Discrete Mathematics and Theoretical Computer Science DMTCS vol. **12:4**, 2010, 59–72

Contextual partial commutations

Christian Choffrut[1] and Robert Mercaş[2†]

[1]*L.I.A.F.A., Université Paris 7, Paris, France*
[2]*GRLMC, Universitat Rovira i Virgili, Dept. de Filologies Romàniques, Tarragona, Spain*

received 15th October 2009, accepted 23rd June 2010.

We consider the monoid $\mathbf{T}$ with the presentation $\langle a, b; aab = aba\rangle$ which is "close" to trace monoids. We prove two different types of results. First, we give a combinatorial description of the lexicographically minimum and maximum representatives of their congruence classes in the free monoid $\{a, b\}^*$ and solve the classical equations, such as commutation and conjugacy in $\mathbf{T}$. Then we study the closure properties of the two subfamilies of the rational subsets of $\mathbf{T}$ whose lexicographically minimum and maximum cross-sections respectively, are rational in $\{a, b\}^*$.

Keywords: Contextual trace monoids, partial commutations

Introduction

Trace monoids are obtained from free monoids by allowing certain pairs of generators to commute, which is the reason why they are also known as free partially commutative monoids. In this work, we investigate a natural extension by imposing on these partial commutations to be controlled by the context, e.g., we may specify that the letters a and b commute when preceded by the letter c but not by the letter d and call them contextual trace monoids, abbreviated as c-trace monoids. The general problem is, we think, out of reach in the near future as this theory has a degree of difficulty higher than that of the standard trace monoids. Our purpose is to draw the attention to this challenging problem by illustrating it with an intriguing special case which shows the richness of the field.

In terms of monoid presentations, the contextual trace monoids are defined by relators consisting of pairs of words of length 3, i.e., with the above example, $cab = cba$ would be a relator. There are other natural monoids presented by sets of relators whose both handsides have the same length. Apart from the trace monoids themselves, the plactic monoids originate from the rules of the jeu de taquin on a set of finite elements – the generators – and their relators consist of pairs of words of length 3, see Chapter 5 of [9]. An investigation of the fine structure of the recognizable subsets of the plactic monoid on two letters is given in [2]. The braid monoid is also defined by relators containing partial commutations and pairs of words of length 3. We believe that contextual monoids deserve more interest than they have raised so

†This work was partially done during the author's stay at the L.I.A.F.A. Research group in Paris, and supported by the ESF Programme "Automata: from Mathematics to Applications"

far. Observe that they are not cancellative which, in particular, rules out the possibility of resorting to techniques inherited from Viennot's heaps of pieces for enumerating them, see [1].

Here, we focus on the particular case of the monoid with two generators a and b which commute only when preceded by an occurrence of a. This is equivalent to saying that the elements a and ab commute: stated that way, we can view the c-trace monoid as "half" the two generator plactic monoid since the latter is determined by the condition that both a and b commute with ab. We prove some combinatorial properties of this structure. In particular, we state a factorization result where Łukasiewicz words are involved, yielding a linear algorithm deciding the equivalence of two words; differently said, the word problem is linear for congruences generated by the relation $aab = aba$. This result is instrumental for solving equations and allows us to characterize the solutions of the elementary equations such as the commutation and conjugacy equations. It also helps us compute the number of different elements of the c-trace monoid of a given length.

The second type of contribution concentrates on the study of the family of rational subsets of c-trace monoids. We are mainly concerned with the problem of determining under which choice of representatives, the cross-section is rational. We study two choices by taking the lexicographically minimal and lexicographically maximal word in each congruence class. We characterize the rational sets of words which are cross-sections in both cases. Then we investigate the closure properties of these two families. Actually, this part is a bit disappointing since there exists only one nontrivial closure property, namely that under product for the cross-section with lexicographically maximal word. As a last example of difference between ordinary and c-traces, we show that the product of two recognizable subsets of contextual traces need not be recognizable.

1 Preliminaries

1.1 Free monoids

Given a finite set Σ called an *alphabet*, whose elements are *letters*, we denote by Σ^* the free monoid it generates. An element u of Σ^* is a *word* and its *length*, i.e., the number of occurrences of letters in u, is denoted by $|u|$. The *empty word* is denoted by 1 and has length 0. A word u is a *prefix* of a word w if there exists a word v such that $w = uv$. It is a *proper prefix* if v is nonempty which implies that the empty word is a proper prefix of each nonempty word and that the empty word has no proper prefix. Given a total ordering $<$ on Σ, it extends to a *lexicographical ordering* of Σ^*, denoted $u \leq_{\text{lex}} v$, by stipulating that u is a prefix of v or that $u = wax$ and $v = wby$ holds for some words w, x, y and some letters $a < b$.

The *Łukasiewicz* language, denoted L, plays a crucial role in the study of the monoid of c-traces. We recall that it is the unique fixed point in Σ^* of the equation $X = aXX + b$. Equivalently, a word w over the alphabet $\{a, b\}$ belongs to the Łukasiewicz language if and only if $|w|_a + 1 = |w|_b$ holds and for all its *proper* prefixes v, i.e, all prefixes, including the empty word, that are different from w itself, we have $|v|_a \geq |v|_b$. Observe that L generates a free monoid which is prefix in the sense that $u, uv \in L^*$ implies $v \in L^*$ as a simple computation shows. When dealing with properties of Łukasiewicz words, it helps bearing in mind the classical paths in the discrete plane, associated with a given word over the binary alphabet $\{a, b\}$: start from the origin and move from the current point (x, y) to the next point $(x+1, y+1)$ in case an occurrence of a is read and to the point $(x + 1, y - 1)$ in case an occurrence of b is read. Then a Łukasiewicz word is a word associated to a path which lies entirely in the positive quadrant except for the last point which is below the x-axis. In particular, a nonempty word belongs to the monoid L^* if the

y-coordinate of the last point of the associated path is negative and is the unique minimum value. The prefixity of the submonoid L^* can also be interpreted in terms of paths.

