ELSEVIER

Available at
www.ComputerScienceWeb.com
POWERED BY SCIENCE @ DIRECT®

Theoretical Computer Science 307 (2003) 117–127

Theoretical
Computer Science

www.elsevier.com/locate/tcs

Semiretracts—a counterexample and some results

Wit Foryś[a,*], Tomasz Krawczyk[a], James A. Anderson[b]

[a] *Institute of Computer Science, Jagiellonian University, Nawojki 11, 30-075 Krakow, Poland*
[b] *University of South Carolina at Spartanburg, Spartanburg, SC 29303, USA*

Abstract

In the paper (Theoret. Comput. Sci. 237 (2000)) Anderson present a theorem which characterizes any semiretract S by means of two retracts R_α and R_ω. The first part of the paper contains a counterexample for this characterization. Then some results are presented which finally lead to the theorem which determines for a given semiretract S the minimal number of retracts $R_1,\dots,R_m$ such that the equality $S = \bigcap_{i=1}^m R_i$ holds.

MSC: 68Q

Keywords: Semiretract; Retract; Free monoid

1. Introduction

Retracts and semiretracts of free monoids were investigated by Head, Anderson and Forys—see Refs. [1–8]. In paper [2], Anderson proved a theorem which gives a characterization of any semiretract S by means of two retracts R_α and R_ω. Namely, the theorem states the equality $S = R_\alpha \cap R_\omega$. Unfortunately, the result appears to be not true. In the first part of the paper we present a counterexample. Then some results are presented which finally lead to the theorem which determines for a given semiretract S the minimal number of retracts $R_1,\dots,R_m$ such that the equality $S = \bigcap_{i=1}^m R_i$ holds.

2. Counterexample

Definition 1. A retraction $r : A^* \to A^*$ is a homomorphism for which $r \circ r = r$. A retract of A^* is the image of $A^*$by a retraction. A semiretract of A^* is the intersection of a family of retracts of A^*.

* Corresponding author.
E-mail addresses: forysw@ii.uj.edu.pl (W. Foryś), tomasz.krawczyk.student@softlab.ii.uj.edu.pl (T. Krawczyk), jim@gw.uscs.edu (J.A. Anderson).

0304-3975/03/$ - see front matter
doi:10.1016/S0304-3975(03)00096-3

Definition 2. A word $w \in A^*$ is called a key-word if there is at least one letter in A that occurs exactly once in w. A letter that occurs once in a key-word w is called a key of w. A set $C \subset A^*$ of key-words is called key-code if there exists an injection $i : C \to A$ for which
(1) for any $w \in C$, $i(w)$ is a key of w,
(2) the letter $i(w)$ occurs in no word of C other than w itself.

Theorem 3. (Head [8]) *$R \subset A^*$ is a retract of A^* iff $R = C^*$ where C is a key-code.*

In [2] Anderson proved the following.

Theorem 4. *For any semiretract S there exist two retracts R_α and R_ω such that $S = R_\alpha \cap R_\omega$.*

The theorem appears to be incorrect according to the counterexample presented below. We use the following notation. $A = \{a, b, c, d, e, f, g, h, i, s\}$—an alphabet used in the counterexample, C_1, C_2, C_3—key-codes of retracts C_1^*, C_2^*, C_3^*, respectively, C—a code of the submonoid $C_1^* \cap C_2^* \cap C_3^*$, C_α, C_ω—key-codes for retracts C_α^*, C_ω^* such that $C_\alpha^* \cap C_\omega^* = C_1^* \cap C_2^* \cap C_3^*$ if exist, when words $sas \in C_1, as \in C_2, sa \in C_3$ where s, a are letters in the alphabet A, a is a key and C_i are key-codes for $i = 1, 2, 3$ then we write this fact in a matrix form (abbreviated three lines):

