ONE VERY PARTICULAR EXAMPLE OF A CONGRUENCE-SIMPLE SEMIRING

VÁCLAV FLAŠKA

ABSTRACT. The existence of congruence-simple semiring S with non-constant multiplication such that $2s = 3t$ for all $s, t \in S$ and $S + S = S$ is proved and hence the most enigmatic class of congruence-simple semirings is not empty.

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 [3] and [4]). Congruence-simple objects (i.e., those possesing precisely two congruence relations) 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 the case for semirings, however. Congruence-simple commutative (finite, resp.) semirings 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 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 [5], [6]). On the other hand, it seems that no example of a congruence-simple semiring of class (5) with non-constant multiplication is known so far. The aim of the present modest note is to show that the class (5) is not empty. Employed methods are purely combinatorial.

2. FIRST STEPS

First of all, notice that a semiring S is zeropotent if and only if S contains a bi-absorbing element o $(= o_S)$ and $2a = o$ for every $a \in S$ ($2s = 2t$ and $2s + t = 2t + t = 3t = 2s$, $s, t \in S$). Let $A = \{a, b\}$ be a two-element set, A^* the free monoid

Date: September 15, 2008.
The work is a part of the research project MSM0021620839 financed by MSMT.

over A (the elements of A^* are non-empty words containing the letters a, b and the empty word ε) and let $A^+ = A^* \setminus \{\varepsilon\}$ (notice that A^+ is the free semigroup over A).

Let T denote the set of all finite subsets of A^+. 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 the 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 the free zeropotent semiring over the two-element set A. In the following text we will use u instead of $\{u\}$, $u \in A^+$, $u_1 + \cdots + u_n$ instead of $\{u_1, \ldots, u_n\}$ and elements of T will be usually denoted by s, t.

Now, put $\beta = \{(uav, ua^2b^2v + ua^2bab^2v), (ubv, ua^2bababv); u, v \in A^*\}$ and denote by α the congruence closure of $\beta \cup \beta^{-1}$. One checks immediately that α is just the congruence of the semiring T generated by the pairs $(a, a^2b^2 + a^2bab^2)$ and (b, a^2babab).

3. Why is α a proper congruence

Put $\rho = \{(ua^2b^2v, uav), (ua^2bab^2v, uav), (ua^2bababv, ubv); u, v \in A^*\}$ and denote by τ the transitive closure of ρ. Clearly, if $w, z \in A^+$ then $(w, z) \in \tau$ if and only if there exists $s \in T \cup \{0\}$ such that the pair $(w + s, z)$ is in the transitive closure of β.

Proposition 1. *There exists at least one $w \in A^+$ such that $(w, o) \in \alpha$ if and only if there exist elements $u, v \in A^*$ and $x \in A^+$ such that $(x, ua^2b^2v) \in \tau$ and $(x, ua^2bab^2v) \in \tau$.*

Proof. The converse implication is almost trivial. If there are such elements u, v and x then $(uav, ua^2b^2v + ua^2bab^2v) \in \alpha$ and there exist $s_1, s_2 \in T \cup \{0\}$ such that $(x + s_1, ua^2b^2v) \in \alpha$ and $(x + s_2, ua^2bab^2v) \in \alpha$. Hence $(uav, x + s_1 + x + s_2) \in \alpha$ and $x + s_1 + x + s_2 = o$.

The direct implication is only a bit more tricky. Suppose that there exists $w \in A^+$ such that $(w, o) \in \alpha$ and consider $s_0, \ldots, s_n \in T$ such that $s_0 = w$, $s_n = o$ and $(s_{i-1}, s_i) \in \beta \cup \beta^{-1}$. We may assume that n is minimal. Now, $w = uav$, $s_1 = ua^2b^2v + ua^2bab^2v$ for some $u, v \in A^*$, $(ua^2b^2v, o) \notin \alpha$ and $(ua^2bab^2v, o) \notin \alpha$ and hence there exist $x \in A^+$ and $t_1, t_2 \in T \cup \{0\}$ such that $(ua^2b^2v, x + t_1) \in \alpha$ and $(ua^2bab^2v, x + t_2) \in \alpha$. If $(x, ua^2b^2v) \in \tau$ and $(x, ua^2bab^2v) \in \tau$ we are through. In the other case we may find $x' \in A^+$ such that $(x', x) \in \tau$, $(x', ua^2b^2v) \in \tau$ and $(x', ua^2bab^2v) \in \tau$ by "walking back" all the steps where we used β^{-1} (notice that if $(w, o) \in \beta^{-1}$ then $(w, o) \in \beta$). □

