Zoltán Ésik (Ed.)

Fundamentals of Computation Theory

9th International Conference, FCT '93
Szeged, Hungary, August 23-27, 1993
Proceedings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80
Vincenz-Priessnitz-Straße 1
D-76131 Karlsruhe, Germany

Juris Hartmanis
Cornell University
Department of Computer Science
4130 Upson Hall
Ithaca, NY 14853, USA

Volume Editor

Zoltán Ésik
Computer Science Department, József Attila University
Aradi v. tere 1, H-6720 Szeged, Hungary

CR Subject Classification (1991): F, G.2, I.3.5, E

ISBN 3-540-57163-9 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-57163-9 Springer-Verlag New York Berlin Heidelberg

Printed in Germany

Typesetting: Camera-ready by authors
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
45/3140-543210 - Printed on acid-free paper

FOREWORD

This volume constitutes the proceedings of the Ninth Conference on Fundamentals of Computation Theory (FCT 93) held in Szeged, August 23–27, 1993. Previous conferences of the FCT series took place in Poznan–Kornik (1977), Wendisch–Rietz (1979), Szeged (1981), Borgholm (1983), Cottbus (1985), Kazan (1987), Szeged (1989) and Berlin (1991). Like its predecessors, the conference was devoted to a broad range of topics of theoretical computer science, including the following categories:

- Semantics and logical concepts in the theory of computing and formal specification
- Automata and formal languages
- Computational geometry, algorithmic aspects of algebra and algebraic geometry, cryptography
- Complexity (sequential, parallel, distributed computing, structure, lower bounds, complexity of analytical problems, general concepts)
- Algorithms (efficient, probabilistic, parallel, sequential, distributed)
- Counting and combinatorics in connection with mathematical computer science

The proceedings contain the texts of 8 invited lectures and 32 short communications selected by the international program committee from a large number of submitted papers. The selection meeting took place on March 13–14 in Szeged. The program committee consisted of L. Babai, S.L. Bloom, L. Budach, R.G. Bukharajev, L. Czaja, Z. Ésik, F. Gécseg, J. Gruska, J. Karhumäki, M. Karpinski, B. Mahr, J. Sakarovitch, I. Simon, I. Wegener.

My sincere thanks go to all members of this committee as well as to all the referees who assisted in the selection process: F.M. Ablaev, M. Bartha, D. Beauquier, J. Berstel, N. Blum, L. Boasson, H. Carstensen, Ch. Choffrut, B. Courcelle, E. Csuhaj-Varju, M. Crochemore, P. Dembinski, V. Diekert, M. Dietzfelbinger, S. Dulucq, P. Fischer, L. Fortnow, U. Freitag, K. Friedl, Ch. Frougny, Z. Fülöp, T. Gaizer, L. Gasieniec, R. Glas, M. Grabowski, E. Grandjean, S. Haddad, T. Harju, D. Hemschlelt, Th. Hofmeister, W. Hohberg, J. Honkala, Gy. Horváth, K.-U. Höffgen, M. Hühne, M. Ito, M. Jantzen, Tao Jiang, S. Jukna, B. Kacewicz, J. Kari, L. Kari, B. Kirsig, Y. Kohayakawa, W. Kozlowski, M. Krause, H.-J. Kreowski, M. Kudlek, V.S. Kugurakov, S.E. Kuznetsov, A.P. do Lago, K.-J. Lange, R.H. Latipov, A. Lentin, B.L. Lorho, W. Lukaszewicz, E.G. Manes, R. Mantaci, A. Mateescu, A. Mazurkiewicz, R.G. Mubarakzianov, I.R. Nasirov, V. Niemi, D. Niwinski, N.N. Nurmeev, V. Oleshchuk, M. Palis, P. Peladeau, M. Pelletier, J.-G. Penaud, M. Penttonen, H. Petersen, S. Pölt, P. Pudlák, M. Raczunas, G. Rahonis, F.I. Salimov, A. Salomaa, L.V. Satyanarayana, D. Sieling, J. Simon, V.D. Soloviev, E.L. Stolov, K. Sutner, A. Szalas, J.L. Szwarcfiter, É. Tardos, W. Thomas, D.R. Troeger, Gy. Turán, F. Vatan, J. Virágh, W. Vogler,

S. Waack, E.G. Wagner, S. Waligórski, I. Walukievicz, P. Weil, A. Weber, K. Werther, D. Wikarski, I. Winkowski, C. Zdobnov and S.V. Zdobnov.

The conference was organized by the Department of Computer Science of the József Attila University. I wish to thank my colleagues T. Gaizer and J. Virágh who helped me in all organization matters. They formed a very small but effective team.

The conference was supported by a COST project of the Commission of the European Communities, the József Attila University, the Szeged branch of the Hungarian Academy of Science, a grant from the Hungarian National Foundation for Scientific Research and the ZENON Computer Engineering and Trading Ltd. I would like to thank them all.

Finally, I would like to express my deepest gratitude to all authors and to Alfred Hofmann of Springer-Verlag for their excellent cooperation in the publication of this volume.