$$A_a = \begin{bmatrix} 1 & & 1 \\ 0 & a & 1 \\ 1 & & 0 \end{bmatrix}.$$

Hence 1 stays for the letter s, 0 for the empty word. The above matrix is associated with the key a. We denote in the sequel by $col_1(a)$ and $col_3(a)$, respectively, the first and the third column of A_a, the matrix associated with a. Now let us consider the following key-codes C_i given in the matrix form:

$$\begin{array}{l} C_1: \\ C_2: \\ C_3: \end{array} \quad A_a = \begin{bmatrix} 0 & & 1 \\ 0 & a & 0 \\ 0 & & 0 \end{bmatrix}, \quad A_b = \begin{bmatrix} 0 & & 1 \\ 1 & b & 0 \\ 1 & & 1 \end{bmatrix}, \quad A_c = \begin{bmatrix} 0 & & 0 \\ 1 & c & 1 \\ 0 & & 1 \end{bmatrix},$$

$$A_d = \begin{bmatrix} 1 & & 1 \\ 0 & d & 0 \\ 0 & & 1 \end{bmatrix}, \quad A_e = \begin{bmatrix} 0 & & 1 \\ 1 & e & 0 \\ 0 & & 0 \end{bmatrix}, \quad A_f = \begin{bmatrix} 0 & & 1 \\ 1 & f & 0 \\ 1 & & 1 \end{bmatrix},$$

$$A_g = \begin{bmatrix} 0 & & 1 \\ 1 & g & 0 \\ 0 & & 0 \end{bmatrix}, \quad A_h = \begin{bmatrix} 0 & & 0 \\ 1 & h & 1 \\ 1 & & 1 \end{bmatrix}, \quad A_i = \begin{bmatrix} 1 & & 0 \\ 0 & i & 0 \\ 0 & & 0 \end{bmatrix}.$$

It is easy to observe that any word in the semiretract $C_1^* \cap C_2^* \cap C_3^*$ has to start in a and finish in i. Now we define two equivalence relations on the set of keys, that is on $K = \{a, b, c, d, e, f, g, h, i\}$. Key letters x, y are in relation xPy iff $col_1(x) = col_1(y)$. Key letters x, y are in relation xSy iff $col_3(x) = col_3(y)$. The set $K_{/P}$ has the following blocks: $P_1=\{a\}$, $P_2=\{b,f,h\}$, $P_3=\{c,e,g\}$, $P_4=\{d,i\}$. The set $K_{/S}$ has the following blocks: $S_1=\{a,e,g\}$, $S_2=\{b,d,f\}$, $S_3=\{c,h\}$, $S_4=\{i\}$. Similarly as in the above matrix form one can write codes C_α and C_ω. In this case we have matrices 2×2. These matrices will be denoted in the sequel by $\bar{A}_x$. We define a product of the above introduced matrices in the following way:

$$\begin{bmatrix} a_{11} & & a_{13} \\ a_{21} & x & a_{23} \\ a_{31} & & a_{33} \end{bmatrix} \otimes \begin{bmatrix} b_{11} & & b_{13} \\ b_{21} & y & b_{23} \\ b_{31} & & b_{33} \end{bmatrix} = \begin{bmatrix} a_{11} & & b_{13} \\ a_{21} & xy & b_{23} \\ a_{31} & & b_{33} \end{bmatrix},$$

if and only if

$$col_3(x) + col_1(y) = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

Hence with the product $A_x \otimes A_y$ a word xy is associated.

