To appear in: FCT01, Lecture Notes in Computer Science vol. 2138, 227-239, 2001, © Springer Verlag.

Divisibility Monoids: Presentation, Word Problem, and Rational Languages

Dietrich Kuske

Department of Mathematics and Computer Science
University of Leicester
LEICESTER
LE1 7RH, UK
D.Kuske@mcs.le.ac.uk

Abstract. We present three results on divisibility monoids. These divisibility monoids were introduced in [11] as an algebraic generalization of Mazurkiewicz trace monoids. (1) We give a decidable class of presentations that gives rise precisely to all divisibility monoids. (2) We show that any divisibility monoid is an automatic monoid [5]. This implies that its word problem is solvable in quadratic time. (3) We investigate when a divisibility monoid satisfies Kleene's Theorem. It turns out that this is the case iff the divisibility monoid is a rational monoid [25] iff it is width-bounded. The two latter results rest on a normal form for the elements of a divisibility monoid that generalizes the Foata normal form known from the theory of Mazurkiewicz traces.

1 Introduction

Different mathematical structures have been proposed to model the behavior of concurrent systems, among them process algebras, sets of partially ordered sets, Petri nets etc. One particular approach in this line of research is that introduced by Mazurkiewicz [21], now known as trace monoids. Since Mazurkiewicz's observation that trace monoids can be used to model the behavior of 1-safe Petri nets, much research has dealt with the topic, see [9] for a collection of surveys. Despite their success, certain limitations of trace monoids have been observed. Therefore, several generalizations were considered. One of these generalizations are divisibility monoids [12].[1] In this paper, we describe the relation to other classes of monoids known in theoretical computer science, namely to automatic [17], rational [25] and Kleene monoids. As corollaries, we obtain a quadratic lower bound for the complexity of the word problem and a characterization of those divisibility monoids that satisfy Kleene's theorem.

Mazurkiewicz traces model the sequential behavior of a parallel system in which the order of two independent actions is regarded as irrelevant. One considers pairs (Σ, I) where Σ is the set of actions, and I is a symmetric and irreflexive binary relation on Σ describing the independence of two actions. The trace monoid or free partially commutative monoid $\mathbb{M}(\Sigma, I)$ is then defined as the quotient $\Sigma^\star/{\sim}$ where $\sim$ is the congruence on the free monoid $\Sigma^\star$ generated by all equations $ab \sim ba$ with $(a, b) \in I$. Thus, originally, trace monoids are defined by a decidable class of presentations.

[1] Similar monoids have been considered in [7, 6] where they are related to braid and other groups traditionally of interest in mathematics.

An algebraic characterization of trace monoids was given only later by Duboc [13]. Divisibility monoids are a lattice theoretically easy generalization of these algebraic conditions. Our first result (Theorem 4) describes a decidable class of presentations that give rise precisely to all divisibility monoids. Since the canonical presentations for trace monoids belong to this class, our result can be seen as an extension of Duboc's characterization to the realm of divisibility monoids.

For trace monoids, the word problem can be solved in linear time [8]. From our presentation result, an exponential algorithm for the word problem in divisibility monoids follows immediately. But we show that one can do much better: The work on automatic groups [15] has been generalized to the realm of semigroups. Intuitively, a semigroup is automatic if it admits a presentation such that the equality can be decided by an automaton and such that the multiplication by generators can be performed by an automaton [17, 5]. In particular, Campbell et al. [5] showed that the word problem for any automatic semigroup is solvable in quadratic time. Theorem 8 shows that any divisibility monoid is an automatic semigroup. Hence, we can infer from the result of Campbell et al. that the word problem for any divisibility monoid can be solved in quadratic time. We do not know whether this result can be improved, but we have serious doubts that a linear time algorithm exists. Kleene [18] showed that in a free finitely generated monoid the recognizable languages are precisely the rational ones. It is known that in general this is false, but Kleene's result was generalized in several directions, e.g. to formal power series by Schützenberger [26], to infinite words by Büchi [4], and to rational monoids by Sakarovitch [25]. In all these cases, the notions of recognizability and of rationality were shown to coincide. This is not the case in trace monoids any more. Even worse, in any trace monoid (which is not a free monoid), there exist rational languages that are not recognizable. But a precise description of the recognizable languages in trace monoids using c-rational expressions could be given by Ochmański [22]. A further generalization of Kleene's and Ochmański's results to concurrency monoids was given in [10]. The proofs by Ochmański as well as by Droste heavily used the internal structure of the elements of the corresponding monoid. The original motivation for the consideration of divisibility monoids in [12] was the search for an algebraic version of these proofs. We succeeded showing that in a divisibility monoid with finitely many residuum functions, the recognizable languages coincide with the (m)c-rational ones (cf. [12] for precise definitions of these terms). Thus, two main directions of generalization of Kleene's Theorem in monoids are represented by Sakarovitch's rational monoids and by trace monoids. Since the only trace monoids that satisfy Kleene's Theorem are free monoids, these two directions are "orthogonal", i.e. the intersection of the classes of monoids in consideration is the set of free monoids. In [12] we already remarked that there are divisibility monoids that satisfy Kleene's Theorem and are not free. Thus, our further extension of Ochmański's result to divisibility monoids [12] is not "orthogonal" any more. In this paper, we describe the class of divisibility monoids that satisfy Kleene's Theorem. Essentially, Theorem 13 says that a divisibility monoid satisfies Kleene's Theorem if and only if it is rational if and only if it is width-bounded. Thus, in the context of divisibility monoids, the classes of Kleene monoids and rational monoids coincide which is not the case in general [23], and we give an internal characterization of these monoids.

