Math. Struct. in Comp. Science (2001), *vol.* 11, *pp.* 743–770. © 2001 Cambridge University Press
DOI: 10.1017/S0960129501003395 Printed in the United Kingdom

Recognizable languages in divisibility monoids

MANFRED DROSTE and DIETRICH KUSKE†

Institut für Algebra, TU Dresden, D-01062 Dresden,

Email: {droste,kuske}@math.tu-dresden.de

Received 12 October 1999; revised 9 October 2000

We define the class of divisibility monoids that arise as quotients of the free monoid $\Sigma^\star$ modulo certain equations of the form $ab = cd$. These form a much larger class than free partially commutative monoids, and we show, under certain assumptions, that the recognizable languages in these divisibility monoids coincide with c-rational languages. The proofs rely on Ramsey's theorem, distributive lattice theory and on Hashigushi's rank function generalized to these monoids. We obtain Ochmański's theorem on recognizable languages in free partially commutative monoids as a consequence.

1. Introduction

Trace theory provides a well-investigated mathematical model for the sequential behaviour of a parallel system in which the order of two independent actions is regarded as irrelevant. This is achieved by considering the free monoid $\Sigma^\star$ of all words over a fixed alphabet Σ modulo the congruence generated by equations of the form $ab = ba$, for pairs of independent actions a, b. These quotient monoids are called trace monoids or free partially commutative monoids, and in the literature much research has dealt, for example, with investigating the recognizable languages in these monoids (Cori and Perrin 1985; Cori and Métivier 1985; Métivier 1986; Ochmański 1985; Zielonka 1987), or with combinatorial problems concerning the possible re-arrangements of words (Cartier and Foata 1969; Choffrut 1995). For surveys on the many results obtained for trace monoids, we refer the reader to Diekert and Rozenberg (1995) and to Diekert and Métivier (1997).

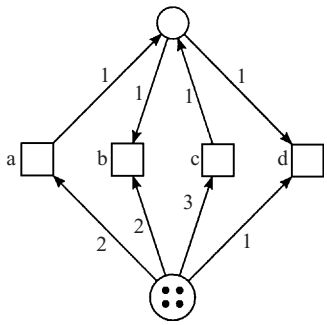
However, there are several areas in computer science where one would like to consider more general equations of the form $ab = cd$, rather than just $ab = ba$ as in trace theory. We point out three particular examples, which are certainly not exhaustive:

(1) Consider an unbounded binary counter and the operations inc, dec, shl, shr, respectively, of incrementing by 1, decrementing by 1, shift to the left by 1, shift to the right by 1. Certainly, the equation $inc \cdot dec = shl \cdot shr$ holds, which is of the form $ab = cd$, and there is obviously no commutation of inc and shl.

† New address: University of Leicester, Department of Mathematics and Computer Science, Leicester, LE1 7RH, U.K.

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

(2) Consider the following Petri net (place/transition-system) with capacities:



The effect of ab on the depicted marking, is the same as the effect of cd, and it is natural to identify $ab = cd$, but again this is not possible in trace monoids.

(3) A third range of examples arises immediately from concurrency monoids. Whereas in trace theory one assumes, for simplicity, a fixed, global independence relation for the actions, in many concurrent systems the independence of two actions is conditional, for example, it may be resource-dependent. Hence, one considers the set of computation sequences of a transition system modulo certain equations of the form $tt' = uu'$. Here t, t', u, u' usually are four different transitions and tt' and uu' get identified provided the actions a, b inducing in the state q the transitions t, u, respectively, are independent of each other in this particular state q. We note that these actions a, b may well be dependent in another state $r \neq q$, and hence we cannot identify $ab = ba$. This approach was investigated, for example, in Katz and Peled (1992), Droste (1992), and Droste and Kuske (1998), and used for the formal verification of real-size industrial protocols in Godefroid and Pirottin (1993).

In order to model such situations, in this paper we introduce and investigate divisibility monoids. We give an algebraic definition that uses only basic concepts of distributive lattice theory (known in mathematics since the 1930's). In particular, these monoids are finitely generated and cancellative. Then we first show that each divisibility monoid arises as a quotient of the free monoid $\Sigma^\star$ modulo certain equations of the form $ab = cd$, as in the above examples.

In subsequent work (Kuske 2000), the systems of equations of this form $ab = cd$ giving rise to divisibility monoids are precisely characterized. It is easy to see that each trace monoid is a divisibility monoid, but Kuske's result shows that there is indeed an abundance of divisibility monoids. For example, up to isomorphism there are 4 trace monoids generated by 3 elements, but there are already precisely 15 divisibility monoids generated by 3 elements. We list all of them here (see Corollary 3.6). We just note here that this abundance of divisibility monoids versus trace monoids increases even further with the number of the generators. With regard to the above examples, we remark that if $\Sigma = \{a, b, c, d\}$, then the monoid $\Sigma^\star/\{ab = cd\}$ is a divisibility monoid (one out of 219 on 4 generators, while there are 8371 on 5 generators). Also, we will show that the class of divisibility monoids is strictly larger than the class of concurrency monoids, which is known to strictly contain all trace monoids.

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

Next we introduce a residuum operation for divisibility monoids. The distributivity laws enable us to develop a calculus of residuals that is very similar to the one used, for different purposes, for example, in Panangaden and Stark (1988) and Stark (1989).

A classical result by Kleene characterizes the recognizable languages in a free, finitely generated monoid $\Sigma^\star$ as the rational ones. This result has been extended in several directions, in particular to other classes of monoids. So, for example, in Sakarovitch (1987) the same result was shown for rational monoids. In trace theory, a celebrated result is Ochmański's characterization of the recognizable languages in trace monoids as c-rational sets (Ochmański 1985). This was generalized to concurrency monoids in Droste (1995). For a wealth of further results on recognizable languages in arbitrary monoids, see Eilenberg (1974).

The main goal of this paper is to investigate the recognizable languages in divisibility monoids. For this, we first define c-rational languages as in trace theory. Assuming a finiteness condition for the residuum operation, we can prove that any c-rational language is recognizable. This uses an extension of the notion of the *rank* of a language, which has already been shown to be very useful in trace theory in Hashigushi (1991). However, unlike in trace theory, here we also have to employ some lattice theory, the residual calculus mentioned above and Ramsey's theorem (for the iteration).

Under an additional labelling assumption on our divisibility monoids, we can also prove the converse of the above result, that is, that any recognizable language is c-rational. With this requirement, our divisibility monoids are more similar to, but still more general than, trace monoids and concurrency monoids.

From these results, we obtain Ochmański's theorem for recognizable trace languages as an immediate consequence. We also solve an open problem from Droste (1995, p. 79), and obtain a strengthening of the results from Droste (1995) for recognizable languages in concurrency monoids as a consequence.

At present, a natural open question is to find a joint generalization of Sakarovitch's results for rational monoids and our result for the recognizable languages in divisibility monoids.

An extended abstract of this paper appeared as Droste and Kuske (1999).

2. Preliminaries

Let $(M, \cdot, 1)$ be a monoid and $L \subseteq M$. A monoid morphism $\eta : M \to S$ into a finite monoid $(S, \cdot, 1)$ *recognizes* L if $\eta^{-1}\eta(L) = L$. The language L is *recognizable* if there exists a monoid morphism that recognizes L. For $x \in M$ let $x^{-1}L := \{y \in M \mid x \cdot y \in L\}$, the left quotient of L with respect to x. Then a classical result (Eilenberg 1974) states that L is recognizable iff the set $\{x^{-1}L \mid x \in M\}$ is finite iff there is a finite M-automaton recognizing L.

Let $L, K \subseteq M$. Then $L \cdot K := \{l \cdot k \mid l \in L, k \in K\}$ is the product of L and K. We use $\langle L \rangle$ to denote the submonoid of M generated by L, that is, $\langle L \rangle = \{l_1 \cdot l_2 \cdot \ldots l_n \mid n \in \mathbb{N}, l_i \in L\}$. For a set Σ we use $\Sigma^\star$ to denote the free monoid generated by Σ. Now let M be a free monoid and $L \subseteq M$. Then $\langle L \rangle$ is a subset of M while $L^\star$ is a set of words whose letters are elements of M. Classical formal language theory usually identifies the set $L^\star$ of words

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

over L and the submonoid $\langle L\rangle$ of M generated by L. In this paper, we have to distinguish between them.

The class of *rational languages* in a monoid M is the smallest class $\mathscr{C}$ satisfying:

1. any finite subset of M is in $\mathscr{C}$;
2. whenever $L, K \in \mathscr{C}$ then $L \cup K \in \mathscr{C}$ and $L \cdot K \in \mathscr{C}$; and
3. whenever $L \in \mathscr{C}$ then $\langle L\rangle \in \mathscr{C}$.

Now let Σ be a finite set and $L \subseteq M := \Sigma^\star$. By Kleene's Theorem, L is recognizable iff it is rational. In any monoid, the set of recognizable languages is closed under the usual set-theoretic operations, like complementation, intersection and difference. As a consequence of Kleene's theorem, the set of rational languages in the free monoid $\Sigma^\star$ enjoys these closure properties.

For $x \in \Sigma^\star$, let $\alpha(x)$ denote the alphabet of x comprising all letters of Σ occurring in x. Then $L_B := \langle B\rangle \cap L \setminus (\bigcup_{A \subset B} \langle A\rangle)$ where $B \subseteq \Sigma$ 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 $B \subseteq \Sigma$. The class of *monoalphabetic-rational languages* (*m-rational* for short) in $\Sigma^\star$ is the smallest class $\mathscr{C}$ satisfying:

1. any finite subset of M is in $\mathscr{C}$;
2. whenever $L, K \in \mathscr{C}$ then $L \cup K \in \mathscr{C}$ and $L \cdot K \in \mathscr{C}$; and
3. whenever $L \in \mathscr{C}$ is monoalphabetic then $\langle L\rangle \in \mathscr{C}$.

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

Lemma 2.1. Let Σ be a finite set. Then a language in $\Sigma^\star$ 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 $B \subseteq \Sigma$ 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 $B = \varnothing$, 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 $(L^\star)_C$ and $(L^\star)_X$ are m-rational. In addition, K is monoalphabetic (its alphabet equals B). Hence $\langle L\rangle_B$ is m-rational. □

Let $(P, \leqslant)$ be a partially ordered set and $x \in P$. Then $\downarrow x$ comprises all elements dominated by x, that is, $\downarrow x := \{y \in P \mid y \leqslant x\}$. If $A \subseteq P$, we write $A \leqslant x$ to denote that $A \subseteq \downarrow x$, that is, that $a \leqslant x$ for all $a \in A$. The partially ordered set $(P, \leqslant)$ is a *lattice* if for any $x, y \in P$ the least upper bound $\sup(x, y) = x \vee y$ and the largest lower bound $\inf(x, y) = x \wedge y$ exist. The lattice $(P, \leqslant)$ is *distributive* if $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ for any $x, y, z \in P$. This is equivalent to $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ for any $x, y, z \in P$. For properties of finite distributive lattices, we refer the reader to Birkhoff (1940).

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

3. Left divisibility monoids

In this section, we will introduce left divisibility monoids and investigate their basic properties.

Let $M = (M, \cdot, 1)$ be a monoid where $1 \in M$ is the unit element. 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. For $x, y \in M$, x *is a left divisor of* y (denoted $x \leqslant y$) if there is $z \in M$ such that $x \cdot z = y$. In general, the relation $\leqslant$ is not antisymmetric. But in a left divisibility monoid (see below, third requirement) it is a partial order.

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 has to be contained in any set generating M.

Definition 3.1. 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. $(\downarrow m, \leqslant)$ is a distributive lattice for any $m \in M$.

Note that this definition uses only basic concepts from lattice theory, for details see Birkhoff (1940). Also, it is simpler than the explicit definition of concurrency monoids, *cf.* Droste (1995, pp. 80–81). By the third clause, the prefix relation in a left divisibility monoid is a partial order relation. Since $y \leqslant z$ immediately implies $x \cdot y \leqslant x \cdot z$, 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, for example, in Birkhoff (1940) under the name 'divisibility monoid'. Despite the fact that we require more than just the fact that $(M, \cdot, \leqslant)$ 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 this paper 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 $1 \leqslant x \leqslant 1$ implies $x = 1$, since by the third clause $\leqslant$ is a partial order. Now $1 = xy = y$.

Since a divisibility monoid $(M, \cdot, 1)$ is generated by the set Σ of its irreducible elements, there is a natural epimorphism from the free monoid $\Sigma^\star$ onto M. This epimorphism will be denoted by [.]. Now let $A \subseteq M$ be finite and $x \in M$ with $A \leqslant x$. Since $(\downarrow x, \leqslant)$ is a lattice, the supremum y of A *in this lattice* exists. Now let $z \in M$ be an upper bound of A in $(M, \leqslant)$ that is not necessarily in the lattice $\downarrow x$. Then y and z have an infimum $y \wedge z$ in $(M, \leqslant)$. This infimum is an upper bound of A dominated by y. Thus $y = y \wedge z \leqslant z$. Hence y is also the supremum of A in the partially ordered set $(M, \leqslant)$. Thus we have shown that any finite set, bounded above, has a supremum in $(M, \leqslant)$. 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 $(M, \leqslant)$ is not necessarily a lattice since it may contain unbounded pairs of elements.

Now we show that multiplying from the left (but not from the right) distributes over infima and suprema.

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

Lemma 3.2. Let $(M, \cdot, 1)$ be a divisibility monoid and $a \in M$. Then the mapping $a : (M, \leqslant) \to (a \cdot M, \leqslant)$ defined by $a(x) := a \cdot x$ is an order isomorphism. In particular, $a \cdot (b \wedge c) = ab \wedge ac$ 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.

Proof. Since the monoid M is cancellative, the mapping a is bijective. Now let $b, c \in M$. If $b \leqslant c$, there exists $d \in M$ with $b \cdot d = c$. Hence $ab \cdot d = ac$, implying $ab \leqslant ac$. Conversely, assume $ab \leqslant ac$. Then we find $d \in M$ such that $abd = ac$. Now $b \leqslant c$ follows by cancellation. Hence the mapping a is an order isomorphism. □

Next we show that in a divisibility monoid the sets $\downarrow m$ are finite.

Lemma 3.3. Let $(M, \cdot, 1)$ be a divisibility monoid and $m \in M$. Then $\downarrow m$ is finite.

