Václav Flaška; Tomáš Kepka; Juha Kortelainen
On separating sets of words. I.

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 49 (2008), No. 1, 33--51

Persistent URL: `http://dml.cz/dmlcz/142772`

On Separating Sets of Words I

VÁCLAV FLAŠKA, TOMÁŠ KEPKA and JUHA KORTELAINEN

Praha

Received 4^{th} October 2007

Various combinatorial properties of non-overlapping words (sets of which are called *separating* in the paper) are studied. Besides, the replacement systems (where the sets of left hand sides are separating) are considered in full detail.

1. Introduction

The aim of the present short note is to initiate a study of special replacement systems (see [8] for general theory) coming from so called separating sets of words in free monoids, meaning sets whose elements do not overlap. The corresponding replacement relation enjoys the diamond and other useful properties and this yields a better insight into structure and behaviour of the related transitive closures. These transitive relations (orders in many cases) may be used later to construct various congruences of free semirings (and, perhaps, other structures), yielding "exotic" examples of cogruence-simple semirings (see [4] and [1])

2. Preliminaries

We assume that the reader is familiar with the basic notation and results of formal language theory and word combinatorics as presented in [5], [6] and [7].

Department of Algebra, MFF UK, Sokolovská 83, 186 75 Praha 8, Czech Republic

Department of Information Processing Science, University of Oulu, P.O.Box 300 FIN-90014, Oulu, Finland

The work is a part of the research project MSM 0021620839 financed by MŠMT.

E-mail adress: flaska@karlin.mff.cuni.cz
E-mail adress: kepka@karlin.mff.cuni.cz
E-mail adress: juha.kortelainen@oulu.fi

Some knowledge of the theory of regulated rewriting ([3]) and string rewriting systems ([2]) is also helpful. We now summon up some of the concepts that are needed in the sequel. Let A^* be the free monoid of *words* over an alphabet A of *letters*. The *empty* word ε, that is the word of length zero, serves as neutral (or unit) element of A^* and we put $A^+ = A^* \setminus \{\varepsilon\}$;notice that A^+ is a free semigroup over A. The words from A^+ are called *nonempty* (or *nontrivial*).

Let $\mathbb{N}$ be the set of all nonnegative integers and $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. For a word $w \in A^*$, the *length* of w, denoted by $|w|$, is the number of occurrences of all the letters $a \in A$ in w. Thus $|\varepsilon| = 0$ and $|a_1 a_2 \dots a_m| = m$ for all $m \in \mathbb{N}_+$ and $a_1, a_2, \dots, a_m \in A$. Furthermore, we put $\mathrm{alph}(\varepsilon) = \emptyset$ and $\mathrm{alph}(a_1 a_2 \dots a_m) = \{a_1, a_2, \dots a_m\}$.

A word z is a *factor* of a word w if $w = uzv$ for some $u, v \in A^*$. If $u \neq \varepsilon$ or $v \neq \varepsilon$ (equivalently, $|z| < |w|$), then z is called a *proper factor*. If $u = \varepsilon$ ($v = \varepsilon$, resp.), then z is called a prefix (suffix, resp.) of w; moreover if $v \neq \varepsilon$ ($u \neq \varepsilon$, resp.), then z is called a *proper prefix* (*proper suffix*, resp.) of w. If u and v are both nonempty, then z is called an *inner factor* of w.

A word $w \in A^+$ is *primitive*, if for each $u \in A^+$ and $n \in \mathbb{N}$, the equality $v = u^n$ implies $n = 1$ (and $v = u$). It is quite easy to see that for each $v \in A^+$ there exist a unique primitive word $t \in A^+$, the *primitive root* of v (denoted by $\sqrt{w}$ in the sequel), and a number $m \in \mathbb{N}_+$ such that $v = t^m$.

Nonempty words x and y are *conjugate* (words of each other) if there exist words x_1 and x_2 such that $x = x_1 x_2$ and $y = x_2 x_1$. Conjugacy is trivially an equivalence relation; if x and y are conjugate we often say that x is a conjugate of y.

The following two results belong to the folklore of combinatorics on words. Respective proofs are not difficult and can be found in [6].

Lemma 2.1. *Two nonempty words commute if and only if they are powers of the same (primitive) word, i.e., they have the same primitive root.*

Lemma 2.2. *Let x and y be nonempty words. The following four conditions are equivalent:*

(i) *the words x and y are conjugate;*

(ii) *the words x and y are of equal length and there exist unique words t_1 and t_2 such that $t_2 \neq \varepsilon$, $t = t_1 t_2$ is primitive, $x \in (t_1 t_2)^+$ and $y \in (t_2 t_1)^+$;*

(iii) *there exists a word z_1 such that $x z_1 = z_1 y$;*

(iv) *there exists a word z_2 such that $z_2 x = y z_2$.*

Furthermore, assume that any of the four conditions above holds and that t_1 and t_2 are as in (ii). *Then, for a word w, we have $xw = wy$ if and only if $w \in (t_1 t_2)^* t_1$.*

It is quite straightforward to see that if a word x is primitive, then each conjugate y of x is also primitive.

3. Bordered and unbordered words

Call a word $w \in A^*$ *bordered* if there exist words $x, y \in A^*$, $x \neq \varepsilon$ such that $w = xyx$. We have the following

Lemma 3.1. *The following conditions are equivalent for a word w:*

(i) *the word w is bordered;*

(ii) *there exist words $u, t, v \in A^+$, $|t| \leq |u| = |v|$, such that $w = ut = tv$;*

(iii) *there exist words $p, q \in A^+$, $|q| = |p| < |w|$, such that $wp = qw$.*

Proof. The implication (i) $\Rightarrow$ (ii) is clear. The implications (ii) $\Rightarrow$ (iii) and (iii) $\Rightarrow$ (i) follow easily from Lemma 2.2. □

A nonempty word w is *unbordered* if it is not bordered (notice that, according to this definition, ε is unbordered). An unbordered word is called *primary* in [7].

Lemma 3.2. *Let $z \in A^+$. Then z is unbordered if and only if no proper non-trivial prefix (suffix, resp.) of z is a suffix (prefix, resp.) of it.*

Proof. Let $v \in A^+$, $v \neq z$ be both prefix and suffix of z. Thus there exist $x, y \in A^+$ such that $z = vx = yv$. According to Lemma 2.2 there exist $p, q \in A^+$ such that $x = pq$ and $y = qp$. Hence $z = vpq = qpv$. At least one of words v, q is not longer that $|v|/2$, which implies that z is bordered. The other implication is obvious. □

Lemma 3.3. *Each nonempty unbordered word is primitive.*

Proof. Let w be a nonempty word that is not primitive. Then $w = t^k$ where t is the primitive root of w and $k \geq 2$. Obviously, w is bordered. □

Remark 3.4. The word $w = aba, a, b \in A$, $a \neq b$, is an example of a primitive bordered word.

A word w is called *almost unbordered* if either $w = \varepsilon$ or $w \neq \varepsilon$ and $\sqrt{w}$ is unbordered.

Lemma 3.5. *Let $z \in A^+$ be an almost unbordered word, $l = \sqrt{z}$, and let $x, y \in A^*$. Then $xz = zy$ if and only if at least one (and then just one) of the following cases takes place:*

(1) $x = y = \varepsilon$;

(2) $\sqrt{x} = \sqrt{y} = l$ *(then, of course, $x = y$);*

(3) *there exists $u \in A^+$ such that $\sqrt{x} = zu$, $\sqrt{y} = uz$ and $zu \neq uz$.*

Proof. We prove only the direct implication, the other one is obvious. If $x = y = \varepsilon$, there is nothing to prove. Suppose that x and y are both nonempty. By Lemma 2.2, $x = (t_1t_2)^r$, $y = (t_2t_1)^r$, and $z = (t_1t_2)^s t_1$ for some numbers $r \in \mathbb{N}_+$, $s \in \mathbb{N}$ and words $t_1, t_2 \in A^*$, $t_2 \neq \varepsilon$ such that t_1t_2 is primitive. Assume that

$t_1t_2 = t_2t_1$ (meaning, since t_1t_2 is primitive, that $t_1 = \varepsilon$). Then $xz = zy$ reduces to $xz = zx$, so by Lemma 2.1, the primitive roots of x, y and z coincide and (2) is true. Suppose, finally, that $t_1t_2 \neq t_2t_1$. Then $t_1 \neq \varepsilon$ and, since l is unbordered, we have $s = 0$. Clearly, $z = t_1$, $t_1t_2 = zt_2$ and $t_2t_1 = t_2z$, so (3) is valid. The proof is now complete. □

