Charles University in Prague
Faculty of Mathematics and Physics
Department of Algebra

Doctoral Thesis

Mgr. Václav Flaška

Congruence-simple semirings and semimodules

Supervisor:
Prof. RNDr. Tomáš Kepka, DrSc.

Prague, 2008

Branch M1 – Algebra, Theory of Numbers and Mathematical Logic

Univerzita Karlova v Praze
Matematicko-fyzikální fakulta
Katedra algebry

Disertační práce

Mgr. Václav Flaška

Kongruenčně jednodnuché polookruhy a polomoduly

Školitel:
Prof. RNDr. Tomáš Kepka, DrSc.

Praha, 2008

Obor M1 – Algebra, teorie čísel a matematická logika

Acknowledgement

I would like to express my thanks to my supervisor, Prof. RNDr. Tomáš Kepka, DrSc., for an interesting topic of the thesis and an introduction to the life of mathematician he gave me throughout my doctoral study. Further, I would like to thank my wife for strengthening my effort while I was working on this thesis and my family for their support during whole my studies. Finally, my thanks belong also to my friends for making this part of my life a happy one.

Contents

1 Introduction

Semirings (i. e., non-empty sets equipped with two binary operations, usually denoted as addition and multiplication, where the addition is commutative and associative, the multiplication is associative and distributes over the addition) are widely used in various branches of mathematics and computer science and in everyday practice as well (the semiring of natural numbers for instance). In spite of this fact, structural properties of semirings are not well understood so far and, in contrast to more fashionable rings, they are studied relatively scarcely (albeit some material is collected in the monographs [5] and [6]). Congruence-simple objects serve a basic building stone for any algebraic structure and these objects are massively popular in some cases (as groups, rings, algebras). This is not case for semirings, however. Congruence-simple commutative (finite, resp.) semirings (i. e. semirings with precisely two congruences) were classified in [1] ([2], resp.) and the classification carries over to the non-commutative case ([1]). Namely, if S $(= S(+, \cdot))$ is a congruence-simple (cg-simple) semiring, then S fits into just one of the following five classes:

(1) S is additively idempotent (i. e., $s = 2s$ for every $s \in S$);

(2) S is additively cancellative (i. e., $s + t \neq s + r$ for all $r, s, t \in S$, $r \neq t$);

(3) $|S| = 2$ and $|S + S| = 1 = |SS|$;

(4) $|S + S| = 1$ and $SS = S$;

(5) S is additively zeropotent (i. e., $2s = 3t$ for all $s, t \in S$) and $S + S = S$.

Examples of congruence-simple semirings from each of the first four classes come readily to mind (see [9], [11]). On the other hand, it seems that no example of a congruence-simple semiring of class (5) with non-trivial multiplication is known so far. The aim of this thesis is to show that the class (5) contains such a semiring and to design a construction pattern which might be used, under further development, to obtain explicit member of class (5).

The thesis is divided into four sections. Brief introduction is followed by the section dealing with special replacement systems. In most of its length, this section uses very general approach which reaches beyond needs of the other sections but seems to be very promising for more combinatorial-algebraic constructions. Third section offers a study of finite maximal separating sets on 2 generators which are further used in constructions. The final section collects some knowledge of congruence-simple additively zeropotent

semirings, introduces a construction pattern for additively zeropotent semirings and proves that class (5) contains semiring with non-trivial multiplication (and a bit more).

2 Replacement systems

This section initiate a study of special replacement systems (see [10] 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) will be used later in section 4 to construct congruences of free zeropotent semirings, where they will ensure some desired properties of factors.

Through the section we use basic notation and results in accordance with customs in formal language theory and word combinatorics as presented in [10], [4], [7] and [8].

2.1 Preliminaries

Let A^* be the free monoid of *words* over a finite 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 $|a_1a_2 \cdots a_m| = m$ for all $m \in \mathbb{N}_+$ and $a_1, a_2, \ldots, a_m \in A$. Furthermore, we put $\mathrm{alph}(\varepsilon) = \emptyset$ and $\mathrm{alph}(a_1a_2 \ldots a_m) = \{a_1, a_2, \ldots, a_m\}$.

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. The set of all prefixes of u is denoted by $\mathrm{pref}(u)$ and the set of all suffixes of u is denoted by $\mathrm{suff}(u)$.

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 $x = x_1x_2$ and $y = x_2x_1$. 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 [7].

Lemma 2.1.1. *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 2.1.2. *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 $t_2 \neq \varepsilon$, $t = t_1t_2$ is primitive, $x \in (t_1t_2)^+$ and $y \in (t_2t_1)^+$;

(iii) there exists a word z_1 such that $xz_1 = z_1y$;

(iv) there exists a word z_2 such that $z_2x = yz_2$.

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 $w \in (t_1t_2)^*t_1$.*

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

2.2 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 2.2.1. *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 2.1.2. □

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 [8].

Lemma 2.2.2. *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 2.1.2 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 than $|v|/2$, which implies that z is bordered. The other implication is obvious. □

Lemma 2.2.3. *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 2.2.4. 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 2.2.5. *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 2.1.2, $x = (t_1t_2)^r$, $y = (t_2t_1)^r$, 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 2.1.1, 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 2.2.6. *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 2.2.7. *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 2.2.5. 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 2.1.2, $y = (uz)^s u$ for some $s \in \mathbb{N}$. Then $x = (uz)^{k+s} u$ and (3) holds since $k > 0$. The proof is now complete. □

Lemma 2.2.8. *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 2.2.5. Then

1. either $xy = yx = \epsilon$; 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 exist $k \in \mathbb{N}_+$ 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 2.1.2, 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 noempty 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 2.2.5, 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 2.1.2, $t = (zw)^m z$, where $m \in N$. We have established the folllowing result:

Theorem 2.2.9. *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) either $|u| = |p|$;

(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 previous theorem. We will use Lemma 2.2.5, which leads to three cases: 1° $uv = vw = \epsilon$, 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 2.1.2, there exist words $t_1, t_2 \in A^*$, $t_2 \neq \varepsilon$ such that $u = (t_1 t_2)^s$, $w = (t_2 t_1)^s$, $v = (t_1 t_2)^r t_1$, $s \geq 1$, $r \geq 0$ and $t_1 t_2$ $(t_2 t_1)$ 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 $t_1 t_2$ 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 2.1.2 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 2.2.10. *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* $u = zpq$*,* $w = qpz$*,* $v = p(qp)^n$*,* $n \geq 0$

2.3 Basic facts about separated pairs of words

An ordered pair (u, v) of words $u, v \in A^*$ is called *overlapping* if there exists 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 2.3.1. *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 2.2.2, 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 *strongly separated* if it is both left and right strongly separated.

The above definitions imply straightforwardly

Lemma 2.3.2. *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 2.3.3. *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 2.3.4. *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 that $up = qv$. By our assumption, $|up| = |qv| \geq |u| + |v|$. Certainly, $|p| \geq |v|$ and $|q| \geq |u|$. By Lemma 2.3.1 (iii), the pair (u, v) is separated. Thus (u, v) is strongly separated. □

Lemma 2.3.5. *Let $(u, v) \in A^* \times A^*$ be a separated pair of words such that $u \neq v$. Then there does 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 2.1.2, there exist words z and w such that $x = zw$, $y = wz$, $u = pzw$ and $y = wzq$. This is a contradiction. □

Corollary 2.3.6. *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 2.3.7. *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 2.3.5.

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 2.1.2 there exist words $t_1, t_2 \in A^*$, $t_2 \neq \varepsilon$, such that t_1t_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. □

Lemma 2.3.8. *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 contradicition. Assume, without loss of generality, that $|x| > |y|$. Then there exist nonempty words p and q such that $x = yq = py$. Now, by Lemma 2.1.2, 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 $(t_1t_2)^{m+n}t_1u(t_1t_2)^n t_1 = (t_1t_2)^n t_1v(t_1t_2)^{m+n}t_1$. 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. □

Lemma 2.3.9. *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 2.3.7, 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 2.3.8. □

Theorem 2.3.10. *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, contrarywise, 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 2.3.8. □

2.4 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 2.4.1. *Let $Z \subseteq A^*$. Then*

(i) the set Z 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

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

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

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

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 2.4.1 (iv)).

Example 2.4.2.

(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.

Maximal (almost) separating sets are more deeply studied in section 3.

2.5 Reduced and meagre words

Let us now consider the (number of) occurrences of one word in another. For all $w, z \in A^*$, let $\mathrm{Tr}(w, z) = \{(u, z, v) \,|\, u, v \in A^*, w = uzv\}$ 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 2.5.1. *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 2.5.2. *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 2.5.3. *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 $w = x_0z_1x_1z_2x_2 \cdots z_mx_m$.*

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 2.5.4. *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 $w = x_0z_1x_1z_2x_2 \cdots z_mx_m$. Moreover,*

$$\begin{aligned}\mathrm{Tr}(w, Z) = \{ \quad & (x_0, z_1, x_1z_2x_2 \cdots z_mx_m), (x_0z_1x_1, z_2, x_2z_3x_3 \cdots z_mx_m), \\ & \ldots, (x_0z_1x_1 \cdots z_{m-1}x_{m-1}, z_m, x_m)\}\end{aligned}$$

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

Proof. The existence of the decomposition is shown in Lemma 2.5.3. The uniqueness follows from Lemma 2.5.2 by induction on $|w|$. □

2.6 The replacement relation ρ

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 $\rho_{z,t}$ be the binary relation on A^* defined by $\rho_{z,t} = \{(uzv, utv) \mid u, v \in A^*\}$. Let $\lambda_{z,t}$ be the reflexive closure of $\rho_{z,t}$, $\lambda_{z,t} = \rho_{z,t} \cup \mathrm{id}_{A^*}$. Obviously $\rho_{z,t}$ 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 $\rho_{Z,\psi}$ by $\rho_{Z,\psi} = \bigcup_{z \in Z} \rho_{z,\psi(z)}$. Let $\lambda_{Z,\psi}$ be the reflexive closure of $\rho_{Z,\psi}$. Certainly, both $\rho_{Z,\psi}$ 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 $\rho_{Z,\psi}$ is irreflexive if and only if $\psi(z) \neq z$ for each $z \in Z$.

Lemma 2.6.1. *Let $Z \subseteq A^*$ and let $\psi : Z \to A^*$ be a function. Then*

(i) $|\{x \in A^* \mid (w, x) \in \rho_{Z,\psi}\}| \leq \mathrm{tr}(w, Z)$;

(ii) $|\{x \in A^* \mid (w, x) \in \lambda_{Z,\psi}\}| \leq \mathrm{tr}(w, Z) + 1$.

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

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

Lemma 2.6.2. *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 $\rho_{Z,\psi}$;

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

(i) $\rho_{Z,\psi}$ *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 $\rho_{Z,\psi}$ 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, $(xz_1y, x\psi(z_1)y)$,$(z_2w, \psi(z_2)w) \in \rho_{Z,\psi}$. Since $\rho_{Z,\psi}$ 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)⇒(iii).

Assume that (iii) holds. Let $u, v \in A^*$ be such that (u, v) and (v, u) are both in $\rho_{Z,\psi}$. 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 $z_1y = \psi(z_2)y'$, 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 lenght-increasing (strictly length-decreasing, resp.) functions ψ and relations $\rho_{Z,\psi}$ and $\lambda_{Z,\psi}$.

Lemma 2.6.4. *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* $(x, w) \in \rho_{Z,\psi}$.

(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 $(w, x) \in \rho_{Z,\psi}$. The following lemma is a direct consequence of the definition.

Lemma 2.6.5. *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 2.6.6. *Let $Z \subseteq A^+$ be a strongly separating set and let $\psi : Z \to A^*$ be a function. Then for each $(u, v) \in \rho_{Z,\psi}$*

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

(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 $\mathrm{tr}(v, Z) \leq \mathrm{tr}(u, Z) + 1$*;*

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

Proof. Let $(u, v) \in \rho_{Z,\psi}$. 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 2.5.4, 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 previous 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 in Z. Since in the substitution one occurrence of z vanishes, the claim $\mathrm{tr}(v, Z) \leq \mathrm{tr}(u, Z) + 1$ holds. Using an analogous reasoning, (iv) is true. □

Lemma 2.6.7. *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) $(pzq, p\psi(z)q), (xzy, x\psi(z)y) \in \rho_{z,\psi(z)}$*;*

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

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

Proof. Recall the definiton: $\rho_{z,\psi(z)} = \{(xzy, x\psi(z)y) \mid x, y \in A^*\}$. 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 $\rho_{z,\psi(z)}$, $p\psi(z)q \neq x\psi(z)y$, 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 2.6.8. *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) $(pz_1q, p\psi(z_1)q) \in \rho_{z_1,\psi(z_1)}$, $(xz_2y, x\psi(z_2)y) \in \rho_{z_2,\psi(z_2)}$;

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

(iii) if $w \in A^*$ is such that $(p\psi(z_1)q, w)$ is in $\rho_{z_2,\psi(z_2)}$ and $(x\psi(z_2)y, w)$ is in $\rho_{z_1,\psi(z_1)}$, 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 2.6.7. □

Proposition 2.6.9. *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 $(w, u) \in \rho_{z_1,\psi(z_1)}$, $(w, v) \in \rho_{z_2,\psi(z_2)}$ 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 $(u, w') \in \rho_{z_2,\psi(z_2)}$ and $(v, w') \in \rho_{z_1,\psi(z_1)}$. 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 2.6.7 applies. If $z_1 \neq z_2$, then Lemma 2.6.8 can be used. □

Remark 2.6.10. Firstly, notice that Proposition 2.6.9 follows from Proposition 2.5.4 in a quite comfortable way. Then, observe that Lemma 2.6.8 remains true for $z_1 = \varepsilon$, $z_1 \neq z_2$ or $z_2 = \varepsilon$, $z_1 \neq z_2$, provided that either $Z \subseteq A \cup \{\varepsilon\}$ or $\psi(\varepsilon) = \varepsilon$ (so that Proposition 2.6.9 is true as well in this case).

Proposition 2.6.11. *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 $(w, u) \in \rho_{Z,\psi}$, $(w, v) \in \rho_{Z,\psi}$ and $u \neq v$, then there exists $x \in A^*$ such that $(u, x) \in \rho_{Z,\psi}$ and $(v, x) \in \rho_{Z,\psi}$;

(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 $(u, x) \in \lambda_{Z,\psi}$ and $(v, x) \in \lambda_{Z,\psi}$ for some $x \in A^*$).

