Term rewriting system for solving the word problem for sloops

Smile Markovski, Ana Sokolova

Faculty of Sciences and Mathematics,
Institute of Informatics, p.f.162
Skopje, Republic of Macedonia
e-mail: {smile,anas}@pmf.ukim.edu.mk

Abstract

The variety of Steiner loops (or sloops) consists of algebras of type $<2,0>$ satisfying the laws (S1), (S2) and (S3). It is shown in [7] that the word problem for the variety of sloops is solvable, but that proof is obtained as a consequence of a theorem of T. Evans [3]. Here we use a direct approach, i.e. we define a term rewriting system that solves the word problem for sloops, in such a way obtaining a more effective algorithm than that given in [3].

AMS mathematics subject classification (2000): 68Q42,08A50,20F10,05B07

Key words: (absolutely) free algebra, sloop (Steiner loop), term rewriting system, variety, word problem

1 Preliminaries

Given a variety $\mathcal{V}$ of algebras of type Ω, we say that the word problem for $\mathcal{V}$ is solvable if there is a decision procedure answering the following question. Given arbitrary terms u, v from an absolutely free finitely generated algebra of type Ω and a finite set of defining relations $\{(u_i, v_i)|\ i = 1, 2, \ldots, n\}$, whether (u, v) is in the congruence generated by the defining relations and the identities defining $\mathcal{V}$. By a suitably defined term rewriting system here we will present such a procedure for the variety of sloops. In what follows we assume that the notions such as free algebra in a variety of algebras, absolutely free algebra (or term algebra), and related ones are known ([8], [9]).

A Steiner loop, or a sloop, is an algebra $(L, \cdot, 1)$, where $\cdot$ is a binary operation and 1 is a constant, that satisfies the following identities

(S1) $\quad 1 \cdot x = x$

(S2) $\quad x \cdot y = y \cdot x$

(S3) $\quad x \cdot (x \cdot y) = y$

A Steiner triple system (STS) is a pair (L, M) where L is a finite set, M is a set containing three-element subsets of L with the property that for any $a, b \in L$ $(a \neq b)$ there is a unique $c \in L$ such that $\{a, b, c\} \in M$. It is evident that any STS on a set L enables a construction of a sloop on the set $L \cup \{1\}$ where $1 \notin L$, and vice versa. So, there is a one-to-one correspondence between Steiner triple systems and finite sloops.

By $\mathbf{Term}_X = (Term_X, \cdot, 1)$ we denote the absolutely free algebra (the term algebra) over a set of free generators X, in the signature $\cdot, 1$.

Further on we will use in great extend the notions and results from [7], and for that sake we present the needed definitions.

The mapping $d : Term_X \to \mathbb{N}$ (the weight of a term), where $\mathbb{N}$ is the set of nonnegative integers, is defined inductively as follows:

$d(1) := 0, \quad d(x) := 0$ for $x \in X, \quad d(t_1 \cdot t_2) := d(t_1) + d(t_2) + 1$.

Note that d counts the number of the operation symbols $\cdot$ in the terms.

In what follows we shall assume that X is a finite ordered set. The ordering of X can be extended to a well ordering of $Term_X$ by using an induction on d as follows. 1 is the smallest element and for any $t, s \in Term_X$ we define: if $d(t) < d(s)$ then $t < s$, and if $d(t) = d(s),\ t = t_1 \cdot t_2,\ s = s_1 \cdot s_2$ then $t < s$ iff $t_1 < s_1$ or $t_1 = s_1,\ t_2 < s_2$.

The definition of the mapping $R : Term_X \to Term_X$ given in [7] (reduction of a term) is a complex one and here we note that R can be defined by induction on d as follows. $R(1) = 1,\ R(x) = x$ for $x \in X$, and for $t, s \in Term_X$, such that $t = R(t),\ s = R(s)$,

$$R(t \cdot s) := \begin{cases} 1 & s = t \\ s & t = 1 \\ t & s = 1 \\ u & s = t \cdot u \text{ or } s = u \cdot t \text{ or} \\ & t = s \cdot u \text{ or } t = u \cdot s \\ s \cdot t & s < t \text{ and none of the previous holds} \\ t \cdot s & \text{otherwise} \end{cases}$$

For arbitrary $s, t \in Term_X$ we define $R(s \cdot t) := R(R(s) \cdot R(t))$.

An element $t \in R(Term_X)$ is called a *reduced* term.

The mapping R has the following properties ([7]).

