Chapter 8

A finite representation

By definition, trace monoids M are finitely presented, i.e. there exists a finite set E of equations of the form $ab = ba$ with $a, b \in \Sigma$ such that M is isomorphic to $\Sigma^\star/E$. Later, an algebraic characterization of trace monoids was found [Dub86]. Differently, divisibility monoids are defined by their algebraic properties. In this chapter, we show that they can be finitely presented (cf. Theorem 8.2.10). Not only will we show that this is possible in general, but we will give a concrete representation for any divisibility monoid (cf. Lemma 8.2.1). Finally, we give a decidable class of finite presentations that give rise to all divisibility monoids. But first, we prove two order-theoretic results that we will need in this context.

8.1 Order-theoretic preliminaries

Lemma 8.1.1 *Let $(M, \leq)$ be a partially ordered set with least element such that*

1. *$\downarrow x$ is finite for any $x \in M$, and*
2. *for any x, y_1, y_2, z with $x \multimap y_1, y_2$ and $\{y_1, y_2\} \leq z$, the least upper bound $y_1 \vee y_2$ in $(M, \leq)$ exists.*

Then any two elements of M that are bounded above have a least upper bound in $(M, \leq)$.

Proof. Let $y_1, y_2, z \in M$ with $y_1, y_2 \leq z$. We have to show that y_1 and y_2 admit a supremum. It can be assumed that y_1 and y_2 are incomparable for otherwise we were done. Since $(M, \leq)$ has a least element there is $x \in M$ with $x \leq y_1, y_2$. Since $\downarrow z$ is finite, the size of the chains in $[x, z]$ is bounded. We will prove the existence of $y_1 \vee y_2$ by induction on the size of these chains.

If any chain in $[x, z]$ has size at most 2, we have $x \multimap y_1, y_2$. Hence $y_1 \vee y_2$ exists. Now assume that any chain in $[x, z]$ has at most $n + 1$ elements. Let C_i for $i = 1, 2$ be maximal chains in $[x, z]$ containing y_i. Since C_i is maximal,

it contains x. Let x_i be the least element of $C_i \setminus \{x\}$. Since y_1 and y_2 are incomparable, this implies $x \prec\!\!\!\cdot\; x_i \leq y_i$ for $i = 1, 2$. Hence the supremum $x_1 \vee x_2 =: a$ exists. Note that x_i is a lower bound of y_i and a. Since $x \prec\!\!\!\cdot\; x_i \leq z$, the chains in the interval $[x_i, z]$ contain at most n elements. Hence by the induction hypothesis $y_i' := y_i \vee a$ exist for $i = 1, 2$. Since $x \prec\!\!\!\cdot\; x_1 \leq a$, the size of the chains in the interval $[a, z]$ is bounded by n. Hence we can apply the induction hypothesis to y_1' and y_2' and obtain the existence of their supremum $y_1' \vee y_2'$.

We show that $b := y_1' \vee y_2'$ is the supremum of y_1 and y_2: Since $y_i \leq y_i'$, we obtain $y_i \leq b$ for $i = 1, 2$. Now let c be an upper bound of y_1 and y_2. Then it is an upper bound of x_1 and x_2 and therefore of a, too. Hence $y_i' \leq c$ for $i = 1, 2$ and therefore $b \leq c$. □

By the Vilhelm-Šik-Jakubik Theorem (cf. [Ste91, Theorem 4.14]), any finite semimodular lattice that is not modular contains a non-modular interval of length 3. Next, we prove a similar result that distinguishes modular from distributive lattices[1]

Lemma 8.1.2 *Let $(L, \leq)$ be a finite modular but non-distributive lattice. Then it contains a non-distributive interval of length 2.*

Proof. Let $[a, b]$ be a minimal non-distributive interval. Since $[a, b]$ is modular and non-distributive, there are mutually distinct elements $y_1, y_2, y_3 \in [a, b]$ with $y_i \wedge y_j = a$ and $y_i \vee y_j = b$ for $1 \leq i < j \leq 3$ by [Bir73, Theorem II.13]. Hence the intervals $[a, y_i]$ and $[y_j, b]$ are transposed for $i \neq j$. Since the lattice $(L, \leq)$ is modular, all these intervals are mutually isomorphic [Bir73, Theorem I.13].

