Constructing sequential bijections

Christophe Prieur[1], Christian Choffrut[1] and Michel Latteux[2]

[1] Université Paris 7, LITP, 2 Pl. Jussieu, 72 251 Paris Cadex 05
[2] Université de Lille1, LIFL, bat. M3, Cité Scientifique, 59 655 Villeneuve d'Ascq Cedex
France

Abstract. We state a simple condition on a rational subset X of a free monoid B^* for the existence of a sequential function that is a one-to-one mapping of some free monoid A^* onto X. As a by-product we obtain new sequential bijections of a free monoid onto another.

1 Introduction

The starting point of the present paper is a simple question. Given two free monoid A^* (the "input" monoid) and B^* (the "output" monoid) respectively generated by m and n elements, design an effective function that is as elementary as possible and that maps bijectively A^* onto B^*. A natural solution uses the free monoid over m (resp. n) letters as a representation set of the integers in base m (resp. n); the problem of the leading zeros can be solved by resorting to the so-called p-adic representation instead of the standard one. But actually we use a less elaborate computation model.

Provide each transition of a finite deterministic automaton on A with an element in the free monoid B^*. The deterministic transducer thus obtained associates with every "input" string an "output" string, i. e., it defines a sequential function from A^* to B^*. This model relies on a memory that is only finite and does not allow afterthoughts. Indeed, it preserves prefixes so that any decision met for input string u envolves all strings having u as a prefix. The property of prefix-preservation can be viewed as follows. Consider the input monoid as a m-ary tree, and label each branch with a string from the output alphabet in such a way that all strings from the output monoids appear exactly once as the label of some path starting from the root. If we further require that the tree be produced by a finite deterministic transducer, then it has only finitely many different subtrees.

The condition on m and n for the existence of a solution was given in [3] by using a decomposition of the free monoid akin to the coset decomposition of groups. Here we address the more general issue of designing, when possible, a sequential function that performs a one-to-one mapping of a free monoid onto a given rational subset of $X \subseteq B^*$. The techniques utilized here rely on the completion of "partial" solutions. Indeed, the interpretation of the problem in terms of a labelled tree still makes sense in this more general setting. It should be intuitive that the input alphabet is immaterial, what counts is that every node has exactly m successors. The labels assigned to the different branches of a given node can be rearranged among the children without violating the bijectivity. Now consider a finite graph with labels in B^* and assume each string in X is the label of exactly one path. Unroll this graph so as to obtain a (not necessarily

m-ary) tree. The techniques developped in this paper allow, under certain conditions, to make the tree uniform without modifying the global set of labels, i. e., to obtain global solutions from partial ones.

In order to state the main result, we need some technical definitions. Denote by 1 the neutral element of B^*. For all $u, v \in B^*$, u is a *prefix* of v if there exists $x \in B^*$ such that $v = ux$. Given a subset $X \subseteq B^*$ and an element $u \in B^*$, set $u^{-1}X = \{x \in B^* \mid ux \in X\}$ and say $u \in X$ has *branching degree* d (relative to X) if the set $u^{-1}X - \{1\}$ has d minimal elements relative to the relation "being a prefix of".

Theorem 1. *Given a rational subset $X \subseteq B^*$ with $1 \in X$, and an integer $d > 1$, assume the following conditions are satisfied*

i) all elements $u \in X$ have branching degree smaller than or equal to d.

ii) for all $u \in X$ there exists $v \in X$, u a prefix of v, such that v has branching degree greater than 1.

Then there exists a sequential function that maps bijectively a free monoid with d generators onto X.

This result extends that of [3] in that it substitutes an arbitrary rational subset X for the free monoid B^*. It has a further interesting consequence taking us back to the initial question. If the complement of X (to which the neutral element 1 is added, to be more precise) satisfies the two conditions of the theorem too, then there exists a natural bijection from a free monoid onto B^* that is built by merging the two sequential functions for X and its complement in some natural way. In particular, this approach shows that suffix codes are not a necessary ingredient for sequential bijections of a free monoid onto another, as was implicitely assumed in [3]. But in spite of providing new and more elaborate solutions for the original problem, the present method fails, at least as exposed here, to recover all solutions given in [3].

Before tackling the problem, let us mention some related problems mainly concerned with the more powerful model of rational functions. Using slightly different definitions of sequential mappings (in fact introducing final states), algorithms for determining under which conditions there exists a sequential function mapping a given rational language onto another have been devised, cf., [7] and [9]. In [6] the same problem is considered where bijective rational transductions are used in place of sequential functions.

2 Preliminaries

We refer to [4], [2] and [8] for a more detailed exposition of the main notions briefly recalled here.

2.1 Free monoids

Given a set A (an *alphabet*) consisting of *letters*, A^* denotes the free monoid it generates. The elements of A^* are *words* or *strings*. The *length* of a word w is denoted by $|w|$. The *empty* word, denoted by 1, is the word of length 0 and A^+ denotes the set of non empty words.

2.2 Sequential functions

The notion of sequential functions of a free monoid into another is standard. We recall it for the sake of completeness. Intuitively, these mappings are realized by finite deterministic automata where all transitions are provided with an output.