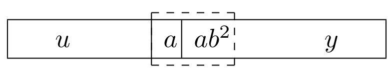
Suppose now that there exist $u, v \in A^*$ and $x \in A^+$ such that $(x, ua^2b^2v) \in \tau$ and $(x, ua^2bab^2v) \in \tau$. Assume that $|u| + |v|$ is minimal (hence neither u nor v contains any of the words a^2b^2, a^2bab^2, a^2babab as a factor) and that x is the shortest possible for (already chosen) u, v. Using standard combinatorial methods it is not difficult to see (words containing other than belowmentioned occurrences of the words a^2b^2, a^2bab^2, a^2babab as a factor can be easily shortened) that $x = ua^2b^2ya^2bab^2v$ (or $x = ua^2bab^2ya^2b^2v$) for some $y \in A^*$ and, moreover, $(ya^2bab^2v, v) \in \tau$ and $(ua^2b^2y, u) \in \tau$ ($(ya^2b^2v, v) \in \tau$ and $(ua^2bab^2y, u) \in \tau$), $u, v \in A^+$. According to the choice of x, we see that y is reduced. Henceforth, $(yav, v) \in \tau$ and $(uay, u) \in \tau$. The following proposition will show that the existence of such u, v and y yields a contradiction.

Proposition 2. *There are no words $u, v \in A^+$, $y \in A^*$ and $c \in A$ such that $(ycv, v) \in \tau$ and $(ucy, u) \in \tau$.*

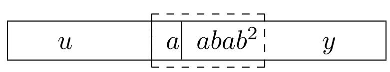
Proof. Proceeding by contradiction, assume that there exist u, v and y such that $|u|+|v|$ is minimal (this means that neither u nor v contains any of the words a^2b^2, a^2bab^2, a^2babab as a factor). Let y be the shortest possible for given u and v (once again, this means that y does not contain any of the words a^2b^2, a^2bab^2, a^2babab as a factor).

First, let $c = a$. Since $(uay, u) \in \tau$ and u and y do not contain any of the words a^2b^2, a^2bab^2, a^2babab as a factor, a in uay must be a factor of one of these words. Thus we have to distinguish the following nine cases:

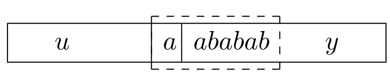
(1) $y = ab^2y'$. Notice that from $(yav, v) \in \tau$ we may deduce that $v = ab^2v'$ (ab^2 as a prefix of v cannot take part in any ρ-step). Thus $(ab^2y'a^2b^2v', ab^2v') \in \tau$, $(y'a^2b^2v', v') \in \tau$ and hence $(y'av', v') \in \tau$. Moreover, $(uay', u) \in \tau$ ($(ua^2b^2y', u) \in \tau$), a contradiction with the minimality of $|u| + |v|$.



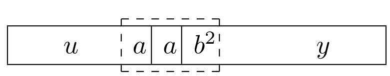
(2) $y = abab^2y'$. Similarly as in the preceding case, $v = abab^2v'$ and $(y'av', v') \in \tau$ and $(uay', u) \in \tau$, a contradiction with the minimality of $|u| + |v|$.



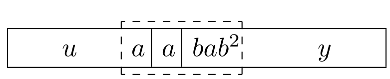
(3) $y = abababy'$. Similarly as in the preceding cases, $v = abababv'$ and $(y'bv', v') \in \tau$ and $(uby', u) \in \tau$, a contradiction with the minimality of $|u| + |v|$.



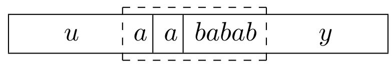
(4) $u = u'a$ and $y = b^2y'$. Similarly as in the preceding cases, $v = b^2v'$ and hence $(y'ab^2v', v') \in \tau$. Thus $y' \in \{y''a, y''a^b; y'' \in A^*\}$ but if we repeat now the argument used to get $v = b^2v'$, we obtain that a suffix of u and y' must coincide, and so $y' = y''a$ and $(u'ay''a, u'a) \in \tau$, $(u'ay'', u') \in \tau$ and $(y''av', v') \in \tau$, a contradiction with the minimality of $|u| + |v|$.



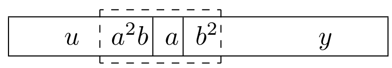
(5) $u = u'a$ and $y = bab^2y'$. Similarly as in the preceding cases, $v = bab^2v'$, $y = bab^2y''a$ and $(u'ay'', u') \in \tau$ and $(y''av', v') \in \tau$, a contradiction with the minimality of $|u| + |v|$.



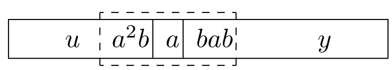
(6) $u = u'a$ and $y = bababy'$. Similarly as in the preceding cases, $v = bababv'$, $y = bababy''a$ and $(u'by'', u') \in \tau$ and $(y''bv', v') \in \tau$, a contradiction with the minimality of $|u| + |v|$.



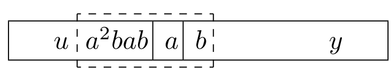
(7) $u = u'a^2b$ and $y = b^2y'$. Similarly as in the preceding cases, $v = b^2v'$, $y = b^2y''a^2b$ and $(u'ay'', u') \in \tau$ and $(y''av', v') \in \tau$, a contradiction with the minimality of $|u| + |v|$.



(8) $u = u'a^2b$ and $y = baby'$. Similarly as in the preceding cases, $v = babv'$, $y = baby''a^2b$ and $(u'by'', u') \in \tau$ and $(y''bv', v') \in \tau$, a contradiction with the minimality of $|u| + |v|$.

