The commutation of finite sets: a challenging problem*

Christian Choffrut
L.I.A.F.A, Université Paris VII,
Tour 55-56, 1er étage,
2 pl. Jussieu – 75 251 Paris Cedex – France
Christian.Choffrut@liafa.jussieu.fr

Juhani Karhumäki
Dept. of Mathematics and TUCS,
University of Turku – 20014 Turku – Finland
Juhani.Karhumaki@cs.utu.fi

Nicolas Ollinger
ENS de Lyon, DMI/MIM,
46, allée d'Italie – 69 364 Lyon Cedex 07 – France
Nicolas.Ollinger@ens-lyon.fr

Abstract

We prove that given a set X of two nonempty words, a set Y of nonempty words commutes with X if and only if either Y is a union of powers of X or $X, Y \subseteq t^+$ for some primitive word t. We also show that the same holds for certain special types of codes, but does not hold in general for sets of cardinality at least four.

1 Introduction

This note deals with a special case of the following general problem. Given a subset of a free semigroup describe, if possible, all subsets which commute with it. We solve the problem when the given subset has exactly two elements.

A simple sufficient condition under which two arbitrary elements of an associative algebra commute is when the two elements belong to the subalgebra generated by a third element. In favorable situations this condition is also necessary. This is precisely what happens for polynomials and series of noncommuting variables over a field with Bergman's Theorem [5], for words in free monoids with the Defect Theorem, elements in free groups and under some restrictions for matrices, [9, p. 222]. In other cases the condition is not necessary but similar conditions are, see [3].

A few words on what is already known in the literature concerning subsets of free semigroups are appropriate. When the subset is a prefix (no element is a prefix of another) the problem was settled in a very nice paper, [14]. The author left as a conjecture that the general case of codes is not substantially different and gave some evidence of it. We give an example showing that for arbitrary subsets the above condition fails to be necessary.

Let us mention a related problem which does not seem to have received an answer yet. It is straightforward to verify that given a subset of the free semigroup, there exists a unique

*The authors acknowledge the support of the Academy of Finland under grant #44087

maximal subset which commutes with it, called its *centralizer*. The question was raised by Conway in [6], whether or not the centralizer of a rational subset of a free semigroup is itself rational. To our knowledge this question is still open. Our result can be viewed as a solution of Conway's problem for two element sets.

Actually, Conway's problem was originally formulated for free monoids and not for free semigroups, and there is no reason why these two variants should be related. Indeed, we give an example of a finite set such that its centralizers with respect to the free monoid and to the free semigroup are not the same modulo the empty word, see Example 4 in Section 4.

Our contribution is mainly to prove that when a subset X of a free semigroup has two noncommuting elements then a subset commutes with X if and only if it is a union of subsets of the form X^i, for some nonnegative integer $i \in \mathbb{N}$. Thus we give an affirmative answer to a question proposed in [15]. We achieve this goal by resorting to a result from the theory of equations in words which can be thought of as an extension of the well celebrated defect theorem. Another important part of our contribution is to give a family of counterexamples in the case of subsets of four or more elements. This last result illustrates that the preceding result cannot be extended to the general case. However, we can extend it to certain special classes of codes, such as elementary codes or synchronizing ones, cf. [15] and [1].

2 Preliminaries

In this section we fix our terminology and recall tools needed in our considerations. Our results, as discussed more in Section 6, are more natural to state in the framework of free semigroups than that of free monoids. Consequently, we have chosen the terminology of free semigroups, and hence, finite set X is assumed to consist of nonempty words only, unless otherwise stated.

2.1 Free monoids and semigroups

We fix a finite *alphabet* A and denote by A^+ (resp. A^*) the free semigroup (resp. monoid) it generates. An element x of A^* is a *finite word*, its *length* is denoted by $|x|$. The word of length 0, denoted by 1, is the unit of A^*. A word x is a *prefix* (resp. *suffix*) of a word y if there exists a word z satisfying $y = xz$ (resp. $y = zx$). We also denote by A^ω (resp. ${}^\omega A$) the set of *infinite words*; i.e, left to right (resp. right to left) infinite sequences of elements in A, and by ${}^\omega A^\omega$ the set of *bi-infinite words*. For a given set of finite words X, an *X-factorization* of a word w (finite, infinite or bi-infinite) is any sequence (finite, infinite or bi-infinite) of elements of X yielding w as their product. A *periodic* word is a word that admit an X-factorization for a singleton X. Notice that for nonperiodic words it is not possible to shift a factorization over the word, whereas this might be the case for bi-infinite periodic words like $\ldots abab \cdot abab \cdot abab \ldots$. The set of all nonempty prefixes and suffixes of a set X are denoted by $\mathrm{Pref}(X)$ and $\mathrm{Suff}(X)$, respectively.