Proof. Use Proposition 2.6.9 (and Remark 2.6.10). □

Example 2.6.12. 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 $(a^2b^2, a^2bab^2) \in \rho_{\varepsilon,ba}$ and $(a^2b^2, b) \in \rho_{a^2b^2,b}$. On the other hand, $\{x \mid (a^2bab^2, x) \in \rho_{a^2b^2,b}\} = \emptyset$ and $\{y \mid (b, y) \in \rho_{\varepsilon,ba}\} = \{bab, b^2a\}$. Consequently, neither Lemma 2.6.8 nor Proposition 2.6.9 remain true in this case.

2.7 When $\mathrm{tr}(w) = |\{x \mid (w,x) \in \rho\}|$

In this subsection, 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 $(\mathrm{ts}(w) =)\ \mathrm{ts}(w, Z, \psi) = |\{x \in A^* \mid (w,x) \in \rho_{Z,\psi}\}|$. Of course (use Lemma 2.6.1 (i)), we have $\mathrm{ts}(w) \leq \mathrm{tr}(w)$.

Proposition 2.7.1. *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* $\psi(z_1) \neq z_1pq$ *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 2.5.4, $w = r_0z_1r_1z_2r_2 \cdots z_mr_m$, $m \geq 0$, $z_i \in Z$, 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$w_1 = r_iz_{i+1}r_{i+1} \cdots z_{j-1}r_{j-1}$. If $z_i = z_j = z$ then $\psi(z)w_1z = zw_1\psi(z)$ and according to Lemma 2.2.8 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 2.3.7, 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 2.6.1.

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

Proposition 2.7.2. *The equivalent conditions of Proposition 2.7.1 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 2.3.9. That is, $zpq = \psi(z) = qpz$ and the rest follows from Lemma 2.2.8. □

2.8 When the relation ρ is antitransitive I

In this subsection, 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 $\rho = \rho_{Z,\psi}$. 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 2.8.1. *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 $z_1 w\psi(z_2) \neq \psi(z_1)wz_2$ we have $(z_1 w\psi(z_2), \psi(z_1)wz_2) \notin \rho$ and $(\psi(z_1)wz_2, z_1 w\psi(z_2)) \notin \rho$.*

Proof. Denote $u = z_1 w\psi(z_2)$ and $v = \psi(z_1)wz_2$. Assume that ρ is antitransitive. Let $z_1, z_2 \in Z$ and $w \in A^*$ be such that $z_1 w\psi(z_2) \neq \psi(z_1)wz_2$. Denote $t = z_1 wz_2$. Obviously, $(t, u) = (z_1 wz_2, z_1 w\psi(z_2))$ and $(t, v) = (z_1 wz_2, \psi(z_1)wz_2)$ 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 $(p, u'), (p, v') \in \rho$, there exist $z_1, z_2 \in Z$ and $x', x'', y', y'' \in A^*$ such that $p = x'z_1y' = x''z_2y''$, $u' = x''\psi(z_2)y''$ 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'. There then exist $w, y \in A^*$ such that $y' = wz_2y$. Denote $x = x'$, so $p = xz_1wz_2y$, $u' = xz_1w\psi(z_2)y$ and $v' = x\psi(z_1)wz_2y$. If $(u', v') \in \rho$ ($(v', u') \in \rho$, resp.), then also $(u, v) \in \rho$ ($(v, u) \in \rho$, resp.), a contradiction with the condition (1). Thus ρ is antitransitive. □

Lemma 2.8.2. *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 2.1.1 and Lemma 2.2.8 we see that if (1) or (2) or (3) is valid, then $zw\psi(z) \neq \psi(z)wz$. □

Corollary 2.8.3. *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 2.8.4. *Let $z_1, z_2 \in Z$, $z_1 \neq z_2$, and let $w \in A^*$. Then $z_1w\psi(z_2) \neq \psi(z_1)wz_2$ 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 $\psi(z_1) = z_1uv$ and $\psi(z_2) \neq vuz_2$;

(2) there exist $u, v \in A^*$, $uv \neq \varepsilon$ such that $\psi(z_1) \neq z_1uv$ and $\psi(z_2) = vuz_2$;

(3) there exist $u, v \in A^*$, $uv \neq \varepsilon$ such that $\psi(z_1) = z_1uv$, $\psi(z_2) = vuz_2$ and $w \neq (uv)^n \cdot u$ for each $n \in \mathbb{N}$;

Proof. By Lemma 2.3.7, the equality $z_1w\psi(z_2) = \psi(z_1)wz_2$ is valid if and only if there exist words $u, v \in A^*$ and $n \in \mathbb{N}$ such that $\psi(z_1) = z_1uv$, $\psi(z_2) = vuz_2$, and $w = (uv)^nu$. The claim easily follows. □

Corollary 2.8.5. *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 $z_1w\psi(z_2) \neq \psi(z_1)wz_2$ for each $w \in A^*$.*

Corollary 2.8.6. *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 $z_1w\psi(z_2) \neq \psi(z_1)wz_2$ for each $w \in A^*$.*

Proposition 2.8.7. *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 $(u, v) \notin \rho$ and $(v, u) \notin \rho$, whenever $u = z_1w\psi(z_2)$, $v = \psi(z_1)wz_2$, 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 2.8.1 and Lemmas 2.8.2 and 2.8.4. □

Proposition 2.8.8. *Assume that ψ is length decreasing. Then the relation ρ is antitransitive if and only if $(u, v) \notin \rho$ and $(v, u) \notin \rho$, whenever $u = z_1w\psi(z_2)$, $v = \psi(z_1)wz_2$, 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 2.8.1 and Lemma 2.8.2 and Corollary 2.8.6. □

Proposition 2.8.9. *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, $(w,u) \in \rho$, $(u,v) \in \rho$ and $(w,v) \in \rho$. 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 2.8.10. *If* $|z| - |\psi(z)|$ *is odd for every* $z \in Z$, *then the relation* ρ *is antitransitive.*

Remark 2.8.11.

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

2.9 More facts about separated pairs of words

Throughout this subsection, let $u, v \in A^*$ be such that $u \neq v$, $|u| = |v|$ and both the pairs (u,v) and (v,u) are separated. According to 2.3.3, these two pairs are strongly separated (clearly, $u \neq \varepsilon \neq v$).

Lemma 2.9.1. $uvx = xuv$ *iff* $x = (uv)^m$ *for some* $m \geq 0$.

Proof. We will proceed by induction on $|x|$. If $x = \varepsilon$, then $m = 0$. If $|x| < |u|$, then $u = xr$, $v = sx$, and so $x = \varepsilon$ and $m = 0$ again. Finally, if $|u| \leq |x|$, then $up = x = qv$, $uvqv = uvx = xuv = upuv$, $vq = pu$, $p = vt$, $q = tu$ and $uvt = up = x = qv = tuv$. If $|t| = |x|$, then $u = \varepsilon = v$, a contradiction. Thus $|t| < |x|$, $t = (uv)^{m_1}$ by induction and $x = uvt = (uv)^m$, $m = m_1 + 1$. □

Lemma 2.9.2. *If* $pux = xvq$ *and* $|x| \leq |pu|$, *then just one of the following two cases takes place:*

(1) $p = vt$, $q = tu$ *and* $x = vtu$ *(then* $|x| = |pu| = |vq|$*);*

(2) $p = xvt$ *and* $q = tux$ *(then* $|x| < |p| = |q|$*).*

Proof. We have $pu = xz$ and $vq = zx$. If $|z| \leq |u|$, then $u = u_1 z$, $v = z v_1$, and hence $z = \varepsilon$. Consequently, $pu = x = vq$ and it follows that $p = vt$, $q = tu$ and $x = vtu$, so that (1) is true. On the other hand, if $|u| < |z|$, then $u_2 u = z = v v_2$, $u_2 = vt$, $v_2 = tu$ and $z = vtu$. From this, $pu = xz = xvtu$, $p = xvt$, $vq = zx = vtux$, $q = tux$ and $|x| < |p|$. □

Lemma 2.9.3. $pux = xvq$ *iff* $p = yvt$, $q = tuy$ *and* $x = (yvtu)^m y$ $(= y(vtuy)^m)$, $m \geq 0$.

Proof. Only the direct implication needs a proof and we will proceed by induction on $|x|$.

If $|x| \leq |pu|$, then either 2.9.2 (1) is true and we put $y = \varepsilon$, $m = 1$, or 2.9.2 (2) is true and we put $y = x$, $m = 0$.

If $|pu| < |x|$, then $pux_1 = x = x_1 vq$, $1 \leq |x_1| < |x|$, and we use induction hypothesis. □

Lemma 2.9.4. $puyv = uyvq$ *iff at least one (and then just one) of the following two cases takes place:*

(1) $p = \varepsilon = q$*;*

(2) $p = uzvt$, $q = tuzv$ *and* $y = (zvtu)^m z$, $m \geq 0$.

Proof. Again, only the direct implication needs a proof.

If $|p| < |u|$, then $u = pr$, $v = sq$, $ryv = uys$ and, by 2.3.7, $r = uu_1$, $s = v_1 v$. Now, $u = puu_1$, $v = v_1 vq$ and $p = \varepsilon = q$.

If $|u| \leq |p|$, then $p = uu_2$, $q = v_2 v$ and $yvv_2 = u_2 uy$. It remains to use 2.9.3 □

Lemma 2.9.5. *Let* $p, q, x, y \in A^*$ *be such that* $|x| \leq |p|$*. Then* $puyvx = xuyvq$ *iff at least one (and then just one) of the following two cases takes place:*

(1) $p = x = q$*;*

(2) $p = xuzvt$ *and* $q = tuzvx$ *and* $y = (zvtu)^m z$, $m \geq 0$.

Proof. As usual, only the direct implication needs a proof. We have $p = xp_1$, $q = q_1 x$, $|p_1| = |q_1|$ and $p_1 uyv = uyvq_1$. The rest follows from 2.9.4. □

Lemma 2.9.6. *Let* $p, q, x, y \in A^*$ *be such that* $|p| < |x|$*. Then* $puyvx = xuyvq$ *iff* $x = puzvt = tuzvq$ *and* $y = (zvtu)^m z$, $m \geq 0$.

Proof. Standard (use 2.9.4). □

2.10 Auxiliary results I

Throughout this subsection, let Z be a strongly separating set of words, $Z \neq \{\varepsilon\}$, and let $p, q, r, s, t, w, z \in A^*$ be such that $ptq = w = rzs$, $z \in Z$ and p, q are (Z-) reduced.

Lemma 2.10.1. *Just one of the following nine cases takes place:*

(a1) $r = pg$, $t = gh$, $q = ks$, $z = hk$, $g \neq \varepsilon \neq h$, $k \neq \varepsilon$ *and* h, k, s *are reduced;*

(a2) $r = pg$, $t = gz$, $q = s$, $g \neq \varepsilon$ *and* s *is reduced;*

(a3) $r = pg$, $t = gzh$, $s = hq$, $g \neq \varepsilon \neq h$;

(a4) $r = p$, $z = th$, $q = hs$, $h \neq \varepsilon$ *and* h, s, r, t *are reduced;*

(a5) $r = p$, $z = t$, $s = q$ *and* r, s *are reduced;*

(a6) $r = p$, $t = zh$, $s = hq$, $h \neq \varepsilon$ *and* r *is reduced;*

(a7) $p = rg$, $z = gh$, $t = hf$, $s = fq$, $g \neq \varepsilon \neq f$, $h \neq \varepsilon$ *and* r, g, h *are reduced;*

(a8) $p = rg$, $z = gt$, $q = s$, $g \neq \varepsilon \neq t$ *and* r, g, t, s *are reduced;*

(a9) $p = rg$, $z = gh = gtf$, $h = tf$, $q = fs$, $g \neq \varepsilon \neq f$ *and* r, g, h, t, f, s *are reduced;*

Proof. It will be divided into three parts:

(i) Let $|p| < |r|$. Then $r = pg$, $g \neq \varepsilon$, $ptq = pgzs$ and $tq = gzs$. Since q is reduced, we have $|g| < |t|$, $t = gh$, $h \neq \varepsilon$, $ghq = gzs$, $hq = zs$ and $pt = pgh = rh$.

If $|h| < |z|$, then $z = hk$, $k \neq \varepsilon$, $hq = zs = hks$, $q = ks$ and (a1) is fulfilled.

If $|h| = |z|$, then $h = z$, $q = s$, $t = gz$ and (a2) is satisfied.

If $|h| > |z|$, then $h = zh_1$, $h_1 \neq \varepsilon$, $h_1 q = s$, $t = gzh_1$ and (a3) is true.

(ii) Let $|p| = |r|$. Then $p = r$ and $tq = zs$.

If $|t| < |z|$, then $z = th$, $h \neq \varepsilon$, $tq = zs = ths$, $q = hs$ and (a4) is valid.

If $|t| = |z|$, then $z = t$, $q = s$ and (a5) holds.

If $|t| > |z|$, then $t = zh$, $h \neq \varepsilon$, $zhq = tq = zs$, $hq = s$ and (a6) follows.

(iii) Let $|p| > |r|$. Then $p = rg$, $g \neq \varepsilon$, $rgtq = ptq = rzs$ and $gtq = zs$. Since g is reduced, we have $|g| < |z|$, $z = gh$, $h \neq \varepsilon$. Moreover, $gtq = zs = ghs$ and $tq = hs$.

If $|h| < |t|$, then $t = hf$, $f \neq \varepsilon$, $hfq = tq = hs$, $fq = s$ and (a7) is clear.

If $|h| = |t|$, then $t = h$, $q = s$, $z = gt$ and (a8) is evident.

If $|h| > |t|$, then $h = tf$, $f \neq \varepsilon$, $tfs = tq = hs$, $q = fs$ and (a9) is visible.

□

Lemma 2.10.2. *Assume that (a1) is true. Then:*

(i) $w = pgzs = pghks$, $z = hk$, $t = gh$, $q = ks$, $g \neq \varepsilon \neq h$, $k \neq \varepsilon$, $|z| \geq 2$, $|t| \geq 2$, h, k, s, p, ks *are reduced and the pair* (t, z) *is not separated.*

(ii) If pg *is reduced, then* $\mathrm{tr}(w) = 1$.

(iii) If t *is reduced, then* g *is reduced.*

(iv) If g *is reduced and* pg *is not reduced, then* $p = p_1u$, $g = vq_1$, $t = vq_1h$, $w = p_1uvq_1zs$, $u \neq \varepsilon \neq v$, $uv \in Z$, p_1, q_1, u, v *are reduced and* $\mathrm{tr}(w) = 2$.

Proof.

(i) The assertion follows easily from (a1).