Szeged, June 1993

Zoltán Ésik

TABLE OF CONTENTS

INVITED LECTURES

COMMUNICATIONS

REWRITING, MÖBIUS FUNCTIONS AND SEMI-COMMUTATIONS*

Volker Diekert

Universität Stuttgart, Institut für Informatik,
Breitwiesenstr. 20–22, D 70565 Stuttgart

1 Introduction

The purpose of this paper is to review some results in the theory of rewriting on traces which has been obtained over the past few years and to discuss some open problems.
The theory of rewriting over free partially commutative monoids (trace rewriting) combines combinatorial aspects from string rewriting (modulo a congruence) and graph rewriting. It leads to feasible algorithms, but some interesting complexity questions are still open. One of the challenging open problems is to improve the known quadratic time bound for the non-uniform complexity of length-reducing systems. For certain one-rule systems we present here a new linear time algorithm for computing irreducible descendants, but we are still not able to handle the general case of multiple rules in linear time.
Semi commutations can be treated from the viewpoint of trace rewriting and there are strong connections to the combinatorics of Möbius-functions. This is reviewed in Sections 5 and 6.
We assume that the reader is familiar with the concept of Mazurkiewcz traces [22]. For the background material we refer to [1, 12, 23] and to the forthcoming book on traces [16]. For basic notions needed here on rewriting systems see [3, 19].

2 Notations

By Σ we denote a finite alphabet, $D \subseteq \Sigma \times \Sigma$ is a reflexive and symmetric dependence relation and $SD \subseteq \Sigma \times \Sigma$ is a reflexive semi-dependence relation which may be asymmetric. The complement $I = \Sigma \times \Sigma \setminus D$ is called the independence relation and the quotient monoid $IM = IM(\Sigma, D) = \Sigma^*/\{ab = ba \mid (a,b) \in I\}$ is Mazurkiewcz' trace monoid. An element $t \in IM$ is a trace. We denote by $|t|$ the length of a trace t, by $|t|_a$ its a-length for some $a \in \Sigma$, and by $\mathrm{alph}(t) = \{a \in \Sigma \mid |t|_a \geq 1\}$ its alphabet. It is convenient to extend the independence relation to a relation over IM. For $u, v \in IM$ we define $(u,v) \in I$, if we have $\mathrm{alph}(u) \times \mathrm{alph}(v) \subseteq I$. A trace is viewed as a dependence graph:

* This research has been partially supported by the ESPRIT Basic Research Action No. 6137 ASMICS II

Let $a_1 \cdots a_n \in \Sigma^*$ be a word, $a_i \in \Sigma$ for $1 \leq i \leq n$. Then the corresponding trace $[a_1 \cdots a_n] \in IM$ is given by the node-labelled acyclic graph $[V, E, \lambda]$ where the set of vertices is any n-point set, say $V = \{1, \ldots, n\}$ with the labelling $\lambda(i) = a_i$, and arcs are from i to j if both $i < j$ and $(a_i, a_j) \in D$. It is convenient to distinguish between the notions of subtrace and factor. A ***subtrace*** s of t is a subgraph of the dependence graph of t such all directed paths starting and ending in s are entirely contained in s. Every subtrace s of t is a factor, i.e., we can write $t = usv$, but this factorization is not unique, in general. The other way, if $t = usv$ then the traces u, s and v can be identified as subtraces of t. Of course, different subtraces may be equal viewed as factors or elements of IM. To be precise, if we speak of a subtrace $s \subseteq t$, we mean that we have identified the vertices belonging to s in the graph t.
A dependence alphabet (Σ, D) (independence alphabet (Σ, I) resp.) will be viewed als an undirected graph where edges are between different dependent (independent resp.) letters. A trace is called connected, if the dependence graph t is connected or, what is the same, if $\mathrm{alph}(t)$ induces a connected subgraph in (Σ, D).

3 Trace rewriting systems

In this section we give some overview on known results and open questions for trace rewriting systems.

Definition: *A trace rewriting system is a (finite) set of rules $S \subseteq IM(\Sigma, D) \times IM(\Sigma, D)$.*

A trace rewriting system S defines a reduction relation $\underset{S}{\Longrightarrow}$ by $x \underset{S}{\Longrightarrow} y$ if $x = ulv, y = urv$ for some $u, v \in IM$ and $(l, r) \in S$. The n-fold iteration of $\underset{S}{\Longrightarrow}$ is denoted by $\overset{n}{\underset{S}{\Longrightarrow}}$ for $n \geq 0$. By $\overset{+}{\underset{S}{\Longrightarrow}}$ ($\overset{*}{\underset{S}{\Longrightarrow}}$ resp. , $\overset{*}{\underset{S}{\Longleftrightarrow}}$ resp.) we denote the transitive (reflexive, transitive resp., reflexive, symmetric, and transitive resp.) closure of $\underset{S}{\Longrightarrow}$. The relation $\overset{*}{\underset{S}{\Longleftrightarrow}}$ is a congruence and its quotient monoid is denoted by IM/S.
A trace rewriting system S is called:

- length-reducing, if $|l| > |r|$ for all $(l, r) \in S$
- noetherian, if there is no infinite derivation chain $x_0 \underset{S}{\Longrightarrow} x_1 \underset{S}{\Longrightarrow} x_2 \cdots$
- confluent, if $\overset{*}{\underset{S}{\Longleftrightarrow}} \subseteq \overset{*}{\underset{S}{\Longrightarrow}} \circ \overset{*}{\underset{S}{\Longleftarrow}}$
- locally confluent, if $\underset{S}{\Longleftarrow} \circ \underset{S}{\Longrightarrow} \subseteq \overset{*}{\underset{S}{\Longrightarrow}} \circ \overset{*}{\underset{S}{\Longleftarrow}}$
- strongly confluent, if $\underset{S}{\Longleftarrow} \circ \underset{S}{\Longrightarrow} \subseteq \overset{\leq 1}{\underset{S}{\Longrightarrow}} \circ \overset{\leq 1}{\underset{S}{\Longleftarrow}}$
- the set of irreducible traces is $\mathrm{Irr}(S) = \{t \in IM \mid \text{ for no } s : t \underset{S}{\Longrightarrow} s\}$.