Corollary 3.6. *Let $x, y, z \in A^+$ be words, z unbordered. Then $xz = zy$ holds if and only if there exists a word w such that $x = zw$ and $y = wz$.*

Lemma 3.7. *Let $z \in A^+$ be an almost unbordered word, $l = \sqrt{z}$, and let $x, y \in A^*$. Then $xzy = yzx$ if and only if at least one (and then just one) of the following cases takes place:*

(1) $x = y$;

(2) $\sqrt{x} = \sqrt{y} = l$, *i.e., x and y commute;*

(3) *there exists $u \in A^+$ and $r, s \in \mathbb{N}_+$, $r \neq s$, such that uz is primitive, $x = (uz)^r u$ and $y = (uz)^s u$.*

Proof. We prove only the direct implication, the other one is obvious. If $x = y$, then (1) holds trivially. Assume $x \neq y$. Suppose, without loss of generality, that $|x| > |y|$. Then $x = yp = qy$ for some nonempty words p and q. The equality $xzy = yzx$ implies that $pz = zq$. We now apply Lemma 3.5. Since p and q are nonempty, either p and q have a common primitive root l or there exist $u \in A^+$ such that the primitive root of p is zu, the primitive root of q is uz and $zu \neq uz$. In the former case there exist m, n $\in \mathbb{N}$, $m \neq n$, such that $x = l^m$ and $y = l^n$, i.e., (2) is true. In the latter case $x = y(zu)^k = (uz)^k y$ for some $k \in \mathbb{N}_+$. By Lemma 2.2, $y = (uz)^s u$ for some $s \in \mathbb{N}$. Then $x = (uz)^{k+s} u$ and (3) holds since $k > 0$. The proof is now complete. □

Lemma 3.8. *Let $z \in A^+$ be an almost unbordered word, $l = \sqrt{z}$, and let $x, y \in A^*$. Then $xyz = zyx$ if and only if at least one (and then just one) of the following cases takes place:*

(1) $xy = yx = \varepsilon$;

(2) $\sqrt{x} = \sqrt{y} = l$;

(3) *there exist $u \in A^+$ and $r, s \in \mathbb{N}$ such that uz and zu are primitive $x = (zu)^r z$, $y = (uz)^s u$* and *$zu \neq uz$.*

Proof. We apply Lemma 3.5. Then

1. either $xy = yx = \varepsilon$; or
2. $\sqrt{xy} = \sqrt{yx} = l$ (implying of course that $xy = yx$), or
3. there exists $u \in A^+$ such that $\sqrt{xy} = zu$, $\sqrt{yx} =$ uz and $zu \neq uz$.

In the first case there is nothing to prove. Consider the second case. Clearly, there exist $m, n \in \mathbb{N}$ such that $x = l^m$ and $y = l^n$, so (ii) is valid. Finally, assume that 3. holds. Then there exists $k \in \mathbb{N}_+$ such that $xy = (zu)^k$ and $yx = (uz)^k$. Since

$uz \neq zu$, both x and y are nonempty. We have $xyx = (zu)^k x = x(uz)^k$ and $yxy = (uz)^k y = y(zu)^k$, so by Lemma 2.2, there exist $r, s \in \mathbb{N}$, $r + s = k$ such that $x = (zu)^r z$ and $y = (uz)^s u$. Obviously (3) is satisfied, so we are done. □

Now, let $z, p, q, u, v \in A^*$ be words such that z is unbordered and nonempty and the equality

$$pzq = uzv \tag{1}$$

is true. We wish to express u and v by means of z. Three cases arise: 1° $|p| = |u|$, 2° $|p| > |u|$, 3° $|p| < |u|$. In the first case, it is clear that $p = u$ does not necessarily depend at all on z.

Case 2° $|p| > |u|$. Let x and y be words such that $p = ux$ and $v = yq$. Then the equality (1) reduces to

$$xz = zy \tag{2}$$

which, by Lemma 3.5, has the solutions $x = (zw)^n$, $y = (wz)^n$ where the parameter $n \in \mathbb{N}_+$ and $w \in A^*$ can be chosen freely so that wz is primitive, the choice $w = \varepsilon$ being quite possible. Recall also that a word is primitive if and only if any conjugate of it is primitive. The parameters p, q, u, v of (1) in the case 2° are restricted by $p = u(zw)^n$, $v = (wz)^n q$ where $n \in \mathbb{N}_+$ and $u, q, w \in A^*$ can be chosen freely as long as wz is primitive.

The case 3° $|p| < |u|$ is analogous to 2°, only the roles of p and u (q and v, resp.) are interchanged. Thus $u = p(zw)^n$, $q = (wz)^n v$ where $n \in \mathbb{N}_+$ and $p, v, w \in A^*$ can be freely chosen so that wz is primitive.

Assume now that (1) holds. Let $t \in A^*$ be a word such that

$$ptq = utv \tag{3}$$

is true. What can we say about t? In the case 1° $|p| = |u|$ again not necessarily much. In the case 2° $|p| > |u|$ and 3° $|p| < |u|$ we are lead to the equality

$$xt = ty \tag{4}$$

which, in the case 2°, allows us to deduce that

$$(zw)^n t = t(wz)^n \tag{5}$$

where $n \in \mathbb{N}_+$ and $w \in A^*$ is such that zw is primitive. By Lemma 2.2, $t = (zw)^m z$, where $m \in N$. We have established the following result:

Theorem 3.9. *Let $z, u, v, p, q \in A^*$ be words such that $z \neq \varepsilon$ is unbordered and $pzq = uzv$ holds. Assume furthermore that $t \in A^*$. Then $utv = ptq$ if and only if at least one (and then just one) of the following conditions takes place:*

(1) *$|u| = |p|$;*

(2) *$p = u(zw)^n$ $(|p| > |u|)$, $t = (zw)^m z$, and $v = (wz)^n q$ where $m \in \mathbb{N}$, $n \in \mathbb{N}_+$ and $u, q, w \in A^*$ are such that zw is primitive;*

(3) $u = p(zw)^n\ (|p| < |u|), t = (zw)^m z$, *and* $q = (wz)^n v$ *where* $m \in \mathbb{N}, n \in \mathbb{N}_+$ *and* $u, q, w \in A^*$ *are such that* zw *is primitive.*

Let $z, u, v, w \in A^*$ be words such that $z \neq \varepsilon$ is unbordered and the equation

$$uvz = zvw \tag{6}$$

is true. We wish to describe u, v, w similarly as in the preceding theorem. We will use Lemma 3.5, which leads to three cases: 1° $uv = vw = \varepsilon$, 2° $\sqrt{uv} = \sqrt{vw} = l$, 3° there exists $p \in A^+$ such that $\sqrt{uv} = zp$, $\sqrt{vw} = pz$ and $zp \neq pz$.

The first case immediately gives $u = v = w = \varepsilon$.

The case 2° may be further divided. If $u = w = \varepsilon$ we obtain $\sqrt{v} = z$. If $u \neq \varepsilon \neq w$ then $uv = vw$ and, according to Lemma 2.2, there exist words $t_1, t_2 \in A^*$, $t_2 \neq \varepsilon$ such that $u = (t_1t_2)^s$, $w = (t_2t_1)^s$, $v = (t_1t_2)^r t_1$, $s \geq 1$, $r \geq 0$ and $t_1t_2\ (t_2t_1)$ is primitive. If $t_1 \neq \varepsilon$ then, since t_1 is both prefix and suffix of $uv = vw$ and z is unbordered, $\sqrt{t_1} = z$. Then $\sqrt{t_2} = z$ also, and we obtain a contradiction with t_1t_2 being primitive. Thus $t_1 = \varepsilon$ and $t_2 = z$. Hence $\sqrt{u} = \sqrt{w} = z$, which means, by length argument, that $u = w$ and either $v = \varepsilon$ or $\sqrt{v} = z$.

