ON SQUARE-INCREASING ORDERED MONOIDS AND IDEMPOTENT SEMIRINGS

ROSTISLAV HORČÍK

Abstract. Let $\mathcal{V}$ be the variety of square-increasing idempotent semirings. Its members can be viewed as semilattice-ordered monoids satisfying $x \leq x^2$. We show that the universal theory of $\mathcal{V}$ is decidable. In order to prove this result, we investigate the class $\mathcal{Q}$ whose members are ordered-monoid subreducts of members from $\mathcal{V}$. In particular, we prove that finitely generated members from $\mathcal{Q}$ are well-partial-ordered and residually finite.

1. Introduction

Semirings are algebraic structures generalizing the concept of a ring by allowing the additive substructure to be only a commutative semigroup instead of an abelian group. They occur in various branches of computer science and mathematics. Let us mention for instance the theory of weighted automata and rational power series [1] or the role of idempotent semirings in tropical geometry [15]. For the purpose of this paper, the term *semiring* refers to an algebra $\mathbf{A} = \langle A, +, \cdot, 1\rangle$ where $\langle A, +\rangle$ is a commutative semigroup, $\langle A, \cdot, 1\rangle$ a monoid, and multiplication distributes over addition on both sides. A semiring $\mathbf{A}$ is said to be *idempotent* if the identity $x = x + x$ holds in $\mathbf{A}$. In that case, the additive substructure of $\mathbf{A}$ forms a semilattice and one can define a partial order on A by setting $a \leq b$ iff $a = a + b$.

This paper deals with the variety $\mathcal{V}$ of idempotent semirings satisfying in addition the identity $x = x + x^2$. We call its members *square-increasing* because the identity $x = x + x^2$ is equivalent to $x \leq x^2$. As the main result, we prove in Section 6 that the universal theory of $\mathcal{V}$ is decidable by showing that a universal formula failing in $\mathcal{V}$ also fails in a finite member of $\mathcal{V}$. In order to achieve this, we investigate the structure of ordered monoids which are embeddable in a member of $\mathcal{V}$. Let us denote the class of such ordered monoids by $\mathcal{Q}$. Members of $\mathcal{Q}$ clearly satisfy the inequality $x \leq x^2$. Nevertheless, not every square-increasing ordered monoid belongs to $\mathcal{Q}$. The class $\mathcal{Q}$ can be axiomatized (as is shown in Section 6) by the following universally quantified Horn formula:

$$z \leq uxv \;\&\; z \leq uyv \implies z \leq uxyv\,. \tag{1}$$

The shape of the above formula comes from the fact that in idempotent semirings the inequality $x \leq x^2$ is equivalent to $x+y \leq xy$, which in turn by distributivity implies $uxv+uyv \leq uxyv$.

Given a finite set Σ and a Σ-generated ordered monoid $\mathbf{M} \in \mathcal{Q}$, one can introduce a compatible quasi-order $\preceq$ on the free monoid Σ^* by setting $x \preceq y$ iff $h(x) \leq h(y)$, where $h\colon \Sigma^* \to M$ is the canonical quotient homomorphism. We prove in Section 5 that this quasi-order satisfies the following conditional inequality

$$\mathsf{c}(y) \subseteq \mathsf{c}(x) \implies x \preceq xyx\,, \tag{2}$$

where $\mathsf{c}(x) \subseteq \Sigma$ denotes the set of letters occurring in x (the so-called content of x). The proof of decidability for the universal theory of $\mathcal{V}$ relies on the fact that finitely generated

members of $\mathcal{Q}$ are well-partially-ordered and thus residually finite. To prove this, we present a modification of Higman's lemma (Section 3), which allows us to prove that every compatible quasi-order $\preceq$ on the free monoid Σ^* satisfying the conditional inequality (2) is well (Section 4).

2. Ordered monoids

Throughout the paper Σ always denotes a finite set called the *alphabet* whose elements are called *letters*. The set of all finite sequences (*words*) of elements from Σ is denoted Σ^*. The symbol ε stands for the empty word. The set of nonempty words $\Sigma^* \setminus \{\varepsilon\}$ is denoted Σ^+. Given a word $w \in \Sigma^*$, a word $u \in \Sigma^*$ is called *prefix* of w if $w = uv$ for some $v \in \Sigma^*$. The set of all letters occurring in w is denoted $\mathsf{c}(w)$.

A *quasi-ordered* set (*qoset* for short) $\mathbf{Q} = \langle Q, \preceq \rangle$ is a set endowed with a reflexive transitive binary relation $\preceq$ on Q. The relation $\preceq$ is called a *quasi-order*. If $\preceq$ is antisymmetric then we call it a *partial order*. Given any subset $P \subseteq Q$, one can restrict $\preceq$ on P and define a qoset $\mathbf{P} = \langle P, \preceq \rangle$. We slightly abuse notation here and denote the restriction of $\preceq$ on P by the same symbol $\preceq$. The qoset $\mathbf{P}$ is called a *subqoset* of $\mathbf{Q}$. Let $\langle Q_1, \preceq_1 \rangle$, $\langle Q_2, \preceq_2 \rangle$ be qosets and $f \colon Q_1 \to Q_2$ a map. Then f is called *monotone* if $x \preceq_1 y$ implies $f(x) \preceq_2 f(y)$ for all $x, y \in Q_1$. Let $\mathbf{Q} = \langle Q, \preceq \rangle$ be a qoset. A subset $U \subseteq Q$ is said to be an *upset* if it is upward closed, i.e., $x \in U$ and $x \preceq y$ implies $y \in U$. The upset generated by a subset $S \subseteq Q$ is denoted $\uparrow S$. We write $\uparrow x$ instead of $\uparrow\{x\}$.

Let $\mathbf{A} = \langle A, \cdot, 1 \rangle$ be a monoid and $\preceq$ a quasi-order on A. We say that $\preceq$ is *compatible* if $x \preceq y$ implies $ux \preceq uy$ and $xu \preceq yu$ for all $x, y, u \in A$. An *ordered monoid* is a structure $\mathbf{A} = \langle A, \cdot, 1, \leq \rangle$ such that $\langle A, \cdot, 1 \rangle$ is a monoid and $\leq$ is a compatible partial order. Note that any monoid can be viewed as an ordered monoid if we order it discretely. In particular, the free monoid Σ^* can be viewed as an ordered monoid $\langle \Sigma^*, \cdot, \varepsilon, = \rangle$. If $\mathbf{A} = \langle A, \cdot, 1, \leq \rangle$ is an ordered monoid then the order-theoretic dual $\mathbf{A}^\partial = \langle A, \cdot, 1, \geq \rangle$ is an ordered monoid as well.

Homomorphisms of ordered monoids are monotone monoid homomorphisms. Let $\mathbf{A}$ and $\mathbf{B}$ be ordered monoids. A homomorphism $h \colon A \to B$ is said to be an *embedding* if for all $x, y \in A$ we have $x \leq y$ iff $h(x) \leq h(y)$.

Let $\mathbf{A}$ be an ordered monoid. A *subalgebra* $\mathbf{B}$ of $\mathbf{A}$ is a submonoid ordered with the restricted order from $\mathbf{A}$. Given an indexed system of ordered monoids $\langle \mathbf{A}_i \mid i \in I \rangle$, we can form the *direct product* $\prod_{i \in I} \mathbf{A}_i$ whose monoid reduct is just the direct product of monoids and it is ordered component-wise, i.e., $\langle a_i \mid i \in I \rangle \leq \langle b_i \mid i \in I \rangle$ if for all $i \in I$ we have $a_i \leq b_i$ in $\mathbf{A}_i$.

A *congruence of an ordered monoid* $\mathbf{A} = \langle A, \cdot, 1, \leq \rangle$ is a compatible quasi-order $\preceq$ on A containing $\leq$ (see [4, 14]). Given a compatible quasi-order $\preceq$, one can define a monoid congruence $\sim$ on $\mathbf{A}$ for $x, y \in A$ as follows:

$$x \sim y \quad \text{iff} \quad x \preceq y \text{ and } y \preceq x \,.$$

The equivalence class of $x \in A$ with respect to $\sim$ is denoted $[x]_\sim$. We define the *quotient ordered monoid* as $\mathbf{A}/{\preceq} = \langle \hat{\mathbf{A}}/{\sim}, \leq \rangle$, where $\hat{\mathbf{A}} = \langle A, \cdot, 1 \rangle$ is the monoid reduct of $\mathbf{A}$ and $[x]_\sim \leq [y]_\sim$ iff $x \preceq y$. In this case the canonical surjective homomorphism $h \colon A \to A/{\sim}$ mapping x to $[x]_\sim$ is monotone.