It is well-known that strong confluence implies confluence and confluence implies local confluence. No other implication holds, in general. If in addition the system S is noetherian then confluence becomes equivalent to local confluence.

A classical result says that it is undecidable whether a finite semi-Thue system is noetherian. More precisely, we can state:

Proposition 3.1 *It is decidable whether a finite trace rewriting system is noetherian if and only if $I\!M$ is commutative.*

Proof: If $I\!M$ is not commutative, we may use an encoding of semi-Thue systems. If $I\!M$ is commutative then the noetherian property can be expressed by some Presburger formula. □

The minimal number of rules which we need to have undecidability is not known. In fact, the following problem is open:

Problem 1 Given a one-rule system $S = \{(l,r)\}, l, r \in I\!M$. Is it decidable whether S is noetherian?

Remark 3.2 For one-rule semi-Thue systems this is an outstanding open problem and for one-rule term rewriting systems the property of being noetherian is undecidable [9]. Of course, a positive solution to Problem 1 would imply the semi-Thue case. However, due to the commutation rules it may happen that there is a negative answer in the trace case and a positive answer in the word case. This is exactly what happens for the decidability of the confluence of noetherian systems.
Indeed, for finite noetherian semi-Thue systems (local) confluence is decidable, since a finite system has finitely many so-called *critical pairs*, only. For trace rewriting systems the notion of a critical pair is not completely clear. Whatever definition we use, there must be finite noetherian systems without any finite computable set of critical pairs. This is due to the following result of P. Narendran and F. Otto:

Proposition 3.3 ([25]) *There exists an alphabet (Σ, D) with exactly one pair of independent letters such that the confluence of finite length-reducing trace rewriting systems is recursively undecidable.*

Problem 2 Let (Σ, D) be a dependence alphabet such that confluence of finite noetherian systems is decidable and let (Σ', D') be an induced subgraph of (Σ, D). Is the confluence of finite noetherian systems decidable for (Σ', D')?

A positive solution of Problem 2 is not obvious, since the confluence of a system depends on the whole alphabet and not only on the letters occurring in the system, c.f. the next example.

Example Let

$$(\Sigma, D) = (a - b - c)\ ,\ (\Sigma', D') = \begin{array}{ccc} a & - & b \\ | & & | \\ d & - & c \end{array}$$

and $S = \{(ab, ba), (bc, cb)\}$. We may view S as a system over $I\!M = I\!M(\Sigma, D)$ or over $I\!M' = I\!M(\Sigma', D')$. The system S is noetherian in both cases. This can be seen by mapping it to $\{a,b\}^* \times \{b,c\}^*$. The system $S \subsetneq \mathbb{M} \times \mathbb{M}$ is confluent, since every trace reduces to a unique normal form in $c^*b^*a^*$. Viewing $S \subseteq \mathbb{M}' \times \mathbb{M}'$ over the monoid $\mathbb{M}'$, the confluence disappears:

$$\mathrm{Irr}(S) \ni badc \underset{S}{\Longleftarrow} abdc \underset{S}{\Longrightarrow} adcb \in \mathrm{Irr}(S)$$

The minimal number of letters required to achieve the undecidability is not known. In particular, we do not know the answer for three letters.

Problem 3 Let $(\Sigma, D) = (a - b - c)$. Is it decidable whether a finite noetherian system is confluent?

A more general problem is to find good (decidable) sufficient conditions for noetherian systems such that confluence becomes decidable. Further details can be found in [12, Chapt.3].

4 Algorithms

A finite trace rewriting system is called *convergent* or *complete* if it is noetherian and confluent. The interest in these systems arise from the fact that complete systems provide us with an effective procedure for deciding the word problem of the quotient monoid $\mathbb{M}/S$. The basic algorithm is to compute irreducible descendants. Assume for simplicity that the system S is length-reducing and no part of the input. If $\mathbb{M}$ is free or commutative, the following simple reduction algorithm computes of input $t \in \mathbb{M}$ in linear time $O(|t|)$ an irreducible element $t \overset{*}{\underset{S}{\Longrightarrow}} \hat{t} \in \mathrm{Irr}(S)$:

```
function reduce(t)
begin
v := 1;
while t ≠ 1 do
        let t = at' for some a ∈ Σ, t' ∈ M;
        v := va; t := t';
        if v = v'l for some (l,r) ∈ S then
        v := v'; t := rt
        endif
endwhile
return v
end
```

An efficient implementation of the algorithm above for traces could be based upon ideas of Hashiguchi and Yamada. In [18] the algorithm of Knuth, Morris, and Pratt is transformed for solving pattern matching problems on traces. This can be used to decide efficiently whether v is reducible.

The main problem however with this algorithm is that if IM is neither free nor commutative, then we do not have reduce(t) $\in$ Irr(S), in general. In [13, 11] we gave some more general decidable and sufficient conditions such that irreducible descendants can be computed following the algorithmic scheme above. However up to now no algorithm is known which satisfies the following two conditions for all finite length-reducing trace rewriting systems:

- it computes irreducible descendants
- it works in linear time on input of a trace t.

Problem 4 Let S be a finite length-reducing trace rewriting system. Does there exist some linear time algorithm for computing irreducible descendants?

