

EQUIVALENCES AND TRANSFORMATIONS OF REGULAR SYSTEMS—APPLICATIONS TO RECURSIVE PROGRAM SCHEMES AND GRAMMARS*

Bruno COURCELLE

Department of Mathematics and Computer Science (Associated CNRS Laboratory), Bordeaux-1 University, 33405 Talence, France

Communicated by M. Nivat

Received January 1985

Revised September 1985

Abstract. This work presents a unified theory of recursive program schemes, context-free grammars, grammars on arbitrary algebraic structures and, in fact, recursive definitions of all kind by means of regular systems. The equivalences of regular systems associated with either all their solutions or their least solutions (in all domains of appropriate type satisfying a set of algebraic laws expressed by equations) are systematically investigated and characterized (in some cases) in terms of system transformations by folding, unfolding and rewriting according to the equational algebraic laws. Grammars are better characterized in terms of polynomial systems which are regular systems involving the operation of set union, and the same questions are raised for them. We also examine conditions insuring the uniqueness of the solution of a regular or of a polynomial system. This theory applies to grammars of many kinds which generate trees, graphs, etc. We formulate some classical transformations of context-free grammars in terms of correct transformations which only use folding, unfolding and algebraic laws and we immediately obtain their correctness.

Contents

0. Introduction	3
0.1. All solutions of a regular system	3
0.2. Polynomial systems	4
0.3. Applications to context-free grammars	5
1. Preliminaries	5
1.1. Terms, trees, magmas	6
1.2. Substitutions	7
1.3. Rewriting systems	7
1.4. Equational classes of F -magmas	9
1.5. ω -complete F -magmas	9
1.6. Equational classes of ω -complete F -magmas	10
1.7. Commutation lemmas for rewriting relations	11

* This work was presented in part to the 26th Symposium on Foundations of Computer Science, Portland, OR, U.S.A., October 1985 and to the 26th Semester of the Stefan Banach International Mathematical Center, Warsaw, Poland, 1985.

2. Regular systems	12
2.1. Definition of regular systems	12
2.2. Solutions	13
2.3. Equivalences of regular systems	13
2.4. Remarks on terminology and notations	14
2.5. Renamings	14
2.6. Singular unknowns	15
2.7. Recursive applicative program schemes as regular systems	15
2.8. Context-free grammars as regular systems	17
2.9. Definitions: transformations of regular systems	17
3. Comparing regular systems with respect to their full sets of solutions	18
4. Transformations by folding, unfolding and rewriting	21
5. Comparing regular systems with respect to their least solutions	29
6. System transformations and \sim -equivalence	35
7. Subsystems and auxiliary unknowns	41
8. Regular systems having a unique solution	46
9. Recursive applicative program schemes as regular systems	49
9.1. Sorts and signatures	49
9.2. Derived signatures	50
9.3. beta and its inverse	51
9.4. Properties of comp_k^n	51
9.5. Recursive applicative program schemes	55
9.5.1. Definitions	55
9.5.2. Construction	55
10. Powerset magmas	56
11. Polynomial regular systems	62
11.1. Definition of polynomial systems	62
11.2. Polynomial systems of special types	63
11.3. Equivalences and preorders on $+$ -regular systems	63
11.4. Examples	64
11.4.1. Finite-state automata	64
11.4.2. Context-free grammars	65
12. Polynomial systems and their sets of solutions	65
13. Polynomial systems and their least solutions	78
14. Transformations of polynomial systems and \sim -equivalence	82
15. Polynomial systems having a unique solution	89
16. Grammars on arbitrary magmas	95
16.1. Derivation trees	96
16.2. Context-free tree grammars: the IO-case	98
16.3. Context-free tree grammars: the OI-case	99
16.4. Derivation sequences	100
16.5. Derivation sequences in $M(F, u)/\leftrightarrow_k^*$	101
16.6. Iterative algorithms	104
16.7. The occurrences of variables in IO-context-free tree languages	106
16.8. The noncircularity test for attribute grammars	106
17. Applications to context-free grammars	108
17.1. Deletion of nonterminals which define no word	108
17.2. Deletion of useless nonterminals	109
17.3. Elimination of ε -rules	109
17.4. Elimination of chain-rules	111
17.5. Chomsky normal form	111
17.6. Invertible grammars	111
17.7. Greibach normal form	112
18. More general grammars	113
Appendix A. Coherent and simplifiable congruences	114
References	120

*A lot of good music remains
to be written in C major.*

A. Schoenberg

0. Introduction

Recursive program schemes, context-free grammars, context-free tree-grammars, graph grammars of certain types, and more generally all forms of mutually recursive definitions can be encompassed within the concept of a *regular system*.

Such systems have been introduced under various names in [30, 35, 36, 37, 39, 48, 54, 83]. They provide a common framework for studying recursive program schemes, either applicative [25, 29, 31, 32, 55] or imperative [35, 46] and for context-free grammars generating words, trees, arbitrary objects (along the lines of [73]). But we felt that many fundamental questions concerning them had not been enough investigated.

0.1. All solutions of a regular system

One of the central ideas of this work is the investigation of the set of all solutions of a regular system as well as of its least solution. Least solutions (as opposed to sets of solutions) have been investigated quite in depth for the following reasons. When one writes a context-free grammar, one is interested in the tuple of languages *generated* by the nonterminals (by means of rewritings) which coincides with the *least solution* of the grammar considered as a regular system (see [51, 78] and Section 2.8). This fact applies to many types of grammars (generating trees, graphs, etc.) and can be used as a foundation stone for the general concept of a grammar over an arbitrary F -magma (i.e., F -algebra), as shown in [73] (see Definition 16.1 below). Another reason is that the function *computed* by a recursive definition (by means of some precisely defined operational semantics) is the least solution (over some well-chosen domain) of the corresponding equation (see [4, 81, 82]). Whence the importance of least solutions for the semantics of programming languages formalized in the framework of denotational semantics [80] or that of recursive program schemes ([46, 55, 81], among many others).

This leads us to define two equivalence relations on the set of regular systems having the same set of unknowns. $S \approx S'$ iff S and S' have the same set of solutions in every domain and $S \sim S'$ iff S and S' have the same least solution in every ω -complete domain. In fact we shall refine these equivalences into $\approx_{\mathcal{E}}$ (and $\sim_{\mathcal{E}}$) by letting \mathcal{E} be a set of equations corresponding to the algebraic laws assumed in the domains. We shall try to get syntactical characterizations of these equivalence relations. In the presence of equations, these equivalences become undecidable as one can guess immediately. But as in the case of program schemes, we shall be more interested by *transformation rules* for regular systems than by decidability results (which may be of exponential complexity when they exist).