Fact 5. *The fact that* $w\in C^*$ *is equivalent to executing the product*

$$A_a \otimes \cdots \otimes A_i = \begin{bmatrix} 0 & & 0 \\ 0 & k(w) & 0 \\ 0 & & 0 \end{bmatrix},$$

where $k(w)$ *denotes a word obtained by erasing all* s *in* w. *Note that the letter* a *is the only one which starts words in* C *and the letter* i *is the only one which ends such words.*

Example 6. $w = asbscsi \in C^*$ *is obtained by executing*

$$A_a \otimes A_b \otimes A_c \otimes A_i.$$

We will use in the sequel all above introduced notations also in the case of an individual key-code C_n and retracts. In particular, for a key-word $s_1 a s_2$ we denote by $col_1^n(a)$ and $col_3^n(a)$, respectively, the first and the third column of the matrix connected with $a - A_a = [s_1\ a\ s_2]$ that is s_1 and s_2 in the considered case. In the code C there is no word in which two keys occur because such case would imply that these two keys appear always in the fixed order. It is easy to observe that if there is a possibility to execute the product $A_a \otimes \cdots \otimes A_x \otimes \cdots \otimes A_y \otimes \cdots \otimes A_i$ then it is possible to execute the product $A_a \otimes \cdots \otimes A_y \otimes \cdots \otimes A_x \otimes \cdots \otimes A_i$ for all $x, y \in \{b,\ldots,h\}$. This observation implies:

Fact 7. *If there exist key-codes* C_α *and* C_ω *such that* $C_\alpha^* \cap C_\omega^* = C_1^* \cap C_2^* \cap C_3^*$ *then for any* $w \in C_\alpha \cup C_\omega$ *is* $|w| \leqslant 3$.

Fact 8. *For any key* $x \neq i$ *the equality* $col_3^\alpha(x) = col_3^\omega(x)$ *does not hold. Hence* $col_3^\alpha(x) = 1 - col_3^\omega(x)$.

In the opposite situation one can find a word associated with $A_a \otimes \cdots \otimes A_x$ which is in $C_\alpha^* \cap C_\omega^*$. Arguing the same way we have:

Fact 9. *For any key $x \neq a$ the equality $col_1^\alpha(x) col_1^\omega(x)$ does not hold. Hence, $col_1^\alpha(x) = 1 - col_1^\omega(x)$.*

Any executable product of matrices $A_a \otimes \cdots \otimes A_i$ should be executable as $\bar{A}_a \otimes \cdots \otimes \bar{A}_i$. Hence:

Fact 10. *col_1^α is constant on S_i and col_3^α is constant on P_i for $i = 1, \ldots, 4$. The same is true for col^ω.*

Now let us consider the following product of matrices:

$$A_a \otimes A_b \otimes A_c \otimes A_i.$$

For this product we have $k(w) = abci$ and finally the word $asbscsi \in C$. Hence, the following product should be executable:

$$\bar{A}_a \otimes \bar{A}_b \otimes \bar{A}_c \otimes \bar{A}_i$$

to obtain $asbscsi \in C_\alpha^* \cap C_\omega^*$. It is easy to observe that in the last case

$$\text{(a) } col_1(b), col_1(c), col_1(i) \in \left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\}$$

and

$$\text{(b) } col_3(a), col_3(b), col_3(c) \in \left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\}.$$

Hence for example in (a) at least two of the columns are equal, say $col_1(c) = col_1(i)$, and the following product is executable:

$$\bar{A}_a \otimes \bar{A}_b \otimes \bar{A}_i$$

which means that a word w such that $k(w) = abc$ is in $C_\alpha^* \cap C_\omega^*$ but of course not in C^*—a contradiction.

3. Semiretracts as the intersection of retracts

The following theorem of Anderson allows us to narrow down the research on semiretracts to the case when all considered retracts have the same, common key-set K.

Theorem 11 (Anderson [2]). *Let $S = \bigcap_{j=1}^m T_j$ denote a semiretract where T_j are retracts with the key-codes D_j and key-sets K_j, respectively. There exist retracts R_i*

for $i=1,\dots,n$ *with key-codes* C_i *and the common key-set* K *such that*

$$S=\bigcap_{i=1}^{m} R_i$$

and $\#K_j \geqslant \#K$ *for* $j=1,\dots,m$.