Given two alphabets A and B, a *sequential transducer* $\mathcal{T}$ is a finite deterministic automaton whose states are all accepting, equipped with an *output function* from the set of transitions into B^*. Formally, we have $\mathcal{T} = (Q, i, \lambda)$ where Q is the set of states and i the initial state; the *next state* function of the *underlying* automaton associates with all pairs (q, a) a state $q.a$ and the *output* function λ associates with all pairs $(q, a) \in Q \times A$ a word in $\lambda(q, a) \in B^*$. These two functions are extended to A^* by induction on the length of the words:

i) for all $q \in Q$, $q.1 = q$

ii) for all $q \in Q, a \in A$, $u \in A^*$, $q.ua = (q.u).a$

iii) for all $q \in Q$, $\lambda(q, 1) = 1$

iv) for all $q \in Q$, $a \in A$, $u \in A^*$, $\lambda(q, ua) = \lambda(q, u)\lambda(q.u, a)$

The cardinality of Q is the *dimension* of the transducer. A function $f : A^* \to B^*$ is *sequential* if there exists a sequential transducer $\mathcal{T}$ such that $f(u) = \lambda(i, u)$ holds for all $u \in A^*$. Observe that all states are final and thus the function is total. We say the function f is *realized* by the transducer $\mathcal{T}$.

The present paper continues the study of the bijective sequential functions of a free monoid into another initiated in [3].

2.3 Rational series

The notion of power series is crucial, since the study of the sequential bijections can be reduced to it via a standard construction.

A $\mathbb{N}$ -*power series* in the *indeterminates* A is a function of A^* into the semiring of non negative integers $\mathbb{N}$. Such a series $\sigma : A^* \to \mathbb{N}$ is usually denoted as a formal sum

$$\sigma = \sum_{u \in A^*} \sigma(u)u$$

where $\sigma(u)$ is the *coefficient* of $u \in A^*$. The set $\mathbb{N}\langle\langle A^*\rangle\rangle$ of power series is provided with a structure of $*$-semiring by defining the addition, the product and the star operations. Indeed, if $\sigma_1, \sigma_2 \in \mathbb{N}\langle\langle A^*\rangle\rangle$ are two power series the sum and the product are defined by

$$(\sigma_1 + \sigma_2)(u) = \sigma_1(u) + \sigma_2(u),$$

$$(\sigma_1\sigma_2)(u) = \sum_{u=u_1u_2} \sigma_1(u_1)\sigma_2(u_2),$$

for all $u \in A^*$. The star of a power series σ with $\sigma(1) = 0$ is defined by

$$\sigma^*(u) = 1 + \sum_{n>0, u=u_1\ldots u_n} \sigma(u_1)\ldots\sigma(u_n)$$

for all $u \in A^*$. In particular a $\mathbb{N}$ -power series is *unambiguous* if its coefficients are 0 or 1.

The *support* of a power series $\sigma \in \mathbb{N}\langle\langle A^* \rangle\rangle$ is the subset consisting of all the elements $u \in A^*$ such that $\sigma(u) \neq 0$. In particular, an unambiguous series is the *characteristic* series of its support. The subsemiring of *polynomials* is the subset of all series having finite support.

The family of $\mathbb{N}$ -*rational* series, denoted by $\mathbb{N}$ -RatA^*, is the least family of series containing the polynomials and closed under addition, product and star.

Closely related to the notion of rational series is that of finite automata. For our purpose, we rely on a generalization of the notion of finite automaton. We call *generalized* automaton a triple $\mathcal{A} = (Q, i, D)$ where Q is the set of *states*, i is the *initial* state and $D \subseteq Q \times A^+ \times Q$ is a finite set of *transitions*, cf. [5]. Given a transition (q, u, q'), we say it *leaves* state q and *enters* state q'. The *degree* of state q, denoted by $\deg_{\mathcal{A}}(q)$ or simply $\deg(q)$ when the automaton $\mathcal{A}$ is understood, is the number of transitions leaving it. The automaton is *uniform* if all states have same degree. A *path* of *length* k in a generalized automaton is a sequence of k transitions of the form (q_0, u_0, q_1), (q_1, u_1, q_2), $\ldots$, $(q_{k-2}, u_{k-2}, q_{k-1})$ (q_{k-1}, u_{k-1}, q_k) where $(q_{i-1}, u_{i-1}, q_i) \in D$ for $i = 1, \ldots, k$. When $k = 1$ and $q_0 = q_k$, the path is a *loop*.

The *behaviour* of (or the series *recognized* by) $\mathcal{A}$ is the $\mathbb{N}$ -power series, denoted by $||\mathcal{A}||$, that assigns to every string $u \in A^*$ the number of paths starting in i and labelled with u. Observe that in the standard terminology we would say that all states are final. As follows from Kleene's Theorem (see e.g., [4], Theorem VII, 5. 1), $||\mathcal{A}||$ is a $\mathbb{N}$ -rational power series. A generalized automaton is *non ambiguous*, if $||\mathcal{A}||$ has coefficients 0 and 1. Two generalized automata are *equivalent* if they have the same behaviour.