The reader may question the introduction of the equivalence relation $\approx_{\mathcal{E}}$ since, at first sight, only $\sim_{\mathcal{E}}$ seems to be of interest in computer science. The motivation comes from the consideration of *program transformations*. When programs are

expressed as systems of recursive equations, transformations by *unfolding*, *folding* and *rewriting according to the algebraic laws* (expressed as equations) are very natural and useful. This applies to context-free grammars as well, although nearly nothing appears in print on this subject. Unfortunately, these transformations are not always correct. To be more precise, if S is transformed into S' in such a way, there are three possibilities:

- (i) S' and S have the same solutions, whence they have the same least solution,
 - (ii) every solution of S is a solution of S' (but not conversely), but S and S' have the same least solution,
 - (iii) the same holds but the least solution of S' is strictly smaller than that of S .
- Few works have been devoted to the correctness issue, i.e., to the problem of drawing the border between cases (i)–(ii) and case (iii) [25, 63, 64].

On the other hand, when manipulating recursive program schemes and context-free grammars, one frequently uses transformations of type (i) above (see for instance [8, Theorem 1.7]), but their theory has never been made (to the author's knowledge). We shall provide a very simple syntactical condition ensuring the preservation of all solutions (see Section 4), which is much simpler than the ones of [25, 63, 64] ensuring the preservation of the least solution. We shall say that a transformation rule is $\approx_{\mathcal{E}}$ -correct if it preserves the set of all solutions, and that it is $\sim_{\mathcal{E}}$ -correct if it preserves the least solution of the system to which it applies, whenever the domain satisfies the set of equations \mathcal{E} . We shall introduce a collection of transformation rules and determine for each whether it is $\approx_{\mathcal{E}}$ -correct or $\sim_{\mathcal{E}}$ -correct.

A natural question is then the *completeness* of a set \mathcal{T} of transformation rules known to be η -correct for some equivalence η (i.e., is it true that, for every S, S' such that $S \eta S'$, the system S can be transformed into S' by a finite sequence of transformations in \mathcal{T} ?).

We shall obtain very few completeness results and mostly when $\mathcal{E} = \emptyset$.

0.2. Polynomial systems

By a polynomial system we mean a regular system written with a set of base functions containing the binary symbol $+$. These systems are always solved in powerset algebras. The equation systems investigated in [73] are of this type.

They provide a convenient way to investigate context-free grammars. Many basic results concerning context-free grammars can be established for polynomial systems, and they are immediately applicable to grammars generating trees, graphs, whatever you want, provided the appropriate algebraic structure is given. We shall provide examples in Section 16.

Since $+$ is interpreted in a fixed way, some equations concerning it and the other functions are always satisfied: associativity, idempotence, distributivity, etc. Let \mathcal{D} be this set. Hence, a polynomial system solved in $\mathcal{P}(\mathbf{M})$ where \mathbf{M} satisfies \mathcal{E} can be considered as a regular system solved in some \mathbf{M}' satisfying $\mathcal{E} \cup \mathcal{D}$ (provided \mathcal{E} satisfies some linearity conditions). We shall see that, in many cases, the theory of

polynomial systems modulo \mathcal{E} reduces to the theory of regular systems modulo $\mathcal{D} \cup \mathcal{E}$. But some (probably difficult) questions remain open. Finally, we shall provide a uniform presentation for several classical ‘iterative’ algorithms: computation of the set of nonterminals of a context-free grammar which generate no word, of those which generate the empty word, of those of an IO-context-free tree grammar which generate no tree. To this list we also add the noncircularity test for attribute grammars since we can consider an attribute grammar as a graph grammar which generates the usual dependency graphs.

0.3. Applications to context-free grammars

Most books on context-free grammars establish the theorem of Ginsburg and Rice [51] saying that the language generated by a nonterminal is equal to the corresponding component of the least solution (in the set of languages) of the (polynomial) system associated with the grammar. But they rarely use it afterwards. Most proofs use inductions on the length of derivations. Actually, they *repeat* in a more or less hidden way the proof of the theorem of Ginsburg and Rice.

Hence, we prefer to base proofs (for instance the correctness proof of the classical transformation which eliminates ε -rules in context free grammars) on the fixed-point characterization of context-free languages rather than on the classical characterization based on derivation sequences. This approach tends to unify manipulations of programs and manipulations of grammars.

In particular, we formulate the classical transformations of reduction, elimination of chain- and ε -rules, Chomsky-normal form in terms of our basic, correct transformations of polynomial systems. This establishes also their correctness.

We also consider the unicity of solutions of polynomial systems. As an application of general results we give necessary and sufficient conditions for the unicity of the solution in $\mathcal{P}(X^+)$ or $\mathcal{P}(X^*)$ of a context-free grammar (considered as a polynomial system).

1. Preliminaries

We review the basic concepts, fix our notations and state a few lemmas. We first precise a few mathematical notations.

We denote by \mathbb{N} the set of nonnegative integers and by \mathbb{N}_+ the set of positive ones. We denote by $[n]$ the interval $\{1, 2, 3, \dots, n\}$ for $n \geq 0$ (with $[0] = \emptyset$).

For sets A and B we denote by $A - B$ the set $\{a \in A \mid a \notin B\}$.

The *domain* of a partial mapping $f: A \rightarrow B$ is denoted by $\mathbf{Dom}(f)$. The restriction of f to a subset A' of A is denoted by $f \upharpoonright A'$.

If f is a mapping $B^n \rightarrow C$ and g_1, \dots, g_n are mappings $A^m \rightarrow B$, we denote by $f \circ (g_1, \dots, g_n)$ the mapping $h: A^m \rightarrow C$ such that $h(a_1, \dots, a_m) = f(g_1(a_1, \dots, a_m), \dots, g_n(a_1, \dots, a_m))$.

The set of total mappings $A \rightarrow B$ is denoted by $[A \rightarrow B]$. The cardinality of a set A is denoted by $\text{Card}(A)$.

The powerset of A is denoted by $\mathcal{P}(A)$.

1.1. Terms, trees, magmas

The notations are mostly those of [26, 28]. As in many previous works we shall use the term F -magma for what is usually called an F -algebra.

We quickly list the corresponding notations:

- F denotes a ranked alphabet with rank function $\rho: F \rightarrow \mathbb{N}$,
- $F_i = \{f \in F \mid \rho(f) = i\}$; an element of F_0 is called a *constant*,
- $X = \{x_1, x_2, \dots, x_n, \dots\}$ is a set of variables (of arity 0) and $X_k = \{x_1, \dots, x_k\}$; alternative sets of variables will be U, Y, U_k, Y_k ,
- $\mathbf{M} = \langle M, \langle f_{\mathbf{M}} \rangle_{f \in F} \rangle$ denotes an F -magma with *domain* M , (the reader should note the typographical distinction between an F -magma \mathbf{M} and its domain M ; this distinction will be kept in all magmas to be defined below),
- $\mathbf{M}(F, X)$ denotes the free F -magma generated by X , with domain $M(F, X)$, considered as a set of terms (and sometimes of trees),
- $t_{\mathbf{M}}: M^k \rightarrow M$ is the mapping defined by t if t is a term defined by the context as an element of $M(F, X_k)$ (some elements of X_k may have no occurrence in t),
- \mathbf{M}/\sim denotes the quotient F -magma when \sim is a congruence on \mathbf{M} .

