Rewriting in Varieties of Idempotent Semigroups

Ondřej Klíma, Miroslav Korbelář, and Libor Polák*

Department of Mathematics and Statistics, Masaryk University
Kotlářská 2, 611 37 Brno, Czech Republic
{klima,korbelar,polak}@math.muni.cz
http://www.math.muni.cz

Abstract. We consider rewriting as a tool for solving identity problems in varieties of idempotent semigroups. It is known that there exist finite canonical term rewrite systems and finite canonical word rewrite systems for only a very limited number of those varieties. We present a finite canonical conditional word rewrite system for a particular variety in which the classical approaches cannot be applied. Moreover, we obtain infinite single letter deleting rewrite systems for each join-irreducible variety.

Keywords: Rewriting, identity problems, varieties of semigroups.

1 Introduction

Rewriting is one of the main tools in algorithmic algebra. In semigroup theory one considers the so-called word problems for finitely presented semigroups (i.e. one looks for an effective description of consequences of a given finite set of relations over a finite alphabet). It was quite unexpected that there are finite presentations where the word problem is solvable and where no finite canonical rewrite system exist – see Squier [14].

On the other hand, solving the identity problems in varieties of universal algebras (i.e. to decide effectively which identities are valid there) is other crucial topic in algorithmic algebra. Again, one possibility to solve them is to use rewriting techniques. In contrary to word problems we have to substitute terms (words) into our rewriting rools. We discuss here rewriting for solving the identity problems in varieties of idempotent semigroups.

The lattice $\mathfrak{L}(\mathcal{B})$ of all varieties of idempotent semigroups was described by Birjukov [3], Fennemore [5], Gerhard [6]. – see Figure 1 in Section 2. The authors also showed that each proper variety in $\mathfrak{L}(\mathcal{B})$ could be defined by $x^2 \simeq x$ and single additional identity. In [11,12] the third author presented a transparent way how to solve the identity problems in all members of $\mathfrak{L}(\mathcal{B})$ using certain

* The first and the third author were supported by the Ministry of Education of the Czech Republic under the project MSM 0021622409 and by the Grant no. 201/09/1313 of the Grant Agency of the Czech Republic. The second author was supported by the project LC 505, the Eduard Čech's Center for Algebra and Geometry.

F. Winkler (Ed.): CAI 2011, LNCS 6742, pp. 185–200, 2011.

invariants. In this paper, we explore the usage and limitations of rewriting to solve the identity problems in varieties of idempotent semigroups.

Basically three variants of rewrite systems for varieties of semigroups are studied currently: term rewrite systems, word rewrite systems and conditional word rewrite systems. In [1], Baader showed that the first two approaches (using finite systems) are quite restrictive, they apply only in a very limited number of varieties – see Section 3. Concerning the third approach, a remarkable conditional word rewrite system for the variety of all idempotent semigroups was found by Siekmann and Szabó in [13].

In our paper, we first show that a word rewrite system for a certain variety ($\mathcal{C}_1$ in our notation) from [1] can be simplified using a new finite conditional word rewriting system. In an other variety ($\mathcal{B}_2$ in our notation), where a finite word rewrite system does not exist, we can apply successfully a simple finite conditional word rewrite system.

All our rules are single letter deleting. Such rules are appropriate when showing confluency – see Remark 1, and when characterizing canonical forms. Therefore, it was a natural task to find single letter deleting identities for a wide class of varieties in $\mathfrak{L}(\mathcal{B})$; more precisely, we do this for all join-irreducible varieties in $\mathfrak{L}(\mathcal{B})$. Moreover, we show that in those varieties one can reach the canonical forms using single letter deleting rules (whose systems are infinite in general). The main result here is the existence of (infinite) word rewrite systems for those varieties. This can be considered as the first step when looking for finite conditional rewrite systems for such varieties. Other varieties of idempotent semigroups are joins of the join-irreducible ones and $u \simeq v$ is an identity in $\mathcal{U} \vee \mathcal{V}$ if and only if the words u and v have the same canonical forms both in $\mathcal{U}$ and in $\mathcal{V}$. This fact implies that in order to efficiently solve the identity problem in proper varieties of idempotent semigroup, it would suffice to have rewrite systems for join-irreducible varieties.

In our paper we first collect some basic facts from universal algebra and about varieties of idempotent semigroups. In Section 3 we start with a general approach of rewriting and we specify it for varieties of groupoids. Then we consider word rewrite systems for varieties of semigroups and we deal with conditional word rewrite systems (we modified a bit the usual definition – for instance, the system from [13] is finite for us – and we also distinguish between letters and words). Each subsection collects also known results.

In Section 4 we consider finite conditional word rewrite systems for the variety $\mathcal{C}_1$ and for the variety of all idempotent semigroups. A nontrivial example is presented in the next section. Finally, Section 6 deals with single letter deleting identities and single letter deleting rewrite systems.

2 Varieties of Idempotent Semigroups

Let $X = \{x_1, x_2, ...\}$ be a fixed countable set of *variables*. As usual, we denote by X^+ the free semigroup over X (i.e. the set of all words over X with the operation of concatenation). Let λ be the empty word and we denote by $X^* = X^+ \cup \{\lambda\}$

the free monoid over X. Let $p(r_1, r_2, \dots)$ be the word resulting from $p \in X^+$ after simultaneous substitutions r_1 for x_1, r_2 for x_2, ... $(r_1, r_2, \dots \in X^+)$.

An *identity* is a pair of words $(p, q) \in X^+ \times X^+$; we write $p \simeq q$. A semigroup S satisfies the identity $p \simeq q$ if for each homomorphism $\alpha : X^+ \to S$, we have $\alpha(p) = \alpha(q)$. We write $\mathsf{Mod}(\Sigma)$ for the class of all semigroups satisfying all identities from a given system Σ of identities. Such classes are called *varieties.* For a variety $\mathcal{V} = \mathsf{Mod}(\Sigma)$, let $\sim_{\mathcal{V}}$ be the set of all identities valid in all members of $\mathcal{V}$; in other words, the set of all *consequences* of the system Σ. Let

$$\to_\Sigma = \{ (sp(r_1, r_2, \dots)t, sq(r_1, r_2, \dots)t) \mid (p, q) \in \Sigma, s, t \in X^*, r_1, r_2, \dots \in X^+ \}.$$

A well-known result, the so-called *completeness of equational logics*, by Birkhoff (see Theorem 14.19 in [4]) assures that $\sim_{\mathcal{V}}$ is the equivalence relation generated by $\to_\Sigma$. Moreover the relations of the form $\sim_{\mathcal{V}}$ are exactly the fully invariant congruences on X^+ (i.e. congruences invariant with respect to substitutions).

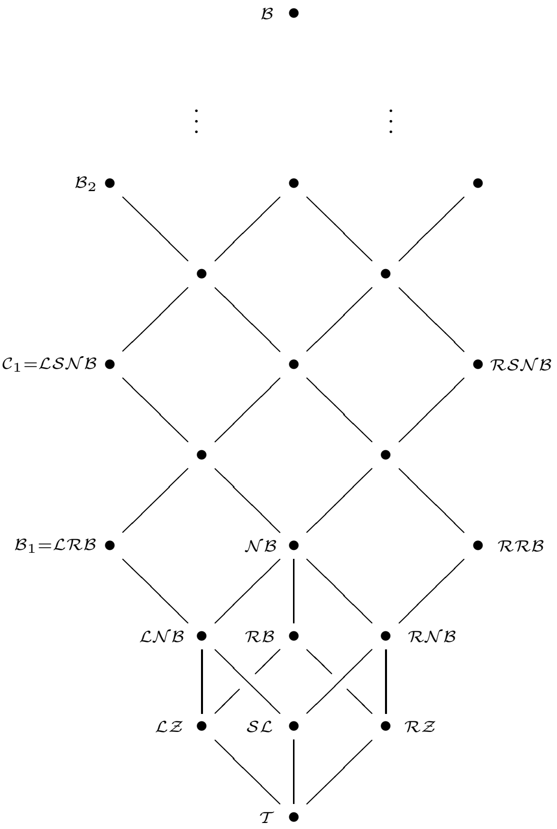

Fig. 1. The lattice of varieties of idempotent semigroups

The lattice of all varieties of idempotent semigroups was independently described by Birjukov [3], Fennemore [5] and Gerhard [6].

