcal{Z}_H(bc)$ with $a = bc$ and

$$\sigma(xy) \le \sigma(z)(4\beta + \varrho + \alpha),$$

whence $\varrho(H, D) \le \mathcal{D}(G_1)(4\beta + \varrho + \alpha)$. ∎

Let $H \subseteq D$ be a saturated submonoid of a reduced atomic monoid D. As a final topic in this section we show that $H \subseteq D$ is strictly saturated if and only if this holds true for the associated block monoid. We briefly recall the concept of (general) block monoids. For proofs and detailed information the reader is referred to [HK2; Section 5] and [Ge2; Section 4].

Let $H \subseteq D$ be a saturated atomic submonoid with class group G of the reduced atomic monoid D. Let $D = \mathcal{F}(P) \times T$ be the canonical decomposition of D and $G_0 = \{[p] \in G \mid p \in P\}$. We define a homomorphism $\iota : \mathcal{F}(G_0) \times T \to G$ by

$$\iota(g_1 \ldots g_n t) = g_1 + \ldots + g_n + [t]$$

(where $g_1, \ldots, g_n \in G$ and $t \in T$) and set

$$\mathcal{B} = \iota^{-1}(0) \subseteq \mathcal{F}(G_0) \times T.$$

Then $\mathcal{B} \subseteq \mathcal{F}(G_0) \times T$ is saturated with class group G and $\mathcal{B}$ is called the *block monoid* of $(H \subseteq D)$. The homomorphism

$$\boldsymbol{\beta} : \mathcal{F}(P) \times T \to \mathcal{F}(G_0) \times T, \quad a = p_1 \ldots p_n t \mapsto \boldsymbol{\beta}(a) = [p_1] \ldots [p_n] t,$$

satisfies $\boldsymbol{\beta}(H) = \mathcal{B}$ and we obtain the following commutative diagram:

$$\begin{array}{ccccc} H & \hookrightarrow & D = \mathcal{F}(P) \times T & \stackrel{[\cdot]}{\to} & G \\ \boldsymbol{\beta}\downarrow & & \boldsymbol{\beta}\downarrow & & \| \\ \mathcal{B} & \hookrightarrow & \mathcal{F}(G_0) \times T & \stackrel{\iota}{\to} & G \end{array}$$

Since $\boldsymbol{\beta}(\mathcal{A}(D)) = \mathcal{A}(\mathcal{F}(G_0) \times T)$ and $\boldsymbol{\beta}^{-1}(\mathcal{A}(\mathcal{F}(G_0) \times T)) = \mathcal{A}(D)$, it follows that $\boldsymbol{\beta}$ induces an epimorphism $\boldsymbol{\beta} : \mathcal{Z}(D) \to \mathcal{Z}(\mathcal{F}(G_0) \times T)$ such that $\boldsymbol{\beta}(\mathcal{Z}_D(a)) = \mathcal{Z}_{\mathcal{F}(G_0) \times T}(\boldsymbol{\beta}(a))$ for every $a \in D$. Similarly, we have $\boldsymbol{\beta}(\mathcal{A}(H)) = \mathcal{A}(\mathcal{B})$ and $\boldsymbol{\beta}^{-1}(\mathcal{A}(\mathcal{B})) = \mathcal{A}(H)$ and hence there is an epimorphism $\boldsymbol{\beta} : \mathcal{Z}(H) \to \mathcal{Z}(\mathcal{B})$ such that $\boldsymbol{\beta}(\mathcal{Z}_H(a)) = \mathcal{Z}_{\mathcal{B}}(\boldsymbol{\beta}(a))$ for every $a \in H$. In particular, $L_H(a) = L_{\mathcal{B}}(\boldsymbol{\beta}(a))$.

PROPOSITION 6.4. *Let $H \subseteq D = \mathcal{F}(P) \times T$ be a saturated atomic submonoid of the reduced atomic monoid D with class group G, $G_0 = \{[p] \in G \mid p \in P\}$ and $\mathcal{B} \subseteq \mathcal{F}(G_0) \times T$ the associated block monoid. Then $\varrho(H, D) = \varrho(\mathcal{B}, \mathcal{F}(G_0) \times T)$ and $H \subseteq D$ is strictly saturated if and only if $\mathcal{B} \subseteq \mathcal{F}(G_0) \times T$ is strictly saturated.*

Proof. This is straightforward from our previous discussion. ∎

7. The catenary degree and local tameness. For the arithmetical relevance of the catenary degree the reader is referred to [Ge3, Ge4, Ge2]. Here we show that if $H \subseteq D$ is strictly saturated, then $c(D) < \infty$ implies that $c(H) < \infty$ (see Theorem 7.4). Together with Proposition 6.3 this generalizes former results (cf. [G-L; Theorem 2] and [Ge2; Theorem 5.4]) and shows the power of the concept of strictly saturated submonoids. A similar transfer result will be proved for local tameness (see Theorem 7.5).

DEFINITION 7.1. Let H be an atomic monoid.

1. Let $a \in H$, $z, z' \in \mathcal{Z}(a)$ and $N \in \mathbb{N} \cup \{\infty\}$. An *$N$-chain* (*of factorizations*) *from z to z'* is a finite sequence $(z_i)_{i=0}^k$ of factorizations $z_i \in \mathcal{Z}(a)$ such that $z = z_0$, $z_k = z'$ and $d(z_{i-1}, z_i) \le N$ for $1 \le i \le k$.