The general notation for terms is with prefixed function symbols, commas and parentheses. The parentheses surrounding the argument are omitted in examples in the case of a unary function symbol. Some binary symbols denoting associative functions will be infix. So a typical example is $x + f(x, gy) + h(x, ggx, y)$ where $\rho(h) = 3$, $\rho(f) = \rho(+)=2$, $\rho(g)=1$.

The set of *subterms* of a term t in $M(F, X)$ is defined as follows:

$$\text{Subterm}(t) = \begin{cases} \{t\} & \text{if } t \in F_0 \cup X, \\ \{t\} \cup \text{Subterm}(t_1) \cup \dots \cup \text{Subterm}(t_k) & \text{if } t = f(t_1, \dots, t_k). \end{cases}$$

A subterm t' of t is *proper* if $t' \neq t$.

The *length* of a term t in $M(F, X)$ is the integer $|t|$ equal to the number of occurrences of symbols of $F \cup X$ in the linear writing of t or the number of nodes of the tree representing t . If $Y \subseteq F \cup X$, then $|t|_Y$ denotes the number of occurrences of symbols from Y in t .

Let $Z \subseteq X$. The set of variables from Z occurring in t is denoted by $\text{Var}_Z(t)$. The notation $\text{Var}(t)$ is used when $Z = X$ or is known from the context.

A term t is *Z-linear* if every x in Z has at most one occurrence in t . As above, the prefix Z is omitted if no ambiguity can arise.

If $G \subseteq F$ and $T \subseteq M(F, X)$, we denote by $G(T)$ the set of terms of the form $f(t_1, \dots, t_k)$ for $k \geq 0$, $f \in G \cap F_k$, $t_1, \dots, t_k \in T$.

1.2. Substitutions

Let $t, t_1, \dots, t_k \in M(F, X)$. We denote by $t[t_1/x_1, \dots, t_k/x_k]$ or by $t[t_i/x_i; 1 \leq i \leq k]$, or by $t[t_1, \dots, t_k]$ if the context clearly defines the sequence x_1, \dots, x_k , the result of the simultaneous substitution of t_i for all occurrences of x_i in t .

There are two extensions of this operation to sets of trees, whose algebraic properties have been investigated in [45]. The first one is

$$A \underset{IO}{[} A_1/x_1, \dots, A_k/x_k] = \{t[t_1/x_1, \dots, t_k/x_k] \mid t \in A, t_1 \in A_1, \dots, t_k \in A_k\},$$

where $A, A_1, \dots, A_k \subseteq M(F, X)$.

The second one is defined in several steps:

$$A \underset{OI}{[} A_1/x_1, \dots, A_k/x_k] = \bigcup_{OI} \{t \underset{OI}{[} A_1/x_1, \dots, A_k/x_k] \mid t \in A\},$$

$$t \underset{OI}{[} A_1/x_1, \dots, A_k/x_k] = \begin{cases} A_i & \text{if } t = x_i, \\ \{t\} & \text{if } t \in F_0 \cup (X - X_k), \\ \{f(u_1, \dots, u_n) \mid u_i \in t_i \underset{OI}{[} A_1/x_1, \dots, A_k/x_k], 1 \leq i \leq n\} & \\ & \text{if } t = f(t_1, \dots, t_n). \end{cases}$$

One has

$$A \underset{IO}{[} A_1/x_1, \dots, A_k/x_k] \subseteq A \underset{OI}{[} A_1/x_1, \dots, A_k/x_k]$$

and the inclusion may be strict.

Let Y be a set of variables. We denote by $\text{Ctx}(F, Y)$ the set of terms in $M(F, Y \cup \{x\})$ having exactly one occurrence of x . The variable x is any variable not in $F \cup Y$. An element c of $\text{Ctx}(F, Y)$ is called a *context* and, if $t \in M(F, Y)$, then $c[t]$ denotes the term $c[t/x]$. It is clear that the precise variable x used in the definition of $\text{Ctx}(F, Y)$ is irrelevant.

In a few cases we shall also use substitutions of the form $t[t_1/y_1, \dots, t_k/y_k]$ where y_1, \dots, y_k are pairwise distinct elements of $X \cup F_0$, i.e., we shall substitute terms for constants and not only for variables.

Finally, the word ‘substitution’ also refers to the mapping $\theta: M(F, X_k) \rightarrow M(F, Y)$ associated with a list t_1, \dots, t_k of elements of $M(F, Y)$ by $\theta(t) = t[t_1/x_1, \dots, t_k/x_k]$.

1.3. Rewriting systems

The basic results can be found in [59, 61].

A *rewriting system* is a subset R of $M(F, X) \times M(F, X)$. With R is associated a *rewriting relation* \rightarrow_R on $M(F, Y)$ (where Y is any set of variables, not necessarily disjoint from X) defined by $t \rightarrow_R t'$ if and only if

$$t = c[r[t_1/x_1, \dots, t_k/x_k]],$$

$$t' = c[r'[t_1/x_1, \dots, t_k/x_k]],$$

for some (r, r') in R , some t_1, \dots, t_k in $M(F, Y)$, some c in $\text{Ctx}(F, Y)$ (with $r, r' \in M(F, X_k)$).

We shall say that R is *ground* if R has no variables, i.e., if $k=0$ or if R has variables that will not be subject to substitution. We shall frequently use U to denote such a set of variables and we shall define such a ground rewriting system R as a subset of $M(F \cup U) \times M(F \cup U)$. (Here $M(F \cup U)$ denotes the same set as $M(F, U)$ but with U merged into the set of function symbols F and not distinguished as a set of variables.)

A term t is *R -irreducible* if $t \rightarrow_R t'$ for no t' . If $t \rightarrow_R^* t'$ and t' is R -irreducible, then t' is a *R -normal form* of t .

The property of *confluence* insures that every term t has *at most one* R -normal form: R is *confluent* if, for all t, t_1, t_2 such that $t \rightarrow_R^* t_1$ and $t \rightarrow_R^* t_2$, there exists a t_3 such that $t_1 \rightarrow_R^* t_3$ and $t_2 \rightarrow_R^* t_3$. This property can be established by means of the concept of *critical pair* (it is a bit technical and we shall not recall it; see [59]).

We now recall some definitions concerning termination, which allow to prove that a term has *at least one* normal form.

Let \leq be a partial order on $M(F, Y)$. A rewriting system R is *compatible with \leq* (or is *\leq -compatible*) if, for all t, t' in $M(F, Y)$, $t \rightarrow_R t'$ implies $t' < t$ (where $<$ denotes the strict partial order associated with \leq). If $<$ is well-founded, i.e., if there is no infinite decreasing sequence $t_1 > t_2 > \dots > t_n > \dots$, then \rightarrow_R is Noetherian (i.e., has no infinite chains of rewritings). If R is Noetherian, then every term has *at least one* R -normal form. If R is Noetherian and confluent, then every term t has a *unique* R -normal form denoted by $\text{nf}_R(t)$.