Varieties of semigroups are usually presented by systems of identities or by structural properties of their members. In [11,12] we studied the varieties of unions of groups (idempotent semigroups are unions of trivial groups) and the basic tools were alternative descriptions of the relations $\sim_{\mathcal{V}}$'s. We used the following "invariants".

For $p \in X^+$, we define

- the *content* $\mathsf{c}(p) \subseteq X$ of p as the set of all variables in p,
- the *head* $\mathsf{h}(p) \in X$ of p as the leftmost variable in p,
- the *tail* $\mathsf{t}(p) \in X$ of p as the rightmost variable in p,
- $0(p) \in X^*$ as the longest initial segment of p containing all but one variable,
- $1(p) \in X^*$ as the longest final segment of p containing all but one variable,
- $\overrightarrow{p} \in X^+$ as the sequence of the first occurrences of variables when reading p from the left,
- $\overleftarrow{p} \in X^+$ as the sequence of the first occurrences of variables when reading p from the right,
- $|p|$ denotes the length of p.

We also put $\mathsf{h}(\lambda) = \mathsf{t}(\lambda) = 0(\lambda) = \lambda$, $0^0(p) = p$, $0^2(p) = 0(0(p))$ and so on.

For the quite simple case of idempotent semigroups the descriptions of the relations $\sim_{\mathcal{V}}$'s is transparently explained in [7], Section 1.1.3.

3 Rewriting on Varieties of Semigroups

3.1 Generalities

An excellent source on rewriting is the book by Baader and Nipkow [2]. We recall here only facts needed in our text.

Consider a binary relation $\rightarrow$ on a set M, called *rewrite relation*. The problem consists in finding an effective description of the equivalence relation $\mathsf{eq}(\rightarrow)$ generated by $\rightarrow$. We denote by ρ^* the reflexive transitive closure of $\rho \subseteq M \times M$. The relation $\rightarrow$ is

- *terminating* if there is no infinite sequence $a_1 \rightarrow a_2 \rightarrow \dots$, $a_1, a_2, \dots \in M$,
- *locally confluent* if for each $a, b, c \in M$ with $b \leftarrow a \rightarrow c$, there exists $d \in M$ such that
$$b \rightarrow^* d \leftarrow^* c\,,$$
- *confluent* if for each $a, b, c \in M$ with $b \leftarrow^* a \rightarrow^* c$, there exists $d \in M$ such that
$$b \rightarrow^* d \leftarrow^* c\,,$$
- *canonical* if it is terminating and confluent.

In [9], Neuman proves that a terminating locally confluent relation is confluent. A $\rightarrow$-*canonical* form of $a \in M$ is an element $b \in M$ that $a \rightarrow^* b$ and there is no $c \in M$ with $b \rightarrow c$. In general, an element needs not have a canonical form or it can have several of them. In the case of a canonical relation $\rightarrow$, every element a possesses exactly one $\rightarrow$-canonical form which we denote by $[a]_\rightarrow$. In this case, the elements a and b are in the same equivalence class of the relation $\mathsf{eq}(\rightarrow)$ if and only if $[a]_\rightarrow = [b]_\rightarrow$.

In fact, the main task in rewriting consists in the following: let $\sim$ be a given (often not effectively) equivalence relation on a set M and we are looking for a finite canonical rewrite relation $\longrightarrow$ on M generating the relation $\sim$.

3.2 Term Rewriting and Known Results for Idempotent Semigroups

We are interested only in the signature of single binary operational symbol. Let G be the free groupoid over X, i.e. the set of all terms over X in the above signature. For $p, r_1, r_2, \dots \in G$ we define $p(r_1, r_2, \dots)$ as the term resulting from $p = p(x_1, x_2, \dots)$ after simultaneous substitutions r_1 for x_1, r_2 for x_2, ... A *term rewrite system* (TRS in short) is a subset T of $G \times G$. The corresponding rewrite relation on G is

$$\rightarrow_T = \{\, (t, t') \in G \times G \mid \text{where } t, r_1, r_2, \dots \in G,\ (u, v) \in T,\ u(r_1, r_2, \dots)$$

$$\text{being a subterm of } t \text{ and } t' \text{ results from } t \text{ by putting}$$

$$v(r_1, r_2, \dots) \text{ in place of } u(r_1, r_2, \dots)\,\}\,.$$

A usage of TRS's for varieties of idempotent semigroups is very restrictive; namely:

Result 1 (Baader [1]). *Let $\mathcal{V}$ be a variety of idempotent semigroups. Then there exists a TRS $T_\mathcal{V}$ such that the rewrite relation $\rightarrow_{T_\mathcal{V}}$ is canonical on G and the equivalence it generates coincides with the fully invariant congruence on G corresponding to the variety $\mathcal{V}$ (i.e. with the set of all groupoid identities which are valid in $\mathcal{V}$) if and only if $\mathcal{V} \in \{\mathcal{LZ}, \mathcal{RZ}, \mathcal{RB}\}$. Moreover, one can take*

- $T_{\mathcal{LZ}} = \{\, (xy)z \rightarrow x(yz),\ xy \rightarrow x \,\}$,
- $T_{\mathcal{RZ}} = \{\, (xy)z \rightarrow x(yz),\ xy \rightarrow y \,\}$,
- $T_{\mathcal{RB}} = \{\, (xy)z \rightarrow xz,\ x(yz) \rightarrow xz,\ xx \rightarrow x \,\}$.

3.3 Word Rewriting and Known Results for Idempotent Semigroups

According to Baader [1], a *word rewrite system* (WRS in short) is a subset W of $X^+ \times X^+$. For a *rule* $(p, q) \in W$ we also write $p \rightarrow q$. A WRS W also defines a rewrite relation $\rightarrow_W$ on X^* by

$$\rightarrow_W = \{\, (sp(r_1, r_2, \dots)t, sq(r_1, r_2, \dots)t) \mid (p, q) \in W, s, t \in X^*, r_1, r_2, \dots \in X^+\}.$$

A usage of WRS's for varieties of idempotent semigroups is applicable also only for a small number of varieties; namely:

Result 2 (Baader [1]). *Let $\mathcal{V}$ be a variety of idempotent semigroups. Then there exists a WRS $W_{\mathcal{V}}$ such that the rewrite relation $\rightarrow_{W_{\mathcal{V}}}$ is canonical and the equivalence it generates coincides with $\sim_{\mathcal{V}}$ if and only if $\mathcal{V}$ equals one of the following varieties:*

(i) $\mathcal{LZ} = \mathsf{Mod}(\, xy \simeq x \,)$,
(ii) $\mathcal{RB} = \mathsf{Mod}(\, x^2 \simeq x, xyx \simeq x \,)$,
(iii) $\mathcal{LRB} = \mathsf{Mod}(\, x^2 \simeq x, xyx \simeq xy \,)$,
(iv) $\mathcal{LQNB} = \mathsf{Mod}(\, x^2 \simeq x, xyxz \simeq xyz \,)$,
(v) $\mathcal{LSNB} = \mathsf{Mod}(\, x^2 \simeq x, xyzxz \simeq xyz \,)$.

or the left-right duals for items (i), (iii)–(v). Moreover, one can take

- $W_{\mathcal{LZ}} = \{\, xy \rightarrow x \,\}$,
- $W_{\mathcal{RB}} = \{\, x^2 \rightarrow x,\ xyz \rightarrow xz \,\}$,
- $W_{\mathcal{LRB}} = \{\, x^2 \rightarrow x,\ xyx \rightarrow xy \,\}$,
- $W_{\mathcal{LQNB}} = \{\, x^2 \rightarrow x,\ xyxz \rightarrow xyz \,\}$,
- $W_{\mathcal{LSNB}} = \{\, x^2 \rightarrow x,\ xyztzx \rightarrow xyztx,\ xzyzx \rightarrow xyzx,\ zxyzx \rightarrow zxyx,$ $zyxzx \rightarrow zyx,\ zyxtzx \rightarrow zyxtx \,\}$.