Let $a \prec\!\!\!\cdot\; a' \leq y_1$. Let $y_2' := y_2 \vee a'$ and $y_3' := y_3 \vee a'$. Then y_2' and y_3' belong to the interval $[a', b]$ which is distributive since it is a proper subinterval of $[a, b]$ (cf. Figure 8.1). Hence we have

$$\begin{array}{rcll} b & = & b \wedge b & \\ & = & (y_1 \vee y_3') \wedge (y_2' \vee y_3') & \text{since } y_i \leq y_i' \leq b \\ & = & (y_1 \wedge y_2') \vee y_3' & \text{since } y_1, y_2', y_3' \in [a', b] \\ & & & \quad \text{and this interval is distributive} \\ & = & (y_1 \wedge (y_2 \vee a')) \vee y_3' & \\ & = & ((y_1 \wedge y_2) \vee a') \vee y_3' & \text{since } a' \leq y_1 \text{ and } [a, b] \text{ is modular} \\ & = & y_3' & \text{since } (y_1 \wedge y_2) = a \leq a' \leq y_3'. \end{array}$$

[1] We give the proof although, by [FGL90, p. 270], it "is a well known result in the folklore of lattice theory".

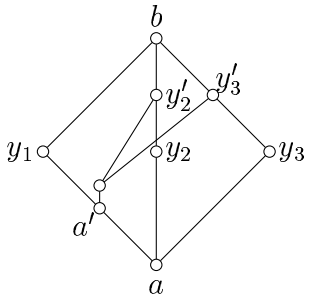

Figure 8.1: The elements from the proof of Lemma 8.1.2

Since $a = a' \wedge y_3$ and $b = y_3' = a' \vee y_3$, the intervals $[a, a']$ and $[y_3, b]$ are transposed and therefore isomorphic. Hence $y_3 \prec\!\!\!\cdot\, b$. Since the intervals $[a, y_i]$ and $[y_j, b]$ are mutually isomorphic, we therefore get $a \prec\!\!\!\cdot\, y_1 \prec\!\!\!\cdot\, b$, i.e. the interval $[a, b]$ has length 2. □

8.2 The finite presentation

Since a divisibility monoid M is generated by the set T of its irreducible elements, there is a congruence $\sim$ on the free monoid $T^\star$ such that the quotient $T^\star/\!\sim$ is isomorphic to M. The following result that was shown in [DK00] states that this congruence is quite natural and that the monoid M is finitely presentable.

Lemma 8.2.1 *Let M be a divisibility monoid and T the set of its irreducible elements. Let $\sim$ denote the least congruence on the free monoid $T^\star$ containing $\{(ab, cd) \mid a, b, c, d \in T \text{ and } a \cdot b = c \cdot d\}$. Then $\sim$ is the kernel of the natural epimorphism* $\mathrm{nat} : T^\star \to M$. *In particular, $M \cong T^\star/\!\sim$.*

Proof. Throughout this proof, we denote the product of $a, b \in T$ in the monoid M by $a \cdot b$, while the word is denoted by ab. Thus, $a \cdot b = \mathrm{nat}(ab) \in M$ and $ab \in T^\star$.

Note that $u \sim v$ implies that u and v have the same length.

Clearly, the kernel of nat contains $\sim$ since $a \cdot b = c \cdot d$ implies $\mathrm{nat}(ab) = \mathrm{nat}(cd)$ for $a, b, c, d \in T$. For the converse, let $u, v \in T^\star$ with $\mathrm{nat}(u) = \mathrm{nat}(v)$. We show $u \sim v$ by induction on the length of u: If $|u| = 0$, clearly, $\mathrm{nat}(u) = \mathrm{nat}(v) = 1$, so $u = v = \varepsilon$. If $|u| = 1$ then $u = v \in T$.