In the case 3°, there exists $m \geq 1$ such that $uv = (zp)^m$ and $vw = (pz)^m$. If $|u| = |z|\ (= |w|)$ then $u = w = z$ and v may be arbitrary word from A^*. If $|u| < |z|$ then $z = uz' = z''w$, where z' is a suffix of z and z'' is a prefix of z, $z' \neq \varepsilon \neq z''$. Hence $uvz''w = uz'vw$, $vz'' = z'v$ and z', z'' are conjugate, a contradiction. If $|u| > |z|$ then $u = zu'$, $w = w'z$ and $zu'vz = zvw'z$. Thus $u'v = vw'$ and according to Lemma 2.2 there exist $p, q \in A^*$, $p \neq \varepsilon$ such that $u' = pq$, $w' = qp$ and $v = p(qp)^n$ for some $n \geq 0$,

We have established the following result:

Theorem 3.10. *Let* $z, u, v, w \in A^*$ *be words such that* $z \neq \varepsilon$ *is unbordered. Then* $uvz = zvw$ *if and only if at least one (and then just one) of the following conditions takes place:*

(1) $u = w = z^m$, $v = z^n, m, n \geq 0$;

(2) $u = w = z$, $\sqrt{v} \neq z$;

(3) *there exist* $p, q \in A^*$, $p \neq \varepsilon$, *such that* $\sqrt{pq} \neq z$ *and* $u = zpq$, $w = qpz$, $v = p(qp)^n$, $n \geq 0$.

4. Basic facts about separated pairs of words

An ordered pair (u, v) of words $u, v \in A^*$ is called *overlapping* if there exist words $x \in A^+$ and $y, z \in A^*$, $yz \neq \varepsilon$, such that $u = yx$ and $v = xz$. The pair (u, v) is *separated* (or *non-overlapping*) if it is not overlapping. A separated pair of words can be characterized in several ways:

Lemma 4.1. *Let $u, v \in A^*$. The following conditions are equivalent for the ordered pair of words (u, v):*

(i) *the pair (u, v) is separated.*

(ii) *if $r, s \in A^*$ and $t \in A^+$ are such that $u = rt$ and $v = ts$, then $r = s = \varepsilon$ (and hence $u = v$).*

(iii) *if $p, q \in A^*$ are such that $up = qv$, then either $|u| \leq |q|$ and $|v| \leq |p|$ or $p = q = \varepsilon$ (and hence $u = v$).*

Proof. Suppose that (u, v) is overlapping. Then $u = yx$ and $v = xz$ for some $x \in A^+$ and $y, z \in A^*$ such that $yz \neq \varepsilon$. Certainly (ii) does not hold. Now $uz = yv$ and either $|u| > |y|$ or $|v| > |z|$ (since yz is nonempty), so (iii) is not true either. On the other hand, if (ii) is not valid, then (u, v) is certainly overlapping. Suppose finally that (iii) is not true. Then $up = qv$ for some $p, q \in A^*$ such that $pq \neq \varepsilon$ and either $|u| > |q|$ or $|v| > |p|$. Assume, without loss of generality, that $|u| > |q|$. Certainly $u = qx$ and $v = xp$ for some nonempty word x, implying (since $pq \neq \varepsilon$) that the pair (u, v) is overlapping. □

From Lemma 3.2, for any word $w \in A^*$, the pair (w, w) is overlapping if and only if w is bordered. As well, the pairs (ε, w) and (w, ε) *are separated for each* $w \in A^*$.

An ordered pair (u, v) of words $u, v \in A^*$ will be called *left (right, resp.) strongly separated* if it is separated and either u (resp. v) is not a factor of v (resp. u) or $u = v$ or $u = \varepsilon$ ($v = \varepsilon$, resp.). The pair will be called *stronlgy separated* if it is both left and right strongly separated.

The above definitions imply straightforwardly:

Lemma 4.2. *The following conditions are equivalent for each word $u \in A^*$:*

(i) *the pair (u, u) is separated;*

(ii) *the pair (u, u) is left strongly separated;*

(iii) *the pair (u, u) is right strongly separated;*

(iv) *the pair (u, u) is strongly separated;*

(v) *the word u is unbordered.*

Certainly the pairs (ε, w) and (w, ε) are strongly separated for each word $w \in A^*$. Also the following lemma is easily verified.

Lemma 4.3. *Let $u, v \in A^*$ be distinct words of equal length, i.e., words such that $u \neq v$ and $|u| = |v|$. Then the following conditions are equivalent:*

(i) *the pair (u, v) is separated;*

(ii) *the pair (u, v) is left strongly separated;*

(iii) *the pair (u, v) is right strongly separated; and*

(iv) *the pair (u, v) is strongly separated.*

Lemma 4.4. *Let $u, v \in A^*$ be such that $u \neq v$. Then the following conditions are equivalent:*

(i) *the pairs (u, v), (v, u) are left strongly separated;*

(ii) *the pairs* (u, v), (v, u) *are right strongly separated;*
(iii) *the pairs* (u, v), (v, u) *are strongly separated;*
(iv) *for each* $w \in A^*$, *if both* u *and* v *are factors of* w, *then* $|u| + |v| \leq |w|$.

Proof. It is easy to see that (i), (ii) and (iii) are pairwise equivalent. The lemma is certainly true if either $u = \varepsilon$ or $v = \varepsilon$, so assume that both u and v are nonempty.

Let us show that (iii) implies (iv). Let $w, p, q, y, z \in A^*$ be words such that $w = puq = yvz$. Since (u, v) is strongly separated, $u \neq v$ and u, v are nonempty, the above occurrences of u and v in w have to be totally separate. This means that either $|p| \geq |yv|$ or $|z| \geq |uq|$. In both cases, $|u| + |v| \leq |w|$ and (iv) is true.

We prove finally that (iv) implies (iii). Surely neither u is a subword of v nor vice versa. Let $p, q \in A^*$ be such thhat $up = qv$. By our assumption, $|up| = |qv| \geq |u| + |v|$. Certainly, $|p| \geq |v|$ and $|q| \geq |u|$. By Lemma 4.1 (iii), the pair (u, v) is separated. Thus (u, v) is strongly separated. □

Lemma 4.5. *Let* $(u, v) \in A^* \times A^*$ *be a separated pair of words such that* $u \neq v$. *Then there do not exist nonempty conjugate words* x *and* y *such that* x *is a suffix of* u *and* y *is a prefix of* v.

Proof. Assume, on the contrary, that $u = px$ and $v = yq$ for some nonempty conjugate words x and y. By Lemma 2.2, there exist words z and w such that $x = zw$, $y = wz$, $u = pzw$ and $y = wzq$. This is a contradiction. □

Corollary 4.6. *Let* $(u, v) \in A^* \times A^*$ *be a separated pair of words such that* $u \neq v$. *Then, for* $p, q, x, y \in A^*$, *the equalities* $u = pxy$ *and* $v = yxq$ *hold if and only if* $u = p$, $v = q$ *and* $x = y = \varepsilon$.

Proof. The direct implication is true by the previous lemma. The reverse implication is clear. □

Lemma 4.7. *Let* $(u, v) \in A^* \times A^*$ *be a separated pair of words such that* $u \neq v$. *If* $x, y, z \in A^*$ *then* $uzx = yzv$ *if and only if at least one (and then just one) of the following conditions takes place:*
(1) $x = v$ *and* $y = u$;
(2) $x = t^m v$, $y = ut^m$, $z = t^n$, $t \neq \varepsilon$, $m, n \in \mathbb{N}$, $r > 0$;
(3) $x = (pq)^r v$, $y = u(qp)^r$, $z = (qp)^s q$, $r, s \in \mathbb{N}$, $r > 0$, $q \neq \varepsilon \neq p$.

Proof. We will prove first that u is a prefix of y and v is a suffix of x. Assume that the claim does not hold, and, without loss of generality, that $u = yd$ where $d \in A^+$. Certainly, $|d| \leq |z|$, otherwise (u, v) is not separated. Then $z = dt$ for some $t \in A^*$ and $dtx = tv$. Obviously, there exists $p \in A^*$ such that $dt = tp$. We note that d and p are conjugate (and nonempty) and $v = px$. Since $u = yd$ we get a contradiction with Lemma 4.5.