A rewriting system R is *right-irreducible* if, for every pair (s, t) in R , t is R -irreducible. It is *left-irreducible* if, for every pair (s, t) in R , s is irreducible w.r.t. $R - \{(s, t)\}$. It is *proper* if it is both left- and right-irreducible. Let us mention that a ground rewriting system is left-irreducible iff it has no critical pair. From the proofs of [59, Lemmas 2.5 and 3.1] one can easily extract the following lemma.

1.1. Lemma. *Let R be a rewriting system which is ground and left-irreducible. For all t, t_1, t_2 such that $t \rightarrow_R t_1$ and $t \rightarrow_R t_2$, if $t_1 \neq t_2$, there exists t_3 such that $t_1 \rightarrow_R t_3$ and $t_2 \rightarrow_R t_3$. Hence, R is confluent.*

Métivier has proved the following results [72, Theorem 7 and Corollary 9].

1.2. Proposition. (1) *Every confluent and Noetherian rewriting system R can be transformed into a proper confluent and Noetherian system R' such that $\text{nf}_{R'} = \text{nf}_R$ (whence R and R' generate the same congruence).*

(2) *There exists at most one rewriting system which is proper, confluent, compatible with some fixed well-founded ordering and which generates some given congruence.*

An obvious corollary of Lemma 1.1 and Proposition 1.2(2) is the following.

1.3. Corollary. *There exists at most one ground rewriting system which is proper, is compatible with some fixed well-founded ordering and which generates some given congruence.*

1.4. Equational classes of F -magmas

Let \mathcal{C} be an arbitrary class of F -magmas. We write $\mathcal{C} \models t = t'$ for t, t' in $M(F, X_k)$ if $t_{\mathbf{M}} = t'_{\mathbf{M}}$ for all \mathbf{M} in \mathcal{C} . Given a subset \mathcal{E} of $M(F, X) \times M(F, X)$, we denote by $\mathcal{V}(\mathcal{E})$ the *variety* defined by \mathcal{E} , i.e., the class of all F -magmas \mathbf{M} such that $t_{\mathbf{M}} = t'_{\mathbf{M}}$ for all (t, t') in \mathcal{E} , (and we denote by $\mathcal{V} = \mathcal{V}(\emptyset)$ the class of all F -magmas). We write $\mathcal{E} \models t = t'$ for $\mathcal{V}(\mathcal{E}) \models t = t'$. We denote by $\leftrightarrow_{\mathcal{E}}$ the rewriting relation \rightarrow_R associated with $R = \{(t, t'), (t', t) \mid t = t' \text{ is an equation of } \mathcal{E}\}$ (the double arrow is used to emphasize the symmetry of this relation).

The following basic result is a syntactical characterization of the semantical equivalence associated with \mathcal{E} .

1.4. Lemma (Birkhoff [9]). $\mathcal{E} \models t = t'$ iff $t \leftrightarrow_{\mathcal{E}}^* t'$.

1.5. ω -complete F -magmas

An ω -complete F -magma is an object $\mathbf{M} = \langle M, \perp_{\mathbf{M}}, \leq_{\mathbf{M}}, \langle f_{\mathbf{M}} \rangle_{f \in F} \rangle$, where $\leq_{\mathbf{M}}$ is a partial order on M with least element $\perp_{\mathbf{M}}$, which is ω -complete (the least upper bound of a countable directed set D exists and is denoted by $\text{Sup}(D)$) and such that, for all f in F , $f_{\mathbf{M}}$ belongs to $(M^{\omega(f)} \rightarrow M)$ (i.e., is monotone and ω -continuous).

There is a free ω -complete F -magma generated by a set X , denoted by $\mathbf{M}_{\Omega}^{\infty}(F, X)$ whose domain consists of infinite trees (see [25, 26, 54]).

We quickly recall one possible construction of $\mathbf{M}_{\Omega}^{\infty}(F, X)$. We denote by $\mathbf{M}_{\Omega}(F, X)$ the $F \cup \{\Omega\}$ -magma $\mathbf{M}(F \cup \{\Omega\}, X)$, where Ω is a new constant (the notation emphasizes its special role). An order on $M_{\Omega}(F, X)$ is defined by

$$t < t' \text{ iff } t' \in t \underset{\text{OI}}{[M_{\Omega}(F, X) / \Omega]}$$

(i.e., if t' is the result of the OI-substitution of terms for occurrences of Ω in t (different terms can be substituted for distinct occurrences of Ω)).

The set $M_{\Omega}^{\infty}(F, X)$ of infinite trees can be formally defined as the *ideal completion* of $\mathbf{M}_{\Omega}(F, X)$ w.r.t. $<$ (see [31, 32, 33, 56, 69, 84]). We shall only need the following facts:

- (1) $M_{\Omega}(F, X) \subset M_{\Omega}^{\infty}(F, X)$.
- (2) $\mathbf{M}_{\Omega}^{\infty}(F, X)$ is ω -complete w.r.t. $<$ and its least element is Ω .
- (3) Every element of $M_{\Omega}^{\infty}(F, X)$ is the least upper bound of an increasing sequence in $M_{\Omega}(F, X)$.
- (4) For every s in $M_{\Omega}(F, X)$, for every increasing sequence $(t_n)_{n \in \mathbb{N}}$ in $M_{\Omega}^{\infty}(F, X)$, $s < \text{Sup}(t_n)$ iff $s < t_n$ for some n .

The F -operations on $M_{\Omega}^{\infty}(F, X)$ are the extensions by continuity of the corresponding operations on $M_{\Omega}(F, X)$. This turns $\mathbf{M}_{\Omega}^{\infty}(F, X)$ into an ω -complete F -magma, which is the free ω -complete F -magma generated by X .

Here is another aspect of this result. A tree t in $M_{\Omega}^{\infty}(F, X_k)$ defines a monotone and ω -continuous mapping $t_{\mathbf{M}}: M^k \rightarrow M$ for every ω -complete F -magma \mathbf{M} by

$$t_{\mathbf{M}} = \text{Sup}\{s_{\mathbf{M}} \mid s \in M_{\Omega}(F, X_k), s < t\}.$$

In the definition of $s_{\mathbf{M}}$ one takes $\perp_{\mathbf{M}}$ as the value of Ω .

Finally, substitutions extend to infinite trees by

$$\begin{aligned} & t_0[t_1/x_1, \dots, t_n/x_n] \\ &= \mathbf{Sup}\{s_0[s_1/x_1, \dots, s_n/x_n] \mid s_0, \dots, s_n \in M_\Omega(F, X), s_i < t_i \text{ for } i=0, \dots, n\} \end{aligned}$$

and the fundamental property is

$$t_0[t_1/x_1, \dots, t_n/x_n]_{\mathbf{M}} = t_{0\mathbf{M}} \circ (t_{1\mathbf{M}}, \dots, t_{n\mathbf{M}})$$

(see [26] for more details).