Our proofs that any divisibility monoid is automatic as well as the proof that any divisibility monoid satisfying Kleene's Theorem is rational, use a normal form for the elements of a divisibility monoid. This normal form generalizes the Foata normal form from trace theory. It is studied in Section 3. Furthermore, we rely on the results by Campbell et al. from [5] on automatic semigroups, by Sakarovitch from [25] on rational monoids, on basic properties of distributive lattices that can be found in [2] and on Ramsey's Theorem [24].

2 Basic definitions

2.1 Order and monoid theoretic definitions

Let $(P, \leq)$ be a partially ordered set and $y \in P$. By $\downarrow y$, we denote the *principal ideal* generated by y, i.e. the set $\{x \in P \mid x \leq y\}$. For $x, y \in P$, we write $x \multimap\!\!< y$ if $x < y$ and there is no element properly between x and y. A set $A \subseteq P$ is an *antichain* if any two distinct elements of A are incomparable. The *width* of a partially ordered set $(P, \leq)$ is the supremum over all natural numbers n such that there exists an antichain $A \subseteq P$ with $n = |A|$. The width of P is denoted by $w(P, \leq)$. If the width of $(P, \leq)$ is finite, any antichain in P has at most $w(P, \leq)$ elements. If the width is infinite, $(P, \leq)$ contains finite antichains of arbitrary size. In particular, the width of a finite partially ordered set is always finite. A *chain* is a set $C \subseteq P$ whose elements are mutually comparable. For $x \in P$, the *height* $h(x)$ in the poset $(P, \leq)$ is the maximal size of a chain all of whose elements are properly below x. The *length* of the poset $(P, \leq)$ is the maximal height of its elements.

A *lattice* is a partially ordered set $(P, \leq)$ where any two elements $x, y \in P$ admit a supremum $x \vee y$ and an infimum $x \wedge y$, i.e. a least upper and a largest lower bound. The lattice $(P, \leq)$ is *distributive* if for any $x, y, z \in P$ we have $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$. For many results concerning lattices see [2]. In particular, any two maximal chains in a finite distributive lattice have the same size.

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.

A subset L of a monoid M is *rational* if it can be constructed from the finite subsets of M by the operations concatenation $\cdot$, union $\cup$ and iteration $\langle . \rangle$ (also known as Kleene-star). 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*. In general, the sets of recognizable and of rational subsets of a monoid are different and even incomparable. If the notions of recognizability and rationality coincide in a monoid M, then the monoid M is said to be a *Kleene monoid*. Kleene showed that this holds in free finitely generated monoids:

Kleene's Theorem [18]. *Let X be a finite set. Then a set $L \subseteq X^\star$ is rational iff it is recognizable.*

Let X be a set and $\beta : X^\star \to X^\star$ a function which is not necessarily an homomorphism. Let furthermore M be a monoid. The function β is a *normal form function for M* if it is idempotent, the kernel $\ker(\beta) = \{(v, w) \in X^\star \times X^\star \mid \beta(v) = \beta(w)\}$ is a monoid congruence, and $X^\star/\ker(\beta) \cong M$. A monoid M is *rational* [25] if there exist a finite alphabet X and a normal form function $\beta : X^\star \to X^\star$ for M such that $\{(v, \beta(v)) \mid v \in X^\star\}$ is a rational subset of the monoid $X^\star \times X^\star$.

In [25, 23], the authors are particularly interested in closure properties of the class of rational monoids. Sakarovitch [25, Theorem 4.1] also shows that any rational monoid is a Kleene monoid (there are Kleene monoids which are not rational, see [23] for an example).

2.2 Divisibility monoids

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 $x \in M$). For $x, z \in M$, x *is a left divisor of* z (denoted $x \leq z$) if there is $y \in M$ such that $x \cdot y = z$. In general, the relation $\leq$ is not antisymmetric, but reflexive and transitive, i.e., a preorder.