We equip the power set of A^+ (or A^*) with the subset product defined by $X \cdot Y = \{x \cdot y \mid x \in X, y \in Y\}$. A subset $X \subseteq A^*$ is a *code* if it generates unambiguously its submonoid, i.e., if for all integers n, m and all words $x_i, y_j \in X$, $i = 1, \ldots, n$, $j = 1, \ldots, m$, the condition $x_1 \ldots x_n = y_1 \ldots y_m$ implies $n = m$ and $x_i = y_i$ for all $i = 1, \ldots, n$. It is a *prefix* if $x, xy \in X$ implies $y = 1$. The cardinality of a set X is denoted by $||X||$.

2.2 Equations

We will need some results concerning the theory of equations in free monoids. Here is the minimal material necessary for our purpose. The interested reader may refer to [4] for a more complete exposition of the subject. The idea is, given a set X of words, to state conditions on relations satisfied by words so that these words may be expressed with as few parameters as possible. The relations in question are stated in terms of one way infinite words. In [10], they are stated in terms of two way infinite words.

Let Ξ be a set of *variables* in one-to-one correspondence with a subset of nonempty words $X \subseteq A^+$, say $\xi_i \leftrightarrow x_i$ for some fixed enumeration of X. An *ω-equation* over the set Ξ is a pair $L(\Xi), R(\Xi)$, more traditionally denoted as $L(\Xi) = R(\Xi)$ of infinite words in Ξ. The subset X *satisfies* the equation $L(\Xi) = R(\Xi)$, if whenever the x_i's are substituted for the ξ_i's, the two handsides, as words in A^ω, are equal.

EXAMPLE 1 *If $\Xi = \{\xi_1, \xi_2, \xi_3\}$ with $x_1 = ab, x_2 = abc, x_3 = cc$, then $x_1 x_3^\omega = x_2 x_3^\omega$ showing that X satisfies the ω-equation $\xi_1\xi_3^\omega = \xi_2\xi_3^\omega$.*

Assume $X \subseteq A^+$ satisfies a system of n ω-equations of the form

$$E: \qquad L_i(\Xi) = R_i(\Xi), i = 1, \ldots, n \tag{1}$$

Define the *dependence graph* of system E as the nondirected graph G whose vertices are the letters of Ξ and whose edges are the pairs $(\xi_k, \xi_l) \in \Xi \times \Xi$ such that ξ_k and ξ_l are the first letters of the left and right handsides of some equations of E. Then we have, see [4, Corollary 4.5]

Proposition 1 (Graph Lemma) *Let E be a system and let $X \subseteq A^+$ be a subset satisfying it. If the dependence graph of E has p connected components then there exists a subset F of cardinality p such that $X \subseteq F^*$.*

Observe that in the example above we have $X \subseteq \{ab, c\}^+$.

The main application of Proposition 1 is when $p = 1$ since in that case we may conclude that all the words in X are powers of a same word. It should be clear how we will proceed if we want to prove that the words of a set X are all powers of a same word: it will suffice to find enough equations, possibly by introducing some new words, in such a way that the corresponding graph satisfy the condition of the proposition.

This proposition was used effectively in [10] to derive a defect theorem for bi-infinite words, which, in turn, is essential for some of our results. In order to formulate it we recall the following notion: the *combinatorial rank* of a finite set $X \subseteq A^+$ is

$$\min\{||F|| \mid X \subseteq F^*\},$$

i.e. the smallest number of words needed to express all words of X as products of these words. Note that F here need not be unique but is, by defect theorem, a code.