Proof. Let $\Sigma \subseteq M$ be the set of irreducible elements of M. Then Σ is a finite set of generators of M. Now assume $n \in \mathbb{N}$ minimal such that there exist $x_1, \ldots, x_n \in \Sigma$ with $\downarrow(x_1 \cdot x_2 \ldots x_n)$ infinite. Then $n \geqslant 2$. 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 3.2, $(\{y \in M \mid x_1 \leqslant y \leqslant m\}, \leqslant) \cong (\downarrow(x_2 \cdot x_3 \ldots x_n), \leqslant)$. Since n is minimal, the sets $\downarrow x_1$ and $\{y \in M \mid x_1 \leqslant y \leqslant m\}$ 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 (Birkhoff 1940, Corollary to Theorem II.13), this implies $x = y$ contradicting $x < y$. □

As finite subsets of $(M, \leqslant)$ that are bounded above have a supremum, the partial order $(M, \leqslant)$ can be seen as the set of compact elements of a Scott-domain. The lemma above ensures that it is also the set of compacts of a dI-domain (*cf.* Berry (1978) and Winskel (1987)). 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 $x = x_1 x_2 \ldots x_n$ with $x_i \in \Sigma$. Then $\{1, x_1, x_1 x_2, \ldots, x\}$ is a maximal chain in the finite distributive lattice $\downarrow x$. Since maximal chains in such finite distributive lattices have the same size, any word u over Σ with $[u] = x$ has length n. Hence we can define the *length* of x to be $|x| = n$.

Since a divisibility monoid M is generated by the set Σ of its irreducible elements, there is a congruence $\sim$ on the free monoid $\Sigma^\star$ such that the quotient $\Sigma^\star/\sim$ is isomorphic to M. The following result shows that this congruence is quite natural and that the monoid M is finitely presentable.

Lemma 3.4. Let M be a divisibility monoid and Σ be the set of its irreducible elements. Let $\sim$ denote the least congruence on the free monoid $\Sigma^\star$ containing $\{(ab, cd) \mid a, b, c, d \in \Sigma \text{ and } a \cdot b = c \cdot d\}$. Then $\sim$ is the kernel of the natural epimorphism $[.] : \Sigma^\star \to M$. In particular, $M \cong \Sigma^\star/\sim$.

Proof. Throughout this proof, we use $a \cdot b$ to denote the product of $a, b \in \Sigma$ in M, while we use ab to denote the word. Thus, $a \cdot b = [ab] \in M$ and $ab \in \Sigma^\star$.

Recall that $u \sim v$ or $[u] = [v]$ implies that u and v have the same length.

Clearly, $\sim$ is contained in $\ker([.])$ since $a \cdot b = c \cdot d$ implies $[ab] = [cd]$ for $a, b, c, d \in \Sigma$.

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

For the converse, let $u, v \in \Sigma^\star$ with $[u] = [v]$. We show $u \sim v$ by induction on the length of u: If $|u| = 0$, clearly, $[u] = [v] = 1$, so $u = v = \varepsilon$. If $|u| = 1$, then $u = v \in \Sigma$.

Now let $u = u_1 u_2 \dots u_n$ and $v = v_1 v_2 \dots v_n$ with $u_i, v_i \in \Sigma$ and $n \geqslant 2$. If $u_1 = v_1$, we get $[u_2 u_3 \dots u_n] = [v_2 v_3 \dots v_n]$ by cancellation. By the induction hypothesis, this implies $u_2 u_3 \dots u_n \sim v_2 v_3 \dots v_n$, and therefore $u_1 u_2 \dots u_n \sim v_1 v_2 \dots v_n$. Thus, assume $u_1 \neq v_1$. Then u_1, v_1 are elements of the finite distributive lattice $\downarrow[u]$. Hence there exist $b, d \in M$ such that $u_1 \cdot b = v_1 \cdot d = u_1 \vee v_1$. One also has $b, d \in \Sigma$, since the distributive lattice $\downarrow[u]$ is semimodular (Birkhoff 1940). Note that $u_1 b \sim v_1 d$. Since $u_1 \vee v_1 \leqslant [u]$, we find $y \in \Sigma^\star$ such that $(u_1 \vee v_1) \cdot [y] = [u]$. Hence $[u_1 u_2 \dots u_n] = [u_1 b y]$ and therefore $[u_2 \dots u_n] = [by]$ by cancellation. The induction hypothesis ensures $u_2 \dots u_n \sim by$. Now we have $[v_1 dy] = (u_1 \vee v_1) \cdot [y] = [u] = [v]$ implying $[dy] = [v_2 v_3 \dots v_n]$. Now $dy \sim v_2 v_3 \dots v_n$ follows from the induction hypothesis since the length of $v_2 v_3 \dots v_n$ equals $n - 1$. Thus, we have $u_1 u_2 \dots u_n \sim u_1 by \sim v_1 dy \sim v_1 v_2 \dots v_n$. □

The definition of divisibility monoids imposes conditions on arbitrary elements of the monoid $(M, \cdot, 1)$. The following theorem characterizes divisibility monoids by requirements on 'short words', only. Lemma 3.4 shows that any divisibility monoid does indeed satisfy these requirements. For a proof of the other implication, see Kuske (2000).

Theorem 3.5. (Kuske 2000) Let $(M, \cdot, 1)$ be a monoid for which the set Σ of its irreducible elements is finite and generates M. Then M is a divisibility monoid if and only if for any $a, b, c, a', b', c' \in \Sigma$, we have:

(*i*) $\downarrow(a \cdot b \cdot c)$ 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 $b \cdot c = b' \cdot c'$,
(*iii*) $a \cdot b = a' \cdot b'$, $a \cdot c = a' \cdot c'$ and $a \neq a'$ imply $b = c$, and
(*iv*) the assertion of Lemma 3.4 holds in M.

Proof (sketch). From what we have shown so far, any divisibility monoid satisfies the conditions given here. For the other implication, we give the main ideas of the proof only. As in Lemma 3.4, let $\sim$ denote the least congruence on $\Sigma^\star$ that contains all pairs (ab, cd) for $a, b, c, d \in \Sigma$ with $a \cdot b = c \cdot d$. Now assume $u, v \in \Sigma^\star$ with $[u]_\sim = [v]_\sim$. Then, by (*iv*), the words u and v have the same length. Since there are only finitely many words of length at most $|u|$, the set $\downarrow[u]_\sim$ is finite. Now let $x, y \in M$ be bounded above by $z = [u]_\sim$. Since $\downarrow z$ is finite, the set of minimal upper bounds of x, y is complete. Now (*iii*) can be used to show that $\{x, y\}$ has a supremum in $\downarrow z$. Hence $\downarrow z$ is a finite lattice for any $z \in M$. Using methods from Kuske (1994a) and Kuske (1994b), one gets that this lattice is distributive.

Note that clearly any two elements $x, y \in M$ have a finite set of maximal lower bounds. To show that this set is a singleton, that is, that the infimum $x \wedge y$ exists, one explores property (*iii*).

To check that M is cancellative, one can again use methods from Kuske (1994a). □

By Lemma 3.4, any divisibility monoid is isomorphic to a monoid $\Sigma^\star / \langle E \rangle$ with $E \subseteq \{(ab, cd) \mid a, b, c, d \in \Sigma\}$. Conversely, Theorem 3.5 ensures that given Σ and $E \subseteq \{(ab, cd) \mid a, b, c, d \in \Sigma\}$ it is decidable whether $\Sigma^\star / \langle E \rangle$ is a divisibility monoid. The authors used

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

this characterization to determine (by hand) all divisibility monoids with three generators, and Christian Pech (Dresden) went on to compute all divisibility monoids with up to five generators using the GAP4-system (GAP 1999).

Corollary 3.6. Up to isomorphism, there are precisely 15 divisibility monoids with 3 generators, namely the free monoid and those defined by the following sets of equations:

$$\begin{array}{lll} \{ab = ba\} & \{ab = ba, bc = cb\} & \{ab = ba, bc = cb, ac = ca\} \\ \{aa = bb\} & \{aa = bb, ac = bc, ca = bc\} & \{aa = bb, bc = cb, ac = ca\} \\ \{ab = bc\} & \{ab = bc, ba = cb\} & \{ab = bc, ba = cb, ac = ca\} \\ & \{ab = bc, ac = cb\} & \{ab = bc, ac = ca\} \\ \{aa = bc\} & \{aa = bc, cc = ba\} & \{aa = bc, bb = ca, cc = ab\} \end{array}$$

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. Furthermore, consider the monoid given by $\{ab = bc, ac = ca\}$. The rational language $\langle (a \cdot c) \rangle \subseteq M$ is not recognizable. Hence M is not a rational monoid since in rational monoids any rational language is recognizable (Sakarovitch 1987). On the other hand, M is not a trace monoid because of the equation $ab = bc$.

In trace theory, there is the notion of independent traces. Algebraically, two traces are independent if they are bounded above and their infimum is the empty trace. We use this lattice-theoretic characterization as the definition. Let M be a divisibility monoid. Two elements x and y are *complementary* (denoted $x \parallel y$) if $x \wedge y = 1$ and $\{x, y\}$ is bounded above. In this case the supremum $x \vee y$ exists in M. 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* denoted $x \uparrow y$ (read 'x after y'). Note that it is defined for complementary elements x and y only. Hence $x \uparrow y$ is defined iff $y \uparrow x$ is defined, and in this case $x(y \uparrow x) = y(x \uparrow y)$. (We could have defined the residuum for any two monoid elements that are bounded above, and this is done, for example, for concurrency monoids, but in our context it turns out to be more appropriate to restrict the definition to complementary monoid elements.) Fixing $x \in M$, we get a unary partial function r_x from M to M by $\mathrm{dom}(\mathrm{r}_x) := \{y \in M \mid x \parallel y\}$ and $\mathrm{r}_x(y) := y \uparrow x$. The function r_x will be called the *residuum function of x*. In the literature, similar residuum functions have already occurred in several contexts, *cf.* Panangaden and Stark (1988), Berry (1978) and Stark (1989). We may turn the (partial) residuum function into a total function on M by the insertion of an additional element. Therefore in this paper, an equation $\mathrm{r}_x(y) = \mathrm{r}_z(y')$ means '$\mathrm{r}_x(y)$ is defined iff $\mathrm{r}_z(y')$ is defined and in this case they are equal'.

Lemma 3.7. Let $(M, \cdot, 1)$ be a divisibility monoid and $x, y \in M$ with $x \parallel y$. The residuum function r_x is injective on its domain. Furthermore, $|y| = |\mathrm{r}_x(y)|$.

Proof. Let $y, y' \in \mathrm{dom}(\mathrm{r}_x)$ with $\mathrm{r}_x(y) = \mathrm{r}_x(y')$. 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

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

of x in the lattice $\downarrow(x \vee y)$. Since complements in a distributive lattice are unique (Birkhoff 1940), this implies $y = y'$.

To show that r_x is length preserving, let $z = x \vee y = x \cdot \mathrm{r}_x(y)$. 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 (Birkhoff 1940). Now the second statement follows immediately. □

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

Lemma 3.8. Let $(M, \cdot, 1)$ be a divisibility monoid and $x, x', y, z \in M$.

1. $x \parallel yz$ iff $x \parallel y$ and $\mathrm{r}_y(x) \parallel z$.
2. $\mathrm{r}_{yz}(x) = \mathrm{r}_z(\mathrm{r}_y(x))$; in other words $x \uparrow (yz) = (x \uparrow y) \uparrow z$.
3. $\mathrm{r}_x(yz) = \mathrm{r}_x(y) \cdot \mathrm{r}_{\mathrm{r}_y(x)}(z)$; equivalently $yz \uparrow x = (y \uparrow x) \cdot (z \uparrow (x \uparrow y))$.
4. If $\mathrm{r}_x = \mathrm{r}_{x'}$ and $y \parallel x$, then $\mathrm{r}_{\mathrm{r}_y(x)} = \mathrm{r}_{\mathrm{r}_y(x')}$.

Proof.

1. First we show the implication $\Rightarrow$. Therefore, let $x \parallel yz$. 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 $y \leqslant yz$. To show $\mathrm{r}_y(x) \parallel z$, note that $\mathrm{r}_y(x)$ is defined since $x \parallel y$ holds. Then $y\mathrm{r}_y(x) = x \vee y$ 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 $\{\mathrm{r}_y(x), z\}$ follows by $x \vee y = y\mathrm{r}_y(x)$ and Lemma 3.2. Furthermore,

$$\begin{aligned} y \cdot (\mathrm{r}_y(x) \wedge z) &= y\mathrm{r}_y(x) \wedge yz && \text{by Lemma 3.2} \\ &= (x \vee y) \wedge yz \\ &= (x \wedge yz) \vee (y \wedge yz) && \text{by distributivity in } (M, \leqslant) \\ &= 1 \vee y = y && \text{since } x \parallel yz \text{ and } y \leqslant yz. \end{aligned}$$

Since M is cancellative, this implies $\mathrm{r}_y(x) \wedge z = 1$.

To show the inverse implication, let $x \parallel y$ and $\mathrm{r}_y(x) \parallel z$. Then $x \wedge yz \leqslant (x \vee y) \wedge yz = y\mathrm{r}_y(x) \wedge yz$. By Lemma 3.2 this equals $y(\mathrm{r}_y(x) \wedge z)$. Since $\mathrm{r}_y(x) \parallel z$, we get $x \wedge yz \leqslant y$. Hence $x \wedge yz = x \wedge y \wedge yz = 1 \wedge yz = 1$ since $x \parallel y$. To show that $\{x, yz\}$ is bounded, note that $\{y\mathrm{r}_y(x), yz\}$ is bounded because of $\mathrm{r}_y(x) \parallel z$ and Lemma 3.2. Hence $\{x \vee y, yz\}$, and therefore $\{x, yz\}$ are bounded.

2.
$$\begin{aligned} yz\mathrm{r}_{yz}(x) &= x \vee yz && \text{by the definition of the function } \mathrm{r}_{yz} \\ &= (x \vee y) \vee yz && \text{since } y \leqslant yz \\ &= y\mathrm{r}_y(x) \vee yz \\ &= y(\mathrm{r}_y(x) \vee z) && \text{Lemma 3.2} \\ &= yz\mathrm{r}_z(\mathrm{r}_y(x)). \end{aligned}$$

Since M is cancellative, this implies $\mathrm{r}_{yz}(x) = \mathrm{r}_z(\mathrm{r}_y(x))$.