3.4 Conditional Word Rewriting Systems: Definitions and Examples

For our purposes we formalize the concept of a conditional word rewrite system as follows. Here we use two alphabets; we substitute variables for elements of the first set and words for elements of the second one.

Let $A = \{a_1, a_2, \dots\}$ and $P = \{p_1, p_2, \dots\}$ be the so-called *rule alphabets*. A *conditional rule* is an triple (ℓ, r, φ) where $\ell, r \in (A \cup P)^+$ and φ is a finite relation on $(A \cup P)^+$. A *φ-substitution* is a mapping σ from A to X and from P to X^* (in fact, a pair of mappings), naturally extended to the domain $(A \cup P)^+$, satisfying

$$(u, v) \in \varphi \text{ implies } \mathsf{c}(\sigma(u)) \subseteq \mathsf{c}(\sigma(v))\,.$$

A *conditional word rewrite system* (CWRS in short) C is a set of conditional rules. It defines a rewrite relation $\rightarrow_C$ on X^+ by

$$\rightarrow_C \,=\, \{\, (s\sigma(\ell)t,\ s\sigma(r)t) \mid (\ell, r, \varphi) \in C,\ \sigma \text{ is a } \varphi\text{-substitution},\ s, t \in X^* \,\}\,.$$

In what follows we are a bit informal, for instance, we write

$$pxqxr \rightarrow pxqr,\ p, q, r \in X^*,\ x \in X,\ \mathsf{c}(q) \subseteq \mathsf{c}(r) \subseteq \mathsf{c}(pxq),$$

instead of

$$(\, pxqxr,\ pxqr,\ \{(q, r),\ (r, pxq)\}\,),\ x \in A,\ p, q, r \in P\,.$$

Notice that a WRS is a special case of a CWRS; we identify P with X and we do not use A and conditions.

A significant example of a finite CRWS follows.

Result 3 (Siekmann and Szabó [13]). *Let $\mathcal{B} = \mathsf{Mod}(x^2 \simeq x)$ be the variety of all idempotent semigroups. Then the conditional rules*

- $p^2 \to p,\ p \in X^+$,
- $pqr \to pr,\ p, q, r \in X^+,\ \mathsf{c}(q) \subseteq \mathsf{c}(p) = \mathsf{c}(r)$

determine a canonical CWRS on X^+ such that the equivalence it generates is exactly $\sim_{\mathcal{B}}$.

The proof of the local confluency is extremely complicated there. Another type of proof is presented in [8] by Neto and Sezinando; the idea of the proof is to show that each class of $\sim_{\mathcal{B}}$ contains just one word on which conditional rules can not be applied. We return to that result in Section 4.

Also Nordahl in [10] claims that a certain finite set of conditional rules determines a canonical CWRS such that the equivalence it generates is the fully invariant congruence on X^+ corresponding to the join of the variety of all idempotent semigroups and the variety of all commutative semigroups.

4 Two Examples of Finite CWRS with Single Letter Deleting Rules

First we present a simple CWRS for the variety $\mathcal{C}_1 = \mathcal{LSNB} = \mathsf{Mod}(\,x^2 \simeq x, xyzxz \simeq xyz\,)$. According to [11,12], the corresponding fully invariant congruence $\approx_1 = \sim_{\mathcal{C}_1}$ can be described as follows:

$$\text{for all } u, v \in X^*, \text{we have } u \approx_1 v \text{ iff } \overrightarrow{u} = \overrightarrow{v} \text{ and } (\,\forall\, k \geq 0\,)\ \mathsf{t}(0^k(u)) = \mathsf{t}(0^k(v)).$$

Let C be a CWRS consisting of the following rules:
(C1) $x^2 \to x,\ x \in X$,
(C2) $pxy \to py,\ x, y \in X,\ p \in X^+,\ x, y \in \mathsf{c}(p)$.

Note that each $u \in X^+$ can be written in a unique way in the following form:

$$(*) \quad u = y_1 w_1 y_2 w_2 \ldots y_n w_n \text{ where } n \geq 1,\ y_1, \ldots, y_n \in X,\ w_1, \ldots, w_n \in X^*,$$

$$\text{and for all } k \in \{0, \ldots, n-1\},\ \text{we have } 0^k(u) = y_1 w_1 y_2 w_2 \ldots y_{n-k} w_{n-k}\,.$$

Lemma 1. *The word of the form $(*)$ is a $\to_C$-canonical form if and only if*
(1) $w_1, \ldots, w_n \in X \cup \{\lambda\}$, *and*
(2) *for all $j \in \{1, \ldots, n\}$, we have $y_j \neq w_j$.*

Proof. First we show that for an arbitrary word $u \in X^+$ written in the form $(*)$ there is such a word v in the form $(*)$ satisfying conditions (1) and (2) such that $u \to_C^* v$. Indeed, if u has form $(*)$ and for some j the length of w_j is more than 1, we apply rule (C2) to shorten this word. Using this repeatedly, we get a word satisfying (1). Then using rule (C1) (repeatedly) we can get the desired form.

By definition of the rules (C1) and (C2), they cannot be applied to reduce words with shape $(*)$ that satisfy properties (1) and (2). □

Lemma 2. *(i) We can derive the defining identities for $\mathcal{C}_1$ from the rules of C.*
(ii) The system C is consistent with $\mathcal{C}_1$, i.e. both rules are identities in $\mathcal{C}_1$.
(iii) If both u and v are $\rightarrow_C$-canonical forms and $u \approx_1 v$, then $u = v$.

Proof. (i): Using rule (C1) one can derive x from xx. Similarly, $xyzxz \rightarrow xyzz$ by (C2) and $xyzz \rightarrow xyz$ by (C1).

(ii): By definition of $\mathcal{C}_1$ we have $(x^2, x) \in \approx_1$ for $x \in X$. Let us consider $x, y \in X$, $p \in X^+$ such that $x, y \in \mathsf{c}(p)$, i.e. we have $pxy \rightarrow py$. We have $\overrightarrow{pxy} = \overrightarrow{p} = \overrightarrow{py}$ and $\mathsf{t}(pxy) = y = \mathsf{t}(py)$. Moreover, $0(pxy) = 0(p) = 0(py)$.