Proposition 2 *Let $X \subseteq A^+$ be a finite set of words over a finite alphabet. Then, if a nonperiodic bi-infinite word w has two X-factorizations, then the combinatorial rank of X is at most $\|X\| - 1$.*

3 Basic Properties

We state a few elementary properties of commuting subsets that actually apply to arbitrary semigroups. Let $X \subseteq A^+$ be a subset. There exists the maximal subset $Z \subseteq A^+$ which commutes with X. Indeed, $Z_1 X = X Z_1$ and $Z_2 X = X Z_2$ imply $(Z_1 + Z_2)X = X(Z_1 + Z_2)$. Furthermore, this maximal subset is a subsemigroup, and it clearly contains the subsemigroup X^+ generated by X. We summarize these remarks as follows:

Proposition 3 *Given a subset $X \subseteq A^+$ there exists a maximal subset (for set inclusion) that commutes with X. It is a subsemigroup containing X^+.*

We define the *centralizer* of X as this maximal subset Z and we denote it by $Z(X)$. We can give some easy bounds for this set:

Proposition 4 *Given a subset $X \subseteq A^+$, the following inclusions hold:*

$$X^+ \subseteq Z(X) \subseteq \mathrm{Pref}(X^+) \cap \mathrm{Suff}(X^+).$$

Proof. The first inclusion is already mentioned above. Consider the second inclusion. Take a word z in $Z(X)$. Let x_0 be a word in X. As $Z(X) \cdot X^{|z|} = X^{|z|} \cdot Z(X)$ we can assert:

$$z \cdot x_0^{|z|} \subseteq X^{|z|} \cdot Z(X).$$

From this we conclude that $z \in \mathrm{Pref}(X^+)$. By symmetric reasons, $z \in \mathrm{Suff}(X^+)$. ■

Notice that all the notions, like a centralizer, that we defined for semigroups can be defined similarly for monoids as discussed more in Section 6. But, in addition to straightforward interpretations of our results to the monoid case we would have only trivial results, like the one showing that the largest monoid commuting with a set $X \subseteq A^*$ containing the empty word is always the whole monoid A^*. Moreover, there is no hope to obtain a characterization similar to that in Theorem 2 for sets of two words. Indeed, for $X = \{1, ab\}$ this maximal monoid is $Y = \{a, b\}^*$, and clearly X and Y are not expressible as unions of powers of a set.

For words (not subsets of words), it is well known that the commutation is equivalent to other simple properties, cf. [4] or [11].

Proposition 5 *Let $x, y \in A^*$ be two arbitrary words. The following conditions are equivalent:*

i) $xy = yx$,

ii) there exist two integers i, j such that $x^i = y^j$,

iii) there exist a word z and two integers i, j such that $x = z^i$ and $y = z^j$,

iv) x and y have a common prefix of length $|x| + |y| - gcd(|x|, |y|)$.

This ideal situation is rarely met in other structures but it is a good source of inspiration. Of course, condition iv) known as Fine and Wilf's periodicity property, see [8], does not make sense in general. For subsets of free semigroups, which is the object of this note, the commutation was studied under the hypothesis that one of the subsets is a code in [14]. Outside this framework, there is little hope of some precise statement, and certainly nothing like Bergman's Theorem holds, cf. [13]. Section 4 is an illustration of this.

For the sake of readability we introduce a logical condition $\mathcal{P}$ that expresses the property encountered in the above mentioned Bergman's Theorem.

Definition 1 *Let X be a set of nonempty words. We say that X satisfies $\mathcal{P}$, or shortly that $\mathcal{P}(X)$ is true, if and only if for every subset of nonempty words Y commuting with X, X and Y are unions of powers of a same set.*

The question whether $\mathcal{P}$ is satisfied for all finite languages was raised in [15], and will be answered negatively in Section 4. However, the problem was affirmatively answered when X is a prefix. Indeed, [14] proved the following:

Theorem 1 *Given a prefix code $X \subseteq A^*$ there exists a unique prefix code Z such that for all $Y \subseteq A^*$, $Y \cdot X = X \cdot Y$ holds if and only if there exist a subset $I \subseteq \mathbb{N}$ and a number j such that $Y = \bigcup_{i \in I} Z^i$ and $X = Z^j$. In other words, $\mathcal{P}$ is satisfied for prefix codes.*

When X is a general code the above referred paper inquires about the commutation of X with another code, not just with an arbitrary subset. Then the equivalence between conditions *i*) and *ii*) of Proposition 5 still holds.