1.2 Monoid presentation

A *monoid presentation* is a pair $\langle \Sigma; R\rangle$ where Σ is the set of *generators* and $R \subset \Sigma^* \times \Sigma^*$ is a set of *relators*. An element of R is indifferently written as (u, v) or $u = v$, which is the traditional notation. Denote by $\sim_R$ the congruence generated by R, by M_R the monoid presented, i.e., the quotient of Σ^* by $\sim_R$ and by $\phi_R : \Sigma^* \to M_R$ the *canonical morphism* which assigns to every word $w \in \Sigma^*$ its class in the congruence $\sim_R$. We drop the index and simply write $\sim$, M and ϕ when R is understood. The identity element of the monoid is denoted by 1. For example, a *trace monoid* has a presentation of the form $\langle \Sigma; \{(ab, ba) \mid (a, b) \in I\}\rangle$, where $I \subseteq \Sigma \times \Sigma$ is a symmetric and irreflexive relation, [10, 5, 8, Chapter 11].

Our notion of *contextual trace monoid* or simply *c-trace monoid* is defined as the quotient of Σ^* by a congruence generated by relators of the form $cab = cba$ for some not necessarily different letters a, b, c of Σ. Its elements are *contextual traces*. One of the simplest contextual monoids which is essentially different from a trace monoid has the monoid presentation $\langle a, b; aab = aba\rangle$. We shall not consider other c-trace monoids and denote by $\mathbf{T}$ this particular monoid throughout the paper. Therefore the congruence $\sim$ is generated by the single relator $aab = aba$. Finally, since the two hand sides of the relator have the same length, two $\sim$-equivalent words have the same length. We may thus speak without ambiguity of the length of an element of $\mathbf{T}$ as the common length of all its representatives.

1.3 Subfamilies of subsets of a monoid

We now briefly recall the classical definitions of the two major subfamilies of subsets of an arbitrary monoid M.

The family $\mathbf{Rat}(M)$ of *rational* sets is the smallest collection of subsets containing the singletons, the empty set and closed under the set union, the concatenation and the star. The family $\mathbf{Rec}(M)$ of *recognizable* sets is the collection of subsets $X \subseteq M$ for which there exists a morphism h from M onto a finite monoid such that $X = h^{-1}h(X)$.

Equivalent definitions for rational and recognizable subsets are as follows. Consider a presentation $\langle \Sigma; R\rangle$ and identify each element of M with the corresponding $\sim$-equivalence class. Then a subset $X \subseteq M$ is rational if it is possible to choose for each equivalence class of X some words (at least one, but not necessarily exactly one) such that the set of all these words form a rational subset of Σ^*. Formally, there exists $Y \in \mathbf{Rat}\,\Sigma^*$ such that $X = \phi(Y)$. It is recognizable if the set of all words in all classes of X form a rational subset of Σ^*. Formally, $\phi^{-1}(X) \in \mathbf{Rat}\,\Sigma^*$. For example with $\langle a, b; ab = ba\rangle$ the subset $(ab)^*$ is not recognizable since the set of words equivalent to some element in $(ab)^*$ is the set of words having as many a's as b's.

We recall that if the monoid is finitely generated, which is the case of c-trace monoids, we have $\mathbf{Rec}(M) \subseteq \mathbf{Rat}(M)$, cf., [11, Theorem 2, p.1348] also [3, Proposition III.2.4].

2 Combinatorics

Here, we introduce the minimum necessary for the rest of the paper. We prove the existence of a unique factorization of a contextual trace as a product of images, in the canonical morphism ϕ, of words related to the Łukasiewicz words and characterize the lexicographically minimum and maximum representatives of a congruence class. This allows us to give a closed formula expressing the number of elements of $\mathbf{T}$ of a given length.

2.1 Lexicographical representatives

The set of Łukasiewicz words is prefix ($u, uv \in L$ implies $v = 1$) and complete in the sense that each word either is a prefix of some word in L or has a prefix in L. Therefore, each word w can be factored uniquely as

$$w = w_1 w_2 \cdots w_r w_{r+1}, \tag{1}$$

where $w_1, w_2, \cdots, w_r$ are Łukasiewicz words and w_{r+1} is a proper prefix of a Łukasiewicz word. The following lemmas show that an equivalence class of the $\sim$-congruence is uniquely determined by its commutative image (i.e., the number of occurrences of each letter a and b) along with the sequence of lengths of the Łukasiewicz factors. The first lemma is trivial since an occurrence of aab or aba cannot overlap two consecutive Łukasiewicz factors.

Lemma 1 *Let $w = w_1 w_2 \cdots w_r w_{r+1}$ and $u = u_1 u_2 \cdots u_s u_{s+1}$ be the factorizations of w and u as in (1). Then $w \sim u$ holds if and only if $r = s$ and for $i = 1, \ldots, r+1$ we have $w_i \sim u_i$.*

It thus remains to consider the conditions under which two prefixes of Łukasiewicz words are equivalent.

Lemma 2 *Let w be a prefix of a Łukasiewicz word and $w' \sim w$. Then w' is also a prefix of a Łukasiewicz word. Furthermore, if w is a Łukasiewicz word so is w'.*

Proof: The statement is true if w' is obtained from w by the substitution of an occurrence of aab for an occurrence of aba or vice versa. It follows by transitivity of the congruence relation. □

Lemma 3 *For each Łukasiewicz word w, we have*

$$a^n b^{n+1} \sim w \sim (ab)^n b,$$

where $n = |w|_a = |w|_b - 1$. Moreover, $a^n b^{n+1}$ is the lexicographically minimum word equivalent to w and $(ab)^n b$ is the maximum.