Let Σ be an alphabet and $u_0, \ldots, u_n, v_0, \ldots, v_n \in \Sigma^*$. A *quasi-inequality* is a universally quantified Horn formula of the following form:

$$u_1 \leq v_1 \;\&\; \ldots \;\&\; u_n \leq v_n \quad \Longrightarrow \quad u_0 \leq v_0 \,. \tag{3}$$

The quasi-inequality (3) is said to hold in an ordered monoid $\mathbf{A}$ if for every homomorphism $h\colon \Sigma^* \to A$ we have $h(u_0) \leq h(v_0)$ whenever $h(u_i) \leq h(v_i)$ for all $i = 1, \ldots, n$. It is known that classes of ordered monoids axiomatized by quasi-inequalities are closed under forming direct products, subalgebras and contains free algebras (see [4, 13]).

3. Well-quasi-orders

In this section we recall several facts on well-quasi-orders. In [11] Higman gave several definitions of a well-quasi-order and proved that they are all equivalent.

DEFINITION 3.1. *Let $\preceq$ be a quasi-order on a set Q. Then the qoset $\langle Q, \preceq\rangle$ is called a* well-quasi-order *(abbreviation: wqo) if any of the following conditions holds:*

1. *Q contains neither infinite strictly decreasing chains nor infinite antichains,*
2. *for each infinite sequence $\langle x_i \mid i \in \mathbb{N}\rangle$ of elements from Q, there exist $i < j$ such that $x_i \preceq x_j$,*
3. *each infinite sequence of elements from Q contains an infinite increasing subsequence,*
4. *every upset of Q is finitely generated,*
5. *every sequence of upsets of Q which is strictly increasing under inclusion is finite.*

An antisymmetric well-quasi-order is called a well-partial-order.

We recall several constructions preserving wqos which will be useful in the sequel (for proofs see e.g. [16, 6]).

LEMMA 3.2. *Let $\langle Q, \preceq\rangle$ be a wqo. Then the following hold:*

1. *$\langle Q, \preceq'\rangle$ is a wqo for every extension $\preceq \subseteq \preceq'$.*
2. *Every subqoset of $\langle Q, \preceq\rangle$ is a wqo.*
3. *If $\langle Q', \preceq'\rangle$ is a wqo then $\langle Q \times Q', \preceq \times \preceq'\rangle$ is a wqo as well.*
4. *Let $\langle Q', \preceq'\rangle$ be a qoset and $f\colon Q \to Q'$ a monotone surjection. Then $\langle Q', \preceq'\rangle$ is also a wqo.*
5. *Let $\langle Q', \preceq'\rangle$ be a wqo and $\preceq''$ a quasi-order on $Q \cup Q'$ containing $\preceq \cup \preceq'$. Then $\langle Q \cup Q', \preceq''\rangle$ is a wqo.*

The following result [11] known as Higman's lemma shows that given a wqo $\langle Q, \preceq\rangle$, one can extend $\preceq$ to Q^* so that this extension remains a wqo. Given two natural numbers m, n such that $m < n$, we define $[m, n] = \{m, m+1, \ldots, n\}$.

DEFINITION 3.3. *Let $\langle Q, \preceq\rangle$ be a qoset. We define a quasi-order $\preceq_H$ on Q^* as follows:*

> *$x_1 \ldots x_k \preceq_H y_1 \ldots y_l$ iff there is a strictly monotone map $f\colon [1, k] \to [1, l]$ such that $x_i \preceq y_{f(i)}$ for all $i \in [1, k]$.*

LEMMA 3.4. *If $\langle Q, \preceq\rangle$ is a wqo then $\langle Q^*, \preceq_H\rangle$ is a wqo.*

We will need a slight modification of the above result. Namely, we further restrict the map f from Definition 3.3.

DEFINITION 3.5. *Let $\langle Q, \preceq\rangle$ be a quasi-order. We define a quasi-order $\sqsubseteq$ on Q^+ as follows:*

> *$x_1 \ldots x_k \sqsubseteq y_1 \ldots y_l$ iff there is a strictly monotone map $f\colon [1, k] \to [1, l]$ such that*
> - *$f(1) = 1$ and $f(k) = l$,*
> - *$x_i \preceq y_{f(i)}$ for all $i \in [1, k]$.*

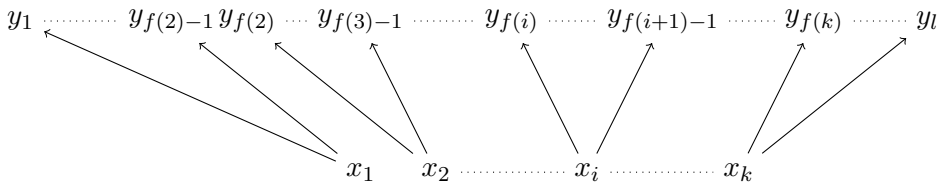

FIGURE 1. The definition of $\leq^+$.

LEMMA 3.6. *If $\langle Q, \preceq\rangle$ is a wqo then $\langle Q^+, \sqsubseteq\rangle$ is a wqo.*

Proof. It is easy to see that $\sqsubseteq$ is reflexive and transitive. Further, observe that Q^+ can be viewed as a union of the set of 1-element sequences and the set of sequences having at least two elements. The set of 1-element sequences can be identified with Q. Moreover, the restriction of $\sqsubseteq$ on Q is just $\preceq$. The set of sequences having at least two elements can be identified with $Q \times Q^* \times Q$. The restriction of $\sqsubseteq$ on $Q \times Q^* \times Q$ is $\preceq \times \preceq_H \times \preceq$ which is wqo by Lemma 3.4 and Lemma 3.2(3). Consequently, the lemma follows by Lemma 3.2(5). □

Concerning well-quasi-orders, we will also need the Generalized Myhill-Nerode Theorem due to Ehrenfeucht, Haussler and Rozenberg [7]. It characterizes regular languages as upsets with respect to a compatible wqo.

THEOREM 3.7. *Let $L \subseteq \Sigma^*$ be a language. Then L is regular if and only if L forms an upset with respect to some compatible well-quasi-order on Σ^*.*

4. Main combinatorial result

In this section we are going to prove the main combinatorial result. It is a certain modification of Higman's lemma together with its consequences. In particular, we will show that every compatible quasi-order $\preceq$ on Σ^* satisfying (2) is well.

We start with a definition how to extend a quasi-order on a set Q to Q^+ similarly as in Definitions 3.3 and 3.5 reflecting the structure of (2).

DEFINITION 4.1. *Let $\langle Q, \leq\rangle$ be a qoset. We define a quasi-order $\leq^+$ on Q^+ by letting $x_1 \dots x_k \leq^+ y_1 \dots y_l$ iff there is a strictly monotone map $f\colon [1, k+1] \to [1, l+1]$ such that*

- *$f(1) = 1$ and $f(k+1) = l+1$,*
- *$x_i \leq y_{f(i)}$ and $x_i \leq y_{f(i+1)-1}$ for all $i \in [1, k]$.*

Then $\leq^*$ denotes the extension of $\leq^+$ on Q^* defined by $\leq^* = \leq^+ \cup \{\langle \varepsilon, \varepsilon\rangle\}$.

The above definition is illustrated in Figure 1. As a particular example consider the set $[0, 9]$ ordered in the usual way. Then we have for instance $10354 \leq^+ 27041256154$ (see Figure 2).