Now let $u = u_1u_2 \dots u_n$ and $v = v_1v_2 \dots v_n$ with $u_i, v_i \in T$ and $n \geq 2$. If $u_1 = v_1$, we get $\mathrm{nat}(u_2u_3 \dots u_n) = \mathrm{nat}(v_2v_3 \dots v_n)$ by cancellation. By the induction hypothesis, this implies $u_2u_3 \dots u_n \sim v_2v_3 \dots v_n$ and therefore $u_1u_2 \dots u_n \sim v_1v_2 \dots v_n$. Thus assume $u_1 \neq v_1$. Then u_1, v_1 are elements of the finite distributive lattice $\downarrow \mathrm{nat}(u)$. Hence there exist $b, d \in M$ such that $u_1 \cdot b = v_1 \cdot d = u_1 \vee v_1$. One even has $b, d \in T$ since the distributive lattice $\downarrow \mathrm{nat}(u)$ is semimodular [Bir73]. Note that $u_1b \sim v_1d$ by the definition of $\sim$. Since $u_1 \vee v_1 \leq \mathrm{nat}(u)$, we find $y \in T^\star$ such that $(u_1 \vee v_1) \cdot \mathrm{nat}(y) = \mathrm{nat}(u)$. Hence $\mathrm{nat}(u_1u_2 \dots u_n) = \mathrm{nat}(u_1by)$ and therefore $\mathrm{nat}(u_2 \dots u_n) = \mathrm{nat}(by)$ by cancellation. The induction hypothesis ensures $u_2 \dots u_n \sim by$. Now we have $\mathrm{nat}(v_1dy) = (u_1 \vee v_1) \cdot \mathrm{nat}(y) = \mathrm{nat}(u) = \mathrm{nat}(v)$ implying $\mathrm{nat}(dy) = \mathrm{nat}(v_2v_3 \dots v_n)$. Now $dy \sim v_2v_3 \dots v_n$ follows from the induction hypothesis since the length of $v_2v_3 \dots v_n$ equals $n - 1$. Thus, we have $u_1u_2 \dots u_n \sim u_1by \sim v_1dy \sim v_1v_2 \dots v_n$. □

In particular, Lemma 8.2.1 states that any divisibility monoid is (up to isomorphism) given by the equations $a \cdot b = c \cdot d$ for irreducible elements a, b, c, d that hold in M. Next, we want to characterize which sets of equations of this form give rise to divisibility monoids.

For the rest of this section, let T be a finite set and E a set of word equations over T of the form $ab = cd$ for $a, b, c, d \in T$. Let $\sim$ denote the least congruence on the free monoid $T^\star$ that contains E. In addition, let $M := T^\star/\!\sim$ be the quotient of the free monoid with respect to $\sim$. Furthermore, we require that the following hold in the monoid M for any $a, b, c, a', b', c' \in T$:

(i) $(\downarrow(a \cdot b \cdot c), \leq)$ is a distributive lattice,

(ii) $a \cdot b \cdot c = a \cdot b' \cdot c'$ or $b \cdot c \cdot a = b' \cdot c' \cdot a$ implies $b \cdot c = b' \cdot c'$, and

(iii) $a \cdot b = a' \cdot b'$, $a \cdot c = a' \cdot c'$ and $a \neq a'$ imply $b = c$.

We will show that M is a divisibility monoid.

Remark 8.2.2 Let $(\overline{M}, \cdot, 1)$ be a divisibility monoid. Let $\overline{T}$ be the set of irreducible generators of $\overline{M}$ and let $\overline{E}$ consist of all equations of the form $a \cdot b = c \cdot d$ with $a, b, c, d \in \overline{T}$ that hold in $\overline{M}$. Then by Lemma 8.2.1, $\overline{M} \cong \overline{T}^\star / \langle\overline{E}\rangle$. Furthermore, the distributivity in (i) is trivial since it holds for any $x \in \overline{M}$. Similarly, (ii) is a special instance of the cancellation property in $\overline{M}$. To show (iii) assume $a \cdot b = a' \cdot b'$, $a \cdot c = a' \cdot c'$ and $a \neq a'$. Then $ab \wedge ac$ exists. Note that a and a' are distinct lower bounds of $\{ab, ac\}$. Hence the infimum of ab and ac lies above a and a' and below ab. But since a and a' are direct predecessors of ab, this implies $ab \wedge ac = ab$. Hence $ab = ac$ implying $b = c$ by cancellation. Thus, any divisibility monoid can be obtained this way.