2. The *catenary degree* $c(H') \in \mathbb{N} \cup \{\infty\}$ of a subset $H' \subseteq H$ is the minimal $N \in \mathbb{N} \cup \{\infty\}$ such that for all $a \in H$ and any two factorizations $z, z' \in \mathcal{Z}(a)$ there is an N-chain of factorizations from z to z'. For brevity, we write $c(a)$ instead of $c(\{a\})$ for every $a \in H$.

Let H be an atomic monoid. Then H is factorial if and only if $c(H) = 0$. If H is not factorial but has finite catenary degree, then as an easy consequence of the definitions we obtain

$$\max \Delta(H) \le c(H) - 2,$$

i.e., the set $\Delta(H)$ is finite.

LEMMA 7.2. *Let D be an atomic monoid and $H \subseteq D$ a strictly saturated submonoid with class group G and $G_1 = \{[v] \in G \mid v \in \mathcal{A}(D)\}$. Let $a \in H$ and $y \in \mathcal{Z}_D(a)$. Then for any two factorizations $x, x' \in Z_H(y)$ there is a $\mathcal{D}(G_1)\varrho(H, D)$-chain of factorizations from x to x'.*

Proof. We suppose that H and D are reduced and define a monoid homomorphism

$$f : \mathcal{Z}(D) \to G$$

by $f(v) = [v]$ for every $v \in \mathcal{A}(D)$ and set $S = \mathrm{Ker}(f) \subseteq \mathcal{Z}(D)$. Then S is a Krull monoid with class group G and G_1 is the set of classes containing prime divisors (cf. [Ge6; Lemma 3]). Thus S has finite catenary degree $c(S) \le \mathcal{D}(G_1)$ (see [Ge2; Propositions 4.2 and 4.3]).

Since $a \in H$ and $y \in \mathcal{Z}_D(a)$, it follows that $y \in S$. Let $z = \prod_{\nu=1}^r z_\nu \in \mathcal{Z}_S(y)$ with $z_\nu = \prod_{i \in I_\nu} v_i \in \mathcal{A}(S)$ and $v_i \in \mathcal{A}(D)$. Then $[z_\nu] = \prod_{i \in I_\nu} [v_i] \in \mathcal{B}(G)$ is irreducible in $\mathcal{B}(G)$. We obtain a bijection

$$g : \mathcal{Z}_S(y) \to Z_H(y), \quad z = \prod_{\nu=1}^r z_\nu \mapsto g(z) = \prod_{\nu=1}^r z_\nu^*.$$

Any two factorizations $z, z' \in \mathcal{Z}_S(y)$ can be concatenated by a $\mathcal{D}(G_1)$-chain of factorizations using the canonical distance function $d = d_S : \mathcal{Z}(S)^2 = \mathcal{F}(\mathcal{A}(S))^2 \to \mathbb{N}$. The function g maps atoms $z_\nu \in S$ to factorizations $z_\nu^* \in H$ whose lengths (in $\mathcal{Z}(H)$) are bounded by $\varrho(H, D)$. Hence any two factorizations $x, x' \in Z_H(y)$ can be concatenated by a $\mathcal{D}(G_1)\varrho(H, D)$-chain of factorizations (using the distance function $d = d_H : \mathcal{Z}(H)^2 \to \mathbb{N}$). ∎

PROPOSITION 7.3. *Every reduced, locally tame, strongly primary BF-monoid H has finite catenary degree with $c(H) \le \max\{t(H, u), \mathcal{M}(u)\}$ for every $u \in \mathcal{A}(H)$.*

Proof. Let H be as in the hypothesis. Fix some $u \in \mathcal{A}(H)$ and set $t = t(H, u)$. We assert that

$$c(H) \le \max\{t, \mathcal{M}(u)\}.$$

For every $a \in H$ there exists some $k = k(a) \in \mathbb{N}$ with $k \le \max L(a)$ such that $u^k \mid a$ but $u^{k+1} \nmid a$. We proceed by induction on $k(a)$. If $a \in H$ with $k(a) = 0$, then

$$c(a) \le \max L(a) < \mathcal{M}(u).$$

Let $a \in H$ and $z, z' \in \mathcal{Z}(a)$ be given with $k = k(a) \ge 1$. Suppose the assertion holds for all $b \in H$ with $k(b) < k$. Since u divides a, there is some factorization $x \in \mathcal{Z}(u^{-1}a)$ such that $d(z, ux) \le t$. Similarly, there is some $x' \in \mathcal{Z}(u^{-1}a)$ with $d(z', ux') \le t$. Clearly, $k(u^{-1}a) < k(a)$. Hence, by induction hypothesis there exists a $\max\{t, \mathcal{M}(u)\}$-chain from x to x', which gives a $\max\{t, \mathcal{M}(u)\}$-chain from z to z'. ■

THEOREM 7.4. *Let $H \subseteq D$ be a strictly saturated submonoid of an atomic monoid D.*

1. *If D has finite catenary degree, then so does H. More precisely,* $c(H) \le (\mathcal{D}(G_1) + c(D))\varrho(H, D)$.
2. *Suppose $D = \coprod_{i \in I} D_i$ where all D_i are reduced, locally tame, strongly primary BF-monoids and there are $u_i \in \mathcal{A}(D_i)$ such that* $\sup\{t_{D_i}(D_i, u_i), \mathcal{M}(u_i) \mid i \in I\} < \infty$. *Then H has finite catenary degree and $\Delta(H)$ is finite.*

