ELSEVIER

Theoretical Computer Science 215 (1999) 329–335

Theoretical Computer Science

Note

A proof of Choffrut's theorem on subsequential functions

Véronique Bruyère [a], Christophe Reutenauer [b,c,*]

[a] *Université de Mons-Hainaut, avenue du Champ de Mars, 6, 7000 Mons, Belgique*
[b] *Université du Québec à Montréal, Canada*
[c] *Département de mathématiques, Case postale 8888, succursale Centre-ville, Montréal, Québec, Canada H3C 3P8*

Received February 1998
Communicated by M. Nivat

Abstract

We prove an extension of the Ginsburg–Rose theorem, and as a corollary, Choffrut's topological characterization of subsequential functions.

Keywords: Subsequential; Machine; Rational

0. Introduction

The aim of the present note is to give a conceptual proof of Choffrut's theorem on subsequential functions. These functions were introduced by Schützenberger, and are the good and ultimate concept for what can be computed sequentially from left to right. They generalize sequential functions, and include many nice examples: integer division and multiplication, decoding of prefix codes (or more generally, codes with finite deciphering delay), pattern substitution, etc.

Choffrut's theorem gives a characterization of these functions by two conditions: they preserve rationality of languages by inverse image, and they satisfy a metric condition, called by him *bounded variation*. These two conditions have a topological flavour, and the second one is especially interesting, in view of the recent interest to the same metric (the prefix distance) in group theory, in the Gromov hyperbolic groups, and more generally the automatic groups, see [5].

* Correspondence address: Département de mathématiques, Case postale 8888, succursale Centre-ville, Montréal, Québec, Canada H3C 3P8. E-mail: christo@math.uqam.ca.

0304-3975/99/$ – see front matter
PII: S0304-3975(98)00163-7

In Berstel's book, Berstel [1], one may find a proof of Choffrut's theorem, which is essentially the same as the original one, see [3]. In Reutenauer [7], the second author has given another proof, by introducing the *differential* of a subsequential function, which generalizes the same notion for sequential functions, see [4]. Unfortunately, this definition is inadequate in general, so that proof is not correct. In the present note, we restrict the definition of a differential to subsequential functions having a prefix-closed domain: this allows us to give our main result (Theorem 2.1), which is a generalization of the theorem of Ginsburg and Rose. Then, another argument allows us to deduce Choffrut's theorem. We have tried to separate the proof in several lemmas, which show clearly the ideas involved; most of them are already in Choffrut's work, but we believe that the present note will clarify things and give more audience to this wonderful result.

A word about terminology: the word "subsequential" is unfortunate, since these functions should be called simply "sequential"; but we keep the usual terminology, and hope that someone will find some day a definite terminology. Also "bounded variation" has also be called "continuous", or "uniformly bounded" in Reutenauer and Schützenberger [8]. We go back to the initial terminology.

1. Notations and terminology

As usual, A^* denotes the *free monoid* generated by the *finite alphabet* A and 1 *the empty word*. In general, *letters* (i.e. elements of A) will be denoted by $a, b, c, \ldots$, and *words* (i.e. elements of A^*) will be denoted by $u, v, w, \ldots$ We denote also by $A^{(*)}$ the free group generated by A, and by $|g|$ the reduced length of an element g of $A^{(*)}$. Also let $A^+ = A^* \setminus 1$.

The *prefix distance* is the distance on A^* defined by $d(u,v) = |u^{-1}v| = |v^{-1}u|$. In this form, it is easy to show that the triangular inequality is satisfied. An alternative definition is $d(u,v) = |u'| + |v'|$, where $u = pu'$, $v = pv'$ and p is the longest common prefix of u and v (cf. [1, p. 104]).