Example 8.2.3 As an example, consider the monoid $M = T^\star / \langle (ab, cd), (de, ed) \rangle$ where a, b, c, d, e are mutually different elements of the finite set T. Properties (i) and (ii) are easily checked by considering all possible situations. The third property is trivially satisfied. Let $\eta : (\mathbb{N} \times \mathbb{N}, +, (0,0)) \to (M, \cdot, 1)$ be the monoid homomorphism defined by $\eta(1,0) = d$ and $\eta(0,1) = e$. Then the preimage of the rational language $L = \langle (d \cdot e) \rangle \subseteq M$ in $\mathbb{N} \times \mathbb{N}$ is $\{(n,n) \mid n \in \mathbb{N}\}$. Since this set is not recognizable, L is not recognizable in M. Hence Kleene's Theorem does not hold in M. Furthermore, in any trace monoid $ab = cd$ for irreducible elements a, b, c and d implies $\{a, b\} = \{c, d\}$. Since this is not satisfied by $(M, \cdot, 1)$, this monoid is not free partially commutative.

Next, consider $M_1 = T^\star / \langle (ab, cc) \rangle$ and $M_2 = T^\star / \langle (aa, bb) \rangle$ where a, b, c are pairwise different elements of the finite set T. Again, these two monoids satisfy the conditions (i),(ii) and (iii). They are no trace monoids by the same argument as above. We only mention for the sake of completeness that these two are neither concurrency monoids as considered in [Dro95, Dro96, DK96, DK98] (where we extend the multiplication freely whenever it was the null element), since in concurrency monoids $ab = cc$ implies $a = b = c$.

Lemma 8.2.4 *Let $a, b, c \in T$. Then $ab \sim ac$ or $ba \sim ca$ implies $b = c$.*

Proof. First let $ab \sim ac$. Then $abb \sim acb$ and $abc \sim acc$. By (ii), this implies $bb \sim cb$ and $bc \sim cc$. Now (iii) ensures $b = c$. Now let $ba \sim ca$. Then $bba \sim bca$ implying by (ii) $bb \sim bc$. By what we saw before, this implies $b = c$. □

If v and w are words over T satisfying $v \sim w$, then w is obtained from v by a finite sequence of transformations according to the set of equations E. We call two words strongly equivalent if this sequence has length 1. More formally, v and w are *strongly equivalent* ($v \approx w$) if there are words $x, y \in T^\star$ and an equation $ab = cd$ in E such that $v = xaby$ and $w = xcdy$. Thus, w can be obtained from v by replacing two consecutive letters by equivalent ones (according to the set of equations E). To recall the position where this change has been made, we sometimes write it as an index to $\approx$, i.e. with the symbols from above, $v \approx_{|x|+1} w$. In the same spirit, let $\approx_{>i} = \bigcup_{j>i} \approx_j$. Then $v \approx_{>i} w$ denotes that one change has been made to obtain w from v and that this change occurred at a position behind i. Then $\sim$ is the least equivalence on the set $T^\star$ that contains the relation $\approx$.

For a word $w \neq \varepsilon$, let w^h denote the first letter (the "head") and w^t the remaining word (the "tail"), i.e. $w^h \in T$ and $w = w^h w^t$. For a sequence $(w_0, w_1, \ldots w_k)$ of nonempty words, we will consider the number of changes in the first position, i.e.

$$\text{changes}(w_0, w_1, \ldots w_k) := |\{i \mid 0 \leq i < k \text{ and } w_i^h \neq w_{i+1}^h\}|.$$

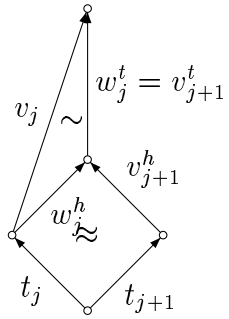

Figure 8.2: Condition (2) and (3) from Lemma 8.2.5

Let $v, w \in T^\star$ with $v \sim w$. The distance $d(v, w)$ denotes the minimal number of changes at the first position in a sequence that transforms v to w. More formally, it is the minimum over all integers changes$(w_0, w_1, \ldots, w_k)$ where w_i are words over T with $v = w_0$, $w_i \approx w_{i+1}$ and $w_k = w$.