3.
$$\begin{aligned} x\mathrm{r}_x(yz) &= x \vee yz = x \vee y \vee yz && \text{since } y \leqslant yz \\ &= y(\mathrm{r}_y(x) \vee z) && \text{Lemma 3.2 and } x \vee y = y\mathrm{r}_y(x) \\ &= y\mathrm{r}_y(x)\mathrm{r}_{\mathrm{r}_y(x)}(z) = (x \vee y)\mathrm{r}_{\mathrm{r}_y(x)}(z) \\ &= x\mathrm{r}_x(y)\mathrm{r}_{\mathrm{r}_y(x)}(z). \end{aligned}$$

Hence $\mathrm{r}_x(yz) = \mathrm{r}_x(y)\mathrm{r}_{\mathrm{r}_y(x)}(z)$.

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

4. Let $z \in \mathrm{dom}(\mathrm{r}_{\mathrm{r}_y(x)})$. By the above and $\mathrm{r}_x = \mathrm{r}_{x'}$, we get $\mathrm{r}_x(y)\mathrm{r}_{\mathrm{r}_y(x)}(z) = \mathrm{r}_x(yz) = \mathrm{r}_{x'}(yz) = \mathrm{r}_{x'}(y)\mathrm{r}_{\mathrm{r}_y(x')}(z) = \mathrm{r}_x(y)\mathrm{r}_{\mathrm{r}_y(x')}(z)$. Now we can conclude $\mathrm{r}_{\mathrm{r}_y(x)}(z) = \mathrm{r}_{\mathrm{r}_y(x')}(z)$. □

Note that the second statement of the lemma above implies, in particular, $\mathrm{r}_z \circ \mathrm{r}_y = \mathrm{r}_{yz}$ where $\circ$ is the usual concatenation of partial functions. Hence the set $\mathbb{R}_M = \{\mathrm{r}_x \mid x \in M\}$ is closed under concatenation. Since r_1 is the identity function on M, $(\mathbb{R}_M, \circ, \mathrm{r}_1)$ is a monoid, *the monoid of residuum functions of* M. The function $r : M \to \mathbb{R}_M : x \mapsto \mathrm{r}_x$ is a monoid antihomomorphism. We say that M *has finitely many residuum functions* if $\mathbb{R}_M$ is finite, that is, there are only finitely many different functions r_x $(x \in M)^\dagger$.

Recall that $[.] : \Sigma^\star \to M$ is a homomorphism. Thus, one can easily define functions $\mathrm{res}_x : \Sigma^\star \to \Sigma^\star$ for $x \in M$ that commute with $[.]$. Here, we define them in such a way that equations like those from Lemma 3.8 hold: recall that for $t \in \Sigma$ and $x \in M$ with $x \parallel t$ we have $|t| = |\mathrm{r}_x(t)|$ by Lemma 3.7 and therefore $\mathrm{r}_x(t) \in \Sigma$. Hence $\mathrm{res}_x(t) := \mathrm{r}_x(t)$ (if $t \parallel x$) is a partial function mapping Σ to Σ. We extend it to a partial function from $\Sigma^\star$ to $\Sigma^\star$ by $\mathrm{res}_x(tu) := \mathrm{res}_x(t)\mathrm{res}_{\mathrm{r}_t(x)}(u)$. Then one can easily check that

$$\mathrm{res}_x(t_1 t_2 \dots t_n) = \mathrm{res}_x(t_1)\mathrm{res}_{\mathrm{r}_{[t_1]}(x)}(t_2)\mathrm{res}_{\mathrm{r}_{[t_1 t_2]}(x)}(t_3)\dots\mathrm{res}_{\mathrm{r}_{[t_1 t_2 \dots t_{n-1}]}(x)}(t_n),$$

and therefore

$$\mathrm{res}_x(uv) = \mathrm{res}_x(u)\mathrm{res}_{\mathrm{r}_{[u]}(x)}(v).$$

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

$$\begin{aligned}
\mathrm{res}_y(\mathrm{res}_x(tu)) &= \mathrm{res}_y(\mathrm{res}_x(t)\mathrm{res}_{\mathrm{r}_t(x)}(u)) \\
&= \mathrm{res}_y(\mathrm{res}_x(t)) \cdot \mathrm{res}_{\mathrm{r}_{\mathrm{res}_x(t)}(y)}(\mathrm{res}_{\mathrm{r}_t(x)}(u)) \\
&= \mathrm{res}_{xy}(t) \cdot \mathrm{res}_{\mathrm{r}_t(x)\mathrm{r}_{\mathrm{res}_x(t)}(y)}(u) \\
&= \mathrm{res}_{xy}(t) \cdot \mathrm{res}_{\mathrm{r}_t(xy)}(u) \\
&= \mathrm{res}_{xy}(tu).
\end{aligned}$$

Now let $v \in \Sigma^\star$. Then we define $\mathrm{res}_v := \mathrm{res}_{[v]}$. Thus, $\mathrm{dom}(\mathrm{res}_v) = \{u \in \Sigma^\star \mid [u] \parallel [v]\}$. We write $u \parallel v$ for $u \in \mathrm{dom}(\mathrm{res}_v)$. Note that, similarly to properties of r_x, we have the following lemma.

Lemma 3.9. Let $(M, \cdot, 1)$ be a divisibility monoid and $u, v, w \in \Sigma^\star$.

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

Furthermore, res_u is injective on its domain and length preserving.

Proof. The proof is immediate by Lemmas 3.8 and 3.7. □

Lemma 3.10. Let $u, v \in \Sigma^\star$. Then $\mathrm{res}_u = \mathrm{res}_v$ iff $\mathrm{r}_{[u]} = \mathrm{r}_{[v]}$.

† We do not know whether there exist divisibility monoids with $\mathbb{R}_M$ infinite.

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

Proof. The implication '⇒' is immediate by the third equation above. Now let $\mathrm{r}_{[u]} = \mathrm{r}_{[v]}$. If $t \in \Sigma$ and $\mathrm{res}_u(t)$ is defined, then $\mathrm{r}_{[u]}(t) = \mathrm{r}_{[v]}(t)$ and therefore $\mathrm{res}_v(t)$ is defined. Furthermore, $\mathrm{res}_u(t) = \mathrm{r}_{[u]}(t) = \mathrm{res}_v(t)$, proving the claim for arguments from Σ. Now let $w \in \Sigma^\star$. Then $\mathrm{res}_u(tw) = \mathrm{res}_u(t)\ \mathrm{res}_{\mathrm{r}_t([u])}(w)$. By the above argument, $\mathrm{res}_u(t) = \mathrm{res}_v(t)$. Furthermore, $\mathrm{r}_{\mathrm{r}_{[t]}([u])} = \mathrm{r}_{\mathrm{r}_{[t]}([v])}$ by Lemma 3.8(4). By the induction hypothesis, this implies $\mathrm{res}_{\mathrm{r}_{[t]}([u])}(w) = \mathrm{res}_{\mathrm{r}_{[t]}([v])}(w)$. Hence $\mathrm{res}_u(tw) = \mathrm{res}_v(t)\ \mathrm{res}_{\mathrm{r}_{[t]}([v])}(w) = \mathrm{res}_v(tw)$. □

Let $\mathrm{Res}_M = \{\mathrm{res}_u \mid u \in \Sigma^\star\}$ be the set of all residuum functions of words over Σ. Then $(\mathrm{Res}_M, \circ, \mathrm{res}_\varepsilon)$ is a monoid and $d : \Sigma^\star \to \mathrm{Res}_M : u \mapsto \mathrm{res}_u$ is a monoid antihomomorphism. Lemma 3.10 together with the equations above implies that $\mathrm{res}_u \mapsto \mathrm{r}_{[u]}$ is a monoid isomorphism from $(\mathrm{Res}_M, \circ, \mathrm{res}_\varepsilon)$ to $(\mathbb{R}_M, \circ, \mathrm{r}_1)$.

Lemma 3.11. Let $x, y \in M$ and $t_i \in \Sigma$ for $i = 1, 2, \ldots, n$ such that $\mathrm{r}_x(y) = [t_1 t_2 \ldots t_n]$. Then there exist $s_i \in \Sigma$ for $i = 1, 2, \ldots, n$ such that $\mathrm{res}_x(s_1 s_2 \ldots s_n) = t_1 t_2 \ldots t_n$. These elements s_i of Σ are unique.

Proof. Since $x \wedge y = 1$, the finite distributive lattices $\downarrow y$ and $[x, x \vee y] = \{z \in M \mid x \leqslant z \leqslant x \vee y\}$ are isomorphic (Birkhoff 1940, Theorem 7.7.13). An isomorphism is given by $a \mapsto a \vee x$ for $a \in \downarrow y$. Inductively, define s_i to be the unique element from M with $[s_1 s_2 \ldots s_i] \vee x = x \cdot [t_1 t_2 \ldots t_i]$. Then one can easily show that s_i does not have a proper divisor. In addition, $t_{i+1} = s_{i+1} \uparrow (x \uparrow [s_1 s_2 \ldots s_i])$, and therefore $\mathrm{res}_x(s_1 s_2 \ldots s_n) = t_1 t_2 \ldots t_n$. The uniqueness is clear since res_x is injective. □

4. Complete grids and the rank

In trace theory, the generalized Levi Lemma (*cf.* Diekert and Métivier (1997)) plays an important role. It was extended to concurrency monoids in Droste (1995). Here, we develop a further generalization to divisibility monoids using complete grids. This enables us to obtain a concept of 'rank' of a language in these monoids, similar to the one given in Hashigushi (1991) for trace monoids. Let M be a divisibility monoid and $x, y \in M$. Recall that $\mathrm{r}_x(y) = y \uparrow x$. Sometimes (for instance in the following definition), it is more convenient to use this notation for the functions res_u too. Therefore, we define $v \uparrow u := \mathrm{res}_u(v)$ whenever the latter is defined for $u, v \in \Sigma^\star$.

Definition 4.1. For $0 \leqslant i \leqslant j \leqslant n$ let $x_j^i, y_i^j \in M$ ($\in \Sigma^\star$, respectively). The tuple $(x_j^i, y_i^j)_{0 \leqslant i \leqslant j \leqslant n}$ is a *complete grid* in M ($\Sigma^\star$, respectively) provided the following hold for any $0 \leqslant i < j \leqslant n$:

— $x_j^i \parallel y_i^{j-1}$;
— $x_j^i \uparrow y_i^{j-1} = x_j^{i+1}$; and
— $y_i^{j-1} \uparrow x_j^i = y_i^j$.

A complete grid can be depicted as in Figure 1. There, edges depict elements from M ($\Sigma^\star$, respectively) and an angle denotes the fact that the two edges correspond to complementary elements. Note that in any of the small squares in Figure 1, the lower left corner is marked by an angle. This indicates that $x_j^i y_i^j = y_i^{j-1} x_j^{i+1}$ because of $x_j^i y_i^j =$

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

$x_j^i(y_i^{j-1} \uparrow x_j^i) = x_j^i \vee y_i^{j-1} = y_i^{j-1}(x_j^i \uparrow y_i^{j-1}) = y_i^{j-1}x_j^{i+1}$. By Lemma 3.8, for any rectangle in the grid $(x_j^i, y_i^j)_{0\leqslant i\leqslant j\leqslant n}$ the bottom and the left-hand side are complementary and their residuum is the top (the right-hand) side, respectively. By induction, it is easy to show that $(x_0^0x_1^0x_2^0\dots x_n^0)\cdot(y_0^ny_1^n\dots y_n^n) = (x_0^0y_0^0)(x_1^1y_1^1)(x_2^2y_2^2)\dots(x_n^ny_n^n)$. The right-hand side of this equation is the diagonal border of the grid in Figure 1.

Let $(M,\cdot,1)$ be a divisibility monoid and $(x_j^i, y_i^j)_{0\leqslant i\leqslant j\leqslant n}$ be a complete grid in M or in $\Sigma^\star$. For a sequence $0 = i_0 < i_1 < \dots < i_{m+1} = n$, we define a subgrid $(a_l^k, b_k^l)_{0\leqslant k\leqslant l\leqslant m}$ as follows: Let $a_l^k := x_{i_l}^{i_k}x_{i_l+1}^{i_k}x_{i_l+2}^{i_k}\dots x_{i_{l+1}-1}^{i_k}$ and $b_k^l := y_{i_k}^{i_{l+1}-1}y_{i_k+1}^{i_{l+1}-1}\dots y_{i_{k+1}-1}^{i_{l+1}-1}$ (for $m = 4$ and $\vec{i} = (0,1,5,7,9)$, this grid is marked by thick lines in Figure 1). Then $(a_l^k, b_k^l)_{0\leqslant k\leqslant l\leqslant m}$ is a complete grid in M or $\Sigma^\star$. We call it the *subgrid generated by the sequence* $(i_k)_{0\leqslant k\leqslant m}$.

Let $(x_j^i, y_i^j)_{0\leqslant i\leqslant j\leqslant n}$ be a complete grid in $\Sigma^\star$. It is immediate that $([x_j^i], [y_i^j])_{0\leqslant i\leqslant j\leqslant n}$ is a complete grid in M. The following lemma deals with the converse implication.

Lemma 4.2. Let $(x_j^i, y_i^j)_{0\leqslant i\leqslant j\leqslant n}$ be a complete grid in M and let $u_j^0, v_j^n \in \Sigma^\star$ with $[u_j^0] = x_j^0$ and $[v_n^j] = y_n^j$ for $0 \leqslant j \leqslant n$. Then there exists a complete grid $(u_j^i, v_i^j)_{0\leqslant i\leqslant j\leqslant n}$ in $\Sigma^\star$ with $[u_j^i] = x_j^i$ and $[v_i^j] = y_i^j$ for $0 \leqslant i \leqslant j \leqslant n$.

Proof. For $1 \leqslant i \leqslant j \leqslant n$ let $u_j^i := \mathrm{res}_{y_i^{j-1}}(u_j^{i-1})$. By induction one can check that $[u_j^i] = x_j^i$, and that therefore $u_j^{i-1} \in \mathrm{dom}(\mathrm{res}_{y_i^{j-1}})$. To construct the elements v_i^j, we use Lemma 3.11: let v_i^j be the unique word over Σ such that $v_i^j \uparrow u_{j+1}^i = v_i^{j+1}$. Then $[v_i^j] = y_i^j$ is immediate since $y_i^j \in M$ is the unique complement of x_{j+1}^i in the distributive lattice $[1, x_{j+1}^i \vee y_i^j]$. It is clear that $(u_j^i, v_i^j)_{0\leqslant i\leqslant j\leqslant n}$ is a complete grid because of $[u_j^i] = x_j^i$ and $[v_i^j] = y_i^j$ for $0 \leqslant i \leqslant j \leqslant n$. □

The elements $h_{i,j}$ from M marking the corners of the small square in Figure 1 are defined by

$$h_{i,j} := (x_0^0x_1^0\dots x_{j-1}^0)\cdot(y_0^{j-1}y_1^{j-1}\dots y_{i-1}^{j-1}).$$

Then $h_{i,j+1} = h_{i,j}\cdot x_j^i$ and $h_{i+1,j} = h_{i,j}\cdot y_i^{j-1}$. Hence, by Lemma 3.2, $h_{i,j} = h_{i,j+1} \wedge h_{i+1,j}$ and $h_{i+1,j+1} = h_{i,j+1} \vee h_{i+1,j}$. These relations will be used in the proof of the following lemma. It can be read as the converse of the equality $(x_0^0x_1^0\dots x_n^0)\cdot(y_0^ny_1^n\dots y_n^n) = (x_0^0y_0^0)(x_1^1y_1^1)(x_2^2y_2^2)\dots(x_n^ny_n^n)$: whenever the product of two elements of M equals the product of finitely many elements, there exists a corresponding complete grid. This lemma is the announced extension of Levi's Lemma from trace theory into our setting of divisibility monoids.