Proposition 1 *$R^n = R$, for each $n \geq 2$, and for all $t, s \in Term_X$ we have:*

(i) $R(1 \cdot t) = R(t)$;
(ii) $R(t \cdot s) = R(s \cdot t)$;
(iii) $R(t \cdot (t \cdot s)) = R(s)$;
(iv) $R(t \cdot s) = t \cdot s \implies R(t) = t,\ R(s) = s$;
(v) $R(R(t) \cdot s) = R(t \cdot s)$;
(vi) $R(R(t) \cdot R(s)) = R(t \cdot s)$;
(vii) $R(t) \neq t \implies R(t) < t$. □

An operation $\circ$ on $R(Term_X)$ is defined by

$$t \circ s := R(t \cdot s) \text{ for all } t, s \in R(Term_X)$$

and it is shown that the following holds([7]).

Proposition 2 *$(R(Term_X), \circ, 1)$ is a free sloop with free base X.* □

Let $E = \{(t_i, s_i) \mid i = 1, \ldots, q,\ t_i \neq s_i\} \subseteq Term_X \times Term_X$ be a finite set of defining relations, and denote by A_X the subset of $Term_X \times Term_X$ defined by $A_X = \{(t, s) \mid t, s \in Term_X,\ t = s$ is an instance of (S1) $-$ (S3)$\}$. Let α be the congruence on $\mathbf{Term}_X$ generated by $E \cup A_X$, i.e. $\alpha = Cg_{\mathbf{Term}_X}(E \cup A_X)$.

Now, the word problem for the variety of sloops is the decision problem whether $u\ \alpha\ v$ for arbitrary given $u, v \in Term_X$.

If $\alpha' = Cg_{\mathbf{Term}_X}(E' \cup A_X)$, where $E' = \{(R(t_i), R(s_i)) \mid i = 1, \ldots, q\}$, then $\alpha = \alpha'$, since $x\ \alpha\ R(x)$ and $x\ \alpha'\ R(x)$ for all $x \in Term_X$. So, from now on we consider $t_i, s_i (i = 1, \ldots, q)$ reduced.

Using the general T. Evans' result in [3] we show in [7] that

Theorem 1 *The word problem for the variety of sloops is solvable.* □

In what follows we present a term rewriting system for solving the word problem for sloops, whose definition in a way captures the ideas of Evans' algorithm for universal algebras but is less complex, directed and precise. Much more, differently then the Evans'procedure, the term rewriting system depends only of E and so, for a given E, one can check whether $u\ \alpha\ v$ for any $u, v \in Term_X$.

In general, a term rewriting system (TRS) is a set of rewrite rules of the form $l_i \longrightarrow r_i$, where $l_i,\ r_i\ (i \in I)$ are terms in some signature Ω and over a set X.

We must also here mention the notion of a context $C[-]$ ([5]). Namely, context $C[-]$ is any term in signature Ω over a set $X \cup \{-\}$ $(- \notin X)$ that has exactly one occurrence of $-$ in it. By replacing any term $t \in Term_X$ for

$-$ in $C[-]$ we get a term $C[t]$ whose subterm is t. Sometimes we shall also use indices, i.e. $C_i[t]$ will denote a context of a certain term t.

Given a TRS on $Term_X$ it generates a relation $\longrightarrow$ (rewrites in one step) on $Term_X$ as follows. For $u, v \in Term_X$, $u \longrightarrow v$ iff there exists a rewrite rule $l_i \longrightarrow r_i$ such that $u = C[l_i]$, $v = C[r_i]$. The transitive and reflexive closure of $\longrightarrow$ is called rewrite relation, and will be denoted by $\rightsquigarrow$. We say that $\rightsquigarrow$ is terminating if there is no infinite sequence $x_0 \longrightarrow x_1 \longrightarrow x_2 \longrightarrow \ldots$ such that $x_i \neq x_{i-1}$.

A TRS is said to be locally confluent if

$$(\forall x, y, z \in Term_X)(\exists w \in Term_X)(x \longrightarrow y \wedge x \longrightarrow z \implies y \rightsquigarrow w \wedge z \rightsquigarrow w)$$

and it is said to be confluent (or Church-Rosser) if

$$(\forall x, y, z \in Term_X)(\exists w \in Term_X)(x \rightsquigarrow y \wedge x \rightsquigarrow z \implies y \rightsquigarrow w \wedge z \rightsquigarrow w).$$

In what follows we shall need the following Newmann's Lemma ([2, 5]):

Lemma 1 *If a TRS is terminating, then it is locally confluent if and only if it is confluent.* $\square$

One important property of a TRS is the unique normal form property (UNF). A TRS has the UNF property if for every term $u \in Term_X$, there is a unique term $u^* \in Term_X$ such that $u \rightsquigarrow u^*$ and for all $w \in Term_X$ if $u^* \rightsquigarrow w$ then $u^* = w$. It is clear that when the TRS has the UNF property, the relation $\leftrightarrow$ on $Term_X$ defined by $u \leftrightarrow v \iff u^* = v^*$ is a congruence on $\mathbf{Term}_X$.