Before showing that the distance is bounded, we give an alternative definition:

Lemma 8.2.5 *Let $v, w \in T^\star$ with $v \sim w$. Then $d(v, w)$ is the least integer m such that there exist $t_j \in T$ and $v_j, w_j \in T^\star$ for $0 \leq j \leq m$ with*

(1) $v = t_0 v_0$,

(2) $v_j \sim w_j$ *for* $0 \leq j \leq m$,

(3) $t_j w_j^h \approx t_{j+1} v_{j+1}^h$, $w_j^t = v_{j+1}^t$, $t_j \neq t_{j+1}$ *for* $0 \leq j < m$, *and*

(4) $t_m w_m = w$.

The second and third statement are visualized by Figure 8.2.

Proof. By the definition of $d(v, w)$, it is sufficient to prove that the existence of $x_i \in T^\star$ with $v = x_0$, $x_i \approx x_{i+1}$, $x_n = w$ and $m =$ changes$(x_0, \ldots, x_n)$ is equivalent to the existence of $t_i \in T$ and $v_i, w_i \in T^\star$ satisfying (1)-(4).

First, let $x_i \in T^\star$ $(0 \leq i \leq n)$ with $v = x_0$, $x_i \approx x_{i+1}$, $x_n = w$, and changes$(x_0, \ldots, x_n) = m$. There exist $0 = i_0 < i_1 < \cdots < i_m < i_{m+1} = n + 1$ with

(a) $x_{i_j - 1}^h \neq x_{i_j}^h$ for $0 < j \leq m$ and

(b) $x_{i_j}^h = x_k^h$ for $0 \leq j \leq m$ and $i_j \leq k < i_{j+1}$.

Let $t_j := x^h_{i_j}$, $v_j := x^t_{i_j}$ and $w_j := x^t_{i_{j+1}-1}$ for $0 \leq j \leq m$. Then $v = x_0 = x^h_0 x^t_0 = t_0 v_0$ ensures property (1). Since $i_m < i_{m+1} = n+1$, we get $i_m \leq n < i_{m+1}$. Now (b) with $j = m$ and $k = n$ implies $t_m = x^h_{i_m} = x^h_n$. This implies $t_m w_m = x^h_n x^t_n = x_n = w$ which in turn proves property (4). To show (2), let $0 \leq j \leq m$. Then $x^h_k = t_j$ for $i_j \leq k < i_{j+1}$ and $t_j v_j = x_{i_j} \approx x_{i_j+1} \approx x_{i_j+2} \cdots \approx x_{i_{j+1}-1} = x^h_{i_{j+1}-1} x^t_{i_{j+1}-1} = t_j w_j$. Hence, by Lemma 8.2.4, the strong equivalence $x_k \approx x_{k+1}$ is induced by some change at a higher position, i.e. $x_k \approx_{>1} x_{k+1}$. But this implies $x^t_k \approx x^t_{k+1}$ and therefore $v_j \sim w_j$. To show (3), note that $t_j \neq t_{j+1}$ holds by (a). By (b) and the definition of w_j, we have $t_j w_j = x^h_{i_{j+1}-1} x^t_{i_{j+1}-1} = x_{i_{j+1}-1}$. Similarly, $t_{j+1} v_{j+1} = x^h_{i_{j+1}} x^t_{i_{j+1}} = x_{i_{j+1}}$ by the definition of t_{j+1} and v_{j+1}. Since $x_{i_{j+1}-1} \approx x_{i_{j+1}}$ we therefore get $t_j w_j \approx t_{j+1} v_{j+1}$. From (a), we obtain $t_j = x^h_{i_{j+1}-1} \neq x^h_{i_{j+1}} = t_{j+1}$. Hence $t_j w_j \approx_1 t_{j+1} v_{j+1}$ and therefore (3).