(ii) Combine (i) and 2.5.4.

(iii) Obvious from $t = gh$.

(iv) Since p, g are reduced and pg is not, we have $pg = p_1z_1q_1$, $p = p_1u$, $g = vq_1$, $z_1 = uv \in Z$, $u \neq \varepsilon \neq v$, p_1, q_1 reduced and $|z_1| \geq 2$. Thus $w = p_1uvq_1zs$ and $\mathrm{tr}(w) = 2$ by 2.5.4.

□

Lemma 2.10.3. *Assume that (a2) is true. Then:*

(i) $w = pgzs$, $t = gz$, $q = s$, $g \neq \varepsilon$, $|t| \geq 2$, s *is reduced and* t *is not reduced.*

(ii) If pg *is reduced, then* $\mathrm{tr}(w) = 1$.

(iii) *If g is reduced and pg is not reduced, then $p = p_1u$, $g = vq_1$, $t = vq_1z$, $w = p_1uvq_1zs$, $u \neq \varepsilon \neq v$, $uv \in Z$, p_1, q_1, u, v are reduced and* $\mathrm{tr}(w) = 2$.

Proof. We can proceed similarly as in the proof of 2.10.2. □

Lemma 2.10.4. *Assume that (a3) is true. Then:*

(i) *$w = pgzs = pgzhq$, $t = gzh$, $s = hq$, $g \neq \varepsilon \neq h$, $|t| \geq 3$ and t is not reduced.*

(ii) *If pg and s are reduced, then* $\mathrm{tr}(w) = 1$.

Proof. Similar to the proof of 2.10.2. □

Lemma 2.10.5. *Assume that (a4) is true. Then:*

(i) *$w = pzs = pths$, $z = th$, $q = hs$, $t \neq \varepsilon \neq h$, $|z| \geq 2$ and h, s, t, hs are reduced.*

(ii) $\mathrm{tr}(w) = 1$.

Proof. Easy. □

Lemma 2.10.6. *Assume that (a5) is true. Then:*

(i) *$w = pzs = pts$, $z = t$, $q = s$, s is reduced and t is not reduced.*

(ii) $\mathrm{tr}(w) = 1$.

Proof. Easy. □

Lemma 2.10.7. *Assume that (a6) is true. Then:*

(i) *$w = pzhq$, $t = zh$, $s = hq$, $h \neq \varepsilon$, $|t| \geq 2$ and t is not reduced.*

(ii) *If hq is reduced, then* $\mathrm{tr}(w) = 1$.

(iii) *If h is reduced and hq is not reduced, then $w = pzp_1uvq_1$, $h = p_1u$, $q = vq_1$, $t = zp_1u$, $u \neq \varepsilon \neq v$, $uv \in Z$, p_1, q_1, u, v are reduced and* $\mathrm{tr}(w) = 2$.

Proof. Similar to the proof of 2.10.2. □

Lemma 2.10.8. *Assume that (a7) is true. Then:*

(i) *$w = rzfq = rghfq$, $z = gh$, $t = hf$, $s = fq$, $g \neq \varepsilon \neq f$, $h \neq \varepsilon$, $|z| \geq 2$, $|t| \geq 2$, h, g, r, rg are reduced and the pair (z, t) is not separated.*

(ii) *If fq is reduced, then* $\mathrm{tr}(w) = 1$.

(iii) *If t is reduced, then f is reduced.*

(iv) *If f is reduced and fq is not reduced, then $f = p_1u$, $q = vq_1$, $t = hp_1u$, $w = rzp_1uvq_1$, $u \neq \varepsilon \neq v$, $uv \in Z$, p_1, q_1, u, v are reduced and* $\mathrm{tr}(w) = 2$.

Proof. Similar to the proof of 2.10.2. □

Lemma 2.10.9. *Assume that (a8) is true. Then:*

(i) *$w = rgts$, $z = gt$, $q = s$, $g \neq \varepsilon \neq t$, $|z| \geq 2$ and r, g, t, s, rg are reduced.*

(ii) $\mathrm{tr}(w) = 1$.

Proof. Easy. □

Lemma 2.10.10. *Assume that (a9) is true. Then:*

(i) *$w = rgtfs$, $z = gtf$, $q = fs$, $g \neq \varepsilon \neq f$, $|z| \geq 2$ and r, g, t, f, s, tf, rg, fs are reduced.*

(ii) $\mathrm{tr}(w) = 1$.

Proof. Easy. □

Lemma 2.10.11. *If* $\mathrm{tr}(w) \geq 2$, *then just one of the five conditions (a1), (a2), (a3), (a6) and (a7) holds.*

Proof. Combine the preceding lemmas of this subsection. □

Lemma 2.10.12.

(i) *If at least one of (a2), (a3), (a5) and (a6) holds, then t is not reduced.*

(ii) *If t is reduced, then just one of (a1), (a4), (a7), (a8), (a9) holds.*

(iii) *If t is reduced and* $\mathrm{tr}(w) \geq 2$, *then just one of (a1), (a7) holds and* $\mathrm{tr}(w) = 2$.

Proof. Combine the preceding lemmas of this subsection. □

Lemma 2.10.13.

(i) *If t is reduced then* $\mathrm{tr}(w) \leq 2$.

(ii) *If $t = \varepsilon$, then (a9) is satisfied.*

(iii) *If $t \in A$ (i. e., $|t| = 1$), then just one of (a4), (a5), (a8), (a9) is true (if (a5) is true, then $z = t \in A$) and* $\mathrm{tr}(w) = 1$.

(iv) *If $|t| \leq 1$, then* $\mathrm{tr}(w) = 1$.

(v) *If $z \in A$ (i. e., $|z| = 1$), then just one of (a2), (a3), (a5), (a6) is true (if (a5) is true, then $t = z \in A$).*

(vi) *If $z \in A$ and* $\mathrm{tr}(w) \geq 2$, *then either (a2) or (a6) holds and t is not reduced.*

Proof. Combine the preceding lemmas of this subsection. □

2.11 Auxiliary results II

In this subsection, let Z be a strongly separating set of words, $Z \neq \{\varepsilon\}$ and let $p_1, q_1, p_2, q_2, t_1, t_2, w_1, w_2 \in A^*$ and $z_1, z_2 \in Z$ be such that $p_1 z_1 q_1 = w_1 = p_2 t_2 q_2$, $p_1 t_1 q_1 = w_2 = p_2 z_2 q_2$ and p_1, q_1 are (Z-) reduced.

Lemma 2.11.1. *Assume that $|p_1| = |p_2|$. Then $p_1 = p_2$, $z_1 q_1 = t_2 q_2$ and $t_1 q_1 = z_2 q_2$. Moreover:*

(i) *If $|t_2| < |z_1|$, then $z_1 = t_2 r_1$, $t_1 = z_2 r_1$, $q_2 = r_1 q_1$, $r_1 \neq \varepsilon$, $|t_1| \geq 2$ and t_1 is not reduced.*

(ii) *If $|t_2| = |z_1|$, then $z_1 = t_2$, $t_1 = z_2$ and $q_1 = q_2$.*

(iii) *If $|t_2| > |z_1|$, then $t_2 = z_1 s_1$, $z_2 = t_1 s_1$, $q_1 = s_1 q_2$, $s_1 \neq \varepsilon$, $|t_2| \geq 2$ and t_2 is not reduced.*

Proof. Easy. □

Lemma 2.11.2. *Assume that $|p_1| < |p_2|$. Then $p_2 = p_1 u_1$, $z_1 q_1 = u_1 t_2 q_2$, $t_1 q_1 = u_1 z_2 q_2$, $u_1 \neq \varepsilon$, $|u_1| < |t_1|$, $t_1 = u_1 u_2$, $u_2 q_1 = z_2 q_2$, $u_2 \neq \varepsilon$, $|t_1| \geq 2$. Moreover:*

(i) *If $|q_1| \leq |q_2|$, then $q_2 = r_2 q_1$, $u_2 = z_2 r_2$, $t_1 = u_1 z_2 r_2$ and t_1 is not reduced.*

(ii) *If $|q_1| > |q_2|$, then $q_1 = v_1 q_2$, $t_1 v_1 = u_1 z_2$, $z_1 v_1 = u_1 t_2$, $z_2 = u_2 v_1$, $v_1 \neq \varepsilon$ and u_2, v_1 are reduced.*

(iii) *If $|q_1| > |q_2|$ and $|z_1| \leq |u_1|$, then $u_1 = z_1 s_2$, $v_1 = s_2 t_2$, $t_1 = z_1 s_2 u_2$, $z_2 = u_2 s_2 t_2$ and neither u_1 nor p_2 nor t_1 is reduced.*

(iv) *If* $|q_1| > |q_2|$ *and* $|z_1| > |u_1|$, *then* $z_1 = u_1v_2$, $t_2 = v_2v_1$, $v_2 \neq \varepsilon$ *and* v_2 *is reduced.*

Proof. Easy. □

Lemma 2.11.3. *Assume that* $|p_1| > |p_2|$. *Then* $p_1 = p_2u_3$, $t_2q_2 = u_3z_1q_1$, $z_2q_2 = u_3t_1q_1$, $u_3 \neq \varepsilon$ *and* p_2, u_3 *are reduced. Moreover:*

(i) *If* $|t_2| \leq |u_3|$, *then* $q_2 = r_3z_1q_1$, $u_3 = t_2r_3$, $p_1 = p_2t_2r_3$, $t_2r_3t_1 = z_2r_3z_1$ *and* t_2, r_3 *are reduced. Further,* $|t_2| < |z_2|$, $z_2 = t_2s_3$, $s_3 \neq \varepsilon$, $r_3t_1 = s_3r_3z_1$, $|z_1| < |t_1|$, $t_1 = kz_1$, $r_3k = s_3r_3$, $k \neq \varepsilon$, $|t_1| \geq 2$ *and* t_1 *is not reduced.*

(ii) *If* $|t_2| > |u_3|$, *then* $t_2 = u_3u_4$, $z_1q_1 = u_4q_2$, $u_4 \neq \varepsilon$ *and* $|t_2| \geq 2$.

(iii) *If* $|t_2| > |u_3|$ *and* $|q_2| \leq |q_1|$, *then neither* u_4 *nor* t_2 *is reduced.*

(iv) *If* $|t_2| > |u_3|$ *and* $|q_2| > |q_1|$, *then* $q_2 = v_3q_1$, $z_1 = u_4v_3$, $u_3t_1 = z_2v_3$, $v_3 \neq \varepsilon$, v_3, u_4 *are reduced,* $|u_3| < |z_2|$, $z_2 = u_3v_4$, $t_1 = v_4v_3$, $v_4 \neq \varepsilon$ *and* v_4 *is reduced.*

Proof. Easy. □

Lemma 2.11.4. *Assume that either* $|t_1| \leq 1$ *or* t_1 *is reduced and the same is true for* t_2. *Then at least one of the following three cases takes place:*

(i) $z_1 = t_2$, $z_2 = t_1$, $p_1 = p_2$ *and* $q_1 = q_2$.

(ii) $z_1 = u_1v_2$, $z_2 = u_2v_1$, $t_1 = u_1u_2$, $t_2 = v_2v_1$, $p_2 = p_1u_1$, $q_1 = v_1q_2$, $u_1, u_2, v_1, v_2 \in A^+$ *and all* u_1, u_2, v_1, v_2 *are reduced.*

(iii) $z_1 = u_4v_3$, $z_2 = u_3v_4$, $t_1 = v_4v_3$, $t_2 = u_3u_4$, $p_1 = p_2u_3$, $q_2 = v_3q_1$, $u_3, u_4, v_3, v_4 \in A^+$ *and all* u_3, u_4, v_3, v_4 *are reduced.*

Proof. It follows from 2.11.1, 2.11.2 and 2.11.3 that only the cases 2.11.1 (ii), 2.11.2 (iv) and 2.11.3 (iv) come into account. □

2.12 Disturbing pairs

Let Z be a strongly separating set of words, $Z \neq \{\varepsilon\}$, and let $\psi : Z \to A^*$ be a mapping. Consider the relations ρ and λ defined in subsections 2.6 and 2.8.

An ordered pair $(z_1, z_2) \in Z \times Z$ will be called *disturbing* if there exist words $u, v, r, s \in A^+$ such that $z_1 = ur$, $z_2 = sv$, $\psi(z_1) = us$ and $\psi(z_2) = rv$.

An ordered pair $(z_1, z_2) \in Z \times Z$ will be called *paradisturbing* if $\psi(z_1) = z_2$ and $\psi(z_2) = z_1$.

Lemma 2.12.1. *Let $(z_1, z_2) \in Z \times Z$ be a disturbing pair, $z_1 = ur$, $z_2 = sv$, $\psi(z_1) = us$,$\psi(z_2) = rv$, $u, v, r, s \in A^+$. Put $w_1 = urv$ and $w_2 = usv$. Then:*

(i) $|z_1| \geq 2$, $|z_2| \geq 2$, $|\psi(z_1)| \geq 2$, $|\psi(z_2)| \geq 2$.

(ii) The words u, v, r and s are reduced.

(iii) $(w_1, w_2) \in \nu$.

(iv) $\mathrm{tr}(w_1) = 1 = \mathrm{tr}(w_2)$.

(v) Both w_1 and w_2 are pseudoreduced.

(vi) $w_1 = w_2$ iff $r = s$.

(vii) If $w_1 = w_2$, then w_1 is strongly pseudoreduced.

Proof. Easy. □

Lemma 2.12.2. *Let $(z_1, z_2) \in Z \times Z$ be a paradisturbing pair. Then:*

(i) $(z_1, z_2) \in \nu$.

(ii) $\mathrm{tr}(z_1) = 1 = \mathrm{tr}(z_2)$.

(iii) Both z_1 and z_2 are weakly pseudoreduced.

Proof. Obvious. □

Proposition 2.12.3. *There exist no disturbing pairs, provided that either $Z \subseteq A$ or $\psi(Z) \subseteq A$.*

Proof. Obvious. □

Proposition 2.12.4. *Suppose that for every $z \in Z$, either $|\psi(z)| \leq 1$ or $\psi(z)$ is reduced. Then the following conditions are equivalent:*

(i) There exist no disturbing and no paradisturbing pairs in $Z \times Z$.

(ii) Every pseudoreduced meagre word is reduced.

Proof.

