# Part II

# Divisibility monoids

# Chapter 7

# Preliminaries

In the introduction, I explained that traces can be defined in two different ways: either as combinatorial structures (dependence graphs) or as elements of a free partially commutative monoid. The first part of the present work generalized the first approach considering $\Sigma$-dags. Now we are going to deal with a generalization of the second approach, i.e. we consider divisibility monoids. It might not be clear at first glance that they indeed generalize trace monoids since the divisibility monoids are defined in a different spirit than trace monoids, but from Theorem 8.2.10 it follows immediately that any trace monoid is a divisibility monoid. It is the aim of this part to carry over large parts of the theory of recognizable languages in the trace monoid to our setting of divisibility monoid.

This chapter starts with some simple monoid-theoretic preliminaries. Then, we introduce left divisibility monoids and show some of their basic properties that will be useful in our further considerations. These definitions as well as the results in the first two sections are taken from [DK99, DK00]. In the last Section 7.3 of this chapter, a Foata Normal Form for the elements of a divisibility monoid is defined and considered. This Foata Normal Form, besides the fact that it stresses the connection with trace monoids, will be useful later in Chapter 10 where we will characterize when a divisibility monoid satisfies Kleene's Theorem.

## 7.1 Monoid-theoretic preliminaries

A triple $(M, \cdot, 1)$ is a *monoid* if $M$ is a set, $\cdot : M \times M \to M$ is an associative operation and $1 \in M$ is the *unit element* satisfying $1 \cdot x = x \cdot 1 = x$ for any $x \in M$. Let $(M, \cdot, 1)$ be a monoid and $X \subseteq M$. Then, by $\langle X \rangle$ we denote the submonoid of $M$ generated by $X$, i.e. the intersection of all submonoids of $M$ that contain $X$. If $\langle X \rangle = M$, $X$ is a *set of generators of* $M$. The monoid $M$ is *finitely generated* if it has a finite set of generators. Let $X$ be a set. Then $X^\star$ denotes the set of all words over $X$. With the usual concatenation of words and the empty word as unit element, this becomes a *free monoid generated by* $X$.

Let $M = (M, \cdot, 1)$ be a monoid. We call $M$ *cancellative* if $x \cdot y \cdot z = x \cdot y' \cdot z$ implies $y = y'$ for any $x, y, y', z \in M$. This in particular ensures that $M$ does not contain a zero element (i.e. an element $z$ such that $z \cdot x = x \cdot z = z$ for any $x \in M$). Now let $x \cdot y = z$. Then, in a cancellative monoid $y$ is uniquely determined. We denote it by $x^{-1}z$. For $x, y \in M$, *$x$ is a left divisor of $y$* (denoted $x \leq y$) if there is $z \in M$ such that $x \cdot z = y$. In general, the relation $\leq$ is not antisymmetric.

**Lemma 7.1.1** *Let $(M, \cdot, 1)$ be a cancellative monoid and $a \in M$. Then the mapping $a : (M, \leq) \to (a \cdot M, \leq)$ defined by $a(x) := a \cdot x$ is a quasi order isomorphism.*

**Proof.** Since the monoid $M$ is cancellative, the mapping $a$ is bijective. Now let $b, c \in M$. If $ab \leq ac$, we find $d \in M$ such that $abd = ac$. Now $b \leq c$ follows by cancellation. The other implication is trivial. □

Let $T := (M \setminus \{1\}) \setminus (M \setminus \{1\})^2$. The set $T$ consists of those elements of $M$ that do not have a proper divisor, its elements are called *irreducible*. Note that $T$ has to be contained in any set generating $M$.

The set of *rational sets* in a monoid $(M, \cdot, 1)$ is the least class $\mathfrak{C} \subseteq 2^M$ such that

- all finite subsets of $M$ belong to $\mathfrak{C}$,
- $X \cdot Y = \{x \cdot y \mid x \in X, y \in Y\}$ and $X \cup Y$ belong to $\mathfrak{C}$ whenever $X, Y \in \mathfrak{C}$, and
- $\langle X \rangle$ belongs to $\mathfrak{C}$ whenever $X \in \mathfrak{C}$.

A set $L \subseteq M$ is *recognizable* iff there exists a finite monoid $(S, \cdot, 1)$ and a homomorphism $\eta : M \to S$ such that $L = \eta^{-1}\eta(L)$. Recognizable sets are sometimes called recognizable *languages*. It is easily verified that the set of recognizable languages in a monoid $(M, \cdot, 1)$ is closed under the usual set-theoretic operations union, intersection and complementation. Furthermore, in any monoid the empty set as well as the whole set are recognizable.

In general, the sets of recognizable and of rational subsets of a monoid are different and even incomparable. For finitely generated monoids, it is known that any recognizable set is rational (and that this property characterizes the finitely generated monoids). The other implication holds in particular in finitely generated free monoids:

**Kleene's Theorem ([Kle56]).** *Let $T$ be a finite set. Then a set $L \subseteq T^\star$ is rational iff it is recognizable.*

Since the set of recognizable languages is closed under the usual set-theoretic operations, the set of rational languages in the free monoid $T^\star$ enjoys these closure properties.

For $x \in T^\star$, let $\alpha(x)$ denote the alphabet of $x$ comprising all letters of $T$ that occur in $x$. Then $L_B := \langle B\rangle \cap L \setminus (\bigcup_{A\subset B} \langle A\rangle)$ with $B \subseteq T$ is the set of elements $x$ of $L$ with $\alpha(x) = B$. If $L$ is rational, the language $L_B$ is rational, too. The language $L$ is *monoalphabetic* if $L = L_B$ for some $B \subseteq T$. The class of *monoalphabetic-rational languages* (m-rational for short) in $T^\star$ is the smallest class $\mathfrak{C} \subseteq 2^{T^\star}$ satisfying

- all finite subsets of $T^\star$ belong to $\mathfrak{C}$,
- $X \cdot Y$ and $X \cup Y$ belong to $\mathfrak{C}$ whenever $X, Y \in \mathfrak{C}$, and
- $\langle X\rangle$ belongs to $\mathfrak{C}$ whenever $X \in \mathfrak{C}$ is monoalphabetic.

The following lemma seems to be folklore but we could not find an explicit reference.

**Lemma 7.1.2** *Let $T$ be a finite set. Then a language in $T^\star$ is rational iff it is m-rational.*

**Proof.** The implication $\Leftarrow$ is trivial. For the other implication, one shows by induction on the size of $B \subseteq T$ that $\langle L\rangle_B$ is m-rational for any rational language $L$. Then the result follows since $\langle L\rangle$ is the union of these languages.

For $B = \emptyset$, the statement is trivial. Now observe that

$$\langle L\rangle_B = K \cdot \langle K\rangle \cdot \bigcup_{X\subset B} \langle L\rangle_X$$

with $K = \bigcup_{\substack{C\neq B \\ C\cup D=B}} \langle L\rangle_C \cdot L_D$. By the induction hypothesis for $C, X \subset B$, the languages $\langle L\rangle_C$ and $\langle L\rangle_X$ are m-rational. In addition, $K$ is monoalphabetic (its alphabet equals $B$). Hence $(L^\star)_B$ is m-rational. □

## 7.2 Definition and basic properties of divisibility monoids

**Definition 7.2.1** A monoid $(M, \cdot, 1)$ is called a *left divisibility monoid* provided the following hold

1. $M$ is cancellative and its irreducible elements form a finite set of generators of $M$,
2. $x \wedge y$ exists for any $x, y \in M$, and
3. $(\downarrow x, \leq)$ is a distributive lattice for any $x \in M$.