1.6. Equational classes of ω -complete F -magmas

For every subset \mathcal{E} of $M_\Omega(F, X) \times M_\Omega(F, X)$ (considered as a set of equations), we denote by $\mathcal{V}^\omega(\mathcal{E})$ the class of all ω -complete F -magmas which satisfy \mathcal{E} (i.e., which belong to $\mathcal{V}(\mathcal{E})$) and by \mathcal{V}^ω the class $\mathcal{V}^\omega(\emptyset)$. We denote by $\mathcal{E} \models t = t'$ the semantical equivalence associated with a class $\mathcal{C} \subseteq \mathcal{V}^\omega$ by the following conditions:

- (1) $t, t' \in M_\Omega^\infty(F, X_k)$ for some k ,
- (2) $t_{\mathbf{M}} = t'_{\mathbf{M}}$ for all \mathbf{M} in \mathcal{C} .

We use the notation $\mathcal{E} \models_\omega$ for $\mathcal{V}^\omega(\mathcal{E}) \models$. Hence, if $\mathcal{C} \subseteq \mathcal{V}$ and t or t' (or both) is not finite, the notation $\mathcal{C} \models t = t'$ is meaningful only if $\mathcal{C} \subseteq \mathcal{V}^\omega$. If \mathcal{E} is a set of equations, the notation $\mathcal{E} \models t = t'$ is meaningless if t or t' is infinite. Note that if t and t' are finite $\mathcal{E} \models t = t'$ implies $\mathcal{E} \models_\omega t = t'$ but the converse does not necessarily hold (see [25]).

We recall from [31, 32, 56] the syntactical characterization of this equivalence. It uses a sequence of definitions.

A preorder on $M_\Omega(F, X_k)$ is defined by

$$t \leq_{\mathcal{E}}^0 t' \text{ iff } t(\leftrightarrow_{\mathcal{E}} \cup <)^* t'.$$

This preorder is extended to $M_\Omega^\infty(F, X_k)$ by

$$t \leq_{\mathcal{E}} t' \text{ iff for all } s \text{ in } M_\Omega(F, X_k) \text{ such that } s < t, \text{ there exists } s' \text{ in } M_\Omega(F, X_k) \text{ such that } s' < t' \text{ and } s \leq_{\mathcal{E}}^0 s'.$$

And finally, for $t, t' \in M_\Omega^\infty(F, X_k)$:

$$t \equiv_{\mathcal{E}} t' \text{ iff } t \leq_{\mathcal{E}} t' \text{ and } t' \leq_{\mathcal{E}} t.$$

The following result is analogous to Lemma 1.4.

1.5. Lemma. *Let $t, t' \in M_\Omega^\infty(F, X_k)$. Then $\mathcal{E} \models_\omega t = t'$ iff $t \equiv_{\mathcal{E}} t'$.*

The relation $\equiv_{\mathcal{E}}$ is a congruence, hence, the quotient F -magma $\mathbf{M}_\Omega^\infty(F, X)/\equiv_{\mathcal{E}}$ is a natural object to consider. Unfortunately, it is not ω -complete in general; it is *not* the free ω -complete F -magma satisfying \mathcal{E} . But such a free object exists and is $\mathbf{M}_{\mathcal{E}} = [\mathbf{M}_\Omega(F, X)/\equiv_{\mathcal{E}}^0]^\infty$, where $\equiv_{\mathcal{E}}^0$ is the equivalence relation associated with the preorder $\leq_{\mathcal{E}}^0$ and $[\mathbf{M}]^\infty$ denotes the ideal completion of \mathbf{M} (see [31, 32, 33, 56] for more details). We only recall that if $h: \mathbf{M}_\Omega^\infty(F, X) \rightarrow \mathbf{M}_{\mathcal{E}}$ is the canonical homomorphism, then $h(t) \leq h(t')$ (respectively $h(t) = h(t')$) iff $t \leq_{\mathcal{E}} t'$ (respectively $t \equiv_{\mathcal{E}} t'$).

1.7. Commutation lemmas for rewriting relations

We conclude this section with a few technical results concerning rewriting systems that will be needed in Sections 3, 4 and 6.

We say that a rewriting system $R \subseteq M(F, X) \times M(F, X)$ is *left-linear* (respectively *right-linear*) if for all (s, t) in R the term s is linear (respectively the term t is linear). It is *linear* if it is both left- and right-linear. It is *balanced* if $|s|_x = |t|_x$ for all (s, t) in R , all x in X .

Let F and X be as above and U be a finite set of constants disjoint from F . In the following lemmas we shall assume that R is a finite rewriting system on $M(F, X)$ and that S and S' are finite ground rewriting systems on $M(F \cup U)$ such that $S, S' \subseteq U \times M(F, U)$.

1.6. Lemma. *Let us assume that R is left-linear. Let $t, t', s \in M(F, U)$ be such that $t \rightarrow_S^p s$ and $t \rightarrow_R^m t'$, for some $p, m \geq 1$. There exist s' in $M(F, U)$ and $p' \geq 0$ such that $s \rightarrow_R^m s'$ and $t' \rightarrow_{S'}^{p'} s'$. Furthermore, $p' \leq p$ if R is right-linear, and $p' = p$ if R is right-linear and balanced.*

Proof. The lemma is proved by induction on m (for all t, s, t' and p). It is clear that the proof reduces to the case $m = 1$. And we do this proof by induction on p . Once again the only interesting case is $p = 1$. So let $t = c[r[t_1, \dots, t_k]]$, $t' = c[r'[t_1, \dots, t_k]]$ for some (r, r') in R with r, r' in $M(F, X_k)$. The consideration of $t \rightarrow_S s$ yields two cases.

Case 1: $s = c'[r[t_1, \dots, t_k]]$ with $c \rightarrow_S c'$ and then one takes $s' = c'[r'[t_1, \dots, t_k]]$.

Case 2: $s = c[r[t_1, \dots, t'_i, \dots, t_k]]$ with $t_i \rightarrow_S t'_i$ for some i . If p' is the number of occurrences of x_i in r' , it is clear that $t' \rightarrow_{S'}^{p'} s'$, where $s' = c[r'[t_1, \dots, t'_i, \dots, t_k]]$.

If furthermore R is right-linear (respectively right-linear and balanced), then, in Case 2, one has $p' \leq 1$ (respectively $p' = 1$). The result follows by induction. \square

1.7. Lemma. *If R is right-linear, then, for all t, t' in $M(F, U)$, $t \rightarrow_{S \cup R}^* t'$ iff there exists s in $M(F, U)$ such that $t \rightarrow_S^* s \rightarrow_R^* t'$.*

Proof. One proves by induction on m that if $t \rightarrow_{S \cup R}^* t'$ and this sequence of rewritings uses m steps of the form \rightarrow_R , then $t \rightarrow_S^* s \rightarrow_R^m t'$ for some s in $M(F, U)$.

The case $m = 0$ is trivial.