(i) implies (ii). Let, on the contrary w_1 be a weakly pseudoreduced with $\mathrm{tr}(w_1) = 1$. Then $w_1 = p_1 z_1 q_1$, where $z_1 \in Z$ and p_1, q_1 are reduced (use 2.6.6). If $w_2 = p_1 t_1 q_1$, $t_1 = \psi(z_1)$, then $(w_1, w_2) \in \rho$, and hence $(w_2, w_1) \in \rho$, since w_1 is weakly pseudoreduced. Consequently, $w_2 = p_2 z_2 q_2$, $z_2 \in Z$, and $w_1 = p_2 t_2 q_2$, $t_2 = \psi(z_2)$. Now, 2.11.4 applies. If 2.11.4 (i) is true, then (z_1, z_2) is paradisturbing. If 2.11.4 (ii) is true, then (z_1, z_2) is disturbing. Finally, if 2.11.4 (iii) is true, then (z_2, z_1) is disturbing.

(ii) implies (i). See 2.12.1 and 2.12.2. □

2.13 Meagre and pseudomeagre words

Let Z be a strongly separating set of words such that $Z \neq \{\varepsilon\}$ (except for 2.13.9) and let $\psi : Z \to A^*$ be a mapping. Consider the relations ρ and λ defined in 2.6 and 2.8.

A word w is called *meagre* if $\mathrm{tr}(w) \leq 1$.

A word w is called *pseudomeagre* if $(w, x) \in \rho$ for at most one $x \in A^*$.

Lemma 2.13.1. *Every meagre word is pseudomeagre.*

Proof. Obvious. □

Lemma 2.13.2. *Let $z \in Z$ be such that $\psi(z) \in \{\varepsilon, z\}$. Then the word z^n, $n \geq 2$, is pseudomeagre but not meagre.*

Proof. It follows from 2.6.6 that $\mathrm{tr}(z^n) = n \geq 2$, and so z^n is not meagre. On the other hand, if $(z^n, x) \in \rho$, then $x = z^{n-1}$ for $\psi(z) = \varepsilon$ and $x = z^n$ for $\psi(z) = z$. □

Lemma 2.13.3. *Let $z_1, z_2, z \in Z$ and $u, v, x \in A^*$ be such that $z_1 x z_2 = uzv$.*

(i) If $u = \varepsilon$, then $z = z_1$ and $v = xz_2$.

(ii) If $v = \varepsilon$, then $z = z_2$ and $u = z_1 x$.

(iii) If $u \neq \varepsilon \neq v$, then $u = z_1 u_1$, $v = v_1 z_2$ and $x = u_1 z v_1$.

Proof.

(i) Easy to see.

(ii) Easy to see.

(iii) If $|u| < |z_1|$, then $z_1 = uy$, $y \neq \varepsilon$, $uyxz_2 = z_1 x z_2 = uzv$, $yxz_2 = zv$, a contradiction. Thus $|u| \geq |z_1|$ and, similarly, $|v| \geq |z_2|$. The rest is clear.

□

Lemma 2.13.4. *Let $z \in Z$ and $x \in A^*$ be such that $\psi(z) = zxz$. Then:*

(i) $\mathrm{tr}(zxz) \geq 2$ and zxz is not meagre.

(ii) zxz is pseudomeagre iff $\psi(z_1) = z_1 v z u z_1$ whenever $z_1 \in Z$ and $x = uz_1 v$ (or $\psi(z) = zuz_1 vz$).

Proof.

(i) Obvious.

(ii) Clearly, $(\varepsilon, z, xz), (zx, z, \varepsilon) \in \mathrm{Tr}(zxz)$, $\varepsilon\psi(z)xz = zxzxz = zx\psi(z)\varepsilon$ and $(zxz, zxzxz) \in \rho$. If x is reduced, then $\mathrm{tr}(zxz) = 2$ by 2.6.6, and hence zxz is pseudomeagre (and the other condition is satisfied trivially).

Now, let $(u_1, z_1, v_1) \in \mathrm{Tr}(zxz)$, $u_1 \neq \varepsilon \neq v_1$. According to 2.13.3, $u_1 = zu$, $v_1 = vz$ and $x = uz_1v$. We have $zxz = zuz_1vz$ and $(zxz, zu\psi(z_1)vz) \in \rho$. Consequently, $zu\psi(z_1)vz = zxzxz$ iff $u\psi(z_1)v = xzx = uz_1vzuz_1v$ and iff $\psi(z_1) = z_1vzuz_1$. The rest is clear.

□

Lemma 2.13.5. *Let $z_1, z_2 \in Z$ and $x, y \in A^*$ be such that $\psi(z_1) = yxz_1$ and $\psi(z_2) = z_2xy$. Then:*

(i) $\mathrm{tr}(z_2xz_1) \geq 2$ *and z_2xz_1 is not meagre.*

(ii) z_2xz_1 is pseudomeagre iff $\psi(z_3) = z_3vyuz_3$ whenever $z_3 \in Z$ and $x = uz_3v$ (or $\psi(z_1) = yuz_3vz_1$ or $\psi(z_2) = z_2uz_3vy$).

Proof.

(i) Obvious.

(ii) Clearly, $(\varepsilon, z_2, xz_1), (z_2x, z_1, \varepsilon) \in \mathrm{Tr}(z_2xz_1)$, $\varepsilon\psi(z_2)xz_1 = z_2xyxz_1 = z_2x\psi(z_1)\varepsilon$ and $(z_2xz_1, z_2xyxz_1) \in \rho$. If x is reduced, then $\mathrm{tr}(z_2xz_1) = 2$ by 2.6.6, and hence z_2xz_1 is pseudomeagre (and the other condition is satisfied trivially).

Now, let $(u_1, z_3, v_1) \in \mathrm{Tr}(z_2xz_1)$, $u_1 \neq \varepsilon \neq v_1$. According to 2.13.3, $u_1 = z_2u$, $v_1 = vz_1$ and $x = uz_3v$. We have $z_2xz_1 = z_2uz_3vz_1$ and $(z_2xz_1, z_2u\psi(z_3)vz_1) \in \rho$. Consequently, $z_2u\psi(z_3)vz_1 = z_2xyxz_1$ iff $u\psi(z_3)v = xyx = uz_3vyuz_3v$ and iff $\psi(z_3) = z_3vyuz_3$. The rest is clear.

□

Proposition 2.13.6. *Suppose that every pseudomeagre word is meagre. Then the following three conditions are satisfied:*

(b1) $\varepsilon \neq \psi(z) \neq z$ *for every $z \in Z$;*

(b2) If $z_1, z_2 \in Z$ and $x, y \in A^*$ are such that $\psi(z_1) = yxz_1$ and $\psi(z_2) = z_2xy$, then $x \neq \varepsilon \neq y$ and x is not reduced;

(b3) *If $z_1, z_2, z_3 \in Z$ and $u, v, y \in A^*$, then either $\psi(z_1) \neq yuz_3vz_1$ or $\psi(z_2 \neq z_2uz_3vy$ or $\psi(z_3) \neq z_3vyuz_3$*

Proof. The condition (b1) follows from 2.13.2. Further, if $\psi(z_1) = yxz_1$ and $\psi(z_2) = z_2xy$, then x is not reduced due to 2.13.5, and hence $x \neq \varepsilon$. Moreover, if $y = \varepsilon$, then z_2z_1 is pseudomeagre, but not meagre, and therefore $x \neq \varepsilon \neq y$ and we have shown (b2). Finally, (b3) follows from 2.13.5. □

Proposition 2.13.7. *Suppose that the following two conditions are satisfied:*

(c1) *$\varepsilon \neq \psi(z) \neq z$ and $\psi(z) \neq zxz$ for all $z \in Z$ and $x \in A^*$;*

(c2) *If $z_1, z_2 \in Z$ and $x, y \in A^*$ are such that $\psi(z_1) \neq \psi(z_2)$, then either $\psi(z_1) \neq yxz_1$ or $\psi(z_2) \neq z_2xy$.*

Then every pseudomeagre word is meagre.

Proof. Let, on the contrary, w be pseudomeagre word, but not meagre. Then $\mathrm{tr}(w) \geq 2$, and therefore $pz_1q = w = rz_2s$, where $(p, z_1, q) \neq (r, z_2, s)$ and $z_1, z_2 \in Z$; we will assume $|rz_2| \leq |pz_1|$, the other case being similar.

Assume, for a moment, that $z_1 = z = z_2$. Then $|r| < |p|$ and we get a contradiction by easy combination of (c1) and 2.10.11. Consequently, $z_1 \neq z_2$ and it follows easily that $|r| < |p|$. Then $\psi(z_1) \neq \psi(z_2)$ and we get a contradiction with (c2). □

Proposition 2.13.8.

(i) *Suppose that $\psi(z) \neq \varepsilon$ and that z is neither a prefix nor a suffix of $\psi(z)$ for every $z \in Z$. Then every pseudomeagre word is meagre.*

(ii) *Suppose that $|\psi(z)| \leq |z|$ for every $z \in Z$. Then every pseudomeagre word is meagre if and only if $\varepsilon \neq \psi(z) \neq z$ for every $z \in Z$.*

Proof. See 2.13.6 and 2.13.7 □

Remark 2.13.9. Let $Z = \{\varepsilon\}$. Then ε is the only meagre word. Moreover:

(i) If $\psi(\varepsilon) = \varepsilon$, then all words are pseudomeagre (and hence there exist pseudomeagre words that are not meagre).

(ii) If $\psi(\varepsilon) = t$ and $|\operatorname{var}(t)| = 1$, $t = a^m$, $a \in A$, $m \geq 1$, then a word w is pseudomeagre iff $w = a^n$, $n \geq 0$. Consequently, there exist pseudomeagre words that are not meagre.

(iii) If $\psi(\varepsilon) = t$ and $|\operatorname{var}(t)| \geq 2$, then ε is the only pseudomeagre word (and hence all pseudomeagre words are meagre).

2.14 Disturbing triples

This subsection is an immediate continuation of the preceding one.

An ordered triple $(z_1, z_2, z_3) \in Z \times Z \times Z$ will be called *disturbing* if there exist $u, v, g, h \in A^+$ and $p \in A^*$ such that $z_1 = uv$, $z_3 = gh$ and $\psi(z_2) = vpg$.

Lemma 2.14.1. *Let $(z_1, z_2, z_3) \in Z \times Z \times Z$ be a disturbing triple, $z_1 = uv$, $z_3 = gh$, $\psi(z_2) = vpg$, $u, v, g, h \in A^+$, $p \in A^*$. Then:*

(i) $|z_1| \geq 2$, $|z_3| \geq 2$ *and* $|\psi(z_2)| \geq 2$.

(ii) The words u, v, g, h are reduced.

(iii) $(u_1, v_1) \in \rho$, $\mathrm{tr}(u_1) = 1$ *and* $\mathrm{tr}(v_1) \geq 2$, *where* $u_1 = uz_2h$ *and* $v_1 = uvpgh$.

Proof. Easy (use 2.6.9). □

Proposition 2.14.2. *There exist no disturbing triples, provided that either $Z \subseteq A$ or $\psi(Z) \subseteq A$.*

Proof. Obvious. □

Proposition 2.14.3. *Suppose that for every $z \in Z$, either $|\psi(z)| \leq 1$ or $\psi(z)$ is reduced. Then the following conditions are equivalent:*

(i) There exist no disturbing triples in $Z \times Z \times Z$.

(ii) If $(w_1, w_2) \in \rho$ and $\mathrm{tr}(w_1) = 1$, then $\mathrm{tr}(w_2) \leq 1$.

(iii) If $(w_1, w_2) \in \rho$ and w_1 is meagre, then w_2 is meagre.

Proof.

(i) implies (ii). We have $w_1 = pz_2q$, $z_2 \in Z$, p, q reduced, and $w_2 = ptq$, $t = \psi(z_2)$. Now, assume that $w_2 = rz_3s$ and 2.10.1 applies. If $|t| \leq 1$, then $\mathrm{tr}(w_2) = 1$ by 2.10.13 (iv), and therefore we will assume that $|t| \geq 2$. Then t is reduced and, according to 2.10.12 (iii) we can assume that (a1) holds, the case (a7) being similar.

By 2.10.2 $w_2 = pghks$, $z_3 = hk$, $t = gh$, $q = ks$, $g \neq \varepsilon \neq h$, $k \neq \varepsilon$ and, moreover, g is reduced, since t is so. If pg is reduced, then $\mathrm{tr}(w_2) = 1$ by 2.10.2 (ii). If pg is not reduced, then, by 2.10.2 (iv), $pg = p_1z_1q_1$, $z_1 = uv$, $p = p_1u$, $g = vq_1$, $t = vq_1h$, $u \neq \varepsilon \neq v$ and the triple (z_1, z_2, z_3) is disturbing.

(ii) implies (iii), (iii) implies (i). Obvious. □

2.15 When the relation ρ is antisymmetric

As usual, let Z be a strongly separating set of words such that $Z \neq \{\varepsilon\}$ (except for 2.15.7, 2.16.11) and let $\psi : Z \to A^*$ be a mapping.

Proposition 2.15.1. *The relation ρ $(= \rho_{Z,\psi})$ is irreflexive if and only if $\psi(z) \neq z$ for every $z \in Z$.*

Proof. Obvious from the definition of ρ. □

Proposition 2.15.2. *The relation ρ is antisymmetric (i. e., $u = v$, whenever $(u, v) \in \rho$ and $(v, u) \in \rho$) if and only if the following three conditions hold:*

(1) If $z_1, z_2 \in Z$ and $x, y \in A^*$ are such that $z_2 = x\psi(z_1)y$ and $\psi(z_2) = xz_1y$, then $\psi(z_2) = z_2$ (and hence $\psi(z_1) = z_1$ as well);

(2) If $z_1, z_2 \in Z$ and $x, y \in A^*$ are such that $z_2 = yx\psi(z_2)$ ($z_2 = \psi(z_2)xy$, resp.) and $\psi(z_1) = z_1xy$ ($\psi(z_1) = yxz_1$, resp.), then $x = \varepsilon = y$ (and hence $\psi(z_1) = z_1$, $\psi(z_2) = z_2$);

(3) If $z_1, z_2 \in Z$ and $x, y, u, v \in A^+$ are such that $z_1 = uy$, $z_2 = xv$, $\psi(z_1) = vy$ and $\psi(z_2) = xu$, then $u = v$ (and hence $\psi(z_1) = z_1$, $\psi(z_2) = z_2$).

Proof. Use 2.5.4. □

Corollary 2.15.3. *Assume that for every $z \in Z$,either $|\psi(z)| \leq 1$ or $\psi(z)$ is reduced. Then:*

(i) The relation ρ is antisymetric if and only the following two conditions hold:

(i1) If $(z_1, z_2) \in (Z \times Z) \cap (A \times A)$ is a paradisturbing pair, then $z_1 = z_2$;

(i2) There exist no disturbing pairs in $Z \times Z$.