Given two alphabets A and B, let f be a *function* (which here means *partial function*) whose domain $\mathrm{dom}(f)$ is *prefix-closed*, that is $uv \in \mathrm{dom}(f) \Rightarrow u \in \mathrm{dom}(f)$. We define its *differential* as the function $\varphi : A^+ \to B^{(*)}$ such that for any word w in A^* and any letter a

$$\varphi(wa) = f(w)^{-1} f(wa),$$

where the left-hand side is undefined if so is the right hand-side. Note that $\mathrm{dom}(\varphi) = \mathrm{dom}(f) \setminus 1$, since f has a prefix-closed domain. This definition extends the definition of Eilenberg [4, p. 314], for a *prefix-preserving function* f (called there initial segment preserving), i.e. a function f with a prefix-closed domain such that for any $uv \in \mathrm{dom}(f)$, $f(u)$ is a prefix of $f(uv)$.

The differential allows to reconstruct f by the formula:

$$f(w) = f(1)\varphi(a_1)\varphi(a_1a_2)\cdots\varphi(a_1a_2\ldots a_n) \tag{1}$$

for any word $w = a_1a_2\ldots a_n$.

Let $f: A^* \to B^*$ be any function. We denote by p_u the longest common prefix of all the words $f(uw)$, $uw \in \mathrm{dom}(f)$; if there is no such uw, $p_u = \emptyset$. Then we define the function $f \cdot u$, called the *derivative of f with respect to u*, by

$$(f \cdot u)(w) = p_u^{-1} f(uw)$$

with the same conventions on emptiness as before.

We shall not define *subsequential* functions here, but use the following characterization (see [3, Proposition 4], or [7, Theorem 1]): a function $f: A^* \to B^*$ is subsequential if and only if the set $\{f \cdot u \mid u \in A^*\}$ is finite.

Note that a subsequential function is a sequential function if and only if it is prefix preserving; we shall use this characterization of sequential function, due to Choffrut, see [1, Proposition IV. 2.6] One can also mimic the second part of the proof of Theorem 1 in Reutenauer [7], where the subsequential transducer which is constructed turns out to be sequential, when the function is prefix preserving.

2. An extension of the Ginsburg–Rose theorem

Theorem 2.1. *Let $f: A^* \to B^*$ be a function with prefix-closed domain. The following properties are equivalent:*

(i) *f is subsequential,*

(ii) *f^{-1} preserves rationality of languages and for some k*

$$d(f(w), f(wa)) < k$$

if w, $wa \in \mathrm{dom}(f)$,

(iii) *the differential φ of f has a finite image and $\varphi^{-1}(t)$ is rational for any t in $B^{(*)}$.*

This result extends the theorem of Ginsburg–Rose on sequential functions, as it is stated in Eilenberg [4, Theorem XI. 6.3], where sequential functions are called generalized sequential partial functions.

Theorem 2.2 (Ginsburg–Rose). *Let f be a prefix-preserving function $A^* \to B^*$. The following properties are equivalent:*

(i) *f is sequential,*

(ii) *f^{-1} preserves rationality of languages and for some k*

$$d(f(w), f(wa)) < k$$

if w, wa in $\mathrm{dom}(f)$,

(iii) *the differential φ of f has a finite image and $\varphi^{-1}(t)$ is rational for any t in B^*.*

In order to deduce the previous theorem from Theorem 2.1, it is enough to use the remarks on sequential functions given in Section 1.

We turn now to the proof of Theorem 2.1. We prove first two lemmas. Following Reutenauer and Schützenberger [8, p. 672], let us call *adjacent* two functions $f, g : A^* \to B^*$ such that

$$\max\{d(f(w), g(w)) \mid w \in \mathrm{dom}(f) \cap \mathrm{dom}(g)\} = N < \infty. \tag{2}$$

Lemma 2.1. *Let f, g be two adjacent functions such that f^{-1}, g^{-1} preserve rationality of languages. Then for any u, v in B^*, the language*

$$L(u,v) = \{w \in A^* \mid \exists p \in B^*,\ f(w) = pu,\ g(w) = pv\}$$

is rational.

This is Lemma 6(i) in Reutenauer and Schützenberger [8], for which we give a lucid proof, by reworking the ideas already present in the work of Choffrut.