3 Systems of equation

As said in the introduction, the present paper is concerned with sequential functions of a free monoid into another that are bijective. Let $\mathcal{T}$ be a sequential transducer realizing a sequential mapping of $f : A^* \to B^*$. Since there is a one to one correspondence between the words of A^* and the paths in the underlying automaton of $\mathcal{T}$, saying that f is a bijection is equivalent to saying that the behaviour of the generalized automaton $\mathcal{A}$ obtained from $\mathcal{T}$ by ripping off the input letter from every transition is the characteristic series of B^*.

From now on, we study sequential bijection in terms of generalized automata. Actually, it is customary to associate with such an automaton a system of equations in the variables $X_q \in \mathbb{N}\langle\langle B^* \rangle\rangle$, for each $q \in Q$, by setting

$$X_q = 1 + \sum_{q' \in Q} \alpha_{q,q'} X_{q'} \tag{1}$$

where $\alpha_{q,q'} = \sum\{u \in B^* \mid (q, u, q') \in D\}$.

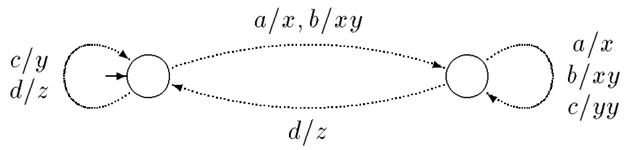
It is well known that such a system has a solution and that this solution is unique if the support of the polynomials $\alpha_{q,q'}$ does not contain the empty element 1. In that case, the value of the component X_i (where i is the initial state) is the behaviour of the automaton $\mathcal{A}$, see [4] Prop. VII, 6.1.

Conversely, assume that the $\alpha_{q,q'}$'s in system (1) are polynomials with non negative integer coefficients and that for each $q \in Q$, the sum of the coefficients of $\sum_{q' \in Q} \alpha_{q,q'}$ equals the cardinality of A. If further the value of the X_i-component is the characteristic series of B^* then the system can be interpreted as defining a sequential bijection of A^* onto B^* by arbitrarily distributing the monomials of $\sum_{q' \in Q} \alpha_{q,q'}$ for each $q \in Q$, to the letters of A.

Example 1. With $B = \{x, y, z\}$ we have

$$\begin{aligned} X_0 &= 1 + (y+z)X_0 + (x+xy)X_1 \\ X_1 &= 1 + zX_0 + (x+xy+yy)X_1 \end{aligned}$$

The sum of the coefficients of the 2 polynomials $y+z+x+xy$, and $z+x+xy+yy$ are equal to 4. Furthermore, the component X_0 is the characteristic series of $\{x, y, z\}^*$. Thus, the system gives rise to a bijective sequential mapping of the free monoid generated by $A = \{a, b, c, d\}$ onto B^*



4 The coset construction

We recall here briefly a previous construction of a bijective mapping from a free monoid A^* into another B^*, [3]. Denoting by $\#A$ the cardinality of A, a necessary condition for the existence of such a mapping is that $\#A > \#B > 1$ or $\#A = \#B$ as can be readily seen. It turns out to be sufficient. The solution reminds the decomposition of a group relative to its cosets since it starts from the equality $B^* = SZ^*$ (as series) where Z is a finite complete suffix code and S the set of its proper suffixes, cf. [1].

Theorem 2. *Let A and B be two alphabets of cardinality m and n respectively. Then there exists a bijective sequential mapping of A^* onto B^* if and only if $m > n > 1$ or $m = n$ holds. Furthermore, if the condition is satsified, there exists a mapping of dimension 2.*

Proof. (Sketch) Let p be an integer such that $k(n-p-1) = m-p-1$ holds for some integer $k > 1$. Decompose $B = B_1 \cup B_2$ with $\#B_1 = p$. Let $Z \subseteq B_2^*$ be a complete suffix code with $m-p$ elements and let S be the set of its proper suffixes that are different from the empty string. Let b be an arbitrary letter of B_2. Then the pair (B^*, Z^*) is the solution of the following system.

$$\begin{aligned} X_0 &= 1 + (B_1 + b)X_0 + (S + Z - b(1+S))X_1 \\ X_1 &= 1 + B_1 X_0 + Z X_1 \end{aligned}$$

Example 2. Example 1 corresponds to $B_1 = \{z\}$, $B_2 = \{x, y\}$, $b = y$ and $Z = \{x, xy, yy\}$

5 Transformation rules

Here we establish some transformation rules that preserve the behaviour of an unambiguous generalized automaton and that allow, under some hypotheses, to convert a given non uniform generalized automaton into a uniform one. The final degree however, depends on the degrees of the initial automaton. These rules are in essence simple transformations of systems of equations in the algebra of power series. We shall apply this technique to any generalized automaton recognizing the characteristic series of B^* in the last section in order to get novel sequential bijections.

5.1 By-pass rule

This operation makes a first state by-pass a second state. It increases the degree of the first state, which is all the purpose, and creates a new state of degree equal to the second one minus one.

By-pass rule: given an unambiguous generalized automaton $\mathcal{A} = (Q, i, D)$ and the non necessarily distinct transitions $(q_0, u, q_1), (q_1, v, q_2) \in D$, perform the following operations

1. create a new state $q_3 \notin Q$
2. delete transition (q_0, u, q_1)
3. add transitions (q_0, u, q_3), (q_0, uv, q_2)
4. for every $(q_1, w, p) \in D$ such that $w \neq v$, add the transition (q_3, w, p)

Proposition 3. *The by-pass rule tranforms an unambiguous generalized automaton $\mathcal{A}$ into an equivalent generalized automaton $\mathcal{A}'$.*

The degrees of the states are preserved except for the conditions $deg_{\mathcal{A}'}(q_3) = deg_{\mathcal{A}}(q_1) - 1$ and $deg_{\mathcal{A}'}(q_0) = deg_{\mathcal{A}}(q_0) + 1$.