(ii) The relation ρ is both irreflexive and antisymmetric if and only if there exist no disturbing nor paradisturbing pairs in $Z \times Z$.

Proposition 2.15.4. *The following conditions are equivalent:*

(i) If $(u, v) \in \rho$ and $(v, v) \in \rho$, then $u = v$.

(ii) If $(u, v) \in \rho$ and $(u, u) \in \rho$, then $u = v$.

(iii) Either $\psi(z) \neq z$ for every $z \in Z$ or $\psi(z) = z$ for every $z \in Z$.

Proof. Easy to check. □

Proposition 2.15.5. *Assume that* $|z_1|-|\psi(z_1)| \neq |\psi(z_2)|-|z_2|$ *for all* $z_1, z_2 \in Z$. *Then the relation* ρ *is both irreflexive and antisymmetric (i. e., it is strictly antisymmetric).*

Proof. Use 2.5.4. □

Proposition 2.15.6. *The relation* ρ *is weakly antisymmetric (i. e.,* $u = v$, *whenever* $(u, v) \in \rho$, $(v, u) \in \rho$, $(u, u) \in \rho$*) if and only if* $\psi(z_1) = z_1$, *whenever* $z_1, z_2, z_3 \in Z$ *and* $p, q, r, s, x, y \in A^*$ *are such that* $pz_1q = rz_2s = x\psi(z_3)y$ *and* $p\psi(z_1)q = xz_3y$.

Proof. Obvious. □

Remark 2.15.7. Let $Z = \{\varepsilon\}$. If $\psi(\varepsilon) = \varepsilon$, then $\rho = \mathrm{id}_{A^*}$, and hence ρ is antisymmetric, but not irreflexive. If $\psi(\varepsilon) \neq \varepsilon$, then ρ is both irreflexive and antisymmetric. Moreover, 2.15.4 is true in both cases.

2.16 When the relation ρ is antitransitive II

This subsection is an immediate continuation of preceding one.

Proposition 2.16.1. *The relation* ρ *is weakly antitransitive (i. e.,* $(w, v) \notin \rho$, *whenever* $u, v, w \in A^*$ *are such that* $u \neq v \neq w \neq u$, $(w, u) \in \rho$ *and* $(u, v) \in \rho$*) if and only if the following condition is satisfied:*

(1) If $z_1, z_2 \in Z$ *and* $x, y, k \in A^*$ *are such that* $\psi(z_1) \neq z_1$, $\psi(z_2) \neq z_2$ *and* $z_1k\psi(z_2) \neq \psi(z_1)kz_2$, *then* $(u, v) \notin \rho$ *and* $(v, u) \notin \rho$, *where* $u = xz_1k\psi(z_2)y$ *and* $v = x\psi(z_1)kz_2y$

Proof. See 2.8.1. □

Lemma 2.16.2. *Let* $z \in Z$ *and* $k \in A^*$. *Then* $zk\psi(z) \neq \psi(z)kz$ *iff* $\psi(z) \neq z$ *and either* $\psi(z) = \varepsilon$ *and* $k \neq z^n$ *for every* $n \geq 0$ *or* $\varepsilon \neq \psi(z) \neq (zu)^m z$ *for all* $u \in A^*$ *and* $m \geq 1$ *or* $\psi(z) = (zv)^t z$ *and* $k \neq (vz)^n v$ *for some* $v \in A^*$, $t \geq 1$ *and every* $n \geq 0$.

Proof. Easy. □

Lemma 2.16.3. *Let* $z \in Z$ *be such that* $\psi(z)$ *is reduced and let* $k \in A^*$. *Then* $zk\psi(z) \neq \psi(z)kz$ *iff either* $\psi(z) \neq \varepsilon$ *or* $\psi(z) = \varepsilon$ *and* $k \neq z^n$ *for every* $n \geq 0$.

Proof. This follows from 2.16.2. □

Lemma 2.16.4. *Let $z_1, z_2 \in Z$, $z_1 \neq z_2$, and $k \in A^*$. Then $z_1 k\psi(z_2) \neq \psi(z_1)kz_2$ iff at least one of the following three conditions is satisfied:*

(1) $\psi(z_1) \neq z_1$ and $\psi(z_2) = z_2$;

(2) $\psi(z_2) \neq z_2$, $\psi(z_1) = z_1uv$ for some $u, v \in A^*$ and either $\psi(z_2) \neq vuz_2$ or $\psi(z_2) = vuz_2$ and $k \neq (uv)^n u$ for every $n \geq o$;

(3) $\psi(z_2) \neq z_2$, $\psi(z_1) \neq z_1xy$ for all $x, y \in A^*$.

Proof. Easy. □

Lemma 2.16.5. *Let $z_1, z_2 \in Z$ be such that $z_1 \neq z_2$ and both $\psi(z_1)$, $\psi(z_2)$ are reduced. Then $z_1k\psi(z_2) \neq \psi(z_1)kz_2$ for every $k \in A^*$.*

Proof. This follows easily from 2.16.4 □

Proposition 2.16.6. *Assume that for every $z \in Z$, either $|\psi(z)| \leq 1$ or $\psi(z)$ is reduced. Then the relation ρ is weakly antitransitive if and only if $(u, v) \notin \rho$ and $(v, u) \notin \rho$, whenever $u = xz_1k\psi(z_2)y$, $v = x\psi(z_1)kz_2y$ and z_1, z_2 are such that:*

(1) If $z_1, \psi(z_1) \in A \cap Z$, then $\psi(z_1) \neq z_1$;

(2) If $z_2, \psi(z_2) \in A \cap Z$, then $\psi(z_2) \neq z_2$;

(3) If $z_1 = z_2 = z$ and $\psi(z) = \varepsilon$, then $k \neq z^n$ for every $n \geq 0$.

Proof. Combine 2.16.1, 2.16.2 and 2.16.4. □

Corollary 2.16.7. *Assume that for every $z \in Z$, $\psi(z) \neq z$ and either $|\psi(z)| \leq 1$ or $\psi(z)$ is reduced (equivalently, either $\psi(z)$ is reduced or $\psi(z) = \varepsilon$ or $\psi(z) \in A$ and $\psi(z) \neq z$). Then the relation ρ is weakly antitransitive if and only if $(u, v) \notin \rho$ and $(v, u) \notin \rho$ (i. e., u, v are incomparable in ρ), whenever $u = xz_1k\psi(z_2)y$, $v = x\psi(z_1)kz_2y$ and $z_1, z_2 \in Z$ are such that either $z_1 \neq z_2$ or $z_1 = z_2$ and $\psi(z_1) \neq \varepsilon$ or $z_1 = z_2$ and $\psi(z_1) = \varepsilon$ and $k \neq z_1^n$ for every $n \geq 0$.*

Proposition 2.16.8. *Assume that $\psi(z_0) \neq z_0$ for at least one $z_0 \in Z$. Then the following conditions are equivalent:*

(i) The relation ρ is irreflexive and weakly antitransitive.

(ii) The relation ρ is strictly antitransitive (i. e., $(w, v) \notin \rho$ whenever $(w, u) \in \rho$ and $(u, v) \in \rho$).

(iii) The relation ρ is antitransitive (i. e., $u = v = w$, whenever $(w, u) \in \rho$, $(u, v) \in \rho$ and $(w, v) \in \rho$).

(iv) The condition 2.16.1 (1) is satisfied and $\psi(z) \neq z$ for every $z \in Z$.

Proof.

(i) implies (ii). Let $(w, u), (u, v), (w, v) \in \rho$. Since ρ is weakly antitransitive, either $w = u$ or $u = v$ or $w = v$. On the other hand, since ρ is irreflexive, we have $w \neq u \neq v \neq w$, a contradiction.

(ii) implies (iii). Obvious.

(iii) implies (iv). Clearly, ρ is weakly antitransitive, and hence 2.16.1 (1) follows from 2.16.1. Moreover, $\psi(z) \neq z$ follows from 2.15.4.

(iv) implies (i). Use 2.15.1 and 2.16.1. □

Proposition 2.16.9. *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 strictly antitransitive.*

Proof. Let $(w, u), (u, v), (w, v) \in \rho$. 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, $|w| - |u| = |z_1| - |\psi(z_1)|$, $|w| - |v| = |z_3| - |\psi(z_3)|$, $|u| - |v| = |z_2| - |\psi(z_2)|$. 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. □

Remark 2.16.10. The condition from 2.16.9 is satisfied e. g. if $|z| - |\psi(z)|$ is odd for every $z \in Z$.

Remark 2.16.11. Let $Z = \{\varepsilon\}$. If $\psi(\varepsilon\} = \varepsilon$, then $\rho = \mathrm{id}_{A^*}$, and hence ρ is antitransitive, but not strictly antitransitive. If $\psi(\varepsilon) \neq \varepsilon$, then ρ is strictly antitransitive.

Proposition 2.16.12. *Assume that $\varepsilon \notin Z$ and for every $z \in Z$ $zx \neq \psi(z) \neq yz$, $x, y \in A^*$. Then ρ is antitransitive.*

Proof. According to 2.8.1, we have to prove that for all $z_1, z_2 \in Z$ and $w \in A^*$ such that $z_1w\psi(z_2) \neq \psi(z_1)wz_2$ we have $(z_1w\psi(z_2), \psi(z_1)wz_2) \notin \rho$ and $(\psi(z_1)wz_2, z_1w\psi(z_2)) \notin \rho$. Suppose, for a contradiction, that there are $z_1, z_2 \in Z$ and $w \in A^*$ such that $(z_1w\psi(z_2), \psi(z_1)wz_2) \in \rho$ (the other case is similar). This means that there exist $u, v \in A^*$ and $z \in Z$ such that $z_1w\psi(z_2) = uzv$ and $\psi(z_1)wz_2 = u\psi(z)v$. If $u = \varepsilon$ then $z = z_1$, $v = w\psi(z_2)$ and $\psi(z_1)wz_2 = \psi(z_1)w\psi(z_2)$, thus $z_2 = \psi(z_2)$, a contradiction. Hence we may assume that $u = z_1u'$ and hence $w\psi(z_2) = u'zv$ and $\psi(z_1)wz_2 = z_1u'\psi(z)v$. Since $z_1x \neq \psi(z_1)$, $z_1 = \psi(z_1)s$ for a proper $s \in A^*$ (s is a suffix of z_1), $w\psi(z_2) = u'zv$ and $wz_2 = su'\psi(z)v$. Now, let $w = s^nw'$, $u' = s^mu''$, w', u'' be such that s is not a prefix of either one of them.

Then $s^n w'\psi(z_2) = s^m u''zv$ and $s^n w' z_2 = s^{m+1} u''\psi(z)v$. If $n \leq m$ then $w'z_2 = s^{m-n+1}u''\psi(z)v$ and (s is not a prefix of w') there exists a suffix of z_1 which is a prefix of z_2, a contradiction. If $n > m$ then $s^{n-m}w'\psi(z_2) = u''zv$ and (s is not a prefix of u'') there exists a suffix of z_1 which is a prefix of z, a contradiction again. □

2.17 Transitive closure of ρ

In this subsection, let $Z \subseteq A^+ \setminus A$ be a strongly separating set and let $\psi : Z \to A$ be a function. Moreover, let τ ($\tau_{Z,\psi}$) denote the transitive closure of ρ ($\rho_{Z,\psi}$) and ξ denote the reflexive transitive closure of ρ.

Lemma 2.17.1.

(i) $\xi = \tau \cup \mathrm{id}_{A^*}$.

(ii) ξ *is a transitive closure of* λ.

(iii) if $(u, v) \in \tau$ *then there exist* $u_0, u_1, \ldots, u_n \in A^+$ *such that* $u_0 = u$, $u_n = v$ *and* $(u_{i-1}, u_i) \in \rho$, $i = 1, \ldots, n$.

Proof. Immediate consequences of definition. □

Proposition 2.17.2. *Let* $u, v, w \in A^+$ *be such that* $(w, u) \in \tau$ *and* $(w, v) \in \tau$. *Then either* $u = v$ *or* $(u, v) \in \tau$ *or* $(v, u) \in \tau$ *or there exists* $w' \in A^+$ *such that* $(u, w') \in \tau$ *and* $(v, w') \in \tau$.

Proof. Let m, n be the lengths of ρ-sequences from w to u, v. We can proceed by double induction on m, n, using 2.6.11. □

Proposition 2.17.3. *Let* $u, v, w \in A^+$ *be such that* $(w, u) \in \xi$ *and* $(w, v) \in \xi$. *Then there exists* $w' \in A^+$ *such that* $(u, w') \in \xi$ *and* $(v, w') \in \xi$.

Proof. Immediate consequence of 2.17.2. □

Proposition 2.17.4. *For every* $u \in A^+$ *there exists precisely one* $\mathrm{r}(u) \in A^+$ *such that* $(u, \mathrm{r}(u)) \in \xi$ *and* $\mathrm{r}(u)$ *is reduced.*

Proof. The existence follows from the fact that whenever $(u, v) \in \rho$ then $|u| > |v|$, the uniqueness follows from 2.17.2. □

Lemma 2.17.5. *Let* $u \in A^+$ *and* $z \in Z$. *Then:*

(i) If $p \in \mathrm{pref}(z)$, $p \neq z$ *and* $v \in A^+$ *is such that* $(up, v) \in \tau$ *then* $p \in \mathrm{suff}(v)$.

(ii) *If* $s \in \mathrm{suff}(z)$, $s \neq z$ *and* $v \in A^+$ *is such that* $(su, v) \in \tau$ *then* $s \in \mathrm{pref}(v)$.

(iii) *If* $p \in \mathrm{pref}(z)$, $p \neq z$, *then* $\mathrm{r}(up) = \mathrm{r}(u)p$.

(iv) *If* $s \in \mathrm{suff}(z)$, $s \neq z$, *then* $\mathrm{r}(su) = s\,\mathrm{r}(u)$.

Proof. We assume that $p \neq \varepsilon$ (this case is trivial). Let $v \in A^+$ be such that $(up, v) \in \rho$. Since Z is strongly separating, the replaced occurence of element from Z must be a factor of u. Hence p is a suffix of v. The rest follows by induction on length of ρ-sequence from up to v and su may be treated analogously. □

Proposition 2.17.6. *There are no words* $u, v \in A^+$, $y \in A^*$ *and* $c \in A$ *such that* $(ycv, v) \in \tau$ *and* $(ucy, u) \in \tau$.