LEMMA 4.2. *Let $\langle Q, \leq\rangle$ be a qoset. Then $\langle Q^+, \leq^+\rangle$ and $\langle Q^*, \leq^*\rangle$ are qosets.*

Proof. We have to show that $\leq^+$ is reflexive and transitive. To see reflexivity, consider a sequence $x_1 \dots x_k \in Q^+$. Observe that the identity map $id\colon [1, k+1] \to [1, k+1]$ satisfies all the conditions from Definition 4.1. Further assume that $x_1 \dots x_k \leq^+ y_1 \dots y_l$ and $y_1 \dots y_l \leq^+ z_1 \dots z_m$. Then there are two strictly monotone maps $f\colon [1, k+1] \to [1, l+1]$ and $g\colon [1, l+1] \to [1, m+1]$ satisfying all the conditions of Definition 4.1. We check that their composition $g \circ f$

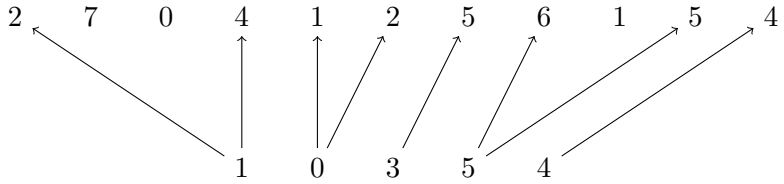

FIGURE 2. An example showing that $10354 \leq^+ 27041256154$ in $[0,9]^+$ where $[0,9]$ is ordered in the usual way.

satisfies all the conditions as well. Clearly, $g \circ f$ is strictly monotone, $g(f(1)) = 1$ and $g(f(k+1)) = m+1$. Further for every $i \in [1,k]$ we have $x_i \leq y_{f(i)} \leq z_{g(f(i))}$ and

$$x_i \leq y_{f(i+1)-1} \leq z_{g(f(i+1)-1+1)-1} = z_{g(f(i+1))-1}\,.$$

Thus $x_1 \dots x_k \leq^+ z_1 \dots z_m$ and consequently $\langle Q^+, \leq^+ \rangle$ is a qoset. Finally, $\langle Q^*, \leq^* \rangle$ is obtained by extending $\langle Q^+, \leq^+ \rangle$ with a single element which is related to itself and unrelated to all other remaining elements in Q^+. Thus it follows that $\leq^*$ is also reflexive and transitive. □

LEMMA 4.3. *If $\mathbf{Q} = \langle Q, \leq \rangle$ is a wqo then $\mathbf{Q}^+ = \langle Q^+, \leq^+ \rangle$ and $\langle Q^*, \leq^* \rangle$ are wqos.*

Proof. Since wqos are closed under finite direct products by Lemma 3.2(3), $\mathbf{Q} \times \mathbf{Q}$ forms a wqo as well. Thus also $\langle (Q \times Q)^+, \sqsubseteq \rangle$ is a wqo by Lemma 3.6. Consider its subqoset $\mathbf{P} = \langle P, \sqsubseteq \rangle$ containing sequences from $(Q \times Q)^+$ of the following form for $k \geq 1$ and $a_0, \dots, a_{k+1} \in Q$:

$$\langle a_0, a_1 \rangle \langle a_1, a_2 \rangle \langle a_2, a_3 \rangle \dots \langle a_{k-1}, a_k \rangle \langle a_k, a_{k+1} \rangle\,.$$

Then $\mathbf{P}$ is also a wqo since wqos are closed under taking subqosets by Lemma 3.2(2). We will show that there is a monotone surjection ψ from $\mathbf{P}$ onto $\mathbf{Q}^+$. Define

$$\psi(\langle a_0, a_1 \rangle \langle a_1, a_2 \rangle \langle a_2, a_3 \rangle \dots \langle a_{k-1}, a_k \rangle \langle a_k, a_{k+1} \rangle) = a_1 a_2 \dots a_{k-1} a_k\,.$$

The map ψ is clearly onto. We check that ψ is monotone. Assume that $p_1 \dots p_{k+1}, q_1 \dots q_{l+1} \in P$ such that $p_1 \dots p_{k+1} \sqsubseteq q_1 \dots q_{l+1}$. By definition of $\mathbf{P}$ there are $a_0, \dots, a_{k+1} \in Q$ such that $p_i = \langle a_{i-1}, a_i \rangle$ for all $i \in [1, k+1]$. Similarly, there are $b_0, \dots, b_{l+1} \in Q$ such that $q_i = \langle b_{i-1}, b_i \rangle$ for all $i \in [1, l+1]$. By Definition 3.5 there is a strictly monotone $f\colon [1, k+1] \to [1, l+1]$ such that $f(1) = 1$, $f(k+1) = l+1$ and $p_i \leq q_{f(i)}$ for all $i \in [1, k+1]$. More precisely, we have for all $i \in [1, k+1]$ the following inequality

$$\langle a_{i-1}, a_i \rangle = p_i \leq q_{f(i)} = \langle b_{f(i)-1}, b_{f(i)} \rangle\,.$$

Thus $a_{i-1} \leq b_{f(i)-1}$ and $a_i \leq b_{f(i)}$ for all $i \in [1, k+1]$. Further, substituting $i+1$ for i in $a_{i-1} \leq b_{f(i)-1}$ we get $a_i \leq b_{f(i+1)-1}$ for all $i \in [0, k]$. All together, f satisfies all conditions from Definition 4.1. Namely, we have $a_i \leq b_{f(i)}$ and $a_i \leq b_{f(i+1)-1}$ for all $i \in [1, k]$. Thus ψ is monotone. Since wqos are closed under images of monotone surjections by Lemma 3.2(4), $\mathbf{Q}^+$ is a wqo. It follows immediately from Lemma 3.2(5) that also $\langle Q^*, \leq^* \rangle$ is a wqo because $Q^* = Q^+ \cup \{\varepsilon\}$ and $\leq^* = \leq^+ \cup \{\langle \varepsilon, \varepsilon \rangle\}$. □

Now we will employ Lemma 4.3 in order to show that every compatible quasi-order $\preceq$ on Σ^* satisfying (2) is well. There is a least compatible quasi-order $\leq_\ell$ on Σ^* satisfying (2). It can be described as the reflexive transitive closure of the relation R defined as follows:

$$w \; R \; w' \text{ iff } w = uxv,\ w' = uxyxv \text{ and } \mathsf{c}(y) \subseteq \mathsf{c}(x) \text{ for some } u, v, x, y \in \Sigma^*.$$

LEMMA 4.4. *If $w \leq_\ell w'$ then $\mathsf{c}(w) = \mathsf{c}(w')$.*

Proof. Recall that $\leq_\ell$ is the reflexive transitive closure of R. If $w = w'$ then obviously $\mathsf{c}(w) = \mathsf{c}(w')$. Otherwise we have $w = w_0\ R\ w_1 \dots\ R\ w_k = w'$ for some $w_i \in \Sigma^*$. Since $w_i\ R\ w_{i+1}$ implies $\mathsf{c}(w_i) = \mathsf{c}(w_{i+1})$, the claim follows by induction on k. □

LEMMA 4.5. *If* $|\Sigma| = 1$ *then* $\leq_\ell$ *is a wqo.*

Proof. Let $a \in \Sigma$. We have $R = \{\langle a^k, a^n\rangle \mid 1 \leq k \leq n\} \cup \{\langle \varepsilon, \varepsilon\rangle\}$, which is already reflexive and transitive. Thus $\leq_\ell$ equals just R and is clearly a wqo. □

Assume that $|\Sigma| = n \geq 2$. Then we can partition Σ^* as follows:

$$\Sigma^* = \bigcup_{i=0}^{n} \Sigma_i\,,\ \text{where } \Sigma_i = \{w \in \Sigma^* \mid |\mathsf{c}(w)| = i\}\,.$$

Note that Σ_n are the words w such that $\mathsf{c}(w) = \Sigma$. Further, we denote

$$\Sigma_{<n} = \Sigma^* \setminus \Sigma_n = \bigcup_{i=0}^{n-1} \Sigma_i\,.$$

Let $w \in \Sigma^*$. Consider the longest prefix u of w such that $u \in \Sigma_{<n}$. If $u \neq w$ then $u \in \Sigma_{n-1}$ is followed by a letter $a \in \Sigma$ so that $ua \in \Sigma_n$. Moreover, the letter a is uniquely determined by u and Σ. Namely, there is a map $\sigma\colon \Sigma_{n-1} \to \Sigma$ defined uniquely by $\sigma(u) \in \Sigma \setminus \mathsf{c}(u)$. One can show by induction that $w \in \Sigma^*$ can be uniquely factored as

$$w = u_1\sigma(u_1) \dots u_k\sigma(u_k)z\,,$$

where $u_i \in \Sigma_{n-1}$, $u_i\sigma(u_i) \in \Sigma_n$ and $z \in \Sigma_{<n}$. Note that $k = 0$ iff $\mathsf{c}(w) \neq \Sigma$. Hence the word w can be viewed as a finite (possibly empty) sequence of words from Σ_{n-1} followed by a word $z \in \Sigma_{<n}$ which does not contain all the letters from Σ. Namely, there is a bijection $\varphi\colon (\Sigma_{n-1})^* \times \Sigma_{<n} \to \Sigma^*$ given by

$$\varphi(u_1 \dots u_k, z) = u_1\sigma(u_1) \dots u_k\sigma(u_k)z\,.$$

Now suppose that we have the least compatible quasi-order $\leq_\ell$ on Σ^* satisfying (2). This quasi-order also restricts to subqosets Σ_{n-1} and $\Sigma_{<n}$. Using Definition 4.1, we can define a quasi-order $\leq_\ell{}^*$ on $(\Sigma_{n-1})^*$. Then the above bijection φ becomes monotone.