Lemma 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 preorder isomorphism.*

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

Definition 2. *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 finite distributive lattice for any $x \in M$.*

A left divisibility monoid is width-bounded *if there exists a natural number $n \in \mathbb{N}$ such that $w(\downarrow\! x, \leq) \leq n$ for any $x \in M$, i.e. if the widths of the distributive lattices $\downarrow\! x$ are uniformly bounded.*

Note that by the third axiom the prefix relation in a left divisibility monoid is a partial order relation. Since, by Lemma 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 [2] 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". "Divisibility semigroups" are investigated in several papers by Bosbach, e.g. [3]. Despite the similarity of the name, we baptized our monoids independently and there seems to be no intimate relation between Bosbach's divisibility semigroups and our divisibility monoids.

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.

By the second requirement on divisibility monoids, the partial order $(M, \leq)$ can be seen as the set of compacts of a Scott-domain. This in particular ensures that any set $A \subseteq M$ that is bounded above in $(M, \leq)$ has a supremum in this partial order. Since, in addition, any element of M dominates a finite[2] distributive lattice, $(M, \leq)$ is even the set of compacts of a dI-domain (cf. [1, 27]). Thus, we have in particular $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$ whenever the left hand side is defined.

Example 3. Using standard results from trace theory [21, 9], it is easily seen that any (finitely generated) trace monoid is a 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 as Theorem 4 below shows.

Since a divisibility monoid $(M, \cdot, 1)$ is generated by the set Σ of its irreducible elements, there is a natural epimorphism $\mathrm{nat} : \Sigma^\star \to M$. Let $|x|$ denote the length of the lattice $\downarrow x$ which equals the size of any maximal chain deduced by 1. It is easily checked that $x \longrightarrow\!\!< y$ iff there exists $a \in \Sigma$ with $x \cdot \mathrm{nat}(a) = y$ for any $x, y \in M$. Hence the maximal chains in $\downarrow x$ correspond to the words $w \in \Sigma^\star$ with $\mathrm{nat}(w) = x$. This implies that any two such words have the same length which equals $|x|$.

Since nat is an epimorphism, there is a congruence $\sim$ on the free monoid $\Sigma^\star$ such that $\Sigma^\star/\sim$ is isomorphic to the divisibility monoid $(M, \cdot)$. Hence, we can reformulate the stipulations in Definition 2 into requirements on the congruence $\sim$. E.g. the property of M to be cancellative would be reformulated to "for any words $u, v, w \in \Sigma^\star$

[2] We just remark that the requirement (in the definition of a divisibility monoid) on the lattices $\downarrow x$ to be finite is not really necessary since it already follows from the other stipulations [12].

with $uv \sim uw$ or $vu \sim wu$, we get $v \sim w$". Although such a reformulation might look more effective than the original definition, it is not finite since it makes statements on words of arbitrary length. We now show that there is a decidable class of finite representations that gives rise precisely to divisibility monoids.

In [12, Lemma 3.4], we showed that the congruence $\sim$ is generated by equations of the from $ab \sim cd$ for $a, b, c, d \in \Sigma$. So let Σ be a finite set and let $\sim$ be a congruence on the free monoid $\Sigma^\star$ that is generated by all equivalences $ab \sim cd$ for $a, b, c, d \in \Sigma$. We aim at a characterization of the fact that $M = \Sigma^\star/\!\sim$ is a divisibility monoid. In this monoid, the elements from Σ (more precisely, the equivalence classes $[a]$ for $a \in \Sigma$) are the irreducible elements since $\sim$ is length preserving. Hence M is finitely generated by its irreducible elements. To ensure that M is cancellative, we need at least that the following holds for any elements $a, b, c, b', c' \in \Sigma$:

$$abc \sim ab'c' \text{ or } bca \sim b'c'a \text{ implies } bc \sim b'c'. \tag{1}$$

Note that (1) requires the cancellation for words of length 3, only. In the same spirit, we now weaken the second requirement concerning the existence of infima: Suppose $b \neq c$, but $ab \sim a'b'$ and $ac \sim a'c'$ for some $a, b, c, a', b', c' \in \Sigma$. Then one can infer from (1) that $ab \not\sim ac$. Since $\sim$ is length preserving, $[a]$ and $[a']$ are maximal lower bounds of $[ab]$ and $[ac]$. Since by the second axiom of divisibility monoids infima of any two elements exist, we obtain $a = a'$. Thus, the following requirement is a weakening of the above mentioned second axiom to words of length 2:

$$ab \sim a'b', ac \sim a'c' \text{ and } b \neq c \text{ imply } a = a' \tag{2}$$

for any letters $a, b, c, a', b', c' \in \Sigma$. The third axiom on divisibility monoids is restricted verbatim to words of length 3:

$$(\downarrow([abc]), \leq) \text{ is a distributive lattice} \tag{3}$$

for any letters $a, b, c \in \Sigma$. The following theorem states that the three properties we identified are sufficient to characterize all divisibility monoids:

Theorem 4. *Let Σ be a finite set and E a set of equations of the form $ab \sim cd$ with $a, b, c, d \in \Sigma$. Let $\sim$ be the least congruence on $\Sigma^\star$ containing E. Then $\Sigma^\star/\!\sim$ is a divisibility monoid if and only if (1), (2) and (3) hold for any $a, b, c, a', b', c' \in \Sigma$. Conversely, each divisibility monoid arises this way.*

We indicated that indeed any divisibility monoid arises this way. For the first statement let $R = \{ab \to cd \mid (ab, cd) \in E\}$ be the (symmetric) semi Thue system associated with the set of equations E. Any two R-equivalent words can be transformed into each other by at most one application of a rule from R at the first position (this statement is proved using deep results from the theory of semimodular and of distributive lattices [2]). From this property of R, one can then infer that $\Sigma^\star/\!\sim$ is a divisibility monoid (cf. [19, Chapter 8] or [20]).