Another case when $\mathcal{P}(X)$ holds, as essentially noted in [15], is the case when X is a subset of t^+ for some word t:

Proposition 6 *Let t be a primitive word and $X \subseteq t^+$, then $Z(X) = t^+$.*

Proof. It is clear that t^+ commutes with X, so we only need to prove that $Z(X) \subseteq t^+$. Let $z \in Z(X)$. By Proposition 4, z is a suffix of a word in t^+, i.e. $z = ut^i$ where u is a proper suffix of t and $i \geq 0$. If $u \neq 1$ then, by the relation $zX \subseteq XZ(X)$, we conclude that $ut^it^j = t^kz'$ for some $j, k \geq 1$ and $z' \in Z(X)$. By comparing the prefixes of length $|t|$ of the two handsides we obtain $ut_1 = t_1u$ where t_1 is a prefix of t of length $|t| - |u|$. Hence, t_1 and u commute and consequently are powers of the same word, see e.g. [4]. By the primitiveness of t we obtain that $u = 1$. ∎

From this result we derive the proof for the sets consisting of two nonempty commuting words.

Corollary 1 *Let $X = \{x, y\}$, with x and y two nonempty words satisfying $xy = yx$. There exists a primitive word $t \in A^+$ such that for all $Z \subseteq A^+$ we have $ZX = XZ$ if and only if $X \subseteq t^+$ and $Z = \bigcup_{i \in I} t^i$ for some $I \subseteq \mathbb{N}$. In other words, $\mathcal{P}(X)$ is true.*

Proof. Because of Proposition 5 there exists a unique minimal length word $t \in A^+$ such that $x, y \in t^+$. By the previous proposition $Z(X) = t^+$ from which we deduce our result. ∎

4 Counterexamples

We first recall an example that was known by one of the authors for quite a long time:

Example 2 *Consider $X = \{a, a^3, b, ba, ab, aba\}$. Then $Y = X \cup \{a^2\}$ commutes with X but the two subsets cannot be expressed as unions of powers of the same subset.*

As we shall see in the next section the above example cannot be sharpened for two element sets. Hence it is interesting to know what happens with larger subsets. In fact, we give here a family of examples that solves this question for subsets of sizes five or more, and then give an example of size four.

Example 3 *Given $n \geq 5$, and set $k = \lfloor \log_2(n-1) \rfloor$. Consider $X = \{a,b\}^k \cup X'$ with $X' \subseteq \{a,b\}^{2k-1}$ such that $\|X\| = n$. Then, as is straightforward to compute, $Y = X \cup \{a,b\}$ commutes with X, but the two subsets cannot be expressed as unions of powers of the same set.*

Notice that for these sets $Z(X) = \{a,b\}^+$ holds, which is again equal to $\mathrm{Pref}(X^+) \cap \mathrm{Suff}(X^+)$. The next example will show that even when this intersection is a semigroup, it is not necessary $Z(X)$.

Example 4 *Consider $X = \{a, ab, ba, bb\}$. Then, as is again straightforward to see, $Y = X \cup X^2 \cup \{bab, bbb\}$ commutes with X but the two subsets cannot be expressed as unions of powers of the same set.*

Indeed, we have $Z(X) = \{a,b\}^+ \setminus \{b\}$which is in particular different from $\mathrm{Pref}(X^+) \cap \mathrm{Suff}(X^+)$. However, $Z(X)$ is finitely generated: $Z(X) = \{a, ab, ba, bb, bab, bbb\}^+$. Notice also that the largest monoid that commutes with X is $A^* \neq Z(X) \cup \{1\}$, thus exhibiting a difference between the semigroup and the monoid cases.

5 Main results

In this section we give some examples when the Bergman type characterization holds.

5.1 Subsets commuting with two words

This section is dedicated to the proof of one of our main results solving our problems for two element sets. The following simple technical Lemma can be found in [14]. For the sake of completeness we reproduce it here.

Lemma 1 *Let $X \subseteq A^+$ be a code such that $Z(X) = X^+$ and let $Y \subseteq A^+$ commute with X. If $y \in Y \cap X^n$ for some integer $n \geq 0$, then $X^n \subseteq Y$.*

Proof. Indeed, let $x_1 x_2 \ldots x_n \in Y$ with $x_i \in X$ for $i = 1, \ldots, n$. Then for all $x \in X$ we have $x_1 x_2 \ldots x_n x \in XY \cap X^{n+1}$. Since X is a code and $Y \subseteq X^+$, this implies $x_2 \ldots x_n x \in Y$, thus by transitivity $X^n \subseteq Y$. ■

Our second lemma resembles Proposition 4.