Proof: By repeated application of $aab \sim aba$, we get $a^n b \sim aba^{n-1}$ if $n > 0$. Consequently, if $n \geq p$ we obtain

$$a^n b^p \sim aba^{n-1} b^{p-1} \sim (ab)^2 a^{n-2} b^{p-2} \sim \cdots \sim (ab)^p a^{n-p}. \tag{2}$$

Concerning the lexicographically minimum word equivalent to w, assume it has an occurrence of the form ba. Then the word starts with a prefix of the form $a^n b^p a$ with $n \geq p$. Applying equation (2) we get

$$a^n b^p a \sim (ab)^p a^{n-p+1} = (ab)^p a^{n+1-p} \sim a^{n+1} b^p,$$

which yields a smaller lexicographically word equivalent to w. Consider now the maximum word equivalent to w and assume by contradiction that it does not have the above form, i.e., it has an occurrence of the form $a^k b$ where $k \geq 2$. Because of $a^k b \sim a^{k-2} aba$ we get a lexicographically greater word, a contradiction. □

As a consequence of the previous two lemmas we get a characterization of the lexicographically minimum and maximum representatives of an equivalence class.

Corollary 4 *With the word in (1), set* $n_i = |w_i|_a$ *for* $i = 1, \cdots, r$ *and* $|w_{r+1}|_a = n_{r+1} \geq p_{r+1} = |w_{r+1}|_b$. *The minimum and maximum words equivalent to the word (1) are respectively*

$$\begin{array}{l} a^{n_1} b^{n_1+1} \cdots a^{n_r} b^{n_r+1} a^{n_{r+1}} b^{p_{r+1}} \\ \textit{and} \\ (ab)^{n_1} b \cdots (ab)^{n_r} b (ab)^{p_{r+1}} a^{n_{r+1}-p_{r+1}}. \end{array} \tag{3}$$

Corollary 5 *Given two words* $u, v \in \{a, b\}^*$ *there exists a linear algorithm that decides whether or not* $u \sim v$ *holds.*

Proof: Indeed, factorize each word u, v as above and test that the sequence of the lengths of the factors which are Łukasiewicz words are equal. Then it suffices to verify that the last factors as in (1), which are proper prefixes of a Łukasiewicz word, have the same number of occurrences of a's and b's. These tests can be executed in real time using a stack. □

2.2 Enumeration and Möbius function

We recall that the *Möbius function* μ of $\mathbf{T}$ is the function of $\mathbf{T}$ into $\mathbb{Z}$ such that $\sum_{x \in M} \mu(x)x$ is the inverse of the characteristic series $\sum_{x \in M} x$ in the algebra $\mathbb{Q}\langle\langle \mathbf{T} \rangle\rangle$. As for trace monoids, the inverse of the characteristic series of $\mathbf{T}$ is a polynomial.

Proposition 6 *The Möbius function of* $\mathbf{T}$ *is the polynomial* $1 - \phi(a) - \phi(b) + \phi(a^2b)$

Proof: Because of Corollary 4, we get that the set of lexicographically maximal representatives is equal to $((ab)^*b)^*(ab)^*a^*$. Now, the inverse of the series

$$(\phi(b) + \phi(ab))^* \phi(a)^* \in \mathbb{Q}\langle\langle M \rangle\rangle$$

is the series

$$(1 - \phi(a))(1 - \phi(b) - \phi(ab)) = 1 - \phi(a) - \phi(b) + \phi(a^2b).$$

□

Denote by T_n the number of elements of length n of the monoid $\mathbf{T}$. This number could be computed by induction on the length via expression (3) but we will obtain it by using the previous proposition.

Lemma 7 $T_n = -1 + \frac{(5-\sqrt{5})(\frac{1-\sqrt{5}}{2})^n + (5+\sqrt{5})(\frac{1+\sqrt{5}}{2})^n}{10}$.

Proof: Consider the commutative image of the characteristic series of $\mathbf{T}$ by mapping $\phi(a)$ and $\phi(b)$ onto the variable x. Then we obtain

$$\Big(\sum_{n \geq 0} T_n x^n\Big)(1 - 2x + x^3) = 1.$$

We compute the first three coefficients directly: $T_0 = 1, T_1 = 2, T_2 = 4$ and more generally $T_n = 2T_{n-1} - T_{n-3}$ for $n \geq 3$. This is equivalent to the conditions $T_0 = 1, T_1 = 2$ and $T_n = 1 + T_{n-1} + T_{n-2}$ for $n \geq 2$. This sequence is similar to the Fibonacci sequence. The result follows from [7]. □

It is worthwhile noticing that each of the integers T_n has as a Fibonacci bit-representation a prefix of $(10)^*$ (no two consecutive 0's or 1's). E.g., we have $T_5 = 12 = 8 + 3 + 1 = 8 \cdot \underline{1} + 5 \cdot \underline{0} + 3 \cdot \underline{1} + 2 \cdot \underline{0} + 1 \cdot \underline{1}$.

3 Equations

In this section we solve the equations which are classical in the free monoids: the simple equation $xy = zt$ known as Levi's Lemma for free monoids and the conjugacy and commutation equations. We are able to solve them by resorting to a natural factorization of the elements of the monoid $\mathbf{T}$.

Given a word $w \in \Sigma^*$ we denote by $\mathrm{exc}(w) = |w|_a - |w|_b$ the *excess* of the number of occurrences of a's over the number of occurrences of b's (or simply its excess). If w is a representative of the c-trace $x \in \mathbf{T}$, then its length and its excess are invariants of its congruence class, so we may use the notations $|x|$ and $\mathrm{exc}(x)$.

Expression (1) shows that all words can be uniquely factored as a product of a word belonging to the free monoid L^* concatenated with a proper prefix of a word on L. We denote by $\mathbf{L}$ the image of $L \subseteq \Sigma^*$ in the monoid $\mathbf{T}$. Let N be the set $\mathbf{L}^*$ and let P be the set of images in the canonical morphism of all proper prefixes of L. Consequently, every element of $\mathbf{T}$ can be uniquely written in the form np with $n \in N$ and $p \in P$ which we call the *np-factorization.* (Considering the path associated with a word as in paragraph 1.1 the symbol P is meant to suggest that the path lies entirely in the quadrant of the plane with positive coordinates). Since equations involve products of elements, it is natural to determine the factorization n_3p_3 of a product of two elements, knowing the factorizations n_1p_1 and n_2p_2 of these two elements. If $\mathrm{exc}(p_1) < -\mathrm{exc}(n_2)$ then the product has the decomposition

$$n_3 = n_1p_1n_2 \quad \text{and} \quad p_3 = p_2. \tag{4}$$

More precisely, there exists a unique factorization $n_2 = n_2'n_2''$ with $n_2', n_2'' \in \mathbf{L}^*$ such that $[p_1n_2'] \in \mathbf{L}$, where $[p_1n_2']$ expresses the fact that the product of p_1 and n_2' is an element of $\mathbf{L}$. If to the contrary, $\mathrm{exc}(p_1) \geq -\mathrm{exc}(n_2)$ then we have

$$n_3 = n_1 \quad \text{and} \quad p_3 = p_1n_2p_2. \tag{5}$$

The next paragraphs rely on these observations which are assumed in the proofs without explicit reference to them.