Note that for a finite set of equations E of the form $ab \sim cd$, it can be checked effectively whether the three properties (1), (2) and (3) are satisfied by the least congruence containing E. Hence Theorem 4 describes a decidable class of finite presentations that give rise to the class of all divisibility monoids. Christian Pech of Dresden using the GAP4-system [16] computed that there are 219 divisibility monoids with 4 generators and 8371 divisibility monoids with 5 generators as opposed to only 10 resp. 34 trace monoids.

3 A Foata Normal Form

Throughout this section, let $(M, \cdot, 1)$ be a fixed divisibility monoid and let Σ denote the set of its irreducible elements. In this section, we will define a Foata normal form for elements of M that generalizes the known Foata normal forms from the theory of Mazurkiewicz traces. These Foata normal forms are the basis for our proofs in the following sections that any divisibility monoid is automatic and that a width-bounded divisibility monoid is rational. We define the set of *cliques* $\mathcal{C}\ell$ to consist of all nonempty subsets of Σ that are bounded above, i.e., $\mathcal{C}\ell = \{A \subseteq \Sigma \mid \emptyset \neq A$ and $\sup(A)$ exists$\}$

Next we define the set $\mathrm{FNF} \subseteq \mathcal{C}\ell^\star$ of Foata normal forms as

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

Since the condition that constitutes membership in FNF is local, FNF is a rational language in the free monoid $\mathcal{C}\ell^\star$. Let $\alpha' : \mathcal{C}\ell \to M$ denote the mapping that associates with any clique $A \in \mathcal{C}\ell$ its supremum $\sup A$ in M. This mapping extends uniquely to a monoid homomorphism α from $\mathcal{C}\ell^\star$ to M. Then $\alpha(A_1 A_2 \dots A_n) = (\sup A_1) \cdot (\sup A_2) \cdots (\sup A_n)$. This mapping is not injective, but surjective since $\alpha(\{a_1\}\{a_2\} \dots \{a_n\}) = a_1 \cdot a_2 \cdots a_n$ for any $a_i \in \Sigma$ and Σ generates M. The set FNF is particularly useful since it provides normal forms for the elements of M, i.e. since the restriction of α to FNF is a bijection:

Lemma 5. *The mapping $\alpha \restriction \mathrm{FNF} : \mathrm{FNF} \to M$ is bijective.*

Proof. To show injectivity, one proves for any $A_1 A_2 \dots A_n \in \mathrm{FNF}$ that A_1 is the set of irreducible elements $a \in \Sigma$ that divide $\alpha(A_1 A_2 \dots A_n)$ and continues by induction.

To show surjectivity, one builds the Foata Normal Form of x inductively by setting $x_1 = x$, $A_i = \{a \in \Sigma \mid a \leq x_i\}$, and $\alpha(A_i) \cdot x_{i+1} = x_i$. □

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.

Now let $\beta : \mathcal{C}\ell^\star \to \mathcal{C}\ell^\star$ be defined by $\beta = \mathrm{fnf} \circ \alpha$, i.e. $\beta(W)$ is the Foata normal form of the element $\alpha(W)$ for any word W over the alphabet $\mathcal{C}\ell$. This function is idempotent. Since fnf is injective, we obtain $\ker(\alpha) = \ker(\beta)$. Since α is a monoid homomorphism, $\ker(\beta)$ is a congruence. Finally $\mathcal{C}\ell^\star / \ker(\beta) = \mathcal{C}\ell^\star / \ker(\alpha) \cong M$ holds since α is surjective. Thus, we obtain

Lemma 6. *The function* $\mathrm{fnf} \circ \alpha : \mathcal{C}\ell^\star \to \mathcal{C}\ell^\star$ *is a normal form function for the divisibility monoid* M.

Next we show that the Foata Normal Form of $\mathrm{nat}(w)$ can be computed from the word $w \in \Sigma^\star$ by an automaton. In general, this automaton has infinitely many states, but for width-bounded divisibility monoids its accessible part will be shown to be finite.

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

1. Q is a set of *states*,
2. $E \subseteq Q \times S \times Q$ 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. 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 S. 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 S consisting of labels of successful computations in $\mathcal{A}$.