4.1 A new linear time algorithm for some one-rule systems

In some restricted cases we know that Problem 4 has a positive answer. Let (Σ, D) be covered by a fixed set C of (maximal) cliques:

$$(\Sigma, D) = \bigcup_{A \in C} (A, A \times A)$$

and $\pi_A : IM(\Sigma, D) \longrightarrow A^*$ be the canonical projection. Then we can represent a trace t efficiently as a tuple of words $(\pi_A(t))_{A \in C}$. Using this data structure, very recently the following result has been shown [2].

Theorem 4.1 *Let $S = \{(l, r)\}$ be a length-reducing one-rule system such that l is connected, $\pi_A(l) \neq 1$ for all $A \in C$, and* alph(r) $\subseteq$ alph(l)*. Then there is some algorithm which computes on input t an irreducible descendant $\hat{t} \in$* Irr(S) *in $O(|t|)$ steps.*

Proof: The key observation to Theorem 4.1 is the following lemma:

Lemma 4.2 *Let $l \in IM$ be connected and $s_1, s_2 \subseteq t$ be subtraces of a trace t such that $s_1 = s_2 = l \in IM$. Write $t = u_i s_i v_i, i = 1, 2$ and assume that $\pi_{a,b}(u_1 s_1)$ is a proper prefix of $\pi_{a,b}(u_2 s_2)$ for some $(a, b) \in D$ where $a \in$* alph(l)*. Then $\pi_{a,b}(u_1 s_1)$ is a proper prefix of $\pi_{a,b}(u_2 s_2)$ for all $(a, b) \in D$ where $(\{a, b\} \cap$* alph(l)$) \neq \emptyset$.

Now, let $\{s_1, \ldots, s_n\}$ be the set of all subtraces of t which are equal (as trace) to l. Then the lemma above allows to define a linear ordering on this set which is based on the prefix relation. Thus, we may assume $s_1 < \cdots < s_n$. Working with the projection to cliques one can show that this chain in computable in $O(|t|)$ steps. The invariant is that we have $n = 0$ if and only if t is irreducible. For the reduction algorithm we may take any $s_i, 1 \leq i \leq n, t = us_iv = ulv$ and then replace t by $t' = urv$. The trace t' is computable in constant time (since S is not part of the input). Next we have to compute the new chain of subtraces equal to l. The crucial point is that there is a constant k such that

$s_1 < \cdots < s_{i-k}$ is the beginning part and $s_{i+k} < \cdots < s_u$ is the final part of the new chain. Moreover, there are at most k new subtraces between s_{i-k} and s_{i+k}. All these new subtraces are located with overlap to the position of the subtrace r in $t = urv$. The hypothesis $(\pi_A(l)) \neq 1$ for all $A \in C$ and $\mathrm{alph}(r) \subseteq \mathrm{alph}(l)$ is used to prove that the new subtraces can be computed in constant time. It follows that the new chain can be computed in constant time, too.

The method of computing irreducible normal forms given in the proof above applies in other cases. For example, a weaker condition than $\mathrm{alph}(r) \subseteq \mathrm{alph}(l)$ is enough, which then includes the free case, see [2]. However, we were not able to solve Problem 4 for multiple-rule systems, in general. So, for various special cases we found linear time algorithms and, interesting enough, in all these cases we were able to decide confluence, too. We have no idea, whether there is any intrinsic connection.

Problem 5 Let S be a finite length-reducing trace rewriting system such that there is some linear time algorithm for computing irreducible descendants. Does this imply that the confluence of S is decidable?

4.2 Confluence of one-rule systems

Most of the following results are from [28, 32]. We need the notion of overlap. Let x, t be traces, then t is called a (proper) *overlap* of x, if we have $x = pt = tq$ for some (non-empty) traces p, q. Recall the following well-known property of words (which is easily proved by induction on the length of t): For words $p, t, q \in \Sigma^*$ with $p \neq 1 \neq q$ and $pt = tq$ it holds $\mathrm{alph}(t) \subseteq \mathrm{alph}(p) = \mathrm{alph}(q)$.

Using projection to cliques this fact immediately extents to connected traces:

Lemma 4.3 ([28]) *Let $p, t, q \in \mathbb{M}$ be traces such that $p \neq 1, q \neq 1, pt = tq$ and pt is connected. Then we have $\mathrm{alph}(t) \subseteq \mathrm{alph}(p) = \mathrm{alph}(q)$.*

Proposition 4.4 ([28]) *Let x be a non-empty connected trace. Then there exist a maximal proper overlap t of x. Every other proper overlap of x is an overlap of t.*

Proof: Let r, s be overlaps of x. View first r, s as prefixes of x and define the prefix t_1 by the union of these subtraces r and s in the dependence graph. Let $(a, b) \in D$ and $\pi_{a,b} : \mathbb{M}(\Sigma, D) \longrightarrow \{a, b\}^*$ the canonical projection. Then we have $\pi_{a,b}(t_1) = \pi_{a,b}(r)$ if $|\pi_{a,b}(r)| \geq |\pi_{a,b}(s)|$ and $\pi_{a,b}(t) = \pi_{a,b}(s)$ otherwise. The latter condition clearly applies to the suffix-construction, too. Thus, let t_2 be the suffix of x defined by the graph theoretical union of the suffixes r and s. Then we obtain

$$\pi_{a,b}(t_1) = \pi_{a,b}(t_2) \text{ for all } (a, b) \in D$$

Hence, we have $t_1 = t_2$ and this is an overlap of x. Furthermore, the equations above and Lemma 4.3 yield that it is a proper overlap. □