Proof. Note that if f, g satisfy the hypothesis, so do their restriction to rational languages. We proceed by a series of reductions. We begin by showing that $L(1,1)$ is rational.

1. Suppose that $f(w)$, $g(w)$ if defined have always the same length. By (2), in order that $f(w) = g(w)$, it is sufficient that either these words have length $\geqslant N$ and have the same suffix of length N, or these words are equal and of length $< N$. Hence,

$$L(1,1) = \bigcup_{|u|=N} (f^{-1}(B^*u) \cap g^{-1}(B^*u)) \cup \bigcup_{|u|<N} (f^{-1}(u) \cap g^{-1}(u))$$

   is a rational language.
2. The general case of $L(1,1)$ may be reduced to part 1 if we show that the language $K = \{w \in A^*, \mid |f(w)| = |g(w)|\}$ is rational (indeed, we then replace f and g by their restriction to K). Now by (2), the length of $f(w)$ and $g(w)$ differ at most by N. Hence $|f(w)| = |g(w)| \Leftrightarrow \exists i \in \{0, 1, \ldots, N\}$ such that $|f(w)| \equiv |g(w)| \equiv i \bmod (N+1)$. Hence,

$$K = \bigcup_{0 \leqslant i \leqslant N} f^{-1}(B^i(B^{N+1})^*) \cap g^{-1}(B^i(B^{N+1})^*),$$

   which is rational by hypothesis.
3. In order to prove rationality of $L(u,v)$, define the function f', g' by $f'(w) = f(w)u^{-1}$ and $g'(w) = g(w)v^{-1}$ (where $x + y^{-1} = \emptyset$ if $xy^{-1} \in B^{(*)} \backslash B^*$). Then $w \in L(u,v) \Leftrightarrow f'(w) = g'(w)$. Hence, it is enough to show that f', g' satisfy to the hypotheses of the lemma (and we are reduced to case 2). But this is clear. □

If $f : A^* \to B^*$ is a function, recall from Section 1 that $f \cdot 1$ is the function $(f \cdot 1)(w) = p^{-1} f(w)$, where p is the longest prefix common to all words $f(w)$, $w \in \mathrm{dom}(f)$.

Lemma 2.2. *Let $f_1, f_2 : A^* \to B^*$ be two functions, $x_1, x_2 \in B^*$, and $h : A^* \to B^{(*)}$ be such that $f_i(w) = x_i h(w)$ for any w in $\mathrm{dom}(f_1) = \mathrm{dom}(f_2) = \mathrm{dom}(h)$.*

Then $f_1 \cdot 1 = f_2 \cdot 1$.

Proof. Observe that if $h(A^*) \subseteq B^*$, then clearly $f_i \cdot 1 = h \cdot 1$ and $f_1 \cdot 1, f_2 \cdot 1$ are equal.

In the general case, for w in $\mathrm{dom}(h)$, $h(w)$ may be written in *reduced* form $y(w)^{-1} k(w)$, where $y(w) \in B^*$ and $k(w) \in B^*$. Then $f_i(w) = x_i y(w)^{-1} k(w) \in B^*$, so that $y(w)$ is a suffix of x_i. Choose $y = y(w_0)$ of maximal length among all $y(w)$, $w \in \mathrm{dom}(h)$. Then $x_i = x_i' y$ and $y = y_i(w) y(w)$ for any w, with $y_i(w) \in B^*$; the latter equation implies that $y_1(w) = y_2(w) = z(w)$, say. Thus, $f_i(w) = x_i'\ y\ y(w)^{-1} k(w) = x_i'\ z(w)\ k(w)$. This implies $f_1 \cdot 1 = f_2 \cdot 1$ by the previous observation. □

Proof of Theorem 2.1. (i) $\Rightarrow$ (ii): It is clear by considering a subsequential transducer for f. This implication is rather easy and details are omitted.