Note that by the third axiom the prefix relation in a left divisibility monoid is a partial order relation. Since, by Lemma 7.1.1, $y \leq z$ implies $x \cdot y \leq x \cdot z$, a left divisibility monoid is a left ordered monoid. Ordered monoids where the order relation is the intersection of the prefix and the suffix relation were investigated e.g. in [Bir73] under the name "divisibility monoid". Despite that we require more than just the fact that $(M, \cdot, \leq)$ be a left ordered monoid this might explain why we call the monoids defined above "left divisibility monoid". Since Birkhoff's divisibility monoids will not appear in our investigations any more, we will simply speak of "divisibility monoids" as an abbreviation for "left divisibility monoid".

Let $(M, \cdot, 1)$ be a divisibility monoid and let $x, y \in M$ with $x \cdot y = 1$. Then $1 \leq x \leq 1$ implies $x = 1$ since by the third axiom $\leq$ is a partial order. Hence we have $y = x \cdot y = 1$, i.e. there are no proper divisors of the unit element.

**Example 7.2.2** Using classical results from trace theory, one can show that any (finitely generated) trace monoid is a left divisibility monoid. Now let $\Sigma = \{a, b, c, d\}$ be an alphabet. Let $\sim^1$ be the least congruence on the free monoid $\Sigma^\star$ that identifies the words $ab$ and $cd$. In a trace monoid, the equality $ab = cd$ implies $\{a, b\} = \{c, d\}$ for any generators $a, b, c, d$. Hence the quotient monoid $\Sigma^\star/\sim^1$ is not a trace monoid. But, as we will see later, it is a divisibility monoid. Similarly, let $\sim^2$ identify $aa$ and $bb$. Again, $\Sigma^\star/\sim^2$ is no trace but a divisibility monoid. Finally, identifying $aa$ and $bc$ again results in a divisibility monoid. The proof that these three monoids are indeed divisibility monoids is delayed to Chapter 8 where we will give a finite representation for divisibility monoids (cf. Theorem 8.2.10).

Since a divisibility monoid $(M, \cdot, 1)$ is generated by the set $T$ of its irreducible elements, there is a natural epimorphism $\mathrm{nat} : T^\star \to M$. Now let $A \subseteq M$ be finite and $x \in M$ with $A \leq x$. Since $(\downarrow x, \leq)$ is a lattice, the supremum $y$ of $A$ *in this lattice* exists. Now let $z \in M$ be an upper bound of $A$ in $(M, \leq)$ which is not necessarily in the lattice $\downarrow x$. Then $y$ and $z$ have an infimum $y \wedge z$ in $(M, \leq)$. This infimum is an upper bound of $A$ dominated by $y$. Thus $y = y \wedge z \leq z$.

Hence $y$ is even the supremum of $A$ in the partially ordered set $(M, \leq)$. Thus we showed that any finite set, bounded above, has a supremum in $(M, \leq)$ (Lemma 7.2.3 below will imply that this holds for any bounded set $A$). This supremum of $A$ can be viewed as the least common multiple of $A$, whereas the infimum of $A$ is the greatest common (left-)divisor of $A$. Note that $(M, \leq)$ is not necessarily a lattice since it may contain unbounded pairs of elements. By Lemma 7.1.1, multiplication in a left divisibility monoid $(M, \cdot, 1)$ from the left (but not from the right) distributes over infima and suprema, i.e. $a \cdot (b \wedge c) = ab \wedge ac$ for any $b, c \in M$ and $a \cdot (b \vee c) = ab \vee ac$ provided $\{b, c\}$ (or, equivalently, $\{ab, ac\}$) is bounded above. This is essential in the following proof that shows that any element of a divisibility monoid has only finitely many left divisors:

**Lemma 7.2.3** *Let $(M, \cdot, 1)$ be a divisibility monoid and $m \in M$. Then $\downarrow m$ is finite.*

**Proof.** Let $T \subseteq M$ be the set of irreducible elements of $M$. Then $T$ is a finite set of generators of $M$. By contradiction, assume $n \in \mathbb{N}$ minimal such that there exist $x_1, \ldots, x_n \in T$ with $\downarrow(x_1 \cdot x_2 \ldots x_n)$ infinite. Then $n \geq 2$. Let $m := x_1 \cdot x_2 \ldots x_n$. Since the set $\downarrow m$ is an infinite distributive lattice, it contains an infinite chain $C$. By Lemma 7.1.1, $(\{y \in M \mid x_1 \leq y \leq m\}, \leq) \cong (\downarrow(x_2 \cdot x_3 \ldots x_n), \leq)$. Since $n$ is minimal, the sets $\downarrow x_1$ and $\{y \in M \mid x_1 \leq y \leq m\}$ are finite. Hence there exist $x, y \in C$ such that $x < y$, $x \vee x_1 = y \vee x_1$ and $x \wedge x_1 = y \wedge x_1$. Since $\downarrow m$ is distributive and complements in a distributive lattice are unique [Bir73, Corollary to Theorem II.13], this implies $x = y$ contradicting $x < y$. □

Thus, for an element $m$ of a divisibility monoid, $(\downarrow m, \leq)$ is a finite distributive lattice. Let $|m|$ denote the length of this lattice which equals the size of any maximal chain deduced by 1. It is easily checked that $x \prec\!\!\!\cdot\; y$ iff there exists $t \in T$ with $x \cdot \mathrm{nat}(t) = y$ for any $x, y \in M$. Hence the maximal chains in $\downarrow m$ correspond to the words $w \in T^\star$ with $\mathrm{nat}(w) = m$. This implies that any two such words have the same length which equals $|m|$.

By the second requirement on divisibility monoids, the partial order $(M, \leq)$ can be seen as the set of compacts of a Scott-domain. The lemma above ensures that it is even the set of compacts of a dI-domain (cf. [Ber78, Win87]). Thus, we have in particular $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$ whenever the left hand side is defined.

Let $M$ again be a divisibility monoid. Two elements $x$ and $y$ are *complementary* (denoted by $x \,\mathbf{co}\, y$) if $x \wedge y = 1$ and $\{x, y\}$ is bounded above. In this case the supremum $z = x \vee y$ exists in $M$. Then $x$ and $y$ are "complementary" elements of the lattice $\downarrow z$ which explains our choice of the name. Since $M$ is cancellative, there is a unique element $z$ such that $y \cdot z = x \vee y$. This element $z$ is called *the residuum of $x$ after $y$* and denoted by $x \uparrow y$. Note that it is defined for comple-

mentary elements $x$ and $y$ only. Hence $x \uparrow y$ is defined iff $y \uparrow x$ is defined and in this case $x(y \uparrow x) = y(x \uparrow y)$. Fixing $x \in M$, we get a unary partial function $r_x$ from $M$ to $M$ by $\mathrm{dom}(r_x) := \{y \in M \mid x \,\mathbf{co}\, y\}$ and $r_x(y) := y \uparrow x$. The function $r_x$ will be called the *residuum function of* $x$. We may turn it into a total function on $M$ by introducing an additional element. Therefore an equation $r_x(y) = r_z(y')$ means "$r_x(y)$ is defined iff $r_z(y')$ is defined and in this case they are equal".