The proposition above does not extend to the unconnected case. If $(a, b) \in I$ is a pair of independent letters, then the trace $ab = ba$ does not have any maximal proper overlap.
In the following we use the Parikh-mapping.

$$\psi : I\!M(\Sigma, D) \longrightarrow \mathbb{N}^{\Sigma}, t \mapsto (n_a)_{a \in \Sigma}$$

where $n_a = |t|_a$ for all $a \in \Sigma$ is the number of a occurring in t

Lemma 4.5 ([32]) *Let $S = \{(l, r)\}$ be a confluent one-rule trace rewriting system such that l is connected, and let s be a proper overlap of l such that $\psi(s) \leq \psi(r)$. Then s is an overlap of the right-hand side r.*

Proof: Let $l = ps = sq$. The pair (pr, rq) must be joinable by the system S. Let $(a, b) \in D$, then the pair $(\pi_{a,b}(pr), \pi_{a,b}(rq))$ must be joinable by the semi-Thue system $(\pi_{a,b}(l), \pi_{a,b}(r))$. Due to this fact and the Parikh condition, one is reduced to consider the case $I\!M = \{a, b\}^*, s = s_1 a s_2, r = s_1 b r_2$, and $a \neq b$. The result now follows by an argument on lexicographical orderings. It shows that the pair (pr, rq) is not joinable in this case. This yields contradiction to the confluence of S. Clearly, any derivation step by $S \subseteq \{a, b\}^* \times \{a, b\}^*$ increases the lexicographical order $<_{lex}$. Since $l\Sigma^* <_{lex} pr$, the rule (l, r) can never be applied totally on the left of any descendant of pr. Therefore $s_1 a$ is a prefix of all t_1 where $pr \underset{(l,r)}{\overset{*}{\Longrightarrow}} t_1$. On the other hand, $s_1 b$ is already a prefix of rq. Using reductions $rq \underset{(l,r)}{\overset{*}{\Longrightarrow}} t_2$, this prefix never becomes lexicographically smaller. Hence, the pair (pr, rq) is not joinable.
□

A very natural condition for trace rewriting is that every letter, which is independent of the left-hand side, has to commute with the right hand side. Indeed, it is exactly this condition which says that the rewriting is defined on the dependence graph. To be more clear, let l be a subtrace of a trace t. Then there is some factorization $x = plq$, which however is not unique. For example, if $p = p'u$ and $(u, l) \in I$, then the same subtrace $l \subseteq t$ yields the factorization $x = p'luq$, too. Applying the rule (l, r) depends therefore on the explicit factorization and not only on the subtrace. We may have $prq \underset{(l,r)}{\Longleftarrow} plq \underset{(l,r)}{\Longrightarrow} p'ruq$. The condition above implies $prq = p'ruq$ and the result is unique.
Formally, we write $I(l) = \{a \in \Sigma \mid (a, l) \in I\}$ and $\mathrm{Com}(r) = \{a \in \Sigma \mid ar = ra\}$. Of course, the condition $I(l) \subseteq \mathrm{Com}(r)$ is satisfied for words whenever $l \neq 1$. It is also verified for complete one-rule trace rewriting systems:

Lemma 4.6 *Let $S = \{(l, r)\}$ be a confluent one-rule trace rewriting system such that l is not a factor of r. Then it holds $I(l) \subseteq \mathrm{Com}(r)$.*

Proof: Let $a \in I(l)$. Then $al = la$ and (ar, ra) must be joinable. Since l is not a factor of r and $a \notin \mathrm{alph}(l)$, both traces are irreducible and hence they are equal.
□

In general, it is a difficult task so determine an appropriate set of traces which has to be tested for checking local confluence. Due to the undecidability result for confluence of noetherian systems, we cannot expect ot find a finite set. In [12, Thm.5.3.11] a combinatorial description of an infinite set of critical pairs is given. In the special case of one-rule systems, this theorem yields the following lemma:

Lemma 4.7 *Let $S = \{(l,r)\}$ be a one-rule trace rewriting system such that the left-hand side l is connected and $I(l) \subseteq \mathrm{Com}(r)$. Then the system S is locally confluent if and only if for all $p,s,q,y \in I\!M$ such that $l = ps = sq, (y,s) \in I$, and s is a proper non-empty overlap of l, the pair (pyr, ryq) is joinable by S.*

We are now prepared to state the main result on the confluence of one-rule systems.

Theorem 4.8 ([32]) *Let $S = \{(l,r)\}$ be a one rule trace rewriting system such that l is connected and $I(l) \subseteq \mathrm{Com}(r)$. Then the following statements are equivalent:*

i) S is confluent,
ii) S is strongly confluent,
iii) Either the maximal proper overlap of l is an overlap of r or there exist $p \neq 1, s, t \in I\!M$ and some $k \geq 2$ such that $l = p^k s, r = st, (l,t) \in I$ and every overlap of l is a proper overlap of s or of the form $p^i s$ for some $0 \leq i \leq k$.

