Contextual partial commutations
April 29, 2009

Christian Choffrut [1]
http://www.liafa.jussieu.fr/∼cc
Christian.Choffrut@liafa.jussieu.fr

Robert Mercas [2]
http://grammars.grlmc.com/GRLMC/PersonalPages/Robert
robertmercas@gmail.com

Abstract

We consider the monoid with presentation $\mathbf{T} = \langle a, b; aab = aba\rangle$ which is "close" to trace monoids. We give a combinatorial description of the lexicographically minimum and maximum representatives in the free monoid $\{a, b\}^*$ and 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 $\{a, b\}^*$.

Introduction

In this work, we investigate a natural extension of the notion of trace monoids. Indeed, such 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. Here, we restrict these partial commutations by assuming that they are controlled by the context, e.g., the letters a and b would commute when preceded by the letter c but not by the letter d. 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.

Next to the trace monoids whose presentations are defined by relators consisting of pairs of words of length 2, other natural monoids can be encountered in the literature. E.g., the relators defining the plactic monoid originate from the rules of the jeu de taquin and consist of pairs of words of

[1] L.I.A.F.A., Université Paris 7, 2 Pl. Jussieu – 75 251 Paris Cedex – France

[2] GRLMC, Universitat Rovira i Virgili, Dept. de Filologies Romniques, Av. Catalunya, 35 – 43002 Tarragona – Spain. 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".

length 3, see Chapter 5 of [7]. 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 far. Observe though, that contextual monoids are not cancelative which 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 where a and b commute only when preceded by an occurrence of a. 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. This result is instrumental for solving equations which will be the subject of a forthcoming work. It also helps us computing the number of different elements of the contextual trace monoid of a given length.

The second type of contribution is the study of the family of rational subsets in contextual trace monoids. We are mainly concerned with the problem of determining under which conditions the set of representatives, for some choice of the representatives, of a rational subset of the contextual trace monoid is a rational set of words. We study two types of representatives, one obtained by taking the lexicographically minimal and the other the lexicographically maximal word in a congruence class. These two types behave very differently and we are able to establish their main closure properties.

1 Preliminaries

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 letters occurring in u, is denoted by $|u|$. The *empty word* is denoted by 1 and has length 0. Given a total ordering $<$ on Σ, it extends to a *lexicographical ordering* of Σ^*, denoted $u \leq_{\text{lex}} v$, if u is a prefix of v or if $u = wax$ and $v = wby$ holds for some words w, x, y and some letters $a < b$.

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. Given a symmetric and irreflexive relation $I \subset \Sigma \times \Sigma$ called the *independence relation*, the *trace* *monoid with independence relation I* is the monoid whose presentation is $\langle \Sigma; \{(ab, ba) \mid (a, b) \in I\}\rangle$, i.e., it is the quotient of the free monoid Σ^* by the congruence generated by the relators $ab = ba$ whenever $(a, b) \in I$, [6, 8, 3, Chap. 11].

We now introduce the notion of *contextual trace monoid* which, to our knowledge, has not yet been explicitly studied and which is defined as the quotient of Σ^* by a congruence generated by relators of the form $cab = cba$ for some $a, b, c \in \Sigma$. Its elements are *contextual traces.* Clearly, the simplest contextual monoid which is essentially different from a trace monoid has the monoid presentation $\langle a, b; aab = aba\rangle$. Unless otherwise stated, we shall not consider other contextual trace monoids and therefore we restrict the notation $\mathbf{T}$ to that particular monoid throughout this paper. We denote by $\sim$ the congruence generated by the 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.

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 by elements 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 Factorization

We recall that the *Łukasiewicz* language is the unique subset of Σ^* which is a fixed point 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 the set of Łukasiewicz words is a prefix set and therefore, each word w can be factored uniquely as

$$w = w_1 w_2 \cdots w_r w_{r+1}, \qquad (1)$$

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 shows that an equivalence class of the congruence $\sim$ is uniquely determined by its length, the sequence of lengths of the Łukasiewicz factors and the difference between the number of occurrences of a and that of b.