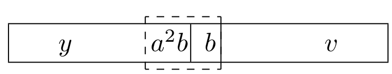


(9) $u = u'a^2bab$ and $y = by'$. Similarly as in the preceding cases, $v = bv'$, $y = by''a^2bab$ and $(u'by'', u') \in \tau$ and $(y''bv', v') \in \tau$, a contradiction with the minimality of $|u| + |v|$.

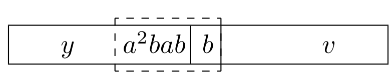


Now, let $c = b$. Since $(ybv, v) \in \tau$ and v and y do not contain any of the words a^2b^2, a^2bab^2, a^2babab as a factor, b in ybv must be a factor of one of these words. Thus we have to distinguish the following eight cases, quite parallel to the preceding nine ones:

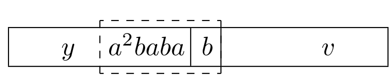
(1) $y = y'a^2b$. According to the foregoing part, $u = u'a^2b$ and $(u'ay', u') \in \tau$ and $(y'av, v) \in \tau$, a contradiction with the minimality of $|u| + |v|$.



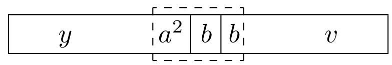
(2) $y = y'a^2bab$. Similarly as in the preceding case $u = u'a^2bab$ and $(u'ay', u') \in \tau$ and $(y'av, v) \in \tau$, a contradiction with the minimality of $|u| + |v|$.



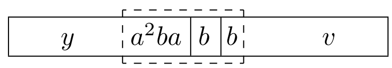
(3) $y = y'a^2baba$. Similarly as in the preceding cases $u = u'a^2baba$ and $(u'by', u') \in \tau$ and $(y'bv, v) \in \tau$, a contradiction with the minimality of $|u| + |v|$.



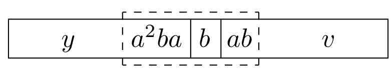
(4) $v = bv'$ and $y = y'a^2$. Similarly as in the preceding case (4), $u = u'a^2$, $y' = by''$, $(u'ay'', u') \in \tau$ and $(y''av', v') \in \tau$, a contradiction with the minimality of $|u| + |v|$.



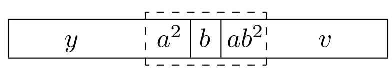
(5) $v = bv'$ and $y = y'a^2ba$. Similarly as in the preceding case, $u = u'a^2ba$, $y' = by''$, $(u'ay'', u') \in \tau$ and $(y''av', v') \in \tau$, a contradiction with the minimality of $|u| + |v|$.



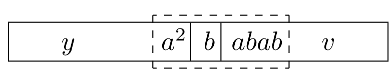
(6) $v = abv'$ and $y = y'a^2ba$. Similarly as in the preceding cases, $u = u'a^2ba$, $y' = aby''$, $(u'by'', u') \in \tau$ and $(y''bv', v') \in \tau$, a contradiction with the minimality of $|u| + |v|$.



(7) $v = ab^2v'$ and $y = y'a^2$. Similarly as in the preceding cases, $u = u'a^2$, $y' = ab^2y''$, $(u'ay'', u') \in \tau$ and $(y''av', v') \in \tau$, a contradiction with the minimality of $|u| + |v|$.



(8) $v = ababv'$ and $y = y'a^2$. Similarly as in the preceding cases, $u = u'a^2$, $y' = ababy''$, $(u'by'', u') \in \tau$ and $(y''bv', v') \in \tau$, a contradiction with the minimality of $|u| + |v|$.



□

4. A very short comment

We have shown that α is a proper congruence of the semiring T. The congruence α was generated by the pairs $(a, a^2b^2 + a^2bab^2)$ and (b, a^2babab) and hence $R = T/\alpha$ satisfies $R = R + R$ (and multiplication on R is non-constant). Now, let γ be a congruence of T containing α and maximal with respect to $(a, o) \notin \gamma$. Obviously, γ is a maximal conngruence of T. Setting $S = T/\gamma$ we get a (non-trivial!) congruence-simple semiring S of class (5) with $S = S + S$ and non-constant multiplication, and hence such semirings exist. Unfortunately, any explicite and transparent construction of these semirings remains an open problem.

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] U. Hebisch and H. J. Weinert, *Halbringe – Algebraische Theorie und Anwendungen in der Informatik, Teubner*, Stuttgart, 1993.
[4] U. Hebisch and H. J. Weinert, *Semirings and semifields* in *Handbook of Algebra, Vol. 1*, pp. 425-462, *Elsevier*, New York, 1995.
[5] C. Monico, On finite congruence-simple semirings, *Journal of Algebra*, **271**(2004), 846-854.
[6] J. Zumbrägel, Classification of finite congruence-simple semirings with zero, (preprint).

MFF UK, Sokolovská 83, 18600 Praha 8
E-mail address: flaska@karlin.mff.cuni.cz