Proof: The implication iii) $\Longrightarrow$ ii) is a nice exercise using Lemma 4.7. ii) $\Longrightarrow$ i) is trivial. i) $\Longrightarrow$ iii) this is technically the most difficult part. If involves results of C. Duboc, [17], on the existence of minimal conjugators and in an essential way Lemma 4.5. For details see [32]. □

If the left-hand side is empty we have:

Proposition 4.9 ([32]) *Let $S = \{(1,r)\}$ be a one-rule trace rewriting system where the left-hand side is empty and $r \neq 1$. Then the following assertions are equivalent:*

i) the system S is strongly confluent,
ii) for all pairs of independent letters $(a,b) \in I$, the letters a,b are in different connected components in $\mathrm{alph}(arb)$.

The following example is due to F. Otto. It shows that confluence does not imply strong confluence for one-rule systems, in general.

Example [32] Let $(\Sigma, D) = (a - c - b)$. Then the system $(1, bcab)$ is not strongly confluent since the trace $abcabb$ is connected. The system can be shown to be confluent.

Conjecture The notion of confluence and strong confluence coincides for one-rule systems if and only if $I\!M$ is a direct product of free monoids, i.e., if and only if D is transitive.

Problem 6 Consider the class of one-rule trace rewriting systems.

- Is confluence decidable?
- Is it decidable, if we have $I(l) \subseteq \mathrm{Com}(r)$?
- Is it decidable, if the left-hand sides is connected, but a factor of the right-hand side?
- Is it decidable, if the left-hand side is disconnected?
- Is it decidable, if the left-hand side is empty (and $(\Sigma, D) = (a - c - b)$)?

Problem 7 Let $S = \{(l, r)\}$ be a confluent one-rule trace rewriting system such that we have $I(l) \subseteq \mathrm{Com}(r)$. Is the system S strongly confluent?

5 Rewriting systems and Möbius functions

Let M be any monoid such that each $t \in M$ admits at most finitely many decompositions $t = u_1 \cdots u_n$ where $u_i \in M \setminus \{1\}$. The ring $\mathbf{Z}\langle\langle M \rangle\rangle$ of *formal power series* over M is the set of mappings from M to the integers $\mathbf{Z}$, where the addition and multiplication for $f, g : \Sigma \to \mathbf{Z}$ and $t \in M$ are defined as follows:

$$(f + g)(t) = f(t) + g(t)$$

$$(fg)(t) = \sum_{t_1 t_2 = t} f(t_1) g(t_2)$$

Power series are also written as formal sums

$$f = \sum_{t \in M} f(t) t$$

in accordance with the natural embedding $M \hookrightarrow \mathbf{Z}\langle\langle M \rangle\rangle$ which identifies the element $t \in M$ with the characteristic function $\chi_{\{t\}} : M \to \mathbf{Z}$.
The *support* of a power series $f \in \mathbf{Z}\langle\langle M \rangle\rangle$ is the set $\mathrm{supp}(f) = \{t \in M \mid f(t) \neq 0\}$. A power series with finite support is called a *polynomial*.
The *Möbius function* of the monoid M can be defined as the formal inverse in $\mathbf{Z}\langle\langle M \rangle\rangle$ of constant function with value 1, see [4, Lem. 2.2]

$$\mu_M = (\sum_{t \in M} t)^{-1}$$

The well-known result of P. Cartier-D. Foata [4, Thm. 1.2] says that the polynomial

$$\mu_M = \sum_{F \in \mathcal{F}} (-1)^{|F|} [F]$$

is the Möbius function of the monoid $IM = IM(\Sigma, D)$. Here $\mathcal{F}$ is the set of all steps and a *step* is a finite subset $F \subseteq \Sigma$ such that $(a, b) \in I$ for all $a, b \in F$, $a \neq b$. A step F yields a well-defined trace $[F]$ by taking the product over its elements: $[F] = \prod_{a \in F} a$. Since the multiplicative monoid of the natural numbers (without zero) is free commutative where the prime numbers are the generators, the result of Cartier and Foata generalizes the classical inversion formula for the Möbius function of natural numbers:

$$f(n) = \sum_{d|n} g(d) \Longleftrightarrow g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$$

Let $S \subseteq \Sigma^* \times \Sigma^*$ be a noetherian and confluent semi-Thue system and let $L = \{l \in \Sigma^* \mid (l, r) \in S\}$ be the set of left-hand sides. An *overlapping-chain* is a sequence $(w_1, \ldots, w_n)$, $n \geq 0$ of words such that $w_1 \in \Sigma$, $w_i \in \mathrm{Irr}(S)$ for $1 \leq i \leq n$ and $w_i w_{i+1} \in \Sigma^* L \setminus \Sigma^* L \Sigma^+$ for $1 \leq i < n$. This means w_1 is a letter, no factor of w_i is in L, a (unique) suffix of $w_i w_{i+1}$ is in L and no other factor of $w_i w_{i+1}$ belongs to L. In particular, $w_i \neq 1$ for all $1 \leq i \leq n$.
The set of overlapping-chains is denoted by $\mathcal{L}$. The mapping

$$\mathcal{L} \to \Sigma^*, (w_1, \ldots, w_n) \mapsto w_1 \ldots w_n$$

is injective. Thus, we may identify $\mathcal{L}$ with a subset of Σ^*.
In [12, Thm. 4.4.2] the following result is shown using a *bijective proof*:

Lemma 5.1 *Let*

$$\mu_S = \sum_{(w_1, \ldots, w_n) \in \mathcal{L}} (-1)^n w_1 \cdots w_n$$
$$\zeta_S = \sum_{w \in R} w$$

Then the power series μ_S, $\zeta_S \in \mathbf{Z}\langle\langle \Sigma^* \rangle\rangle$ are formal inverses of each other.