Proof. 1. Let $a \in H$ and $x, x' \in \mathcal{Z}_H(a)$ be given. We choose factorizations $y \in Z_D(x)$ and $y' \in Z_D(x')$. Since D has finite catenary degree $c(D)$, there exists a $c(D)$-chain of factorizations $y = y_0, y_1, \ldots, y_l = y'$ from y to y'. By Lemma 6.2.4 there are factorizations

$$x_i \in Z_H(y_i) \quad \text{and} \quad \widetilde{x}_i \in Z_H(y_{i+1}), \qquad \text{for } 0 \le i \le l-1,$$

with $d(x_i, \widetilde{x}_i) \le (\mathcal{D}(G_1) + c(D))\varrho(H, D)$. Furthermore, by Lemma 7.2 there are $\mathcal{D}(G_1)\varrho(H, D)$-chains

from $x \in Z_D(y)$ to $x_0 \in Z_D(y)$,
from $\widetilde{x}_{i-1} \in Z_D(y_i)$ to $x_i \in Z_D(y_i)$ for $1 \le i \le l-1$, and
from $\widetilde{x}_{l-1} \in Z_D(y_l)$ to $x' \in Z_D(y_l)$.

Putting all together we obtain a $(\mathcal{D}(G_1) + c(D))\varrho(H, D)$-chain from x to x'.

2. This follows from part 1 and Proposition 7.3. ■

THEOREM 7.5. *Let $H \subseteq D$ be a strictly saturated submonoid of an atomic monoid D with class group G and $G_1 = \{[u] \in G \mid u \in \mathcal{A}(D)\}$. Let $H' \subseteq H$ and $X \subseteq \mathcal{Z}(H)$ with* $\sup\{\sigma(x) \mid x \in X\} = M \in \mathbb{N}_+$. *If $t_D(H', Z_D(X))$ is finite, then so is $t_H(H', X)$. More precisely,*

$$t_H(H', X) \le M + \varrho(H, D)\mathcal{D}(G_1)(M\mathcal{D}(G_1) + t_D(H', Z_D(X))).$$

In particular, if D is a (locally) tame BF-monoid, then the same is true for H.

Proof. Without restriction we may suppose that H and D are reduced. Let $a \in H'$, $z = \prod_{i=1}^m u_i \in \mathcal{Z}_H(a)$ with $u_i \in \mathcal{A}(H)$ and $x \in X$. We have to find an upper bound for $t_H(a, x)$.

As explained at the beginning of Section 6, z induces a factorization $\widetilde{z} = \prod_{i=1}^m \widetilde{z}_i \in Z_D(z) \subseteq \mathcal{Z}_D(a)$ with $\widetilde{z}_i \in \mathcal{Z}_D(u_i)$, whence $\sigma(\widetilde{z}_i) \le \mathcal{D}(G_1)$ for $1 \le i \le m$. Similarly, x induces a factorization $\widetilde{x} \in Z_D(X)$ with $\sigma(\widetilde{x}) \le \sigma(x)\mathcal{D}(G_1) \le M\mathcal{D}(G_1)$.

By definition of tameness in D, there exists a factorization $\widetilde{z}' \in \mathcal{Z}_D(a)$ with $\widetilde{x} \mid \widetilde{z}'$ and $d(\widetilde{z}, \widetilde{z}') = t \le t_D(H', Z_D(X))$. Therefore, after a suitable renumbering we may write $\widetilde{z}'$ in the form

$$\widetilde{z}' = \prod_{i=1}^{m-t} \widetilde{z}_i y'$$

where $y' \in \mathcal{Z}(D)$ with $\sigma(y') \le t\mathcal{D}(G_1)$. Set

$$\widetilde{x}_1 = \gcd_{\mathcal{Z}(D)}\Big(\prod_{i=1}^{m-t} \widetilde{z}_i, \widetilde{x}\Big).$$

Then there are $\widetilde{x}_2, \widetilde{y}_2 \in \mathcal{Z}(D)$ such that $\widetilde{x} = \widetilde{x}_1\widetilde{x}_2$ and $y' = \widetilde{x}_2\widetilde{y}_2$. After a further renumbering we have, for some $\widetilde{y}_1 \in \mathcal{Z}(D)$,

$$\prod_{i=1}^{m-t} \widetilde{z}_i = \prod_{i=1}^{m-t-s} \widetilde{z}_i\widetilde{x}_1\widetilde{y}_1$$

with $s \le \sigma(\widetilde{x}_1) \le \sigma(\widetilde{x})$ and $\sigma(\widetilde{y}_1) \le \sigma(\widetilde{x}_1)(\mathcal{D}(G_1) - 1)$. Setting $\widetilde{y} = \widetilde{y}_1\widetilde{y}_2$ we get

$$\widetilde{z}' = \prod_{i=1}^{m-t-s} \widetilde{z}_i\widetilde{x}_1\widetilde{y}_1\widetilde{x}_2\widetilde{y}_2 = \prod_{i=1}^{m-t-s} \widetilde{z}_i\widetilde{x}\widetilde{y}$$

with

$$\sigma(\widetilde{y}) \le \sigma(\widetilde{x})(\mathcal{D}(G_1) - 1) + \sigma(y') \le \mathcal{D}(G_1)(M\mathcal{D}(G_1) + t).$$