For the TRS we shall define, we shall also prove its UNF property as well as that for any $u, v \in Term_X$, $u\ \alpha\ v$ iff certain terms uniquely corresponding to u and v respectively, rewrite to the same normal form.

2 Definition of the TRS and the main results

In this section we give a definition of the TRS for solving the word problem for sloops and state the main results, without clarifying all the details in the definitionsand without proofs, for sake of readability. All the detailed construction as well as proofs will be given in the next section.

Given a set E of defining relations and a generating set X, both finite, we take Y to be the set of all subterms of t_i, s_i $(i = 1, \ldots, q)$ union $X \cup \{1\}$ and take an equivalent disjoint set $B = \{1', b_1, \ldots, b_n\}$ to Y and a bijection $b : Y \longrightarrow B$, such that $b(1) = 1'$. For simplicity we shall also denote $1'$ by 1. The restriction of b over $X \cup \{1\}$ extends to a monomorphism from

$Term_X$ into $Term_B$, and the image of any term $t \in Term_X$ under this monomorphism will be denoted by $\bar{t}$. It is in fact a transcription from the alphabet X into the alphabet $b(X)$.

Then we deal with $\mathbf{Term}_B$. By an inductive construction we obtain two finite sets $D \subseteq B \cdot (B \cdot B)$ and $V \subseteq B \cup B \cdot B$ that "capture all the consequences" of the defining relations in E.

The TRS on $Term_B$ is defined by the following four rules schema.

$(WPS1)$	$t \longrightarrow R(t)$	$t \in Term_B,\ t \neq R(t)$
$(WPS2)$	$b_i \longrightarrow 1$	$b_i \in V \cap B$
$(WPS3)$	$b_i \longrightarrow b_j$	$b_j b_i \in V \cap B \cdot B$
$(WPS4)$	$b_i b_j \longrightarrow b_k$	$b_k(b_i b_j) \in D$

Proposition 3 *The relation $\longrightarrow$ has the UNF property and if t^* denotes the UNF of $t \in Term_B$ then:*

(i) $(\forall x \in Term_B)\ x^* = R(x)^*$;

(ii) $x = yz \in Term_B \implies x^* = (y^* z^*)^*$;

(iii) $(\forall x, y, z \in Term_B)(x^* = y^* \implies (zx)^* = (zy)^* \wedge (xz)^* = (yz)^*)$;

(iv) $(\forall x, y \in Term_B)\ ((xy)^* = 1 \iff x^* = y^*)$. □

Define a relation β on $Term_{b(X)}$ by $s\ \beta\ t \iff s^* = t^*$.

Proposition 4 *The relation β is a congruence on $\mathbf{Term}_{b(X)}$ and, for all $t \in Term_{b(X)}$, $t\ \beta\ R(t)$.* □

Theorem 2 $(\forall u, v \in Term_X)(u\ \alpha\ v \iff \bar{u}\ \beta\ \bar{v})$. □

Now, since $Term_{b(X)} \subseteq Term_B$, the solvability of the word problem for sloops is a consequence of the property that for each $u \in Term_X$ the UNF $\bar{u}^*$ of $\bar{u}$ can be found in finitely many steps.

3 Precise definitions and proofs of the results

First in this section, we focus to construction of the sets D and V, and then we present proofs of all the results.

By induction on weight d, define a mapping $P : Term_X \to \mathcal{P}(Term_X)$ as follows.

$$P(t) := \begin{cases} \{t\} & t \in X \cup \{1\} \\ \{t\} \cup P(t_1) \cup P(t_2) & t = t_1 t_2 \end{cases}$$

Let

$$Y = \left(X \cup \left(\bigcup_{i=1}^{q} P(t_i) \right) \cup \left(\bigcup_{i=1}^{q} P(s_i) \right) \right) \setminus \{1\}.$$

The set Y is finite. Let $n = |Y|$, $B = \{b_1, \ldots, b_n\}$ be a set such that $B \cap Y = \emptyset$, and let $b : Y \to B$ be a bijection that we extend to bijection from $Y \cup \{1\}$ into $B \cup \{1\}$ by $b(1) = 1$.