3.1 Conjugacy equation

The classical notion of conjugacy of two elements of a group can be extended to monoids in two different ways yielding a priori two different notions, which we call transposition and conjugacy. Two elements x, y are *transposed* if there exist two elements $u, v \in \mathbf{T}$ such that $x = uv$ and $y = vu$. We denote by T this relation. Two elements x, y are *conjugate* if there exists an element $z \in \mathbf{T}$ such that $xz = zy$. We denote by C this relation. The following observation is crucial: the submonoid $\mathbf{L}^*$ is free and prefix in the sense that

$$x, xy \in \mathbf{L}^* \Rightarrow y \in \mathbf{L}^*. \tag{6}$$

Indeed, let u, v and w be inverse images of x, y and xy in Σ^*. By Lemma 2, for some $u' \in \Sigma^*$ we have $w \sim u'v$, $u \sim u'$ and $u' \in L^*$. Then $w \in L^*$ implies $u'v \in L^*$ and finally $v \in L^*$, i.e., $y \in \mathbf{L}^*$. Therefore the notation $x^{-1}y$ is unambiguous if x and y belong to L^*.

Theorem 8 *In the monoid* $\mathbf{T}$ *we have* $C = T^2$*, i.e.,* x *and* y *are conjugate if and only if there exists* $z \in \mathbf{T}$*, such that both* x *and* y *are transposed to* z*.*

Proof: We consider the equation $xz = zy$ and the three decompositions $x = n_1p_1$, $z = n_2p_2$ and $y = n_3p_3$. Using the decompositions (4) and (5) there are four different cases according to whether or not $\mathrm{exc}(p_1) < -\mathrm{exc}(n_2)$ holds and whether or not $\mathrm{exc}(p_2) < -\mathrm{exc}(n_3)$ holds.

Case 1: $\mathrm{exc}(p_1) < -\mathrm{exc}(n_2)$ and $\mathrm{exc}(p_2) < -\mathrm{exc}(n_3)$. This implies

$$n_1p_1n_2 = n_2p_2n_3 \quad \text{and} \quad p_2 = p_3.$$

Decompose

$$n_2 = n_2'n_2'', \quad n_3 = n_3'n_3'', \quad n_2', n_2'', n_3', n_3'' \in \mathbf{L}^* \tag{7}$$

so that

$$n_1[p_1n_2']n_2'' = n_2[p_2n_3']n_3'' \tag{8}$$

holds where the elements in brackets belong to $\mathbf{L}$ and $n_2' \in \mathbf{L}^*$ (resp. $n_3' \in \mathbf{L}^*$) is the unique prefix of n_2 (resp. n_3) such that $p_1n_2' \in \mathbf{L}$ (resp. $p_2n_3' \in \mathbf{L}$).

Apply (6) to equation (8). Via simple considerations of lengths, n_2' is a prefix of n_1. Cancel out the prefix n_2' from the two hand sides of the above equation and observe that because of the above remark, we have $n_2'^{-1}n_1 \in \mathbf{L}^*$. Then it holds

$$(n_2')^{-1}n_1[p_1n_2']n_2'' = n_2''[p_2n_3']n_3''.$$

Since all the above factors are in the free monoid generated by the prefix code $\mathbf{L}$, we apply the result to the conjugacy equation in free monoids and there exist $u, v \in \mathbf{L}^*$ such that

$$(n_2')^{-1}n_1[p_1n_2'] = uv, \;\; [p_2n_3']n_3'' = vu.$$

Since $p_1n_2', p_2n_3' \in \mathbf{L}$ this implies that they are the last and the first factor in $\mathbf{L}$ of the element v.

If $v \in \mathbf{L}$ then we obtain

$$(n_2')^{-1}n_1 = n_3'' = u, \quad p_1n_2' = p_2n_3' = v$$

and we obtain

$$\begin{aligned} x &= n_2'(n_2')^{-1}n_1p_1 = n_2'up_1, \\ y &= n_3'n_3''p_2 = n_3'up_2 \end{aligned}$$

which shows that $(x, y) \in T^2$.

Otherwise, v is a product of at least two elements in $\mathbf{L}$ which implies $v = v_1v'v_2$ where $v_2 = [p_1n_2']$ and $v_1 = [p_2n_3']$ i.e., $(n_2')^{-1}n_1 = uv_1v'$ and $n_3'' = v'v_2u$. We obtain

$$\begin{aligned} x &= n_2'(n_2')^{-1}n_1p_1 = n_2'uv_1v'p_1 = n_2'up_2n_3'v'p_1, \\ y &= n_3'n_3''p_2 = n_3'v'v_2up_2 = n_3'v'p_1n_2'up_2, \end{aligned}$$

and hence, $(x, y) \in T$.

Case 2: $\mathrm{exc}(p_1) < -\mathrm{exc}(n_2)$ and $\mathrm{exc}(p_2) \geq -\mathrm{exc}(n_3)$. This implies

$$n_1p_1n_2 = n_2 \quad \text{and} \quad p_2 = p_2n_3p_3,$$

i.e., $x = y = 1$.

Case 3: $\text{exc}(p_1) \geq -\text{exc}(n_2)$ and $\text{exc}(p_2) < -\text{exc}(n_3)$. This implies

$$n_1 = n_2 p_2 n_3 \quad \text{and} \quad p_3 = p_1 n_2 p_2,$$

i.e., $x = n_1 p_1 = n_2 p_2 n_3 p_1$ and $y = n_3 p_3 = n_3 p_1 n_2 p_2$ which shows that $(x, y) \in T$.