(iii): Let u and v be $\rightarrow_C$-canonical forms. By Lemma 1 we can write $u = y_1 w_1 \dots y_n w_n$ and $v = y'_1 w'_1 \dots y'_m w'_m$, with $n, m \geq 1$, $y_1 \dots, y_n, y'_1, \dots y'_m \in X$ and $w_1, \dots, w_n, w'_1, \dots, w'_n \in X \cup \{\lambda\}$. Since $u \approx_1 v$, we have $y_1 y_2 \dots y_n = \overrightarrow{u} = \overrightarrow{v} = y'_1 y'_2 \dots y'_m$ from which $n = m$ and $y_1 = y'_1$, …, $y_n = y'_n$ follows. Now for each $k \in \{0, \dots, n-1\}$ we consider w_{n-k} and w'_{n-k}. If $w_{n-k} \in X$ then $\mathsf{t}(0^k(u)) = w_{n-k}$ and if $w_{n-k} = \lambda$ then $\mathsf{t}(0^k(u)) = y_{n-k}$. Similarly for $\mathsf{t}(0^k(v))$. Recall that $\mathsf{t}(0^k(u)) = \mathsf{t}(0^k(v))$ follows from the assumption $u \approx_1 v$. If $w_{n-k} = \lambda$ and $w'_{n-k} \in X$ at the same moment, then $y'_{n-k} = y_{n-k} = \mathsf{t}(0^k(u)) = \mathsf{t}(0^k(v)) = w'_{n-k}$ which contradicts condition (ii) in Lemma 1. The case $w_{n-k} \in X$ and $w'_{n-k} = \lambda$ is impossible from the same reason. Thus $w_{n-k} = w'_{n-k} = \lambda$ or $w_{n-k}, w'_{n-k} \in X$. In the second case we have $w_{n-k} = \mathsf{t}(0^k(u)) = \mathsf{t}(0^k(v)) = w'_{n-k}$ and we can conclude with $w_{n-k} = w'_{n-k}$ in all cases. Hence we get $u = v$. □

Theorem 1. *For each $u, v \in X^+$, we have that $u \simeq v$ is an identity in $\mathcal{C}_1$ if and only if the words u and v have the same $\rightarrow_C$-canonical forms.*

Proof. Since the rewriting using the rules C shortens the words, the relation $\rightarrow_C$ is terminating. We show that this relation is also locally confluent. Let $u \in X^+$ that can be rewritten to v and to w in single step using C. Those two words have $\rightarrow_C$-canonical forms, say $\overline{v}$ and $\overline{w}$. By Lemma 2 (ii) we have that $\overline{v} \approx_1 u \approx_1 \overline{w}$ and Lemma 2 (iii) gives that $\overline{v} = \overline{w}$.

To complete the proof we have to show that $\mathsf{eq}(\rightarrow_C) = \approx_1$. The $\subseteq$-part follows from Lemma 2 (ii). Lemma 2 (iii) gives the opposite inclusion. □

The second example of finite CWRS with single letter deleting rules follows.

Remark 1. Having letters instead of words in certain places of a CWRS often leads to the same canonical forms and showing the (local) confluency is much easier. For instance, we can modify the second rule from Result 3 to

$$pxr \rightarrow pr,\ p, r \in X^+,\ x \in X,\ x \in \mathsf{c}(p) = \mathsf{c}(r)\,.$$

On the other hand such modified rules slow down the rewriting.

5 A Finite CWRS for the Variety $\mathcal{B}_2$

We consider the variety $\mathcal{B}_2 = \mathsf{Mod}(\,x^2 \simeq x,\ xyz \simeq xyzxzyz\,)$ using the identities from [5]. According to Proposition 1, proved later in Section 6, the second identity can be replaced by $xyzxyx \simeq xyzyx$. By [11,12], the corresponding fully invariant congruence $\sim_2$ can be effectively described as follows:

$$\text{for all } \; u, v \in X^*, \text{ we have } u \sim_2 v \text{ if and only if } (\ \forall\ k \geq 0\ )\ \overleftarrow{0^k(u)} = \overleftarrow{0^k(v)}\,.$$

Let D be the CWRS consisting of the following rules:
(D1) $xx \to x,\ x \in X$,
(D2) $pxqx \to pqx,\ p, q \in X^*,\ x \in X,\ \mathsf{c}(qx) \subseteq \mathsf{c}(p)$,
(D3) $pxqxr \to pxqr,\ p, q, r \in X^*,\ x \in X,\ \mathsf{c}(q) \subseteq \mathsf{c}(r) \subseteq \mathsf{c}(pxq)$.

Lemma 3. *Let u be as in $(*)$ with*

$$w_1 = y_{1,1} \ldots y_{1,\ell_1},\ \ldots,\ w_n = y_{n,1} \ldots y_{n,\ell_n},\ \textit{where } y_{i,j} \in X,\ \ell_i \geq 0\,.$$

Then u is a $\to_D$-canonical form if and only if
(1) $y_1 \neq y_{1,1},\ \ldots,\ y_n \neq y_{n,1}$,
(2) $|\{y_{1,1}, \ldots, y_{1,\ell_1}\}| = \ell_1,\ \ldots,\ |\{y_{n,1}, \ldots, y_{n,\ell_n}\}| = \ell_n$,
(3) *for $j = 2, \ldots, n$, if $0^{n+1-j}(u) = sy_{j,1}t$ with $s, t \in X^*$ and $y_{j,1} \notin \mathsf{c}(t)$, then $\mathsf{c}(ty_j) \not\subseteq \{y_{j,2}, \ldots, y_{j,\ell_j}\}$.*

Proof. First we show that for an arbitrary word $u \in X^+$ written in the form $(*)$ there is such a word v in the form $(*)$ satisfying conditions (1) – (3) such that $u \to_C^* v$. We use rule (D1) to guarantee condition (1).

Let u have the form $(*)$ with (1) being satisfied. Let $j \in \{2, \ldots, n\}$, $y_{j,\ell} = y_{j,\ell'}$, $\ell \neq \ell'$. We use rule (D2) with the first x being $y_{j,\ell}$ and the second one being $y_{j,\ell'}$. Using this repeatedly, we get a word satisfying (1) and (2).

Let u have the form $(*)$ with (1) and (2) being satisfied. Let $j \in \{2, \ldots, n\}$, $0^{n+1-j}(v) = sy_{j,1}t$, $s, t \in X^*$, $y_{j,1} \notin \mathsf{c}(ty_j) \subseteq \{y_{j,2}, \ldots, y_{j,\ell_j}\}$. We use rule (D3) where the x's in (D3) are the above mentioned occurrences of $y_{j,1}$ and $p = s$, $q = ty_j$ and $r = y_{j,2} \ldots y_{j,\ell_j}$. Using this repeatedly, we get a word satisfying (1) – (3).

Now we show that rules (D1) – (D3) are not applicable to a word u of the form $(*)$ satisfying (1) – (3). (D1) cannot be applied to such a u because (1) and (2) prevent the occurrence of a subword xx in u.

Concerning (D2): due to $\mathsf{c}(qx) \subseteq \mathsf{c}(p)$ the xqx part of $pxqx$ should be placed between some y_j and y_{j+1} in u. But it contradicts (2).

Finally, we show that also rule (D3) is not applicable. Indeed, take a word u of the form $(*)$ satisfying (1) – (3). Let us examine the possible subwords of u with shape $pxqxr$, as in (D3). Notice that $q = \lambda$ is not possible and therefore also $r \neq \lambda$. Due to $\mathsf{c}(r) \subseteq \mathsf{c}(pxq)$ the word r is a segment of some w_j in u. Due to $y_j \notin \mathsf{c}(y_1 w_1 \ldots y_{j-1} w_{j-1})$, the right x in $pxqxr$ is not y_j from $(*)$. We can suppose that $x \notin \mathsf{c}(q)$, otherwise $q = q_1 x q_2$ and we can put $p' = pxq_1$ and use $p'xq_2xr \to p'xq_2r$ instead with the same effect. If $w_j = w'xrw''$ then $w' = \lambda$ due to $\mathsf{c}(w') \subseteq \mathsf{c}(q) \subseteq \mathsf{c}(r)$ and condition (2). Hence $x = y_{j,1}$ and if we consider s and t from (3) we have $q = ty_j$. Thus $\mathsf{c}(q) \not\subseteq \{y_{j,2}, \ldots, y_{j,\ell_j}\}$ and consequently $\mathsf{c}(q) \not\subseteq \mathsf{c}(r)$, leading to a contradiction. □

Lemma 4. *(i) We can derive the defining identities for $\mathcal{B}_2$ from the rules of D.*
(ii) The system D is consistent with $\mathcal{B}_2$, i.e. the rules are identities in $\mathcal{B}_2$.
(iii) If both u and v are $\rightarrow_D$-canonical forms and $u \sim_2 v$, then $u = v$.

Proof. (i): Using rule (D1) one can derive x from xx. Using (D2) with $p = xyz$ and $q = y$ one can obtain $xyzxyx \rightarrow_D xyzyx$.