The restriction $b|_{X \cup \{1\}}$ can in a unique way be extended to a monomorphism $^{-}\colon Term_X \to Term_B$, and the image of $t \in Term_X$ will be denoted by $\bar{t}$.

For the construction that follows we shall need two types of mappings: $\to_{l,k}$: $Term_B \to Term_B$ for $l \neq k$, and $\to_l$: $Term_B \to Term_B$ for $l, k \in \{1, \ldots, n\}$ defined inductively by d as follows.

$$\to_{l,k}(t) := \begin{cases} t & t \neq b_l,\ t \in B \\ b_k & t = b_l \\ R(\to_{l,k}(t_1) \cdot \to_{l,k}(t_2)) & t = t_1 \cdot t_2 \end{cases}$$

$$\to_{l}(t) := \begin{cases} t & t \neq b_l,\ t \in B \\ 1 & t = b_l \\ R(\to_{l}(t_1) \cdot \to_{l}(t_2)) & t = t_1 \cdot t_2 \end{cases}$$

Note that the element b_l does not appear in the terms $\to_{l,k}(t)$ and $\to_l(t)$.

Now, we shall define the sets $D, V \subseteq Term_B$. First we form sets D_i and V_i.

Let $V_0 = \emptyset$ and let $D_0 = M_1 \cup M_2 \cup M_3$, where

$$\begin{aligned}
M_1 &= \{b_l \mid \{b_l, 1\} = \{b(t_i), b(s_i)\},\ (t_i, s_i) \in E\}, \\
M_2 &= \{b_l b_k \mid l < k,\ \{b_l, b_k\} = \{b(t_i), b(s_i)\},\ (t_i, s_i) \in E\}, \\
M_3 &= \{b_j(b_l b_k) \mid u = u_1 u_2 \in Y,\ \{b_l, b_k, b_j\} = \{b(u), b(u_1), b(u_2)\},\ l < k\}.
\end{aligned}$$

Note that, for each $u = u_1 u_2 \in Y$, there are 3 different elements in M_3, since we assumed that t_i, s_i are reduced.

If D_m and V_m are formed we put $D_{m,0} = D_m$ and $V_{m,0} = V_m$. If $D_{m,s}$ is formed and if:

1) $D_{m,s} \cap B \neq \emptyset$ and $b_l \in D_{m,s} \cap B$ is the element with smallest index, then we define

$$D_{m,s+1} = \to_l (D_{m,s}) \setminus \{1\}, \quad V_{m,s+1} = V_{m,s} \cup \{b_l\}.$$

(Then $b_l \notin D_{m,s+1}$ and b_l does not appear in the terms of $D_{m,s+1}$.)

2) $D_{m,s} \cap B = \emptyset$, $D_{m,s} \cap B \cdot B \neq \emptyset$ and $b_l b_k \in D_{m,s} \cap B \cdot B$ is the element with lexicographically smallest index lk, then we define

$$D_{m,s+1} = \rightarrow_{l,k} (D_{m,s}) \setminus \{1\}, \quad V_{m,s+1} = \rightarrow_{l,k} (V_{m,s}) \cup \{b_l b_k\}.$$

(Then $b_l b_k \notin D_{m,s+1}$ and b_l does not appear in the terms of $D_{m,s+1}$.)

3) $D_{m,s} \cap B = \emptyset$ and $D_{m,s} \cap B \cdot B = \emptyset$ then

$$D'_m = D_{m,s}, \quad V_{m+1} = V_{m,s},$$

and finish here with forming the sets $D_{m,i}$.

Note that 3) is achieved after finitely many steps since $D_{m,s} \cap B \neq \emptyset$ or $D_{m,s} \cap B \cdot B \neq \emptyset$ implies that $|D_{m,s+1}| < |D_{m,s}|$. Also, all terms in $D_{m,s}$ and $V_{m,s}$ are reduced ones.

Now we put $D_{m+1} = D'_m \cup \{b_l b_k \mid l < k,\ b_{i1}(b_{i2} b_{i3}),\ b_{j1}(b_{j2} b_{j3}) \in D'_m,\ \{i_1, i_2, i_3\} = \{l, i, j\},\ \{j_1, j_2, j_3\} = \{k, i, j\}\}$.