Conversely, let t_j, v_j and w_j satisfy (1)-(4) and consider the sequence

$$(t_0 v_0, t_0 w_0, t_1 v_0, t_1 w_1, \ldots, t_n v_n, t_n w_n).$$

Since $v_j \sim w_j$, we can put additional words between $t_j v_j$ and $t_j w_j$ all of which start with t_j such that the resulting sequence has the desired form. □

Now we can show that the distance is bounded by 1.

Lemma 8.2.6 *Let $v, w \in T^\star$ with $v \sim w$. Then*

(1) $d(v, w) \leq 1$ and

(2) if $v^h = w^h$, then $v^t \sim w^t$.

Proof. First of all suppose $d(v, w) \leq 1$ and $v^h = w^h$. Since v and w have the same first letter, $d(v, w) \neq 1$, i.e. $d(v, w) = 0$. Hence there is a sequence of words transforming v to w that leaves the first letter unchanged. This implies $v^t \sim w^t$. Thus, (1) implies (2) and we have to show the first statement, only. This is done by induction on the length of v which equals that of w. If $|v| \leq 1$, we get $d(v, w) = 0$. Next we consider the case $|v| = 2$. Then $(\downarrow[v^h v^t v^t], \leq)$ is a distributive lattice by (i). Using (ii), one gets that $(\downarrow[v], \leq)$ is a sublattice. Since it is of length 2, it contains at most 2 elements different from 1 and from $[v]$. Hence $d(v, w) \leq 1$.

By induction, we assume that (1) and (2) hold for any $v', w' \in T^\star$ with $v' \sim w'$ and $|v'| < |v|$.

Assume $n := d(v, w) > 1$. By Lemma 8.2.5, there are $t_i \in T$ and $v_i, w_i \in T^\star$ for $0 \leq i \leq n$ such that

$v = t_0 v_0$,
$v_i \sim w_i$ for $0 \leq i \leq n$,
$t_i w^h_i \approx t_{i+1} v^h_{i+1}$, $w^t_i = v^t_{i+1}$, $t_i \neq t_{i+1}$ for $0 \leq i < n$, and
$t_n w_n = w$.

We prove that there exist words $x, y \in T^\star$ satisfying $w_0 \sim x$, $y \sim v_2$ and $t_0x^h \approx t_2y^h$ or $t_0x^h = t_2y^h$. Once we will have found them, we can conclude $t_0w_0 \sim_{>1} t_0x(\approx_1 \cup =)t_2y \sim_{>1} t_2v_2$ which decreases the number of changes at the first position, contradicting $n = d(v, w)$.

First we consider the case $t_0 = t_2$ and show that $x = w_0$ and $y = v_2$ are the desired elements: By $t_0w_0^h \approx t_1v_1^h$ and $t_0v_2^h = t_2v_2^h \approx t_1w_1^h$, (iii) implies $v_1^h = w_1^h$ since $t_0 \neq t_1$. Thus we have $t_0x^h = t_0w_0^h \approx t_1v_1^h = t_1w_1^h \approx t_2v_2^h = t_0y^h$. Applying Lemma 8.2.4 to t_0x^h and t_0y^h, we get $x^h = y^h$, i.e. $t_0x^h = t_2y^h$ as required.

Now let $t_0 \neq t_2$. If $v_1^h = w_1^h$, we had $t_0w_0^h \sim t_1v_1^h = t_1w_1^h \sim t_2v_2^h$. As we saw above, $\downarrow[t_0w_0^h]$ contains at most 2 elements different from 1 and from $[t_0w_0^h]$. Since t_0, t_1 and t_2 are three elements of this set, we derived a contradiction. Hence we showed $v_1^h \neq w_1^h$. By the induction hypothesis for v_1 and w_1, we get $d(v_1, w_1) \leq 1$. Since they start with different letters, their distance is 1, i.e. there are in particular $a, b \in T$ and $z \in T^\star$ such that $v_1 \sim_{>1} v_1^haz \approx_1 w_1^hbz \sim_{>1} w_1$. This ensures