(ii): By construction, we have $xx \sim_2 x$ for $x \in X$.

Consider $pxqx \rightarrow pqx$, $p, q \in X^*$, $x \in X$, $\mathsf{c}(qx) \subseteq \mathsf{c}(p)$. Then $\overleftarrow{pxqx} = \overleftarrow{pqx}$ and $0(pxqx) = 0(pqx)$. Thus $pxqx \sim_2 pqx$.

Consider $pxqxr \rightarrow pxqr$, $p, q, r \in X^*$, $x \in X$, $\mathsf{c}(q) \subseteq \mathsf{c}(r) \subseteq \mathsf{c}(pxq)$. Then $\overleftarrow{pxqxr} = \overleftarrow{pxqr}$ and $0(pxqxr) = 0(pxqr)$. Thus $pxqxr \sim_2 pxqr$.

(iii): Notice that, for a canonical form w with $|\mathsf{c}(w)| \geq 2$, the word $0(w)$ is again a canonical form. Furthermore, for $w, t \in X^*$ with $|\mathsf{c}(w)| \geq 2$, the fact $w \sim_2 t$ gives $0(w) \sim_2 0(t)$. Indeed, $w \sim_2 t$ implies

$$(\ \forall\ k \geq 0\ )\ \overleftarrow{0^k(u)} = \overleftarrow{0^k(v)}\,.$$

Using it for $k = \ell + 1$, $\ell \geq 0$ we obtain

$$(\ \forall\ \ell \geq 0\ )\ \overleftarrow{0^\ell(0(w))} = \overleftarrow{0^\ell(0(t))}$$

which gives $0(w) \sim_2 0(t)$.

Let u be as in Lemma 3 and let v be another word satisfying $u \sim_2 v$. We use induction with respect to $n = |\mathsf{c}(u)|$. For $n = 1$, we have $u = v \in X$. Let $n \geq 2$. Then $0(u) \sim_2 0(v)$ by the remark in the previous paragraph and by the induction assumptions we have $0(v) = 0(u)$. We can write $u = 0(u)y_n y_{n,1} \dots y_{n,\ell_n}$ and $v = 0(u)y_n z_{n,1} \dots z_{n,\ell'_n}$. Now suppose that $\ell_n < \ell'_n$ (the case $\ell_n > \ell'_n$ is similar). Due to (2) and $\overleftarrow{u} = \overleftarrow{v}$ we have $v = 0(u)y_n z_{n,1} \dots z_{n,\ell''_n} y_{n,1} \dots y_{n,\ell_n}$. From (1) we have $y_n \neq z_{n,1}$. Let consider the last occurrence of $z_{n,1}$ in $0(u)$ from the right, i.e. $0(u) = u' z_{n,1} u''$, where $z_{n,1} \notin \mathsf{c}(u'')$. Again due to $\overleftarrow{u} = \overleftarrow{v}$ we have $\mathsf{c}(u'' y_n) \subseteq \mathsf{c}(z_{n,2} \dots z_{n,\ell''_n} y_{n,1} \dots y_{n,\ell_n})$. Now we can use rule (D3) on v for $p = u'$, $x = z_{n,1}$, $q = u'' y_n$, $r = z_{n,2} \dots z_{n,\ell''_n} y_{n,1} \dots y_{n,\ell_n}$, leading to a contradiction.

Thus $\ell_n = \ell'_n$ then $u = v$ by (2) and by $\overleftarrow{u} = \overleftarrow{v}$. □

The proof of the following result is, in fact, the same as that of Theorem 1. The only difference is the usage of Lemma 4 instead of Lemma 2.

Theorem 2. *For each $u, v \in X^+$, we have that $u \simeq v$ is an identity in $\mathcal{B}_2$ if and only if the words u and v have the same $\rightarrow_D$-canonical forms.* □

6 Single Letter Deleting Identities and Single Letter Deleting Rewrite Systems

To solve the identity problem, a natural goal is to have a WRS for each variety of idempotent semigroups. As mentioned in the introduction one can restrict consideration to the join-irreducible varieties from $\mathfrak{L}(\mathcal{B})$ which are on the sides of the lattice $\mathfrak{L}(\mathcal{B})$ on Figure 1. They can be described inductively by using the invariant 0 and left-right duality. These descriptions follow from [12], Theorem 3.6.

For a word $u = x_1 x_2 \dots x_m \in X^*$, with $x_1, x_2, \dots, x_m \in X$, the word $u^{\mathsf{r}} = x_m \dots x_2 x_1$, is called the *reverse* of u. Furthermore, for a relation ρ on X^+ we consider the *reverse relation* ρ^{r} given by $\rho^{\mathsf{r}} = \{\, (u^{\mathsf{r}}, v^{\mathsf{r}}) \mid (u, v) \in \rho \,\}$.

Now we define ρ^0 in the following way: for all $u, v \in X^*$, we have

$$u \; \rho^0 \; v \quad \text{if} \quad (\, \forall\, k \geq 0 \,)\ (0^k(u) \; \rho \; 0^k(v))\,.$$

Denote $\sim_1 = \sim_{\mathcal{LRB}}$, i.e $u \sim_1 v$ if and only if $\overrightarrow{u} = \overrightarrow{v}$. Then $\sim_1^{\mathsf{r}} = \sim_{\mathcal{RRB}}$. For each $n \geq 1$, we inductively define $\sim_{n+1} = (\sim_n^{\mathsf{r}})^0$. In particular, $\sim_2$ coincides with the relation used in Section 5. We denote the corresponding varieties of idempotent semigroups $\mathcal{B}_n$, i.e. $\sim_{\mathcal{B}_n} = \sim_n$. We also denote by $\sim_0 = \{\, (u, v) \in X^* \times X^* \mid \mathsf{c}(u) = \mathsf{c}(v) \,\}$. Then $\sim_0^{\mathsf{r}} = \sim_0$, $\sim_1 = (\sim_0^{\mathsf{r}})^0$ and $\mathcal{B}_0 = \mathcal{SL}$.

If we start from the variety $\mathcal{C}_1 = \mathcal{LSNB}$ we obtain the following similar sequence of varieties We denote $\approx_1 = \sim_{\mathcal{C}_1} = \sim_{\mathcal{LSNB}}$ (see Section 4). Now for each $n \geq 1$ we define inductively $\approx_{n+1} = (\approx_n^{\mathsf{r}})^0$ and we denote the corresponding varieties of idempotent semigroups $\mathcal{C}_n$, i.e. $\approx_{\mathcal{C}_n} = \approx_n$. We also put $u \approx_0 v$ if and only if u and v have the same content and the first letter. Now $\approx_1 = (\approx_0^{\mathsf{r}})^0$, $\approx_0^{\mathsf{r}} \neq \approx_0$ and $\mathcal{C}_0 = \mathcal{LNB}$ is not a join-irreducible variety. The positions in the lattice of varieties of idempotent semigroups is depicted at Figure 2.