As an example, consider the trace monoid over the dependence alphabet $(\Sigma, D)$. Then the infimum of two traces $s$ and $t$ is trivial whenever no letter occurs in $s$ as well as in $t$. In this case the set $\{s, t\}$ is bounded iff any letter from $s$ is independent from any letter from $t$. Hence $s$ and $t$ are complementary if and only if they are independent in the sense of trace theory. Now assume $s$ and $t$ to be independent traces. Then their supremum equals $st = ts$. Hence the residuum of $s$ after $t$ equals $s$, i.e. the residuum function $r_t$ is contained in the identity function $\mathrm{id}_{\mathbb{M}(\Sigma,D)}$ and is completely given by the set of letters that occur in $t$. In other words, the notion of a "residuum function" in a trace monoid is pretty trivial, but in the context of divisibility monoids it turns out to be of great importance as most of our proofs rely on this concept.

**Lemma 7.2.4** *Let $(M, \cdot, 1)$ be a divisibility monoid and $x, y \in M$ with $x \,\mathbf{co}\, y$. The residuum function $r_x$ is injective on its domain. Furthermore, $|y| = |r_x(y)|$.*

**Proof.** Let $y' \in \mathrm{dom}(r_x)$ with $r_x(y) = r_x(y')$. Then $x \wedge y = x \wedge y' = 1$. By the definitions of $\uparrow$ and $r_x$ we get $x \vee y = x(y \uparrow x) = x(y' \uparrow x) = x \vee y'$. Hence $y$ and $y'$ are complements of $x$ in the lattice $\downarrow(x \vee y)$. Since complements in a distributive lattice are unique [Bir73], this implies $y = y'$.

To show that $r_x$ is length preserving, let $z = x \vee y = x \cdot r_x(y)$. Then $x$ is the complement of $y$ in the distributive lattice $\downarrow z$. Hence the height of $z$ is the sum of the heights of $x$ and $y$ in this lattice [Bir73]. □

Next we show some formulas satisfied by the residuum functions that will be useful in our subsequent considerations.

**Lemma 7.2.5** *Let $(M, \cdot, 1)$ be a divisibility monoid and $x, x', y, z \in M$.*

1. *$x \,\mathbf{co}\, yz$ iff $x \,\mathbf{co}\, y$ and $r_y(x) \,\mathbf{co}\, z$.*
2. *$r_{yz}(x) = r_z(r_y(x))$; in other words $x \uparrow (yz) = (x \uparrow y) \uparrow z$.*
3. *$r_x(yz) = r_x(y) \cdot r_{r_y(x)}(z)$; equivalently $yz \uparrow x = (y \uparrow x) \cdot (z \uparrow (x \uparrow y))$.*
4. *If $r_x = r_{x'}$ and $y \,\mathbf{co}\, x$ then $r_{r_y(x)} = r_{r_y(x')}$.*

**Proof.** 1. First we show the implication $\Rightarrow$. Therefore, let $x \,\mathbf{co}\, yz$. Then $x \wedge yz = 1$ and the set $\{x, yz\}$ is bounded above. Hence $x \wedge y = 1$ and $\{x, y\}$ is bounded above since $y \leq yz$, i.e. $x \,\mathbf{co}\, y$. To show that $r_y(x) \,\mathbf{co}\, z$, note that $r_y(x)$ is defined since $x$ and $y$ are complementary. Then $yr_y(x) = x \vee y$ by the definition of $r_y$. Note that $\{x, yz\}$ and therefore $\{x, y, yz\}$ is bounded above. Hence $\{x \vee y, yz\}$ is bounded above. Now the boundedness of $\{r_y(x), z\}$ follows by $x \vee y = yr_y(x)$ and Lemma 7.1.1. Furthermore,

$$\begin{array}{rcll} y \cdot (r_y(x) \wedge z) & = & yr_y(x) \wedge yz & \text{by Lemma 7.1.1} \\ & = & (x \vee y) \wedge yz & \\ & = & (x \wedge z) \vee (y \wedge yz) & \text{by distributivity} \\ & = & 1 \vee y = y & \text{since } x \,\mathbf{co}\, yz \text{ and } y \leq yz \end{array}$$

Since $M$ is cancellative, we showed $r_y(x) \wedge z = 1$.

To show the inverse implication, let $x \,\mathbf{co}\, y$ and $r_y(x) \,\mathbf{co}\, z$. Then $x \wedge yz \leq (x \vee y) \wedge yz = yr_y(x) \wedge yz$. By Lemma 7.1.1 this equals $y(r_y(x) \wedge z)$. Since $r_y(x) \,\mathbf{co}\, z$ we get $x \wedge yz \leq y$. Hence $x \wedge yz = x \wedge y \wedge yz = 1 \wedge yz = 1$ since $x \,\mathbf{co}\, y$. To show that $\{x, yz\}$ is bounded, note that $\{yr_y(x), yz\}$ is bounded by $r_y(x) \,\mathbf{co}\, z$ and Lemma 7.1.1. Hence $\{x \vee y, yz\}$ and therefore $\{x, yz\}$ are bounded which finishes the proof of the first statement.
2. Since $M$ is cancellative, the following equation implies $r_{yz}(x) = r_z(r_y(x))$:

$$\begin{array}{rcll} yzr_{yz}(x) & = & x \vee yz & \text{by the definition of the function } r_{yz} \\ & = & (x \vee y) \vee yz & \text{since } y \leq yz \\ & = & yr_y(x) \vee yz & \\ & = & y(r_y(x) \vee z) & \text{by Lemma 7.1.1} \\ & = & yzr_z(r_y(x)). & \end{array}$$

3. Similarly, $r_x(yz) = r_x(y)r_{r_y(x)}(z)$ follows from the following equation since we can cancel $x$ from the left:

$$\begin{array}{rcll} xr_x(yz) & = & x \vee yz = x \vee y \vee yz & \text{since } y \leq yz \\ & = & yr_y(x) \vee yz & \text{since } x \vee y = yr_y(x) \\ & = & y(r_y(x) \vee z) & \text{by Lemma 7.1.1} \\ & = & yr_y(x)r_{r_y(x)}(z) = (x \vee y)r_{r_y(x)}(z) & \\ & = & xr_x(y)r_{r_y(x)}(z). & \end{array}$$

4. Let $z \in \mathrm{dom}(r_{r_y(x)})$. By the second statement and $r_x = r_{x'}$, we obtain $r_x(y)r_{r_y(x)}(z) = r_x(yz) = r_{x'}(yz) = r_{x'}(y)r_{r_y(x')}(z) = r_x(y)r_{r_y(x')}(z)$. Now we can conclude $r_{r_y(x)}(z) = r_{r_y(x')}(z)$ by cancelling $r_x(y)$ from the left. $\square$

Note that the second statement implies $r_z \circ r_y = r_{yz}$ where $\circ$ is the usual concatenation of partial functions. Hence the set $\mathbb{R}_M = \{r_x \mid x \in M\}$ is closed under concatenation. Since $r_1$ is the identity function on $M$, $(\mathbb{R}_M, \circ, r_1)$ is a

monoid, *the monoid of residuum functions of* $M$. The function $r : M \to \mathbb{R}_M$ with $r(x) := r_x$ is a monoid antihomomorphism. We say that $M$ *has finitely many residuum functions* if $\mathbb{R}_M$ is finite, i.e. there are only finitely many different functions $r_x$ ($x \in M$). Actually, it is not clear whether this is a definite restriction since we do not know any divisibility monoid with infinitely many residuum functions. But, on the other hand, we did not succeed in proving that any divisibility monoid has finitely many residuum functions.