If $\widetilde{y} \in \mathcal{Z}_D(b)$, then $b \in H$ and by Lemma 6.2 there is some $y \in Z_H(\widetilde{y}) \subseteq \mathcal{Z}_H(b)$ with $\sigma(y) \le \sigma(\widetilde{y})\varrho(H, D)$. Setting

$$z' = \prod_{i=1}^{m-t-s} u_i x y$$

we obtain

$$\begin{aligned} t_H(a, x) &\le d(z, z') \le \max\{s + t, \sigma(x) + \sigma(y)\} \\ &\le M + \varrho(H, D)\mathcal{D}(G_1)(M\mathcal{D}(G_1) + t_D(H', Z_D(X))). \end{aligned}$$

Hence, $t_H(H', X)$ is restricted by the above bound. ∎

Corollary 7.6. *Let $H \subseteq D$ be a strictly saturated submonoid of an atomic monoid D and $I \subseteq H$ a subset. Then every generating system $E \subseteq I$ of bounded length, which is tame in D, is tame in H.*

Proof. Suppose $E \subseteq I$ is a generating system, tame in D, with bound N and $\sup\{\sup L_H(e) \mid e \in E\} = M$. Let $a \in I$; then there is some $e \in E$ with $t_D(a, \mathcal{Z}_D(e)) \le N$. By Theorem 7.5 it follows that

$$t_H(a, \mathcal{Z}_H(e)) \le M + \varrho(H, D)\mathcal{D}(G_1)(M\mathcal{D}(G_1) + N),$$

which implies the assertion. ∎

8. The Structure Theorem revisited. In this section we use the results from our monoid-theoretical investigations (in particular, Propositions 4.7, 4.8 and Corollary 7.6) to apply the abstract Structure Theorem 3.2 to concrete monoids.

Let H be a BF-monoid with finite, non-empty set $\Delta(H)$ and with $\varphi(H) < \infty$. Let $a \in H$; then by Theorem 3.2.3 there exists some $\psi \in \mathbb{N}$ satisfying the following property (P):

(P) for all $b \in H$ with $a^\psi \mid b \mid a^k$ for some $k \ge \psi$, the sets $L(b)$ are almost arithmetical progressions with the same difference $\delta \in \Delta(H)$ bounded by $\varphi(H)$.

Obviously, if $\psi \in \mathbb{N}$ satisfies (P), then so does every $\psi' \in \mathbb{N}$ with $\psi' \ge \psi$. Let $\psi(a) \in \mathbb{N}$ denote the minimum of all $\psi \in \mathbb{N}$ satisfying (P) and define

$$\psi(H) = \sup\{\psi(a) \mid a \in H\} \in \mathbb{N} \cup \{\infty\}.$$

Obviously, $\psi(H) < \infty$ if and only if there exists some $\psi \in \mathbb{N}$ satisfying property (P) for every $a \in H$.

Suppose that $\Delta(H) = \emptyset$. Then all sets of lengths contain exactly one element. In order to simplify formulations, we say that H satisfies the Structure Theorem for Sets of Lengths and set $\varphi(H) = 0$ and $\psi(H) = 1$.

Proposition 8.1. *Let H be a finitely generated monoid. Then H is a tame FF-monoid with finite catenary degree, finite set $\Delta(H)$ and $\varphi(H) < \infty$. Thus the Structure Theorem for Sets of Lengths holds and $\psi(H) < \infty$.*

Proof. By [HK4; Theorem 2] and [Ge4; Proposition 3.4], H is a tame FF-monoid. Hence it has finite catenary degree and $\Delta(H)$ is finite (cf. [Ge4; Proposition 3.3]). If $\Delta(H) = \emptyset$, then nothing more has to be proved. Suppose $\Delta(H) \ne \emptyset$. By Proposition 4.7 all subsets are tamely generated, whence Proposition 4.8 implies that $\varphi(H) < \infty$ and that the Structure Theorem for Sets of Lengths holds.

Suppose H is generated by $u_1, \ldots, u_s \in \mathcal{A}(H)$. For $\emptyset \ne I \subseteq \{1, \ldots, s\}$ set $u_I = \prod_{i \in I} u_i$ and define

$$\psi = \max\{\psi(u_I) \mid \emptyset \ne I \subseteq \{1, \ldots, s\}\} \in \mathbb{N}.$$

Let $a = \prod_{i\in I} u_i^{k_i} \in H$ be given with $\emptyset \neq I \subseteq \{1,\ldots,s\}$ and $k_i \in \mathbb{N}_+$. We show that $\psi(a) \le \psi$, which implies that $\psi(H) \le \psi$. Let $b \in H$ with $a^\psi \mid b \mid a^k$ for some $k \ge \psi$. Then

$$u_I^{\psi(u_I)} \mid a^\psi \mid b \mid a^k \mid u_I^{k \max\{k_i \mid i\in I\}}.$$

Therefore, by definition of $\psi(u_I)$ the set $L(b)$ is an almost arithmetical progression bounded by $\varphi(H)$. ∎

Proposition 8.2. *Let $H \subseteq D = \prod_{i=1}^n D_i$ be a strictly saturated submonoid with class group G. Suppose that $G_1 = \{[u] \in G \mid u \in \mathcal{A}(D)\}$ is finite and that all D_i are locally tame, strongly primary BF-monoids. Then H is a locally tame BF-monoid with finite catenary degree, finite set $\Delta(H)$ and $\varphi(H) < \infty$. Thus the Structure Theorem for Sets of Lengths holds and $\psi(H) < \infty$.*

Proof. H is a BF-monoid, since it is a saturated submonoid of a BF-monoid (cf. [HK4; Theorem 3]). From Theorem 7.5 it follows that H is locally tame. By Theorem 7.4, $c(H)$ and $\Delta(H)$ are finite. If $\Delta(H) = \emptyset$ we are done; hence suppose that $\Delta(H) \neq \emptyset$. For every $\mathbf{d} \in \Delta(H)^r$ the set $\Phi_{\mathbf{d}}(H)$ has a generating system of bounded length which is tame in H (cf. Proposition 5.6 and Corollary 7.6). Therefore, Proposition 4.8 implies that $\varphi(H) < \infty$.