Lemma 1. *Let $w = uv$ such that u is the prefix of a Łukasiewicz word and $w' = u'v' \sim w$ where $|u| = |u'|$. Then u' is also a prefix of a Łukasiewicz word. Furthermore, if u is a Łukasiewicz word so is u'.*

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 2. *For each Łukasiewicz word w, we have*

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

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

Proof. By repeated application of $aab \sim aba$, we get $a^n ba \sim aba^{n-1}$ 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 least 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 greatest 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 3. *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 smallest and greatest 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 4. *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 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

Denote by L_n the number of elements of length n of the monoid $\mathbf{T}$.

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

Proof. The problem amounts to enumerating the number of lexicographically minimum representatives of length n as expressed in (3). Then either $r = 0$ which means that the word is of the form $a^i b^j$ with $i \geq j$ and $i + j = n$, yielding $\lceil \frac{n}{2} \rceil$ nonequivalent words, or it starts with some prefix of the form $a^i b^{i+1}$ and is followed by a lexicographically minimum representative of length $n - (2i + 1)$. Consequently the recurrence relation is

$$\begin{aligned} L_{2n+1} &= n + 1 + L_{2n} + L_{2n-2} + \ldots + L_0, \\ L_{2n} &= n + L_{2n-1} + L_{2n-3} + \ldots + L_1. \end{aligned}$$

Rewriting

$$\begin{aligned} L_{2n+1} &= n + 1 + L_{2n} + L_{2n-2} + \ldots + L_0 \\ &= 1 + L_{2n} + (n + L_{2n-2} + \ldots + L_0) = 1 + L_{2n} + L_{2n-1} \end{aligned}$$

and

$$\begin{aligned} L_{2n} &= n + L_{2n-1} + L_{2n-3} + \ldots + L_1 \\ &= 1 + L_{2n-1} + (n - 1 + L_{2n-3} + \ldots + L_1) = 1 + L_{2n-1} + L_{2n-2}. \end{aligned}$$

we obtain the conditions $L_0 = 1, L_1 = 2$ and $L_n = 1 + L_{n-1} + L_{n-2}$ for $n \geq 2$. This sequence is similar to the Fibonacci sequence. The result follows from [5]. □

It is worthwhile noticing that each of these L_ns has as a Fibonacci bit-representation a prefix of $(10)^*$ (no two consecutive 0's or 1's). E.g., we have $L_5 = 12 = 8 + 3 + 1 = 8 \cdot \underline{1} + 5 \cdot \underline{0} + 3 \cdot \underline{1} + 2 \cdot \underline{0} + 1 \cdot \underline{1}$.

3 Rational subsets with rational cross-sections

We recall that the family of rational subsets of an arbitrary monoid M, denoted $\mathrm{Rat}(M)$, is the smallest collection $\mathcal{F}$ of subsets containing the empty set and all singletons, and closed under set union, set product and star, i.e.

- $X, Y \in \mathcal{F}$ implies $X \cup Y \in \mathcal{F}$ and $XY \in \mathcal{F}$,
- $X \in \mathcal{F}$ implies $X^* \in \mathcal{F}$.

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 of Σ^*, the set

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

is rational, see [4, Thm 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 contextual 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 a rational set of the free monoid. 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 P 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 6. *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 $H^* P$ which is clearly not rational, since its intersection with the rational set $a^+ b^+ a$ is the set $\{a^i b^{i+1} a \mid i \geq 0\}$. The set of all maximal representatives is the rational set $(ab, b)^*a^*$. This shows that $\mathbf{T}$ does not belong to $\mathcal{F}_{\min}$ but it belongs to $\mathcal{F}_{\max}$. 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 $X \in \mathrm{Rat}(\Sigma^*)$ be a subset of M. The following more or less trivial lemma shows that X is actually in $\mathrm{Rat}(M)$. So there is no distinction between the expression "a rational subset of the submonoid M of Σ^*" and "a rational subset of $\mathrm{Rat}(\Sigma^*)$ that is contained in M".