Proof. Assign a system of equations with $\mathcal{A}$ as in section 3. If q_0 and q_1 are equal introduce a new variable and duplicate the equation associated with $q_0 = q_1$. Rename the indices of the variables X_j of the system as $\{0, 1, \ldots, n-1\}$ so that X_0, X_1 are associated with q_0 and q_1. Finally, let X_k, for some $0 \leq k < n$ be associated with q_2. This process ends up with a system of n equations in the n unknowns $X_j \in \mathbb{N}\langle\langle A^* \rangle\rangle$ where X_0, X_1 and X_k are associated with q_0 and q_1, q_2 respectively.

$$X_j = E_j \text{ for } 0 \leq j < n \tag{2}$$

By hypothesis, there exist $F_0, F_1 \in \mathbb{N}\langle\langle A^* \rangle\rangle$ such that

$$\begin{aligned} E_0 &= uX_1 + F_0 \\ E_1 &= vX_k + F_1 \end{aligned}$$

holds. The by-pass rule consists in introducing a new unknown X_n and the new system of equations

$$X_j = \begin{cases} uX_n + uvX_k + F_0 & \text{if } j = 0 \\ E_j & \text{if } j \neq 0, n \\ F_1 & \text{if } j = n \end{cases} \tag{3}$$

It suffices to prove that systems (2) and (3) are equivalent. Indeed, for every solution $(X_j)_{0\le j<n}$ of system (2), there is a X_n such that $(X_j)_{0\le j\le n}$ is a solution of system (3). The only unknown for which this requires a verification is X_0

$$\begin{aligned} X_0 &= E_0 = uX_1 + F_0 = u(vX_k + F_1) + F_0 \\ &= uvX_k + uX_n + F_0 \end{aligned}$$

Conversely, for every solution $(X_j)_{0\le j\le n}$ of system (3), $(X_j)_{0\le j<n}$ is a solution of system (2). Again, only X_0 needs verification

$$\begin{aligned} X_0 &= uX_n + uvX_k + F_0 = uF_1 + uvX_k + F_0 \\ &= u(F_1 + vX_k) + F_0 = uX_1 + F_0 = E_0 \end{aligned}$$

5.2 Pumping rule

The purpose of this operation is to use the existence of a loop in a first state in order to "pump" new transitions for the second state. It increases the degree of the first state by one.

Pumping rule: given an unambiguous generalized automaton $\mathcal{A} = (Q, D, i)$ and the non necessarily distinct transitions $(q_0, u, q_1), (q_1, s, q_1), (q_1, v, q_2) \in D$ with $(s, q_1) \neq (v, q_2)$, perform the following operations

1. create a new state $q_3 \notin Q$
2. delete transition (q_0, u, q_1)
3. add transitions (q_0, u, q_3), (q_0, uv, q_2)
4. add transitions (q_3, s, q_3) and (q_3, sv, q_2) and for every $(q_1, w, p) \in D$ such that $w \neq v$ and $w \neq s$ add the transition (q_3, w, p)

Proposition 4. *The pumping rule tranforms an unambiguous generalized automaton $\mathcal{A}$ into an equivalent generalized automaton $\mathcal{A}'$ The degrees of the states are preserved except for the conditions $deg_{\mathcal{A}'}(q_3) = deg_{\mathcal{A}}(q_1)$ and $deg_{\mathcal{A}'}(q_0) = deg_{\mathcal{A}}(q_0) + 1$.*

Proof. Proceeding as for the by-pass rule by assigning a system of equations to $\mathcal{A}$ we obtain a system of n equations in the n unknowns $X_j \in \mathbb{N}\langle\langle A^*\rangle\rangle$ where X_0, X_1 and X_k are associated with q_0 and q_1, q_2 respectively.

$$X_j = E_j \text{ for } 0 \le j < n \tag{4}$$

By hypothesis, since $(s, q_1) \neq (v, q_2)$ holds, there exist $F_0, F_1 \in \mathbb{N}\langle\langle A^*\rangle\rangle$ such that

$$\begin{aligned} E_0 &= uX_1 + F_0 \\ E_1 &= sX_1 + vX_k + F_1 \end{aligned}$$

holds. The pumping rule consists in introducing a new unknown X_n and the new system of equations

$$X_j = \begin{cases} uX_n + uvX_k + F_0 & \text{if } j = 0 \\ E_j & \text{if } j \neq 0, n \\ sX_n + svX_k + F_1 & \text{if } j = n \end{cases} \tag{5}$$

Every solution $(X_j)_{0\le j<n}$ of system (4), there is a X_n such that $(X_j)_{0\le j\le n}$ is a solution of system (5). Indeed, observe that unknown X_1 in system (4) satisfies

$$X_1 = s^*(vX_k + F_1)$$

and unknown X_n in system (5) satisfies

$$X_n = s^*(svX_k + F_1)$$

i. e., $sX_1 + F_1 = X_n$. Now compute X_0 in system (4)

$$\begin{aligned} X_0 &= E_0 = uX_1 + F_0 = u(sX_1 + vX_k + F_1) + F_0 \\ &= uX_n + uvX_k + F_0 \end{aligned}$$