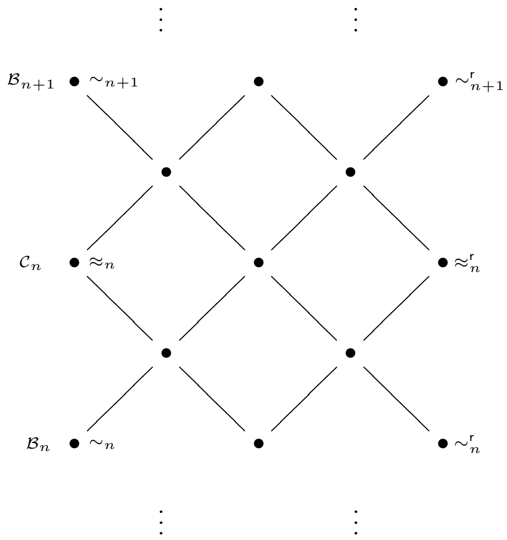

Fig. 2. A part of the lattice of varieties of idempotent semigroups

Remark 2. For each $n \geq 1$ we have $\sim_n \subseteq \approx_{n-1} \subseteq \sim_{n-1}$ and consequently the considered relations are contained in $\sim_1$. Let $\sim$ be a relation $\sim_n$ or $\approx_n$ for some

$n \geq 1$. For $u, v \in X^*$ such that $u \sim v$ we have $\overrightarrow{u} = \overrightarrow{v}$. In particular, if $0(u) = u_0$, which means $u = u_0 x u_1$, $u_0, u_1 \in X^*$, $x \notin \mathsf{c}(u_0)$, $\mathsf{c}(u_1) \subseteq \mathsf{c}(u_0 x)$, then $v = v_0 x v_1$ such that $v_0, v_1 \in X^*$, $x \notin \mathsf{c}(v_0)$, $\mathsf{c}(v_1) \subseteq \mathsf{c}(v_0 x)$ and consequently $0(v) = v_0$. Note also that for each $k \geq 1$ from $u \sim v$ it follows that $0^k(u) \sim 0^k(v)$. These easy observations will be used many times later without a precise reference.

We show that each of the varieties $\mathcal{B}_n$ and $\mathcal{C}_n$ is defined by single identity of the following special form. For our purpose we need identities different from the identities given in [3,5,6]. We denote $u_1 = xy_1x$, $v_1 = xy_1$ and then for each $n \geq 1$ we define inductively $u_{n+1} = xy_1y_2 \dots y_{n+1}u_n^{\mathsf{r}}$ and $v_{n+1} = xy_1y_2 \dots y_{n+1}v_n^{\mathsf{r}}$. The identity $u_n \simeq v_n$ is referred as π_n.

Proposition 1. *For each $n \geq 1$, we have $\mathcal{B}_n = \mathsf{Mod}(\, x^2 \simeq x, \pi_n \,)$.*

Proof. For $n = 1$ the statement follows from $\mathcal{B}_n = \mathcal{LRB}$. Thus assume $n \geq 2$. We denote $w_n = xy_1 \dots y_n$.

It is enough to prove that $u_n \sim_n v_n$ and that the identity π_n is not valid in the variety $\mathcal{V}$ which covers variety $\mathcal{B}_n$ in the lattice of varieties of idempotent semigroups. Indeed, from this we have $\mathcal{B}_n \subseteq \mathsf{Mod}(\, x^2 \simeq x, \pi_n \,) \subsetneq \mathcal{V}$ which gives the result. The variety $\mathcal{V}$ is the join of the variety $\mathcal{B}_n$ and the dual variety for $\mathcal{C}_{n-1}$. This means that we need to show $(u_n, v_n) \in \sim_n$ and $(u_n, v_n) \notin \approx_{n-1}^{\mathsf{r}}$. One can show these statements by induction with respect to n.

We see that for each $k > 0$ we have $0^k(u_n) = 0^k(w_n) = 0^k(v_n)$ and trivially $0^k(u_n) \sim_{n-1}^{\mathsf{r}} 0^k(v_n)$. Hence $(u_n, v_n) \in \sim_n$ if and only if $(u_n, v_n) \in \sim_{n-1}^{\mathsf{r}}$. By the induction assumption we have $(u_{n-1}, v_{n-1}) \in \sim_{n-1}$, hence $(u_{n-1}^{\mathsf{r}}, v_{n-1}^{\mathsf{r}}) \in \sim_{n-1}^{\mathsf{r}}$ and consequently $u_n = w_n u_{n-1}^{\mathsf{r}} \sim_{n-1}^{\mathsf{r}} w_n v_{n-1}^{\mathsf{r}} = v_n$, which finishes the proof of the first statement.

For the relation $\approx_{n-1}^{\mathsf{r}}$ and $n = 2$ we can see that $u_2 = xy_1y_2xy_1x$ and $v_2 = xy_1y_2y_1x$, i.e. $u_2^{\mathsf{r}} = xy_1xy_2y_1$ and $v_2^{\mathsf{r}} = xy_1y_2y_1x$. Since $0(u_2^{\mathsf{r}}) = xy_1x$ and $0(v_2^{\mathsf{r}}) = xy_1$ have not the same last letters, we can conclude $(u_2^{\mathsf{r}}, v_2^{\mathsf{r}}) \notin \approx_1$, thus $(u_2, v_2) \notin \approx_1^{\mathsf{r}}$. We proved the second part for $n = 2$ and we can assume $n \geq 3$.

Now, $(u_n, v_n) \in \approx_{n-1}^{\mathsf{r}}$ if and only if $(u_{n-1}w_n^{\mathsf{r}}, v_{n-1}w_n^{\mathsf{r}}) \in \approx_{n-1}$ which is not true because $0(u_{n-1}w_n^{\mathsf{r}}) = u_{n-1}$, $0(v_{n-1}w_n^{\mathsf{r}}) = v_{n-1}$ and we have the induction assumption that $(u_{n-1}, v_{n-1}) \notin \approx_{n-2}^{\mathsf{r}}$. □

In a similar way we can construct identities for the varieties $\mathcal{C}_n$. We put $s_1 = xy_1y_2xy_1$ and $t_1 = xy_1y_2y_1$. Furthermore, for every $n \geq 1$ we put $s_{n+1} = xy_1 \dots y_{n+2}s_n^{\mathsf{r}}$ and $t_{n+1} = xy_1 \dots y_{n+1}t_n^{\mathsf{r}}$. The identity $s_n \simeq t_n$ is referred as σ_n. Then one can prove the following result in the same way as Proposition 1.

Proposition 2. *For each n we have $\mathcal{C}_n = \mathsf{Mod}(x^2 \simeq x, \sigma_n)$.*

For $n \geq 1$ we consider a rewrite relation $\longrightarrow_n$ on X^* given in the following way: for $u, v \in X^*$ we put $u \longrightarrow_n v$ if v is a subword of u, $|v| = |u| - 1$ and $u \sim_n v$. Similarly, for $u, v \in X^*$ we put $u \Longrightarrow_n v$ if v is a subword of u, $|v| = |u| - 1$ and $u \approx_n v$. Note that the relations $\longrightarrow_n$ and $\Longrightarrow_n$ are not defined for $n = 0$ although some statements concerning $\sim_n$ and $\approx_n$ are also valid in this case.

Lemma 5. *Let $\mathcal{V}$ be one of the varieties $\mathcal{B}_n$, $\mathcal{C}_n$ or their dual, where $n \geq 0$. If $u, v, w \in X^*$ are such that $|v| \geq 2$ and $uvw \sim_{\mathcal{V}} uw$, then there exist words v_0, v_1, v_2 such that $v = v_0v_1v_2$, $1 \leq |v_1| < |v|$ and $uvw \sim_{\mathcal{V}} uv_0v_2w$.*

Proof. We prove the statement by induction with respect to n and the size of the set $\mathsf{c}(uvw)$. We show the detailed proof for varieties $\mathcal{B}_n$ and their duals. If $\mathcal{V} = \mathcal{B}_0$ then we have $\mathsf{c}(uvw) = \mathsf{c}(uw)$. This means that $\mathsf{c}(v) \subseteq \mathsf{c}(uw)$. Let v_0 be the empty word, v_1 be the first letter of v and v_2 be such that $v = v_0v_1v_2 = v_1v_2$. Then $\mathsf{c}(v_2) \subseteq \mathsf{c}(uw)$ and $\mathsf{c}(uv_2w) = \mathsf{c}(uw) = \mathsf{c}(uvw)$ follows.