Later, we will need the following

**Lemma 7.2.6** *Let $M$ be a divisibility monoid and $x, y \in M$ with $x \mathbin{\mathbf{\infty}} y$ and $r_x \subseteq \mathrm{id}_M$. Then $r_{r_y(x)} \subseteq \mathrm{id}_M$.*

**Proof.** Let $z \in \mathrm{dom}(r_{r_y(x)})$, i.e. $z \mathbin{\mathbf{\infty}} r_y(x)$. Then (by Lemma 7.2.5(1)) $x \mathbin{\mathbf{\infty}} yz$ implying $r_x(yz) = yz$. But $r_x(yz) = yz \upharpoonright x = (y \upharpoonright x) \cdot (z \upharpoonright (x \upharpoonright y)) = y \cdot r_{r_y(x)}(z)$ by Lemma 7.2.5(3). Since we can cancel $y$ from the left, we get $z = r_{r_y(x)}(z)$, i.e. $r_{r_y(x)} \subseteq \mathrm{id}_M$. □

Recall that $\mathrm{nat} : T^\star \to M$ is a homomorphism. Thus, one can easily define functions $\mathrm{res}_x : T^\star \to T^\star$ for $x \in M$ such that $\mathrm{nat} \circ \mathrm{res}_x = r_x \circ \mathrm{nat}$. E.g. one could choose any normal form function NF: $M \to T^\star$ with $\mathrm{nat} \circ \mathrm{NF}(x) = x$ for $x \in M$ and then define $\mathrm{res}_x(w) := \mathrm{NF} \circ r_x \circ \mathrm{nat}(w)$. But then $\mathrm{im}(\mathrm{res}_x)$ consists of normal forms, only. Thus, this partial function was not injective on its domain. In addition, an equation similar to Lemma 7.2.5(3) was very unlikely to hold. Therefore, we follow another way: Recall that for $t \in T$ and $x \in M$ with $x \mathbin{\mathbf{\infty}} t$ we have $|t| = |r_x(t)|$ by Lemma 7.2.4 and therefore $r_x(t) \in T$. Hence $\mathrm{res}_x(t) := r_x(t)$ (if $t \mathbin{\mathbf{\infty}} x$) is a partial function mapping $T$ to $T$. We extend it to a partial function from $T^\star$ to $T^\star$ by $\mathrm{res}_x(tu) := \mathrm{res}_x(t)\mathrm{res}_{r_t(x)}(u)$. Then one can easily check that

$$\mathrm{res}_x(t_1 t_2 \dots t_n) = \mathrm{res}_x(t_1)\mathrm{res}_{r_{\mathrm{nat}(t_1)}(x)}(t_2)\mathrm{res}_{r_{\mathrm{nat}(t_1 t_2)}(x)}(t_3) \dots \mathrm{res}_{r_{\mathrm{nat}(t_1 t_2 \dots t_{n-1})}(x)}(t_n)$$

and therefore

$$\mathrm{res}_x(uv) = \mathrm{res}_x(u)\mathrm{res}_{r_{\mathrm{nat}(u)}(x)}(v). \tag{7.1}$$

Now let $x, y \in M$, $t \in T$ and $u \in T^\star$. We get immediately $\mathrm{res}_{xy}(t) = r_{xy}(t) = r_y(r_x(t)) = \mathrm{res}_y(\mathrm{res}_x(t))$ since $r_x$ and $r_y$ are length preserving. Now we can conclude

$$\begin{aligned}
\mathrm{res}_y(\mathrm{res}_x(tu)) &= \mathrm{res}_y(\mathrm{res}_x(t)\mathrm{res}_{r_t(x)}(u)) && \text{by (7.1)}\\
&= \mathrm{res}_y(\mathrm{res}_x(t)) \cdot \mathrm{res}_{r_{\mathrm{res}_x(t)}(y)}(\mathrm{res}_{r_t(x)}(u)) && \text{by (7.1)}\\
&= \mathrm{res}_{xy}(t) \cdot \mathrm{res}_{r_t(x) r_{\mathrm{res}_x(t)}(y)}(u)\\
&= \mathrm{res}_{xy}(t) \cdot \mathrm{res}_{r_t(xy)}(u)\\
&= \mathrm{res}_{xy}(tu).
\end{aligned}$$

Now let $v \in T^\star$ be a word over $T$. Then we define $\mathrm{res}_v := \mathrm{res}_{\mathrm{nat}(v)}$. Thus, $\mathrm{dom}(\mathrm{res}_v) = \{u \in T^\star \mid \mathrm{nat}(u) \mathbin{\mathbf{\infty}} \mathrm{nat}(v)\}$. We write $u \mathbin{\mathbf{\infty}} v$ for $u \in \mathrm{dom}(\mathrm{res}_v)$. Note that, similarly to $r_x$, we have the following

**Lemma 7.2.7** *Let $(M, \cdot, 1)$ be a divisibility monoid and $u, v, w \in T^\star$.*

$$\begin{aligned} \mathrm{res}_{vw}(u) &= \mathrm{res}_w(\mathrm{res}_v(u)), \\ \mathrm{res}_u(vw) &= \mathrm{res}_u(v)\ \mathrm{res}_{\mathrm{res}_v(u)}(w), \text{ and} \\ \mathrm{nat}(\mathrm{res}_v(u)) &= r_{\mathrm{nat}(v)}(\mathrm{nat}(u)). \end{aligned}$$

*Furthermore,* $\mathrm{res}_u$ *is injective on its domain and length preserving.*

**Proof.** Immediate by Lemmas 7.2.4 and 7.2.5. □

Let $\mathbb{D}_M = \{\mathrm{res}_u \mid u \in T^\star\}$ be the set of all residuum functions of words over $T$. Then $(\mathbb{D}_M, \circ, \mathrm{res}_\varepsilon)$ is a monoid and $\mathrm{res} : T^\star \to \mathbb{D}_M : u \mapsto \mathrm{res}_u$ is a monoid antihomomorphism by Lemma 7.2.7. Since $\mathrm{nat}(t) = t$ for $t \in T$, in this case the third equation can be written as $\mathrm{res}_v(t) = r_{\mathrm{nat}(v)}(t)$. Using the first and the third equation from Lemma 7.2.7, the mapping $\mathrm{res}_u \mapsto r_{\mathrm{nat}(u)}$ turns out to be a monoid homomorphism from $(\mathbb{D}_M, \circ, \mathrm{res}_\varepsilon)$ onto $(\mathbb{R}_M, \circ, r_1)$. The following lemma shows that it is injective, i.e. that it is even an isomorphism.