Now, there exist $x', y' \in A^*$ such that $x = x'v$ and $y = uy'$. Hence $uzx'v = uy'zv$ and $zx' = y'z$. Either $x' = y' = \varepsilon$, which leads to case (1) or, according to Lemma 2.2 there exist words $t_1, t_2 \in A^*$, $t_2 \neq \varepsilon$, such that $t_1 t_2$ is primitive, and numbers $r, s \in \mathbb{N}$, $r > 0$, satisfying $y' = (t_1t_2)^r$, $x' = (t_2t_1)^r$ and $z = (t_1t_2)^s t_1$. If $t_1 = \varepsilon$ then $x' = y'$ and case (2) takes place. If $t_1 \neq \varepsilon$, then case (3) takes place. $\square$

Lemma 4.8. *Let $(u, v) \in A^* \times A^*$ be a separated pair of words such that $u \neq v$. Then $xuy \neq yvx$ for all $x, y \in A^*$.*

Proof. Assume, contrarywise, that there exist words $x, y \in A^*$ for which $xuy = yvx$. If $|x| = |y|$, then $x = y$ and $u = v$, a contradiction. Assume, without loss of generality, that $|x| > |y|$. Then there exist nonempty words p and q such that $x = yq = py$. Now, by Lemma 2.2, there exist words $t_1, t_2 \in A^*$, $t_2 \neq \varepsilon$, such that t_1t_2 is a primitive word, and numbers $m, n \in \mathbb{N}$, $m > 0$, satisfying $p = (t_1t_2)^m$, $q = (t_2t_1)^m$ and $y = (t_1t_2)^n t_1$. Obviously, $xuy = yvx$ implies $(t_1t_2)^{m+n} t_1 u (t_1t_2)^n t_1 = (t_1t_2)^n t_1 v (t_1t_2)^{m+n} t_1$. Then $(t_1t_2)^m u = v (t_1t_2)^m$ meaning that u and v are conjugate. Since (distinct) conjugate words cannot form a separated pair, we have a contradiction. $\square$

Lemma 4.9. *Let $(u, v) \in A^* \times A^*$ be a separated pair of words such that $u \neq v$. Then $uxy \neq yxv$ for all $x, y \in A^*$.*

Proof. Let, on the contrary, $uxy = yxv$. According to Lemma 4.7, u is a prefix of y and v is a suffix of y. Thus $y = uy'v$, since the pair (u, v) is separated. But then $uxuy'v = uy'vxv$ and $xuy' = y'vx$, which is a contradiction with Lemma 4.8. $\square$

Theorem 4.10. *Let $u, v \in A^*$, $u \neq v$, be words such that pairs (u, v) and (v, u) are separated. Assume furthermore that $d, t, x, y \in A^*$ are words for which the equality*

$$dut = xvy \tag{7}$$

is true. Then $dwt \neq xwy$ for each $w \in A^*$.

Proof. Assume, countratywise, that $w \in A^*$ is such that $dwt = xwy$. Since $u \neq v$, both (u, v) and (v, u) are separated, and (7) holds, the exposed occurrences of u in dut and v in xvy have to be totally separated. This implies that either $|d| \geq |xv|$ or $|x| \geq |du|$. Assume, without loss of generality, that $|d| \geq |xv|$. Let $y_1 \in A^*$ be such that $d = xvy_1$. The equality (7) implies that $y = y_1ut$. Now $dwt = xwy$ allows us to deduce that $vy_1w = wy_1u$. Since (v, u) is separated and $u \neq v$, the word w must be of the form $w = vpu$, where $p \in A^*$. Substituting vpu for w in $vy_1w = wy_1u$ gives $y_1vp = puy_1$. This is a contradiction with Lemma 4.8. $\square$

5. Separating sets of words

A set $Z \subseteq A^*$ is called *separating (strongly separating)* if all ordered pairs from $Z \times Z$ are separated (strongly separated, resp.). The definition of a strongly (left or right) separated pair of words implies straightforwardly:

Lemma 5.1. *Let $Z \subseteq A^*$. Then*

(i) *the set is strongly separating if and only if every pair in $Z \times Z$ is left strongly separated;*

(ii) *the set Z is strongly separating if and only if every pair in $Z \times Z$ is right strongly separated;*

(iii) *if Z is a separating set, then every word from Z is unbordered;*

(iv) *if Z is a separating set (strongly separating set, resp.), then $Z \cup \{\varepsilon\}$ is a separating set (strongly separating set, resp.).*

Applying Axiom of Choice (i.e., Zorn Lemma) we see that each separating (strongly separating, resp.) set is contained in a maximal separating (strongly separating, resp.) set. This can be seen for instance as follows. Consider a separating set $Z \subseteq A^*$. Let $Z_0 = Z$ and

$$U_0 = \{w \in A^* \setminus Z_0 \mid \forall\, z \in Z_0 : (z,w) \text{ and } (w,z) \text{ are separated}\}.$$

Let $k \in \mathbb{N}$ and assume that Z_k and U_k are given. Let $w_k \in U_k$ be the minimal element with respect to lexicographical order (assuming that A is well ordered). Let $Z_{k+1} = Z_k \cup \{w_k\}$ and

$$U_{k+1} = \{w \in A^* \setminus Z_{k+1} \mid \forall\, z \in Z_{k+1} : (z,w) \text{ and } (w,z) \text{ are separated}\}.$$

Obviously, $\lim_{n\to\infty} Z_n$ is a maximal separating set.

A (strongly) separating set Z will be called *almost maximal* if $Z \cup \{\varepsilon\}$ is maximal (see Lemma 5.1 (iv)).

Example 5.2.

(i) The empty set $\emptyset$ and the one-element set $\{\varepsilon\}$ are strongly separating.

(ii) The set A of variables is an almost maximal strongly separating set.

Example 5.3.

(i) If $A = \emptyset$, then $\emptyset$ and $\{\varepsilon\}$ are the only separating sets and they are strongly separating.

(ii) Let $A = \{a\}$ be a one-element set. Then the sets $\emptyset$, $\{a^m\}$, $\{a^m, \varepsilon\}, m \geq 0$, are the only separating sets and all these sets are strongly separating.

(iii) Let $A = \{a,b\}$ be a two-element set. Then the sets $\{ab\}$, $\{a,b\}$, $\{a^2(ba)^i b^2, a^2(ba)^m b \mid 0 \leq i < m\} \geq 1$, $\{a^2(ba)^i b^2 \mid i \geq 0\}$ are almost maximal strongly separating sets.

6. Reduced and meagre words

Let us now consider the (number of) occurrences of one word in another. For all $w, z \in A^*$, let $\mathrm{Tr}(w,z) = \{(u,z,v) \mid u,v \in A^*,\ w = uzv\}$ and $\mathrm{tr}(w,z) = |\mathrm{Tr}(w,z)|$.

Let $w, z \in A^*$ Certainly if $|w| < |z|$, then $\mathrm{Tr}(w,z) = \emptyset$ and $\mathrm{tr}(w,z) = 0$. On the other hand, if $|w| \geq |z|$, then $\mathrm{Tr}(w,z)$ may be nonempty; the upper bound $tr(w,z) \leq |w| - |z| + 1$ is easily verified. As a special case $\mathrm{tr}(w,\varepsilon) = |w| + 1$.

We generalize the functions Tr and tr as follows. For any $w \in A^*$ and any set $S \subseteq A^*$ of words, let $\mathrm{Tr}(w,S) = \bigcup_{z\in S} \mathrm{Tr}(w,z)$ and $\mathrm{tr}(w,S) = \sum_{z\in S} \mathrm{tr}(w,z)$.

A word w is *S-reduced if* $\mathrm{tr}(w,S) = 0$ and *S-meagre* if $\mathrm{tr}(w,S) \leq 1$. When S is clear we use the terms *reduced* and *meagre*, respectively. Certainly, if $S = \emptyset$, then every word is reduced. Contrarywise, when $\varepsilon \in S$, then no word is reduced and ε is the only meagre word. On the other hand, if $S = A$, then ε is the only reduced word and $A \cup \{\varepsilon\}$ is the set of all meagre words.

Assume now that $Z \subseteq A^+$ is strongly separating. Clearly, each word in Z is Z-meagre; for each $z \in Z$, the total number of occurrences of the words from Z in z is one.