The common set of keys K is called in the sequel a set of keys of a semiretract S. It is assumed that any k in K occurs in a word of the base of S. As a result of the above theorem the research on semiretracts could be done under the assumption that any semiretract S is given by the intersection of retracts with the same set of keys. We modify a bit the notational convention used in the counterexample. Let $S=\bigcap_{i=1}^{n} R_i$, K a common set of keys. Let us fix the order of retracts—$R_1,\dots,R_n$. For any $k\in K$ there exist words: $w_1\in C_1,\dots,w_n\in C_n$ all with the key k. We write this fact in a matrix form (abbreviated n-lines):

$$A_k=\begin{bmatrix} u_1 & & v_1\\ \vdots & & \vdots\\ u_i & k & v_i\\ \vdots & & \vdots\\ u_n & & v_n \end{bmatrix}.$$

Hence, in the first column of A_k there are prefixes u_i of w_i and in the third column there are suffixes v_i of w_i such that $w_i=u_ikv_i$ for $i=1,\dots,n$. The matrix A_k is associated with the key k. We denote in the sequel by $col_{\mathrm{L}}(k)$ and $col_{\mathrm{R}}(k)$, respectively, the first (left) and the third (right) column of A_k having in mind that the middle column is composed of n copies of the letter k. For any column word vectors define their product $\otimes$ putting

$$\begin{bmatrix} u_1\\ u_2\\ \vdots\\ u_n \end{bmatrix}\otimes\begin{bmatrix} v_1\\ v_2\\ \vdots\\ v_n \end{bmatrix}=\begin{bmatrix} u_1v_1\\ u_2v_2\\ \vdots\\ u_nv_n \end{bmatrix}.$$

Now extend ultimately the product $\otimes$ to the above introduced matrices. Formally, the definition of $\otimes$ should cover any $n\times 3$ word matrices (with word entries). For A_k and $A_{\bar{k}}$ we put:

$$\begin{bmatrix} u_1 & & v_1\\ \vdots & & \vdots\\ u_i & k & v_i\\ \vdots & & \vdots\\ u_n & & v_n \end{bmatrix}\otimes\begin{bmatrix} \overline{u_1} & & \overline{v_1}\\ \vdots & & \vdots\\ \overline{u_i} & \bar{k} & \overline{v_i}\\ \vdots & & \vdots\\ \overline{u_n} & & \overline{v_n} \end{bmatrix}=\begin{bmatrix} u_1\overline{u_1} & & v_1\overline{v_1}\\ \vdots & & \vdots\\ u_i\overline{u_i} & k\bar{k} & v_i\overline{v_i}\\ \vdots & & \vdots\\ u_n\overline{u_n} & & v_n\overline{v_n} \end{bmatrix}$$

if and only if

$$col_{\mathrm{R}}(k) \otimes col_{\mathrm{L}}(\bar{k}) = \begin{bmatrix} w \\ w \\ \vdots \\ w \end{bmatrix}$$

for some $w \in A^*$. Hence with the product $A_k \otimes A_{\bar{k}}$ the word $k\bar{k}$ composed of two keys is associated and the result of the product is denoted $A_{k\bar{k}}$. The word w in the above definition as the word which occurs between the keys k and $\bar{k}$ is denoted as $bk(k, \bar{k})$.

Definition 12. Let $k, \bar{k} \in K$ be any keys. We say that $\bar{k}$ follows k (k precedes $\bar{k}$) iff $A_k \otimes A_{\bar{k}}$ is defined. We say that a key $k \in K$ is initial if

$$col_{\mathrm{L}}(k) = \begin{bmatrix} w \\ w \\ \vdots \\ w \end{bmatrix}$$

for some $w \in A^*$. We say that a key $k \in K$ is final if

$$col_{\mathrm{R}}(k) = \begin{bmatrix} w \\ w \\ \dots \\ w \end{bmatrix}$$

for some $w \in A^*$. For an initial (final) key $k \in K$ the word w is denoted as $l(k)$ ($r(k)$) respectively.