Without restriction we may assume that H and D are reduced. For every subset $\emptyset \neq I \subseteq \{1,\ldots,n\}$ for which

$$H \cap \prod_{i\in I} (D_i \setminus \{1\}) \neq \emptyset$$

we fix some $c_I = \prod_{i\in I} c_i \in H$ with $1 \neq c_i \in D_i$. Define

$$\psi = \max\{\mathcal{M}(c_i^{\psi(c_I)}) \mid i \in I \text{ and } \emptyset \neq I \subseteq \{1,\ldots,n\} \text{ as above}\} \in \mathbb{N}.$$

We show that $\psi(a) \le \psi$ for every $a \in H$, which implies that $\psi(H) \le \psi$.

Let $1 \neq a = \prod_{i\in I} a_i \in H$ be given with $1 \neq a_i \in D_i$, $\emptyset \neq I \subseteq \{1,\ldots,n\}$ and let $b \in H$ such that $a^\psi \mid b \mid a^k$ for some $k \ge \psi$. Since

$$\max L_{D_i}(a_i^\psi) \ge \max L_{D_i}(a_i^{\mathcal{M}(c_i^{\psi(c_I)})}) \ge \mathcal{M}(c_i^{\psi(c_I)})$$

it follows that $c_i^{\psi(c_I)} \mid a_i^\psi$ in D_i for every $i \in I$. Therefore $c_I^{\psi(c_I)}$ divides a^ψ in D and hence in H. Since D_i is primary, there is some $l_i \in \mathbb{N}$ such that $a_i \mid c_i^{l_i}$ in D_i. Thus there is some $l \in \mathbb{N}$ such that $a^k \mid c_I^l$ in H. Summing up we obtain

$$c_I^{\psi(c_I)} \mid a^\psi \mid b \mid a^k \mid c_I^l,$$

whence the assertion follows from the definition of $\psi(c_I)$. ∎

Theorem 8.3. *Let $H \subseteq D = \mathcal{F}(P) \times \prod_{i=1}^n D_i$ be a strictly saturated submonoid with class group G. Suppose that $G_1 = \{[u] \in G \mid u \in \mathcal{A}(D)\}$ is finite and that all D_i are locally tame, strongly primary BF-monoids. Then*

H is a locally tame BF-monoid with finite catenary degree, finite set $\Delta(H)$ and $\varphi(H) < \infty$. Thus the Structure Theorem for Sets of Lengths holds and $\psi(H) < \infty$.

Proof. By Theorem 7.5, H is locally tame and, by Theorem 7.4, it has finite catenary degree. All assertions on lengths of factorizations hold for H if and only if they hold for the associated block monoid $\mathcal{B}$ (cf. [Ge2; Section 4] and [HK2; Section 5]). By Proposition 6.4, $\mathcal{B} \subseteq \mathcal{F}(G_0) \times \prod_{i=1}^n D_i$ is a strictly saturated submonoid with $G_0 = \{[p] \in G \mid p \in P\} \subseteq G_1$. Since G_0 is finite, $\mathcal{F}(G_0) \times \prod_{i=1}^n D_i = \prod_{g \in G_0} \mathcal{F}(\{g\}) \times \prod_{i=1}^n D_i$ is a finite product of locally tame, strongly primary BF-monoids. Therefore, Proposition 8.2 implies the assertion. ∎

The main example for the above class of monoids are weakly Krull monoids H with weak divisor theory $\varphi : H \to D = \coprod_{i \in I} D_i$ such that the following holds: the weak divisor class group is finite, all primary components D_i are finitely primary and for almost all D_i we have $D_i \simeq (\mathbb{N}, +)$. If all D_i are isomorphic to $(\mathbb{N}, +)$, then H is a Krull monoid and the weak divisor theory $\varphi : H \to D \simeq \mathcal{F}(P)$ is a divisor theory.

Under stronger assumptions main parts of the above theorem were already proved in [Ge1; Satz 1] and [Ge3; Theorem 6.2]; for geometric versions of this result the reader is referred to [HK1] and [HK2; Section 3]. However, the finiteness of $\psi(H)$ is new even for Krull monoids.

In the rest of this section we show that there exists a locally tame Krull monoid H with finite catenary degree and finite set $\Delta(H)$ but which does not satisfy the Structure Theorem for Sets of Lengths (see Theorem 8.5). In particular, we show that every finite set $L \in \mathbb{N}_+ \setminus \{1\}$ can be realized as a set of lengths in a Krull monoid. This already follows from Proposition 3.4. However, if G is an infinite abelian group, then $\mathcal{B}(G)$ is not locally tame, nor does it have finite catenary degree. Recall that Krull monoids are FF- and hence BF-monoids.