$$t_0w_0^ha \approx_1 t_1v_1^ha \approx_2 t_1w_1^hb \approx_1 t_2v_2^hb.$$

Hence t_0 and t_2 are different elements of the distributive lattice $(\downarrow[t_0w_0^ha], \leq)$. Therefore, there are $c, d, e \in T$ with $t_0c \sim t_2d$ and $t_0ce \sim t_0w_0^ha$. The latter in particular implies $ce \sim w_0^ha$ by (ii). Thus we have

$$t_2v_2^hb \sim t_0w_0^ha \sim t_0ce \approx_1 t_2de$$

which implies $v_2^hb \sim de$ by (ii) again. From the induction hypothesis (2), applied to the equivalence $v_1^haz \sim v_1 = v_1^hv_1^t$, the equivalence $az \sim v_1^t = w_0^t$ follows. Similarly, $bz \sim w_1^t = v_2^t$ follows from $w_1^hbz \sim w_1 = w_1^hw_1^t$. Hence we have

- $w_0 = w_0^hw_0^t \sim w_0^haz \approx_1 cez =: x$,
- $v_2 = v_2^hv_2^t \sim v_2^hbz \approx_1 dez =: y$, and
- $t_0x^h = t_0c \approx t_2d = t_2y^h$.

This proves that $x = cez$ and $y = dez$ satisfy the desired properties. □

Corollary 8.2.7 *$(M, \cdot, 1)$ is left cancellative and hence the left divisor relation $\leq$ is a partial order on M.*

Proof. Cancellation is immediate by Lemma 8.2.6 (2). To prove the antisymmetry of $\leq$, one uses the simple observation that $1 = [\varepsilon]$ has no left divisor. □

Recall that any equivalence class $[v]_\sim$ is finite since all its elements have the same length. Hence $\downarrow[v]_\sim$ is finite as well since prefixes of $[v]_\sim$ correspond to

prefixes of words equivalent to v. Hence the partially ordered set $(M, \leq)$ satisfies the first condition in Lemma 8.1.1. The following lemma shows that the second condition is satisfied as well:

Lemma 8.2.8 *Let $x \in M$ and $s, t \in T$ with $s \neq t$ such that $\{xs, xt\}$ is bounded above in $(M, \leq)$. Then there exists $a \in T$ such that xsa is the least upper bound of xs and xt in $(M, \leq)$.*

Proof. Since by Lemma 7.1.1 the function $y \mapsto xy$ is an order isomorphism, it is sufficient to consider the case $x = 1$. Let $y \in M$ with $s, t \leq y$. By Lemma 8.2.6, there are $a_y, b_y \in T$ with $sa_y \approx ta_y$ and $[sa_y] \leq y$. Now let $z \in M$ be some upper bound of s and t. Then, as for y, we obtain $a_z, b_z \in T$ with $sa_z \approx ta_z$ and $[sa_z] \leq z$. Now (iii) implies $a_y = a_z$. Hence xsa_y is the supremum of xs and xt in the partially ordered set $(M, \leq)$. □

By Lemma 8.1.1, the partially ordered set $\downarrow[v]_\sim$ is a lattice. Using the Vilhelm-Šik-Jakubik Theorem and Lemma 8.1.2, we show that it is distributive:

Lemma 8.2.9 *For $x, y \in M$, $(\downarrow x, \leq)$ is a distributive lattice and $x \wedge y$ exists.*

Proof. The set $\downarrow x \subseteq \{[v] \mid v \in T^\star, |v| \leq |x|\}$ is finite. By Lemma 8.2.8, we can apply Lemma 8.1.1. Hence $(\downarrow x, \leq)$ is a lattice since any two elements of $\downarrow x$ are bounded above. It is even semimodular by Lemma 8.2.8. To show that it is modular, consider some interval $[y, yabc]$ of $\downarrow x$ with $y \in M$ and $a, b, c \in T$. By left-cancellation (Corollary 8.2.7), it is sufficient to deal with the case $y = 1$. But then $[1, abc] = \downarrow(abc)$ which is distributive by (i) and therefore in particular modular. Hence by the Vilhelm-Šik-Jakubik Theorem [Ste91, Theorem 4.14], $\downarrow x$ is modular. To show distributivity, we consider some interval of length 2 and argue similarly using Lemma 8.1.2.