Conversely, for every solution $(X_j)_{0\le j\le n}$ of system (5), $(X_j)_{0\le j<n}$ is a solution of system (4). Again, only X_0 needs verification

$$\begin{aligned} X_0 &= uX_n + uvX_k + F_0 = us^*(svX_k + F_1) + uvX_k + F_0 \\ &= us^*vX_k + us^*F_1 + F_0 = uX_1 + F_0 = E_0 \end{aligned}$$

6 Uniformizing an unambiguous generalized automaton

Uniformizing an unambiguous generalized automaton without modifying its behaviour, i.e., making all its nodes have the same degree, whatever the degree, is not always possible. We shall give sufficient conditions for achieving this goal. We first need a few definitions.

Given an unambiguous generalized automaton $\mathcal{A} = (Q, i, D)$ a subset $\emptyset \neq Q' \subseteq Q$ is *stable* if for any state $q \in Q'$ and any transition $(q, u, q') \in D$, $q' \in Q'$ holds. It is a *minimal stable* subset if it is stable and if it does not properly contain a stable subset. Clearly, for every state there exists a path from it to some minimal stable subset. Also, any minimal stable subset Q' is strongly connected in the sense that for all $q, q' \in Q'$ there exists a path from q to q'.

An unambiguous generalized automaton $\mathcal{A} = (Q, i, D)$ is *uniform of degree d* if all states q have degree d. It has *limit degree $d \le 1$* if all states of some minimal stable subset have degree $d \le 1$. Otherwise it has limit degree $d = \max\{\deg(q) \mid q \in Q\}$.

The following procedure transforms an unambiguous generalized automaton $\mathcal{A}$ with limit degree $d > 1$ into an equivalent generalized automaton $\mathcal{A}'$ (i. e., $||\mathcal{A}|| = ||\mathcal{A}'||$) that is uniform of degree d' for some arbitrary $d' \ge d$.

1. Let Q_i, $i = 1, \ldots, r$ be the minimal stable subsets of the automaton. Identify in each Q_i a state ℓ_i as follows. If there exists $\ell \in Q_i$ with a loop, set $\ell_i = \ell$. Otherwise, by hypothesis on the limit degree, there exists an element $\ell \in Q_i$ and a cycle $\ell = q_0, q_1, \ldots, q_k = q_0$ with $\deg(q_{k-1}) > 1$. Apply repeatedly the by-pass rule backwards to the transitions $(q_{k-2}, u_{k-2}, q_{k-1})$, (q_{k-1}, u_{k-1}, q_k) for some $u_{k-2}, u_{k-1} \in B^*$, then to the transitions $(q_{k-3}, u_{k-3}, q_{k-2})$, $(q_{k-2}, u_{k-2}u_{k-1}, q_k)$ for some $u_{k-3} \in B^*$, ... then to the transitions (q_0, u_0, q_1), $(q_1, u_1 \ldots u_{k-2}u_{k-1}, q_k)$ for some $u_0 \in B^*$, cf. example 3. Then set $\ell_i = \ell$. In all cases we end up with a state ℓ_i having a transition (ℓ_i, u, ℓ_i).

2. If one of the above states ℓ_i does not have degree d', increase its degree by applying the by-pass rule to the transitions (ℓ_i, u, ℓ_i), (ℓ_i, u, ℓ_i), as many times as needed.
3. Whenever there exists a state with degree less than d', choose any such state q_0 with minimal distance to a state q with a loop and degree d'.
   i) if the distance is one, then apply the pumping rule to the states q_0, q.
   ii) if the distance is greater than one, let q_1 and q_2 be the first and second states along a path of minimal length from q_0 to q. Let (q_0, u, q_1), (q_1, w, q_2), $(q_1, v, q_3) \in D$ with $(q_1, v, q_3) \neq (q_1, w, q_2)$. Then apply the by-pass rule to the transitions $(q_0, u, q_1), (q_1, v, q_3)$.

Proposition 5. *The previous procedure transforms an unambiguous generalized automaton $\mathcal{A}$ with limit degree $d > 1$ into an equivalent generalized automaton $\mathcal{A}'$ that is uniform with degree d'.*