Let r be the least positive integer such that $D_{r+1} = D'_r$. Such an r exists because if $|D_{m+1}| = |D'_m| + p$ for some $p > 0$, then $|D'_{m+1}| \leq |D_{m+1}| - 2p = |D'_m| - p < |D'_m|$. Namely, if $b_l b_k \in D_{m+1} \setminus D'_m$ then by 2) we have that $b_l b_k \notin D'_{m+1}$ and some term of form $b_i(b_j b_l)$ (or $b_l(b_j b_i)$ or $b_i(b_l b_j)$ $\ldots$) belonging to D_{m+1} will not be in D'_{m+1} anymore.

Finaly, we define the sets D and V by: $D = D_{r+1}$, $V = V_{r+1}$.

The next proposition follows from the definition of D and V.

Proposition 5 (i) $D \cap B = D \cap B \cdot B = \emptyset$

(ii) $b_j(b_l b_k) \in D \implies |\{b_l, b_k, b_j\}| = 3$

(iii) $b_l \in V,\ b_j(b_k b_i) \in D \implies l \notin \{k, i, j\}$

(iv) $b_l \in V,\ b_i b_k \in V \implies l \notin \{i, k\}$

(v) $b_l b_k \in V,\ b_j(b_m b_i) \in D \implies l \notin \{m, i, j\}$

(vi) $b_j b_i \in V, b_k b_l \in V \implies k \neq i \neq l \neq j$. $\quad (vii)$ $b_j b_i \in V \implies i < j$.

$\square$

In order to clarify that D and V form a kind of closed set of defining relations, we define a mapping $e : Term_B \longrightarrow Term_X$ by induction on d in the following way.

$$e(x) := \begin{cases} b^{-1}(x) & x \in B \\ e(x_1)e(x_2) & x = x_1 x_2 \end{cases}$$

Note that $x = e(\bar{x})$ for each $x \in Term_X$.

Proposition 6 *For each $b_i \in V \cap B$, $b_i b_j \in V \cap B \cdot B$ and each $b_k(b_i b_j) \in D$ we have*

$$e(b_i)\ \alpha\ 1, \quad e(b_i)\ \alpha\ e(b_j), \quad e(b_k)\ \alpha\ e(b_i b_j).$$

Proof Let $b_j(b_lb_k) \in D_0,\ l < k$. Then $e(b_lb_k) = b^{-1}(b_l)b^{-1}(b_k),\ e(b_j) = b^{-1}(b_j)$ and there exists $t \in Y,\ t = t_1t_2,\ \{b_l, b_k, b_j\} = \{b(t), b(t_1), b(t_2)\}$, such that $t_1t_2\ \alpha\ t$ (by reflectivity) and $tt_1\ \alpha\ t_2,\ tt_2\ \alpha\ t_1,\ t_1t\ \alpha\ t_2,\ t_2t\ \alpha\ t_1$, since $A_X \subseteq \alpha$ and α is a congruence. Next, $b_lb_k \in D_0$ in fact means that $(e(b_l), e(b_k)) \in E \subseteq \alpha$ or $(e(b_k), e(b_l)) \in E$, so the proposition holds, and by the same reason the case $b_l \in D_0$ implies $e(b_l)\ \alpha\ 1$. Hence, the proposition holds for D_0, V_0. Assume it holds for D_m, V_m and it also holds for $D_{m,s}, V_{m,s}$.

Let $x, y \in B \cup B\cdot B \cup B\cdot(B\cdot B)$. If $e(b_l)\ \alpha\ 1$ then $e(x)\ \alpha\ e(\rightarrow_l (x))$ by the definition of $\rightarrow_l$, since $\alpha(\supseteq A_X)$ is a congruence (and then $t\ \alpha\ R(t)$for each $t \in Term_X$). Out of the same reason $e(b_l)\ \alpha\ e(b_k)$ implies $e(x)\ \alpha\ e(\rightarrow_{l,k} (x))$. Thus,

$$e(b_l)\ \alpha\ 1 \wedge e(x)\ \alpha\ e(y) \Longrightarrow\ e(\rightarrow_l (x))\ \alpha\ e(\rightarrow_l (y)),$$

$$e(b_l)\ \alpha\ e(b_k)\ \wedge\ e(x)\ \alpha\ e(y)\ \Longrightarrow\ e(\rightarrow_{l,k} (x))\ \alpha\ e(\rightarrow_{l,k} (y)).$$

As a consequence we have that the proposition holds for $D_{m,s+1}$ and $V_{m,s+1}$ too.