(ii) $\Rightarrow$ (iii): That φ has finite image is clear, since $\varphi(wa) = f(w)^{-1} f(wa)$ has reduced length $< k$ in the free group. Let $t \in B^*$ such that $\varphi^{-1}(t)$ is nonempty. Then, by definition of φ, t must be of the form $u^{-1}v$, for some u, v in B^*. We may suppose that u, v have no common prefix: then $u^{-1}v$ is a reduced word in $B^{(*)}$. Fix $a \in A$. We have $\varphi(wa) = t \Leftrightarrow f(w)^{-1}\ f(wa) = u^{-1}v \Leftrightarrow f(w) = xu, f(wa) = xv$ for some word x in B^* (indeed, write $f(w) = x'u', f(wa) = x'v'$, where u', v' have no common prefix; then $f(w)^{-1} f(wa) = u'^{-1}v' = u^{-1}v^{-1}$ implies that $u' = u, v' = v$). This shows that we may apply Lemma 2.1 to the functions f and g with $g(w) = f(wa)$, which are adjacent and preserve rationality under inverse image by assumption. We obtain $wa \in \varphi^{-1}(t) \Leftrightarrow w \in L(u, v)$, hence $\varphi^{-1}(t)$ is rational since A is finite.

(iii) $\Rightarrow$ (i): It is enough to show that the functions $f \cdot u$, $u \in A^*$, are in finite number. The languages $\varphi^{-1}(t)$, $t \in \mathrm{Im}(\varphi)$, are all rational and in finite number. Hence, there exists a right congruence $\sim$ on A^* of finite index such that $u \sim v$ implies that: $u \in \mathrm{dom}(f) \Leftrightarrow v \in \mathrm{dom}(f)$ and $u \in \varphi^{-1}(t) \Leftrightarrow v \in \varphi^{-1}(t)$ for any t in $\mathrm{Im}(\varphi)$. Thus, $u \sim v$ implies $\varphi(u) = \varphi(v)$.

We show that $u \sim v$ implies $f \cdot u = f \cdot v$, which will finish the proof. Let $w = a_1 \ldots a_n$, $a_i \in A$. By (1) in Section 1, we have

$$f(uw) = f(u)\varphi(ua_1)\varphi(ua_1a_2) \cdots \varphi(ua_1 \ldots a_n)$$

and

$$f(vw) = f(v)\varphi(va_1)\varphi(va_1a_2) \cdots \varphi(va_1 \ldots a_n).$$

We have $ua_1 \ldots a_i \sim va_1 \ldots a_i$ since $\sim$ is a right congruence. Hence,

$$\varphi(ua_1 \ldots a_i) = \varphi(va_1 \ldots a_i).$$

Thus, there exists a function $h : A^* \to B^{(*)}$ (depending on u, v) such that $f(uw) = f(u)h(w), f(vw) = f(v)h(w)$. By Lemma 2.2 applied to the functions $f_1(w) = f(uw)$, $f_2(w) = f(vw)$ (observe that $\mathrm{dom}(f_1) = \mathrm{dom}(f_2) = \mathrm{dom}(h)$), we deduce $f_1 \cdot 1 = f_2 \cdot 1$, thus $f \cdot u = f \cdot v$. □

3. Choffrut's theorem

A function $f:A^*\to B^*$ has bounded variation if for any ℓ, there exists k such that for any u,v in $\mathrm{dom}(f)$, $d(u,v)<\ell \Rightarrow d(f(u),f(v))<k$, where d is the prefix distance (see Section 1). It is not difficult to show that this is equivalent to the condition: for any x,y, the functions $w\mapsto f(wx)$ and $w\mapsto f(wy)$ are adjacent; hence also to the condition displayed in Theorem 2.1(ii) when f has a prefix-closed domain. By considering a subsequential transducer, it is easy to show that each subsequential function has bounded variation. This shows implication (i) $\Rightarrow$ (ii) of the next result.