For $m > 0$, one can assume by induction that $t \rightarrow_S^* t_1 \rightarrow_R t_2 \rightarrow_S^* t_3 \rightarrow_R^{m-1} t'$. Since R^{-1} is left-linear, Lemma 1.6 can be applied to t_1, t_2, t_3 and yields the existence of s such that $t_1 \rightarrow_S^* s \rightarrow_R t_3$. Hence, $t \rightarrow_S^* s \rightarrow_R^m t'$ as desired. \square

1.8. Lemma. *Let us assume that $S \cup S'$ is left-irreducible.*

(1) *For all t, t_1, t_2 in $M(F, U)$, if $t \rightarrow_S t_1$ and $t \rightarrow_{S'} t_2$, either $t_1 = t_2$ or there exists s such that $t_1 \rightarrow_{S'} s$ and $t_2 \rightarrow_S s$.*

(2) *For all t, t' in $M(F, U)$, $t \rightarrow_{S \cup S'}^* t'$ iff there exists s such that $t \rightarrow_S^* s$ and $s \rightarrow_{S'}^* t'$.*

Proof. Part (1) is an easy extension of Lemma 1.1. Part (2) is an easy consequence of part (1) by means of classical arrow-chasing. \square

1.9. Lemma. *Let us assume that $S \cup S'$ is left-irreducible and that R is linear. For all t, t' in $M(F, U)$, $t \rightarrow_{S \cup R \cup S'^{-1}}^* t'$ iff there exist s and s' in $M(F, U)$ such that $t \rightarrow_S^* s \rightarrow_R^* s' \xrightarrow{S'}^* t'$.*

Proof. We prove by induction on m that, if $t \rightarrow_{S \cup R \cup S'^{-1}}^* t'$ with m steps of the form \rightarrow_R , then there exist s and s' such that $t \rightarrow_S^* s \rightarrow_R^m s' \xrightarrow{S'}^* t'$.

The case $m = 0$ is an immediate consequence of Lemma 1.8.

For $m > 0$ and by induction, one can assume that

$$t \xrightarrow{S \cup S'^{-1}}^* t_1 \xrightarrow{R} t_2 \xrightarrow{S}^* t_3 \xrightarrow{R}^{m-1} t_4 \xleftarrow{S'}^* t'.$$

By Lemma 1.7 there exists a t'_2 such that

$$t_1 \xrightarrow{S}^* t'_2 \xrightarrow{R} t_3.$$

By Lemma 1.8 there exists an s such that $t \rightarrow_S^* s \xrightarrow{S'}^* t'_2$, hence, we have

$$t \xrightarrow{S}^* s \xleftarrow{S'}^* t'_2 \xrightarrow{R}^m t_4 \xleftarrow{S'}^* t'.$$

By Lemma 1.6 there exists an s' such that $s \rightarrow_R^m s' \xrightarrow{S'}^* t_4$. Hence, s and s' are as desired. \square

2. Regular systems

We define regular systems and some relations between them. We present the basic examples of regular systems: recursive applicative program schemes and context-free grammars.

2.1. Definitions of regular systems

Let F be a finite ranked alphabet, let U be a finite set of variables.

A *regular system* S over F with set of unknowns U is a *sequence* of equations of the form $u = t$ with u in U and t in $M(F, U)$ and such that for each u in U there is one and only one equation with left-hand side u . The set of unknowns of S is denoted by $\mathbf{Unk}(S)$. It is equivalent to define S as a *set* of equations as above and to assume that $\mathbf{Unk}(S)$ is linearly ordered.

We shall also use the latter definition, and in order to avoid the necessity of defining each time the order on $\mathbf{Unk}(S)$ we shall assume that $\mathbf{Unk}(S)$ is always a subset of some fixed infinite set of unknowns \mathcal{U} which is linearly ordered in a fixed way. Another technical assumption will be made in the construction that precedes Lemma 12.9. The set $\mathbf{Unk}(S)$ inherits a linear order from \mathcal{U} in an obvious way.

All our definitions and theorems will be formulated with respect to a regular system S which will always be of the general form $\langle u_i = t_i; 1 \leq i \leq n \rangle$ with $\mathbf{Unk}(S) = \{u_1, u_2, \dots, u_n\}$ (ordered in this way) and $t_i \in M(F, \mathbf{Unk}(S))$ for all i .

We shall refer to F as the *base alphabet* and to $u_i = t_i$ as *the equation defining u_i* . Let U be a finite subset of \mathcal{U} . If $u \mapsto t_u$ is a mapping associating t_u in $M(F, U)$ with u in U , we can form a regular system $S' = \langle u = t_u; u \in U \rangle$. And U is linearly ordered as a subset of \mathcal{U} .

As we are dealing with syntax, we immediately define special types of regular systems.

A system S (as above) is *uniform* if $t_i \in F(\mathbf{Unk}(S))$ for all i ; it is *quasi-uniform* if $t_i \in F(\mathbf{Unk}(S)) \cup \mathbf{Unk}(S)$ for all i ; it satisfies the *Greibach condition* (or is a *Greibach system*) if $t_i \in F(M(F, \mathbf{Unk}(S)))$ for all i .

If S' is another system, then S' is a *subsystem of S* (denoted by $S' \subseteq S$) if $\mathbf{Unk}(S') \subseteq \mathbf{Unk}(S)$ and if every equation of S' is an equation of S . If $U' \subseteq \mathbf{Unk}(S)$ we denote by $S \upharpoonright U'$ the set of equations $\langle u_i = t_i; u_i \in U' \rangle$. It is not necessarily a subsystem of S . But we can always consider it as a regular system over $F \cup U - U'$, with set of unknowns U' .

2.2. Solutions

Let S be a regular system. Let \mathbf{M} be an F -magma. A *solution* of S in \mathbf{M} is an n -tuple $m = (m_1, \dots, m_n)$ in M^n such that $m_i = t_{i\mathbf{M}}(m)$ for all $i = 1, \dots, n$. We shall also write this as $m = S_{\mathbf{M}}(m)$ by letting $S_{\mathbf{M}}: M^n \rightarrow M^n$ denote the target-tupling of $t_{1\mathbf{M}}, \dots, t_{n\mathbf{M}}$ (i.e., $S_{\mathbf{M}}(m) = (t_{1\mathbf{M}}(m), \dots, t_{n\mathbf{M}}(m))$).

We shall denote by $\mathbf{Sol}_{\mathbf{M}}(S)$ the set of all solutions of S in \mathbf{M} (this set may be empty).

Let now \mathbf{M} be an ω -complete F -magma. Every regular system S has a least solution in \mathbf{M} denoted by $\mu\text{-Sol}_{\mathbf{M}}(S)$ and classically characterized by

$$\mu\text{-Sol}_{\mathbf{M}}(S) = \mathbf{Sup}_{i \geq 0} (S_{\mathbf{M}}^i(\perp_{\mathbf{M}}^n))$$

as a consequence of the Fix-point Lemma (see [65] on various aspects of this lemma).