Lemma 2 *Let $X \subseteq A^+$ and Y commutes with X. If $z \in Y$, then for all $u \in X^\omega$ (resp. $v \in {}^\omega X$), $zu \in X^\omega$ (resp. $vz \in {}^\omega X$).*

Proof. Let $z \in Y$ and $u = u_1 u_2 \ldots \in X^\omega$ with $u_i \in X$ for all i. We define recursively an infinite word $\overline{v} = v_1 v_2 \ldots \in X^\omega$ with $v_i \in X$ for all i. As $z \in Y$, there exist $z_1 \in Y$ and $v_1 \in X$ such that $zu_1 = v_1 z_1$. Recursively, assuming that $z_n \in Y$ and $v_n \in X$ are already defined we consider the identity $z_n u_{n+1} = v_{n+1} z_{n+1}$ to define $z_{n+1} \in Y$ and $v_{n+1} \in X$. It follows that $zu = \overline{v}$. By symmetric reasons we conclude the case $v \in {}^\omega X$. ■

Now, we characterize the centralizer of a set consisting of two noncommuting words.

Proposition 7 *Let $X = \{x, y\}$ be a subset consisting of two noncommuting words. Then $Z(X) = X^+$.*

Proof. Set $Z = Z(X)$. By Lemma 2, for all $z \in Z$ there exist two infinite words $u, v \in X^\omega$ such that $zx^\omega = u$ and $zy^\omega = v$. Consequently, we have two infinite equations

$$zx^\omega = x_1 \dots x_n \dots \text{ and } zy^\omega = y_1 \dots y_n \dots \tag{2}$$

with $x_i, y_i \in X$, $i \geq 0$. If the two words zx^ω and zy^ω were equal then, by Proposition 5, x and y would commute contradicting the hypothesis. Let i be the minimal integer for which $x_i \neq y_i$. Observe that if $z \in X^*$ we are done, so we assume $z \neq x_1 \dots x_{i-1}$.

If $|z| < |x_1 \dots x_{i-1}|$, then there exists a unique nonempty word t such that $x_1 \dots x_{i-1} = zt$. By cancelling out the common prefix of length $|z|$ in equation (2) we obtain

$$x^\omega = tx_i \dots x_n \dots \text{ and } y^\omega = ty_i \dots y_n \dots$$

Since t, x, y are three different nonempty words we may conclude by Proposition 1.

On the other hand, if $|x_1 \dots x_{i-1}| < |z|$ then there exists a unique nonempty word t such that $x_1 \dots x_{i-1} t = z$. By cancelling the common prefix of length $|x_1 \dots x_{i-1}|$, we obtain

$$tx^\omega = x_i \dots x_n \dots \text{ and } ty^\omega = y_i \dots y_n \dots$$

Since t, x_i, y_i are three different nonempty words we conclude as above. ∎

The previous results together with Corollary 1 solves completely the case when X consists of two nonempty words.

Theorem 2 *Let $X = \{x, y\}$ be a subset of two nonempty words. Then a subset $Y \subseteq A^+$ commutes with X if and only if there exist a subset $I \subseteq \mathbb{N}$ such that*

$$Y = \bigcup_{i \in I} X^i \quad \text{if } X \text{ is a code, and}$$
$$Y = \bigcup_{i \in I} t^i \quad \text{if } X \subseteq t^+ \text{ with } t \in A^+ \text{ and primitive.}$$

In other words, $\mathcal{P}$ is satisfied for sets of two nonempty words.

5.2 The case of codes

We prove here some extensions of the previous theorem, as well as some of [14]. We give a general result dealing with subsets commuting with codes and then apply it to several families of codes to establish the property $\mathcal{P}$ for these codes.

Proposition 8 *Let $X \subseteq A^+$ be a code, and $z \in Z(X)$ be such that $z \notin X^+$. Then for each $u \in X^\omega$ and $v \in {}^\omega X$, there exists two X-factorizations of the word vzu, namely $v \cdot zu$ and $vz \cdot u$ with $u = u_0 u_1 u_2 \dots$, $v = \dots v_{-2} v_{-1} v_0$, $zu = u'_0 u'_1 u'_2 \dots$, $vz = \dots v'_{-2} v'_{-1} v'_0$. Moreover, there exist no indices i, j, k, l such that $zu_0 \dots u_i = u'_0 \dots u'_j$ and $v_k \dots v_0 z = v'_l \dots v'_0$.*

Proof. Assuming the hypothesis, the existence of these X-factorizations comes directly from Lemma 2. The conditions for indices follows from facts that $z \notin X^+$ and X is a code. ∎

The statement of Proposition 8 is illustrated in Figure 1.