Lemma 4.3. Let $z_0, z_1, \dots, z_n, x, y \in M$ with $x\cdot y = z_0\cdot z_1\cdots z_n$. Then there exists a complete grid $(x_j^i, y_i^j)_{0\leqslant i\leqslant j\leqslant n}$ in M such that:

— $x = x_0^0x_1^0\dots x_n^0$;
— $y = y_0^ny_1^n\dots y_n^n$; and
— $z_i = x_i^iy_i^i$ for $i = 0,1,\dots,n$.

The complete grid whose existence is claimed by the lemma above is also unique. But in this paper, we will not need the uniqueness.

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

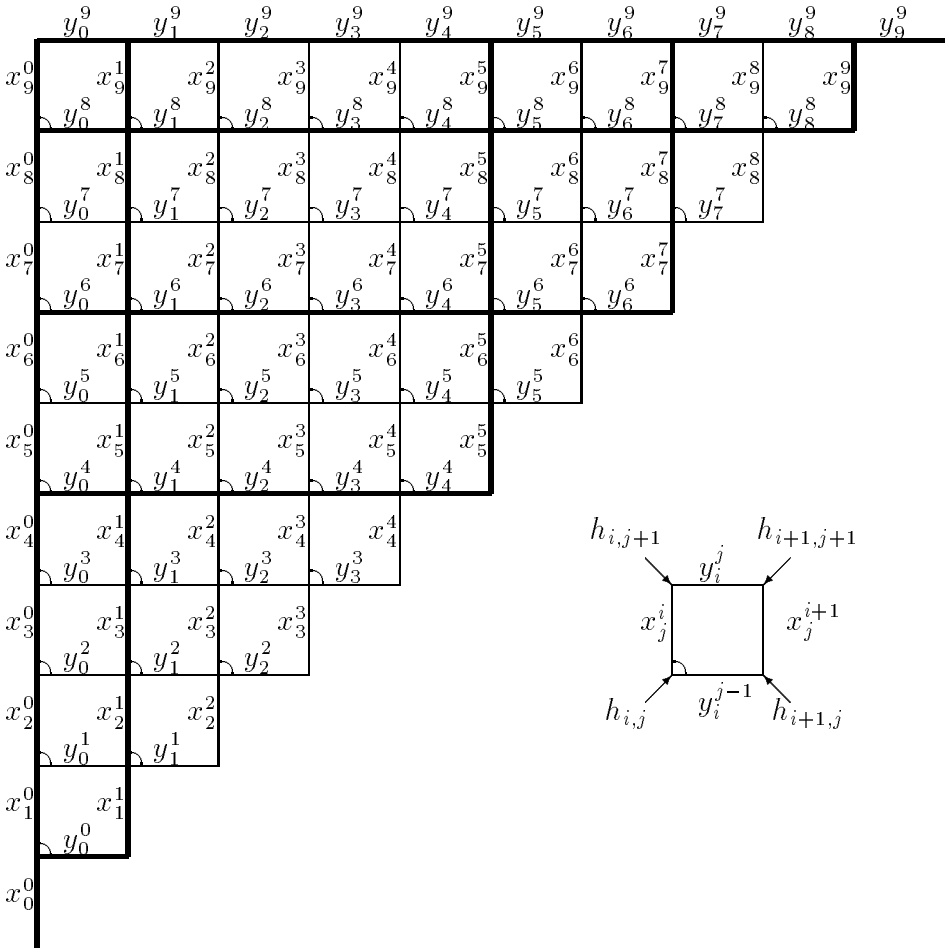


Fig. 1. A complete grid

Proof. Let $h_{0,j} := x \wedge z_0 z_1 \dots z_{j-1}$ and $h_{j,j} = z_0 \cdot z_1 \dots z_{j-1}$ (for $1 \leqslant j \leqslant n+1$). Note that $h_{0,j} \leqslant h_{0,j+1}$ and $h_{j,j} \leqslant h_{j+1,j+1}$. Furthermore, let $h_{i,j} := h_{0,j} \vee h_{i,i}$ for $0 < i < j \leqslant n+1$. Then $h_{i+1,j+1} = h_{0,j+1} \vee h_{i+1,i+1} = h_{0,j+1} \vee h_{0,j} \vee h_{i+1,i+1} \vee h_{i,i} = h_{i,j+1} \vee h_{i+1,j}$.

Now let $0 \leqslant i < j \leqslant n+1$. Then $h_{0,j+1} \wedge h_{i+1,i+1} = x \wedge z_0 z_1 \cdots z_j \wedge z_0 z_1 \cdots z_i = h_{0,i+1} \leqslant h_{0,j}$, and so

$$\begin{aligned}
h_{i,j+1} \wedge h_{i+1,j} &= (h_{0,j+1} \vee h_{i,i}) \wedge (h_{0,j} \vee h_{i+1,i+1}) \\
&= (h_{0,j+1} \wedge h_{0,j}) \vee (h_{0,j+1} \wedge h_{i+1,i+1}) \vee (h_{i,i} \wedge h_{0,j}) \vee (h_{i,i} \wedge h_{i+1,i+1}) \\
&= h_{0,j} \vee h_{0,i+1} \vee (h_{i,i} \wedge h_{0,j}) \vee h_{i,i} \\
&= h_{0,j} \vee h_{i,i} \qquad \text{(since } h_{0,i+1} \leqslant h_{0,j} \text{ and } h_{i,i} \wedge h_{0,j} \leqslant h_{i,i}\text{)} \\
&= h_{i,j}.
\end{aligned}$$

Now the elements x_j^i and y_i^j for $0 \leqslant i \leqslant j \leqslant n$ of the complete grid are the monoid elements uniquely determined by $h_{i,j+1} = h_{i,j} \cdot x_j^i$ and $h_{i+1,j+1} = h_{i,j+1} \cdot y_i^j$.

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

Since $h_{i,j+1} \wedge h_{i+1,j} = h_{i,j}$ and $h_{i+1,j+1} = h_{i,j+1} \vee h_{i+1,j}$, Lemma 3.2 implies $x_j^i \wedge y_i^{j-1} = 1$ and $x_j^i \vee y_i^{j-1} = x_j^i y_i^j = y_i^{j-1} x_j^{i+1}$. Hence $x_j^i \parallel y_i^{j-1}$, $x_j^i \uparrow y_i^{j-1} = x_j^{i+1}$ and $y_i^{j-1} \uparrow x_j^i = y_i^j$. Thus, we have shown that $(x_j^i, y_i^j)_{0 \leqslant i \leqslant j \leqslant n}$ is a complete grid in M.

Note that $x_0^0 x_1^0 \dots x_n^0 = h_{0,n+1} = x \wedge z_0 z_1 \dots z_n = x \wedge xy = x$. Furthermore, $h_{j,j} \cdot z_j = h_{j+1,j+1} = h_{j,j} \cdot x_j^j \cdot y_j^j$ implies $z_j = x_j^j \cdot y_j^j$ since M is cancellative. Hence we have

$$\begin{aligned} x(y_0^n y_1^n \dots y_n^n) &= (x_0^0 x_1^0 \dots x_n^0)(y_0^n y_1^n \dots y_n^n) \\ &= (x_0^0 y_0^0)(x_1^1 y_1^1)(x_2^2 y_2^2) \dots (x_n^n y_n^n) \\ &= z_0 z_1 \dots z_n = xy. \end{aligned}$$

This equality implies $y = y_0^n y_1^n \dots y_n^n$. □

One cannot expect that the elements y_i^j in a complete grid completely determine the elements x_j^i. The following lemma describes the freedom we have in choosing these elements: as long as we keep the residuum functions in the first column, we can complete the whole grid.

Lemma 4.4. Let $(x_j^i, y_i^j)_{0 \leqslant i \leqslant j \leqslant n}$ be a complete grid in M, $w_j^0 \in M$ with $\mathrm{r}_{x_j^0} = \mathrm{r}_{w_j^0}$ for $0 \leqslant j \leqslant n$. Then there exists a complete grid $(w_j^i, y_i^j)_{0 \leqslant i \leqslant j \leqslant n}$ in M.

Proof. By Lemma 3.8(1), $x_j^0 \parallel y_0^{j-1} y_1^{j-1} \dots y_{j-1}^{j-1}$ for any $0 \leqslant j \leqslant n$. Since the residuum functions of x_j^0 and w_j^0 coincide, this implies $w_j^0 \parallel y_0^{j-1} y_1^{j-1} \dots y_{i-1}^{j-1}$ for $0 \leqslant i \leqslant j \leqslant n$. Hence $w_j^i := w_j^0 \uparrow (y_0^{j-1} y_1^{j-1} \dots y_{i-1}^{j-1})$ is defined. Using Lemma 3.8(1), we get $w_j^i \parallel y_i^{j-1}$. By Lemma 3.8(2), $w_j^{i+1} = w_j^i \uparrow y_i^{j-1}$. Since $x_j^i = x_j^0 \uparrow y_0^{j-1} y_1^{j-1} \dots y_{i-1}^{j-1}$ and $\mathrm{r}_{x_j^0} = \mathrm{r}_{w_j^0}$, Lemma 3.8(4) implies $\mathrm{r}_{x_j^i} = \mathrm{r}_{w_j^i}$. Hence $y_i^j = \mathrm{r}_{x_j^i}(y_i^{j-1}) = \mathrm{r}_{w_j^i}(y_i^{j-1}) = y_i^{j-1} \uparrow w_j^i$. □

Recall that $[\mathrm{res}_v(u)] = \mathrm{r}_{[v]}([u])$ for any words u, v. Using Lemma 4.2, one gets the following corollary as a direct consequence.

Corollary 4.5. Let $(u_j^i, v_i^j)_{0 \leqslant i \leqslant j \leqslant n}$ be a complete grid in $\Sigma^\star$, and $w_j^0 \in \Sigma^\star$ with $\mathrm{res}_{u_j^0} = \mathrm{res}_{w_j^0}$ for $0 \leqslant j \leqslant n$. Then there exists a complete grid $(w_j^i, v_i^j)_{0 \leqslant i \leqslant j \leqslant n}$ in $\Sigma^\star$.

In a similar way to the above, a direct consequence of Lemma 4.3 is the existence of complete grids in the free monoid $\Sigma^\star$.

Corollary 4.6. Let $z_0, z_1, \dots, z_n, u, v \in \Sigma^\star$ with $[uv] = [z_1 z_2 \dots z_n]$. Then there exists a complete grid $(u_j^i, v_i^j)_{0 \leqslant i \leqslant j \leqslant n}$ in $\Sigma^\star$ such that:

1. $[u] = [u_0^0 u_1^0 \dots u_n^0]$;
2. $[v] = [v_0^n v_1^n \dots v_n^n]$; and
3. $[z_i] = [u_i^i v_i^i]$ for $i = 0, 1, \dots, n$.

Note that in general we cannot omit the brackets, that is, these equations do not necessarily hold in $\Sigma^\star$. But if the words z_i are actually from $\Sigma \cup \{\varepsilon\}$ (that is, their length is at most 1), we can replace the third statement by

3′. $z_i = u_i^i v_i^i$ for $i = 0, 1, \dots, n$.

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

Now we can introduce the notion of rank in the present context. For traces, it was defined and shown to be very useful in Hashigushi (1991), *cf.* Diekert and Rozenberg (1995) and Diekert and Métivier (1997).

Definition 4.7. Let $u, v \in \Sigma^\star$ and $X \subseteq \Sigma^\star$ such that $[uv] \in [X] := \{[w] \mid w \in X\}$. Let $\mathrm{rk}(u, v, X)$ denote the minimal integer n such that there exists a complete grid $(u_j^i, v_i^j)_{0 \leqslant i \leqslant j \leqslant n}$ in $\Sigma^\star$ with:

1. $[u] = [u_0^0 u_1^0 \dots u_n^0]$;
2. $[v] = [v_0^n v_1^n \dots v_n^n]$;
3. $u_0^0 v_0^0 u_1^1 v_1^1 \dots u_n^n v_n^n \in X$.

Let $u, v \in \Sigma^\star$ and $X \subseteq \Sigma^\star$ such that $[uv] \in [X] := \{[w] \mid w \in X\}$. Then there exists $z \in X$ with $[z] = [uv]$. Let $z = z_1 z_2 \dots z_n$ with $z_i \in \Sigma$. Then $n = |uv|$, and by Corollary 4.6 and the consideration above, we find an appropriate complete grid. Hence $\mathrm{rk}(u, v, X) \leqslant |uv|$. If not only $[uv] \in [X]$ but also $uv \in X$, we can choose $n = 0$, $u_0^0 = u$ and $v_0^0 = v$, and obtain $\mathrm{rk}(u, v, X) = 0$. We define the *rank* $\mathrm{rk}(X)$ *of* X by

$$\mathrm{rk}(X) := \sup\{\mathrm{rk}(u, v, X) \mid u, v \in \Sigma^\star, [uv] \in [X]\} \in \mathbb{N} \cup \{\infty\}.$$

A word language $X \subseteq \Sigma^\star$ is *closed* if $[u] \in [X]$ implies $u \in X$ for any $u \in \Sigma^\star$. Since $\mathrm{rk}(u, v, X) = 0$ whenever $uv \in X$, the rank of a closed language equals 0.

Theorem 4.8. Let $(M, \cdot, 1)$ be a divisibility monoid with finitely many residuum functions (that is, the monoid $\mathbb{R}_M$ is finite). Let $X \subseteq \Sigma^\star$ be recognizable and $n := \mathrm{rk}(X)$ be finite. Then $[X]$ is recognizable in M.