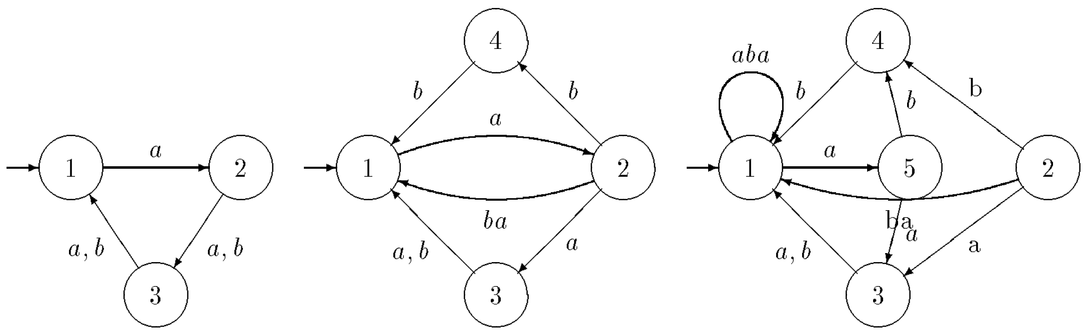
Proof. Fix a state $\ell = \ell_i$. Consider step 1 and use the same notations as in the above procedure. The by-pass rule applied to the transitions $(q_{k-i-1}, u_{k-i-1}, q_{k-i})$ and $(q_{k-i}, u_{k-i} \dots u_{k-1}, q_k)$ erases the only transition $(q_{k-i-1}, u_{k-i-1}, q_{k-i})$ and creates the transition $(q_{k-i-1}, u_{k-i-1}, q_k)$. Assume by contradiction that some state q that could reach ℓ before the application of the rule no longer reaches it afterwards. Then there existed a path from q to ℓ that used transition $(q_{k-i-1}, u_{k-i-1}, q_{k-i})$ exactly once. But now q_{k-i-1} is directedly connected to ℓ so that the former path can take the shortcut $(q_{k-i-1}, u_{k-i-1}, \ell)$. As for the new created state, say p, since q_{k-i} has degree at least 2, there is a transition (q_{k-i}, v, q') with $(v, q') \neq (u_{k-i} \dots u_{k-1}, q_k)$ so that (p, v, q') is created. Thus there exists a path from p to q' and from q' to ℓ. The same assertion holds for step 2 since no transition is erased.

Thus, before step 3, each state can reach a state of degree d' having a loop. Consider the quantity

$$E = \sum_{q \in Q} (d' - \deg(q)) \lambda_q$$

where $\deg(q)$ is the degree of $q \in Q$ and λ_q the minimal distance of q to a state with a loop and degree d'. When $\lambda_q = 1$, then each application of i) decrements the quantity E by one. When $\lambda_q > 1$, then ii) produces a new state of degree $d' - 1$ at distance $\lambda_q - 1$ of q and reduces the quantity $\deg(q)$ by one. Thus, E decreases in all cases by one.

Example 3 (Creating a loop in state 1*).*

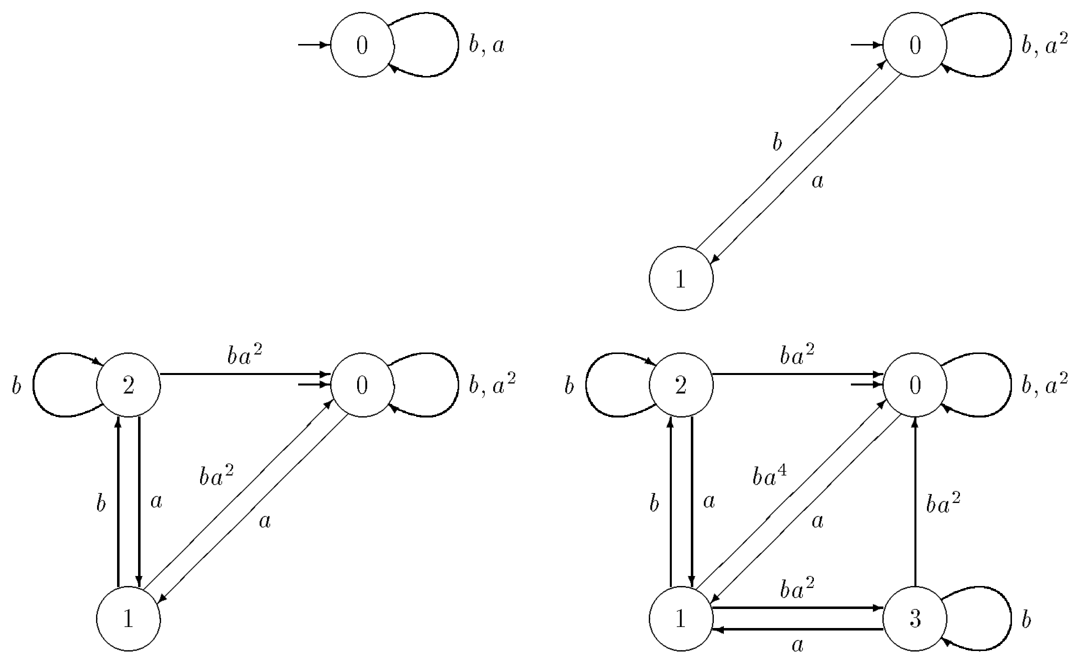


Example 4 (Application of the by-pass and the pumping rules). Starting with the generalized automaton reduced to one state 0 and having the only transitions $(0, a, 0)$ and $(0, b, 0)$ that recognizes $\{a, b\}^*$ we obtain in 3 steps a uniform generalized automaton of degree 3.

Step 1: by-pass of state 0 by itself, with transitions $(0, a, 0)$, $(0, a, 0)$

Step 2: pumping of state 0 from state 1, with transitions $(1, b, 0)$, $(0, b, 0)$, $(0, a^2, 0)$

Step 3: pumping of state 0 from state 1, with transitions $(1, ba^2, 0)$, $(0, b, 0)$, $(0, a^2, 0)$



7 Applications to sequential bijections

In this last section we generalize the example of the previous section by showing for a fixed rational subset $X \subseteq B^*$ how to design, when possible, a bijective sequential mapping of some free monoid A^* onto X .