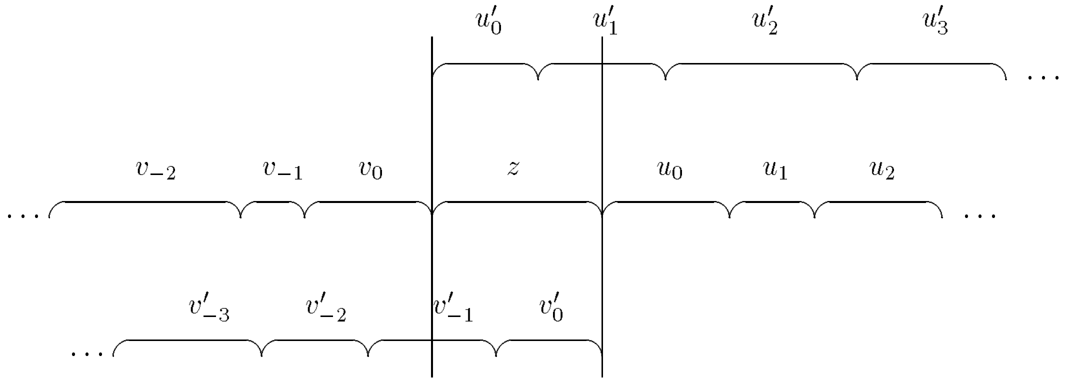

Fig. 1. The illustration of Proposition 8.

Before proving some corollaries, we recall a few definitions. An *elementary set* is a set X such that $X \subseteq F^*$ implies $\|X\| \leq \|F\|$. It can be shown, see [15], that elementary sets are codes and that, by definition, they allow no defect effect, see [4]. A *synchronizing pair*, see [1], of a subset X is a pair $p, q \in X^*$ such that for all $u, v \in A^*$, $upqv \in X^*$ implies $up, qv \in X^*$.

Theorem 3 *$\mathcal{P}$ is satisfied for elementary codes.*

Proof. From the assumption $z \in Z(X) \setminus X^+$ we can derive, using Proposition 8 and Proposition 2, a contradiction. Here we need the fact that vzu, with $v \in {}^{\omega}X$ and $u \in X^{\omega}$, can be chosen nonperiodic, which indeed is easy since X is elementary. Hence the result follows from Lemma 1. ∎

Some other simple but interesting corollaries of Proposition 8 are as follows:

Theorem 4 *$\mathcal{P}$ is satisfied for codes containing a word of length one.*

Proof. We consider $z \in Z(X) \setminus X^+$ and $a \in A \cap X$. Using Proposition 8 with $u = a^{\omega}$ and $v = {}^{\omega}a$ we obtain a contradiction. Hence no such z exists. ∎

Theorem 5 *$\mathcal{P}$ is satisfied for codes with a synchronizing pair.*

Proof. We consider $z \in Z(X) \setminus X^+$ and p, q a synchronizing pair of X. Using Proposition 8 with u and v containing pq as a factor we obtain a contradiction. Hence no such z exists. ∎

6 Conclusions and Open problems

We have found a simple characterization for sets commuting with a given finite set X in the case where X consists of two nonempty words, as well as in the case where X is a certain type of code, for example, elementary. Our proofs are rather short, but they rely essentially on an important, but not much used, lemma on combinatorics of words, namely the so-called Graph Lemma. In fact, our results are among the first nontrivial applications of this lemma.

As shown in the examples of Section 4, it seems unlikely that there exists a simple condition for two arbitrary, even finite, sets to commute. In [14] it is conjectured that a code X commutes with a set Y if and only if X and Y are unions of powers of a same set, in other words that X satisfies the condition $\mathcal{P}$. To our knowledge this is still an open question and we will not venture to make any guess. It should be possible to extend our result for three word codes, but even this seems to require some nontrivial combinatorics. Another interesting open problem is the question whether the condition $\mathcal{P}$ holds for every three element set.