Lemma 6.1. *Let $p, q, x, y \in A^*$ and $z_1, z_2 \in Z$ be words such that $pz_1q = xz_2y$. If p and x (q and y, resp.) are reduced, then $p = x$, $q = y$ and $z_1 = z_2$.*

Proof. Assume without loss of generality that p and x are reduced. We first show that $p = x$. Assume, contrarywise, that $|p| > |x|$, the case $|p| < |x|$ being shown in a similar manner. Now, since Z is strongly separating, $p = xz_2w$ for some word w. This contradicts the fact that p is reduced. Thus we deduce that $p = x$. Again, since Z is strongly separating, the words z_1 and z_2 are equal. This finally implies that $q = y$ and we are done. □

Lemma 6.2. *Let $p, q, x, y \in A^*$ and $z \in Z$ be words such that x and y are reduced and $xy = pzq$. Then there are words $u, v \in A^+$ such that $x = pu$, $y = vq$ and $z = uv$. Moreover, both p and q are reduced and $|z| \geq 2$.*

Proof. If $|x| \leq |p|$, then $p = xt$ for some $t \in A^*$, and so $y = tzq$. Obviously, y is not reduced, a contradiction. Assume thus that $|p| < |x|$, so $x = pu$, where u is a nonempty word. Analogously, we may show that $y = vq$ for some word $v \neq \varepsilon$. Certainly $z = uv$ and since u and v are nonempty, the length of z is at least two. As a factor of x (y, resp.) the word p (q, resp.) is reduced. □

Suppose that the words u and v are reduced and uv is not. Then there exists exactly one word $z \in Z$ such that $z = xy$ for some nonempty suffix x of u and nonempty prefix y of v Since Z is strongly separating, the words z, x and y are uniquely determined.

Lemma 6.3. *Let $w \in A^*$. There exist $m \in \mathbb{N}$, reduced words $x_0, x_1, \ldots, x_m \in A^*$ and $z_1, z_2, \ldots, z_m \in Z$ such that $w = x_0z_1x_1z_2x_2 \ldots z_mx_m$.*

Proof. We proceed by induction on $|w|$. The result is clear for reduced or meagre w, so the basic step of the induction is easily verified. In the general case the remark preceding this lemma is applied. □

Proposition 6.4. *Let $Z \subseteq A^+$ be a strongly separating set. For each $w \in W$ there exist uniquely determined $m \in \mathbb{N}$, reduced $x_0, x_1, \ldots, x_m \in A^*$ and $z_1, z_2, \ldots, z_m \in Z$ such that $w = x_0 z_1 x_1 z_2 x_2 \ldots z_m x_m$. Moreover,*

$$\mathrm{Tr}(w,Z) = \{(x_0, z_1, x_1 z_2 x_2 \ldots z_m x_m), (x_0 z_1 x_1, z_2, x_2 z_3 x_3 \ldots z_m x_m), \ldots (x_0 z_1 x_1 \ldots z_{m-1} x_{m-1}, z_m, x_m)\}$$

and $\mathrm{tr}(w,Z) = m$.

Proof. The existence of the decomposition is shown in Lemma 6.3. The uniqueness follows from Lemma 6.2 by induction on $|w|$. □

7. The replacement relation

We wish to study certain types of string rewriting (or reduction) systems, in particular those, where the production rules are such that the words x on the left hand side of the rules $x \to y$ form a (strongly) separating set. For the sake of completeness we start the considerations from the very beginning, binary relations on the free monoid A^*.

Call a binary relation α on A^* *stable*, if $(x,y) \in \alpha$ implies $(uxv, uyv) \in \alpha$ for all $u, v \in A^*$.

For each $z, t \in A^*$ let $\varrho_{z,t}$ be the binary relation on A^* defined by $\varrho_{z,t} = \{(uzv, utv) \mid u, v \in A^*\}$ Let $\lambda_{z,t}$ be the reflexive closure of $\varrho_{z,t}$, $\lambda_{z,t} = \varrho_{z,t} \cup \mathrm{id}_{A^*}$. Obviously $\varrho_{z,t}$ is the stable closure of the one element relation (z,t) and $\lambda_{z,t}$ is the reflexive stable closure of (z,t).

Let $Z \subseteq A^*$ and $\psi : Z \to A^*$ be a function. Define the relation $\varrho_{Z,\psi}$ by $\varrho_{Z,\psi} = \bigcup_{z \in Z} \varrho_{z,\psi(z)}$. Let $\lambda_{Z,\psi}$ be the reflexive closure of $\varrho_{Z,\psi}$. Certainly, both $\varrho_{Z,\psi}$ and $\lambda_{Z,\psi}$ are stable.

Recall that a binary relation ξ over a set X is irreflexive if $(x,x) \notin \xi$ for all $x \in X$. Again, one easily sees that the relation $\varrho_{Z,\psi}$ is irreflexive if and only if $\psi(z) \neq z$ for each $z \in Z$.

Lemma 7.1. *Let $Z \subseteq A^*$ and let $\psi : Z \to A^*$ be a function. Then*
(i) $|\{x \in A^* \mid (w,x) \in \varrho_{Z,\psi}\}| \leq \mathrm{tr}(w,Z)$;
(ii) $|\{x \in A^* \mid (w,x) \in \lambda_{Z,\psi}\}| \leq \mathrm{tr}(w,Z) + 1$.

Proof. The definition above and the definition of $tr(w,Z)$ imply the claims straightforwardly. □

The result below is also a consequence of the preceding definitions.

Lemma 7.2. *Let $Z \subseteq A^*$ and let $\psi : Z \to A^*$ be a function. For each $w \in A^*$, the following conditions are equivalent.*
(i) *w is Z-reduced*

(ii) *for each* $x \in A^*$, (w,x) *is not in* $\varrho_{Z,\psi}$;
(iii) *for each* $y \in A^*$, $(w,y) \in \lambda_{Z,\psi}$ *implies* $y = w$.

Recall that a binary relation ξ relation over a set X is *antisymmetric* if the condition (x,y), $(y,x) \in \xi$ implies $x = y$ for each $x, y \in X$.

Lemma 7.3. *Let* $Z \subseteq A^*$ *and let* $\psi : Z \to A^*$ *be a function. The following conditions are equivalent.*

(i) $\varrho_{Z,\psi}$ *is antisymmetric;*
(ii) $\lambda_{Z,\psi}$ *is antisymmetric;*
(iii) $\psi(z_1) = z_1$ *and* $\psi(z_2) = z_2$ *whenever* $x, y, w \in A^*$ *and* $z_1, z_2 \in Z$ *are such that* $xz_1y = \psi(z_2)w$ *and* $x\psi(z_1)y = z_2w$.

Proof. Certainly (i) and (ii) are equivalent. Assume that $\varrho_{Z,\psi}$ is antisymmetric and let $x, y, w \in A^*$ and $z_1, z_2 \in Z$ be such that $xz_1y = \psi(z_2)w$ and $x\psi(z_1)y = z_2w$. Surely, $(xz_1y, x\psi(z_1)y), (z_2w, \psi(z_2)w) \in \varrho_{Z,\psi}$. Since $\varrho_{Z,\psi}$ is antisymmetric, we have $xz_1y = x\psi(z_1)y$ and $z_2w = \psi(z_2)w$ implying that $\psi(z_1) = z_1$ and $\psi(z_2) = z_2$. Thus (i) $\Rightarrow$ (iii).

Assume that (iii) holds. Let $u, v \in A^*$ be such that (u,v) and (v,u) are both in $\varrho_{Z,\psi}$. Then there exist $x, y, x', y' \in A^*$ and $z_1, z_2 \in Z$ such that $u = xz_1y$, $v = x\psi(z_1)y$, $v = x'z_2y'$ and $u = x'\psi(z_2)y'$. Suppose that $|x'| \geq |x|$, the case $|x'| < |x|$ being treated in a similar way. There exists $p \in A^*$ such that $x' = xp$. Then $pz_2y' = \psi(z_1)y$ and $z_1y = p\psi(z_2)y'$, so by (iii), $\psi(z_1) = z_1$ and $\psi(z_2) = z_2$ implying that $u = v$. □

Let $X, Y \subseteq A^*$ and let $f : X \to Y$ be a function. Then f is *length-increasing (strictly length-increasing*, resp.) if $|x| \leq |f(x)|$ ($|x| < |f(x)|$, resp.) for each $x \in X$. The function f is *length-decreasing* (*strictly length-decreasing*, resp.) if $|x| \geq |f(x)|$ ($|x| > |f(x)|$, resp.) for each $x \in X$.

Let us state some simple results concerning strictly length-increasing (strictly length-descreasing, resp.) functions ψ and relations $\varrho_{Z,\psi}$ and $\lambda_{Z,\psi}$.