Proof. Assume for a contradiction, that there exist such u, v and y and that $|u| + |v|$ is minimal (this means that both u and v are reduced, otherwise we can use $\mathrm{r}(u)$ and $\mathrm{r}(v)$). Let y be the shortest possible for given u and v (once again, this means that y is reduced). $(ucy, u) \in \tau$ and hence $u = u'p$, $y = sy'$ and $z = pcs$ for some $z \in Z$. Thus $(sy'cv, v) \in \tau$ and, due to 2.17.5, $v = sv'$, which implies $(y'csv', v') \in \tau$. $y'csv'$ cannot be reduced and thus $y' = y''p'$, $z' = p'cs$ for an appropriate $z' \in Z$ (y' and v' are reduced and s is suffix of an element of Z). This yields to $(u'pcsy''p', u'p) \in \tau$ and hence $p' \in \mathrm{suff}(u'p)$ (due to 2.17.5 again), thus $p \in \mathrm{suff}(p')$ or $p' \in \mathrm{suff}(p)$. Moreover, we know that both pcs and $p'cs$ are elements of strongly separating set Z and hence $p = p'$. Finally, we get to $(u'pcsy'', u') \in \tau$ and $(y''pcsv', v') \in \tau$. Let $c' \in A$ be such that $(pcs, c') \in \rho$. We obtain $(u'c'y'', u') \in \tau$ and $(y''c'v', v') \in \tau$, a contradiction with minimality of $|u| + |v|$, since $ps \neq \varepsilon$. □

Lemma 2.17.7. *Let* $u, v \in A^*$ *be such that* $(u, v) \in \rho$, $z \in Z$ *be such that* z *is a factor of* u *and* $c \in A$ *be such that* $(z, c) \in \rho$. *Then* $u = u_1 z u_2$ *and* $v = v_1 z u_2$, *where* $(u_1, v_1) \in \rho$ *or* $v = u_1 z v_2$, *where* $(u_2, v_2) \in \rho$ *or* $v = u_1 c u_2$.

Proof. Obvious. □

Lemma 2.17.8. *Let* $u, v \in A^*$ *be such that* $(u, v) \in \tau$, $z \in Z$ *be such that* z *is a factor of* u, $c \in A$ *be such that* $(z, c) \in \rho$ *and* $(v_0, v_1, \ldots, v_m)$ *be a reducing sequence from* u *to* v. *Then either* z *is a factor of* v *and* $u = u_1 z u_2$, $v = v_1 z v_2$, $(u_1, v_1) \in \xi$, $(u_2, v_2) \in \xi$ *or there exists index* i, $1 \leq i \leq m$, *such that* v_i *is made from* v_{i-1} *through replacing word* z *by letter* c.

Proof. Immediate consequence of 2.17.7. □

Lemma 2.17.9. *Let $u, v \in A^*$ be such that $(u, v) \in \tau$, $z \in Z$ be such that z is a factor of u and z is not a factor of v and $c \in A$ be such that $(z, c) \in \rho$. Then there exists a reducing sequence $(w_0, w_1, \ldots, w_m)$ from u to v such that w_1 is made from w_0 through replacing word z by letter c.*

Proof. Let $(v_0, v_1, \ldots, v_m)$ be a reducing sequence from u to v. According to 2.17.8 there exists index i, $1 \leq i \leq m$, such that v_i is made from v_{i-1} through replacing word z by letter c. Let $w_0 = v_0$, w_j be made from v_{j-1} through replacing word z by letter c for $1 \leq j < i$ and $w_j = v_j$ for $i \leq j \leq m$. $(w_0, w_1, \ldots, w_m)$ is obviously a reducing sequence from u to v and the rest is clear. □

Corollary 2.17.10. *Let $u, v \in A^*$ be such that $(u, v) \in \tau$, $z \in Z$ be such that z is a factor of u and $c \in A$ be such that $(z, c) \in \rho$. Then either z is a factor of v and $u = u_1 z u_2$, $v = v_1 z v_2$, $(u_1, v_1) \in \xi$, $(u_2, v_2) \in \xi$ or there exists a reducing sequence $(w_0, w_1, \ldots, w_m)$ from u to v such that w_1 is made from w_0 through replacing word z by letter c.*

Proof. Consequence of 2.17.8 and 2.17.9. □

Lemma 2.17.11. *If $u, v \in A^*$ and $z_k, z_l \in Z$, $z_k \neq z_l$ then $(uz_k v, uz_l v) \notin \tau$.*

Proof. Suppose for a contradiction that there exist $u, v \in A^*$ and $z_k, z_l \in Z$, $z_k \neq z_l$ such that $(uz_k v, uz_l v) \in \tau$. Assuming 2.17.10, either $(u\psi(z_k)v, uz_l v) \in \tau$ (a contradiction yields from $|u\psi(z_k)v| < |uz_l v|$) or z_k is a factor of u or v (and a contradiction yields again from the lengths of "sides" of z_k). □

Proposition 2.17.12. *Let $u, v \in A^*$ be reduced, $z_k, z_l \in Z$, $z_k \neq z_l$, and $w \in A^*$ be ρ-maximal word such that $(w, uz_k v) \in \tau$ and $(w, uz_l v) \in \tau$. Then $w = uz_k x z_l v$, $x \in A^*$, x is reduced, $(uz_k x, u) \in \tau$ and $(xz_l v, v) \in \tau$ or $w = uz_l x z_k v$, $x \in A^*$, x is reduced, $(uz_l x, u) \in \tau$ and $(xz_k v, v) \in \tau$.*

Proof. Suppose that $z \in Z$ is a factor of w and $c \in A$ is such that $(z, c) \in \rho$. We will use 2.17.10 for $(w, uz_k v) \in \tau$ and for $(w, uz_l v) \in \tau$. Notice that, since u and v are reduced, the only factor of $uz_k v$ ($uz_l v$, resp.), which is an element of Z is z_k (z_l, resp.). If z is a factor of both $uz_k v$ and $uz_l v$ then $z_k = z = z_l$, a contradiction. If there exist reducing sequence $(w_0, w_1, \ldots, w_m)$ from w to $uz_k v$ such that w_1 is made from w_0 through replacing word z by letter c and reducing sequence $(w'_0, w'_1, \ldots, w'_{m'})$ from w to $uz_l v$ such that w'_1 is made from w'_0 through replacing word z by letter c then $w = w_0 = w'_0$ and $w_1 = w'_1$ and we achieve a contradiction with ρ-maximality of w.

Hence either $z = z_k$, $w = u_1 z_k v_1$, $(u_1, u) \in \xi$, $(v_1, v) \in \xi$ and there exists reducing sequence $(w'_0, w'_1, \ldots, w'_{m'})$ from w to $uz_l v$ such that w'_1 is made from

w'_0 through replacing word z_k by letter c or $z = z_l$, $w = u_1 z_l v_1$, $(u_1, u) \in \xi$, $(v_1, v) \in \xi$ and there exists reducing sequence $(w_0, w_1, \ldots, w_m)$ from w to $uz_k v$ such that w_1 is made from w_0 through replacing word z_l by letter c.

Word w is certainly not reduced, thus it must contain as a factor at least two words from Z (or one word from Z at least twice), otherwise there exists unique w' such that $(w, w') \in \rho$, which would have desired properties, a contradiction with ρ-maximality of w.

Suppose, for a while, that w contains as a factor twice word z_k, i. e. $w = y_1 z_k y_2 z_k y_3$ and, according to the second paragraph of the proof, $(y_1 z_k y_2, u) \in \xi$ and there exists reducing sequence $(w'_0, w'_1, \ldots, w'_{m'})$ from w to $uz_l v$ such that $w'_1 = y_1 c y_2 z_k y_3$. But then also $(y_1 c y_2, u) \in \xi$ and $(y_1 c y_2 z_k y_3, uz_k v) \in \tau$ and $(y_1 c y_2 z_k y_3, uz_l v) \in \tau$, a contradiction with ρ-maximality of w. Similarly, w may contain as a factor only one occurence of z_l.

Finally, we obtained that w contains as a factors at least two occurences of words from Z and at most one occurence of z_k and one occurence of z_l. Thus $w = u' z_k x z_l v'$ (or $w = u' z_l x z_k v'$), where u', x, v' are reduced and moreover $(u', u) \in \xi$, $(x z_l v', v) \in \xi$, $(u' z_k x, u) \in \xi$, $(v', v) \in \xi$ (or $(u', u) \in \xi$, $(x z_k v', v) \in \xi$, $(u' z_l x, u) \in \xi$, $(v', v) \in \xi$). Since u, v, u' and v' are reduced we obtain $u' = u$, $v' = v$, $(uz_k x, u) \in \tau$ and $(x z_l v, v) \in \tau$ (or $(uz_l x, u) \in \tau$ and $(x z_k v, v) \in \tau$). □

Proposition 2.17.13. *For all $u, v \in A^*$, $w \in A^+$ and $z, z' \in Z$ such that $\psi(z) = \psi(z') = c \in A$ either $(w, uzv) \notin \tau$ or $(w, uz'v) \notin \tau$.*

Proof. Suppose for a contradiction an existence of $u, v \in A^*$, $w \in A^+$ and $z, z' \in Z$ such that $\psi(z) = \psi(z') = c \in A$, $(w, uzv) \in \tau$ and $(w, uz'v) \in \tau$. We may assume without loss of generality that u and v are reduced and w is ρ-maximal. According to 2.17.12 either $w = uzxz'v$, $x \in A^*$, x is reduced, $(uzx, u) \in \tau$ and $(xz'v, v) \in \tau$ or $w = uz'xzv$, $x \in A^*$, x is reduced, $(uz'x, u) \in \tau$ and $(xzv, v) \in \tau$. In both cases $(ucx, u) \in \tau$ and $(xcv, v) \in \tau$, a contradiction with 2.17.6. □

3 Maximal strongly separating sets

3.1 Preliminaries

Throughout the entire section, whenever we speak about separating set, we mean strongly separating set which does not contain ε. This will allow us to maintain readability of the text without need of further definitions. Moreover, we will assume in this section that $A = \{a, b\}$.

Lemma 3.1.1. *Let $Z \subset A^+$. Then Z is a separating set if and only if for all $z_1, z_2 \in Z$ and $w \in A^+$ such that both z_1 and z_2 are factors (different occurences if $z_1 = z_2$) of w $|w| \geq |z_1| + |z_2|$.*

Proof. Immediate consequence of definition. □

Lemma 3.1.2. *Let $Z \subset A^+$. Then Z is a maximal separating set if and only if Z is separating set and for every $u \in A^+ \setminus Z$ there exists $z \in Z$ such that (at least) one of the following conditions takes place:*

(1) z is a factor of u;

(2) u is a factor of z;

(3) $\mathrm{pref}(z) \cap \mathrm{suff}(u) \neq \{\varepsilon\}$;

(4) $\mathrm{pref}(u) \cap \mathrm{suff}(z) \neq \{\varepsilon\}$.

Proof. Immediate consequence of definition. □

3.2 First observation

Remark 3.2.1. Let Z be a separating set. If $Z \cap A \neq \emptyset$ then $Z \subseteq A$.

Proof. Suppose that $a \in Z$ ($b \in Z$ being similar). Then either $Z = \{a\}$ or there exists $z \in Z$, $z \neq a$. Since Z is separating, z does not contain a as factor (a is element of Z) and hence $z = b^n$, $n \geq 1$. If $n \geq 2$, we get contradiction with 3.1.1 ($w = b^{n+1}$), thus $n = 1$ and $Z = A$. □

Remark 3.2.2. Let Z be a separating set. If $Z \neq A$ then $|z| > 1$ for every $z \in Z$.

Let Z be a separating set, $Z \neq A$. It is obvious that every word from Z must begin and end with different letters and, moreover, all words from Z must begin with the same letter and end with the other one. For the rest of this section we assume that all words in separating sets begin with a and end with b (which allows us to omit the assumption $Z \neq A$ as well).

Let Z be a finite maximal separating set and let $N \in \mathbb{N}$ be greater than the length of the longest word of Z (precise value of N is not important, we need N just to be big enough for purposes shown in the sequel). Consider the word $a^N b^N$. Certainly $a^N b^N \notin Z$ but according to 3.1.2 there exists $z \in Z$ such that z is a factor of $a^N b^N$ (condition (2) cannot take place due to our choose of N and conditions (3) and (4) are excluded due to the assumption that z begins with a and end with b). Consider the word $a^N (ba)^N b^N$. Once again there must exist a word $z' \in Z$ which is a factor of $a^N (ba)^N b^N$. Since Z is separating, z' cannot be a factor of $a(ba)^N b$ and we may summarize this paragraph in following lemma:

Lemma 3.2.3. *Let Z be a finite maximal separating set. Then there exist $z, z' \in Z$ such that $z = a^{k_0} b^{l_0}$ $k_0, l_0 \geq 1$ and $z' = a^k (ba)^m b$, $k \geq 1$, $m \geq 0$ or $z' = a(ba)^m b^l$, $l \geq 1$, $m \geq 0$. Moreover, either $k \geq 2$ ($l \geq 2$, resp.) or $m = 0$.*

The preceding lemma allows us to distinguish types of finite maximal separating sets: left ($k \geq 2$) and right ($l \geq 2$) (the case $m = 0$ will be treated in the following lemma). In the rest of this section we will assume that finite maximal separating sets are of the left type (we do not loose generality by this choice as everything further stated would work similarly for the right type.)

Lemma 3.2.4. *Z is a finite maximal separating set and $|Z| = 1$ if and only if $Z = \{a^n b\}$ for some $n \in \mathbb{N}$.*

Proof. The direct implication is trivial consequence of lemma 3.2.3. Obviously the set $\{a^n b\}$ is separating. The maximality is proved easily using lemma 3.1.2 if we divide words of A^+ into the three categories: $\{bu; u \in A^*\}$, $\{a^m; m \in \mathbb{N}\}$, $\{a^m bu; m \in \mathbb{N}, u \in A^*\}$. □

Remark 3.2.5. Complete list (without the restrictions stated above) of one-element maximal separating sets is $\{a^n b\}$, $\{ab^n\}$, $\{b^n a\}$, $\{ba^n\}$, $n \in \mathbb{N}$.