**Lemma 7.2.8** *Let $u, v \in T^\star$. Then $\mathrm{res}_u = \mathrm{res}_v$ iff $r_{\mathrm{nat}(u)} = r_{\mathrm{nat}(v)}$.*

**Proof.** The implication $\Rightarrow$ is immediate by the third equation from Lemma 7.2.7. Now let $r_{\mathrm{nat}(u)} = r_{\mathrm{nat}(v)}$. If $t \in T$ and $\mathrm{res}_u(t)$ is defined, then $r_{\mathrm{nat}(u)}(t) = r_{\mathrm{nat}(v)}(t)$ and therefore $\mathrm{res}_v(t)$ is defined. Furthermore, $\mathrm{res}_u(t) = r_{\mathrm{nat}(u)}(t) = \mathrm{res}_v(t)$ proving the claim for arguments from $T$. Now let $w \in T^\star$. Then $\mathrm{res}_u(tw) = \mathrm{res}_u(t)\ \mathrm{res}_{r_t(\mathrm{nat}(u))}(w)$. By the above argument, $\mathrm{res}_u(t) = \mathrm{res}_v(t)$. Furthermore, by Lemma 7.2.5(4), $r_{r_t(\mathrm{nat}(u))} = r_{r_t(\mathrm{nat}(v))}$. Now $\mathrm{res}_{r_t(\mathrm{nat}(u))}(w) = \mathrm{res}_{r_t(\mathrm{nat}(v))}(w)$ follows from the induction hypothesis. Hence $\mathrm{res}_u(tw) = \mathrm{res}_v(t)\ \mathrm{res}_{r_t(\mathrm{nat}(v))}(w) = \mathrm{res}_v(tw)$. □

Let $u, u', v, w \in T^\star$. If $\mathrm{res}_w(u) = v$ and $\mathrm{nat}(u) = \mathrm{nat}(v)$, by the third equation in Lemma 7.2.7, it holds $\mathrm{nat}(\mathrm{res}_w(u')) = \mathrm{nat}(v)$. Conversely, assume $\mathrm{nat}(\mathrm{res}_w(u')) = \mathrm{nat}(v)$. Then the following lemma shows that there exists $u \in T^\star$ with $\mathrm{res}_w(u) = v$ (by the injectivity of $r_{\mathrm{nat}(w)}$ in addition $\mathrm{nat}(u) = \mathrm{nat}(u')$).

**Lemma 7.2.9** *Let $x, y \in M$ and $t_i \in T$ for $1 \leq i \leq n$ such that $r_x(y) = \mathrm{nat}(t_1 t_2 \ldots t_n)$. Then there exist $s_i \in T$ for $1 \leq i \leq n$ such that $\mathrm{res}_x(s_1 s_2 \ldots s_n) = t_1 t_2 \ldots t_n$. These elements $s_i$ of $T$ are unique.*

**Proof.** Since $x \wedge y = 1$, the intervals $[1, y]$ and $[x, x \vee y]$ are transposed and therefore isomorphic by [Bir73, Theorem I.13] and an isomorphism is given by $a \mapsto a \vee x$ for $a \in {\downarrow}y$. Inductively, define $s_i$ to be the unique element in $M$ with

$\mathrm{nat}(s_1 s_2 \dots s_i) \vee x = x \cdot \mathrm{nat}(t_1 t_2 \dots t_i)$. Then one can easily show that $s_i$ does not have a proper divisor. In addition, $t_{i+1} = s_{i+1} \uparrow (x \uparrow \mathrm{nat}(s_1 s_2 \dots s_i))$ and therefore $\mathrm{res}_x(s_1 s_2 \dots s_n) = t_1 t_2 \dots t_n$. The uniqueness is immediate by the proof. □

## 7.3 A Foata Normal Form

Throughout this section, let $(M, \cdot, 1)$ be a fixed divisibility monoid and let $T$ denote the set of its irreducible elements. For simplicity, let $\mathbb{J}(x)$ denote the join-irreducible elements of the distributive lattice $\downarrow x$ for any $x \in M$. We define the set of *cliques* $\mathcal{Cl}$ to consist of all nonempty subsets of $T$ that are bounded above. Since any subset of $M$ that is bounded above has a supremum, we have $\mathcal{Cl} = \{A \subseteq T \mid \emptyset \neq A \text{ and } \sup(A) \text{ exists}\}$. Let $A \in \mathcal{Cl}$. Then any two distinct elements $s, t \in A$ are bounded above. Furthermore, since $s$ is an atom in the partially ordered set $(M, \leq)$, the infimum of $s$ and $t$ belongs to $\{1, s\}$. But $s$ and $t$ are incomparable. Hence we showed that any two distinct elements of $A$ are complementary. But this property does not characterize the cliques. The reason is that even if any two elements of $A \subseteq T$ are bounded above, the set $A$ need not be bounded.

Next we define the set FNF consisting of words over $\mathcal{Cl}$ as

$$\{A_1 A_2 \dots A_n \in \mathcal{Cl}^\star \mid \forall t \in A_{i+1} \forall B \in \mathcal{Cl} : \sup B \neq (\sup A_i) \cdot t \text{ for } 1 \leq i < n\}.$$

Since the condition that constitutes membership in FNF is local, FNF is a rational language in $\mathcal{Cl}^\star$. In addition, FNF is closed under cancellation from the left and from the right, i.e. $U, V, W \in \mathcal{Cl}^\star$ with $UVW \in \mathrm{FNF}$ implies $V \in \mathrm{FNF}$. Let $\alpha' : \mathcal{Cl} \to M$ denote the mapping that associates with any clique $A \in \mathcal{Cl}$ its supremum $\sup A$ in $M$. This mapping can be extended uniquely to a monoid homomorphism $\alpha$ from $\mathcal{Cl}^\star$ to $M$. Then $\alpha(A_1 A_2 \dots A_n) = (\sup A_1) \cdot (\sup A_2) \cdot \dots \cdot (\sup A_n)$. This mapping is surjective since $\alpha(\{t_1\}\{t_2\} \dots \{t_n\}) = t_1 \cdot t_2 \cdot \dots \cdot t_n$ for any $t_i \in T$ and $T$ generates $M$. On the other hand, it is easily seen not to be injective. The set FNF is particularly useful since it provides normal forms for the elements of $M$, i.e. since the restriction of $\alpha$ to FNF is a bijection (cf. Lemma 7.3.3). But before we can prove this lemma, we need some more order theory:

Let $(L, \leq)$ be a distributive lattice and $x \in L$. Then the set $\uparrow x$ together with the partial order $\leq \cap (\uparrow x \times \uparrow x)$ is a distributive lattice with join-irreducible elements $\mathbb{J}(\uparrow x)$. Note that in general $\mathbb{J}(\uparrow x) \neq \mathbb{J}(L) \cap \uparrow x$. The following lemma relates the join-irreducible elements of $L$ and those of $(\uparrow x, \leq)$.