Theorem 13. *Let $k_1, \dots, k_p \in K$ be a sequence of keys of the semiretract S such that* (1) *k_1 is a initial key*, (2) *k_p is a final key*, (3) *k_{i+1} follows k_i for $i = 1, \dots, p-1$ then the word*

$$w = l(k_1)k_1 bk(k_1, k_2)k_2 bk(k_2, k_3) \dots\dots k_p r(k_p)$$

is in the base (*code*) *C of the semiretracts S.*
Moreover, *for any word w in C there exist keys $k_1, \dots, k_p \in K$ such that the above is true.*

The statement of the theorem is obvious.

Any sequence of keys $k_1, \dots, k_p \in K$ fulfilling assumptions (1)–(3) is called *a generating key sequence.*

Corollary 14. *Finding a word from the base* (*code*) *of the semiretract is equivalent to finding a sequence of keys which fulfils the conditions from the above theorem.*

Now we define two relations λ, ρ on the set of keys K.

Definition 15. Key letters $k_1, k_2 \in K$ are in relation λ iff there exist $k \in K$ such that $A_k \otimes A_{k_1}$ and $A_k \otimes A_{k_2}$ are defined. Key letters $k_1, k_2 \in K$ are in relation ρ iff there exist $k \in K$ such that $A_{k_1} \otimes A_k$ and $A_{k_2} \otimes A_k$ are defined.

The following lemma whose proof is straightforward and so omitted is essential for our considerations.

Lemma 16. *Relations λ and ρ are equivalence on K. In $K_{/\lambda}$ there exists an equivalence class that contains exactly all initial keys. In $K_{/\rho}$ there exists an equivalence class that contains exactly all final keys.*

For any block $L_i \in K_{/\lambda}$ different than the block of final keys, there exists a block $P_j \in K_{/\rho}$ such that for any $k \in L_i$ and $\bar{k} \in P_j$ the product $A_k \otimes A_{\bar{k}}$ is defined. In other words the key $\bar{k}$ follows the key k. In this case we say that L_i is attached to P_j. Now we are ready to describe the procedure that produces generating key sequences $k_1, \ldots, k_p \in K$ for a semiretract S:
(1) choose a key k_1 from the block of initial keys of λ,
(2) find a block P_i of ρ that contains k_1,
(3) if k_1 is not a final key then find a block L_j of λ that is attached to P_i,
(4) choose a key k_2 from the block L_j,
(5) repeat steps 2–4 until the chosen key is final,
(6) write down all the obtained keys in the order that they were produced.

Theorem 17. *Any sequence of keys obtained by the above procedure is a generating key sequences for a semiretract S.*

Theorem 18. *Let S be a semiretract with key set K. Denote $L_1, \ldots, L_k$ blocks of the relation λ and $P_1, \ldots, P_k$ blocks of the relation ρ. If $\#L_i \geqslant 2$ and $\sharp P_i \geqslant 2$ for $i = 1, \ldots, k$ then for any retract R with the key set $\bar{K}$ such that $S \subset R$ it holds $\#\bar{K} \geqslant \#K$.*

Proof. Suppose that $\#\bar{K} < \#K$. There exists a key $\bar{k} \in \bar{K}$ such that in the key word $w = u\bar{k}v$ for $u, v \in A^*$ some semiretract keys $k_i, k_j \in K$ occur. Let us consider the case $w = \ldots \bar{k} \ldots k_i \ldots k_j \ldots$. The form of w implies that in any word in S in which occur letters $\bar{k}, k_i, k_j$ the order of these letters is preserved and there is no possibility to obtain other keys different from k_i, k_j after $\bar{k}$. This is a contradiction to the assumptions $\#P_i \geqslant 2$ and $S_i \geqslant 2$. Remaining cases can be proven analogically.