2.3. Equivalences of regular systems

Let \mathcal{T} be an arbitrary class of F -magmas. Let S be a regular system. We define an equivalence relation on $M(F, \mathbf{Unk}(S))$ by letting

$$t \approx_{S, \mathcal{T}} t' \text{ iff } t_{\mathbf{M}}(m) = t'_{\mathbf{M}}(m) \text{ for all } \mathbf{M} \text{ in } \mathcal{T} \text{ and for all } m \text{ in } \mathbf{Sol}_{\mathbf{M}}(S).$$

If S and S' are two regular systems with the same set of unknowns we let

$$S \cong_{\mathcal{T}} S' \text{ iff } \mathbf{Sol}_{\mathbf{M}}(S) \subseteq \mathbf{Sol}_{\mathbf{M}}(S') \text{ for all } \mathbf{M} \text{ in } \mathcal{T}$$

$$\text{iff } t \approx_{S, \mathcal{T}} t' \text{ for every equation } (t, t') \text{ of } S'.$$

$$S \approx_{\mathcal{T}} S' \text{ iff } \mathbf{Sol}_{\mathbf{M}}(S) = \mathbf{Sol}_{\mathbf{M}}(S') \text{ for all } \mathbf{M} \text{ in } \mathcal{T}, \text{ i.e.,}$$

$$\text{iff } S \cong_{\mathcal{T}} S' \text{ and } S' \cong_{\mathcal{T}} S.$$

If $\mathcal{T} = \{\mathbf{M}\}$, the subscript \mathcal{T} is replaced by \mathbf{M} . If $\mathcal{T} = \mathcal{V}(\mathcal{E})$ for some set of equations \mathcal{E} , the subscript \mathcal{T} is replaced by \mathcal{E} . If $\mathcal{T} = \mathcal{V}$ ($= \mathcal{V}(\emptyset)$) the subscript \mathcal{T} is omitted. Analogous definitions can be given for ω -complete magmas and least solutions.

Let $\mathcal{T} \subseteq \mathcal{V}^\omega$ and t, t', S , and S' be as above. Then,

$$t \sim_{S, \mathcal{T}} t' \text{ iff } t_{\mathbf{M}}(\mu\text{-Sol}_{\mathbf{M}}(S)) = t'_{\mathbf{M}}(\mu\text{-Sol}_{\mathbf{M}}(S)) \text{ for all } \mathbf{M} \text{ in } \mathcal{T}$$

$$S \preceq_{\mathcal{T}} S' \text{ iff } \mu\text{-Sol}_{\mathbf{M}}(S) \in \text{Sol}_{\mathbf{M}}(S')$$

$$\text{(whence } \mu\text{-Sol}_{\mathbf{M}}(S') \leq_{\mathbf{M}} \mu\text{-Sol}_{\mathbf{M}}(S) \text{ for all } \mathbf{M} \text{ in } \mathcal{T}$$

$$\text{iff } t \sim_{S, \mathcal{T}} t' \text{ for every equation } (t, t') \text{ of } S',$$

$$S \sim_{\mathcal{T}} S' \text{ iff } \mu\text{-Sol}_{\mathbf{M}}(S) = \mu\text{-Sol}_{\mathbf{M}}(S') \text{ for all } \mathbf{M} \text{ in } \mathcal{T}, \text{ i.e.,}$$

$$\text{iff } S \preceq_{\mathcal{T}} S' \text{ and } S' \preceq_{\mathcal{T}} S.$$

As above we shall replace the subscript \mathcal{T} by \mathbf{M} , \mathcal{E} , or we shall omit it if $\mathcal{T} = \{\mathbf{M}\}$, $\mathcal{T} = \mathcal{V}^\omega(\mathcal{E})$ or $\mathcal{T} = \mathcal{V}^\omega (= \mathcal{V}^\omega(\emptyset))$, respectively. We shall mainly use the last two cases.

The following facts are clear (where \mathcal{E} is a set of equations):

$$(2.3.1) \ t \approx_{S, \mathcal{E}} t' \text{ implies } t \sim_{S, \mathcal{E}} t',$$

$$(2.3.2) \ S \cong_{\mathcal{E}} S' \text{ implies } S \preceq_{\mathcal{E}} S',$$

$$(2.3.3) \ S \approx_{\mathcal{E}} S' \text{ implies } S \sim_{\mathcal{E}} S'.$$

Similar implications hold when \mathcal{E} is replaced by \mathbf{M} , where $\mathbf{M} \in \mathcal{V}^\omega$.

2.4. Remarks on terminology and notations

The term ‘regular system’ has been used in [26] to designate regular systems in the sense of Section 1.1 which are uniform. The regular systems of this paper would be called “extended regular systems with finite right-hand sides” in the terminology of [26]. (We are sorry for that, but we think the present terminology is more appropriate than the one of [26] for this paper.) They have been introduced and investigated in [36–39, 45, 75] (“systems of regular equations”), and in [24] (allowing infinitely many equations).

Finally, as a mnemonic hint to notations, the reader should note that \approx and its modifications refer to *all* solutions of regular systems (in unordered F -magmas) whereas \sim refers to their *least* solutions in ω -complete F -magmas.

2.5. Renamings

Let $S = \langle u_i = t_i; i \in [n] \rangle$ and S' be another regular system. We say that S' is a *renaming of S* if there exists a bijection $\alpha: \text{Unk}(S) \rightarrow \text{Unk}(S')$ such that $S' = \langle \alpha(u_i) = t_i[\alpha(u_j)/u_j; 1 \leq j \leq n]; i \in [n] \rangle$. We write this $S' = \alpha(S)$. If α is *monotone*,

i.e., if $\alpha(u_i)$ has rank i in $\mathbf{Unk}(S')$, then $\mathbf{Sol}_{\mathbf{M}}(S) = \mathbf{Sol}_{\mathbf{M}}(S')$ and $\mu\text{-Sol}_{\mathbf{M}}(S) = \mu\text{-Sol}_{\mathbf{M}}(S')$ for all \mathbf{M} in \mathcal{V} (or in \mathcal{V}^ω).

Note that we do not write $S \approx S'$ and $S \sim S'$, since in Section 2.3 we require that S and S' have the same unknowns. The reason is that we want to express \approx and \sim as sequences of transformations of systems which preserve the sets of unknowns (see Sections 4 and 6). This restriction in the definitions of \approx and \sim (and of $\approx_{\mathcal{T}}$, $\sim_{\mathcal{T}}$, $\lesssim_{\mathcal{T}}$, $\leq_{\mathcal{T}}$) is not a loss of generality since, for any two systems S and S' with the same number of unknowns and such that $\mathbf{Sol}_{\mathbf{M}}(S) = \mathbf{Sol}_{\mathbf{M}}(S')$ for all \mathbf{M} in $\mathcal{T} \subseteq \mathcal{V}$ (respectively $\mu\text{-Sol}_{\mathbf{M}}(S) = \mu\text{-Sol}_{\mathbf{M}}(S')$ with \mathbf{M} in \mathcal{V}^ω) there exists a monotone renaming α such that $\alpha(S) \approx_{\mathcal{T}} S'$ (respectively $\alpha(S) \sim_{\mathcal{T}} S'$) (a similar property can be stated for $\lesssim_{\mathcal{T}}$ and $\leq_{\mathcal{T}}$). Hence, we do not lose anything by restricting our definitions of $\approx_{\mathcal{T}}$, $\sim_{\mathcal{T}}$, etc. to pairs of systems with same sets of unknowns. It is also to have easier formulated (and more concrete) system transformations that we use explicit unknowns (with names, e.g., $u, v, w, u_1, u'_1, \dots$) and not just integers as, for instance, in [42] and all the subsequent papers on iterative theories.