Lemma 7.4. *Let* $Z \subseteq A^*$ *and let* $\psi : Z \to A^*$ *be a strictly length-increasing (strictly length-decreasing, resp.) function. Then*

(i) ϱ *is irreflexive and antisymmetric.*
(ii) λ *is reflexive and antisymmetric.*
(iii) $|x| < |w|$ ($|x| > |w|$, *resp.*) *for each* $(x,w) \in \varrho_{Z,\psi}$.
(iv) $|x| \leq |w|$ ($|x| \geq |w|$, *resp.*) *for each* $(x,w) \in \lambda_{Z,\psi}$.

A word $w \in A^*$ is *almost* $((Z,\psi)-)$ *reduced* if $x = w$ whenever $(w,x) \in \varrho_{Z,\psi}$. The following lemma is a direct consequence of the definition.

Lemma 7.5. *Let* $Z \subseteq A^*$ *and let* $\psi : Z \to A^*$ *be a function. Then*

(i) *a word* $w \in A^*$ *is almost reduced if and only if* $\psi(z) = z$ *for all* $z \in Z$ *such that* z *is a factor of* w;
(ii) *if* $\psi(z) \neq z$ *for all* $z \in Z$, *then each almost reduced word is reduced.*

We now turn our attention to strongly separating sets.

Lemma 7.6. *Let $Z \subseteq A^+$ be a strongly separating set and let $\psi : Z \to A^*$ be a function. Then for each $(u, v) \in \varrho_{Z,\psi}$*

(i) $\operatorname{tr}(u, Z) \leq \operatorname{tr}(v, Z) + 1$;

(ii) *if v is reduced, then u is meagre;*

(iii) *if either $|\psi(z)| \leq 2$ or $\psi(z)$ is reduced for every $z \in Z$, then* $\operatorname{tr}(v, Z) \leq$ $\leq \operatorname{tr}(u, Z) + 1$;

(iv) *if $|\psi(z)| \leq 1$ for every $z \in Z$, then* $\operatorname{tr}(v, Z) \leq \operatorname{tr}(u, Z)$.

Proof. Let $(u, v) \in \varrho_{Z,\psi}$. Then there exist $x, y \in A^*$ and $z \in Z$ such that $u = xzy$ and $v = x\psi(z)y$. Clearly, z is the only word in Z that exists in u and possibly does not exist in v. By Proposition 6.4, the claim (i) is true as well as (ii). Consider (iii) and assume that either $|\psi(z')| \leq 2$ or $\psi(z')$ is reduced for every $z' \in Z$. If $\psi(z)$ is reduced, then u is meagre by the preceding case. If, on the other hand, $|\psi(z)| \leq 2$, then the substitution of $\psi(z)$ for z in u produces to v at most two new occurrences of words from Z. Since in the substitution one occurrence of z vanishes, the claim $\operatorname{tr}(v, Z) \leq \operatorname{tr}(u, Z) + 1$ holds. Using an analogous reasoning, (iv) is true. □

Lemma 7.7. *Let $Z \subseteq A^*$ be a strongly separating set and let $\psi : Z \to A^*$ be a function. Assume furthermore that $p, q, x, y \in A^*$ and $z \in Z$ are words such that $pzq = xzy$ and $p\psi(z)q \neq x\psi(z)y$. Then*

(i) $(pzq, p\psi(z)q), (xzy, x\psi(z)y) \in \varrho_{z,\psi(z)}$;

(ii) *there exists $w \in A^*$ such that $(p\psi(z)q, w)$ and $(x\psi(z)y, w)$ are both in $\varrho_{z,\psi(z)}$;*

(iii) *if $w \in A^*$ is such that $(p\psi(z)q, w)$ and $(x\psi(z)y, w)$ are both in $\varrho_{z,\psi(z)}$, then $w \neq p\psi(z)q$ and $w \neq x\psi(z)y$.*

Proof. Recall the definition: $\varrho_{z,\psi(z)} = \{(xzy, x\psi(z)y) \mid x, y \in A^*\}$. Trivially, (i) is true. Since $\psi(z) \neq z$ (otherwise $p\psi(z)q = pzq = xzy = x\psi(z)y$, a contradiction), (iii) is true as well.

Consider (ii). Since $(pzq, p\psi(z)q)$ and $(xzy, x\psi(z)y)$ are in $\varrho_{z,\psi(z)}$, $p\psi(z)q \neq$ $\neq x\psi(z)y$, and Z is strongly separating, the word $pzq = xzy$ is necessarily of the form $y_1zy_2zy_3$ for some words $y_1, y_2, y_3 \in A^*$, where

$$\{p\psi(z)q, x\psi(z)y\} = \{y_1\psi(z)y_2zy_3, y_1zy_2\psi(z)y_3\}.$$

Then, choosing $w = y_1\psi(z)y_2\psi(z)y_3$, it is clear that (ii) holds. □

Lemma 7.8. *Let $Z \subseteq A^+$ be a strongly separating set and let $\psi : Z \to A^*$ be a function. Assume furthermore that $p, q, x, y \in A^*$ and $z_1, z_2 \in Z$, $z_1 \neq z_2$, are such that $pz_1q = xz_2y$. Then*

(i) $(pz_1q, p\psi(z_1)q) \in \varrho_{z_1,\psi(z_1)}$, $(xz_2y, x\psi(z_2)y) \in \varrho_{z_2,\psi(z_2)}$;

(ii) *there exists $w \in A^*$ such that $(p\psi(z_1)q, w) \in \varrho_{z_2,\psi(z_2)}$ and $(x\psi(z_2)y, w) \in$ $\in \varrho_{z_1,\psi(z_1)}$;*

(iii) *if* $w \in A^*$ *is such that* $(p\psi(z_1)q, w)$ *is in* $\varrho_{z_2,\psi(z_2)}$ *and* $(x\psi(z_2)y, w)$ *is in* $\varrho_{z_1,\psi(z_1)}$, *then* $\psi(z_1) \neq z_1$ *implies that* $w \neq x\psi(z_2)y$ *and* $\psi(z_2) \neq z_2$ *implies that* $w \neq p\psi(z_1)q$.

Proof. The proof is quite analogous to that of 7.7. □

Propositin 7.9. *Let* $Z \subseteq A^*$ *be a strongly separating set and let* $\psi : Z \to A^*$ *be a function. Let furthermore* $u, v, w \in A^*$ *and* $z_1, z_2 \in Z$ *be such that* $(w,u) \in \varrho_{z_1,\psi(z_1)}$, $(w,v) \in \varrho_{z_2,\psi(z_2)}$ *and either* $1°$ $u \neq v$ *and* $z_1 = z_2$ *or* $2°$ z_1 *and* z_2 *are both nonempty and* $z_1 \neq z_2$. *Then there exists* $w' \in A^*$ *such that* $(u, w') \in \varrho_{z_2,\psi(z_2)}$ *and* $(v, w') \in \varrho_{z_1,\psi(z_1)}$. *Moreover, if* $\psi(z_1) \neq z_1$ ($\psi(z_2) \neq z_2$, *resp.*) *or* $z_1 = z_2$, *then* $w' \neq v$ ($w' \neq u$, *resp.*).

Proof. There are $p, q, x, y \in A^*$ such that $w = pz_1q = xz_2y$, $u = p\psi(z_1)q$ and $v = x\psi(z_2)y$. If $z_1 = z_2$, then Lemma 7.7 applies. If $z_1 \neq z_2$, then Lemma 7.8 can be used. □

Remark 7.10. Firstly, notice that Proposition 7.9 follows from Proposition 6.4 in a quite comfortable way. Then, observe that Lemma 7.8 remains true for $z_1 = \varepsilon$, $z_1 \neq z_2$ or $z_2 = \varepsilon$, $z_1 \neq z_2$, provided that either $Z \nsubseteq A \cup \{\varepsilon\}$ or $\psi(\varepsilon) = \varepsilon$ (so that Proposition 7.9 is true as well in this case).

Proposition 7.11. *Let* $Z \subseteq A^*$ *be a strongly separating set and let* $\psi : Z \to A^*$ *be a function. Assume that either* $1°$ $\varepsilon \notin Z$ *or* $2°$ $Z \subseteq A \cup \{\varepsilon\}$ *or* $3°$ $\varepsilon \in Z$ *and* $\psi(\varepsilon) = \varepsilon$. *Then*

(i) *if* $u, v, w \in A^*$ *are such that* $(w,u) \in \varrho_{Z,\psi}$, $(w,v) \in \varrho_{Z,\psi}$ *and* $u \neq v$, *then there exists* $x \in A^*$ *such that* $(u,x) \in \varrho_{Z,\psi}$ *and* $(v,x) \in \varrho_{Z,\psi}$;

(ii) *the relation* $\lambda_{Z,\psi}$ *is upwards confluent (i.e., if* $(w,u) \in \lambda_{Z,\psi}$ *and* $(w,v) \in \lambda_{Z,\psi}$ *then* $(u,x) \in \varrho_{Z,\psi}$ *and* $(v,x) \in \varrho_{Z,\psi}$ *for some* $x \in A^*$).