We have already treated the case $|Z| = 1$ and hence we may proceed to following proposition:

Proposition 3.2.6. *Let Z be a finite maximal separating set and $|Z| > 1$. Then there exist $1 \leq m \leq |Z| - 1$, $k_0, k_1, \ldots, k_m \geq 2$, $l_0, l_1, \ldots, l_{m-1} \geq 2$ and $z_0, z_1, \ldots, z_m \in Z$ such that $z_i = a^{k_i} (ba)^i b^{l_i}$, $i = 0, 1, \ldots, m-1$ and $z_m = a^{k_m} (ba)^m b$.*

Proof. Combining lemma 3.2.3 and lemma 3.2.4, we obtain that there exist $m \geq 1$, $k_m \geq 2$ and $z_m \in Z$ such that $z_m = a^{k_m} (ba)^m b$. Considering words

$a^N(ba)^i b^N$, $i = 0, 1, \ldots, m-1$ we get (similarly as in lemma 3.2.3) that there exist $z_0, z_1, \ldots, z_{m-1} \in Z$ such that $z_i = a^{k_i}(ba)^i b^{l_i}$, $k_i \geq 1$, $l_i \geq 1$, $i = 0, 1, \ldots, m-1$. In order to keep the set Z separating $k_i \geq 2$, $l_i \geq 2$, $i = 0, 1, \ldots, m-1$. Finally, words $z_0, z_1, \ldots, z_m$ are pair-wise distinct and hence $m \leq |Z| - 1$. □

Lemma 3.2.7. *Z is a finite maximal separating set and $|Z| = 2$ if and only if $Z = \{a^2b^2, a^2bab\}$.*

Proof. Let Z be a finite maximal separating set and $|Z| = 2$. According to 3.2.6 $m = 1$ and there exist $k_0, k_1, l_0 \geq 2$ and $z_0, z_1 \in Z$ such that $z_0 = a^{k_0}b^{l_0}$, $z_1 = a^{k_1}bab$. Consider the word $a^N ba^2 b^N$. Similarly as in lemma 3.2.3 we obtain that either z_0 or z_1 is a factor of $a^N ba^2 b^N$ and hence $k_0 = 2$. Similarly, using words $a^N b^2 ab^N$ and $a^N ba^2 bab^N$, we get $l_0 = 2$ and $k_1 = 2$. Thus $Z = \{a^2b^2, a^2bab\}$.

It remains to prove that Z is maximal (separating set). Let $u \in A^+$ be such that a^2 is not a factor of u. Then either $u = a$ or $u = bv$ or $u = abv$, $v \in A^*$. All cases can be treated by Z easily using 3.1.2. Let $u = u'a^2u''$, $u', u'' \in A^*$ such that u'' does not contain a^2 as a factor and $a \notin \mathrm{pref}(u'')$. Then u is a member of one of the classes $u'a^2$, $u'a^2b$, $u'a^2b^2v$, $u'a^2ba$, $u'a^2babv$, $v \in A^*$. All cases are once again treated by Z using 3.1.2. □

Lemma 3.2.8. *Z is a finite maximal separating set and $|Z| = 3$ if and only if $Z \in \{\{a^2b^2, a^2bab^2, a^2babab\}, \{a^2b^3, a^2b^2ab, a^2bab\}, \{a^3b^2, a^2ba^2b^2, a^2bab\}, \{a^2b^2, a^3bab, a^2ba^2bab\}, \{a^3b^2, a^3bab, a^3ba^2b\}\}$.*

Proof. Let Z be a finite maximal separating set and $|Z| = 3$. According to 3.2.6 $m \in \{1, 2\}$. If $m = 2$ then there exist $k_0, k_1, k_2, l_0, l_1 \geq 2$ and $z_0, z_1, z_2 \in Z$ such that $z_0 = a^{k_0}b^{l_0}$, $z_1 = a^{k_1}bab^{l_1}$, $z_2 = a^{k_1}babab$. Similarly as in lemma 3.2.7 we obtain that $Z = \{a^2b^2, a^2bab^2, a^2babab\}$.

If $m = 1$ then there exist $k_0, k_1, l_0 \geq 2$ and $z_0, z_1 \in Z$ such that $z_0 = a^{k_0}b^{l_0}$, $z_1 = a^{k_1}bab$. Consider the word $a^N ba^2 b^N$. Z is a maximal separating set and hence there exists, according to lemma 3.1.2, an element of Z which is a factor of $a^N ba^2 b^N$. This yields that either $k_0 = 2$ or $z' = a^{k'}ba^2b^{l'}$, $z' \in Z$ and $k_0 \geq 3$. In the latter case, by choosing more appropriate words, we obtain that $Z = \{a^3b^2, a^2ba^2b^2, a^2bab\}$. Let further $k_0 = 2$. Consider the word $a^N ba^2 bab^N$. Either $k_1 = 2$ or $z' = a^{k'}ba^2bab^{l'}$, $k_1 \geq 3$ or $z' = a^{k'}ba^2b$, $k_1 \geq 3$. In the second case, we obtain $Z = \{a^2b^2, a^3bab, a^2ba^2bab\}$, in the third case $Z = \{a^3b^2, a^3bab, a^3ba^2b\}$. If $k_0 = k_1 = 2$ then $l_0 \geq 3$ (we want Z to be three-element set) and hence $Z = \{a^2b^3, a^2b^2ab, a^2bab\}$.

All the possible sets are obviously separating. The maximality can be proved similarly as in 3.2.7. □

Lemma 3.2.9. *Z is a finite maximal separating set and $|Z| = 4$ if and only if $Z \in \{\{a^2b^2, a^2bab^2, a^2bababab\}, \{a^2b^2, a^2bab^3, a^2bab^2ab, a^2bababab\}, \{a^2b^3, a^2b^2ab, a^2bab^2, a^2bababab\}, \{a^2b^4, a^2b^3ab, a^2b^2ab, a^2bab\}, \{a^2b^3, a^2b^2ab^2, a^2b^2ababab, a^2bab\}, \{a^4b^2, a^2ba^3b^2, a^2ba^2b^2, a^2bab\}, \{a^3b^2, a^3ba^2b^2, a^2ba^2ba^2b^2, a^2bab\}, \{a^3b^2, a^2ba^2b^2, a^3bab, a^2ba^2bab\}, \{a^2b^2, a^4bab, a^2ba^3bab, a^2ba^2bab\}, \{a^2b^2, a^3bab, a^3ba^2bab, a^2ba^2ba^2bab\}, \{a^3b^2, a^4bab, a^3ba^2b, a^3ba^3bab\}, \{a^3b^2, a^3bab, a^4ba^2b, a^3ba^3ba^2b\}, \{a^4b^2, a^3ba^3b^2, a^3bab, a^3ba^2b\}, \{a^4b^2, a^4bab, a^4ba^2b, a^4ba^3b\}\}$.*

Proof. The proof is purely technical and all required techniques were already introduced, henceforth we note only the result. □

3.3 More properties

In this subsection further properties of maximal separating sets are studied. We recall that we assume that finite maximal separating sets have at least two elements (and does not equal A), are of left type and their elements begin with a (and end with b).

Proposition 3.3.1. *For every $n \in \mathbb{N}$ there exists finite maximal separating set Z, $|Z| = n$.*

Proof. Case $n = 1$ is treated by 3.2.4. Let $n \geq 2$ and $Z = \{a^2(ba)^ib^2, a^2(ba)^{n-1}b; i = 0, \ldots, n-2\}$. Z is separated (the squares at the beginning and the end of the words succesfully blocks any overlap). The maximality can be proved similarly as in 3.2.7. Let $u \in A^+$ be such that a^2 is not a factor of u. Then either $u = a$ or $u = bv$ or $u = abv$, $v \in A^*$. All cases can be treated easily by 3.1.2. Let $u = u'a^2u''$, $u', u'' \in A^*$ such that u'' does not contain a^2 as a factor and $a \notin \mathrm{pref}(u'')$. Then u is a member of one of the classes $u'a^2(ba)^i$, $u'a^2(ba)^ib$, $u'a^2(ba)^ib^2v$, $u'a^2(ba)^{n-1}bv$, $i = 0, \ldots, n-1$, $v \in A^*$. All cases are once again treated using 3.1.2. □

Remark 3.3.2. $\{a^nba^ib; i = 0, \ldots, n-1\}$, $n \geq 2$ are finite maximal separating sets.

Proposition 3.3.3. *Let $Z = \{z^{(1)}, z^{(2)}, \ldots, z^{(n)}\}$ be a finite maximal separating set. Then $z^{(i)} = a^{k^{(i)}}bu^{(i)}a^{l^{(i)}}b$, $u^{(i)} \in A^*$, $i = 1, \ldots, n$, $k^{(i)} \geq 2$, $l^{(i)} \geq 0$ and* $\min\ k^{(i)} = \max\ l^{(i)} + 1$.

Proof. The shape of elements of Z is immediate consequence of 3.2.4 ($a^mb \in Z$ would mean that $Z = \{a^mb\}$, a contradiction with $|Z| \geq 2$). Let $k = \min\ k^{(i)}$ and $l = \max\ l^{(i)}$. If $k \leq l$ then we get a contradiction with Z being separating (there is an element of Z with suffix a^lb and an element of Z with prefix a^kb). Consider the word $u = (a^{l+1}b)^N$. Z is maximal separating set

and hence according to 3.1.2 there exists $z \in Z$ which overlaps with u, thus $k \leq l + 1$. □

We will call the l from the proof of the preceding proposition a characteristic power (of set Z).

Remark 3.3.4. For every $l \in \mathbb{N}$ there exists a finite maximal separating set such that l is its characteristic power.

Proof. For $l = 1$ we can take arbitrary set from the proof of 3.3.1, for $l \geq 2$ we can take sets from 3.3.2. □

Lemma 3.3.5. *Let Z be a finite maximal separating set and $z \in Z$. Then $a^2 \in \mathrm{pref}(z)$.*

Proof. Z is of left type and hence $a^k(ba)^m b \in Z$ for some $k \geq 2$ and $m \geq 1$. In order to maintain Z separating the statement must hold. □

Let Z be a finite maximal separating set. From 3.1.2 we already know that for every $u \in A^+$ there exists $z \in Z$ such that u and z have non-trivial overlap. Surprisingly, we can say more about the overlap:

Proposition 3.3.6. *Let Z be a finite maximal separating set and $u \in A^+$, $|u| \geq 2$. Then there exists $z \in Z$ such that (at least) one of following conditions takes place:*

(1) z is a factor of u;

(2) u is a factor of z;

(3) there exists $v \in \mathrm{pref}(z) \cap \mathrm{suff}(u)$ such that $|v| \geq 2$;

(4) there exists $v \in \mathrm{pref}(u) \cap \mathrm{suff}(z)$ such that $|v| \geq 2$.

Proof. Let $u \in A^+$. Consider the word $a^N u b^N$. According to 3.1.2, there exists $z \in Z$ such that z is a factor of $a^N u b^N$. Clearly, z is not a factor of any of words a^{N+1}, $a^N b$, $a b^N$, b^{N+1} (under given assumptions on Z) and hence z has with u overlap of length at least 2. □

4 Zeropotent semirings

4.1 General approach

Let S be a semiring. A non-empty subset I of S is called *a bi-ideal* of S if $(S+I) \cup SI \cup IS \subseteq I$ (i.e., I is an ideal both of the additive and the multiplicative semigroup of the semiring S). A semiring S will be called *bi-ideal-simple* if $|S| \geq 2$ and $I = S$ whenever I is a bi-ideal of S with $|I| \geq 2$. Immediately from definitions, we receive:

Proposition 4.1.1. *Every congruence-simple semiring is bi-ideal-simple.*

Proof. If I is a bi-ideal, then the relation $(I \times I) \cup \mathrm{id}_S$ is a congruence of S. □

Let S be an additively zeropotent semiring. This means that there exists an element o in S such that $s + s = o = o + s$ for every $s \in S$. Let $\mathrm{Ann}(s) = \{t \in S; s + t = o\}$.

Lemma 4.1.2. *Let S be a zs-semiring and $\sim$ a congruence on S. Then $[o]_\sim$ is a bi-ideal of S.*

Proof. Obvious. □

Proposition 4.1.3. *Let S be an additively zeropotent semiring such that $S = S + S$ and $SS \neq o$. S is congruence simple iff S is bi-ideal simple and for all $r, s \in S$, $r \neq s$, there exist $t, t' \in W$ such that $\mathrm{Ann}(trt') \neq \mathrm{Ann}(tst')$.*

Proof. If S is congruence simple, then it is bi-ideal simple. It is easy to see that relation $\sim$, defined as $r \sim s$ iff for all $t, t' \in W$ $\mathrm{Ann}(trt') = \mathrm{Ann}(tst')$ is a congruence. Hence, $\sim = \mathrm{id}_S$ ($\sim = S \times S$ would mean that $\mathrm{Ann}(s) = \mathrm{Ann}(o) = S$ for every $s \in S$ and hence $S + S = o$) and for all $r, s \in S$, $r \neq s$, there exist $t, t' \in S$ such that $\mathrm{Ann}(trt') \neq \mathrm{Ann}(tst')$.

Suppose now that S is bi-ideal simple, for all $r, s \in S$, $r \neq s$, there exist $t, t' \in W$ such that $\mathrm{Ann}(trt') \neq \mathrm{Ann}(tst')$ and $\sim$ is a congruence on S, $\sim \neq \mathrm{id}_S$. Then there exist $r, s \in S$, $r \neq s$, such that $r \sim s$. Moreover, there exist $t, t' \in S$ such that $\mathrm{Ann}(trt') \neq \mathrm{Ann}(tst')$, hence there exists $t'' \in S$ such that $trt' + t'' \neq tst' + t''$, $o \in \{trt' + t'', tst' + t''\}$. Since $trt' + t'' \sim tst' + t''$, $[o]_\sim \neq \{o\}$. S is bi-ideal simple, thus $[o]_\sim = S$ and $\sim = S \times S$. □

The preceding proposition connects congruence-simplicity and bi-ideal-simplicity for our particular class of semirings much stronger than it is possible in general.

Following few simple lemmas show the way for obtaining a bi-ideal-simple semiring. We denote by B_s the bi-ideal generated by s.

Lemma 4.1.4. *Let S be an additively zeropotent semiring such that $S = S + S$ and $SS \neq o$ and $s, t \in S$. Then $B_{s+t} \subseteq B_s$, $B_{st} \subseteq B_s$ and $B_{ts} \subseteq B_s$.*

Proof. Obvious. □

Lemma 4.1.5. *$B = \{s \in S \mid B_s \neq S\}$ is a bi-ideal and S/B is bi-ideal simple.*

Proof. Easy. □

4.2 Construction pattern

Let T denote the set of all finite subsets of A^+ (A is a finite alphabet, $|A| = n$). Now, define an operation addition on T by $E + F = E \cup F$ if $E \neq \emptyset \neq F$, $E \cap F = \emptyset$, and $E + F = \emptyset$ otherwise. It is easy to see that $T(+)$ is a free zeropotent commutative semigroup over A^+, $o_T = \emptyset$ and that $T + T = \{E \in T; |E| \neq 1\} = T \setminus A^+$.