We recall that a state q of a finite deterministic automaton (in the usual sense), is a *sink* whenever $q = q.a$ holds for all letters a of the alphabet.

Theorem 6. *Given a rational subset $X \subseteq B^*$ with $1 \in X$, the following conditions are equivalent*

1. *the minimal automaton of X satisfies the two conditions*
   i) *every cycle which does not visit a sink contains a terminal state*
   ii) *for every terminal state there are two paths whose labels are not a prefix of one another that lead from this state to some terminal states.*

2. *there exists an alphabet A of cardinality greater than 1 and a sequential bijection of $f : A^* \to B^*$ that maps A^* onto X.*

Proof. 1) implies 2). Indeed, let $\mathcal{A} = (Q, q_-, Q_+)$ be the minimal automaton (in the usual sense) recognizing X where q_- stands for the initial state and Q_+ for the set of final states. The condition of the theorem is equivalent to saying that the maximal length of a path connecting two final states without visiting a final state inbetween, is bounded by the cardinality of the set of states. An unambiguous generalized automaton recognizing X is obtained as follows. The set of states is Q_+. The set of transitions is D where $D \subseteq Q_+ \times B^+ \times Q_+$ with $(q_0, u, q_1) \in D$ if and only if u is the label of a path from q_0 to q_1 in $\mathcal{A}$ that does not visit a terminal state between the two end states.

Consider a terminal state q and two paths labelled by two words, not a prefix of each other, say xau and xbv where x is the maximum common prefix, a and b are two different letters and $u, v \in B^*$. Without loss of generality, we may assume that there is no terminal state visited by the path starting in q and labelled by x and that the paths labelled by au and bv starting in $q.x$, do not visit a terminal state except at their ends. Thus, there are two transitions leaving q, namely $(q, xau, q.xau)$ and $(q, xbv, q.xbv)$. Therefore, the unambiguous generalized automaton recognizing X has limit degree greater than 1. It suffices to apply the procedure described in section 6.

2) implies 1). If f maps bijectively A^* onto X, then there exists an integer p such that every $u \in X$ has a proper prefix $v \in X$ of length at least $|u| - p$. Assume there exists in the minimal automaton recognizing X a cycle starting in q not visiting a sink and consisting of non terminal states only. Consider a shortest path from q to some terminal state $q_+ \in Q_+$. Set $q_-.u = q$, $q.v = q$ and $q.w = q_+$ where v is the label of the cycle through q and where u and w are suitable words. Now, no prefix of $uv^p w$ of length greater than or equal to $|uv^p w| - p$ is recognized by the automaton. This leads to a contradiction.

Let q be an arbitrary terminal state of the minimal automaton, $u \in B^*$ a word taking the initial state to q and $x \in A^*$ such that $f(x) = u$. Since all words $f(xy)$, when y ranges over A^* have different images, the number of their images grows exponentially and their length grows linearly as a function of $|y|$. Thus these images can not be pairwise comparable relative to the relation “being a prefix of” which shows that there are among them two words that are not prefix of one another.

As a consequence, if a rational subset $X \subseteq B^*$ and $B^* - X \cup \{1\}$ satisfy the conditions of the previous theorem, then we proceed as follows. We add a new initial state with no entering transition to both unambiguous generalized automata and we make the union of two copies of them with the two initial states merged. Then we apply the uniformization procedure of section (6) in order to get a sequential bijection of a free monoid into B^*. The converse uses an analog argument as that of the previous theorem, thus we have

Theorem 7. *Given a rational subset $X \subseteq B^*$ with $1 \in X$, the following conditions are equivalent*

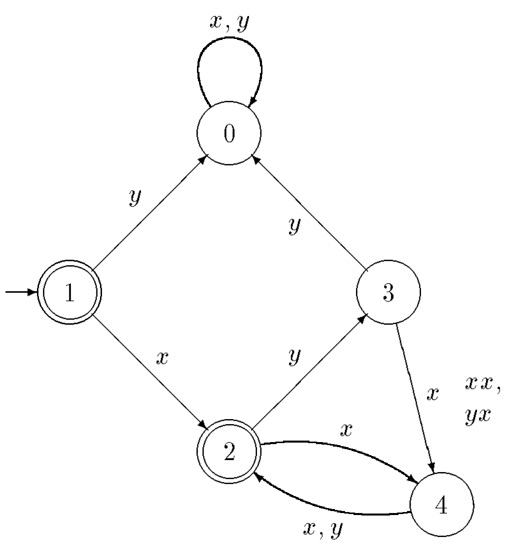
1. *the minimal automaton of X satisfies the two conditions*

   i) *every cycle which does not visit a sink contains a terminal and a non terminal state*

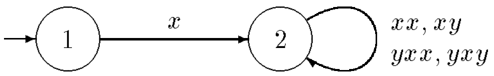
ii) *for every terminal (resp. non terminal) state there are two paths whose labels are not a prefix of one another that lead from this state to some terminal (resp. non terminal) states.*