Case 4: $\text{exc}(p_1) \geq -\text{exc}(n_2)$ and $\text{exc}(p_2) \geq -\text{exc}(n_3)$. This implies

$$n_1 = n_2 \quad \text{and } p_1 n_2 p_2 = p_2 n_3 p_3.$$

This yields $p_1 n_1 \in P$ and therefore $p_3 n_3 \in P$. Since furthermore $p_1 n_1$ and $p_3 n_3$ have the same length and the same excess, we have $p_1 n_1 = p_3 n_3$, proving that $(x, y) \in T^2$.

The remaining inclusion follows, since $T \subseteq C = C^2$. □

The previous result deserves a few observations. The following is an immediate consequence.

Corollary 9 *The conjugacy relation is symmetric and therefore, it is an equivalence relation.*

Next we show that indeed, the two relations T and C are different, i.e., $C = T^2$ holds but $C \neq T$.

Proposition 10 $C = T^2$ *holds but* $C \neq T$.

Proof: In order to simplify the notations, we identify the letters with their images in the canonical morphism. With $x = abbabbab, z = abbabba, y = abbbabba$ we obtain $xz = zy$. Set $x_1 = abb$, $x_2 = abbab$, $y_1 = abbb$ and $y_2 = abba$. Then it holds $x = x_1 x_2$ and $y = y_1 y_2$. Furthermore we have $(abbab)(abb) = (abba)(abbb)$, i.e., $x_2 x_1 = y_2 y_1$.

We now verify that the elements are not transposed. Indeed, since the element $abbabbab$ has a unique representative, all its transposed are obtained by splitting the word $x = uv$ (as a word) and by considering the element of $\mathbf{T}$ represented by vu. The only possible way of obtaining y is by considering the decompositions of x where v begins with the letter a, which leaves only $(abb)(abbab)$ and $(abbabb)(ab)$. Then we get $(abbab)(abb) = abb.aabbb$ and $(ab)(abbabb) = aabbb.abb$. □

Proposition 11 *Let x be a c-trace with exc$(x) = -k$ where $k > 0$. Then it is conjugate to a c-trace $y \in \mathbf{L}^k$.*

All c-traces of fixed length and fixed positive excess define a unique conjugacy class.

Proof: Let w represent x and decompose it in $w = w_1 w_2$ where w_1 is the shortest prefix with $\text{exc}(w_1) = -k$. Then $w_2 w_1 \in L^k$ and its congruence class y is in $\mathbf{L}^k$. If $\text{exc}(w) \geq 0$ then the word $w_2 w_1$ belongs to P, and we know that all words in P of a fixed length and fixed excess are equivalent in the canonical congruence. □

Proposition 12 *Given two c-traces x and y it can be tested in linear time whether they are conjugate.*

Proof: By the previous proposition, we proceed as follows. We are given two c-traces x and y of the same length and excess k. If $k \geq 0$ we verify the equality of the two c-traces and we are done. Otherwise we construct two c-traces $x', y' \in \mathbf{L}^{-k}$ which are respectively conjugate to x and y. Consider the minimum representatives u and v of x' and y'. Then u and v are conjugate if and only if so are x and y. But conjugacy can be tested in linear time in free monoids [4]. □

3.2 Factorization

Here we consider the problem of determining the relationship between two different factorizations of a given element, which is known as Levi's Lemma in the case of free monoids.

Theorem 13 *Four elements $x, y, s, t \in \mathbf{T}$ satisfy the condition $xy = st$ if and only if one of the following two conditions hold*

(i) there exists an element $w \in \mathbf{T}$ such that

$$\begin{array}{cc} x = sw, & t = wy \\ & \textit{or} \\ s = xw, & y = wt. \end{array}$$

(ii) there exist five elements $u, v_1, v_2, w_1, w_2 \in \mathbf{T}$ such that $v_1 w_1 = v_2 w_2 \in P$

$$\begin{array}{ll} x = uv_1, & y = w_1 \\ s = uv_2, & t = w_2. \end{array}$$

Proof:

Because of the symmetry between left and right hand sides there are three cases to consider. We set $x = n_1 p_1$, $y = n_2 p_2$, $s = n_3 p_3$ and $t = n_4 p_4$.

Case 1. $\mathrm{exc}(p_1) \leq -\mathrm{exc}(n_2)$ and $\mathrm{exc}(p_3) \leq -\mathrm{exc}(n_4)$. This implies

$$n_1[p_1 n_2']n_2'' = n_3[p_3 n_4']n_4'', \quad p_2 = p_4$$

for some $n_2 = n_2' n_2''$, $n_4 = n_4' n_4''$ and $p_1 n_2', p_3 n_4' \in \mathbf{L}$. If $n_1 = n_3$ then we have $n_2'' = n_4''$ which yields a solution of the second form. Otherwise, assume without loss of generality that n_1 is a proper prefix of n_3. Because all elements are in the free submonoid $\mathbf{L}^*$, for some $m \in \mathbf{L}^*$ we have $n_1 p_1 n_2' m = n_3$ and $n_2'' = m[p_3 n_4']n_4''$ and therefore

$$\begin{array}{ll} x = n_1 p_1, & y = n_2' m p_3 n_4 p_2 \\ s = n_1 p_1 n_2' m p_3, & t = n_4 p_4 \end{array}$$

which is of the first kind.

Case 2. $\mathrm{exc}(p_1) \leq -\mathrm{exc}(n_2)$ and $\mathrm{exc}(p_3) > -\mathrm{exc}(n_4)$. This implies

$$n_1[p_1 n_2']n_2'' = n_3, p_2 = p_3 n_4 p_4.$$

This yields

$$\begin{array}{ll} x = n_1 p_1, & y = n_2 p_3 n_4 p_4 \\ s = n_1 p_1 n_2 p_3, & t = n_4 p_4 \end{array}$$

which is of the first kind.