Lemma 7. *Let M be a finitely generated submonoid of Σ^* and let $X \in \mathrm{Rat}(\Sigma^*)$ be a subset that is contained in M. Then X is in $\mathrm{Rat}(M)$.*

Proof. Denote by G a set of generators of M. Let Q be the set of states of an 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 8. *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 $X \in \mathrm{Rat}(\Sigma)^*$ and $Y \in \mathrm{Rat}(\Delta)^*$.*

3.1 Lexicographically minimal cross-sections

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

Proposition 9. *A subset $X \subseteq H^*P$ 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 $\mathrm{Rat}\{a, b\}^*$.*

Proof. Observe that X is rational if and only if $X \setminus a^*b^*$ is rational and the Proposition holds for X if and only if it holds for $X \setminus a^*b^*$, so we assume that $X \cap a^*b^* = \emptyset$. Only one direction needs be proved. Consider the following three rational functions which extract specific factors of a word in $\{a,b\}^*$. When applied to a word in H^*P defined by its decomposition as in (3), these factors are respectively the first maximum factor 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.

$$\begin{array}{ll} h(ubav) = ub, & u \in a^*b^+, \\ g(ubavbaw) = avb, & v \in a^*b^*, \\ f(ubav) = ub, & v \in a^*b^*. \end{array}$$

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

$$h(X), g(X) \subseteq \{a^ib^j \mid 0 \leq i \leq j-1\} = HH_0^*.$$

Now, if X is rational, by the pumping Lemma there exists an integer k such that $h(X), g(X) \subseteq \{a^ib^j \mid 0 \leq i \leq k, i \leq j-1\} = \left(\bigcup_{i=0}^k (H_i)\right)H_0^*$ holds and thus $f(X) \in \left(\bigcup_{i=0}^k (H_i)\right)^*$. Since $f(X)$ is in $\mathrm{Rat}(\{a,b\}^*)$, this implies $f(X) \in \mathrm{Rat}\left(\bigcup_{i=0}^k (H_i)\right)^*$ by Lemma 7. 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 8. □

The closure properties of the family $\mathcal{F}_{\min}$ 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 either 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 $\min(X^*) = \{a^ib^i \mid i \geq 0\}$.

3.2 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 $X \subseteq \mathbf{T}$. Observe that we have $\max(\mathbf{T}) = \{ab, b\}^* a^*$.

Proposition 10. *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 $Y \in \mathrm{Rat}\{ab, b\}^*$ and $Z \in \mathrm{Rat}\{a\}^*$.*

Proof. Only one direction needs to be proved. Let $\{c, d\}$ be two new symbols. Consider the morphism $h : \{c, d\}^* \to \{a, b\}^*$ defined by $h(c) = ab$ and $h(d) = b$ and the injective partial rational function $g : \{c, d\}^*\{a\}^* \to \{a, b\}^*$ which assigns to uv, with $u \in \{c, d\}^*$ and $v \in \{a\}^*$ the word $h(u)v$. By Lemma 8, a rational subset $X \subseteq \{c, d\}^*\{a\}^*$ is a finite union of products of the form of YZ where $Y \in \mathrm{Rat}\{c, d\}^*$ and $Z \in \mathrm{Rat}\{a\}^*$. Then the result follows by considering its image under the rational function g. □

Proposition 11. *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 12. *The family $\mathcal{F}_{max}$ is closed under concatenation.*

Proof. We prove the claim for the concatenation of XY with ZT with $X, Z \in \mathrm{Rat}\,\{ab, b\}^*$ and $Y, T \in \mathrm{Rat}\,\{a\}^*$. Actually it suffices 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 $\mathrm{Rat}\,\{a\}^*$ are finite unions of products of subsets of these two types. Concerning the set Z, we use the characterization of Proposition 10.

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 greatest word has a unique factorization of the form

$$u_1 b u_2 \dots u_n b a^\lambda, \quad u_i \in (ab)^*, i = 1, \dots, n \tag{4}$$

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 (4) where $n = qk + r$, $0 < r \leq k$ is described as follows. It contains all the words

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

and the subset

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

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

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

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

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

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

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

[8] 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.