LEMMA 4.6. *The map* $\varphi\colon \langle(\Sigma_{n-1})^*, \leq_\ell{}^*\rangle \times \langle\Sigma_{<n}, \leq_\ell\rangle \to \langle\Sigma^*, \leq_\ell\rangle$ *is monotone.*

Proof. Let $\langle u_1 \dots u_k, z\rangle, \langle v_1 \dots v_l, w\rangle \in (\Sigma_{n-1})^* \times \Sigma_{<n}$ such that $u_1 \dots u_k \leq_\ell{}^* v_1 \dots v_l$ and $z \leq_\ell w$. We have to show that

$$u_1\sigma(u_1) \dots u_k\sigma(u_k)z \leq_\ell v_1\sigma(v_1) \dots v_l\sigma(v_l)w\,.$$

Since $\leq_\ell$ is compatible, it suffices to prove that

$$u_1\sigma(u_1) \dots u_k\sigma(u_k) \leq_\ell v_1\sigma(v_1) \dots v_l\sigma(v_l)\,.$$

Notice that $u_1 \dots u_k = \varepsilon$ iff $v_1 \dots v_l = \varepsilon$ because ε is related by $\leq_\ell{}^*$ only to ε. Thus the result easily follows in this case. Now suppose that $k, l > 0$. By Definition 4.1 there is a strictly monotone map $f\colon [1, k+1] \to [1, l+1]$ such that $f(1) = 1$, $f(k+1) = l+1$ and for all $i \in [1, k]$ we have $u_i \leq_\ell v_{f(i)}$ and $u_i \leq_\ell v_{f(i+1)-1}$. Thus $\mathsf{c}(u_i) = \mathsf{c}(v_{f(i)}) = \mathsf{c}(v_{f(i+1)-1})$ by Lemma 4.4

and consequently we have $\sigma(u_i) = \sigma(v_{f(i)}) = \sigma(v_{f(i+1)-1})$. Recall that $\mathsf{c}(u_i\sigma(u_i)) = \Sigma$. Thus by (2) we have for every $i \in [1,k]$:

$$\begin{aligned}(4)\quad u_i\sigma(u_i) &\leq_\ell u_i\sigma(u_i)v_{f(i)+1}\sigma(v_{f(i)+1})\dots v_{f(i+1)-2}\sigma(v_{f(i+1)-2})u_i\sigma(u_i)\\ &\leq_\ell v_{f(i)}\sigma(v_{f(i)})v_{f(i)+1}\sigma(v_{f(i)+1})\dots v_{f(i+1)-2}\sigma(v_{f(i+1)-2})v_{f(i+1)-1}\sigma(v_{f(i+1)-1})\,.\end{aligned}$$

Note that $v_1\sigma(v_1)\dots v_l\sigma(v_l)$ can be factored as $w_1\dots w_k$, where for every $i \in [1,k]$ we have

$$w_i = v_{f(i)}\sigma(v_{f(i)})\dots v_{f(i+1)-1}\sigma(v_{f(i+1)-1})\,,$$

because $f(1) = 1$ and $f(k+1) = l+1$. By (4) we have $u_i\sigma(u_i) \leq w_i$ for all $i \in [1,k]$. Thus the result follows since the quasi-order $\leq_\ell$ is compatible. □

LEMMA 4.7. *Let Σ be a finite set of cardinality n. Then $\langle \Sigma^*, \leq_\ell\rangle$ is a wqo.*

Proof. By induction on n. If $n = 1$ then the result follows by Lemma 4.5. Assume that $n > 1$. Given a proper subset $\Gamma \subsetneq \Sigma$, the restriction of $\leq_\ell$ on Γ^* still satisfies (2). Thus by the induction hypothesis $\langle \Gamma^*, \leq_\ell\rangle$ is a wqo for every proper subset $\Gamma \subsetneq \Sigma$. Observe that $\Sigma_{<n} = \bigcup_{\Gamma\subsetneq\Sigma}\Gamma^*$. Since this union is finite, $\langle \Sigma_{<n}, \leq_\ell\rangle$ is a wqo by Lemma 3.2(5) and its subqoset $\langle \Sigma_{n-1}, \leq_\ell\rangle$ is a wqo by Lemma 3.2(2). By Lemma 4.3 $\langle (\Sigma_{n-1})^*, \leq_\ell{}^*\rangle$ is a wqo. Thus also $\langle (\Sigma_{n-1})^*, \leq_\ell{}^*\rangle \times \langle \Sigma_{<n}, \leq_\ell\rangle$ is a wqo by Lemma 3.2(3). Consequently, the result follows by Lemma 4.6 and Lemma 3.2(4). □

Since $\leq_\ell$ is the least quasi-order on Σ^* satisfying (2) and wqos are closed under extensions by Lemma 3.2(1), we obtain the following theorem.

THEOREM 4.8. *Let Σ be a finite set and $\preceq$ a compatible quasi-order on Σ^* satisfying $x \preceq xyx$ for every $x, y \in \Sigma^*$ such that $\mathsf{c}(y) \subseteq \mathsf{c}(x)$. Then $\preceq$ is a well-quasi-order.*

As a direct corollary of Theorem 4.8 we obtain the following regularity condition via the Generalized Myhill-Nerode Theorem (Theorem 3.7).

COROLLARY 4.9. *Let $L \subseteq \Sigma^*$ be a language closed under the following rule:*

$$(5)\qquad uxv \in L\,,\ \mathsf{c}(y) \subseteq \mathsf{c}(x) \implies uxyxv \in L\,.$$

Then L is regular.

Proof. It suffices to show that L forms an upset with respect to $\leq_\ell$ which is a wqo by Lemma 4.7. Let $w \in L$ and $w \leq_\ell w'$. Since $\leq_\ell$ is the reflexive transitive closure of the relation R, we have $w = w_0\ R\ w_1 \dots w_{k-1}\ R\ w_k = w'$. As L satisfies (5), we have $w_i \in L$ implies $w_{i+1} \in L$. Thus the result follows by induction on k. □

5. Algebras freely generated over $\mathcal{Q}$

Now we are going to use the main result of the previous section in order to prove that finitely generated members of $\mathcal{Q}$ are well-partial-ordered. Obviously, it is sufficient to prove it for members which are freely generated over $\mathcal{Q}$ by a finite set. We start with a description of these members.

Let A be a set and $\mathcal{P}(A)$ the set of all subsets of A. A *closure operator* on $\mathcal{P}(A)$ is a map $\gamma\colon \mathcal{P}(A) \to \mathcal{P}(A)$ satisfying the following conditions for all $X, Y \in \mathcal{P}(A)$:

- $X \subseteq \gamma(X)$,
- $\gamma(\gamma(X)) = \gamma(X)$,
- $X \subseteq Y$ implies $\gamma(X) \subseteq \gamma(Y)$.

Let γ be a closure operator on $\mathcal{P}(A)$. To simplify our notation we write $\gamma\{x\}$ instead of $\gamma(\{x\})$ for $x \in A$. A subset $X \subseteq A$ is called γ-*closed* if $X = \gamma(X)$. The γ-closed sets are closed under arbitrary intersections. Conversely, if $\mathcal{C} \subseteq \mathcal{P}(A)$ is a *closure system* (i.e., a system of subsets of A closed under arbitrary intersection), then there is a closure operator γ on $\mathcal{P}(A)$ whose γ-closed sets are precisely those in $\mathcal{C}$. For details on closure operators see e.g. [5].

Let Σ be a finite alphabet. A subset $L \subseteq \Sigma^*$ is called a *mingle set* if it is closed under the following rule where $u, x, y, v \in \Sigma^*$:

$$uxv, uyv \in L \implies uxyv \in L\,. \tag{6}$$

Mingle sets form a closure system because they are closed under arbitrary intersections. Let γ be the corresponding closure operator on $\mathcal{P}(\Sigma^*)$. Thus given a subset $S \subseteq \Sigma^*$, $\gamma(S)$ is the smallest set closed under (6) containing S. It can be also described as

$$\gamma(S) = \bigcup_{n\in\mathbb{N}} S_n, \text{ where } S_0 = S \text{ and } S_{n+1} = S_n \cup \{uxyv \in \Sigma^* \mid uxv, uyv \in S_n\}\,. \tag{7}$$

We define the following quasi-order on Σ^*:

$$x \leq_\gamma y \quad \text{iff} \quad \gamma\{y\} \subseteq \gamma\{x\} \quad \text{iff} \quad y \in \gamma\{x\}\,.$$

It is easy to see that $\leq_\gamma$ is a quasi-order.