Case 3. $\mathrm{exc}(p_1) > -\mathrm{exc}(n_2)$ and $\mathrm{exc}(p_3) > -\mathrm{exc}(n_4)$. This implies that $p_1 n_2$ and $p_3 n_4$ are prefixes of L and thus so are $p_1 n_2 p_2$ and $p_3 n_4 p_4$. Furthermore, because of the unique np-factorization $p_1 n_2 p_2 = p_3 n_4 p_4$ holds. We obtain a solution of the second kind. $\square$

3.3 Commutation

The equation $xy = yx$ is solved in this section.

Theorem 14 *Two elements x and y commute if and only if one of the following two conditions holds*

(i) there exists an element $z \in \mathbf{T}$ and two integers i and j such that $x = z^i$ and $y = z^j$.

(ii) there exists $n \in N$, $p_1, p_2 \in P$ where $-exc(n) \leq exc(p_1), exc(p_2)$ such that $x = np_1$ and $y = np_2$.

Proof: Because of the symmetry of the two hand sides there are three cases. We set $x = n_1p_1$ and $y = n_2p_2$ as previously.

Case 1: $\mathrm{exc}(p_1) < -\mathrm{exc}(n_2)$ and $\mathrm{exc}(p_2) < -\mathrm{exc}(n_1)$. This implies

$$n_1p_1n_2 = n_2p_2n_1 \quad \text{and} \quad p_1 = p_2.$$

Because of the hypotheses we may write $n_1 = n_1'n_1''$, $n_2 = n_2'n_2''$ with $n_1', n_1'', n_2', n_2'' \in \mathbf{L}^*$, $p_1n_2 = [p_1n_2']n_2''$ and $p_2n_1 = [p_1n_1']n_1''$ with $[p_1n_2'], [p_1n_1'] \in \mathbf{L}$.

If $n_1 = n_2$ then we get a solution of the first kind. Otherwise, without loss of generality we assume n_1 is a proper prefix of n_2. In the equation

$$n_1[p_1n_2']n_2'' = n_2[p_2n_1']n_1'' \tag{9}$$

all elements belong to the free submonoid $\mathbf{L}^*$. Now, since $p_1 = p_2$ and since $[p_1n_2'], [p_1n_1'] \in \mathbf{L}$, both n_1' and n_2' consist of the same number of elements of $\mathbf{L}$. Because of equation (9) they are both prefixes of the same element in $\mathbf{L}^*$ and thus they are equal, implying $[p_1n_1'] = [p_2n_2']$. We set $p = p_1 = p_2$ and $n' = n_1' = n_2'$. After cancellation of the common prefix n', equation (9) becomes

$$n_1''[pn']n_2'' = n_2''[pn']n_1''.$$

All the above elements belong to the free submonoid $\mathbf{L}^*$ and we know that the general solution of this equation is of the following form where i, j, k are positive integers and u, v are arbitrary elements

$$n_1'' = (uv)^iu, [pn'] = (vu)^kv, n_2'' = (uv)^ju.$$

The c-trace $[pn']$ belongs to $\mathbf{L}$, thus $j = 0$. This yields

$$x = n_1'(uv)^iup = n'(upn')^iup = (n'up)^{i+1},$$
$$y = n_1'(uv)^jup = n'(upn')^jup = (n'up)^{j+1}.$$

Denoting $z = (n'up)$, we get that $x = z^{i+1}$ and $y = z^{j+1}$, which is a solution of the first kind.

Case 2: $\mathrm{exc}(p_1) \geq -\mathrm{exc}(n_2)$ and $\mathrm{exc}(p_2) < -\mathrm{exc}(n_1)$ which yields $n_1 = n_2p_2n_1$ and $p_1 = p_1n_2p_2$. This implies $x = y = 1$.

Case 3: $\mathrm{exc}(p_1) \geq -\mathrm{exc}(n_2)$ and $\mathrm{exc}(p_2) \geq -\mathrm{exc}(n_1)$. This implies

$$n_1 = n_2 \quad \text{and } p_1n_2p_2 = p_2n_1p_1.$$

This solution is clearly of the second type. □

4 Rational subsets with rational cross-sections

We assume the reader has some familiarity with the theory of binary rational relations on Σ^*, which are exactly the subsets of the product monoid $\Sigma^* \times \Sigma^*$ recognized by two-tape automata. We shall only use the fact that given such a relation R and a rational subset X of Σ^*, the set

$$\{v \in \Sigma^* \mid (u, v) \in R \text{ for some } u \in X\}$$

is rational, see [6, Theorem IX. 3.1].

In this section we consider the problem of determining under which condition the set of representatives, also known as a *cross-section*, of a rational subset of the c-trace monoid is a rational subset of Σ^*. We investigate both the lexicographically minimal and maximal representatives. We recall that for ordinary trace monoids, there are traditionally two main sets of representatives: the lexicographical and the Foata normal forms. In both cases the set of representatives is rational. However, for arbitrary rational subsets (i.e., different from the monoid itself), this is no longer true (when a and b commute, the set of lexicographical normal forms of $(ab)^*$ is $\{a^n b^n \mid n \geq 0\}$ with the ordering $a < b$ and the set of Foata normal forms of $(aab)^*$ is $\{(ab)^n a^n \mid n \geq 0\}$).

Here we consider the sets of lexicographically minimal and maximal representatives. We set for all integers $k \geq 0$, $H_k = \{a^i b^{i+1} \mid 0 \leq i \leq k\}$ and $H = \bigcup_{k \geq 0} H_k$. We let K be the set of proper prefixes of H, i.e., prefixes of H which are not in H. We introduce two new subfamilies of rational subsets of $\mathbf{T}$.

Definition 15 *The family $\mathcal{F}_{min}$ (resp. $\mathcal{F}_{max}$) is the family of rational subsets of $\mathbf{T}$ whose minimal (resp. maximal) representatives form a rational set of Σ^*.*

Then the set of minimal representatives of the monoid $\mathbf{T}$ is H^*K which is clearly not rational, since its intersection with the rational set a^+b^+a is the set $\{a^i b^j a \mid 0 \leq i < j\}$. The set of all maximal representatives is the rational set $(ab, b)^* a^*$. This shows that $\mathbf{T}$ does not belong to $\mathcal{F}_{\text{min}}$ but it belongs to $\mathcal{F}_{\text{max}}$. We tackle the general problem of an arbitrary rational subset of $\mathbf{T}$.