**Lemma 7.3.1** *Let $(L, \leq)$ be a finite distributive lattice and $x \in \mathbb{J}(L)$. The mapping $f : \mathbb{J}(L) \setminus \downarrow x \to \mathbb{J}(\uparrow x)$ with $f(y) = x \vee y$ is an order isomorphism.*

**Proof.** Let $y \in \mathbb{J}(L) \setminus {\downarrow}x$. First we show that $f(y) \in \mathbb{J}({\uparrow}x)$: Let $a, b \in L$ with $x \leq \{a, b\}$ and $a \vee b = x \vee y$. Then we have $y = y \wedge (x \vee y) = y \wedge (a \vee b) = (y \wedge a) \vee (y \wedge b)$. Since $y$ is join-irreducible in $(L, \leq)$, this implies (without loss of generality) $y = y \wedge a$, i.e. $y \leq a$. Thus, we have $\{x, y\} \leq a \leq x \vee y$. Hence, $a = x \vee y$ proving that $x \vee y$ is join-irreducible in the distributive lattice $(x{\uparrow}, \leq)$.

To show that $f$ is order preserving and reflecting, let $y_1, y_2 \in \mathbb{J}(L)$. Clearly, $y_1 \leq y_2$ implies $x \vee y_1 \leq x \vee y_2$. Suppose conversely $x \vee y_1 \leq x \vee y_2$. Then $y_1 \leq x \vee y_2$. Since $y_1 \not\leq x$, we obtain $y_1 \leq y_2$ from the fact that $y_1$ is prime in $(L, \leq)$. □

**Lemma 7.3.2** *Let $W = A_1 A_2 \dots A_n \in$ FNF and $x := \alpha(W) \in M$. Then we have $A_1 = \{t \in T \mid t \leq x\}$, and $\alpha(A_1 A_2 \dots A_i) = \sup\{y \in \mathbb{J}(x) \mid h(y, \mathbb{J}(x)) < i\}$ for $1 \leq i \leq n$.*

**Proof.** Since $t \leq \alpha(A_1) \leq \alpha(W) = x$ for $t \in A_1$, the inclusion "$\subseteq$" is immediate. For simplicity, let $A = \{t \in T \mid t \leq x\}$. Then $A \in \mathcal{C}\ell$ and $({\downarrow}(\sup A), \leq)$ is isomorphic to the power set of $A$, ordered by inclusion. If $A_1 \neq A$, there is $t \in T$ with $\sup(A_1) \cdot t \leq \alpha(A) \leq x = \alpha(A_1)\alpha(A_2 A_3 \dots A_n)$. By cancellation, we get $t \leq \alpha(A_2 A_3 \dots A_n)$. Inductively, this implies $t \in A_2$ since $A_2 A_3 \dots A_n \in$ FNF. Hence we found $t \in A_2$ and a clique $A \in \mathcal{C}\ell$ such that $\sup(A_1) \cdot t \leq \sup(A)$. Since $({\downarrow}\sup(A), \leq)$ is isomorphic to the powerset of $A$, there is $B \subseteq A$ with $\sup(A_1) \cdot t = \sup(B)$, contradicting $A_1 A_2 \in$ FNF.

Note that $\{y \in \mathbb{J}(x) \mid h(y, \mathbb{J}(x)) < 1\} = \{t \in T \mid t \leq x\}$. Hence the second statement holds for $i = 1$. Now assume

$$a := \alpha(A_1 A_2 \dots A_{i-1}) = \sup\{y \in \mathbb{J}(x) \mid h(y, \mathbb{J}(x)) < i - 1\}.$$

Then $a \cdot z = x$ with $z = \alpha(A_i A_{i+1} \dots A_n)$. Since $A_i A_{i+1} \dots A_n \in$ FNF, by the first statement, $A_i = \{t \in T \mid t \leq z\}$ follows. Thus $\alpha(A_1 A_2 \dots A_i) = \alpha(A_1 A_2 \dots A_{i-1}) \cdot \alpha(A_i) = a \cdot \sup\{t \in T \mid t \leq z\}$. Then $\alpha(A_1 A_2 \dots A_i) = a \vee \sup\{at \mid t \in T, t \leq z\}$ by Lemma 7.1.1. Note that $\{at \mid t \in T, t \leq z\}$ is the set of elements of the distributive lattice $([a, az], \leq)$ of height 1 in this lattice. Hence it is the set of elements of height 0 in the set $(\mathbb{J}([a, az]), \leq)$ of join-irreducibles. Now Lemma 7.3.1 implies

$$\begin{aligned} \{at \mid t \in T, t \leq z\} &= \{y \in \mathbb{J}([a, az]) \mid h(y, \mathbb{J}([a, az])) = 0\} \\ &= \{a \vee y' \mid y' \in \mathbb{J}(az) \setminus {\downarrow}a \text{ and } h(y', \mathbb{J}(az) \setminus {\downarrow}a) = 0\}. \end{aligned}$$

Since ${\downarrow}a \cap \mathbb{J}(az) = \{y' \in \mathbb{J}(az) \mid h(y', \mathbb{J}(az)) < i - 1\}$, we get

$$\{at \mid t \in T, t \leq z\} = \{a \vee y' \mid y' \in \mathbb{J}(az) \text{ and } h(y', \mathbb{J}(az)) = i - 1\}$$

and therefore

$$\begin{aligned}\alpha(A_1A_2\dots A_i) &= a \vee \sup\{a \vee y' \mid y' \in \mathbb{J}(az) \text{ and } h(y', \mathbb{J}(az)) = i-1\} \\ &= a \vee \sup(y \in \mathbb{J}(az) \mid h(y, \mathbb{J}(az) = i-1\} \\ &= \sup\{y' \in \mathbb{J}(az) \mid h(y', \mathbb{J}(az)) < i\}.\end{aligned}$$

□

Now the bijectivity of $\alpha \restriction \mathrm{FNF}$ follows:

**Lemma 7.3.3** *The mapping $\alpha \restriction \mathrm{FNF} : \mathrm{FNF} \to M$ is bijective.*

**Proof.** The injectivity follows inductively from the first statement of Lemma 7.3.2. To show surjectivity, let $x, y \in M \setminus \{1\}$, $A = \{t \in T \mid t \leq x\}$, $a = \sup(A)$, $a \cdot y = x$ and $B = \{t \in T \mid t \leq y\}$. It is sufficient to show that $AB \in \mathrm{FNF}$, i.e. that $A, B \in \mathcal{C\ell}$ and that $\sup(C) \neq \sup(A) \cdot t$ for any $t \in B$ and $C \in \mathcal{C\ell}$. But $A$ and $B$ are nonempty since $x \neq 1 \neq y$, and $A$ and $B$ have suprema since they are bounded by $x$ and $y$, respectively. Thus, $A, B \in \mathcal{C\ell}$. Now assume $t \in B$ and $C \in \mathcal{C\ell}$ with $\sup(C) = \sup(A) \cdot t$. Then, for any $s \in C$: $s \leq \sup(A) \cdot t \leq x$ implies $s \in A$, i.e. $C \subseteq A$. But this contradicts $\sup(C) > \sup(A)$. □

Thus, for any $x \in M$, the set $\alpha^{-1}(x) \cap \mathrm{FNF}$ is a singleton. We denote the unique preimage of $x$ in FNF by $\mathrm{fnf}(x)$ and call it the *Foata Normal Form* of $x$. An immediate consequence of the second statement of Lemma 7.3.2 is

**Corollary 7.3.4** *Let $x \in M$. Then $|\mathrm{fnf}(x)|$ exceeds the length of the partially ordered set $(\mathbb{J}(x), \leq)$ by 1.*

Next we show that the Foata Normal Form of $\mathrm{nat}(w)$ can be computed from the word $w \in T^\star$ by an automaton. In general, this automaton has infinitely many states. But for "width-bounded divisibility monoids" (cf. Section 10.2) it will be shown to be finite. This finiteness will be the basis for our proof that "width-bounded divisibility monoids" are rational and therefore satisfy Kleene's Theorem.