Further, we will show that $\leq_\gamma$ is compatible with the multiplication on the free monoid Σ^*. Recall the notion of left and right quotient of $L \subseteq \Sigma^*$ by $u \in \Sigma^*$:

$$u^{-1}L = \{w \in \Sigma^* \mid uw \in L\}\,, \quad Lu^{-1} = \{w \in \Sigma^* \mid wu \in L\}\,.$$

Note that mingle sets are closed under the quotient operations, i.e., if $L \subseteq \Sigma^*$ is a mingle set then so are $u^{-1}L$ and Lu^{-1} for every $u \in \Sigma^*$. Let $u \in \Sigma^*$ and assume that $w \leq_\gamma w'$, i.e., $w' \in \gamma\{w\}$. We have $w \in u^{-1}\gamma\{uw\}$. Since mingle sets are closed under the quotients, we have $w' \in \gamma\{w\} \subseteq \gamma(u^{-1}\gamma\{uw\}) = u^{-1}\gamma\{uw\}$. Consequently, $uw' \in \gamma\{uw\}$, i.e., $uw \leq_\gamma uw'$. Analogously, one can show that $wu \leq_\gamma w'u$.

The quasi-order $\leq_\gamma$ satisfies the property (1). Indeed, if $uxv, uyv \in \gamma\{z\}$ then $uxyv \in \gamma\{z\}$ by (6). Thus $\Sigma^*/{\leq_\gamma}$ belongs to $\mathcal{Q}$. Moreover, $\Sigma^*/{\leq_\gamma}$ is in fact the free Σ-generated ordered monoid in the quasi-variety $\mathcal{Q}$ as is shown in the following lemma.

LEMMA 5.1. *Let $\mathbf{A} = \langle A, \cdot, 1, \leq\rangle$ be a finitely generated ordered monoid satisfying* (1) *and $h\colon \Sigma^* \to A$ a surjective monoid homomorphism. Then for every $w, w' \in \Sigma^*$ we have $w \leq_\gamma w'$ implies $h(w) \leq h(w')$.*

Proof. Let $w \leq_\gamma w'$, i.e., $w' \in \gamma\{w\}$. By (7) we have $\gamma\{w\} = \bigcup_{n\in\mathbb{N}} S_n$. Thus $w' \in S_n$ for some $n \in \mathbb{N}$. We will show $h(w) \leq h(w')$ by induction on n. The base case for $n = 0$ is trivial because $S_0 = \{w\}$ and $h(w) \leq h(w)$. For the inductive step assume that the claim holds for all elements in S_{n-1}. By (7) we have $w' = uxyv$ for some $u, x, y, v \in \Sigma^*$ such that $uxv, uyv \in S_{n-1}$. Then by induction hypothesis we have $h(w) \leq h(uxv) = h(u)h(x)h(v)$ and similarly $h(w) \leq h(u)h(y)h(v)$. Thus $h(w) \leq h(u)h(x)h(y)h(v) = h(uxyv) = h(w')$ follows by (1). □

Thus if we show that $\leq_\gamma$ on Σ^* is a wqo then it follows that all finitely generated members in $\mathcal{Q}$ are well-partial-ordered. In order to show that $\leq_\gamma$ is a well-quasi-order, it suffices by Theorem 4.8 to prove that $\leq_\gamma$ satisfies (2). This is proved in the following lemma.

LEMMA 5.2. *Let $w \in \Sigma^*$ such that $\mathsf{c}(w) = \Gamma \subseteq \Sigma$. Then $w \leq_\gamma wzw$ for every $z \in \Gamma^*$.*

Proof. If we show that $w \leq_\gamma waw$ for all $a \in \Gamma$, then we are clearly done since $\leq_\gamma$ satisfies (1). Let $a \in \Gamma$. The word w can be factored as $w = w_1 a w_2$ for some $w_1, w_2 \in \Sigma^*$. First, applying (1) for $u = w_1$, $x = y = aw_2$ and $v = \varepsilon$, we have $w \leq_\gamma w_1 a w_2 a w_2 = waw_2$. Similarly, we obtain $waw_2 \leq_\gamma waaw_2$ by (1). By transitivity we have

$$w \leq_\gamma waaw_2\,. \tag{8}$$

Second, again using (1), we obtain

$$w \leq_\gamma w^2 = ww_1 a w_2\,. \tag{9}$$

Finally, applying (1) to (8) and (9), we obtain

$$w \leq_\gamma waw_1 a w_2 = waw\,.$$

□

Since $\leq_\gamma$ satisfies (2), it is a well-quasi-order by Theorem 4.8. Thus using Lemma 5.1, we obtain the following theorem.

THEOREM 5.3. *The class of ordered monoids $\mathcal{Q}$ defined by* (1) *is locally well-partial-ordered, i.e., every finitely generated member is well-partial-ordered.*

Moreover, the fact that $\leq_\gamma$ is a wqo has the following consequence.

COROLLARY 5.4. *Let $L \subseteq \Sigma^*$ be a language. If L is closed under* (6) *then it is regular.*

Proof. By Theorem 3.7 it is sufficient to prove that L forms an upset with respect to $\leq_\gamma$. Suppose that $x \in L$ and $x \leq_\gamma y$. Thus $y \in \gamma\{x\}$. Since L is closed under (6), we have $L = \gamma(L)$. Consequently, $y \in \gamma\{x\} \subseteq \gamma(L) = L$. □

Let $\mathbf{A} = \langle A, \cdot, 1 \leq \rangle$ be an ordered monoid and $L \subseteq A$ an upset with respect to $\leq$. We define a binary relation $\preceq_L \subseteq A \times A$ as follows:

$$x \preceq_L y \quad \text{iff} \quad \forall u, v \in A\,(uxv \in L \Rightarrow uyv \in L)\,.$$

This relation is in fact a congruence of ordered monoids known as *syntactic congruence* of L in $\mathbf{A}$ introduced in [17, 14] (although [17, 14] work with the dual quasi-order). Then $\sim_L$ denotes the corresponding monoid congruence, i.e., $\sim_L = \preceq_L \cap (\preceq_L)^{-1}$. When $\mathbf{A}$ is a finitely generated free ordered monoid $\langle \Sigma^*, \cdot, \varepsilon, = \rangle$ (hence L is just a language), we have that $\sim_L$ is of finite index iff L is regular by well-known Myhill-Nerode Theorem.

Now we are going to apply our previous results in order to show that finitely generated members of $\mathcal{Q}$ are residually finite.

THEOREM 5.5. *Finitely generated ordered monoids in $\mathcal{Q}$ are residually finite. More precisely, let $\mathbf{A}$ be a finitely generated member of $\mathcal{Q}$ and $a, b \in A$ such that $a \not\leq b$. Then there is a finite ordered monoid $\mathbf{A}_a \in \mathcal{Q}$ (not depending on b) and a homomorphism of ordered monoids $h_a \colon A \to A_a$ such that $h_a(a) \not\leq h_a(b)$.*

Proof. Let $\mathbf{A} = \langle A, \cdot, 1, \leq \rangle$ be a finitely generated member in $\mathcal{Q}$ and $a, b \in A$ such that $a \not\leq b$, i.e., $b \notin {\uparrow}\{a\}$. Consider the upset $L_a = {\uparrow}\{a\}$ and the corresponding syntactic congruence $\preceq_{L_a}$. Take for $\mathbf{A}_a$ the quotient $\mathbf{A}/{\preceq_{L_a}}$. Then there is a canonical surjective homomorphism $h_a \colon A \to A/{\sim_{L_a}}$ mapping $x \in A$ to its congruence class $[x]_{\sim_{L_a}}$. Moreover, $h_a(a) \not\leq h_a(b)$ since $a \not\preceq_{L_a} b$ (note that $a \in L_a$ and $b \notin L_a$). Next we show that the corresponding monoid congruence $\sim_{L_a}$ is of finite index. Since $\mathbf{A}$ is finitely generated, there is a surjective monoid homomorphism $g \colon \Sigma^* \to A$ for some finite Σ. By Lemma 5.1 we have that $w \leq_\gamma w'$ implies

$g(w) \leq g(w')$. Consequently, $g^{-1}[L_a] = \{w \in \Sigma^* \mid g(w) \in L_a\}$ forms an upset with respect to $\leq_\gamma$. Since $\leq_\gamma$ is well, $g^{-1}[L_a]$ is a regular language by Theorem 3.7. Consequently, $\sim_{g^{-1}[L_a]}$ is of finite index. Since g is surjective, every element in A is of the form $g(w)$ for some $w \in \Sigma^*$. We have

$$\begin{aligned} g(w) \preceq_{L_a} g(w') \quad &\text{iff} \quad \forall u, v \in \Sigma^*(g(uwv) \in L_a \implies g(uw'v) \in L_a) \\ &\text{iff} \quad \forall u, v \in \Sigma^*(uwv \in g^{-1}[L_a] \implies uw'v \in g^{-1}[L_a]) \\ &\text{iff} \quad w \preceq_{g^{-1}[L_a]} w'. \end{aligned}$$

Thus $g(w) \sim_{L_a} g(w')$ iff $w \sim_{g^{-1}[L_a]} w'$. Consequently, $\sim_{L_a}$ has to be of finite index.