Now let $n \geq 1$ and let $\mathcal{V} = \mathcal{B}_n$. Let u, v, w be as in the statement, in particular we have $uvw \sim_n uw$. If $\mathsf{c}(uvw) = \mathsf{c}(u)$ then $0(uvw) = 0(u)$. By the induction assumption for $uvw \sim^{\mathsf{r}}_{n-1} uw$ there are v_0, v_1, v_2 such that $v = v_0v_1v_2$, $1 \leq |v_1| < |v|$ and $uvw \sim^{\mathsf{r}}_{n-1} uv_0v_2w$. Since $0(uvw) = 0(u) = 0(uv_0v_2w)$ we get $uvw \sim_n uv_0v_2w$.

Let assume now, that $0(uvw) = us$, where s is a prefix of v such that $|s| < |v|$. This means that $v = sxt$, where $x \in X$, $\mathsf{c}(tw) \subseteq \mathsf{c}(usx)$, $x \notin \mathsf{c}(us)$. Since $\mathsf{c}(uw) = \mathsf{c}(uvw)$ we have $x \in \mathsf{c}(w)$. We consider the first occurrence of x in w, i.e. $w = w_0xw_1$, where $w_0, w_1 \in X^*$ and $x \notin \mathsf{c}(w_0)$. Now from the assumption $uvw \sim_n uw$ we get $us = 0(uvw) \sim_n 0(uw) = uw_0$. We can multiply it by $w = w_0xw_1$ to obtain $usw \sim_n uw_0w_0xw_1 \sim_{\mathcal{B}} uw_0xw_1 = uw$. So, if s is not the empty word λ we are done, we can put $v_0 = s$, $v_1 = xt$ and $v_2 = \lambda$. If $s = \lambda$ then $t \neq \lambda$ and we have $u \sim_n uw_0$. We can multiply it by $xw = xw_0xw_1$ to obtain $uxw \sim_n uw_0xw_0xw_1 \sim_{\mathcal{B}} uw_0xw_1 = uw$. Thus we have the statement for $v_0 = sx = x$, $v_1 = t$ and $v_2 = \lambda$.

Finally, assume that $0(uvw) = uvw_0$ for a certain prefix w_0 of w. This means $w = w_0xw_1$ where $\mathsf{c}(w_1) \subseteq \mathsf{c}(uvw_0x)$ and $x \notin \mathsf{c}(uvw_0)$. Hence we have $0(uw) = uw_0$. Now we use the induction assumption for the smaller set $\mathsf{c}(uvw_0) \subsetneq \mathsf{c}(uvw)$. From $uvw \sim_n uw$ we have $uvw_0 \sim_n uw_0$ and there are v_0, v_1, v_2 such that $v = v_0v_2v_2$ and $uvw_0 \sim_n uv_0v_2w_0$. When we multiply it by xw_1 we obtain $uvw \sim_n uv_0v_2w$. □

Lemma 6. *Let $n \geq 1$ and $u, v, w \in X^*$.*

i) If $uvw \sim_n uw$, then $uvw \longrightarrow^*_n uw$.
ii) If $uvw \approx_n uw$, then $uvw \Longrightarrow^*_n uw$.

Proof. It follows from Lemma 5 by induction with respect to the length of v. □

Lemma 7. *Let $\sim$ be one of the relations $\sim_n$, $\sim^{\mathsf{r}}_n$, $\approx_n$ and $\approx^{\mathsf{r}}_n$ with $n \geq 1$. Let $u, v, w, s \in X^*$ and $x, y \in X$, $x \neq y$.*

i) If $s = uxvyw \sim uxvw \sim uvyw$, then $uvw \sim s$ or $uw \sim s$.
ii) If $s = uxvxw \sim uxvw \sim uvxw$, then $uvw \sim s$ or $uxw \sim s$.

Proof. i) We prove the statement by induction with respect to n and with respect to the number of letters used in s. We prove it even for $n = 0$. So, let $\sim\, = \,\sim_0$, which means that $t_1 \sim t_2$ if and only if $\mathsf{c}(t_1) = \mathsf{c}(t_2)$. From the assumption $uxvyw \sim uxvw \sim uvyw$ we get that $x \in \mathsf{c}(uvyw)$ and $y \in \mathsf{c}(uxvw)$. Since $x \neq y$, we have $x, y \in \mathsf{c}(uvw)$ and we get $\mathsf{c}(uvw) = \mathsf{c}(s)$, i.e. $uvw \sim s$.

Assume that the statement holds for $\sim_n$, which gives the statement for $\sim^{\mathsf{r}}_n$ immediately. Let $\sim \, = \, \sim_{n+1}$ and $s = uxvyw \sim uxvw \sim uvyw$. Similarly to the proof of Lemma 5 we distinguish the cases depending on $0(uxvyw)$.

If $0(uxvyw) = u_0$, where u_0 is a proper prefix of u, then $u = u_0 z u_1$, $z \in X$, $u_0, u_1 \in X^*$, $z \notin \mathsf{c}(u_0)$ and $\mathsf{c}(u_1 xvyw) \subseteq \mathsf{c}(u_0 z)$. Hence $0(uxvw) = 0(uvyw) = 0(uvw) = 0(uw) = u_0$. Since these words are identical we have $uvw \sim_{n+1} s$ if and only if $uvw \sim^{\mathsf{r}}_n s$ and we have the same for uw. From the assumption $s = uxvyw \sim_{n+1} uxvw \sim_{n+1} uvyw$ we have $s = uxvyw \sim^{\mathsf{r}}_n uxvw \sim^{\mathsf{r}}_n uvyw$ and by the induction assumption we obtain $uvw \sim^{\mathsf{r}}_n s$ or $uw \sim^{\mathsf{r}}_n s$. Thus we get $uvw \sim s$ or $uw \sim s$.

If $0(uxvyw) = u$ then $x \notin \mathsf{c}(u)$ and $\mathsf{c}(vyw) \subseteq \mathsf{c}(ux)$. We distinguish two cases $x \in \mathsf{c}(v)$ and $x \notin \mathsf{c}(v)$. In the first case let $v_0, v_1 \in X^*$ be words such that $v = v_0 x v_1$, $x \notin \mathsf{c}(v_0)$. Then $0(uvyw) = uv_0$ and we have $u \sim uv_0$. We multiply it by $xvw = xv_0xv_1w$ and we obtain $uxvw \sim uv_0xv_0xv_1w \sim_{\mathcal{B}} uv_0xv_1w = uvw$ which means that $uvw \sim s$. In the second case $x \notin \mathsf{c}(v)$, since $x \in \mathsf{c}(uvyw)$ we have $x \in \mathsf{c}(w)$, i.e. $w = w_0 x w_1$ for some words $w_0, w_1 \in X^*$, $x \notin \mathsf{c}(w_0)$. Then $u = 0(uxvyw) \sim_{n+1} 0(uvyw) = uvyw_0$. If we multiply it by $w = w_0xw_1$ we get $uw \sim_{n+1} uvyw_0w_0xw_1 \sim_{\mathcal{B}} uvyw_0xw_1 = uvyw \sim s$.

If $0(uxvyw) = uxv_0$, where $v_0 \in X^*$ is a prefix of v, $|v_0| < |v|$ then $v = v_0 z v_1$, $z \in X$, $v_1 \in X^*$, $z \notin \mathsf{c}(uv_0)$. Then $0(uvyw) = uv_0$ and we get $uxv_0 = 0(uxvyw) \sim 0(uvyw) = uv_0$. If we multiply it by zv_1w we obtain $s \sim uxvw \sim uvw$.

If $0(uxvyw) = uxv$ then $y \notin \mathsf{c}(uxv)$, but $y \in \mathsf{c}(uxvyw) = \mathsf{c}(uxvw)$. Let w_0, w_1 be words such that $w = w_0 y w_1$ and $y \notin \mathsf{c}(w_0)$. Hence we have $uxv = 0(uxvyw) \sim 0(uvyw) = uv$. We multiply it by $w = w_0yw_1$ and we obtain $uxvw \sim uvw$.