An *automaton over a monoid $M$* is a quintuple $\mathcal{A} = (Q, M, E, I, F)$ where

1. $Q$ is a set of *states*,
2. $E \subseteq Q \times M \times Q$ is a set of *transitions*, and
3. $I, F \subseteq Q$ are the sets of *initial and final states*, respectively.

The automaton $\mathcal{A}$ is *finite* if $E$ is. We will write $p \xrightarrow{a} q$ for $(p, a, q) \in E$. A *computation* in $\mathcal{A}$ is a finite sequence of transitions:

$$p_0 \xrightarrow{a_1} p_1 \xrightarrow{a_2} p_2 \cdots \xrightarrow{a_n} p_n.$$

It is *successful* if $p_0 \in I$ and $p_n \in F$. The *label* of the computation is the element $a_1 \cdot a_2 \cdots a_n$ of the monoid $M$. For a computation with first state $p_0$, last state $p_n$ and label $a$, we will usually write $p_0 \xrightarrow{a} p_n$ without mentioning the intermediate states. The *behavior of* $\mathcal{A}$ is the subset $|\mathcal{A}|$ of $M$ consisting of labels of successful computations in $\mathcal{A}$.

If the monoid $M$ is a direct product $M_1 \times M_2$ of two monoids, it is convenient to think of $M_1$ as the input and of $M_2$ as the output of the automaton. Then the automaton computes from an input in $M_1$ an output from $M_2$. In our context, the input will be in the free monoid $T^\star$ and the output in the free monoid $\mathcal{C}\ell^\star$ (actually, in the recognizable language FNF $\subseteq \mathcal{C}\ell^\star$). Therefore, we will construct an automaton $\mathcal{A}_M$ over the monoid $T^\star \times \mathcal{C}\ell^\star$ as follows. The state set is the direct product of $M$ and $\mathcal{C}\ell_\varepsilon := \mathcal{C}\ell \cup \{\varepsilon\}$, the only initial state is $(1, \varepsilon)$ and the set of final states is $\{1\} \times \mathcal{C}\ell_\varepsilon$. Now let $(x, A), (z, C) \in M \times \mathcal{C}\ell_\varepsilon$ and $(t, B) \in T \times \mathcal{C}\ell_\varepsilon$. Then $(x, A) \xrightarrow{(t,B)} (z, C)$ iff

**1.** $t \leq x$, $B = \varepsilon$, $t \cdot z = x$ and $C = A$, or

**2.** $t \between x$, $B = C \neq \varepsilon$, $AB \in$ FNF, and $t \cdot z = x \cdot (\sup B)$.

Since the transition relation is defined for labels from $T \times \mathcal{C}\ell_\varepsilon$, only, the length of a computation equals that of the input word from $T^\star$. Furthermore, the transition relation $E$ in this automaton is deterministic since, for any state $(x, A)$ and any $(t, B) \in T \times \mathcal{C}\ell_\varepsilon$ at most one of the conditions $t \leq x$ or $t \between x$ can be satisfied. Thus, the starting state and the label of a computation determine its last state completely. This final state is described in the following lemma.

**Lemma 7.3.5** *Let $w \in T^\star$, $B_1 B_2 \ldots B_m \in \mathcal{C}\ell^\star$, $z \in M$ and $C \in \mathcal{C}\ell_\varepsilon$. Then in the automaton $\mathcal{A}_M$, $(1, \varepsilon) \xrightarrow{(w, B_1 B_2 \ldots B_m)} (z, C)$ iff*

**(i)** $|\mathrm{fnf} \circ \mathrm{nat}(w)| = m$,

**(ii)** $\mathrm{fnf}(\mathrm{nat}(w) \cdot z) = B_1 B_2 \ldots B_m$, *and*

**(iii)** $C = B_m$.

**Proof.** We prove the lemma by induction on the length of the input word $w$. Since the only computation with input word $\varepsilon \in T^\star$, starting in $(1, \varepsilon)$, is $(1, \varepsilon) \xrightarrow{(\varepsilon, \varepsilon)} (1, \varepsilon)$, the statement is obvious for $|w| = 0$. Now assume that the statement holds whenever $|w| < n$.

Now, let $v \in T^\star$ and $t \in T$ with $vt = w$ and $|w| = n$ and assume that $(1,\varepsilon) \overset{(w,B_1B_2\ldots B_m)}{\longrightarrow} (z,C)$ holds. First, consider the case that the last transition in this computation is of the first kind, i.e. that $(1,\varepsilon) \overset{(v,B_1B_2\ldots B_m)}{\longrightarrow} (t\cdot z,C) \overset{(t,\varepsilon)}{\to} (z,C)$. Then $\mathrm{fnf}(\mathrm{nat}(w)z) = \mathrm{fnf}(\mathrm{nat}(v)\cdot tz)$ which equals $B_1B_2\ldots B_m$ by the induction hypothesis. Thus, (ii) holds. To show (i), note that $m = |\mathrm{fnf}(\mathrm{nat}(v))| \leq |\mathrm{fnf}(\mathrm{nat}(vt)\cdot z)| = m$, i.e. $|\mathrm{fnf}(\mathrm{nat}(vt))| = m$. Finally, (iii) holds since by the induction hypothesis $C = B_m$. Now assume that the last transition is of the second kind, i.e. there is a state $(x,A)$ such that $(1,\varepsilon) \overset{(v,B_1B_2\ldots B_{m-1})}{\longrightarrow} (x,A) \overset{(t,B_m)}{\to} (z,C)$ with $t \,\mathbf{\omega}\, x$, $B_m = C \neq \varepsilon$, $AB_m \in \mathrm{FNF}$, and $tz = x(\sup B_m)$. By the induction hypothesis, $|\mathrm{fnf}(\mathrm{nat}(v))| = m-1$, $\mathrm{fnf}(\mathrm{nat}(v)\cdot x) = B_1B_2\ldots B_{m-1}$ and $A = B_{m-1}$. Then $\mathrm{nat}(vt)\cdot z = \mathrm{nat}(v)\cdot x\cdot \sup(B_m) = \alpha(B_1B_2\ldots B_m)$. Since the words $B_1B_2\ldots B_{m-1}$ and $B_{m-1}B_m = AB_m$ belong to FNF, we have $B_1B_2\ldots B_m \in \mathrm{FNF}$, i.e. we showed (ii). It remains to show that $m$ is the length of $\mathrm{fnf}(vt)$. Clearly, $m-1 = |\mathrm{fnf}(\mathrm{nat}(v))| \leq |\mathrm{fnf}(\mathrm{nat}(vt)\cdot z)| = m$. Now assume $|\mathrm{fnf}(\mathrm{nat}(vt))| = m-1$. Then, by Corollary 7.3.4, the partially ordered set $(\mathbb{J}(\mathrm{nat}(vt)),\leq)$ has length $m-2$, i.e. $\mathbb{J}(\mathrm{nat}(vt)) \subseteq \{y \in \mathbb{J}(\mathrm{nat}(w)z) \mid h(y,\mathbb{J}(\mathrm{nat}(w)z)) \leq m-2\}$. Hence from Lemma 7.3.2 we get