Using the addition, we also define a multiplication on T by $E \cdot F = \sum u_i \cdot v_j$, $u_i \in E$, $v_j \in F$. Again it is quite easy to see that $T(+, \cdot)$ becomes a free zeropotent semiring over the set A.

Let $Z \subset A^+$ be a strongly separating set such that $|z| \geq 2$ for every $z \in Z$ and $Z_1, Z_2, \ldots, Z_n$ be such that $Z_i \neq \emptyset$, $Z_1 \cup Z_2 \cup \cdots \cup Z_n = Z$ and $Z_i \cap Z_j = \emptyset$, $i \neq j$ (this means, amongst others, that $|Z| \geq n$). Put $\beta = \{(ua_iv, u \sum_{z \in Z_i} zv); i = 1, \ldots, n,\ u, v \in A^*\}$, denote by γ the transitive closure of β and denote by α the reflexive and transitive closure of $\beta \cup \beta^{-1}$. One checks immediately that α is just the congruence of the semiring T generated by pairs $(a_i, \sum_{z \in Z_i} z)$, $i = 1, \ldots, n$.

Before we proceed to prove that α is non-trivial congruence, we will check under which conditions $S + S = S$ holds for $S = T/\alpha$. Let $\lhd$ be a relation defined on A as $a_i \lhd a_j$ if $a_i \in \mathrm{alph}(z)$ for some $z \in Z_j$. Let $\lhd^*$ be a reflexive and transitive closure of $\lhd$. These definitions lead immediately to the following lemma:

Lemma 4.2.1. *$S = S + S$ if and only if for every $a_i \in A$ there exists $a_j \in A$ such that $a_j \lhd^* a_i$ and $|Z_j| \geq 2$.*

Corollary 4.2.2. *If $|A| = 2$ then $S = S + S$ if and only if $|Z| \geq 3$.*

Proof. Combine the preceding lemma and reasoning before 3.2.3. □

Let $\psi : Z \to A$ be defined by $\psi(z) = a_i$ for $z \in Z_i$. Let ρ, τ and ξ be defined as in section 2 (i. e. $\rho = \{((uzv, ua_iv); i = 1, \ldots, n\ z \in Z_i\})$.

Lemma 4.2.3. *Let $(s,t) \in \gamma$, $s = \sum_{i=1}^{k} w_i$, $t = \sum_{i=1}^{k'} w'_i$, $w_i \in A^+$ and let $s_0, s_1, \ldots, s_m$ be a β-sequence from s to t, $s_i \neq o$, $0 \leq i \leq m$. Then for every $1 \leq j' \leq k'$ there exists $1 \leq j \leq k$ such that $(w'_{j'}, w_j) \in \xi$.*

Proof. By induction on m. □

Lemma 4.2.4. *Let $r, s, t \in T$ be such that $(s,r) \in \gamma$ and $(s,t) \in \gamma$. Then there exists $s' \in T$ such that $(r,s') \in \gamma \cup \mathrm{id}_T$ and $(t,s') \in \gamma \cup \mathrm{id}_T$.*

Proof. Let $s_0, s_1, \ldots, s_m$ be a β-sequence from s to r. We will prove the assertion by induction on m. If $m = 1$ then $s = ua_iv + s'$, $r = u\sum_{z \in Z_i} zv + s'$ for some $1 \leq i \leq n$, $u, v \in A^*$, $s' \in T$. If $t_0, t_1, \ldots, t_k$ is a β-sequence from s to t, we may obtain a $\gamma \cup \mathrm{id}_T$-sequence $t'_0, t'_1, \ldots, t'_k$ from r to s' where t'_j is derived from t_j, $0 \leq j \leq k$, by replacing occurences of a_i originated in ua_iv by $\sum_{z \in Z_i} z$.

Suppose that for $m \leq k$ assertion holds and let $m = k + 1$. Hence there exists (by induction) $s'_{m-1} \in T$ such that $(s_{m-1}, s'_{m-1}) \in \gamma \cup \mathrm{id}_T$ and $(t, s'_{m-1}) \in \gamma \cup \mathrm{id}_T$. If $s_{m-1} = s'_{m-1}$ then $(t, s_{m-1}) \in \gamma \cup \mathrm{id}_T$ and $(t,r) \in \gamma$, leading to $s' = r$. If $(s_{m-1}, s'_{m-1}) \in \gamma$ then, by induction, there exists $s' \in T$ such that $(r,s') \in \gamma \cup \mathrm{id}_T$ and $(s'_{m-1}, s') \in \gamma \cup \mathrm{id}_T$, and hence $(t,s') \in \gamma \cup \mathrm{id}_T$. □

Corollary 4.2.5. *Let $(s,t) \in \alpha$, $s, t \in T$, $s \neq t$. Then there exists a sequence $s_0, s_1, \ldots, s_m$, $m \geq 1$, such that $s_0 = s$, $s_m = t$ and one of the following three cases takes place:*

(1) $(s_{i-1}, s_i) \in \beta$ for all $1 \leq i \leq m$ (i. e., $(s,t) \in \gamma$);

(2) $(s_i, s_{i-1}) \in \beta$ for all $1 \leq i \leq m$ (i. e., $(t,s) \in \gamma$);

(3) there exists $1 \leq j < m$ such that $(s_{i-1}, s_i) \in \beta$ for all $1 \leq i \leq j$ and $(s_i, s_{i-1}) \in \beta$ for all $j+1 \leq i \leq m$ (i. e., $(s, s_j) \in \gamma$ and $(t, s_j) \in \gamma$);

Proof. Easy consequence of Lemma 4.2.4. □

Lemma 4.2.6. *Let $(s,t) \in \gamma$ and let $s_0, s_1, \ldots, s_m$ be a β-sequence from s to t, $s_i \neq o$, $0 \leq i \leq m$. Let $s = \sum_{i=1}^{k} t_i$, $t_i \in T$. Then there exist $m(i) \in \mathbb{N} \cup \{0\}$, $s_j^{(i)} \in T$, $0 \leq j \leq m(i)$, $1 \leq i \leq k$, such that $s_0^{(i)} = t_i$, $s_0^{(i)}, s_1^{(i)}, \ldots, s_{m(i)}^{(i)}$ is a β-sequence, $m = \sum_{i=1}^{k} m(i)$ and $t = \sum_{i=1}^{k} s_{m(i)}^{(i)}$.*

Proof. By induction on m. □

Lemma 4.2.7. *If $r, s \in T$ are such that $(s,o) \in \gamma$ and $(s,r) \in \beta$ then $(r,o) \in \gamma$.*

Proof. Easy. □

Lemma 4.2.8. *Let $s \in T$. If $(o, s) \in \gamma$ then $(s, o) \in \gamma$.*

Proof. If $(s, o) \in \beta$ then $s = ua_iv + u\sum_{z\in Z_i} zv + s'$, $u, v \in A^*$, $s' \in T$. But then $(u\sum_{z\in Z_i} zv + u\sum_{z\in Z_i} zv + s', s) \in \beta$ and we are done. The rest of proof follows by induction on length of β-sequence from o to s, using 4.2.7. □

Corollary 4.2.9. *Let $(s, o) \in \alpha$, $s \in T$, $s \neq o$. Then there exists a sequence $s_0, s_1, \ldots, s_m$, $m \geq 1$, such that $s_0 = s$, $s_m = o$ and $(s_{i-1}, s_i) \in \beta$ for all $1 \leq i \leq m$ (i. e., $(s, o) \in \gamma$).*

Proof. Easy consequence of 4.2.5 and 4.2.8. □

Proposition 4.2.10. *For every $w \in A^+$ $(w, o) \notin \alpha$.*

Proof. Suppose, for a contradiction, that there exists at least one $w \in A^+$ such that $(w, o) \in \alpha$, and hence, according to Corollary 4.2.9, $(w, o) \in \gamma$. We will choose w and β-sequence $s_0, s_1, \ldots, s_m$ from w to o such that m is minimal. Obviously, $w = ua_kv$, $u, v \in A^*$, $a_k \in A$, $s_1 = u\sum_{z\in Z_k} zv$ and $m > 1$.

Let $Z_k = \{z_1, z_2, \ldots, z_l\}$. If $l = 1$, we get a contradiction with choose of w such that m is minimal and hence we may assume that $l \geq 2$. According to Lemma 4.2.6, there exist $m(i) \in \mathbb{N} \cup \{0\}$, $s_j^{(i)} \in T$, $0 \leq j \leq m(i)$, $1 \leq i \leq l$, such that $s_0^{(i)} = z_i$, $s_0^{(i)}, s_1^{(i)}, \ldots, s_{m(i)}^{(i)}$ is a β-sequence, $m = \sum_{i=1}^{l} m(i)$ and $t = \sum_{i=1}^{l} ks_{m(i)}^{(i)}$. Since $s_m = o$, there exists a word w' which appears twice as a summand in s_m. If both appearances originate in the same $s_{m(i)}^{(i)}$, we obtain a contradiction with minimality of m (we could choose $w = uz_iv$). If w' is a summand of two different $s_{m(i)}^{(i)}$, $s_{m(j)}^{(j)}$ then, according to 4.2.3, $(w', uz_iv) \in \xi$ and $(w', uz_jv) \in \xi$ and we obtain contradiction with 2.17.13 and 2.17.11. □

We have shown that α is a proper congruence of the semiring T. Now, T is a finitely generated algebraic structure, and therefore α is contained in a proper maximal congruence δ of T. Setting $R = T/\delta$ we get a (non-trivial!) congruence-simple semiring R of class (5), and hence such semirings exist. The following subsection deals with particular cases for which more can be said about such a maximal congruence.

4.3 Further steps towards simplicity

Let $A = \{a, b\}$ in this subsection and Z be a strongly separating set, $|Z| \geq 3$ ($Z = Z_a \cup Z_b$). Let S be a zeropotent semiring defined as in the preceding subsection. According to 4.2.2 $S = S + S$ holds.

Lemma 4.3.1. *Following conditions are equivalent for every $w \in A^+$:*

(1) $B_w = S$;

(2) $a \in B_w$;

(3) There exists $w' \in A^+$ such that w is a factor of w' and $(w', a) \in \xi$.

Proof. Easy. □

The following two propositions provides us basic tools to determine which elements of A^+ might be congruent with o (in maximal congruence).

Proposition 4.3.2. *If Z is an almost maximal strongly separating set then for every $w \in A^+$, $B_w = S$ (and hence $w \notin B$).*

Proof. We will proceed by induction on length of w. Clearly, $B_a = B_b = S$. Let $w \in A^+$ be such that $|w| \geq 2$. According to 3.3.6 there exist $u \in A^+$ and $z \in Z$ such that both w and z are factors of u, $|u| \leq |w| + |z| - 2$ and $u \in B_w$. Let w' is made from u through replacing z by an appropriate letter. Then $|w'| < |w|$ (and hence $B_{w'} = S$) and $w' \in B_w$. Therefore $S = B_{w'} \subseteq B_w$. □

Proposition 4.3.3. *If $Z' \supset Z$ is an almost maximal strongly separating set then for every $y \in Z' \setminus Z$, $B_y \neq S$ (and hence $y \in B$).*

Proof. According to 4.3.1 we have to analyze the set K of words which are in τ with a. Obviously, $a \in K$, $Z_a \subset K$ and for every element of K word created by replacing letter a (b, resp.) in it with an element of Z_a (Z_b, resp.) forms another element of K. On the other hand, all elements of K (a excluding) can be achieved from a by finitely many steps of described process. Thus y which does not overlap with any element of Z cannot be an element of K. □

We would like to notice that the preceding proposition does not need the assumption $|A| = 2$.

Lemma 4.3.4. *Let $Z = \{a^2b^2, a^2bab^2, a^2bababab\}$, $Z_a = \{a^2b^2, a^2bab^2\}$ and $Z_b = \{a^2bababab\}$. Then $a^2 + a^4baba + a^5bab \in B$.*

Proof. Let $s = a^2 + a^4baba + a^5bab$. We will prove that B_s does not contain any element of $S \setminus \{o\}$ such that sum of lengths ot its summands is lower than $|a^2| + |a^4baba| + |a^5bab|$. Obviously s contains as summands only reduced words, $s \cdot b = a^2b + a^4bababab + a^5bab^2 = a^2b + a^2b + a^5bab^2 = o$ and $s \cdot ab = a^3b + a^4baba^2b + a^5bababab = a^3b + a^4baba^2b + a^3b = o$. If we multiply s from left by reduced word we will obtain reduced words (as summands) and if we multiply s from right with an element of a^2A^* we wil obtain reduced words as well. Hence summands of s cannot be shortened. □

The preceding lemma showed us that S is not congruence-simple. Unfortunately, it seems that similar witness of non-simplicity may be found for other Z as well, and hence a natural conjecture occurs that S proposed by the construction is not congruence-simple itself for arbitrary Z. The proof of this conjecture and an explicit construction of maximal congruence on S remain open problems.

References

[1] R. El Bashir and T. Kepka, Congruence-simple semirings, *Semigroup Forum*, **75**(2007), 588-608.

[2] R. El Bashir, J. Hurt, A. Jančařík and T. Kepka, Simple commutative semirings, *Journal of Algebra*, **236**(2001), 277-306.

[3] V. Flaška, T. Kepka and J. Šaroch, Bi-ideal-simple semirings, *CMUC* **46**(2005), 391-397.

[4] M. A. Harrison, *Introduction to Formal Language Theory*, *Addison-Wesley*, Reading, 1978.

[5] U. Hebisch and H. J. Weinert, *Halbringe – Algebraische Theorie und Anwendungen in der Informatik, Teubner*, Stuttgart, 1993.

[6] U. Hebisch and H. J. Weinert, *Semirings and semifields* in *Handbook of Algebra, Vol. 1*, pp. 425-462, *Elsevier*, New York, 1995.

[7] M. Lothaire, *Algebraic Combinatorics on Words*, *Cambridge University Press*, Cambridge, 2002.

[8] A. de Luca, *Finiteness and Regularity in Semigroups and Formal Languages*, *Springer-Verlag New York, Inc.*, Secaucus, 1999.

[9] C. Monico, On finite congruence-simple semirings, *Journal of Algebra*, **271**(2004), 846-854.

[10] Terese, *Term Rewriting Systems*, *Cambridge University Press*, Cambridge, 2003.

[11] J. Zumbrägel, *Classification of finite congruence-simple semirings with zero*, (preprint).