Finally, if $0(uxvyw) = uxvyw_0$ where $w_0 \in X^*$ is a prefix of w, $|w_0| < |w|$ then $w = w_0 z w_1$, $z \in X$, $w_1 \in X^*$, $z \notin \mathsf{c}(uxvyw_0)$. Then from the assumption $s = uxvyw \sim uxvw \sim uvyw$ we obtain $s' = uxvyw_0 \sim uxvw_0 \sim uvyw_0$. If we use the induction assumption for the set $\mathsf{c}(s')$ then we get $uvw_0 \sim s'$ or $uw_0 \sim s'$. If we multiply it by zw_1 we obtain the statement.

For relations $\approx_n$ the only difference is that at the beginning for $\approx_0$ we need to check in addition that all considered words have the same first letter.

ii) For $\sim_n$ the statement can be proved in the same manner. The only difference is that it does not hold for $n = 0$. Indeed, if $u = w = \lambda$, and $v = z \neq x$, $z \in X$, then we have the assumption $xzx \sim_0 xz \sim_0 zx$ because they have the content $\{x, z\}$. But $v = z$ and x have different content. This means that we need to prove the statement for $\sim_1$ first. Assume that $\overrightarrow{uxvxw} = \overrightarrow{uvxw}$. If $x \in \mathsf{c}(u)$ then we see that $\overrightarrow{uvxw} = \overrightarrow{uvw}$. If $x \notin \mathsf{c}(uv)$ then from $\overrightarrow{uxvxw} = \overrightarrow{uvxw}$ we see that $\mathsf{c}(v) \subseteq \mathsf{c}(u)$ and consequently $\overrightarrow{uvxw} = \overrightarrow{uxw}$. Finally, if $x \notin \mathsf{c}(u)$ but $x \in \mathsf{c}(v)$, then $\overrightarrow{uvxw} = \overrightarrow{uvw}$. We prove the statement for $n = 1$. The induction step can we done in the same way as in the proof of item i). For the relations $\approx_n$ one can prove the statement in similar way. □

Theorem 3. *Let n be an arbitrary natural number. Then the rewrite relations $\longrightarrow_n$ and $\Longrightarrow_n$ are canonical. Moreover, for all $u, v \in X^*$, we have $u \sim_n v$ if and only if $[u]_{\longrightarrow_n} = [v]_{\longrightarrow_n}$ and $u \approx_n v$ if and only if $[u]_{\Longrightarrow_n} = [v]_{\Longrightarrow_n}$.*

Proof. The relation $\longrightarrow_n$ is strictly size-decreasing, hence it is terminating. We show that $\longrightarrow_n$ is locally confluent. Assume that $s = uxvyw \longrightarrow_n uxvw$ and $uxvyw \longrightarrow_n uvyw$. We need to find t such that $uxvw \longrightarrow_n^* t$ and $uvyw \longrightarrow_n^* t$. First, assume in addition that $x \neq y$. By Lemma 7 (i) we know that $uvw \sim_n s$ or $uw \sim_n s$. In the first case we have $uxvw \longrightarrow_n uvw$ and also $uvyw \longrightarrow_n uvw$. In the second case we have $uxvw \sim_n uw$ and $uvyw \sim_n uw$. Now we use Lemma 6 to state $uxvw \longrightarrow_n^* uw$ and also $uvyw \longrightarrow_n^* uw$. Now we assume that $x = y$. By Lemma 7 part ii) we have that $uvw \sim s$ or $uxw \sim s$ and one can finish the proof in the same way as in the case $x \neq y$. We proved that $\longrightarrow_n$ is terminating and locally confluent and, consequently, it is confluent.

To prove the second part of the statement we first assume that $[u]_{\longrightarrow_n} = w = [v]_{\longrightarrow_n}$. Then $u \longrightarrow_n^* w$ and $v \longrightarrow_n^* w$ from which it follows that $u \sim_n w \sim_n v$.

Now we assume that $u \sim_n v$. This means that $u \simeq v$ is an identity for $\mathcal{B}_n$. By Proposition 1, we know that $\mathcal{B}_n = \mathsf{Mod}(x^2 \simeq x, \pi_n)$. From the completeness of equational logic, there is a sequence of words $u = u_1, u_2, \ldots, u_n = v$ such that each pair (u_i, u_{i+1}) is of the form $(sp(r_1, r_2, \ldots)t, sq(r_1, r_2, \ldots)t)$ where $p(x_1, x_2, \ldots) \simeq q(x_1, x_2, \ldots)$. More precisely

$$(p, q) \in I = \{(x, x^2), (x^2, x), (u_n, v_n), (v_n, u_n)\}$$

where u_n and v_n form the identity π_n from Proposition 1. Each identity from I is of a very special form, namely it is a letter deleting one. After applying a considered substitution, we get that $p(r_1, r_2, \ldots)$ arises from $q(r_1, r_2, \ldots)$ by removing a certain factor or vice-versa $q(r_1, r_2, \ldots)$ arises from $p(r_1, r_2, \ldots)$ in the same way. Consequently, the same holds for each pair (u_i, u_{i+1}). Since $u_i \sim_n u_{i+1}$ we can apply Lemma 6 to get that for each i we have $u_i \longrightarrow_n^* u_{i+1}$ or $u_{i+1} \longrightarrow_n^* u_i$. In both cases we can deduce $[u_i]_{\longrightarrow_n} = [u_{i+1}]_{\longrightarrow_n}$ because $\longrightarrow_n$ is a canonical rewrite relation. Hence we get $[u]_{\longrightarrow_n} = [u_1]_{\longrightarrow_n} = [u_2]_{\longrightarrow_n} = \cdots = [u_n]_{\longrightarrow_n} = [v]_{\longrightarrow_n}$.

The proof for $\Longrightarrow_n$ is analogical. □

References

1. Baader, F.: Rewrite Systems for Varieties of Semigroups. In: Stickel, M.E. (ed.) CADE 1990. LNCS, vol. 449, pp. 396–410. Springer, Heidelberg (1990)
2. Baader, F., Nipkow, T.: Term Rewriting and All That. Camb. Univ. Press, Cambridge (1999)
3. Birjukov, A.P.: Varieties of Idempotent Semigroups. Algebra i Logika 9, 255–273 (1970); English translation in Algebra and Logic 9, 153–164 (1971)
4. Burris, S., Sankappanavar, H.P.: A Course in Universal Algebra. Springer, New York (1981)
5. Fennemore, C.F.: All Varieties of Bands I, II. Math. Nachr. 48, 237–252, 253-262 (1971)
6. Gerhard, J.A.: The Lattice of Equational Classes of Idempotent Semigroups. J. Algebra 15, 195–224 (1970)
7. Klíma, O.: Ph.D. thesis: Unification Modulo Associativity and Idempotency (2003), `http://www.math.muni.cz/~klima/Math/Thesis/thesis.html`

8. Neto, O., Sezinando, H.: Band Monoid Languages Revisited. Semigroup Forum 61(1), 32–45 (2000)
9. Newman, M.H.A.: On Theories with a Combinatorial Definition of 'Equivalence'. Annals of Mathematics 43(2), 223–243 (1942)
10. Nordahl, T.E.: On the Join of the Variety of All Bands and the Variety of All Commutative Semigroups via Conditional Rewrite Rules. In: Ito, M. (ed.) Words, Languages & Combinatorics, pp. 365–372. World Scientific, Singapore (1992)
11. Polák, L.: On Varieties of Completely Regular Semigroups I. Semigroup Forum 32, 97–123 (1985)
12. Polák, L.: On Varieties of Completely Regular Semigroups II. Semigroup Forum 36(3), 253–284 (1987)
13. Siekmann, J.H., Szabó, P.: A Noetherian and Confluent Rewrite System for Idempotent Semigroups. Semigroup Forum 25(1), 83–110 (1982)
14. Squier, C.C.: Word Problems and a Homological Finiteness Condition for Monoids. Journal of Pure and Applied Algebra 49, 201–217 (1987)