Finally, we show that $\mathbf{A}_a$ belongs to $\mathcal{Q}$. To see this, we have to prove that $z \preceq_{L_a} uxv$ and $z \preceq_{L_a} uyv$ implies $z \preceq_{L_a} uxyv$. Assume that $z \preceq_{L_a} uxv$ and $z \preceq_{L_a} uyv$. Let $u', v' \in A$ such that $u'zv' \in L_a$. By our assumption we have $u'uxvv', u'uyvv' \in L_a$. By definition of L_a this means $a \leq u'uxvv'$ and $a \leq u'uyvv'$. Since $\mathbf{A}$ is in $\mathcal{Q}$, we get $a \leq u'uxyvv'$ by (1). Thus $u'uxyvv' \in L_a$ and consequently $z \preceq_{L_a} uxyv$. □

6. Applications to idempotent semirings

In this section we are going to apply the previous results to the theory of idempotent semirings. In particular we will prove that the universal theory of idempotent semirings satisfying $x = x + x^2$ is decidable.

An *idempotent semiring* is a structure $\mathbf{A} = \langle A, +, \cdot, 1\rangle$ where $\langle A, +\rangle$ is a semilattice (i.e., a commutative semigroup satisfying the identity $x = x + x$), $\langle A, \cdot, 1\rangle$ is a monoid and multiplication distributes over addition on both sides (i.e., the identity $u(x + y)v = uxv + uyv$ holds in $\mathbf{A}$). Given an idempotent semiring $\mathbf{A}$, one can define a compatible partial order on A as follows for all $a, b \in A$:

$$a \leq b \quad \text{iff} \quad a = a + b\,. \tag{10}$$

Then + becomes the meet operation with respect to this partial order. One can also define the dual partial order by viewing + as join. However, in this paper we always treat + as meet.

Let $\mathcal{V}$ be the variety of idempotent semirings satisfying $x = x + x^2$, i.e., $x \leq x^2$ holds in $\mathcal{V}$. Note that $x \leq x^2$ is in fact equivalent to $x + y \leq xy$ in idempotent semirings. Indeed, the latter inequality implies $x = x + x \leq x^2$. Conversely, we have $x + y \leq (x + y)^2 \leq xy$.

We are going to show that the ordered submonoids of members from $\mathcal{V}$ are precisely the ordered monoids from $\mathcal{Q}$. The easy inclusion is the content of the following lemma.

LEMMA 6.1. *The quasi-inequality* (1) *holds in every member of* $\mathcal{V}$.

Proof. Assume that $z \leq uxy, uyv$. Then

$$z \leq uxv + uyv = u(x + y)v \leq u(x + y)^2v \leq uxyv\,.$$

□

Conversely, we will show that every member $\mathbf{M} \in \mathcal{Q}$ is embeddable into a member from $\mathcal{V}$. We will prove even a stronger result showing that the embedding preserves existing sums in $\mathbf{M}$. An element $c \in M$ denoted $a + b$ is a *sum* of $a \in M$ and $b \in M$ if for all $u, v \in M$ the element ucv is the meet of uav and ubv. This is needed in the proof of our main result (Theorem 6.7). For this purpose we will use so-called *nuclear completions* (see [12, 10, 9]).

Let $\mathbf{M}$ be a monoid. Then it is well known that $\mathcal{P}(\mathbf{M}) = \langle \mathcal{P}(M), \cup, \cdot, \{1\}\rangle$ forms an idempotent semiring if we define the multiplication for $X, Y \subseteq M$ as follows:

$$X \cdot Y = \{xy \in M \mid x \in X,\ y \in Y\}\,.$$

Note that the induced partial order in $\mathcal{P}(\mathbf{M})$ by (10) is the order-theoretic dual of the partial order given by the usual set-theoretic inclusion $\subseteq$.

We will need certain homomorphic images of $\mathcal{P}(\mathbf{M})$ which are induced by a special closure operator on $\mathcal{P}(M)$. Given a closure operator γ on $\mathcal{P}(M)$, one can define an algebra on the set $\mathcal{P}(M)_\gamma = \gamma[\mathcal{P}(M)]$ of γ-closed subsets of M. Namely, define $\mathcal{P}(\mathbf{M})_\gamma = \langle \mathcal{P}(M)_\gamma, \cup_\gamma, \cdot_\gamma, \gamma\{1\}\rangle$, where

$$X \cup_\gamma Y = \gamma(X \cup Y)\,,$$
$$X \cdot_\gamma Y = \gamma(X \cdot Y)\,.$$

Consider the map from $\mathcal{P}(\mathbf{M})$ onto $\mathcal{P}(\mathbf{M})_\gamma$ given by $X \mapsto \gamma(X)$. This map is always a semilattice homomorphism, i.e., $\gamma(X \cup Y) = \gamma(X) \cup_\gamma \gamma(Y)$, but it need not be in general a semiring homomorphism. Nevertheless, if it is then the algebra $\mathcal{P}(\mathbf{M})_\gamma$ is an idempotent semiring. Such closure operators are called *nuclei* and one can characterize them by means of quotients. Given $u \in M$ and $L \subseteq M$, the quotient operations are defined as follows:

$$u^{-1}L = \{x \in M \mid ux \in L\} \quad \text{and} \quad Lu^{-1} = \{x \in M \mid ux \in L\}\,.$$

The above definition can be extended to quotients by subsets. For $U \subseteq M$ we define

$$U^{-1}L = \bigcap_{u \in U} u^{-1}L \quad \text{and} \quad LU^{-1} = \bigcap_{u \in U} Lu^{-1}\,.$$

Note that we have $U \cdot V \subseteq L$ iff $V \subseteq U^{-1}L$ iff $U \subseteq LV^{-1}$.

LEMMA 6.2. *The map $X \mapsto \gamma(X)$ is a semiring homomorphism iff γ-closed sets are closed under the quotients, i.e., for all $u \in M$ and $L \in \mathcal{P}(M)_\gamma$ we have $u^{-1}L, Lu^{-1} \in \mathcal{P}(M)_\gamma$.*

Proof. ($\Rightarrow$) Assume that γ is a semiring homomorphism. In particular, we have $\gamma(X \cdot Y) = \gamma(X) \cdot_\gamma \gamma(Y) = \gamma(\gamma(X) \cdot \gamma(Y))$. Let $L \subseteq M$ and $u \in M$. Using the fact that γ is a homomorphism, we obtain

$$\{u\} \cdot \gamma(u^{-1}L) \subseteq \gamma(\gamma\{u\} \cdot \gamma(u^{-1}L)) = \gamma(\{u\} \cdot u^{-1}L) \subseteq \gamma(L) = L\,.$$

Thus $\gamma(u^{-1}L) \subseteq u^{-1}L$. Thus $u^{-1}L$ is γ-closed. One can prove $Lu^{-1} \in \mathcal{P}(M)_\gamma$ analogously.