Proof. Since X is recognizable, there is a finite monoid S and a homomorphism $\eta : \Sigma^\star \to S$ that recognizes X. Since the mapping $u \mapsto \mathrm{res}_u$ is an antihomomorphism from $\Sigma^\star$ into the finite monoid $(\mathrm{Res}_M, \circ, \mathrm{res}_\varepsilon)$, we may assume that $\eta(u) = \eta(v)$ implies $\mathrm{res}_u = \mathrm{res}_v$. For $x \in M$ let

$$R(x) := \{(\eta f(x_0), \eta f(x_1) \dots \eta f(x_n))_{f \in \mathrm{Res}_M} \mid x_0, x_1, \dots, x_n \in \Sigma^\star \text{ and } x = [x_0 x_1 \dots x_n]\}.$$

Then $R(x)$ is a subset of $(S^{n+1})^{|\mathrm{Res}_M|}$. Since Res_M and S are finite, there are only finitely many sets $R(x)$. Once we have shown $R(x) = R(z) \Rightarrow x^{-1}[X] = z^{-1}[X]$, we thus have that $\{x^{-1}[X] \mid x \in M\}$ is finite. Hence $[X]$ is recognizable.

So let $R(x) = R(z)$ and let $y \in x^{-1}[X]$, that is, $xy \in [X]$. Since $\mathrm{rk}(X) = n$, there exists a complete grid $(u_j^i, v_i^j)_{0 \leqslant i \leqslant j \leqslant n}$ in $\Sigma^\star$ such that:

— $x = [u_0^0 u_1^0 \dots u_n^0]$;
— $y = [v_0^n v_1^n \dots v_n^n]$; and
— $u_0^0 v_0^0 u_1^1 v_1^1 \dots u_n^n v_n^n \in X$.

Then $(\eta f(u_0^0), \eta f(u_1^0) \dots \eta f(u_n^0))_{f \in \mathrm{Res}_M} \in R(x) = R(z)$. Hence there exist words $w_j^0 \in \Sigma^\star$ with:

(1) $\eta f(w_j^0) = \eta f(u_j^0)$ for each $0 \leqslant j \leqslant n$ and $f \in \mathrm{Res}_M$; and
(2) $z = [w_0^0 w_1^0 \dots w_n^0]$.

In (1), consider $f = \mathrm{res}_\varepsilon$, which equals the identity on $\Sigma^\star$. Then $\eta(w_j^0) = \eta(u_j^0)$, and therefore (by our assumption on η) $\mathrm{res}_{w_j^0} = \mathrm{res}_{u_j^0}$. Hence we can apply Corollary 4.5 and

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

obtain a complete grid $(w_j^i, v_i^j)_{0\leqslant i\leqslant j\leqslant n}$ in $\Sigma^\star$. Now consider $f = \mathrm{res}_{v_0^{j-1}v_1^{j-1}\dots v_{j-1}^{j-1}} \in \mathrm{Res}_M$. Note that $w_j^j = w_j^0 \uparrow (v_0^{j-1}v_1^{j-1}\dots v_{j-1}^{j-1}) = f(w_j^0)$. Hence $\eta(w_j^j) = \eta f(w_j^0) = \eta f(u_j^0) = \eta(u_j^j)$. Now we can conclude

$$\begin{aligned}\eta(w_0^0v_0^0w_1^1v_1^1\dots w_n^nv_n^n) &= \eta(w_0^0)\eta(v_0^0)\eta(w_1^1)\eta(v_1^1)\dots\eta(w_n^n)\eta(v_n^n)\\ &= \eta(u_0^0)\eta(v_0^0)\eta(u_1^1)\eta(v_1^1)\dots\eta(u_n^n)\eta(v_n^n)\\ &= \eta(u_0^0v_0^0u_1^1v_1^1\dots u_n^nv_n^n) \in \eta(X).\end{aligned}$$

Hence $w_0^0v_0^0w_1^1v_1^1\dots w_n^nv_n^n \in X$. Since $([w_j^i],[v_i^j])_{0\leqslant i\leqslant j\leqslant n}$ is a complete grid in M, we obtain $zy = [w_0^0v_0^0w_1^1v_1^1\dots w_n^nv_n^n] \in [X]$. Hence $y \in z^{-1}[X]$, and therefore $x^{-1}[X] = z^{-1}[X]$, as claimed above. □

5. From c-rational to recognizable languages

In this section we prove closure properties of the set of recognizable languages in a divisibility monoid. These closure properties correspond to c-rational languages, which we introduce first.

In trace theory, there is the notion of a connected trace. Algebraically, a trace x is connected if it cannot be written as the supremum of two non-trivial traces, that is, if the distributive lattice $\downarrow x$ has no non-trivial pair of complementary elements. We use this characterization as definition: let $(M,\cdot,1)$ be a divisibility monoid. An element $x \in M$ is *connected* if the distributive lattice $\downarrow x$ does not contain any pair of complementary elements. In other words, there are *no* complementary $y,z \in M\setminus\{1\}$ such that $x = y\vee z = y\mathrm{r}_y(z)$. A set $X \subseteq M$ is *connected* if all of its elements are connected; a language $X \subseteq \Sigma^\star$ is *connected* if $[X] \subseteq M$ is connected.

A language $X \subseteq \Sigma^\star$ is *residually closed* if for any $u \in X$ and $v \in \Sigma^\star$ with $u \parallel v$ the following holds:

$$v \in X \iff \mathrm{res}_u(v) \in X.$$

Thus X is residually closed if it is closed under the application of res_u and res_u^{-1} for elements u of X. Note that this need not hold for all $u \in \Sigma^\star$. A language $L \subseteq M$ is *residually closed* iff $\{w \in \Sigma^\star \mid [w] \in L\}$ is residually closed.

Now we define c-rational languages: the class of *c-rational languages* in a divisibility monoid M is the smallest class $\mathscr{C}$ satisfying:

1. any finite subset of M is in $\mathscr{C}$;
2. whenever $L,K \in \mathscr{C}$ we have $L\cup K \in \mathscr{C}$ and $L\cdot K \in \mathscr{C}$; and
3. whenever $L \in \mathscr{C}$ is connected and residually closed we have $\langle L\rangle \in \mathscr{C}$.

Now we are going to show that the set of recognizable languages is closed under multiplication.

Lemma 5.1. Let $(M,\cdot,1)$ be a divisibility monoid and $X,Y \subseteq \Sigma^\star$ be closed. Then $\mathrm{rk}(XY) \leqslant 1$.

Proof. Let $u,v \in \Sigma^\star$ with $[uv] \in [XY]$. Then there exist $z_0 \in X$ and $z_1 \in Y$ such that $[uv] = [z_0z_1]$. By Corollary 4.6, there exists a complete grid $(u_j^i, v_i^j)_{0\leqslant i\leqslant j\leqslant 1}$ in $\Sigma^\star$ such that

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

$$[u] = [u_0^0 u_1^0], \qquad [v] = [v_0^1 v_1^1],$$
$$[z_0] = [u_0^0 v_0^0], \text{ and } \quad [z_1] = [u_1^1 v_1^1].$$

Since X and Y are closed, this implies $u_0^0 v_0^0 \in X$ and $u_1^1 v_1^1 \in Y$. Hence $\mathrm{rk}(u, v, XY) \leqslant 1$. □

Corollary 5.2. Let $(M, \cdot, 1)$ be a divisibility monoid with finitely many residuum functions. Let $K, L \subseteq M$ be recognizable. Then $K \cdot L$ is recognizable.

Proof. Let $X := \{u \in \Sigma^\star \mid [u] \in K\}$ and $Y := \{u \in \Sigma^\star \mid [u] \in L\}$. Then $K \cdot L = [XY]$, and X and Y are closed and recognizable in $\Sigma^\star$. Hence, by Kleene's theorem, XY is recognizable in $\Sigma^\star$. By Lemma 5.1, the rank of XY is finite. Hence Theorem 4.8 ensures that $[XY]$ is recognizable in M. □

The rest of this section is mainly devoted to the proof that $\langle L \rangle$ is recognizable for any recognizable language $L \subseteq M$ that is connected and residually closed.

Lemma 5.3. Let $(M, \cdot, 1)$ be a divisibility monoid with finitely many residuum functions and let $a_1, a_2, b, c, \overline{v} \in \Sigma^\star$ such that $\mathrm{res}_{a_1 a_2} = \mathrm{res}_b = \mathrm{res}_{a_1 a_2 b}$, $c \parallel a_1 a_2$, $(c \uparrow a_1)\overline{v} \parallel a_2 b$ and $a_1 \neq \varepsilon \neq \overline{v}$. Then $[(a_1 \uparrow c)\overline{v}]$ is not connected.

Proof. Throughout this proof, we make extensive use of the equations given in Lemma 3.9 without referring to it again.

By $\mathrm{res}_{a_1 a_2} = \mathrm{res}_{a_1 a_2 b} = \mathrm{res}_b \circ \mathrm{res}_{a_1 a_2} = \mathrm{res}_{a_1 a_2} \circ \mathrm{res}_{a_1 a_2}$, the function $\mathrm{res}_{a_1 a_2}$ is idempotent. Since it is, in addition, an injective partial function, it is contained in the identity on $\Sigma^\star$, that is, $\mathrm{res}_{a_1 a_2}(w) = w$ for $w \in \mathrm{dom}(\mathrm{res}_{a_1 a_2})$.

By $(c \uparrow a_1)\overline{v} \parallel a_2 b$, we get, in particular, $(c \uparrow a_1)\overline{v} \parallel a_2$, and $(c \uparrow a_1)\overline{v} \uparrow a_2 \in \mathrm{dom}(\mathrm{res}_b)$. Now we can conclude (with $\tilde{v} := \overline{v} \uparrow (a_2 \uparrow (c \uparrow a_1))$)

$$\begin{aligned} b \quad &\parallel \quad (c \uparrow a_1)\overline{v} \uparrow a_2 \\ &= \quad ((c \uparrow a_1) \uparrow a_2)\ (\overline{v} \uparrow (a_2 \uparrow (c \uparrow a_1))) \\ &= \quad [c \uparrow a_1 a_2]\tilde{v} \\ &= \quad c\tilde{v}. \end{aligned}$$

Thus we get $c\tilde{v} = (c \uparrow a_1)\overline{v} \uparrow a_2 \in \mathrm{dom}(\mathrm{res}_{a_1 a_2})$, and therefore $c\tilde{v} \uparrow a_1 a_2 = c\tilde{v}$. In particular, we have $a_1 \parallel c\tilde{v}$ implying $(a_1 \uparrow c) \parallel \tilde{v}$.

Hence we have $(c \uparrow a_1)\overline{v} \uparrow a_2 = c\tilde{v} = (c\tilde{v} \uparrow a_1) \uparrow a_2$. This implies $(c \uparrow a_1)\overline{v} = c\tilde{v} \uparrow a_1$ since res_{a_2} is injective. Note that $c\tilde{v} \uparrow a_1 = (c \uparrow a_1)(\tilde{v} \uparrow (a_1 \uparrow c))$. Hence, by cancellation, we get $\overline{v} = \tilde{v} \uparrow (a_1 \uparrow c)$. This implies $[\tilde{v}] \vee [a_1 \uparrow c] = [(a_1 \uparrow c)\overline{v}]$.

Since $a_1 \neq \varepsilon$ and res_c is length preserving, we have $a_1 \uparrow c \neq \varepsilon$, that is, $[a_1 \uparrow c] \neq 1$. Similarly, $\overline{v} \neq \varepsilon$ implies $[\tilde{v}] \neq 1$. Finally, $(a_1 \uparrow c) \parallel \tilde{v}$ proves that $[(a_1 \uparrow c)\overline{v}]$ is not connected. □

Before proving that the iteration of a residually closed and connected language in M has finite rank, we cite Ramsey's theorem in a form that best suits our needs in the proof of Theorem 5.4 (*cf.* Cameron (1994)).

Theorem. (Ramsey 1930) Let r be a positive integer. Then there is a positive integer $R(r)$

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

such that for any mapping f of the 2-element subsets of $\{1,2,\ldots,R(r)\}$ into $\{1,2,\ldots,r\}$ there exist $1 \leqslant \alpha \leqslant \beta \leqslant \gamma \leqslant R(r)$ with $f(\{\alpha,\beta\}) = f(\{\beta,\gamma\}) = f(\{\alpha,\gamma\})$.

Theorem 5.4. Let $(M,\cdot,1)$ be a divisibility monoid with finitely many residuum functions. Let $X \subseteq \Sigma^\star$ be closed, connected and residually closed. Then $\mathrm{rk}(\langle X\rangle)$ is finite.

Proof. Let $u,v \in \Sigma^\star$ with $[uv] \in [\langle X\rangle] = \langle [X]\rangle$. Then we have that there exist $n \in \mathbb{N}$ and $x_0,x_1,\ldots,x_n \in X$ such that $[uv] = [x_0x_1\ldots x_n]$. By Corollary 4.6, there exists a complete grid $(u^i_j, v^j_i)_{0\leqslant i\leqslant j\leqslant n}$ in $\Sigma^\star$ such that $[u] = [u^0_0u^0_1\ldots u^0_n]$, $[v] = [v^n_0v^n_1\ldots v^n_n]$ and $[x_i] = [u^i_iv^i_i]$. Since X is closed and connected, the latter implies that $u^i_iv^i_i \in X$ is connected.

There exist $m \leqslant n$ and $-1 = i_0 < i_1 < i_2 \cdots < i_m < i_{m+1} = n+1$ such that:

— $u^{i_k}_{i_k}$ and $v^{i_k}_{i_k}$ are nonempty for $0 < k < m+1$;
— u^i_i or v^i_i is empty whenever $0 \leqslant k \leqslant m$ and $i_k < i < i_{k+1}$.

Assume, there are $1 \leqslant \alpha \leqslant \beta \leqslant \gamma \leqslant m$ such that

$$\mathrm{res}_{u^0_{i_\alpha}u^0_{i_\alpha+1}\ldots u^0_{i_\beta}-1} = \mathrm{res}_{u^0_{i_\beta}u^0_{i_\beta+1}\ldots u^0_{i_\gamma}-1} = \mathrm{res}_{u^0_{i_\alpha}u^0_{i_\alpha+1}\ldots u^0_{i_\gamma}-1}.$$

With $a_1 = u^0_{i_\alpha}$, $a_2 = u^0_{i_\alpha+1}u^0_{i_\alpha+2}\ldots u^0_{i_\beta-1}$, $b = u^0_{i_\beta}u^0_{i_\beta+1}\ldots u^0_{i_\gamma-1}$, $c = v_0^{i_\alpha-1}v_1^{i_\alpha-1}\ldots v_{i_\alpha-1}^{i_\alpha-1}$ and $\overline{v} = v^{i_\alpha}_{i_\alpha}$, the assumptions of Lemma 5.3 are satisfied. Thus $[u^{i_\alpha}_{i_\alpha}v^{i_\alpha}_{i_\alpha}]$ is not connected, which is a contradiction. Therefore, α,β,γ with the property given above cannot exist.