Lemma 7. *There exists an automaton* $\mathcal{A}_M$ *with state set* $M \times (\mathcal{C}\ell \cup \{\varepsilon\})$ *over the monoid* $\Sigma^\star \times \mathcal{C}\ell^\star$ *that has a computation* $(1, \varepsilon) \xrightarrow{(w, B_1 B_2 \ldots B_m)} (z, C)$ *iff*

$$B_m = C,\ \mathrm{fnf}(\mathrm{nat}(w) \cdot z) = B_1 B_2 \ldots B_m, \textit{ and } |\mathrm{fnf} \circ \mathrm{nat}(w)| = m.$$

for any $w \in \Sigma^\star$, $B_i \in \mathcal{C}\ell$ *for* $1 \le i \le m$, $z \in M$ *and* $C \in \mathcal{C}\ell_\varepsilon = \mathcal{C}\ell \cup \{\varepsilon\}$.

Proof. For $(x, A), (z, C) \in M \times \mathcal{C}\ell_\varepsilon$ and $(a, B) \in \Sigma \times \mathcal{C}\ell_\varepsilon$, there is a transition $(x, A) \xrightarrow{(a,B)} (z, C)$ iff

1. $a \le x$, $B = \varepsilon$, $a \cdot z = x$, and $C = A$, or
2. $a \not\le x$, $B = C \ne \varepsilon$, $AB \in \mathrm{FNF}$, and $a \cdot z = x \cdot (\sup B)$. □

We can think of $(1, \varepsilon) \xrightarrow{(w, B_1 B_2 \ldots B_m)} (z, C)$ as denoting the fact that, on input of the word $w \in \Sigma^\star$, the automaton outputs $B_1 B_2 \ldots B_m$ and reaches the state (z, C). Thus, by the lemma above, the automaton stores the last letter of its output B_m from $\mathcal{C}\ell$ in the second component C of the state reached. Furthermore, it outputs the Foata normal form of some element $\mathrm{nat}(w) \cdot z$ of M that is an extension of the input. The "difference" between the input $\mathrm{nat}(w)$ and the output $\alpha(B_1 B_2 \ldots B_m)$ (seen as elements of M) equals z and is stored in the first component of the reached state. The last property mentioned in the lemma above ensures that the Foata normal forms of $\mathrm{nat}(w)$ and of $\mathrm{nat}(w) \cdot z$ have the same length m. Intuitively, the difference between the input $\mathrm{nat}(w)$ and the output $\alpha(B_1 B_2 \ldots B_m)$ is not too "large".

Note that the automaton outputs only elements of FNF. Even more, if $z = 1$ the automaton outputs the Foata normal form of the input. Let $(1, \varepsilon)$ be the only initial state and let the set of final states be $\{1\} \times \mathcal{C}\ell_\varepsilon$. Then the behavior of the automaton $\mathcal{A}_M$ is (the graph of) the function $\mathrm{fnf} \circ \mathrm{nat} : \Sigma^\star \to \mathcal{C}\ell^\star$.

4 Divisibility monoids are automatic – the word problem

Since the equations that define a divisibility monoid are length preserving, the word problem for any divisibility monoid is decidable. In this section, we show that it can be solved in quadratic time.

For an alphabet Σ, let $\Sigma_\varepsilon = \Sigma\dot{\cup}\{\varepsilon\}$ and $\Sigma_2 = \Sigma_\varepsilon \times \Sigma_\varepsilon \setminus \{(\varepsilon,\varepsilon)\}$. Let furthermore $v = s_1 s_2 \dots s_m$ and $w = t_1 t_2 \dots t_n$ be words over Σ with $s_i, t_j \in \Sigma$. We define

$$(v,w)^\diamond = \begin{cases} (s_1,t_1)(s_2,t_2)\dots(s_n,t_n)(\varepsilon,t_{n+1})(\varepsilon,t_{n+2})\dots(\varepsilon,t_m) & \text{if } n < m \\ (s_1,t_1)(s_2,t_2)\dots(s_n,t_n) & \text{if } n = m \\ (s_1,t_1)(s_2,t_2)\dots(s_m,t_m)(s_{m+1},\varepsilon)(s_{m+2},\varepsilon)\dots(s_n,\varepsilon) & \text{if } n > m \end{cases}$$

Then $(v,w)^\diamond$ is an element of the free monoid $\Sigma_2^\star$. Now let M be a monoid, Σ a finite set, $L \subseteq \Sigma^\star$ a recognizable language in the free monoid $\Sigma^\star$ and $\eta : \Sigma^\star \to M$ a homomorphism. Then (Σ, L, η) is an *automatic structure for* M [5] if $\eta(L) = M$ and if the sets

$$L_= = \{(v,w)^\diamond \mid v,w \in L \text{ and } \eta(v) = \eta(w)\} \text{ and}$$
$$L_a = \{(v,w)^\diamond \mid v,w \in L \text{ and } \eta(va) = \eta(w)\}$$

are rational subsets of $\Sigma_2^\star$ for any $a \in \Sigma$. The monoid M is an *automatic monoid* if it admits an automatic structure.