Finally, if $b_{i_1}(b_{i_2}b_{i_3}), b_{j_1}(b_{j_2}b_{j_3}) \in D'_m,\ \{i_1, i_2, i_3\} = \{i, j, k\},\ \{j_1, j_2, j_3\} = \{i, j, l\}$, then by inductive hypothesis $e(b_ib_j)\ \alpha\ e(b_k),\ e(b_ib_j)\ \alpha\ e(b_l)$, and we get $e(b_k)\ \alpha\ e(b_l)(e(b_l)e(b_k))\ \alpha\ e(b_l)(e(b_ib_j)e(b_ib_j))\ \alpha\ e(b_l)$. Hence, it holds also for D_{m+1}, V_{m+1} as well. $\square$

Proposition 7 *The relation $\rightsquigarrow$ is terminating i.e. there is no infinite sequence $x_0 \longrightarrow x_1 \longrightarrow \ldots$ where $x_i \neq x_{i+1}$.* $\square$

The proof of Proposition 7 is a direct consequence of the next lemma.

Lemma 2 $(\forall x, y \in Term_B)\ (x \longrightarrow y\ \Longrightarrow\ x > y)$.

Proof The construction of the sets D and V, Proposition 1 (vii) and Proposition 5 (vii) imply that the assertion is true for the rewrite rules $(WPS1) - (WPS4)$. Furthermore, for any context $C[-]$ and any rewrite rule $l_i \longrightarrow r_i$ we have $C[l_i] > C[r_i]$. $\square$

Proposition 8 *The relation $\longrightarrow$ is confluent.*

Proof By Nemann's lemma and Proposition 7 it is enough to show that the relation $\longrightarrow$ is locally confluent. Let $x, y, z \in Term_B,\ x \longrightarrow y,\ x \longrightarrow z$. The existence of $w \in Term_B$ such that $y \rightsquigarrow w,\ z \rightsquigarrow w$ holds trivially in the cases when $x \in B$ or $y = z$ or $x = C[x_1x_2],\ y = C[x'_1x_2],\ z = C[x_1x'_2]$ (then we can take $w = C[x'_1x'_2]$) or $x = C[x_1],\ y = C[R(x_1)],\ x_1 = C_1[x_2],\ z = C[C_1[R(x_2)]]$ (then we can take $w = y$.) By induction on the well ordering of $Term_B$ we shall prove that it holds in all the other cases. It is enough to prove it when $x = x_1x_2,\ y = R(x) = R(R(x_1)R(x_2))$ and z is obtained after application of $(WPS2)$, $(WPS3)$ or $(WPS4)$. Then

$$y = R(x) = \begin{cases} 1 & R(x_1) = R(x_2) \\ R(x_2) & R(x_1) = 1 \\ R(x_1) & R(x_2) = 1 \\ t & R(x_1) = tR(x_2) \text{ or } R(x_1) = R(x_2)t \\ & \text{or } R(x_2) = tR(x_1) \text{ or } R(x_2) = R(x_1)t \\ R(x_2)R(x_1) & R(x_2) < R(x_1) \text{ and none of the above holds} \\ R(x_1)R(x_2) & \text{otherwise} \end{cases}$$

and $z = z_1x_2,\ \ x_1 \longrightarrow z_1$ or $z = x_1z_2,\ \ x_2 \longrightarrow z_2$.

It is enough to consider the following possibilities.

1. $y = 1,\ z = z_1x_2$. Then we have $x_1 < x,\ x_1 \longrightarrow z_1,\ x_1 \longrightarrow R(x_1)$ and, by inductive hypothesis, there exists $w_1 \in Term_B$ such that $z_1 \rightsquigarrow w_1,\ R(x_1) \rightsquigarrow w_1$. Now $z = z_1x_2 \longrightarrow z_1R(x_2) \rightsquigarrow w_1R(x_2) \rightsquigarrow w_1w_1 \longrightarrow 1$.

2. $y = t,\ R(x_1) = tR(x_2),\ z = x_1z_2$. In this case we have $x_2 \longrightarrow z_2,\ x_2 \longrightarrow R(x_2),\ x_2 < x$, so there exists $w_1 \in Term_B$ such that $z_2 \rightsquigarrow w_1,\ R(x_2) \rightsquigarrow w_1$. Then $z \longrightarrow (tR(x_2))z_2 \rightsquigarrow (tR(x_2))w_1 \rightsquigarrow (tw_1)w_1 \longrightarrow t$.