Theorem 3.1 (Choffrut). *Let f be a function $A^*\to B^*$. Then the two following conditions are equivalent:*

(i) *f is subsequential.*

(ii) *f^{-1} preserves rationality of languages and f has bounded variation.*

Proof. It remains to prove (ii)$\Rightarrow$(i). We construct a function $g:A^*\to B^*$ which has a prefix-closed domain, which satisfies condition (ii) of Theorem 2.1 and such that $f=g\,|\,\mathrm{dom}(f)$. This will imply that f is subsequential: indeed, $f=g\circ h$, with $h=\mathrm{id}\,|\,\mathrm{dom}(f)$ and $\mathrm{dom}(f)=f^{-1}(B^*)$ is rational; hence h is subsequential, and it is well-known that the composition of two subsequential functions is subsequential.

Let $\mathscr{A}$ be a finite deterministic automaton recognizing $\mathrm{dom}(f)$; we assume that each state in $\mathscr{A}$ is accessible and coaccessible; for any state q in $\mathscr{A}$, let u_q be some word in A^* such that $q\cdot u_q$ is a final state in $\mathscr{A}$, with $u_q=1$ if q is final. Define $g(w)=f(wu_q)$, if $q_\circ\cdot w=q$, where $q_\circ$ is the initial state of $\mathscr{A}$. Then clearly $g(w)=f(w)$, if $w\in\mathrm{dom}(f)$, since then $q_\circ\cdot w$ is final and $u_q=1$. Furthermore, if w,w' are close for d, then so are wu_q and $w'u_{q'}$ (since there are only finitely many words u_q), and the bounded variation of g follows from that of f.

We show that g^{-1} preserves rationality. This follows from the next formula, for any $L\subset B^*$,

$$\begin{aligned} g^{-1}(L) &= \bigcup_{q\in Q}\{w\in A^*\mid q_\circ\cdot w=q,\ f(wu_q)\in L\}\\ &= \bigcup_{q\in Q}\{w\in A^*\mid q_\circ\cdot w=q\}\cap(f^{-1}(L)u_q^{-1}), \end{aligned}$$

where Ku^{-1} means $\{w\in A^*\mid wu\in K\}$ for $K\subseteq A^*$. Hence, g^{-1} preserves rationality.

4. More

If $f:A^*\to B^*$ is a function, define, as in Mohri [6], the function $g:A^*\to B^*$ by $g(w)=$ longest common prefix of all words $f(wu), wu\in\mathrm{dom}(f)$ (and $g(w)=\emptyset$ if no such u exists). Moreover, define $h:A^*\to B^*$ by $f(w)=g(w)h(w)$, with $\mathrm{dom}(h)=\mathrm{dom}(f)$.

Suppose that f is subsequential. Then, using the minimal subsequential transducer for f (see [6, 7]), one may show that g is a sequential function, that h has finite image and that h^{-1} preserves rationality. Conversely, these three conditions easily imply that f is subsequential.

Now, suppose that f^{-1} preserves rationality and has bounded variation, i.e. satisfies condition (ii) of Choffrut's theorem. Using the latter, one deduces that g and h satisfy the three properties above. However, it would be interesting to show directly, without this theorem, these three conditions. For an efficient algorithm allowing the construction of the minimal subsequential transducer, see [2].

References

[1] J. Berstel, Transductions and context-free languages, Teubner, 1979.
[2] D. Breslauer, The suffix tree of a tree and minimizing sequential transducers, Theoret. Comput. Sci. 191 (1998) 131–144.
[3] C. Choffrut, A generalization of Ginsburg and Rose's characterization of g–s–m mappings, Lect. Notes Comput. Sci. 71 (1979) 88–103.
[4] S. Eilenberg, Automata, Languages and Machines, vol. A, Academic Press, 1974.
[5] D. Epstein, J. Cannon, D. Holt, S. Levy, M. Paterson, W. Thurston, Word Processing in Groups, Jones and Bartlett, Boston, London, 1992.
[6] M. Mohri, Minimization algorithms for sequential transducers, Theoret. Comput. Sci. (1998) to appear.
[7] C. Reutenauer, Subsequential functions: characterizations, minimization, examples, Lect. Notes Comput. Sci. 464 (1990) 62–79.
[8] C. Reutenauer, M. Schützenberger, Minimization of rational word functions, SIAM J. Comput. 20 (1991) 669–685.