Finally, there remains to find a natural and hopefully efficient way to generate the centralizer of a rational set and to prove or disprove that it is rational, or even recursive. This problem relates to the more general problem of solving equations where the unknowns are subsets of a free monoid. The linear case where only unions are allowed amounts to associating a rational expression to a finite automaton and was solved a long time ago, see [7, Chap. VII. 6]. The case where unions and intersections are allowed was settled in [2]. Observe though that in all these cases the left handside is always reduced to one unknown.

We conclude with a short discussion on why we considered our problems, like Conway's problem, over the free semigroup and not over the free monoid. In fact, there are four potential choices: commutation can be considered over the free monoid A^* or over the free semigroup A^+, and the set X can be with or without the empty word 1. In each of these cases we can consider both Conway's problem or the existence of the Bergman type of characterization of sets commuting with a given finite X. We summarize our knowledge about these problems.

First assume that the semigroup is the free semigroup A^+. Now, it is reasonable to assume that X does not contain the empty word (the other case would be very unnatural, indeed), and so we are in the considerations of this paper. We know that the Bergman type of characterization holds for two element sets, and that the Conway's problem is nontrivial. Moreover, we have an example of a nontrivial centralizer, i.e. an $X \subseteq A^+$ such that its centralizer is properly inbetween X^+ and A^+.

In the case when the semigroup is the free monoid both the cases where $1 \in X$ and $1 \notin X$ are meaningful. However, in the first case Conway's problem has a trivial answer: the centralizer of X, i.e. the largest monoid commuting with X, is the whole monoid A^*, and hence always rational. Moreover, the Bergman type of result does not hold for two element sets: the set $X = 1 + ab$ and its centralizer $Z(X) = \{a, b\}^*$ are not expressible as unions of powers of a common set.

The remaining case when the semigroup is the monoid A^* and X does not contain the empty word is similar to the case considered here. Now we have the Bergman type of characterization for sets commuting with a two element set. Also Conway's problem is nontrivial, but interestingly not the same as in the case of semigroups. Indeed, we do not have here an example of a nontrivial centralizer of a finite set, as in the case of semigroups, cf. discussion after Example 4.

References

[1] J. Berstel and D. Perrin. *Theory of Codes*. Academic Press, 1985.

[2] J. Brzozowski and E. Leiss. On equations for regular languages, finite automata and sequential networks. *Theoretical Computer Science*, 10:19–35, 1980.

[3] C. Choffrut and F. D'Alessandro. Commutativity in free inverse monoids. *Theoretical Computer Science*, 204:35–54, 1998.

[4] C. Choffrut and J. Karhumäki. Combinatorics of words. In: G. Rozenberg and A. Salomaa, editors, *Handbook of Formal Languages*, volume 1, pages 329–438. Springer Verlag, 1997.

[5] P. M. Cohn. *Free Rings and Their Relations.* Academic Press, 1985.

[6] J. H. Conway. *Regular Algebra and Finite Machines.* Chapman Hall, 1971.

[7] S. Eilenberg. *Automata, Languages and Machines*, volume A. Academic Press, 1974.

[8] N. J. Fine and H. S. Wilf. Uniqueness theorems for periodic functions. *Proc. Am. Math. Soc.*, 3(2):109–114, 1965.

[9] F. R. Gantmacher. *The Theory of Matrices*, volume one. Chelsea Publishing Company, 1959.

[10] J. Karhumäki, J. Manuch, and W. Plandowski. On defect effect of bi-infinite words. In *MFCS'98*, volume 1450, pages 674–682. Lecture Notes in Computer Science, 1998.

[11] M. Lothaire. *Combinatorics on Words*, volume 17 of *Encyclopedia of Mathematics and its Applications.* Addison-Wesley, 1983.

[12] R.C. Lyndon and M.P. Schützenberger. The equation $a^m = b^n c^p$ in a free group. *Michigan Mathematical Journal*, 9:289–298, 1962.

[13] A. Mateescu, A. Salomaa, and S. Yu. On the decomposition of finite languages. Technical Report 222, TUCS, 1988.

[14] B. Ratoandromanana. Codes et motifs. *RAIRO Inform. Théor.*, 23(4):425–444, 1989.

[15] A. Salomaa. *Jewels of Formal Languages.* Computer Science Press, 1981.