The set $\downarrow x \cap \downarrow y$ is finite and bounded. Hence, by Lemma 8.1.1, it has a least upper bound which is the maximal lower bound of x and y, i.e. $x \wedge y$ exists. □

Now we can prove the main theorem of this chapter.

Theorem 8.2.10 *Let T be a finite set and E a set of equations of the form $ab = cd$ with $a, b, c, d \in T$. Let $\sim$ be the least congruence on $T^\star$ containing E. Then $M := T^\star/\sim$ is a divisibility monoid if and only if (i)-(iii) hold for any $a, b, c, b', c' \in T$:*

(i) $(\downarrow(a \cdot b \cdot c), \leq)$ *is a distributive lattice,*

(ii) $a \cdot b \cdot c = a \cdot b' \cdot c'$ *or* $b \cdot c \cdot a = b' \cdot c' \cdot a$ *implies* $b \cdot c = b' \cdot c'$*, and*

(iii) $a \cdot b = a' \cdot b'$, $a \cdot c = a' \cdot c'$ *and* $a \neq a'$ *imply* $b = c$.

Furthermore, each divisibility monoid arises this way.

Proof. By Remark 8.2.2, it remains to show that T and E satisfying (i)-(iii) define a divisibility monoid. By Corollary 8.2.7 and Lemma 8.2.9, it remains to prove that $(M, \cdot, 1)$ is right cancellative. For this, it suffices to show that $xa = ya$ with $x, y \in M$ and $a \in T$ implies $x = y$. By contradiction, assume that $x \neq y$. Since the lattice $\downarrow xa$ is distributive, $z := x \wedge y \prec\!\!\!\cdot\, x, y$, i.e. there are $b, c \in T$ with $x = zb$ and $y = zc$. Hence $zba = zca$. Now $ba = ca$ follows from Corollary 8.2.7. Lemma 8.2.4 ensures $b = c$ and therefore $x = y$. □

Let (Σ, D) be a dependence alphabet. Let E denote the set of all equations $ab = ba$ for $(a, b) \in \Sigma^2 \setminus D$. Then $\mathbb{M}(\Sigma, D) = \Sigma^* / \langle E \rangle$. One can easily check that the three properties (i), (ii) and (iii) of the theorem above hold. Hence a trace monoid is indeed a divisibility monoid. On the other hand, there are many divisibility monoids that are not trace monoids as the following corollary exemplifies. The list of divisibility monoids with three generators was determined (by hand) together with Manfred Droste, and Christian Pech (Dresden) went on to compute all divisibility monoids with up to five generators using the GAP4-system [GAP99]:

Corollary 8.2.11 *There are precisely* 15 *divisibility monoids with* 3 *generators, namely the free monoid and those defined by the following sets of equations:*

$\{ab = ba\}$	$\{ab = ba, bc = cb\}$	$\{ab = ba, bc = cb, ac = ca\}$
$\{aa = bb\}$	$\{aa = bb, ac = bc, ca = bc\}$	$\{aa = bb, bc = cb, ac = ca\}$
$\{ab = bc\}$	$\{ab = bc, ba = cb\}$	$\{ab = bc, ba = cb, ac = ca\}$
	$\{ab = bc, ac = cb\}$	$\{ab = bc, ac = ca\}$
$\{aa = bc\}$	$\{aa = bc, cc = ba\}$	$\{aa = bc, bb = ca, cc = ab\}$

Furthermore, there are 219 *divisibility monoids with* 4 *generators and* 8371 *divisibility monoids with* 5 *generators.*

Note that only the monoids described in the first line (and the free monoid) are trace monoids with three generators. Also, up to isomorphism, there are only 10 trace monoids with 4, and 34 trace monoids with 5 generators.