To apply Ramsey's theorem, consider the mapping f from the 2-elements subsets of $\{1,2,\ldots,m\}$ into Res_M with $f(\{\alpha,\beta\}) = \mathrm{res}_{u^0_{i_\alpha}}\mathrm{res}_{u^0_{i_\alpha+1}}\ldots\mathrm{res}_{u^0_{i_\beta-1}}$ for $\alpha \leqslant \beta$. Since Res_M is finite, Ramsey's theorem implies $m \leqslant R(|\mathrm{Res}_M|)$.

Let $0 \leqslant k \leqslant m$ and $i_k < i < i_{k+1}$. Then $u^i_iv^i_i \in X$. Since one of u^i_i and v^i_i is empty, the other belongs to X, that is, $u^i_i, v^i_i \in X \cup \{\varepsilon\}$.

Now we show $u^i_j, v^j_i \in X \cup \{\varepsilon\}$ by induction on j for $i_k < i \leqslant j < i_{k+1}$.

Assume $i_k + 1 = j$. Then the claim is trivial since $i = j$ follows. Now assume that for any $i_k \leqslant i \leqslant l \leqslant i_{k+1}$ with $l < j$ we have $u^i_l, v^l_i \in X \cup \{\varepsilon\}$. Then $u^i_j \uparrow (v^{j-1}_i v^{j-1}_{i+1}\ldots v^{j-1}_{j-1}) = u^j_j \in X \cup \{\varepsilon\}$. Note that the upper index $j-1$ of the v's is properly between i_k and j. Hence, by the induction hypothesis, $v^{j-1}_{i'} \in X \cup \{\varepsilon\}$ for $i' = i, i+1,\ldots,j-1$. Since X, and therefore $X \cup \{\varepsilon\}$, is residually closed, we get $u^i_j \in X \cup \{\varepsilon\}$. On the other hand, $v^j_i = v^{j-1}_i \uparrow u^i_j$. By the induction hypothesis, $v^{j-1}_i \in X \cup \{\varepsilon\}$. Hence $v^j_i \in X \cup \{\varepsilon\}$ since u^i_j is an element of this residually closed language.

Now consider the complete grid $(a^i_j, b^i_j)_{0\leqslant i\leqslant j\leqslant 2m+1}$ generated by the sequence $(i_1, i_1+1, i_2, i_2+1,\ldots,i_m,i_m+1)$. Then

$$\begin{aligned}
a^{2k}_{2k} &= u^{i_k+1}_{i_k+1}u^{i_k+1}_{i_k+2}u^{i_k+1}_{i_k+3}\ldots u^{i_k+1}_{i_{k+1}-1},\\
b^{2k}_{2k} &= v^{i_{k+1}-1}_{i_k+1}v^{i_{k+1}-1}_{i_k+2}v^{i_{k+1}-1}_{i_k+3}\ldots v^{i_{k+1}-1}_{i_{k+1}-1},\\
a^{2k+1}_{2k+1} &= u^{i_k}_{i_k}, \text{ and}\\
b^{2k+1}_{2k+1} &= v^{i_k}_{i_k}.
\end{aligned}$$

Note that all the factors of a^{2k}_{2k} and of b^{2k}_{2k} belong to $X \cup \{\varepsilon\}$. Hence $a^{2k}_{2k}b^{2k}_{2k} \in \langle X\rangle$. Thus, the complete grid $(a^i_j, b^j_i)_{0\leqslant i\leqslant j\leqslant 2m+1}$ satisfies:

— $[u] = [u^0_0u^0_1\ldots u^0_n] = [a^0_0a^0_1\ldots a^0_{2m+1}]$;

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

— $[v] = [v_0^n v_1^n \dots v_n^n] = [b_0^{2m+1} b_1^{2m+1} \dots b_{2m+1}^{2m+1}]$; and
— $a_i^i b_i^i \in \langle X \rangle$.

Therefore $\mathrm{rk}(u, v, \langle X \rangle) \leqslant 2m + 1 \leqslant 2R(|\mathrm{Res}_M|) + 1$. □

Corollary 5.5. Let $(M, \cdot, 1)$ be a divisibility monoid with finitely many residuum functions. Let $L \subseteq M$ be connected, recognizable, and residually closed. Then $\langle L \rangle$ is recognizable.

Proof. Let $X := \{w \in \Sigma^\star \mid [w] \in L\}$. Note that M and X satisfy the assumptions of Theorem 5.4. Hence the rank $\mathrm{rk}(\langle X \rangle)$ is finite. By Kleene's theorem, $\langle X \rangle$ is recognizable in $\Sigma^\star$. By Theorem 4.8, $\langle L \rangle = [\langle X \rangle]$ is recognizable in M. □

Theorem 5.6. Let $(M, \cdot, 1)$ be a divisibility monoid with finitely many residuum functions, and let $L \subseteq M$ be c-rational. Then L is recognizable.

Proof. By Lemma 3.3, $\downarrow x$ is finite for any $x \in M$. Hence finite languages in M are recognizable. By Corollary 5.2 and 5.5, the set of recognizable languages in M is closed under products and the operation $\langle . \rangle$ applied to connected and residually closed languages. □

6. From recognizable to mc-rational languages

In this section, we will derive conditions on divisibility monoids M that are sufficient to ensure that all recognizable languages in M are c-rational. Let $(M, \cdot, 1)$ be a divisibility monoid. Recall that an equation $[ab] = [cd]$, where a, b, c, d are irreducible generators of M, states that the different sequential executions ab and cd give rise to the same effect. If now $a \neq c$, the effect of a in the execution cd has to be resumed by that of d. Therefore, we consider the least equivalence $\equiv$ on the irreducible generators of M identifying a and d that occur in an equation $ab = cd$ with $a \neq c$. To show that any recognizable language is c-rational, we need the property that $[ab] = [cd]$ and $a \equiv c$ imply $a = c$ for any irreducible elements $a, b, c, d \in \Sigma$. It is immediate that this is equivalent to the existence of a function $\ell : \Sigma \to \Gamma$ into some set Γ satisfying $\ell(s) = \ell(s \uparrow t)$ and $\ell(s) \neq \ell(t)$ for any $s, t \in \Sigma$ with $s \parallel t$. Such a function is called a *labelling function*. Since Σ is finite, we can assume Γ to be finite too. A divisibility monoid M together with a labelling function ℓ is a *labelled divisibility monoid* (M, ℓ).

Remark 6.1. The following observation was made by one of the referees. Let $(M, \cdot, \ell)$ be a labelled divisibility monoid. Then the reflexive closure of the relation $\{(\ell(a), \ell(c)) \mid \nexists b, d \in \Sigma : ab = cd\}$ on Γ is a dependence relation on the set Γ of labels. Let $\mathbb{M}$ be the generated trace monoid. Then the labelling function ℓ extends to a homomorphism from M onto $\mathbb{M}$. But this homomorphism is not injective. Let M be given by $ab = bc$ with $\ell(a) = \ell(c) = x$ and $\ell(b) = y$. Then $\mathbb{M}$ is the free commutative monoid with two generators, but M is not commutative. Furthermore, in M, the element $abab$ is connected. But its label sequence $xyxy$ is not connected in the trace monoid $\mathbb{M}$. Thus, the extension of ℓ to a monoid homomorphism does not map c-rational sets to c-rational sets.

Unfortunately, neither the referee nor we know whether this observation might help in any of our proofs.

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

The *label sequence* of a word $u_0u_1 \dots u_n \in \Sigma^\star$ is the word $\ell(u_0)\ell(u_1)\dots\ell(u_n) \in \Gamma^\star$. We extend the mapping ℓ to words over Σ by $\ell(tw) = \{\ell(t)\} \cup \ell(w)$. Hence ℓ is a monoid morphism into the finite monoid $(2^\Gamma, \cup, \varnothing)$. By Lemma 3.4, $[u] = [v]$ implies $\ell(u) = \ell(v)$ for any $u, v \in \Sigma^\star$. Therefore, it is reasonable to define $\ell([u]) := \ell(u)$, that is, to extend ℓ to a monoid morphism from $(M, \cdot, 1)$ to $(2^\Gamma, \cup, \varnothing)$.

A language $L \subseteq M$ is *monoalphabetic* if $\ell(x) = \ell(y)$ for any $x, y \in L$. The class of *mc-rational languages* in the labelled divisibility monoid M is the smallest class $\mathscr{C}$ satisfying

1. any finite subset of M is in $\mathscr{C}$,
2. whenever $L, K \in \mathscr{C}$ we have $L \cup K \in \mathscr{C}$ and $L \cdot K \in \mathscr{C}$, and
3. whenever $L \in \mathscr{C}$ is connected and monoalphabetic we have $\langle L \rangle \in \mathscr{C}$.

Note the difference between c- and mc-rational sets: to build a c-rational set, the iteration can be applied to connected and residually closed sets; while for mc-rational sets, we require that the iteration is applied to connected and monoalphabetic sets. In other words, we have replaced the requirement 'residually closed' by 'monoalphabetic'. In an unlabelled divisibility monoid, this latter notion does not make any sense; but for labelled divisibility monoids, Corollary 6.2 shows that the notion of mc-rationality is actually a strengthening of that of c-rationality.

Lemma 6.1. Let (M, ℓ) be a labelled divisibility monoid and $x, y \in M$ with $x \parallel y$. Then $\ell(x) \cap \ell(y) = \varnothing$, $\ell(y) = \ell(y \uparrow x)$, and $\ell(x) \cup \ell(y) = \ell(x \vee y)$.

Proof. Suppose $\ell(x) \cap \ell(y) \neq \varnothing$. Then there exist $x_1, x_2, y_1, y_2, \in M$ and $s, t \in \Sigma$ such that $x = x_1 s x_2$, $y = y_1 t y_2$ and $\ell(s) = \ell(t)$. Clearly, $x_1 s \parallel y_1 t$. By Lemma 3.8, we have $s \parallel (y_1 t \uparrow x_1) = (y_1 \uparrow x_1)(t \uparrow (x_1 \uparrow y_1))$. Hence $s' := s \uparrow (y_1 \uparrow x_1) \parallel (t \uparrow (x_1 \uparrow y_1)) =: t'$. Furthermore, $\ell(s) = \ell(s')$ and $\ell(t) = \ell(t')$. But this contradicts the definition of a labelling function. Hence the first statement is shown.

By a simple induction on the length of x and y, we get $\ell(y \uparrow x) = \ell(y)$, that is, the second statement. Now the last assertion follows since $\ell(x \vee y) = \ell(x(y \uparrow x)) = \ell(x) \cup \ell(y \uparrow x) = \ell(x) \cup \ell(y)$. □

Corollary 6.2. Let $(M, \cdot, 1, \ell)$ be a labelled divisibility monoid. Then any mc-rational language in M is c-rational.

Proof. Let $x, y \in M$ with $\ell(x) = \ell(y)$ and $x \parallel y$. Then Lemma 6.1 ensures $x = y = 1$. Hence any monoalphabetic language is residually closed. This implies that mc-rational languages are c-rational. □

Now let $\preceq$ be a linear order on the set Γ and let $u \in \Sigma^\star$. We say that the word u *is in lexicographical normal form* if $[u] = [v]$ implies that the label sequence of v is lexicographically larger than or equal to that of u. Let LNF be the set of all words in lexicographic normal form.

Remark 6.2. The abovementioned referee also made the following observation. Let M and $\mathbb{M}$ be the monoids from Remark 6.1 and suppose $x \prec y$. Then $abab \in \Sigma^\star$ with label sequence $xyxy$ is in lexicographic normal form as the only equivalent words $bcab$ and $bcbc$

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

have label sequences $yxxy$ and $yxyx$. But the word $xyxy$ is not in lexicographic normal form when viewed as a trace from $\mathbb{M}$ (here, it equals $xxyy$).

Note that so far there may exist different words u and v in LNF with $[u] = [v]$. We will now show that this is impossible.

Lemma 6.3. Let M be a divisibility monoid and $u, v \in \Sigma^\star$. If u and v have the same label sequence and $[u] = [v]$, then $u = v$.

Proof. Let s (t) be the first letter of u (of v, respectively) and suppose $s \neq t$. Then $[s]$ and $[t]$ are incomparable since they have the same length. Thus their infimum is properly smaller than $[s]$. Since 1 is the only element that is properly smaller than the irreducible element $[s]$, we get $[s] \wedge [t] = 1$. Since $[s]$ and $[t]$ are bounded above by $[u] = [v]$, we have $s \parallel t$. Hence $\ell(s) \neq \ell(t)$, contradicting the fact that the label sequences of u and v coincide. Now the proof can easily be completed by induction. □

Hence, for any $x \in M$ there exists at most one $u \in \mathrm{LNF}$ such that $x = [u]$. Since, on the other hand, the lexicographical order on $\Gamma^\star$ is a well-order, the set of label sequences of words u with $[u] = x$ has a least element. Hence, for any $x \in M$ there exists one and only one $u \in \mathrm{LNF}$ with $x = [u]$. This word is called *the lexicographic normal form of* x. We denote it by $\mathrm{lexNF}(x)$.

Lemma 6.4. Let $(M, \cdot, 1, \ell)$ be a labelled divisibility monoid. Then LNF is recognizable in the free monoid $\Sigma^\star$.

Proof. Recall that $\mathrm{Res}_M = \{\mathrm{res}_u \mid u \in \Sigma^\star\}$ is a monoid consisting of partial functions from $\Sigma^\star$ to $\Sigma^\star$. These functions are length preserving. In particular, they map elements of Σ to elements of Σ. Hence $\mathrm{Res}_M \restriction \Sigma := \{\mathrm{res}_u \restriction \Sigma \mid u \in \Sigma^\star\}$ is a monoid. It is finite since Σ is finite. Recall, furthermore, that the mapping $\Sigma^\star \to \mathrm{Res}_M$ defined by $u \mapsto \mathrm{res}_u$ is a monoid antihomomorphism. Hence the mapping from $\Sigma^\star$ to $\mathrm{Res}_M \restriction \Sigma$ with $u \mapsto \mathrm{res}_u \restriction \Sigma$ is a monoid antihomomorphism also. For $S \subseteq \Sigma$, $d \in \mathrm{Res}_M$ or $d \in \mathrm{Res}_M \restriction \Sigma$, let $d(S)$ denote the finite set $\{d(s) \mid s \in S \cap \mathrm{dom}(d)\}$.