$$\begin{aligned}\mathrm{nat}(vt) &= \sup \mathbb{J}(\mathrm{nat}(vt))\\ &\leq \sup\{y \in \mathbb{J}(\mathrm{nat}(w)z) \mid h(y,\mathbb{J}(\mathrm{nat}(w)z)) \leq m-2\}\\ &= \alpha(B_1B_2\ldots B_{m-1}) = \mathrm{nat}(v)x\end{aligned}$$

by the induction hypothesis. Hence $t \leq x$ by cancellation, contradicting $t \,\mathbf{\omega}\, x$. Thus, we showed $|\mathrm{fnf}(\mathrm{nat}(vt))| = m$, i.e. (iii).

Conversely, let $|\mathrm{fnf}(\mathrm{nat}(vt))| = m$, $\mathrm{fnf}(\mathrm{nat}(vt)\cdot z) = B_1B_2\ldots B_m$ and $C = B_m$. We want to show $(1,\varepsilon) \overset{(vt,B_1B_2\ldots B_m)}{\longrightarrow} (z,C)$. First, assume $|\mathrm{fnf}(\mathrm{nat}(v))| = m$. Then $(t\cdot z,C) \overset{(t,\varepsilon)}{\to} (z,C)$. Since $|\mathrm{fnf}(\mathrm{nat}(v))| = m$, $\mathrm{fnf}(\mathrm{nat}(v)\cdot t\cdot z) = B_1B_2\ldots B_m$ and $C = B_m$, we can apply the induction hypothesis and get $(1,\varepsilon) \overset{(v,B_1B_2\ldots B_m)}{\longrightarrow} (t\cdot z,C)$. Thus, $(1,\varepsilon) \overset{(vt,B_1B_2\ldots B_m)}{\longrightarrow} (z,C)$.

Now consider the case $|\mathrm{fnf}(\mathrm{nat}(v))| < m$. Since $\mathrm{nat}(v) \prec\!\!\!\cdot\, \mathrm{nat}(vt)$ in the partially ordered set $(M,\leq)$, there is $y \in \mathbb{J}(\mathrm{nat}(vt))$ with $\mathbb{J}(\mathrm{nat}(v))\dot\cup\{y\} = \mathbb{J}(\mathrm{nat}(vt))$. Hence the length of $(\mathbb{J}(\mathrm{nat}(v)),\leq)$ and that of $(\mathbb{J}(\mathrm{nat}(vt)),\leq)$ differ at most by one, i.e. $|\mathrm{fnf}(\mathrm{nat}(v))| = m-1$ by Corollary 7.3.4. Therefore, $\mathrm{nat}(v) \leq \alpha(B_1B_2\ldots B_{m-1})$ by Corollary 7.3.4. Since the length of the partially ordered set $(\mathbb{J}(\alpha(B_1B_2\ldots B_{m-1}),\leq))$ is $m-2$ and that of $(\mathbb{J}(\mathrm{nat}(vt)),\leq)$ equals $m-1$, we get $\mathrm{nat}(vt) \not\leq \alpha(B_1B_2\ldots B_{m-1})$.

From $\mathrm{nat}(v) \leq \alpha(B_1B_2\ldots B_{m-1})$, we deduce the existence of $x \in M$ such that $\mathrm{nat}(v)\cdot x = \alpha(B_1B_2\ldots B_{m-1})$. This implies in particular $\mathrm{fnf}(\mathrm{nat}(v)\cdot x) = B_1B_2\ldots B_{m-1}$. In addition, $\mathrm{nat}(v)\cdot x\cdot\alpha(B_m) = \alpha(B_1B_2\ldots B_{m-1}B_m) = \mathrm{nat}(vt)\cdot z$. Hence $x\alpha(B_m) = t\cdot z$. To show $(x,B_{m-1}) \overset{(t,B_m)}{\to} (z,B_m)$, it remains to prove $t \,\mathbf{\omega}\, x$. Since $\{t,x\} \leq t\cdot z$ and $t \in T$, it is sufficient to ensure $t \not\leq x$. So assume $t \leq x$.

Then $\mathbb{J}(\mathrm{nat}(vt)) \subseteq \mathbb{J}(\mathrm{nat}(v) \cdot x)$. Hence the length of $\mathbb{J}(\mathrm{nat}(vt))$ is bounded by that of $(\mathbb{J}(\mathrm{nat}(v) \cdot x), \leq)$ which equals $m-2$ since $\mathrm{fnf}(\mathrm{nat}(v) \cdot x) = B_1 B_2 \ldots B_{m-1}$. But this contradicts $|\mathrm{fnf}(\mathrm{nat}(vt))| = m$. Hence indeed $(x, B_{m-1}) \overset{(t,B_m)}{\rightarrow} (z, B_m)$.

Recall that $|\mathrm{fnf}(\mathrm{nat}(v))| = m-1$ and $\mathrm{fnf}(\mathrm{nat}(v) \cdot x) = B_1 B_2 \ldots B_{m-1}$. Hence, we can use the induction hypothesis and obtain $(1, \varepsilon) \overset{(v, B_1 B_2 \ldots B_{m-1})}{\longrightarrow} (x, B_{m-1})$. But this implies $(1, \varepsilon) \overset{(vt, B_1 B_2 \ldots B_m)}{\longrightarrow} (z, B_m)$ since $(x, B_{m-1}) \overset{(t,B_m)}{\rightarrow} (z, B_m)$. □

Now we can show that the automaton $\mathcal{A}_M$ computes for any input word $w \in T^\star$ the Foata Normal Form $\mathrm{fnf} \circ \mathrm{nat}(w)$ of the associated element of the divisibility monoid $M$:

**Theorem 7.3.6** *Let $M$ be a divisibility monoid. Then the behavior $|\mathcal{A}_M|$ of the automaton $\mathcal{A}_M$ is the relation $\{(w, \mathrm{fnf}(\mathrm{nat}(w)) \mid w \in T^\star\}$ in $T^\star \times \mathcal{C}\ell^\star$, i.e. the automaton computes the function $\mathrm{fnf} \circ \mathrm{nat} : T^\star \to \mathcal{C}\ell^\star$.*

**Proof.** By Lemma 7.3.5, an element $(w, W)$ of $T^\star \times \mathcal{C}\ell^\star$ is the label of a successful computation, i.e. of a computation that starts in $(1, \varepsilon)$ and ends in $\{1\} \times \mathcal{C}\ell_\varepsilon$, if and only if $\mathrm{fnf}(\mathrm{nat}(w) \cdot 1) = W$. □