Proposition 8.4. *For every finite subset $L \subseteq \mathbb{N}_+ \setminus \{1\}$ there exists a finitely generated reduced Krull monoid H with $L \in \mathcal{L}(H)$ and $c(H) \leq \max \Delta(L) + 2$.*

Proof. We proceed by induction on the number of elements of L. For this we show that there is some element $a \in H$ having the following properties:

(i) $L(a) = L$,

(ii) a has exactly one factorization z^* with $\sigma(z^*) = \min L$ and this factorization is squarefree,

(iii) a has an irreducible divisor $u \in \mathcal{A}(H)$ such that $w \in \mathcal{Z}(a)$ and $u \mid w$ implies $w = z^*$.

Suppose $L = \{k\}$ for some $k \in \mathbb{N}_+$. Then let H be the free abelian monoid with basis $u_1, \ldots, u_k$ and set $a = \prod_{i=1}^{k} u_i$. Obviously, all required properties are satisfied.

To do the induction step let $L \subseteq \mathbb{N}_+ \setminus \{1\}$ be a finite set with $\#L \geq 2$ and suppose that the monoid H', $a' \in H'$, $z' = \prod_{j=1}^{\psi} u_j \in \mathcal{Z}_{H'}(a')$ and $u = u_1$ satisfy the properties for the set $L' = L \setminus \{\min L\}$. Define

$$H = [H', v, w] \subseteq \mathcal{Q}(H') \times \Gamma = G$$

and $a = a'$, where $\mathbb{Z} \simeq \Gamma = \mathcal{Q}(\mathcal{F}(\{v\}))$ and $w = v^{-1}(u_1 \ldots u_d)$ with $d = \min L' - \min L + 2$. Clearly, H is a finitely generated reduced monoid with $\mathcal{Q}(H) = G$. By properties (i)–(iii) for H' we infer that

$$\mathcal{Z}_H(a) = \mathcal{Z}_{H'}(a) \cup \Big\{ z^* = vw \prod_{j=d+1}^{\psi} u_j \Big\},$$

which implies

$$L_H(a) = L_{H'}(a) \cup \{\sigma(z^*)\} = L' \cup \{2 + \min L' - d\} = L.$$

Obviously, z^* is squarefree in $\mathcal{Z}(H)$ and z^* is the only factorization of a in H with $\sigma(z^*) = \min L$. Furthermore, we have $v \in \mathcal{A}(H)$, $v \mid a$ and v appears only in the factorization z^*. Thus properties (i)–(iii) are satisfied by H, a, z^* and v. We proceed in two steps to verify the remaining assertions.

1. To prove that H is a Krull monoid it remains to show that H is root closed (cf. [HK3; Theorem 5]). Let $y = xv^{\varphi} \in G$ with $x \in \mathcal{Q}(H')$ and $\varphi \in \mathbb{Z}$ such that $y^m = b \in H$ for some $m \in \mathbb{N}_+$. Since $vw \in H'$, the element b has a factorization which is not divisible by vw.

Case 1: $b = cv^s = x^m v^{\varphi m}$ with $c \in H'$ and $s \in \mathbb{N}$. Then

$$cx^{-m} = v^{\varphi m - s} \in \mathcal{Q}(H') \cap \Gamma = \{1\}.$$

This implies that $x^m = c \in H'$, whence $x \in H'$, since H' is root closed. Furthermore, $\varphi = s/m \in \mathbb{N}$ and thus $y = xv^{\varphi} \in H$.

Case 2: $b = cw^s = x^m v^{\varphi m}$ with $c \in H'$ and $s \in \mathbb{N}$. Then

$$cx^{-m}(u_1 \ldots u_d)^s = v^{\varphi m + s} \in \{1\}.$$

This implies that $-\varphi = s/m \in \mathbb{N}$ and

$$((u_1 \ldots u_d)^{\varphi} x)^m = c \in H'.$$

Since H' is root closed, it follows that $(u_1 \ldots u_d)^{\varphi} x \in H'$, whence

$$y = xv^{\varphi} = x(u_1 \ldots u_d)^{\varphi} w^{-\varphi} \in H.$$

2. To verify the assertion on the catenary degree, let $b \in H$ and $z = v^r w^s x, z' = v^{r'} w^{s'} x' \in \mathcal{Z}_H(b)$ be given with $r, r', s, s' \in \mathbb{N}$ and $x, x' \in \mathcal{Z}(H')$.

Since $vw = u_1 \dots u_d$ there is a d-chain of factorizations from z to

$$\widetilde{z} = v^{r-t} w^{s-t} \widetilde{x}$$

with $t = \min\{r, s\}$ and $\widetilde{x} \in \mathcal{Z}(H')$. Similarly, there is a d-chain from z' to

$$\widetilde{z}' = v^{r'-t'} w^{s'-t'} \widetilde{x}'$$

with $t' = \min\{r', s'\}$ and $\widetilde{x}' \in \mathcal{Z}(H')$. By comparing the associated product decompositions in G it follows that $r - t = r' - t'$ and $s - t = s' - t'$. By induction hypothesis there is a $c(H')$-chain of factorizations from $\widetilde{x}$ to $\widetilde{x}'$ with $c(H') \le \max \Delta(L') + 2$. Putting all this together we obtain an N-chain from x to x' with

$$N \le \max\{\min L' - \min L + 2, \max \Delta(L') + 2\} = \max \Delta(L) + 2. \ \blacksquare$$