Now let $u = u_0 u_1 \dots u_n$ with $u_i \in \Sigma$. We show that $u \in \mathrm{LNF}$ iff for any $0 \leqslant i < j \leqslant n$ the following holds

$$u_j \in \mathrm{res}_{u_i u_{i+1} \dots u_{j-1}}(\Sigma) \Rightarrow \ell(u_i) \prec \ell(u_j). \tag{$\star$}$$

Once we have achieved this, we proceed as follows: since $\mathrm{Res}_M \restriction \Sigma$ is a finite monoid, any language $X_d := \{u \in \Sigma^\star \mid \mathrm{res}_u \restriction \Sigma = d\}$ for $d \in \mathrm{Res}_M \restriction \Sigma$ is recognizable in $\Sigma^\star$. By Kleene's theorem, X_d is rational. Now, by the characterization above, the set of words over Σ that are not in lexicographical normal form equals the rational language

$$\Sigma^\star \setminus \mathrm{LNF} = \bigcup_{\substack{s \in \Sigma \\ d \in \mathrm{Res}_M \restriction \Sigma}} \Sigma^\star \{s\} X_d \; (d \circ \mathrm{res}_s)(\{t \in \Sigma \mid \ell(t) \preceq \ell(s)\}) \Sigma^\star.$$

Hence LNF is recognizable.

It remains to prove the characterization of words in lexicographical normal form. Let $u \in \mathrm{LNF}$ and assume there are i, j with $0 \leqslant i < j \leqslant n$ such that $u_j \in \mathrm{res}_{u_i u_{i+1} \dots u_{j-1}}(\Sigma)$ and $\ell(u_i) \geq \ell(u_j)$. Then there is $t \in \Sigma$ with $u_j = \mathrm{res}_{u_i u_{i+1} \dots u_{j-1}}(t)$. Hence $[u] = [u_0 \dots u_{i-1} t \, \mathrm{res}_t(u_i \dots u_{j-1}) \, u_{j+1} \dots u_n]$. Since $\ell(u_i) \geq \ell(u_j) = \ell(t)$, we have that the label sequence of u is larger than

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

or equal to that of $u_0 \dots u_{i-1} t \, \mathrm{res}_t(u_i \dots u_{j-1}) u_{j+1} \dots u_n$. Since u is in lexicographical normal form, this implies, in particular, $\ell(u_i) = \ell(t)$, contradicting $t \in \mathrm{dom}(\mathrm{res}_{u_i})$. Thus, u satisfies $(\star)$.

Conversely, let the word u satisfy condition $(\star)$. Let $v \in [u]$ with $u \neq v$. We claim that u is lexicographically smaller than v. Note that any suffix of u satisfies $(\star)$. Hence we may assume that the first letter t of v is different from u_0. Then $[t]$ and $[u_0]$ are bounded above by $[u]$. Since they are different irreducible elements in M, their infimum is trivial. Hence $[t] \parallel [u_0]$, implying $\ell(t) \neq \ell(u_0)$. Let j be the least integer such that $\ell(t) \in \ell(u_0 u_1 \dots u_j)$. By Lemma 6.1, $[t]$ and $[u_0 u_1 \dots u_j]$ are not complementary. Since they are bounded by $[u]$, the infimum cannot be 1. Hence $[t] \leqslant [u_0 u_1 \dots u_j]$. Since, on the other hand, the infimum of $[t]$ and $[u_0 u_1 \dots u_{j-1}]$ is trivial, the supremum of these two equals $[u_0 u_1 \dots u_j]$. Hence $u_j = \mathrm{res}_{u_0 u_1 \dots u_{j-1}}(t)$. Since u satisfies $(\star)$, this implies $\ell(u_0) \prec \ell(u_j) = \ell(t)$, and hence our claim. Thus $u \in \mathrm{LNF}$. □

The crucial point in Ochmański's proof of the c-rationality of recognizable languages in trace monoids is that whenever a square of a word w is in lexicographic normal form, w is actually connected. This does not hold any more for labelled divisibility monoids.

Example 6.5. Consider the divisibility monoid from Remark 6.1. We saw that the square word *abab* is in lexicographic normal form. But its root *ab* is not connected as the corresponding element of M is the supremum of a and b.

However, we can show that whenever a product of $|\Gamma| + 2$ words having the same set of labels is in lexicographic normal form, it is connected (*cf.* Corollary 6.7). This will enable us to show that recognizable languages are mc-rational.

For a set $A \subseteq \Gamma$ and $u \in \Sigma^\star$, let $n_A(u)$ denote the number of maximal factors w of u with $\ell(w) \subseteq A$ or $\ell(w) \cap A = \varnothing$. The number $n_A(u)$ is the number of blocks of elements of A and of $\Gamma \setminus A$ in the label sequence of u. For example, let $u = u_1 u_2 \dots u_n$ with $u_i \neq \varepsilon$, $\ell(u_{2i}) \subseteq A$ and $\ell(u_{2i+1}) \subseteq \Gamma \setminus A$ for all suitable i. Then $n = n_A(u) = n_{\Gamma \setminus A}(u)$. Furthermore, we put $n_A(x) := n_A(\mathrm{lexNF}(x))$ for $x \in M$.

Lemma 6.6. Let $(M, \cdot, 1, \ell)$ be a labelled divisibility monoid, $x, y \in M$ and $x \parallel y$. Then $n_{\ell(x)}(x \vee y) \leqslant |\Gamma| + 1$.

Proof. If $n_{\ell(x)}(x \vee y) = 1$, the statement is trivial. So let $n_{\ell(x)}(x \vee y) \geqslant 2$. We may assume that there exist words $u, v \in \Sigma^+$ and $u' \in \Sigma^\star$ with $\ell(u) \subseteq \ell(x) =: A$, $\ell(v) \subseteq \Gamma \setminus A$ and $\mathrm{lexNF}(x \vee y) = uvu'$. Now let a be the first letter of u, and b the first one of v.

First we will show $\ell([ub] \wedge y) = \ell(b)$. Let $h := [ub] \wedge y$. Then there exist uniquely determined $k, l \in M$ with $[ub] = h \cdot k$ and $y = h \cdot l$. By Lemma 3.2, $k \parallel l$. Hence $\ell(k) \cap \ell(l) = \varnothing$ by Lemma 6.1. We write $\#_e h$ for the number of occurrences of the letter $e \in \Gamma$ in the label sequence of any representative of $h \in M$, which is well-defined by Lemma 3.4 and the requirements on ℓ. So we get, on the other hand, $\#_e[ub] = \#_e h + \#_e k$ and $\#_e y = \#_e h + \#_e l$ for any $e \in \Gamma$. Hence $\#_e h = \min(\#_e[ub], \#_e y)$. Note that $\ell(b) \in \ell(y)$. Hence $\ell(b) \in \ell(h)$. Now let $e \in \ell(y) \setminus \ell(b)$. Then $e \notin \ell(x)$ and therefore $\#_e h = 0$. Thus $\ell([ub] \wedge y) = \ell(b)$.

Hence there exists a word $w \in \Sigma^\star$ with $x \vee y = [w]$ such that the label sequence of

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

w starts with $\ell(b)$. Since the label sequence of the lexicographical normal form of $x \vee y$ starts with $\ell(a)$, we get $\ell(a) \prec \ell(b)$.

Since $n_A(x \vee y) = n_{\Gamma \setminus A}(x \vee y)$, we may assume that the label sequence of $\mathrm{lexNF}(x \vee y)$ starts with a letter from A. So let $\mathrm{lexNF}(x \vee y) = u_0 v_0 u_1 v_1 \dots u_n v_n$ with $u_i \neq \varepsilon$ for all $i \leqslant n$, $v_i \neq \varepsilon$ for $i < n$, $\ell(u_i) \subseteq A$ and $\ell(v_i) \subseteq \Gamma \setminus A$. Let a_i (b_i) be the first letter of u_i for $i \leqslant n$ (v_i for $i < n$, respectively). Using Lemma 3.2, we can apply the above result inductively and obtain $\ell(a_i) \prec \ell(b_i) \prec \ell(a_{i+1})$ for each $i < n$. Hence $2n + 1 \leqslant |\Gamma|$. □

Corollary 6.7. Let $X \subseteq \Sigma^\star$ be a monoalphabetic language. Let $w \in X^{|\Gamma|+2} \cap \mathrm{LNF}$. Then $[w]$ is connected.

Proof. Let $n = |\Gamma|+1$. Then there exist $x_i \in [X]$ with $[w] = x_0 x_1 \dots x_n$. Now let $x, y \in M$ with $x \parallel y$ and $x \vee y = [w]$. Then $\ell(x) \cap \ell(y) = \varnothing$ by Lemma 6.1. If $\ell(x_i) \cap \ell(x) \neq \varnothing$ and $\ell(x_i) \cap (\Gamma \setminus \ell(x)) \neq \varnothing$ for all $0 \leqslant i \leqslant n$, we would obtain $n_{\ell(x)}([w]) > n \geqslant |\Gamma| + 1$, contradicting Lemma 6.6. Hence there exists $i \in \{0, 1, \dots, n\}$ such that $\ell(x_i) \subseteq \ell(x)$ or $\ell(x_i) \subseteq \Gamma \setminus \ell(x)$.

First consider the case $\ell(x_i) \subseteq \ell(x)$. Since X is monoalphabetic, this implies $\ell(x_j) = \ell(x_i) \subseteq \ell(x)$ for all $0 \leqslant j \leqslant n$. Now $\ell(y) \subseteq \ell(w) \subseteq \ell(x)$ and $\ell(x) \cap \ell(y) = \varnothing$ imply $\ell(y) = \varnothing$. Hence $y = 1$.

Now consider the case $\ell(x_i) \subseteq \Gamma \setminus \ell(x)$. By Lemma 6.1, $\ell(x) \cup \ell(y) = \ell([w]) \supseteq \ell(x_i)$, implying $\ell(x_i) \subseteq \ell(y)$. Now we can argue as above (with x and y interchanged) and obtain $x = 1$. □

Corollary 6.8. Let $(M, \cdot, 1, \ell)$ be a labelled divisibility monoid. Let $L \subseteq M$ be recognizable. Then L is mc-rational.

Proof. Let $X := \{u \in \Sigma^\star \mid [u] \in L\} \cap \mathrm{LNF}$. Since any $x \in M$ has a unique lexicographical normal form, we have $[X] = L$. Then X is recognizable in $\Sigma^\star$ and therefore rational. By Lemma 2.1, it can be constructed from finite languages in $\Sigma^\star$ by the operations $\cdot$, $\cup$ and $\langle . \rangle$ applied to monoalphabetic languages only. Since $X \subseteq \mathrm{LNF}$, any intermediate language in the construction of X is also contained in LNF. Let Y be such an intermediate language and suppose that the iteration $\langle . \rangle$ is applied to Y. Hence Y is monoalphabetic. Then $\langle Y \rangle$ is another intermediate language and therefore contained in LNF. Hence, by Corollary 6.7, $[Y]^{|\Gamma|+2}$ is connected. Note that $\langle Y \rangle = (\bigcup_{0 \leqslant i \leqslant |\Gamma|+1} Y^i)\ \langle Y^{|\Gamma|+2} \rangle$. Therefore, we can construct $[X] = L$ as required. □

We can summarize our results on recognizable, c-rational and mc-rational languages as follows.

Theorem 6.9. Let $(M, \cdot, 1)$ be a labelled divisibility monoid with finitely many residuum functions. Let $L \subseteq M$. Then the following are equivalent:

1. L is recognizable.
2. L is c-rational.
3. L is mc-rational.

Proof. The implications $2 \to 1 \to 3 \to 2$ are Theorem 5.6, Corollary 6.8 and 6.2, respectively. □

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

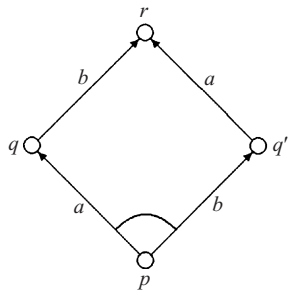
7. Automata with concurrency relations

In this section we outline how to derive the results of Droste (1995) for recognizable languages in concurrency monoids as a consequence of Theorem 6.9. First, we recall the basic definitions on automata with concurrency relations. For more details and explanations, see Droste (1995).

Definition 7.1. A quadruple $\mathscr{A} = (Q, E, T, \|)$ is an *automaton with concurrency relations* provided:

1. Q and E are finite sets of *states* (or situations) and *events* (or actions), respectively.
2. $T \subseteq Q \times E \times Q$ is a set of transitions assumed deterministic, that is, whenever (p, a, q), $(p, a, r) \in T$, we have $q = r$.
3. $\| = (\|_q)_{q \in Q}$ is a collection of irreflexive, symmetric binary relations on E; it is required that whenever $a \|_p b$, there exist transitions (p, a, q), (p, b, q'), (q, b, r) and (q', a, r) in T.

A transition $t = (p, a, q)$ intuitively represents a potential computation step in which event a happens in state p of $\mathscr{A}$ and $\mathscr{A}$ changes from state p to state q. The concurrency relations $\|_p$ describe the concurrency information for pairs of events at state p. The last requirement can be seen in the following diagram:



The angle at p indicates that $a \|_p b$ holds.

Now we want the concurrency relations of $\mathscr{A}$ to induce an equivalence relation on $T^\star$ so that equivalent words are not differentiated by the order in which the concurrent actions appear. For this, we let $\sim$ be the smallest congruence on $T^\star$ making all sequences $(p, a, q)(q, b, r)$ and $(p, b, q')(q', a, r)$ with $a \|_p b$ equivalent. Observe that $\sim$ is an equivalence relation on $T^\star$ such that two equivalent computation sequences have the same length. We let $[u]$ denote the equivalence class of u with respect to $\sim$. Also, we let $1 := [\varepsilon]$. Defining $\mathbb{M}^+(\mathscr{A}) = T^\star/\sim$, we now obtain the *monoid* $\mathbb{M}^+(\mathscr{A})$ *associated with* $\mathscr{A}$. It is easily seen that the irreducible elements of this monoid are precisely the elements from T. We define a labelling function $\ell : T \to E$ on this set by $(p, a, q) \mapsto a$. Then $(\mathbb{M}^+(\mathscr{A}), \ell)$ is a monoid together with a labelling of the irreducible elements. Under some additional conditions on $\mathscr{A}$, this is a labelled divisibility monoid (*cf.* Theorem 7.4). The following example shows that not every labelled divisibility monoid occurs in this way.