($\Leftarrow$) Since γ is monotone, we have $\gamma(X \cdot Y) \subseteq \gamma(\gamma(X) \cdot \gamma(Y))$. Conversely, we have $X \cdot Y \subseteq \gamma(X \cdot Y)$. Thus $Y \subseteq X^{-1}\gamma(X \cdot Y)$. Since γ-closed sets are closed under quotients, we obtain

$$\gamma(Y) \subseteq \gamma(X^{-1}\gamma(X \cdot Y)) = X^{-1}\gamma(X \cdot Y)\,.$$

Similarly, we get $\gamma(X) \subseteq \gamma(X \cdot Y)\gamma(Y)^{-1}$. Thus $\gamma(X) \cdot \gamma(Y) \subseteq \gamma(X \cdot Y)$. Consequently, $\gamma(\gamma(X) \cdot \gamma(Y)) = \gamma(X \cdot Y)$. □

Now we are ready to prove that every ordered monoid from $\mathcal{Q}$ can be embedded into an idempotent semiring from $\mathcal{V}$ in such a way that the embedding preserves existing sums. Let $\mathbf{A} = \langle A, \cdot, 1, \leq\rangle$ be a member of $\mathcal{Q}$. Consider the idempotent semiring $\mathcal{P}(\mathbf{A}) = \langle \mathcal{P}(A), \cup, \cdot, \{1\}\rangle$. Next we are looking for a suitable closure operator (nucleus) γ such that $\mathcal{P}(\mathbf{A})_\gamma \in \mathcal{V}$ into which $\mathbf{A}$ would be embeddable. A natural candidate for the corresponding closure system would be the set of all upward closed subsets of A closed under the rule

$$uxv, uyv \in L \implies uxyv \in L\,. \tag{11}$$

It is easy to check that this system is closed under arbitrary intersection and also quotient. Thus $\mathcal{P}(\mathbf{A})_\gamma$ is an idempotent semiring by Lemma 6.2. Moreover, one can show that $\mathcal{P}(\mathbf{A})_\gamma \in \mathcal{V}$ and $\mathbf{A}$ embeds into it via $x \mapsto \gamma\{x\}$. Nevertheless, this construction need not preserve existing sums. For that we need our γ-closed sets to be closed under existing sums.

In order to overcome this problem, we define a smaller closure system. Let $\mathcal{C}$ be the least closure system containing all principal upsets $\uparrow x$ for $x \in A$ and closed under quotients. More precisely, the system can be constructed as follows. First, we close the set of all principal upsets by quotients obtaining the system $\mathcal{B} = \{u^{-1}(\uparrow z)v^{-1} \mid u, v, z \in A\}$. Next we close $\mathcal{B}$ under arbitrary intersections obtaining the closure system $\mathcal{C}$. The closure system $\mathcal{C}$ is closed under quotients because for an indexed set $\{B_i \in \mathcal{B} \mid i \in I\}$ we have $u^{-1}\bigcap_i B_i = \bigcap_i u^{-1}B_i$ and analogously for the right quotient. Let γ be the corresponding closure operator which is a semiring homomorphism by Lemma 6.2. Consequently, $\mathcal{P}(A)_\gamma$ is an idempotent semiring.

It remains to check that $\mathcal{P}(A)_\gamma \in \mathcal{V}$ and $a \mapsto \gamma\{a\}$ is an embedding preserving existing sums. For the first, observe that the elements $u^{-1}(\uparrow z)v^{-1}$ are subsemigroups of $\mathbf{A}$, i.e.,

$$u^{-1}(\uparrow z)v^{-1} \cdot u^{-1}(\uparrow z)v^{-1} \subseteq u^{-1}(\uparrow z)v^{-1}\,.$$

Indeed, if $z \leq uxv, uyv$ then $z \leq uxyv$ because $\mathbf{A}$ satisfies (1). Since every γ-closed set is an intersection of elements from $\mathcal{B}$, we have $X \cdot X \subseteq X$ for every $X \in \mathcal{P}(A)_\gamma$ because subsemigroups are closed under arbitrary intersections. Consequently, $X \cdot_\gamma X = \gamma(X \cdot X) \subseteq \gamma(X) = X$. Thus $\mathcal{P}(\mathbf{A})_\gamma$ satisfies the identity $x = x + x^2$.

For the second, it suffices to prove that $\mathbf{A}$ can be embedded into $\mathcal{P}(\mathbf{A})_\gamma$ via the map f given by $a \mapsto \gamma\{a\}$ and this map preserves existing sums. Note that $f(a) = \uparrow a$. The map f is clearly an order-embedding because $a \leq b$ iff $f(a) = \uparrow a \supseteq \uparrow b = f(b)$. Next we check that f is a monoid homomorphism, i.e., we have to show $f(ab) = f(a) \cdot_\gamma f(b)$. Since $\gamma\colon \mathcal{P}(A) \to \mathcal{P}(A)_\gamma$ is a semiring homomorphism, we have

$$f(ab) = \gamma\{ab\} = \gamma(\{a\} \cdot \{b\}) = \gamma\{a\} \cdot_\gamma \gamma\{b\} = f(a) \cdot_\gamma f(b)\,.$$

Finally, we check that f preserves existing sums. Let $a, b \in A$ such that $a + b$ exists in A. Since $f(a + b)$ is γ-closed and f is monotone, we easily have

$$f(a + b) = \uparrow(a + b) = \gamma(\uparrow(a + b)) \supseteq \gamma(\uparrow a \cup \uparrow b) = f(a) \cup_\gamma f(b)\,.$$

For the converse, we will prove that γ-closed sets are closed under existing sums. Let $a, b \in u^{-1}(\uparrow z)v^{-1} \in \mathcal{B}$. Thus we have $z \leq uav, ubv$. Suppose that $a + b$ exists in $\mathbf{A}$. Since $u(a + b)v$ is the meet of uav and ubv, we have $z \leq u(a + b)v$, i.e., $a + b \in u^{-1}(\uparrow z)v^{-1}$. Hence all γ-closed sets from $\mathcal{B}$ are closed under existing sums. Consequently, every γ-closed set is closed under existing sums because γ-closed sets are just intersections of sets from $\mathcal{B}$. It follows that $a + b \in f(a) \cup_\gamma f(b)$ because $a, b \in \gamma(\gamma\{a\} \cup \gamma\{b\}) = f(a) \cup_\gamma f(b)$. Consequently, $f(a + b) = \gamma\{a + b\} \subseteq f(a) \cup_\gamma f(b)$. All together we have proved the following claim.

LEMMA 6.3. *Every member of $\mathcal{Q}$ is embeddable (as an ordered monoid) into a member of $\mathcal{V}$ and the embedding preserves existing sums.*

Combining Lemma 6.1 and 6.3 we obtained the following theorem.

THEOREM 6.4. *Let $\mathcal{V}$ be the variety of idempotent semirings satisfying $x = x + x^2$. The class of ordered monoids in $\mathcal{Q}$ is the class of ordered submonoids of members from $\mathcal{V}$.*

Now we are ready to prove the decidability of the universal theory of $\mathcal{V}$. The method we are going to use relies on the notion of finite embeddability property introduced in [8]

and studied in [2, 3]. The finite embeddability property is crucial for decidability because it implies existence of finite counter-models for non-valid universal sentences.

We are going to recall the definition of the finite embeddability property together with a couple of auxiliary definitions. Let $\mathbf{A} = \langle A, \langle f_i^{\mathbf{A}} \mid i \in K\rangle\rangle$ be an algebra and $B \subseteq A$. Then $\mathbf{B} = \langle B, \langle f_i^{\mathbf{B}} \mid i \in K\rangle\rangle$ is a *partial subalgebra* of $\mathbf{A}$ where for every n-ary operation f_i, $i \in K$, we define

$$f_i^{\mathbf{B}}(a_1, \dots, a_n) = \begin{cases} f_i^{\mathbf{A}}(a_1, \dots, a_n) & \text{if } f_i^{\mathbf{A}}(a_1, \dots, a_n) \in B, \\ \text{undefined} & \text{otherwise.} \end{cases}$$

Given an algebra $\mathbf{C}$ of the same type as $\mathbf{A}$ and a one-to-one map $g\colon B \to C$, we call g an *embedding* of $\mathbf{B}$ into $\mathbf{C}$ if for every n-ary operation f_i, $i \in K$, and $a_1, \dots, a_n \in B$ we have

$$g(f_i^{\mathbf{B}}(a_1, \dots, a_n)) = f_i^{\mathbf{C}}(g(a_1), \dots, g(a_n))\,,$$

whenever $f_i^{\mathbf{B}}(a_1, \dots, a_n)$ is defined. Finally, we say that a partial subalgebra $\mathbf{B}$ of $\mathbf{A}$ is *embeddable* into $\mathbf{C}$ if there is an embedding $g\colon B \to C$.

DEFINITION 6.5. *Let $\mathcal{K}$ be a class of algebras of the same type. Then $\mathcal{K}$ is said to have the* finite embeddability property *(FEP) if every finite partial subalgebra $\mathbf{B}$ of any member $\mathbf{A} \in \mathcal{K}$ is embeddable into a finite member $\mathbf{C} \in \mathcal{K}$.*

Let $\mathcal{K}$ be a class of algebras of the same type having the FEP. If φ is a universal sentence in the language of $\mathcal{K}$ which fails in $\mathcal{K}$, then it has to fail in a finite member of $\mathcal{K}$ by the FEP. This is the crucial observation in the proof of the following claim proved in [3, Section 1].