Example Let $I \subseteq \Sigma \times \Sigma$ be an independence relation and $\leq$ be a partial ordering of Σ^* such that $(I \cap \leq)$ is transitive. Then the system $S = \{(ab, ba) \mid (a, b) \in (I \cap \leq)\}$ is complete, [24]. There is a one-to-one correspondence between overlapping chains and steps. Indeed, if $(w_1, \ldots, w_n) \in \mathcal{L}$, then $w_i \in \Sigma, (w_i, w_j) \in I$ for all $i \neq j$ and $w_i \leq w_j$ for $i \leq j$. Conversely, if $F \in \mathcal{F}$ is a step, then we can write $F = \{w_1, \ldots, w_n\}$ such that $w_1 < \cdots < w_n$ and we have $(w_1, \ldots, w_n) \in \mathcal{L}$. In this case the formula of Cartier anf Foata is an immediate consequence.

Let $\mu_M \in \mathbf{Z}\langle\langle M \rangle\rangle$ be the Möbius function of a monoid M, which is a quotient of Σ^*. A formal power series $\mu \in \mathbf{Z}\langle\langle \Sigma^* \rangle\rangle$ is called an *unambiguous lifting* of μ_M, if first, the support of μ maps bijectively onto the support of μ_M, and if second, $\mu^{-1} \in \mathbf{Z}\langle\langle \Sigma^* \rangle\rangle$ is the characteristic function over a cross section of M in Σ^*.

Theorem 5.2 ([10]) *Let $IM = IM(\Sigma, D)$ and $I = \Sigma \times \Sigma$ the independence relation. Then the following assertions are equivalent:*

i) There is an unambiguous lifting of μ_{IM} in $\mathbf{Z}\langle\langle \Sigma^* \rangle\rangle$.
ii) There is a transitive orientation of I, i.e., there is an ordering $\leq$ such that $I \cap \leq$ is transitive.
iii) There is a finite complete semi-Thue system $S \subseteq \Sigma^* \times \Sigma^*$ such that $\Sigma^*/S = IM$.

Proof: The equivalence of ii) and iii) is in [24, 27]. The implication i) $\Longrightarrow$ ii) is done by a direct computation on traces up to length three and the (most difficult) final implication ii) $\Longrightarrow$ i) is immediate from 5.1. □

For a homological interpretation of Theorem 5.2 the reader is referred to [20]. Here we continue with a complete system which always exist, but which is infinite if the underlying ordering does not define a transitive orientation. Let $\leq$ be any partial ordering of Σ such that all independent letters are comparable. Then every trace $t \in IM$ has a unique lexicographical normal form $\hat{t} \in \Sigma^*$. The set of all lexicographical normal forms is the set of irreducible words of the following complete semi-Thue system.

$$S = \{(bua, abu) \mid a \leq b, (bu, a) \in I, a, b \in \Sigma, u \in \Sigma^*\}$$

Moreover, we may assume that for all rules above the words bu and ua are in lexicographical normal form.

Problem 8 Is it possible to compute the formal inverse of the characteristic function of the lexicographical normal forms by using overlapping-chains such that the formula of Cartier-Foata becomes a corollary.

A positive solution of the problem above would be another hint for a close connection between the combinatorics of Möbius functions and complete rewriting systems. This might be of particular interest with respect to some homological interpretation mentioned above, see also [30].

6 Semi commutations and Möbius functions

A *semi dependence* relation ($over\,\Sigma$) is a reflexive relation $\mathrm{SD} \subseteq \Sigma \times \Sigma$, the pair (Σ, SD) is called a *semi dependence alphabet.* A semi dependence yields a semi commutation by the following set of rules: $S = \{ab \Rightarrow ba \mid (a,b) \notin \mathrm{SD}, a, b \in \Sigma\}$. The definition of a semi traces induced by a word $u \in \Sigma^*$ is the set of words derivable from u by application of semi commutation rules:

$$[u\rangle = \{v \in \Sigma^* \mid u \overset{*}{\underset{SC}{\Longrightarrow}} v\}$$

The theory of semi commutations and semi traces is of growing interest, see e.g. [6, 7, 8, 5, 15, 21, 26, 29, 31].
A basic question is to characterize when the composition of two semi commutations is again a semi commutation. The answer is given by a graph theoretical characterization of Y. Roos and P.A. Wacrenier:

Theorem 6.1 ([29]) *Let* $\mathrm{SD}, \mathrm{SE} \subseteq \Sigma \times \Sigma$ *be semi dependence relations with associated semi commutations* S *and* T*. Then the composition* $\overset{*}{\underset{S}{\Longrightarrow}} \circ \overset{*}{\underset{T}{\Longrightarrow}}$ *is defined by some semi commutation if and only if there is no cycle of pairwise different letters*

$$\{(x_0, x_1), (x_1, x_2), \ldots, (x_i, x_{i+1}), \ldots (x_n, x_0),\}$$

such that every edge is in $\mathrm{SD} \cup \mathrm{SE}$ *and, in addition, we have*

$$\begin{aligned}(x_0, x_n) &\in \mathrm{SE} \setminus \mathrm{SD} \\ (x_i, x_{i+1}) &\in \mathrm{SD} \setminus SE \\ \{x_0, \dots, x_i\} \times \{x_{i+1}, \dots, x_n\} &\subseteq \Sigma \times \Sigma \setminus (\mathrm{SD} \cup \mathrm{SE})\end{aligned}$$