Theorem 19. *Let $S = \bigcap_{j=1}^{n} T_j$ denote a semiretract where T_j are retracts with the (common) key-set K. Let λ and ρ are equivalence relations introduced above. If there exists a class L_i (P_i) of the relation λ (ρ) such that $L_i = \{k\}$ ($P_i = \{k\}$) then there exist retracts R_i for $i = 1, \ldots, n$ with the (common) key-set $K \backslash \{k\}$ such that*

$$S = \bigcap_{i=1}^{n} R_i.$$

Proof. Consider the case k is not an initial key and assume the block $L_i = \{k\}$ is attached to the block P_i. We claim that $k \notin P_i$. Assuming the contrary we come to the following conclusions:

- the key k follows only k, and
- k is not the final key.

If k would be a final key and it would be possible to continue the product $\otimes$ by A_k then k should also be an initial key, a contradiction. Hence, it is possible to concatenate words defined by keys in P_i with the word defined by the key k to obtain new key words with keys as in P_i. Respectively, we modify retracts T_i with the key-set K to R_i with the key-set $K \backslash \{k\}$ without any influence on the equality $S = \bigcap_{i=1}^n R_i$. The same works if k is an initial key.

Note 1. It is worth observing that after gluing the words from blocks P_i and L_i, as described above, the number of blocks of the relations λ and ρ diminish to 1.

The above theorem allows us to construct an algorithm which generates retracts with the minimal common key sets for a semiretracts S. The algorithm is applied until every block of the relations λ and ρ has at least 2 elements (excluding initial and final blocks). The preceding theorem guarantees that the obtained retracts have minimal common key-set.

Theorem 20. *Let $S = \bigcap_{i=1}^n R_i$ be a semiretracts and K the minimal key-set for retracts R_i. S is a retract if and only if $K_{/\lambda}$ consists of exactly one block of initial keys and $K_{/\rho}$ consists of exactly one block of final keys.*

Proof. If S is a retracts the conclusion is obvious. If any key is initial and final then $C = \{l(k_i)k_i r(k_i) : k_i \in K\}$ is the base of S. Because C is a key code it follows that S is a retract.

Theorem 21. *If $\#A = 3$ then any semiretract S is a retract.*

Proof. Let K denote the minimal key set of the semiretract S. If $\#K = 3$ then $S = A^*$ and the conclusion is true. If $\#K = 2$ then relations λ and ρ define in K exactly one block of initial keys and final keys. And both these blocks are equal K because of the minimality of K. From the previous theorem it follows that S is a retract.

4. Minimal number of retracts

Definition 22. Any k factorizations of w of the form $w = u_i v_i$ for $i = 1, \dots, k$ where $u_i, v_i \in A^*$ and such that $u_i \neq u_j$ for some i, j are called a k-factorization of a word $w \in A^*$.

A k-factorization of a word $w \in A^*$ is denoted in matrix form

$$L(w) = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{bmatrix}, \quad R(w) = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix}$$

and of course

$$L(w) \otimes R(w) = \begin{bmatrix} w \\ w \\ \vdots \\ w \end{bmatrix}.$$

Definition 23. Let $F = \{(w_1, \ldots, w_n) : n \in \mathbb{N},\ w_i \in A^*\}$ denote the set of all finite word sequences. We define the function $\Phi : F \to \mathbb{N}$ putting $\Phi(w_1, \ldots, w_n) = k$ if and only if

(1) there exist a k-factorizations of the words $w_1, \ldots, w_n$ such that $L(w_i) \otimes R(w_j)$ is defined if and only if $i = j$.

(2) k is the minimal number for which there exist k-factorizations fulfilling the above property 1.

Below some properties of the introduced function Φ are listed:

(1) $\Phi(w_1, \ldots, w_n) = \Phi(w_{\delta(1)}, \ldots, w_{\delta(n)})$ where δ is any permutation.

(2) $\Phi(w_1, \ldots, w_n) \geqslant \Phi(u_1, \ldots, u_n)$ where u_i is a subword of w_i for $i = 1, \ldots, n$.