Example 7.2. Let $\Sigma = \{a, b, c\}$ and let $\sim$ be the least congruence on $\Sigma^\star$ satisfying $ab \sim bc$ and $ba \sim cb$. Then $M = \Sigma^\star/\sim$ is a divisibility monoid. A labelling function is given by the mapping ℓ with $\ell(b) = 1$ and $\ell(c) = \ell(a) = 2$. Now suppose there is an automaton with

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

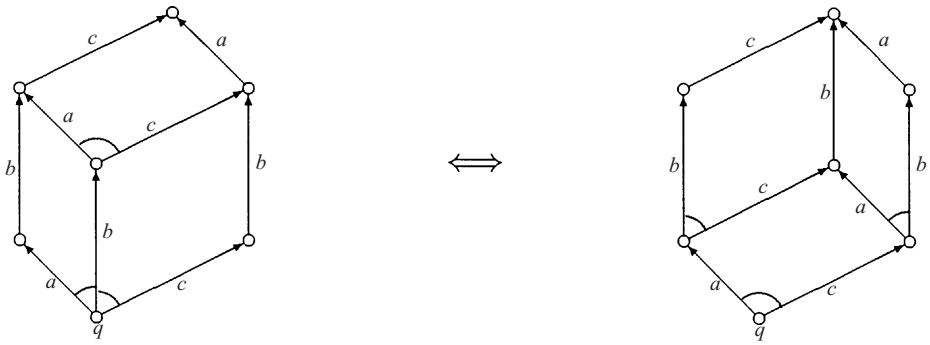
concurreny relations $\mathscr{A}$ such that $\mathbb{M}^+(\mathscr{A}) \cong M$. Then the set Σ can be seen as the set of transitions of $\mathscr{A}$. We try to extract some information on the domains and the codomains of these transitions. The main tool for this is the easy observation that equivalent words over Σ have the same initial state. Since $bc = ab$, the initial states of a and of b have to be equal. Similarly, the initial states of b and of c are equal because of $ba \sim cb$. The equation $bc \sim ab$ in addition implies that the actions occurring in the transitions a and c are the same. Hence the determinism of $\mathscr{A}$ implies $a = c$, a contradiction.

For $a \in E$ and $p \in Q$, let $p.a = q$ if there exists a transition $(p, a, q) \in T$, and $p.a = \perp$ otherwise. This will simplify the notation in the following definition where we also assume $\|_\perp = \varnothing$. Thus, for instance, $a \parallel_{q.b} c$ holds iff there exists a transition $(q, b, r) \in T$ with $a \parallel_r c$.

Definition 7.3. An automaton with concurrency relations $\mathscr{A}$ is called *stably concurrent*, if for all $q \in Q$ and $a, b, c \in E$ the following equivalence holds:

$$a \parallel_q b,\ b \parallel_q c \text{ and } a \parallel_{q.b} c \iff a \parallel_q c,\ b \parallel_{q.a} c \text{ and } a \parallel_{q.c} b.$$

The equivalence in this definition can be depicted as follows:



The requirement of the implication '⇒' has also been called cube axiom, and the implication '⇐' is called the inverse cube axiom.

Theorem 7.4. Let $\mathscr{A}$ be a stably concurrent automaton. Then $(\mathbb{M}^+(\mathscr{A}), \cdot, \ell)$ is a labelled divisibility monoid with finitely many residuum functions.

Cancellation from the left and the existence of infima for any two monoid elements follows from Droste (1992), cancellation from the right has been shown in (Bracho et al. 1997), and the distributivity of the lattice $(\downarrow m, \leqslant)$ was proved in Kuske (1994a) and Kuske (1994b). It is obvious that the monoid $\mathbb{M}^+(\mathscr{A})$ is generated by its irreducible elements T and that this set is finite. Hence the monoid is a divisibility monoid (alternatively, one can use Theorem 3.5 to show this). It has only finitely many residuum functions by Droste (1995). The monoid is also labelled by Droste (1992). Now it is immediate by Theorem 6.9 that recognizable, c-rational and mc-rational languages coincide in $\mathbb{M}^+(\mathscr{A})$.

Corollary 7.5. Let $\mathscr{A}$ be a stably concurrent automaton and let $L \subseteq \mathbb{M}^+(\mathscr{A})$. Then L is recognizable iff it is c-rational iff it is mc-rational.

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

In Droste (1995), a similar equivalence between recognizable and c-rational languages has been shown. But there, the languages are in another monoid, which we will introduce next.

Note that

$$I = \mathbb{M}^+(\mathscr{A}) \cdot \{[(p,a,q)(q',b,r)] \mid (p,a,q),(q',b,r) \in T \text{ and } q \neq q'\} \cdot \mathbb{M}^+(\mathscr{A})$$

is a two-sided ideal in the monoid $\mathbb{M}^+(\mathscr{A})$. Let $\mathbb{M}(\mathscr{A})$ denote the Rees-quotient of $\mathbb{M}^+(\mathscr{A})$ with respect to this ideal and let $\mu : \mathbb{M}^+(\mathscr{A}) \to \mathbb{M}(\mathscr{A})$ denote the canonical epimorphism associated with this quotient. Then $\mathbb{M}(\mathscr{A})$ is (isomorphic to) the monoid of computations of $\mathscr{A}$ considered, for example, in Droste (1995). This latter monoid arises by factoring the set of computation sequences of $\mathscr{A}$ by the equivalence relation $\sim$ introduced above for $T^\star$; we take concatenation of computation sequences as a partial product operation and introduce a zero in order to have this product defined everywhere.

Let $\mathscr{A}$ be stably concurrent and $L \subseteq \mathbb{M}(\mathscr{A})$. The set of c-rational languages in $\mathbb{M}(\mathscr{A})$ is defined similarly to those in a divisibility monoid as follows.

The class of *c-rational languages* in $\mathbb{M}(\mathscr{A})$ is the smallest class $\mathscr{C}$ satisfying:

1. any finite subset of M is in $\mathscr{C}$;
2. whenever $L, K \in \mathscr{C}$ then $L \cup K \in \mathscr{C}$ and $L \cdot K \in \mathscr{C}$; and
3. $\langle L \rangle \in \mathscr{C}$ provided $L \in \mathscr{C}$ is connected and $0 \notin L \cdot L$.

Note the difference between the definition of c-rational languages in a divisibility monoid and in $\mathbb{M}(\mathscr{A})$: the restrictions that apply to the operator $\langle . \rangle$ differ. One can show using Droste (1992) that $0 \notin L \cdot L$ implies that $\mu^{-1}(L) \subseteq \mathbb{M}^+(\mathscr{A})$ is residually closed. Therefore, a language $\mu^{-1}(L)$ is c-rational in $\mathbb{M}^+(\mathscr{A})$ whenever $L \subseteq \mathbb{M}(\mathscr{A})$ is c-rational in $\mathbb{M}(\mathscr{A})$.

Let $L \subseteq \mathbb{M}(\mathscr{A})$ be c-rational. Then $\mu^{-1}(L) \subseteq \mathbb{M}^+(\mathscr{A})$ is c-rational in the divisibility monoid. Hence it is recognizable. Since the monoid morphism μ is surjective, this implies that L is recognizable.

Now let $L \subseteq \mathbb{M}(\mathscr{A})$ be recognizable in $\mathbb{M}(\mathscr{A})$. Then it is easy to see that $L' = L \setminus \{0\}$ is recognizable. Hence the preimage $K := \mu^{-1}(L') \subseteq \mathbb{M}^+(\mathscr{A})$ is recognizable and therefore c-rational. In addition, $K \cap I = \varnothing$ since $0 \notin L'$. Therefore, in the c-rational construction of K, the operator $\langle . \rangle$ is applied to languages R such that (1) any $x \in R$ is connected and (2) $x \cdot y \notin I$ for any $x, y \in R$. Hence this c-rational construction is legal in $\mathbb{M}(\mathscr{A})$ also. Therefore, $\mu(\mu^{-1}(L'))$ is c-rational in $\mathbb{M}(\mathscr{A})$. Since this equals L' and since $\{0\}$ is c-rational, we showed that L is c-rational in $\mathbb{M}(\mathscr{A})$.

Corollary 7.6. Let $\mathscr{A}$ be a stably concurrent automaton and let $L \subseteq \mathbb{M}(\mathscr{A})$. Then L is recognizable iff it is c-rational.

This strengthens Droste (1995, Theorem 2), which needed an additional assumption on $\mathscr{A}$ in order to obtain that all recognizable languages in $\mathbb{M}(\mathscr{A})$ are c-rational.

8. Open problems

In Sakarovitch (1987), is was shown that in rational monoids recognizable sets are precisely the rational ones. Thus, he generalized Kleene's Theorem to rational monoids.

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

Another generalization of Kleene's Theorem to trace monoids is Ochmański's Theorem on recognizable and c-rational sets. The intersection of the trace and the rational monoids are the classically known free monoids, that is, these two generalizations of Kleene's Theorem are 'orthogonal'. Here, we have generalized Ochmański's result even further to divisibility monoids. This extension is not 'orthogonal' to Sakarovitch's approach any more: for instance $\{a, b, c\}^\star / \langle ab = bc \rangle$ is both, a rational monoid and a divisibility monoid, but not a trace monoid. Furthermore, in Kuske (2000), it is shown that a divisibility monoid is rational iff it satisfies Kleene's Theorem. Still, the classes of rational and of divisibility monoids are incomparable. So a natural question remains open whether one can find a common generalization of Sakarovitch's and Ochmański's results. This work is currently in progress.

Another question is whether our results can be derived from Ochmański's for trace languages. Clearly, this cannot get a definite negative answer since the term 'can be derived' is too imprecise. The only answer we have so far is that we were not able to achieve such a connection.

Also, it remains open at present whether any divisibility monoid has finitely many residuum functions.

References

Berry, G. (1978) Stable models of typed λ-calculi. In: 5th ICALP. *Springer-Verlag Lecture Notes in Computer Science* **62** 72–89.

Birkhoff, G. (1940) *Lattice Theory*. Colloquium Publications **25**, American Mathematical Society, Providence. (The numbers in citations refer to the third edition, seventh printing from 1993.)

Bracho, F., Droste, M. and Kuske, D. (1997) Representation of computations in concurrent automata by dependence orders. *Theoretical Computer Science* **174** 67–96.

Cameron, P. J. (1994) *Combinatorics*, Cambridge University Press.

Cartier, P. and Foata, D. (1969) Problemes combinatoires de commutation et rearrangements. *Springer-Verlag Lecture Notes in Mathematics* **85**.

Choffrut, C. (1995) Combinatorics on trace monoids I. In: Diekert, V. and Rozenberg, G. *The Book of Traces*, World Scientific Publ. Co., Chapter 3.

Cori, R. and Métivier, Y. (1985) Recognizable subsets of some partially abelian monoids. *Theoretical Computer Science* **35** 241–254.

Cori, P. and Perrin, D. (1985) Automates et commutations partielles. *R.A.I.R.O. - Informatique Théorique et Applications* **19** 21–32.

Diekert, V. and Métivier, Y. (1997) Partial commutation and traces. In: Rozenberg, G. and Salomaa, A. (eds.) *Handbook of Formal Languages*, Volume 3, Springer 457–533.

Diekert, V. and Rozenberg, G. (1995) *The Book of Traces*, World Scientific Publ. Co.

Droste, M. (1992) Concurrent automata and domains. *International Journal of Foundations of Computer Science* **3** 389–418.

Droste, M. (1995) Recognizable languages in concurrency monoids. *Theoretical Computer Science* **150** 77–109.

Droste, M. and Kuske, D. (1998) Recognizable and logically definable languages of infinite computations in concurrent automata. *International Journal of Foundations of Computer Science* **9** 295–313.

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press

Droste, M. and Kuske, D. (1999) On recognizable languages in divisibility monoids. In: Ciobanu, G. and Paun, Gh. (eds.) FCT99. *Springer-Verlag Lecture Notes in Computer Science* **1684** 246–257.

Eilenberg, S. (1974) *Automata, Languages and Machines*, Volume A, Academic Press, New York.

GAP Group, Aachen, St Andrews (1999) *GAP – Groups, Algorithms, and Programming, Version 4.2*, `http://www-gap.dcs.st-and.ac.uk/~gap`.

Godefroid, P. and Pirottin, D. (1993) Refining dependencies improves partial-order verification methods. In: 5th Conf. on Computer Aided Verification. *Springer-Verlag Lecture Notes in Computer Science* **697** 438–449.

Hashigushi, K. (1991) Recognizable closures and submonoids of free partially commutative monoids. *Theoretical Computer Science* **86** 233–241.

Katz, S. and Peled, D. (1992) Defining conditional independence using collapses. *Theoretical Computer Science* **101** 337–359.

Kuske, D. (1994a) *Modelle nebenläufiger Prozesse – Monoide, Residuensysteme und Automaten*, Ph. D. thesis, Universität GHS Essen.

Kuske, D. (1994b) Nondeterministic automata with concurrency relations. In: Colloquium on Trees in Algebra and Programming. *Springer-Verlag Lecture Notes in Computer Science* **787** 202–217.

Kuske, D. (2000) *Contributions to a Trace Theory beyond Mazurkiewicz Traces*, Habilitationsschrift, TU Dresden.

Métivier, Y. (1986) On recognizable subsets of free partially commutative monoids. In: ICALP'86. *Springer-Verlag Lecture Notes in Computer Science* 254–264.

Ochmański, E. (1985) Regular behaviour of concurrent systems. *Bull. Europ. Assoc. for Theor. Comp. Science* **27** 56–67.

Panangaden, P. and Stark, E. W. (1988) Computations, residuals and the power of indeterminacy. In: Automata, Languages and Programming. *Springer-Verlag Lecture Notes in Computer Science* **317** 439–454.

Ramsey, F. P. (1930) On a problem of formal logic. *Proc. London Math. Soc.* **30** 264–286.

Sakarovitch, J. (1987) Easy multiplications. I. The realm of Kleene's Theorem. *Information and Computation* **74** 173–197.

Stark, E. W. (1989) Concurrent transition systems. *Theoretical Computer Science* **64** 221–269.

Winskel, G. (1987) Event structures. In: Brauer, W., Reisig, W. and Rozenberg, G. (eds.) Petri nets: Applications and Relationships to Other Models of Concurrency. *Springer-Verlag Lecture Notes in Computer Science* **255** 325–392.

Zielonka, W. (1987) Notes on finite asynchronous automata. *R.A.I.R.O. - Informatique Théorique et Applications* **21** 99–135.

https://doi.org/10.1017/S0960129501003395 Published online by Cambridge University Press