PROPOSITION 6.6. *Let $\mathcal{K}$ be a finitely axiomatized class of algebras of the same finite type (i.e., it contains only finitely many finitary operations). If $\mathcal{K}$ has the FEP then the universal theory of $\mathcal{K}$ is decidable.*

THEOREM 6.7. *The variety $\mathcal{V}$ of idempotent semirings defined by $x = x + x^2$ has the finite embeddability property.*

Proof. Let $\mathbf{A} \in \mathcal{V}$ and $B \subseteq A$ a finite subset. Thus $\mathbf{B}$ forms a finite partial subalgebra of $\mathbf{A}$. We have to embed it into a finite member of $\mathcal{V}$.

Consider the ordered submonoid $\mathbf{M}$ of $\mathbf{A}$ generated by B. We have $\mathbf{M} \in \mathcal{Q}$ by Lemma 6.1. Since $\mathbf{M}$ is finitely generated, it is well-partial-ordered by Theorem 5.3. Note that if $x+y \in B$ then $uxv + uyv = u(x + y)v$ exists in M for all $u, v \in M$.

By Theorem 5.5 we have for every pair $a, b \in B$ such that $a \not\leq b$ a finite ordered monoid $\mathbf{M}_a \in \mathcal{Q}$ (not depending on b) and a homomorphism of ordered monoids $h_a\colon M \to M_a$ such that $h_a(a) \not\leq h_a(b)$. Recall that $\mathbf{M}_a = \mathbf{M}/{\preceq_{L_a}}$ and $h_a(x) = [x]_{\sim_{L_a}}$ where $L_a = {\uparrow}\{a\}$.

Consider the direct product $\prod_{a\in B} \mathbf{M}_a$ which belongs to $\mathcal{Q}$ since $\mathcal{Q}$ is closed under direct products. We define a homomorphism of ordered monoids $h\colon M \to \prod_{a\in B} M_a$ by $h(x) = \langle h_a(x) \mid a \in B\rangle$. Then the restriction of h on B is an order-embedding by the choice of h_a's. Let $\mathbf{C}$ be the subalgebra of $\prod_{a\in B} \mathbf{M}_a$ induced by the image of h, i.e., $C = h[M]$. Then $\mathbf{C} \in \mathcal{Q}$ as $\mathcal{Q}$ is closed under forming subalgebras and C is finite since B and all M_a's are finite.

LEMMA 6.8. *The map $h\colon M \to C$ preserves existing sums.*

Proof. Suppose that $x + y$ is an existing sum in $\mathbf{M}$, i.e., $u(x + y)v$ is the meet of uxv and uyv for all $u, v \in M$. We have to show that $h(x + y)$ is a sum of $h(x)$ and $h(y)$ in $\mathbf{C}$. Since h is surjective, every element of C is of the form $h(z)$ for $z \in M$. Let $u, v \in M$. Clearly,

$h(u)h(x+y)h(v) = h(u(x+y)v) \leq h(uxv) = h(u)h(x)h(v)$ because h is monotone. Similarly, $h(u)h(x+y)h(v) \leq h(u)h(y)h(v)$.

Conversely we have to show that $h(z) \leq h(uxv), h(uyv)$ implies $h(z) \leq h(u(x+y)v)$. Assume that $h(z) \leq h(uxv), h(uyv)$. Thus for all $a \in B$ we have $z \preceq_{L_a} uxv, uyv$, i.e., $a \leq u'zv'$ implies $a \leq u'uxvv', u'uyvv'$ for all $u', v' \in M$. This in turn implies that $a \leq u'u(x+y)vv'$ since $x+y$ is a sum. Thus $z \preceq_{L_a} u(x+y)v$ for all $a \in B$ which implies $h(z) \leq h(u(x+y)v)$. □

Now the ordered monoid $\mathbf{C}$ can be embedded into its completion $\mathcal{P}(\mathbf{C})_\gamma \in \mathcal{V}$ via $f(c) = \gamma\{c\}$ as in the proof of Lemma 6.3. Moreover, $\mathcal{P}(C)_\gamma$ is finite because C is finite. Thus $f \circ h \colon M \to \mathcal{P}(C)_\gamma$ is a homomorphism of ordered monoids whose restriction to B is one-to-one. Moreover $f \circ h$ preserves existing sums by Lemma 6.3 and Lemma 6.8. Thus $f \circ h$ is an embedding of the finite partial subalgebra $\mathbf{B}$ of $\mathbf{A}$ into the finite algebra $\mathcal{P}(\mathbf{C})_\gamma \in \mathcal{V}$. □

COROLLARY 6.9. *The universal theory of idempotent semirings satisfying $x = x + x^2$ is decidable.*

Acknowledgment

The author wishes to thank Petr Savický and anonymous referees for helpful comments and remarks. The work of the author was partly supported by the grant GAP202/11/1632 of the Czech Science Foundation and partly by the long-term strategic development financing of the Institute of Computer Science (RVO:67985807).

References

[1] J. Berstel and Ch. Reutenauer. *Rational Series and Their Languages*, volume 12 of *EATCS Monographs*. Springer Verlag, 1988.

[2] Willem J. Blok and Clint J. van Alten. The finite embeddability property for residuated lattices, pocrims and BCK-algebras. *Algebra Universalis*, 48(3):253–271, 2002.

[3] Willem J. Blok and Clint J. van Alten. On the finite embeddability property for residuated ordered groupoids. *Transactions of the American Mathematical Society*, 357(10):4141–4157, 2005.

[4] Stephen L. Bloom. Varieties of ordered algebras. *Journal of Computer and System Sciences*, 13(2):200–212, October 1976.

[5] Brian A. Davey and Hilary A. Priestley. *Introduction to Lattices and Order*. Cambridge University Press, Cambridge, 1990.

[6] Aldo de Luca and Stefano Varricchio. *Finiteness and Regularity in Semigroups and Formal Languages*. Springer-Verlag, 1999.

[7] A. Ehrenfeucht, D. Haussler, and G. Rozenberg. On regularity of context-free languages. *Theoretical Computer Science*, 27(3):311–332, 1983.

[8] Trevor Evans. Some connections between residual finiteness, finite embeddability and the word problem. *J. London Math. Soc. 1*, 1:399–403, 1969.

[9] Nikolaos Galatos and Peter Jipsen. Residuated frames with applications to decidability. *Transactions of the American Mathematical Society*, 365(3):1219–1249, 2013.

[10] Nikolaos Galatos, Peter Jipsen, Tomasz Kowalski, and Hiroakira Ono. *Residuated Lattices: An Algebraic Glimpse at Substructural Logics*, volume 151 of *Studies in Logic and the Foundations of Mathematics*. Elsevier, Amsterdam, 2007.

[11] Graham Higman. Ordering by divisibility in abstract algebras. *Proceedings of the London Mathematical Society*, 2:326–336, 1952.

[12] Hiroakira Ono. Completions of algebras and completeness of modal and substructural logics. In P. Balbiani, N. Suzuki, F. Wolter, and M. Zakharyaschev, editors, *Advances in Modal Logic*, volume 4, pages 335–353. King's College Publications, 2003.

[13] Don Pigozzi. Partially ordered varieties and quasivarieties. http://orion.math.iastate.edu/dpigozzi/, 2003. Revised notes of lectures on joint work with Katarzyna Palasinska given at the CAUL, Lisbon in September of 2003, and at the Universidad Catolica, Santiago in November of 2003.

[14] Jean-Éric Pin. Syntactic semigroups. In G. Rozenberg and A. Salomaa, editors, *Handbook of formal languages*, volume 1, chapter 10, pages 679–746. Springer, 1997.
[15] Jürgen Richter-Gebert, Bernd Sturmfels, and Thorsten Theobald. First steps in tropical geometry. In *Idempotent mathematics and mathematical physics. Proceedings of the international workshop, Vienna, Austria, February 3–10, 2003*, pages 289–317. Providence, RI: American Mathematical Society (AMS), 2005.
[16] Joseph G. Rosenstein. *Linear Orderings*. Academic Press, New York, 1982.
[17] Marcel-Paul Schützenberger. Une théorie algébrique du codage. *Séminaire Dubreil. Algèbre et Théorie des Nombres*, 9:1–24, 1955–1956.

(R. Horčík) Institute of Computer Science, The Czech Academy of Sciences, Pod Vodárenskou věží 2, 182 07 Prague 8, Czech Republic.
E-mail address: horcik@cs.cas.cz