3. $y = t,\ R(x_1) = tR(x_2),\ z = z_1x_2$. Now $x_1 \longrightarrow z_1,\ x_1 \longrightarrow R(x_1) = tR(x_2),\ x_1 < x$, so $z_1 \rightsquigarrow w_1,\ R(x_1) \rightsquigarrow w_1$ for some $w_1 \in Term_B$. We have two cases.

(i) $R(x_1)R(x_2) < x$. Since $R(x_1)R(x_2) \rightsquigarrow w_1R(x_2),\ R(x_1)R(x_2) = (tR(x_2))R(x_2) \longrightarrow t$, by inductive hypothesis and Newmann's Lemma there exists $w \in Term_B$ such that $w_1R(x_2) \rightsquigarrow w,\ t \rightsquigarrow w$. Hence, $z = z_1x_2 \rightsquigarrow w_1x_2 \longrightarrow w_1R(x_2) \rightsquigarrow w$ and $y = t \rightsquigarrow w$.

(ii) $R(x_1)R(x_2) = x$. Then $x_1 = R(x_1),\ x_2 = R(x_2),\ x_1 = tx_2$ and $x_1 \longrightarrow z_1$, i.e. $tx_2 \longrightarrow z_1$. Now, if $z_1 = tx_2'$ and $x_2 \longrightarrow x_2'$ then $z = z_1x_2 = (tx_2')x_2 \longrightarrow (tx_2')x_2' \longrightarrow t = y$, if $z_1 = wx_2$ and $t \longrightarrow w$ then $z = z_1x_2 = (wx_2)x_2 \longrightarrow R(w)$ and $y = t \longrightarrow w \longrightarrow R(w)$.

4. $y = R(x_2)R(x_1),\ z = z_1x_2$. Then $x_1 < x,\ x_1 \longrightarrow z_1,\ x_1 \longrightarrow R(x_1)$, and there exists $w_1 \in Term_B$ such that $z_1 \rightsquigarrow w_1,\ R(x_1) \rightsquigarrow w_1$ which implies $y \rightsquigarrow R(x_2)w_1,\ z \rightsquigarrow w_1x_2 \longrightarrow w_1R(x_2)$. By Proposition 1 (ii) we have $w = R(R(x_2)w_1) = R(w_1R(x_2))$. □

Proof of Proposition 3 By the termination and the confluence of the TRS we get that the relation $\longrightarrow$ has the UNF property, and then $(i) - (iii)$ are clear. For proving (iv) identities of sloops are used. If $x^* = y^*$ then, by (iii), $1 = (xx)^* = (xy)^*$. If $(xy)^* = 1$ then, by (ii), $y^* = (x(xy))^* = (x^*(xy)^*)^* = (x^*1)^* = x^*$. □

Now, Proposition 4 is straightforward.

Lemma 3 *The UNF of each element of the sets $D_{m,s}$, $V_{m,s}$ is 1.*

Proof By the definition of the TRS we have $x^* = 1$ for each $x \in D \cup V$. Assume the statement is true for each $x \in D_{m+1} \cup V_{m+1}$ and each $x \in D_{m,s+1} \cup V_{m,s+1}$. If $x \in (D_{m,s} \cup V_{m,s}) \setminus (D_{m,s+1} \cup V_{m,s+1})$ then there are two possibilities. First one is $b_l b_k \in V_{m,s+1}$, $\rightarrow_{l,k} (x) \in D_{m,s+1} \cup V_{m,s+1}$ and then $b_l^* = b_k^*$ and Proposition 3 (ii) and (iii) imply $x^* = (\rightarrow_{l,k} (x))^* = 1$.The other one is $b_l \in V_{m,s+1}$, $\rightarrow_l (x) \in D_{m,s+1} \cup V_{m,s+1}$ and then $b_l^* = 1$ implies $x^* = (\rightarrow_l (x))^* = 1$. $\square$

Corollary 1 $(\forall x \in Y)\ \bar{x}^* = b(x)^*$.

Proof $\bar{x} = b(x)$ for each $x \in X \cup \{1\}$, and if $x = x_1 x_2 \in Y$ then $\bar{x} = \bar{x}_1 \bar{x}_2$ and $b(x)(b(x_1)b(x_2)) \in D_0$ or $b(x)(b(x_2)b(x_1)) \in D_0$. By inductive hypothesis $\bar{x}_1^* = b(x_1)^*$, $\bar{x}_2^* = b(x_2)^*$, also $(b(x_1)b(x_2))^* = b(x)^*$ by Lemma 3 and Proposition 3 (iv), which further on implies $\bar{x}^* = (\bar{x}_1^* \bar{x}_2^*)^* = (b(x_1)b(x_2))^* = b(x)^*$. $\square$

Now we can give the proof of Theorem 2.