We start with a simple observation. Let M be a finitely generated submonoid of a free monoid Σ^* and let $X \in \mathbf{Rat}(\Sigma^*)$ be a subset of M. The following more or less trivial lemma shows that X is actually in $\mathbf{Rat}(M)$. Consequently, there is no distinction between the expression "a rational subset of the submonoid M of Σ^*" and "a rational subset of Σ^* that is contained in M".

Lemma 16 *Let M be a finitely generated submonoid of Σ^* and let $X \in \mathbf{Rat}(\Sigma^*)$ be a subset that is contained in M. Then X is in $\mathbf{Rat}(M)$.*

Proof: Denote by G a set of generators of M. Let Q be the set of states of a deterministic automaton recognizing X, q_0 its initial state and F its set of final states and denote by $q \cdot a$ the transition defined from the state q when reading the letter a. Consider the following two-tape automaton: the set of states is the direct product of Q with the set P of all proper prefixes of G, the initial state is the pair $[q_0, 1]$, the set of final states is the set $F \times \{1\}$ and the set of transitions is the set of quadruples $([q, u], a, 1, [q \cdot a, ua])$ if ua is a proper prefix of some word in G, and $([q, u], a, ua, [q \cdot a, 1])$ if $ua \in G$. This automaton recognizes all pairs (x, x) where $x \in X$. By erasing all first components of the labels of the automaton we get an automaton whose labels are in $G \cup \{1\}$ completing the proof. □

The following result concerning the bounded rational subsets is folklore. It will be used later.

Lemma 17 *Let Σ and Δ be two disjoint alphabets. Then every rational subset of $(\Sigma \cup \Delta)^*$ that is contained in $\Sigma^* \Delta^*$ is a finite union of products of the form XY where $X \in \mathbf{Rat}(\Sigma)^*$ and $Y \in \mathbf{Rat}(\Delta)^*$.*

4.1 Lexicographically minimal cross-sections

The following characterizes the lexicographically minimal cross-sections in Σ^* which are rational.

Proposition 18 *A subset $X \subseteq H^*K$ is rational in $\{a,b\}^*$ if and only if there exists an integer k such that X is a finite union of subsets of the form AB where A is a rational subset of the monoid generated by H_k and $B \subseteq a^*b^*$ is in $\mathbf{Rat}\{a,b\}^*$.*

Proof: It is clear that the condition is sufficient. Let us prove that it is necessary and observe that if X is rational then so are $X \cap a^*b^* = X \setminus \Sigma^* ba \Sigma^*$ and $X \setminus a^*b^*$. Thus we assume that $X \cap a^*b^* = \emptyset$. Consider the following three rational functions and relators which extract specific factors of a word in $\{a,b\}^*$. When applied to a word in H^*K defined by its decomposition as in (3), these factors are respectively the longest prefix in HH_0^*, an arbitrary maximum factor in HH_0^* and the prefix of the word when the maximal final factor in a^*b^* is deleted.

$$\begin{array}{lcl} h(ubav) & = & \{ub \mid u \in a^*b^+\}, \\ g(w) & = & \{avb \mid w = ubavbaz \text{ and } v \in a^*b^*\}, \\ f(ubav) & = & \{ub \mid v \in a^*b^*\}. \end{array}$$

Then, for all subsets $X \subseteq H^*K$ we have

$$h(X), g(X) \subseteq \{a^i b^j \mid 0 \leq i < j\} = HH_0^*.$$

Now, if X is rational, by the pumping Lemma there exists an integer k such that $h(X), g(X) \subseteq \{a^i b^j \mid 0 \leq i \leq k, i \leq j-1\} = H_k H_0^*$ holds and thus $f(X) \subseteq H_k H_0^*$ too. Since $f(X)$ is in $\mathbf{Rat}\{a,b\}^*$, this implies $f(X) \in \mathbf{Rat}(H_k^*)$ by Lemma 16. Consider the right syntactic congruence of the rational set X, let $A_1, \ldots, A_p$ be its (rational) equivalence classes and let $B_1, \ldots, B_p$ be the corresponding right contexts, i.e., for all $u \in A_i$ and for all $v \in \Sigma^*$ we have $uv \in X$ if and only if $v \in B_i$. We have

$$X = \bigcup_{i=0}^{p} (f(X) \cap A_i) B_i$$

which completes the proof via Lemma 17. □

The closure properties of the family $\mathcal{F}_{\text{min}}$ are straightforward. Given a subset $X \subset \mathbf{T}$, we denote by $\min(X)$ the set of all lexicographically minimal representatives of the elements in X.

The family is closed under intersection, because $\min(X \cap Y) = \min(X) \cap \min(Y)$ holds, and under subset subtraction because of $\min(X \setminus Y) = \min(X) \setminus \min(Y)$ but not under complement ($\min(\Sigma^*)$ is not rational). It is not closed under product or star. Indeed, consider $\min(X) = a^*$ and $\min(Y) = (ab^2)^*$. If we intersect $\min(XY)$ with a^*b^*, then we get the subset $\{a^{m+n}b^{2n} \mid m \geq n-1\}$, which is not rational. Concerning the star, if $\min(X) = \{ab\}$, we have $\min(X^*) = \{a^i b^i \mid i \geq 0\}$.

4.2 Lexicographically maximal cross-sections

The following characterizes the lexicographically maximal cross-sections in Σ^* which are rational. We denote by $\max(X)$ the set of lexicographically maximal representatives of the subset $X \subseteq \mathbf{T}$. We already observed that $\max(\mathbf{T}) = \{ab, b\}^*a^*$ holds.