It turns out that the theorem above is closely related to the confluence of semi commutation systems. Indeed, it is an easy exercise to see that a semi commutation system $S = \{(ab, ba) \mid (a, b) \notin \mathrm{SD}\}$ is confluent if and only if the composition $\overset{*}{\underset{S}{\Longrightarrow}} \circ \overset{*}{\underset{S^{-1}}{\Longrightarrow}}$ is defined by some semi commutation.
In this case we have $(\overset{*}{\underset{S}{\Longrightarrow}} \circ \overset{*}{\underset{S}{\Longleftarrow}}) = (\overset{*}{\underset{S}{\Longrightarrow}} \circ \overset{*}{\underset{S^{-1}}{\Longrightarrow}}) = \overset{*}{\underset{S}{\Longleftrightarrow}}$. Therefore Theorem 6.1 generalizes results by Diekert et al. [15] and the complexity results shown there imply:

Corollary 6.2 *Both problems are co-NP complete:*
Is the composition of two semi commutations a semi commutation again?
Is a given semi commutation confluent?

In the remaining part of the paper we relate the confluence of semi commutation systems to unambiguous liftings of Möbius functions in a relative situation. Let $D \subseteq D' \subseteq \Sigma \times \Sigma$ be an inclusion of (symmetric) dependence relations, $I\!M = I\!M(\Sigma, D)$ and $I\!M' = I\!M(\Sigma, D')$. The canonical projection $p : I\!M \longrightarrow I\!M'$ extends uniquely to a surjective ring homomorphism

$$p : \mathbf{Z}\langle\langle I\!M \rangle\rangle \to \mathbf{Z}\langle\langle I\!M' \rangle\rangle, \ \sum_{t \in M} f(t)t \mapsto \sum_{t' \in M'} \Big(\sum_{p(t) = t'} f(t) \Big) t'$$

The notion of unambiguous lifting is now defined with respect to p as above. Let $\mu_{I\!M'} \in \mathbf{Z}\langle\langle I\!M' \rangle\rangle$ be the Möbius function of $I\!M'$. A formal power series $\mu \in \mathbf{Z}\langle\langle I\!M \rangle\rangle$ is called an *unambiguous lifting* if the following two conditions are satisfied:

- The function μ is the formal inverse of a characteristic series over a (rational) cross section of $I\!M'$ in $I\!M$.
- The support of μ maps bijectively onto the support of $\mu_{I\!M'}$.

Theorem 6.3 ([14]) *There is a canonical one-to-one correspondence between unambiguous liftings of Möbius functions and confluent semi commutations.*

The proof of the Theorem 6.3 is very long and technically involved. It is based on a combinatorial analysis and some tedious computations. All details can be found in [14]. Let us sketch some basic ideas. We define two mappings: A mapping from semi commutations to Möbius functions and vice versa.
Let $\mathrm{SD} \subseteq \Sigma \times \Sigma$ be any semi dependence relation, such that the semi commutation system $S = \{(ab, ba) \mid (a, b) \notin \mathrm{SD}\}$ is confluent. Define the monoids $I\!M = I\!M(\Sigma, \mathrm{SD} \cup \mathrm{SD}^{-1})$ and $I\!M' = I\!M(\Sigma, \mathrm{SD} \cap \mathrm{SD}^{-1})$. Then, of course,

$$\zeta(S) = \sum_{t \in \mathrm{Irr}(S)} t$$

is a rational cross section of M' in M. The mapping from semi commutations to Möbius functions is defined by $S \mapsto \mu(S) = \zeta(S)^{-1}$. One has to show that the support of $\mu(S)$ maps bijectively onto the support of $\mu_{M'}$. To see this consider those traces $s \in IM$ which can be written as a product $s = a_1 \cdots a_n$ where $a_i \in \Sigma$ and $(a_i, a_j) \notin \mathrm{SD}$ whenever $i < j$. Following the terminology of Diekert et al. such traces are called *soft*, since the semi trace $[a_1 \cdots a_n\rangle$ contains soft arcs only, see [15]. Since SD is confluent, there is a bijection between soft traces and steps of IM'. A lengthy computation shows the formula:

$$\zeta(S)^{-1} = \sum_{s \text{ is soft}} (-1)^{|s|} s$$

The mapping in the other direction is obtained as follows: If $\mu \in \mathbf{Z}\langle\langle IM \rangle\rangle$ is an unambiguous lifting of $\mu_{IM'}$ then one defines

$$\mu \mapsto S(\mu) = \{(ab, ba) \mid \mu(ab) = 1\}$$

One can show that $S(\mu)$ defines a confluent semi commutation. The proof depends heavily on the graph-theoretical characterization for confluence given in [15], see also Thm. 6.1 above.
The final (and most difficult) part is to show that we have $\mu(S(\mu)) = \mu$.

Remark 6.4 Let $\mu \in \mathbf{Z}\langle\langle IM \rangle\rangle$ be an unambiguous lifting of $\mu_{IM'}$ and $S(\mu) = \{(ab, ba) \mid \mu(ab) = 1\}$ A direct verification of the equality

$$\mu^{-1} = \sum_{t \in \mathrm{Irr}(S(\mu))} t$$

would probably lead to a new proof of the graph-theoretical characterization for confluence.

Problem 9 Is it possible to extend the homological result of Y. Kobayashi [20] to the relative situation $D \subsetneq D' \subsetneq \Sigma \times \Sigma$?

Acknowledgement I would like to thank Friedrich Otto for helpful comments on a draft of this paper and Heike Photien for her great help in producing the LaTeXversion of my handwritten manuscript.