THEOREM 8.5. 1. *For every system $\mathcal{L}$ of finite sets $L \subseteq \mathbb{N}_+ \setminus \{1\}$ there exists a locally tame Krull monoid H with $\mathcal{L} \subseteq \mathcal{L}(H)$ and $c(H) \le \sup \Delta(\mathcal{L}) + 2$.*

2. *There exists a locally tame Krull monoid H with finite catenary degree and finite set $\Delta(H)$ which does not satisfy the Structure Theorem for Sets of Lengths.*

Proof. 1. For every $L \in \mathcal{L}$ let H_L have the properties of Proposition 8.4. Then we define

$$H = \coprod_{L \in \mathcal{L}} H_L.$$

Since finitely generated monoids are locally tame, each H_L is a locally tame Krull monoid, whence H is a locally tame Krull monoid. Furthermore,

$$\mathcal{L} \subseteq \bigcup_{L \in \mathcal{L}} \mathcal{L}(H_L) \subseteq \mathcal{L}(H)$$

and

$$c(H) = \sup\nolimits_{L \in \mathcal{L}} c(H_L) \le \sup\nolimits_{L \in \mathcal{L}} \{\max \Delta(L) + 2\}.$$

2. By part 1 it is sufficient to find a system $\mathcal{L}$ with finite set $\Delta(\mathcal{L})$ such that the sets $L \in \mathcal{L}$ are not almost arithmetical multiprogressions bounded by some fixed $M \in \mathbb{N}_+$.

For this choose some $d \in \mathbb{N}_+$ with $d \ge 2$ and set

$$L_n = \{n + kd \mid 0 \le k \le 2n\} \cup \{n + nd + 1\}$$

for every $n \in \mathbb{N}_+$. Then

$$\mathcal{L} = \{L_n \mid n \in \mathbb{N}_+\}$$

has the required properties. $\blacksquare$

9. Applications to integral domains. Let R be an integral domain. Then $R^\bullet = R \setminus \{0\}$ denotes its multiplicative monoid, $R^\times = R^{\bullet\times}$ its group of units and $R^{\#} = R^{\bullet}/R^{\times}$ the reduced multiplicative monoid. Obviously, $R^{\#}$ is isomorphic to $\mathcal{H}(R)$, the monoid of principal ideals. We say that R is a *local domain* if it has just one maximal ideal. The proof of the following lemma may be found in [Ge5; Theorem 2].

LEMMA 9.1. *Let R be an integral domain.*

1. *$R^{\bullet}$ is primary if and only if R is a one-dimensional, local domain.*
2. *$R^{\bullet}$ is finitely primary if and only if R is a one-dimensional, local domain, the complete integral closure $\widehat{R}$ is a semilocal principal ideal domain and the conductor $\widehat{R}/R$ is non-zero.*

LEMMA 9.2. *Let R be a noetherian domain. Then $R^{\bullet}$ is a BF-monoid and the following conditions are equivalent*:

(a) *R is a one-dimensional, local domain,*
(b) *$R^{\bullet}$ is primary,*
(c) *$R^{\bullet}$ is strongly primary,*

If the integral closure $\overline{R}$ is a finite R-module, then there are further equivalent conditions:

(d) *$R^{\bullet}$ is a locally tame, strongly primary BF-monoid,*
(e) *$R^{\bullet}$ is finitely primary.*

Proof. $R^{\bullet}$ is a BF-monoid by [HK4; Theorem 7]. By Lemma 9.1 conditions (a) and (b) are equivalent. Lemmata 5.2 and 5.3 show that (e)$\Rightarrow$(d)$\Rightarrow$(c)$\Rightarrow$(b).

(a)$\Rightarrow$(c). Let R be a one-dimensional local domain with maximal ideal $\mathfrak{m} = R \setminus R^{\times}$ and let $a \in R^{\bullet} \setminus R^{\times}$. Then $\sqrt{aR} = \mathfrak{m}$ and there is some $n \in \mathbb{N}_+$ such that $\mathfrak{m}^n \subseteq aR \subseteq \mathfrak{m}$. Thus aR is strongly primary and the assertion follows from Lemma 5.2.

(a)$\Rightarrow$(e). Suppose that R is one-dimensional, local, noetherian and $\overline{R}$ is a finite R-module. Then $R^{\bullet}$ is finitely primary by [HK6; Proposition 6]. ∎

An integral domain R is said to be *weakly Krull* (cf. [A-M-Z]) if

$$R = \bigcap_{\mathfrak{p} \in \mathfrak{X}(R)} R_{\mathfrak{p}}$$

where $\mathfrak{X}(R)$ denotes the set of height-one prime ideals and the intersection is of finite character. Let R be weakly Krull. Then the canonical homomorphism

$$\varphi : R^{\bullet} \to D = \coprod_{\mathfrak{p} \in \mathfrak{X}(R)} R_{\mathfrak{p}}^{\#}$$

is a weak divisor theory. The monoid $\mathcal{I}_t(R)$ of t-invertible t-ideals (equipped with t-multiplication) is isomorphic to D and the t-class group $C_t(R) =$

$\mathcal{I}_t(R)/\mathcal{H}(R)$ is isomorphic to the weak divisor class group (cf. [HK5; Section 4]). If R is one-dimensional, then $\mathcal{I}_t(R)$ coincides with the monoid of invertible ideals (equipped with usual ideal multiplication) and $C_t(R) = \mathrm{Pic}(R)$.