(3) $\Phi(w_1, \ldots, w_n) \geqslant \Phi(w_1, \ldots w_{i-1}, w_{i+1}, w_n)$ for any $i \in \{1, \ldots, n\}$.

(4) $\Phi(w_1, \ldots, w_n) = 2$ if words $w_1, \ldots, w_n$ are mutually different.

Let S be a semiretract with key set K and $K_{/\lambda} = \{L_0, \ldots, L_k\}$, $K_{/\rho} = \{P_1, \ldots, P_{k+1}\}$ denote sets of blocks (equivalence classes) of relations λ and ρ, respectively. Assume additionally that L_0 contains all initial keys, P_{k+1} all final keys and that the block L_i is attached to P_i for $i = 1, \ldots, k$. For P_i and L_i attached let $k_1 \in P_i$, $k_2 \in L_i$ and

$$col_{\mathrm{R}}(k_1) = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix}, \quad col_{\mathrm{L}}(k_2) = \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix}.$$

Let u_i be the shortest word and u_j the longest one in the column $col_{\mathrm{R}}(k_1)$. Then $u_j = u_i v$ and similarly $vw_j = w_i$ for some $v \in A^*$. We call the word v the source for the pair P_i and L_i (it is easy to observe, that the definition is correct—the defined source word v does not depend on the choice of the keys k_1 and k_2).

Definition 24. Let P_i and L_i be attached blocks. We say that w separates blocks P_i and L_i if w is a word of the maximal length containing the source of the pair P_i and L_i and w is a subword of $bk(k_1, k_2)$ for any keys $k_1 \in P_i$, $k_2 \in L_i$. The separating word w is defined properly. We denote respectively right(k_1) and left(k_2) the words that satisfy the following equality $bk(k_1, k_2) = \text{right}(k_1) w\, \text{left}(k_2)$.

Example 25. Let $P_i = \{k_1, k_2\}$ and $L_i = \{k_3, k_4\}$ and

$$A_{k_1} = \begin{bmatrix} s & & abb \\ s & k_1 & ab \\ 0 & & ab \end{bmatrix}, \quad A_{k_3} = \begin{bmatrix} ca & & s \\ bca & k_3 & s \\ bca & & 0 \end{bmatrix},$$

$$A_{k_2} = \begin{bmatrix} s & & cb \\ s & k_2 & c \\ 0 & & c \end{bmatrix}, \quad A_{k_4} = \begin{bmatrix} cb & & 0 \\ bcb & k_4 & s \\ bcb & & 0 \end{bmatrix}.$$

The word b is the source and we have $bk(k_1,k_3)=abbca$, $bk(k_1,k_4)=abbcb$, $bk(k_2,k_3)=cbca$, $bk(k_2,k_4)=cbcb$. The separating word is equal b_0c_1—the maximal extension of the source. right$(k_1)=ab$, left$(k_3)=a$ and right$(k_2)=c$, left$(k_4)=b$. Before formulating the main result of our paper let us come back to the semiretract from the counterexample. We have the following blocks (blocks P_i and L_i are associated):
$L_0=\{a\}$—block of initial keys
$P_1=\{a,e,g\}$, $L_1=\{b,f,h\}$
$P_2=\{b,d,f\}$, $L_2=\{c,e,g\}$
$P_3=\{c,h\}$, $L_3=\{d,i\}$
$P_4=\{i\}$—block of final keys. The separating word is just s for any pair of associated blocks. We have $\Phi(a,a,a)=3$, so

$$r_1 = \begin{bmatrix} a \\ 0 \\ 0 \end{bmatrix}, \quad l_1 = \begin{bmatrix} 0 \\ a \\ a \end{bmatrix}, \quad r_2 = \begin{bmatrix} a \\ 0 \\ a \end{bmatrix}, \quad l_2 = \begin{bmatrix} 0 \\ a \\ 0 \end{bmatrix},$$