2. *there exists an alphabet A of cardinality greater than 1, a decomposition $A = A_1 \cup A_2$ and a sequential bijection of $f : A^* \to B^*$ that maps $1 + A_1 A^*$ onto X, and therefore $A_2 A^*$ onto $B^* - X$.*

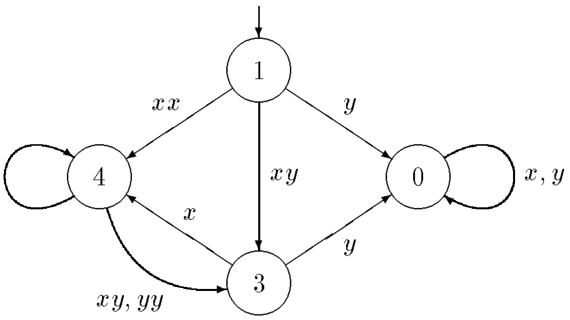
Let us illustrate the theorem with the language $R = 1 + (xx + xy + yxx + yxy)^*$. We first construct the "canonical" generalized automaton recognizing R (the one obtained naturally from the minimal automaton as in the proof of theorem 6) then the canonical generalized automaton recognizing $A^* - R + 1$. Then we make the union of the two



Deterministic complete automaton of R

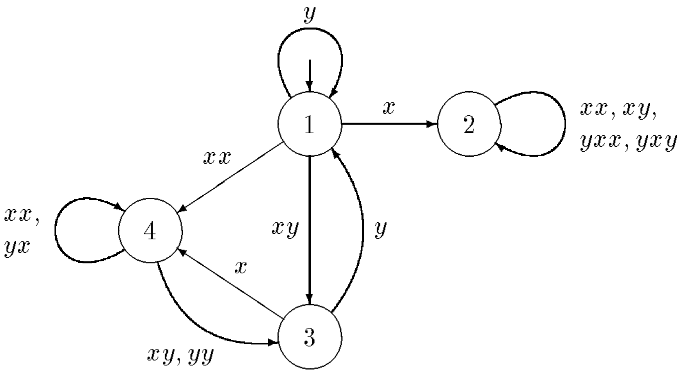


Generalized automaton of R

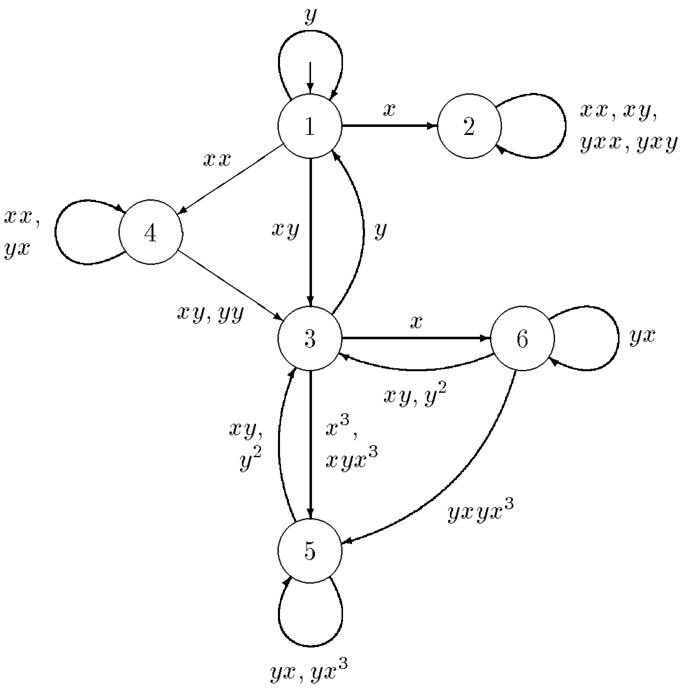


Generalized automaton of $A^* - R + 1$

We obtain a new automaton by merging the two initial states and by identifying state 0 of $A^* - R + 1$ with the new initial state.



Applying the procedure of section 6 yields the final generalized wchich can be made into a bijection of a 4-generator onto a 2-generator free monoid.



References

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

2. J. Berstel and C. Reutenauer. *Rational Series and Their Languages*, volume 12 of *EATCS Monograph on Theoretical Computer Science*. Academic Press, 1988.
3. C. Choffrut. Bijective sequential mappings of a free monoid onto another. *RAIRO Informatique Théorique et Applications*, 28:265–276, 1994.
4. S. Eilenberg. *Automata, Languages and Machines*, volume A. Academic Press, 1974.
5. K. Hashiguchi. Algorithms for determining the number of non-terminals sufficient for generating a regular language. In B. Monien J. Leach Albert and M. Rodríguez Artalejo, editors, *ICALP 91*, number 510 in LNCS, pages 641–648. Springer Verlag, 1991.
6. H. A. Maurer and M. Nivat. Rational bijections of rational sets. *Acta Informatica*, 13:365–378, 1980.
7. R. Mac Naughton. A decision procedure for generalizd mappability-onto of regular sets. In *STOC Conference*, pages 206–218, 1971.
8. A. Salomaa and M. Soittola. *Automata-Theoretic Aspects of Formal Power Series*. Springer, 1978.
9. K. B. Salomon. The decidability of a mapping problem for generalized sequential machines with final states. *J. of Comput. and Sys. Sci.*, 10(2):200–218, 1975.