Proof. Use Proposition 7.9 (and Remark 7.10). □

Example 7.12. Assume that $\{a,b\} \subseteq A$, put $Z = \{\varepsilon, a^2b^2\}$ (clearly, Z is a strongly separating set), $\psi(\varepsilon) = ba$, $\psi(a^2b^2) = b$. Then $(a^2b^2, a^2bab^2) \in \varrho_{\varepsilon,ba}$ and $(a^2b^2, b) \in \varrho_{a^2b^2,b}$. On the other hand, $\{x \mid (a^2bab^2, x) \in \varrho_{a^2b^2,b}\} = \emptyset$ and $\{y \mid (b,y) \in \varrho_{\varepsilon,ba}\} = \{bab, b^2a\}$. Consequently, neither Lemma 7.8 nor Proposition 7.9 remain true in this case.

8. When $\mathrm{tr}(w) = |\{x \mid (w,x) \in \varrho\}|$

In this section, let Z be a strongly separating set of words with $\varepsilon \notin Z$ and let $\psi : Z \to A^*$. For every $w \in A^*$, put $(\mathrm{ts}(w) =)$ $\mathrm{ts}(w, Z, \psi) = |\{x \in A^* \mid (w,x) \in \varrho_{Z,\psi}\}|$. Of course (use Lemma 7.1 (i)), we have $\mathrm{ts}(w) \leq \mathrm{tr}(w)$.

Proposition 8.1. *The following conditions are equivalent:*

(i) $\mathrm{ts}(w) = \mathrm{tr}(w)$ *for every* $w \in A^*$.

(ii) $|\{x \mid (w,x) \in \lambda\}| = \mathrm{tr}(w) + 1$ *for every* $w \in A^*$.

(iii) $\psi(z) \neq \varepsilon$ *for all* $z \in Z$ *and if* $z_1, z_2 \in Z$ *and* $p, q \in A^*$, *then either* $\psi(z_1) \neq$ $\neq z_1pq$ *or* $\psi(z_2) \neq qpz_2$.

Proof. (i) implies (iii). Assume, on the contrary, that $\psi(z_1) = z_1pq$ and $\psi(z_2) = qpz_2$. If $w = z_1pz_2$, then $\mathrm{tr}(w) = \mathrm{tr}(p) + 2$ and $\mathrm{ts}(w) \leq \mathrm{ts}(p) + 1 < \mathrm{tr}(w)$.

(iii) implies (i). Let, on the contrary, $w \in A^*$ be such that $\mathrm{ts}(w) < \mathrm{tr}(w)$. According to Proposition 6.4, $w = r_0z_1r_1z_2r_2 \dots z_mr_m$, $m \geq 0$, $z_i \in Z$, r_i reduced. Now, $\mathrm{tr}(w) = m$, and hence $m \geq 2$ and there are $1 \leq i < j \leq m$ such that $\psi(z_i)w_1z_j = z_iw_1\psi(z_j)$, where $w_1 = r_iz_{i+1}r_{i+1} \dots z_{j-1}r_{j-1}$. If $z_i = z_j = z$ then $\psi(z)w_1z = zw_1\psi(z)$ and according to Lema 3.8 either $\psi(z) = z^r$ or there exist $u \in A^+$ and $s \in \mathbb{N}$ such that $\psi(z) = (zu)^sz$ both cases leading to contradiction. Thus $z_i \neq z_j$ and, according to Lemma 4.7, either $\psi(z_i) = z_i$ and $\psi(z_j) = z_j$ or $\psi(z_i) = z_ip$ and $\psi(z_j) = pz_j$, $p \neq \varepsilon$ or $\psi(z_i) = z_ipq$ and $\psi(z_j) = qpz_j$, $p \neq \varepsilon \neq q$, all cases leading to contradiction.

(ii) implies (i). Use Lemma 7.1.

(i) and (iii) implies (ii). By (iii), $\psi(z) \neq z$ for every $z \in Z$. Now, (ii) follows from (i). □

Proposition 8.2. *The equivalent conditions of Proposition 8.1 follow from each of the following three conditions:*

(1) $\psi(z) \neq z, \varepsilon$ *and* $|\psi(z)| \leq |z|$ *for every* $z \in Z$;

(2) $\psi(z) \neq \varepsilon$ *and* $\psi(z)$ *is reduced for every* $z \in Z$;

(3) $\psi(z) \neq z,\ zxz, \varepsilon$ *for all* $z \in Z$, $x \in A^*$ *and if* $z_1, z_2 \in Z$ *are such that* $\psi(z_1) \neq \psi(z_2)$, *then the pair* $(\psi(z_1), \psi(z_2))$ *is separated.*

Proof. The result is clear when (1) or (2) is true. Now, let (3) be true and let $\psi(z_1) = z_1pq$ and $\psi(z_2) = qpz_2$. If $\psi(z_1) \neq \psi(z_2)$, then the pair $(\psi(z_1), \psi(z_2))$ is separated, and therefore $p = \varepsilon = q$ and $\psi(z_1) = z_1$, a contradiction. Thus $\psi(z_1) = \psi(z_2)$ and we get $z_1 = z_2 = z$ by Lemma 4.9. That is, $zpq = \psi(z) = qpz$ and the rest follows from Lemma 3.8. □

9. When the replacement relation is antitransitive – first observations

In this section, let Z be a strongly separating set of words such that $\varepsilon \notin Z$ and let $\psi : Z \to A^*$ be a function such that $\psi(z) \neq z$ for every $z \in Z$. Denote $\varrho = \varrho_{Z,\psi}$. Obviously, the relation ϱ is irreflexive.

Recall that a binary relation ξ over a set X is (*strictly* 2-) *antitransitive* if for all $x, y, z \in X$ the condition $(x,y), (y,z) \in \xi$ implies $(x,z) \notin \xi$. Equivalently, ξ is (strictly 2-) antitransitive if for all $x, y, z \in X$ the condition $(x,y), (x,z) \in \xi$ implies $(y,z) \notin \xi$. Surely, an antitransitive relation has to be irreflexive.

Proposition 9.1. *The relation ϱ is antitransitive if and only if the following condition is satisfied.*

(1) *For all $z_1, z_2 \in Z$ and $w \in A^*$ such that $z_1 w\psi(z_2) \neq \psi(z_1) w z_2$ we have $(z_1 w\psi(z_2), \psi(z_1) w z_2) \notin \varrho$ and $(\psi(z_1) w z_2, z_1 w\psi(z_2)) \notin \varrho$.*

Proof. Denote $u = z_1 w\psi(z_2)$ and $v = \psi(z_1) w z_2$. Assume that ϱ is antitransitive. Let $z_1, z_2 \in Z$ and $w \in A^*$ be such that $z_1 w\psi(z_2) \neq \psi(z_1) w z_2$. Denote $t = z_1 w z_2$. Obviously, $(t, u) = (z_1 w z_2, z_1 w\psi(z_2))$ and $(t, v) = (z_1 w z_2, \psi(z_1) w z_2)$ are both in ϱ. Since ϱ is antitransitive, neither (u, v) nor (v, u) is in ϱ.