$$r_3 = \begin{bmatrix} 0 \\ a \\ a \end{bmatrix}, \quad l_3 = \begin{bmatrix} a \\ 0 \\ 0 \end{bmatrix}$$

is a 3-factorization for words (a,a,a). It is easy to observe that there is no 2-factorization for (a,a,a). Let us define the family of retracts in the following way. If $k\in P_i$ then define $col_{\mathrm{R}}(k)=r_i$ and $col_{\mathrm{L}}(k)=l_i$. The resulting semiretract (the intersection of the defined family of retracts) is the same as in the counterexample.

Theorem 26. *For any semiretract $S=\bigcap_{i=1}^{n} P_i$* where $P_1,\ldots,P_n$ are retracts of A^* there exist

$$m = \min\{\Phi(w_1,\ldots,w_r):\ w_i \textit{ separates } L_i \textit{ and } P_i\ i=1,\ldots,r\}$$

retracts $R_1,\ldots,R_m$ of A^* *such that $S=\bigcap_{i=1}^{m} R_i$ and $m\leqslant n$. All considered retracts have the key set K. m is the minimal number of retracts satisfying the equality defining semiretract S.*

Proof. Consider a sequence $(w_1,\ldots w_r)$ such that $\Phi(w_1,\ldots w_r)=m$. Let k denote a key which is an element of the blocks P_i and L_j. Hence w_i is a separating word of P_i and L_i and w_j is a separating word of P_j and L_j. Now let us define m key words with the key k:

$$\begin{bmatrix} R_1(w_j)\mathrm{left}(k) & k & \mathrm{right}(k)L_1(w_j) \\ \vdots & \vdots & \vdots \\ R_i(w_j)\mathrm{left}(k) & k & \mathrm{right}(k)L_i(w_j) \\ \vdots & \vdots & \vdots \\ R_m(w_j)\mathrm{left}(k) & k & \mathrm{right}(k)L_m(w_j) \end{bmatrix},$$

where $R_i(w)$ ($L_i(w)$) denotes the value in the i—the line of $R(w)$ ($L(w)$) and $L(w)$ and $R(w)$ are given by m-factorization of the word w. Finally, we obtain m retracts $R_1,\dots,R_m$ of A^* with the key set K. Just from the definition of the m-factorization it follows that the sets of blocks of λ and ρ for the obtained retracts $R_1,\dots,R_m$ are the same as for $P_1,\dots,P_n$. Therefore, the order of the keys is the same. The way of selection of right(k) and left(k) ensures the equalities of the words generated by a key sequence. Conversely, the existence of m retracts implicates that there exists the sequence $(w_1,\dots w_r)$ for which $\Phi(w_1,\dots w_r)\leqslant m$. Hence the theorem is proved.

References

[1] J.A. Anderson, Semiretracts of a free monoid, Theoret. Comput. Sci. 134 (1994) 3–11.
[2] J.A. Anderson, The intersection of retracts of A^*, Theoret. Comput. Sci. 237 (2000) 439–445.
[3] J.A. Anderson, W. Forys, Regular languages and semiretracts, International Conference on Words, Kyoto, 2000.
[4] J.A. Anderson, W. Forys, T. Head, Retracts and semiretracts of free monoids, AMS Meeting, San Francisco, 1991.
[5] W. Forys, On the family of retracts of free monoids, Internat. J. Comput. Math. 33 (1990) 95–97.
[6] W. Forys, T. Head, The poset of retracts of a free monoid, Internat. J. Comput. Math. 37 (1990) 45–48.
[7] W. Forys, T. Head, Retracts of free monoids are nowhere dense with respect to finite group and p-adic topologies, Semigroup Forum, 1990, pp. 117–119.
[8] T. Head, Expanded subalphabets in the theories of languages and semigroups, Internat. J. Comput. Math. 12 (1982) 113–123.