We will show that any divisibility monoid is automatic. More precisely, let M be a divisibility monoid. For $A \in \mathcal{C}\ell$, choose a word $w_A \in \Sigma^\star$ with $\mathrm{nat}(w_A) = \alpha(A)$. Then the mapping $\mathcal{C}\ell \to \Sigma^\star : A \mapsto w_A$ admits a unique extension to a monoid homomorphism $\psi : \mathcal{C}\ell^\star \to \Sigma^\star$. Let $L = \psi(\mathrm{FNF})$ denote all words over Σ of the form $\psi(A_1)\psi(A_2)\dots\psi(A_n)$ for some cliques A_i such that $A_1 A_2 \dots A_n$ is a Foata normal form. We are going to prove that the triple $(\Sigma, L, \mathrm{nat})$ is an automatic structure for the divisibility monoid M:

Note that $\alpha = \mathrm{nat} \circ \psi$. Since, by Lemma 5, the mapping $\alpha \restriction \mathrm{FNF}$ is surjective, we obtain $M = \alpha(\mathrm{FNF}) = \mathrm{nat} \circ \psi(\mathrm{FNF}) = \mathrm{nat}(L)$.

Next, we show that $L_=$ is rational. Recall that $\mathrm{FNF} \subseteq \mathcal{C}\ell^\star$ is rational. Hence its image L with respect to the homomorphism ψ is rational, too. This implies immediately that the set $\{(v,v)^\diamond \mid v \in L\}$ is rational in $\Sigma_2^\star$. Now let $v, w \in L$ with $\mathrm{nat}(v) = \mathrm{nat}(w)$. Then $v = \psi \circ \mathrm{fnf} \circ \mathrm{nat}(v) = \psi \circ \mathrm{fnf} \circ \mathrm{nat}(w) = w$. Hence we showed $L_= = \{(v,v)^\diamond \mid v \in L\}$ which is rational in $\Sigma_2^\star$.

It remains to show that for $a \in \Sigma$ the set L_a is rational in $\Sigma_2^\star$. Note that $L_a = \{(v, \psi(\mathrm{fnf} \circ \mathrm{nat}(va))) \mid v \in L\}$. To show that this set is rational, we have to construct an automaton that outputs $\psi(\mathrm{fnf} \circ \mathrm{nat}(va))$ on input of v for $v \in L$. Since this can indeed be achieved (cf. [20]), we obtain

Theorem 8. *Let M be a divisibility monoid. Then M is an automatic monoid.*

Using that the word problem for automatic monoids can be solved in quadratic time [5], we obtain immediately

Corollary 9. *Let M be a divisibility monoid. Then the word problem for M can be solved in quadratic time.*

5 When does Kleene's Theorem hold?

As mentioned in the introduction, Kleene's Theorem holds in a divisibility monoid M iff it is width-bounded iff it is rational. To obtain this result, we first sketch the proof that any width-bounded divisibility monoid is rational. The crucial step in the proof is expressed by the following lemma

Lemma 10. *Let $(M, \cdot, 1)$ be a width-bounded divisibility monoid and $n \in \mathbb{N}$ such that $w(\downarrow x, \leq) \leq n$ for any $x \in M$. Let $x, z \in M$ with $|\mathrm{fnf}(xz)| = |\mathrm{fnf}(x)|$. Then $|z| < 2(n+1)|\Sigma|$.*

Using Lemma 7, we obtain that the automaton $\mathcal{A}_M$ has only finitely many reachable states for M width-bounded, i.e., the reachable part $\mathcal{A}$ of the automaton $\mathcal{A}_M$ is a finite automaton. Note that the behavior of $\mathcal{A}$ and that of $\mathcal{A}_M$ coincide. Thus, by [14], the behavior $|\mathcal{A}| = |\mathcal{A}_M| = \{(w, \mathrm{fnf} \circ \mathrm{nat}(w)) \mid w \in \Sigma^\star\}$ is a rational set in the monoid $\Sigma^\star \times \mathcal{C}\ell^\star$.

We consider again the homomorphism $\psi : \mathcal{C}\ell^\star \to \Sigma^\star$ that we constructed in the previous section. Since ψ is a homomorphism, the set $\{(W, \psi(W)) \mid W \in \mathcal{C}\ell^\star\}$ is rational in $\mathcal{C}\ell^\star \times \Sigma^\star$. Furthermore, $\mathrm{nat} \circ \psi = \alpha$ and therefore $\mathrm{fnf} \circ \alpha = \mathrm{fnf} \circ \mathrm{nat} \circ \psi$. Hence the function $\mathrm{fnf} \circ \alpha$ is the product of two rational functions $\mathrm{fnf} \circ \mathrm{nat}$ and ψ. This implies by [14] that the set $\{(W, \mathrm{fnf} \circ \alpha(W)) \mid W \in \mathcal{C}\ell^\star\}$ is rational since $\Sigma^\star$ is a free monoid. Recall that by Lemma 6, the function $\mathrm{fnf} \circ \alpha$ is a normal form function for the divisibility monoid M. Hence we showed that a width-bounded divisibility monoid indeed admits a rational normal form function, i.e. is a rational monoid:

Proposition 11. *Any width-bounded divisibility monoid is rational.*

By [25, Theorem 4.1], this proposition implies that any width-bounded divisibility monoid is a Kleene monoid. The remainder of this section is devoted to the inverse implication: Let M be a divisibility monoid that is not width-bounded, i.e., for any $n \in \mathbb{N}$, there is $z \in M$ such that the width of the distributive lattice $\downarrow z$ is at least n. This implies, that for any $k \in \mathbb{N}$, there exists $z \in M$, such that the lattice $(\{1, 2, 3, \ldots, k\}^2, \leq)$ (with the coordinatewise order) can be embedded into the lattice $\downarrow z$. Let f be such embedding. If the divisibility monoid M has finitely many residuum functions (see below), we can apply Ramsey's Theorem [24] twice and obtain $1 \leq i < i' \leq n$, $1 \leq j < j' \leq n$, and $x, y \in M$ such that $f(i,j) \cdot x = f(i,j')$, $f(i',j) \cdot x = f(i',j')$, $f(i,j) \cdot y = f(i',j)$, and $f(i,j') \cdot y = f(i',j')$. By cancellation, this implies $x \cdot y = y \cdot x$. Furthermore $x \parallel y$ since f is a lattice embedding and M is cancellative. This was the proof of the following lemma that we state after defining residuum functions: Let M be a divisibility monoid and $x, y \in M$. We say that x and y are *complementary* (denoted $x \parallel y$) if $x \wedge y = 1$ and the set $\{x, y\}$ is bounded above. Hence, two nonidentity elements of M are complementary if they are complements in one of the lattices $\downarrow z$ with $z \in M$. Since bounded elements have a supremum, there exists $y' \in M$ with $x \cdot y' = x \vee y$. This element y' is uniquely determined by x and y since M is cancellative. We call it the *residuum of y after x* and denote it by $r_x(y)$. Thus, r_x is a partial function from M to M whose domain is the set of elements that are complements of x. Let $\mathbb{R}_M$ denote the set of all partial functions r_x for some $x \in M$. The divisibility monoid M is said to have *finitely many residuum functions* if $\mathbb{R}_M$ is finite.[3]

Lemma 12. *Let $(M, \cdot, 1)$ be a divisibility monoid with finitely many residuum functions that is not width-bounded. Then there exist $x, y \in M \setminus \{1\}$ such that $x \parallel y$ and $x \cdot y = y \cdot x$.*

Now we can characterize the divisibility monoids that satisfy Kleene's Theorem.

Theorem 13. *Let $(M, \cdot, 1)$ be a divisibility monoid. Then the following assertions are equivalent*
1. M is width-bounded,
2. M is a rational monoid and has finitely many residuum functions, and
3. M is a Kleene monoid and has finitely many residuum functions.

Proof. A width-bounded divisibility monoid is rational by Proposition 11. Now let $s_i, t_i \in M$ for $1 \leq i \leq n$ such that $x = s_1 \cdot s_2 \cdots s_n$ and $y = t_1 \cdot t_2 \cdots t_n$ are complementary. Then the elements $s_1 \cdot s_2 \cdots s_k \vee t_1 \cdot t_2 \cdots t_{n-k}$ for $1 \leq k < n$ form an antichain that is bounded above by $z = x \vee y$. Hence the lattice $\downarrow z$ has width at least $n-1$. Now let M be width-bounded such that the lattices $\downarrow z$ have width at most $n-2$. Then, as we just saw, at most one of two complementary elements of M has length at least n. Let M_n denote the finite set of elements of M of length at most n. For $x \in M \setminus M_n$, the domain of r_x is therefore contained in M_n and, since r_x is length-preserving, so is its image. Hence there are only finitely many residuum functions r_x for $x \in M \setminus M_n$. Since M_n is finite, M therefore has only finitely many residuum functions.

Any rational monoid is a Kleene monoid by [25, Theorem 4.1]. For the remaining implication assume by contradiction M not to be width-bounded. Then, by Lemma 12, there are $x, y \in M \setminus \{1\}$ such that $x \cdot y = y \cdot x$ and $x \parallel y$. Hence the mapping $(0,1) \mapsto x$ and $(1,0) \mapsto y$ can be extended to a monoid embedding from $(\mathbb{N} \times \mathbb{N}, +)$ into M. The image of $\{(n,n) \mid n \in \mathbb{N}\}$ in M under this embedding is a rational set which is not recognizable. Thus, M is not a Kleene-monoid. □

6 Open questions

There are several open questions that call for a treatment: Is the lower bound for the complexity of the word problem given in Corollary 9 optimal? We did not consider the nonuniform word problem, i.e. the complexity of an algorithm that takes as input a

[3] It is not known whether this class is a proper subclass of all divisibility monoids.

presentation as described in Theorem 4 and two words and outputs whether these two words denote the same monoid element. Furthermore, we still do not know whether there exist divisibility monoids with infinitely many residuum functions.