Assume that ϱ satisfies the condition (1). Let (p, u') and (p, v') be in ϱ. If $u' = v'$, then $(u', v') = (v', u')$ is not in ϱ since ϱ is irreflexive. Suppose that $u' \neq v'$. Since $(p, u'), (p, v') \in \varrho$, there exist $z_1, z_2 \in Z$ and $x', x'', y', y'' \in A^*$ such that $p = x' z_1 y' = x'' z_2 y''$, $u' = x''\psi(z_2) y''$ and $v' = x'\psi(z_1) y'$. Since Z is strongly separating and $\varepsilon \notin Z$, the exposed occurrences of the words z_1 and z_2 in p are totally separated. Assume, without loss of generality, that the exposed occurrence of z_2 in p is a factor of y'. Then there exist $w, y \in A^*$ such that $y' = w z_2 y$. Denote $x = x'$, so $p = x z_1 w z_2 y$, $u' = x z_1 w\psi(z_2) y$ and $v' = x\psi(z_1) w z_2 y$. If $(u', v') \in \varrho$ ($(v', u') \in \varrho$, resp.), then also $(u, v) \in \varrho$ ($(v, u) \in \varrho$, resp.), a contradiction with the condition (1) occurs. Thus ϱ is anitransitive. □

Lemma 9.2. *Let $z \in Z$ and $w \in A^*$. Then $zw\psi(z) \neq \psi(z) wz$ if and only if at least one of the following three cases takes place:*

(1) *$\psi(z) = \varepsilon$ and $w \neq z^n$ for every $n \in \mathbb{N}$;*

(2) *$\psi(z) \neq \varepsilon$ and $\psi(z) \neq (zu)^m \cdot z$ for all $u \in A^*$ and $m \in \mathbb{N}_+$;*

(3) *$\psi(z) = (zu)^m \cdot z$ where $u \in A^*$ and $m \in \mathbb{N}_+$ and $w \neq (uz)^n \cdot u$ for each $n \in \mathbb{N}$.*

Proof. It is straightforward to see that if neither (1) nor (2) nor (3) is true, then $zw\psi(z) = \psi(z) wz$. On the other hand, by applying Lemma 2.1 and Lemma 3.8 we see that if (1) or (2) or (3) is valid, then $zw\psi(z) \neq \psi(z) wz$. □

Corollary 9.3. *Let $z \in Z$ be such that $\psi(z)$ is reduced and let $m \in A^*$. Then $zm\psi(z) \neq \psi(z) mz$ if and only if either 1° $\psi(z) \neq \varepsilon$ or 2° $\psi(z) = \varepsilon$ and $m \neq z^n$ for each $n \in \mathbb{N}$.*

Lemma 9.4. *Let $z_1, z_2 \in Z$, $z_1 \neq z_2$, and let $w \in A^*$. Then $z_1 w\psi(z_2) \neq \psi(z_1) w z_2$ if and only if at least one of the following three cases is satisfied:*

(1) *there exist $u, v \in A^*$, $uv \neq \varepsilon$ such that $\psi(z_1) = z_1 uv$ and $\psi(z_2) \neq vuz_2$;*

(2) *there exist $u, v \in A^*$, $uv \neq \varepsilon$ such that $\psi(z_1) \neq z_1 uv$ and $\psi(z_2) = vuz_2$;*

(3) *there exist $u, v \in A^*$, $uv \neq \varepsilon$ such that $\psi(z_1) = z_1 uv$, $\psi(z_2) = vuz_2$ and $w \neq (uv)^n \cdot u$ for each $n \in \mathbb{N}$;*

Proof. By Lemma 4.7, the equality $z_1 w\psi(z_2) = \psi(z_1) w z_2$ is valid if and only if there exist words $u, v \in A^*$ and $n \in \mathbb{N}$ such that $\psi(z_1) = z_1 uv$, $\psi(z_2) = vuz_2$, and $w = (uv)^n u$. The claim easily follows. □

Corollary 9.5. *Let $z_1, z_2 \in Z$ be such that $z_1 \neq z_2$ and at least one of the words $\psi(z_1)$ and $\psi(z_2)$ is reduced. Then $z_1 w \psi(z_2) \neq \psi(z_1) w z_2$ for each $w \in A^*$.*

Corollary 9.6. *Let $z_1, z_2 \in Z$ be such that $z_1 \neq z_2$ and either $|\psi(z_1)| \leq |z_1|$ or $|\psi(z_2)| \leq |z_2|$. Then $z_1 w \psi(z_2) \neq \psi(z_1) w z_2$ for each $w \in A^*$.*

Proposition 9.7. *Assume that for each $z \in Z$, either $|\psi(z)| \leq 1$ or $\psi(z)$ is reduced. Then the relation ϱ is antitransitive if and only if $(u,v) \notin \varrho$ and $(v,u) \notin \varrho$, whenever $u = z_1 w \psi(z_2)$, $v = \psi(z_1) w z_2$, where $z_1, z_2 \in Z$ are such that either 1° $z_1 \neq z_2$ or 2° $z_1 = z = z_2$ and $\psi(z) \neq \varepsilon$ or 3° $z_1 = z = z_2$ and $\psi(z) = \varepsilon$ and $w \neq z^n$ for each $n \in \mathbb{N}$.*

Proof. Combine Proposition 9.1 and Lemmas 9.2 and 9.4. □

Proposition 9.8. *Assume that ψ is length $-$ decreasing. Then the relation ϱ is antitransitive if and only if $(u,v) \notin \varrho$ and $(v,u) \notin \varrho$, whenever $u = z_1 w \psi(z_2)$, $v = \psi(z_1) w z_2$, where $z_1, z_2 \in Z$ are such that either 1° $z_1 \neq z_2$ or 2° $z_1 = z = z_2$ and $\psi(z) \neq \varepsilon$, or 3° $z_1 = z = z_2$, $\psi(z) = \varepsilon$ and $w \neq z^n$ for each $n \in \mathbb{N}$.*

Proof. Combine Proposition 9.1 and Lemma 9.2 and Corollary 9.6. □

Proposition 9.9. *Assume that $|z_1| + |z_2| - |z_3| \neq |\psi(z_1)| + |\psi(z_2)| - |\psi(z_3)|$ for all $z_1, z_2, z_3 \in Z$. Then the relation ϱ is antitransitive.*

Proof. Let, on the contrary, $(w,u) \in \varrho$, $(u,v) \in \varrho$ and $(w,v) \in \varrho$. Then $pz_1q = w = rz_3s$, $p\psi(z_1)q = u = xz_2y$, $r\psi(z_3)s = v = x\psi(z_2)y$. Consequently $|w| - |u| = |z_1| - |\psi(z_1)|$, $|w| - |v| = |z_3| - |\psi(z_3)|$ and $|u| - |v| = |z_2| - |\psi(z_2)|$. From this, we get $|z_3| - |\psi(z_3)| = |w| - |v| = |w| - |u| + |u| - |v| = |z_1| - |\psi(z_1)| + |z_2| - |\psi(z_2)|$ and $|z_1| + |z_2| - |z_3| = |\psi(z_1)| + |\psi(z_2)| - |\psi(z_3)|$, a contradiction. □

Corollary 9.10. *If $|z| - |\psi(z)|$ is odd for every $z \in Z$, then the relation ϱ is antitransitive.*

Remark 9.11.

(i) The relation $\lambda = \lambda_{Z,\psi}$ is antisymmetric (i.e., $u = v$, whenever $(u,v) \in \lambda$ and $(v,u) \in \lambda$) iff ϱ is (strictly) antisymmetric.

(ii) The relation λ is almost antitransitive (i.e. $(w,v) \notin \lambda$, whenever $(w,u) \in \lambda$ and $(u,v) \in \lambda$ and $v \neq w \neq u \neq v$) iff ϱ is antitransitive.

(iii) The relation λ is antitransitive (i.e. $(w,v) \notin \lambda$, whenever $(w,u) \in \lambda$ and $(u,v) \in \lambda$ and $w \neq u \neq v$) iff ϱ is antitransitive and (strictly) antisymmetric.

Remark 9.12. If $Z = \{\varepsilon\}$ and $\psi(\varepsilon) \neq \varepsilon$, then ϱ is both antisymmetric and antitransitive.

References

[1] EL BASHIR, R. AND KEPKA, T., Congruence-simple semirings (preprint).

[2] BOOK, R. AND OTTO, F., *String-Rewriting Systems*, Springer-Verlag New York, Inc., New York Y, 1993.

[3] DASSOW, J., AND PAUN, G., *Regulated Rewriting in Formal Language Theory*, Springer-Verlag, Berlin 1989

[4] FLAŠKA, V., KEPKA, T. AND ŠAROCH, J., Bi-ideal-simple semirings, CMUC 46 (2005), 391 – 397.

[5] HARRISON, M., A., *Introduction to Formal Langage Theory*, Addison-Wesley, Reading, Reading Massachusetts, 1978.

[6] LOTHAIRE, M., *Algebraic Combinatorics on Words*, Cambridge University Press, Cambridge, 2002.

[7] DE LUCA, A., *Finiteness and Regulariy in Semigroups and Formal Languages*, Springer-Verlag New York, Inc. Secaucus NJ, 1999.

[8] TERESE, *Term Rewriting Systems*, Cambridge University Press, Cambridge, 2003.