A weakly Krull domain R is said to be *of finite type* (cf. [HK2; Section 6]) if its integral closure $\overline{R}$ is a Krull domain and a finitely generated R-module. Krull domains and noetherian weakly Krull domains R whose integral closures $\overline{R}$ are finite R-modules (including orders in global fields) are the most important examples of weakly Krull domains of finite type.

THEOREM 9.3. *Let R be a weakly Krull domain of finite type.*

1. *The monoid $\mathcal{I}_t(R)$ is a locally tame BF-monoid with finite catenary degree, finite set $\Delta(\mathcal{I}_t(R))$ and $\varphi(\mathcal{I}_t(R)) < \infty$. Thus the Structure Theorem for Sets of Lengths holds and $\psi(\mathcal{I}_t(R)) < \infty$.*
2. *If the number of classes in the t-class group $C_t(R)$ containing multiplicative irreducible ideals is finite, then all assertions above hold for $R^\bullet$.*

Proof. As discussed above we have

$$R^{\#} \simeq \mathcal{H}(R) \subseteq \mathcal{I}_t(R) \simeq \coprod_{\mathfrak{p}\in\mathfrak{X}(R)} R_{\mathfrak{p}}^{\#}.$$

All $R_{\mathfrak{p}}^{\#}$ are finitely primary and hence locally tame, strongly primary BF-monoids. For almost all $\mathfrak{p} \in \mathfrak{X}(R)$ the localization $R_{\mathfrak{p}} = \overline{R}_{\mathfrak{p}}$ is a discrete valuation ring and hence $R_{\mathfrak{p}}^{\#}$ is isomorphic to $(\mathbb{N}, +)$ (cf. [HK2; Lemma 6.3]). Therefore, Theorem 8.3 implies the assertion with $H = D = \mathcal{I}_t(R)$.

Because of the above finiteness condition Theorem 8.3 implies the assertion with $H = \mathcal{H}(R)$ and $D = \mathcal{I}_t(R)$. ∎

REFERENCES

[An] D. D. Anderson (ed.), *Factorization in Integral Domains*, Lecture Notes in Pure and Appl. Math. 189, Marcel Dekker, 1997.

[A-M-Z] D. D. Anderson, J. L. Mott and M. Zafrullah, *Finite character representations for integral domains*, Boll. Un. Mat. Ital. B (7) 6 (1992), 613–630.

[Bo] N. Bourbaki, *Commutative Algebra*, Springer, 1989.

[Ch-Ge] S. Chapman and A. Geroldinger, *Krull domains and monoids, their sets of lengths and associated combinatorial problems*, in: [An], 73–112.

[Ge1] A. Geroldinger, *Über nicht-eindeutige Zerlegungen in irreduzible Elemente*, Math. Z. 197 (1988), 505–529.

[Ge2] —, *Chains of factorizations in weakly Krull domains*, Colloq. Math. 72 (1997), 53–81.

[Ge3] —, *Chains of factorizations and sets of lengths*, J. Algebra 188 (1997), 331–362.

[Ge4] —, *The catenary degree and tameness of factorizations in weakly Krull domains*, in: [An], 113–153.

[Ge5] A. Geroldinger, *On the structure and arithmetic of finitely primary monoids*, Czechoslovak Math. J. 46 (1996), 677–695.
[Ge6] —, *T-block monoids and their arithmetical applications to certain integral domains*, Comm. Algebra 22 (1994), 1603–1615.
[G-L] A. Geroldinger and G. Lettl, *Factorization problems in semigroups*, Semigroup Forum 40 (1990), 23–38.
[Gi] R. Gilmer, *Commutative Semigroup Rings*, The University of Chicago Press, 1984.
[HK1] F. Halter-Koch, *Über Längen nicht-eindeutiger Faktorisierungen und Systeme linearer diophantischer Ungleichungen*, Abh. Math. Sem. Univ. Hamburg 63 (1993), 265 –276.
[HK2] —, *Finitely generated monoids, finitely primary monoids and factorization properties of integral domains*, in: [An], 31–72.
[HK3] —, *The integral closure of a finitely generated monoid and the Frobenius problem in higher dimensions*, in: Semigroups, C. Bonzini, A. Cherubini and C. Tibiletti (eds.), World Scientific, 1993, 86–93.
[HK4] —, *Finiteness theorems for factorizations*, Semigroup Forum 44 (1992), 112–117.
[HK5] —, *Divisor theories with primary elements and weakly Krull domains*, Boll. Un. Mat. Ital. B (7) 9 (1995), 417–441.
[HK6] —, *Elasticity of factorizations in atomic monoids and integral domains*, J. Théor. Nombres Bordeaux 7 (1995), 367–385.
[Ka] F. Kainrath, *Factorization in Krull monoids with infinite class group.*
[Na1] W. Narkiewicz, *Finite abelian groups and factorization problems*, Colloq. Math. 42 (1979), 319–330.
[Sc] H. Scheid, *Zahlentheorie*, 2. Auflage, B.I. Wissenschaftsverlag, 1994.
[Sl] J. Śliwa, *Remarks on factorizations in algebraic number fields*, Colloq. Math. 46 (1982), 123–130.
[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, 1997.

Institut für Mathematik
Karl-Franzens-Universität
Heinrichstraße 36
8010 Graz, Austria
E-mail: alfred.geroldinger@kfunigraz.ac.at

Received 20 August 1997;
revised 20 March 1998