References

1. G. Berry. Stable models of typed λ-calculi. In *5th ICALP*, Lecture Notes in Comp. Science vol. 62, pages 72–89. Springer, 1978.
2. G. Birkhoff. *Lattice Theory*. Colloquium Publications vol. 25. American Mathematical Society, Providence, 1973.
3. B. Bosbach. Representable divisibility semigroups. *Proc. Edinb. Math. Soc., II. Ser.*, 34(1):45–64, 1991.
4. J.R. Büchi. On a decision method in restricted second order arithmetics. In E. Nagel et al., editor, *Proc. Intern. Congress on Logic, Methodology and Philosophy of Science*, pages 1–11. Stanford University Press, Stanford, 1960.
5. C. M. Campbell, E. F. Robertson, N. Ruškuc, and R. M. Thomas. Automatic semigroups. *Theoretical Computer Science*, 250:365–391, 2001.
6. R. Corran. *On monoids related to braid groups*. PhD thesis, University of Sydney, 2000.
7. P. Dehornoy and L. Paris. Gaussian groups and Garside groups, two generalizations of Artin groups. *Proc. London Math. Soc.*, 79:569–604, 1999.
8. V. Diekert. *Combinatorics on Traces*. Lecture Notes in Comp. Science vol. 454. Springer, 1990.
9. V. Diekert and G. Rozenberg. *The Book of Traces*. World Scientific Publ. Co., 1995.
10. M. Droste. Recognizable languages in concurrency monoids. *Theoretical Comp. Science*, 150:77–109, 1995.
11. M. Droste and D. Kuske. On recognizable languages in divisibility monoids. In G. Ciobanu and Gh. Paun, editors, *FCT99*, Lecture Notes in Comp. Science vol. 1684, pages 246–257. Springer, 1999.
12. M. Droste and D. Kuske. Recognizable languages in divisibility monoids. *Mathematical Structures in Computer Science*, 2000. To appear.
13. C. Duboc. Commutations dans les monoïdes libres: un cadre théorique pour l'étude du parallelisme. Thèse, Faculté des Sciences de l'Université de Rouen, 1986.
14. C.C. Elgot and G. Mezei. On relations defined by generalized finite automata. *IBM J. Res. Develop.*, 9:47–65, 1965.
15. D.B.A. Epstein, J.W. Cannon, D.F. Holt, S.V.F. Levy, M.S. Paterson, and W.P. Thurston. *Word Processing In Groups*. Jones and Bartlett Publishers, Boston, 1992.
16. The GAP Group, Aachen, St Andrews. *GAP – Groups, Algorithms, and Programming, Version 4.2*, 1999. (`http://www-gap.dcs.st-and.ac.uk/~gap`).
17. J.F.P. Hudson. Regular rewrite systems and automatic structures. In J. Almeida, G.M.S. Gomes, and P.V. Silva, editors, *Semigroups, Automata and Languages*, pages 145–152, Singapure, 1996. World Scientific.
18. S.C. Kleene. Representation of events in nerve nets and finite automata. In C.E. Shannon and J. McCarthy, editors, *Automata Studies*, Annals of Mathematics Studies vol. 34, pages 3–40. Princeton University Press, 1956.
19. D. Kuske. Contributions to a Trace Theory beyond Mazurkiewicz Traces. Technical report, TU Dresden, 1999.
20. D. Kuske. On rational and on left divisibility monoids. Technical Report MATH-AL-3-1999, TU Dresden, 1999.
21. A. Mazurkiewicz. Concurrent program schemes and their interpretation. Technical report, DAIMI Report PB-78, Aarhus University, 1977.
22. E. Ochmański. Regular behaviour of concurrent systems. *Bull. Europ. Assoc. for Theor. Comp. Science*, 27:56–67, 1985.
23. M. Peletier and J. Sakarovitch. Easy multiplications. II. Extensions of rational semigroups. *Information and Computation*, 88:18–59, 1990.
24. F.P. Ramsey. On a problem of formal logic. *Proc. London Math. Soc.*, 30:264–286, 1930.
25. J. Sakarovitch. Easy multiplications. I. The realm of Kleene's Theorem. *Information and Computation*, 74:173–197, 1987.
26. M.P. Schützenberger. On the definition of a family of automata. *Inf. Control*, 4:245–270, 1961.
27. G. Winskel. Event structures. In W. Brauer, W. Reisig, and G. Rozenberg, editors, *Petri nets: Applications and Relationships to Other Models of Concurrency*, Lecture Notes in Comp. Science vol. 255, pages 325–392. Springer, 1987.