Proposition 19 *A subset $X \subseteq \{ab, b\}^* a^*$ is rational if and only if it is a finite union of products of the form YZ where $Y \in \mathbf{Rat}\{ab, b\}^*$ and $Z \in \mathbf{Rat}\{a\}^*$.*

Proof: Only one direction need be proven. Consider the right syntactic congruence of the rational set X. Let $A_1, \ldots, A_p$ be its (rational) equivalence classes whose corresponding right contexts $B_1, \ldots, B_p$ are contained in a^* and thus contained in $\mathbf{Rat}\{a\}^*$. Then we obtain $A_i \subseteq \{ab, b\}^*$ and thus $A_i \in \mathbf{Rat}\{ab, b\}^*$. Finally, we have

$$X = \bigcup_{i=0}^{p} A_i B_i$$

which completes the proof. □

Proposition 20 *The family $\mathcal{F}_{max}$ is closed under the Boolean operations.*

Proof: Indeed, we have $\max(\mathbf{T} \setminus X) = \max(\mathbf{T}) \setminus \max(X)$. Now, $\max(\mathbf{T})$ and $\max(X)$ are rational subsets of $\{ab, b\}^*\{a\}^*$, thus their difference is a rational subset of $\{a, b\}^*$. □

The family $\mathcal{F}_{\max}$ is not closed under star. Indeed, consider the subset X, which is a singleton, whose representative is $(ab)a$. Then the subset of maximal representatives of X^* is the nonrational subset $\{(ab)^n a^n \mid n \geq 0\}$. However it is closed under product as shown in the next theorem.

Theorem 21 *The family $\mathcal{F}_{max}$ is closed under concatenation.*

Proof: By Proposition 19, it suffices to prove the case of $(XY)(ZT)$ with $X, Z \in \mathbf{Rat}\,\{ab, b\}^*$ and $Y, T \in \mathbf{Rat}\,\{a\}^*$. It suffices further to show that $\max(YZ)$ is of the right form. A further simplification allows us to consider the cases where $Y = \{a\}$ and where $Y = (a^k)^*$, since all rational subsets of $\mathbf{Rat}\,\{a\}^*$ are finite unions of products of subsets of these two types.

Let us first settle the case $Y = \{a\}$ and let us verify that $\max(aZ)$ is actually the image of Z under a rational function. Consider the rational function defined by

$$\begin{aligned} f(ubv) &= uabv, && \text{where } u \in (ab)^*, \\ f(uv) &= uav, && \text{where } u \in (ab)^*, v \in a^* \end{aligned}$$

then $\max(aZ) = f(Z)$.

The second case is a bit more technical. The idea is as follows. A lexicographically maximum word has a unique factorization of the form

$$u_1 b u_2 \ldots u_n b a^{\lambda}, \quad u_i \in (ab)^*, i = 1, \ldots, n. \tag{10}$$

The idea is to replace the pk initial occurrences of b (each following some u_i) in the above factorization by ab, for all possible integers $p \geq 0$. If $pk > n$ then $pk - n$ occurrences of a's are added after the last occurrence of b. Formally, the set of words associated with the word (10) where $n = qk + r$, $0 < r \leq k$ is described as follows. It contains all the words

$$u_1(ab)u_2 \ldots u_{sk}(ab)u_{sk+1} b \ldots u_n b a^{\lambda}, \text{ for some } 0 \leq s \leq q$$

and all the words in the subset

$$u_1(ab)u_2 \ldots u_n(ab)a^{\lambda+k-r}(a^k)^*.$$

This is clearly achieved by a rational relation proving that $\max((a^k)^* Z)$ is a rational subset of Σ^*. □

4.3 Recognizable subsets

In this last paragraph we show that the class of recognizable subsets of the c-trace monoid is not closed under product. As observed in paragraph 1.3, $X \subseteq \mathbf{T}$ is recognizable if and only if $\phi^{-1}(X)$ is recognizable where ϕ is the canonical morphism from Σ^* onto $\mathbf{T}$. Now consider the two recognizable subsets of $\mathbf{T}$, $X = a^*$ and $Y = (abb)^*$. Then we know that the set of maximal representatives of the product is (this is a special case of the construction in Theorem 21)

$$(abab)^*a^* \cup (abab)^*(abb)^*.$$

Denote by P_2 and L_2 respectively, the set of prefixes of the Łukasiewicz language having an even number of occurrences of b's and the set of Łukasiewicz words having an even number of occurrences of b's. Then we have

$$\phi^{-1}(XY) = P_2 \cup L_2(abb)^*.$$

In particular, if a word in $\phi^{-1}(XY)$ is a product of Łukasiewicz words, then all its factors, except maybe the first one, are equal to abb. Let n be the number of states of an automaton recognizing $\phi^{-1}(XY)$. Consider a Łukasiewicz word having a factor of the form b^n. An easy application of the pumping lemma leads us to a contradiction.

References

[1] Marie Albenque and Philippe Nadeau. Growth function for a class of monoids. In *Proceedings of FPSAC 2009*, 2009.

[2] André Arnold, Mathias Kanta, and Daniel Krob. Recognizable subsets of the two letter plactic monoid. *Information Processing Letters*, 64:53–59, 1997.

[3] Jean Berstel. *Transductions and Context-Free Languages*. Teubner Verlag, 1979.

[4] Kellogg S. Booth and George S. Lueker. Linear algorithms to recognize interval graphs and test for the consecutive ones property. In *STOC*, pages 255–265, 1975.

[5] Volker Diekert. *Combinatorics on Traces*, volume 454 of *Lecture Notes in Computer Science*. Springer, 1990.

[6] Samuel Eilenberg. *Automata, Languages and Machines*, volume A. Academic Press, 1974.

[7] http://www.research.att.com/∼njas/sequences/A000071.

[8] Gérard Lallement. *Semigroups and Combinatorial Applications*. John Wiley & Sons, 1979.

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

[10] Antoni Mazurkiewicz. Trace theory. In Wilfried Brauer, Wolfgang Reisig, and Grzegorz Rozenberg, editors, *Petri Nets, Applications and Relationship to other Models of Concurrency*, volume 255 of *Lecture Notes in Computer Science*, pages 279–324. Springer, Berlin-Heidelberg-New York, 1987.

[11] Jr. McKnight. Kleene quotient theorems. *Pacific Journal of Mathematics*, 14:1343–1352, 1964.