Proof of Theorem 2 By Corollary 1 we have $\bar{t}_i \rightsquigarrow b(t_i)^*$, $\bar{s}_i \rightsquigarrow b(s_i)^*$ for each $(t_i, s_i) \in E$. Note that $b(t_i), b(s_i) \in B$ i.e. $b(t_i)^*, b(s_i)^* \in B \cup \{1\}$. It is clear that $b(t_i)^* = b(s_i)^*$, for $t_i = 1$ or $s_i = 1$ and for $b(t_i)b(s_i) \in V$ or $b(s_i)b(t_i) \in V$, and if it is not the case then there exists $b_j \in B$ such that $b(t_i)b_j \in V$, $b(s_i)b_j \in V$ or $b(s_i), b(t_i) \in V$. Hence, $(\bar{t}_i, \bar{s}_i) \in \beta$.

If $(x, y) \in A_X$ then $\bar{x}\ \beta\ \overline{R(x)} = \overline{R(y)}\ \beta\ \bar{y}$.

Since both α and β are congruences we get $x\ \alpha\ y \implies \bar{x}\ \beta\ \bar{y}$.

For the reverse implication first we should note that $e(x)\ \alpha\ e(y) \implies e(C[x])\ \alpha\ e(C[y])$ for any $x, y \in Term_B$ (α is a congruence), and by simple inductive arguments we also have $e(x)\ \alpha\ e(R(x))$. If $b_l \longrightarrow 1$, $b_l \longrightarrow b_k$, $b_l b_k \longrightarrow b_j$ are rewrite rules, then $e(b_l)\ \alpha\ 1$, $e(b_l)\ \alpha\ e(b_k)$, $e(b_l b_k)\ \alpha\ e(b_j)$ by Proposition 6. Consequently, if $x \longrightarrow y$ for some $x, y \in Term_B$ then $e(x)\ \alpha\ e(y)$, hence $x \rightsquigarrow y \implies e(x)\ \alpha\ e(y)$ (α is transitive). Finally, if $\bar{u}\ \beta\ \bar{v}$ for some $u, v \in Term_X$, then $u = e(\bar{u})\ \alpha\ e(\bar{u}^*) = e(\bar{v}^*)\ \alpha\ e(\bar{v}) = v$. $\square$

A couple of conclusion remarks at the end. One could notice that the construction of D and V is similar to Evans' ([3]) construction of closed set of defining relations, using the particular properties of the variety of sloops, but there are a few major differences. The construction of the sets D and V is given by a simple algorithm, so the UNF can be found quite easily. Furthermore, once D and V are formed, the TRS defined by them can be applied for any two terms $u, v \in Term_X$ for which we want to check whether they are in relation α. That is quite different than the Evans' algorithm, where $u, v \in Term_X$ are used in it's design, i.e. it is of local character. Furthermore, the computer implementation of our algorithm is straightforward.

References

[1] R. U. Bruck: *A survey of Binary Systems*, Berlin - Götingen - Heidelberg, 1958

[2] N.Dershowitz, J.P.Jouannaud: *Rewrite Systems*, Handbook of Theoretical Computer Science, Volume B, Formal Models and Semantics, The MIT Press, 1990

[3] Trevor Evans: *The word problem for abstract algebras* , The Journal of The London Mathematical Society, vol. XXVI, 1951, 64-71

[4] P.M.Hall: *Combinatorial Theory*, Blaisdell publishing company, Walthand Massachusetts, Toronto, London, 1967

[5] J.W.Klop: *Term Rewriting Systems*, Handbook of Logic in Computer science, Volume 2, Clarendon Press - Oxford, 1992

[6] S. Markovski, A. Sokolova: *Free Basic Process Algebra*, Contributions to General Algebra, vol. 11, 1998, 157-162

[7] S. Markovski , A. Sokolova: *Free Steiner loops* (to be printed in Matematički Glasnik, Zagreb, Croatia)

[8] R. N. McKenzie, W. F. Taylor, G. F. McNulty: *Algebras, Lattices, Varieties*, Wadsworth & Brooks, Monterey, California, 1987

[9] D. M. Smirnov: *Mnogoobraziya Algebr*, Nauka, Novosibirsk, 1992