2.6. Singular unknowns

In regular systems we allow equations of the form $u = u'$ and even of the form $u = u$. Here are a few technical definitions to deal with these equations.

For u, u' in $\mathbf{Unk}(S)$ we write $u \rightarrow u'$ if $u = u'$ is an equation of S .

An unknown u is *singular* if $u \rightarrow^+ u$. It is *powersingular* if $u \rightarrow^* v$ for some singular unknown v . We denote by $\mathbf{Sing}(S)$ and by $\mathbf{Psing}(S)$ the sets of singular and powersingular unknowns of S .

Finally, we let γ_S be the binary relation on $\mathbf{Unk}(S)$ such that $u \gamma_S u'$ iff $u \rightarrow^* v$ and $u' \rightarrow^* v$ for some v in $\mathbf{Sing}(S)$. If $u, u' \in \mathbf{Psing}(S)$ and $u \gamma_S u'$ does not hold, we say that u and u' are *independent*. The reason is that a solution of S can be constructed where u and u' have distinct values (see the proof of Proposition 3.2(1) below). Otherwise, if $u \gamma_S u'$, then u and u' have the same value for every solution of S , i.e., $u \approx_S u'$.

If u is powersingular, then its value in the least solution of S in every ω -complete F -magma \mathbf{M} is $\perp_{\mathbf{M}}$. We write this $u \sim_S \Omega$, where Ω is the special constant always denoting the least element of an ω -complete magma (see Section 1.5). Hence, $u \sim_S u'$ for every u, u' in $\mathbf{Psing}(S)$ (whereas $u \approx_S u'$ if and only if $u \gamma_S u'$ for u, u' in $\mathbf{Psing}(S)$). This will be proved in Proposition 5.14.

2.7. Recursive applicative program schemes as regular systems

We only present an example. A more detailed treatment will be given in Section 9.

A typical example of a recursive applicative program scheme is the pair (Σ, t) , where Σ is the system of equations

$$\begin{aligned} \theta(x_1, x_2) &= f(x_1, \theta(x_2, \psi(x_2, x_1))), \\ \psi(x_1, x_2) &= g(f(x_2, x_2), \psi(x_1, x_2)), \end{aligned}$$

defining two functions θ and ψ by mutual recursion and where $t = \theta(x_1, \psi(x_2, x_2))$. This term plays the role of the ‘main program’ written in terms of auxiliary recursively defined functions θ and ψ .

Every ω -complete F -magma \mathbf{D} (where $F = \{f, g\}$) can be considered as an *interpretation* for (Σ, t) and a function $t_{\mathbf{D}}: D \times D \rightarrow D$ can be associated with (Σ, t) and \mathbf{D} . There are several ways to define $t_{\mathbf{D}}$. One of them consists in *solving* Σ in \mathbf{D} , i.e., in finding the least pair $(\theta_{\mathbf{D}}, \psi_{\mathbf{D}})$ of continuous functions: $D \times D \rightarrow D$ which satisfies Σ (where $f_{\mathbf{D}}, g_{\mathbf{D}}$ give meaning to f, g) in an obvious way. This approach has been investigated at length in various works ([25, 26, 29–32, 34, 55, 56]).

Solving Σ in \mathbf{D} corresponds exactly to solving the regular system S with unknowns θ, ψ and consisting of the following two equations:

$$\theta = \mathbf{comp}(f, \pi_1, \mathbf{comp}(\theta, \pi_2, \mathbf{comp}(\psi, \pi_2, \pi_1))),$$

$$\psi = \mathbf{comp}(g, \mathbf{comp}(f, \pi_2, \pi_2), \psi),$$

in the ω -complete H -magma \mathbf{M} , where $H = \{\mathbf{comp}, f, g, \pi_1, \pi_2\}$ with $\rho(\mathbf{comp}) = 3$, $\rho(f) = \rho(g) = \rho(\pi_1) = \rho(\pi_2) = 0$ and such that:

- $M = (D \times D \rightarrow D)$ (the set of ω -continuous functions: $D \times D \rightarrow D$),
- $f_{\mathbf{M}} = f_{\mathbf{D}}$,
- $g_{\mathbf{M}} = g_{\mathbf{D}}$,
- $\pi_{i\mathbf{M}}$ is the i th projection $D \times D \rightarrow D$, $i = 1, 2$,
- $\mathbf{comp}_{\mathbf{M}}(\alpha, \beta, \gamma) = \alpha \circ (\beta, \gamma)$ for α, β, γ in $(D \times D \rightarrow D)$.

It can be shown that $(\theta_{\mathbf{D}}, \psi_{\mathbf{D}}) = \mu\text{-Sol}_{\mathbf{M}}(S)$.

Such program schemes have been investigated in the above cited works as systems of *algebraic equations* (like Σ) rather than as systems of regular equations (like S).

In S , the base functions of Σ and the recursively defined ones are treated as objects (i.e., as elements of the domain where S is solved) and their composition is made explicit by means of the base function \mathbf{comp} . The variables disappear and are replaced by constants, denoting projection functions. The composition of functions is used in Σ of course, but as a syntactic construction.

A system like Σ is certainly more readable than the corresponding regular system S . It is close to real ALGOL or LISP procedure definitions. A system like S is close to an FP-program [3].

The main advantage of regular systems is that their theory is easier than that of algebraic systems, and more general since it applies also to context-free grammars of words, trees, and graphs as the present paper will show. It also applies to higher-type recursion as shown in [37, 39, 48] and to imperative program schemes [26, 35].

Not all existing results on recursive applicative program schemes can be conveniently presented in terms of regular systems, at least at first look (e.g., [7, 22, 25]) and the formalism of algebraic systems remains necessary, but the most one can do with regular systems the better it is.

2.8. Context-free grammars as regular systems

A context-free grammar is usually defined as a triple $G = \langle N, T, P \rangle$ consisting of two finite disjoint alphabets N (nonterminal symbols) and T (terminal symbols) and a finite subset P of $N \times (N \cup T)^*$ called the set of production rules. By using P as a rewriting system, one defines $L(G, u)$ the *language generated by G from the nonterminal symbol u* (and $L(G, u) \subseteq T^*$).

It is also classical to associate with G the system of equations $S_G = \langle u = p_u; u \in N \rangle$, where p_u is a term (we shall say a polynomial in Sections 10–17) in $M(F, N)$ defined as follows.

We let $F = \{+, \cdot, \varepsilon, \Omega\} \cup T$, where $+$, \cdot are binary and all its other elements are nullary. The infix notation will be used for $+$ and \cdot and, since they will denote associative operations, parentheses will be omitted. Then we let $P_u = \{w \in (N \cup T)^* \mid (u, w) \in P\}$. If $P_u = \emptyset$, then $p_u = \Omega$. Otherwise, $p_u = \bar{w}_1 + \cdots + \bar{w}_m$ where $P_u = \{w_1, \dots, w_m\}$ and $w \mapsto \bar{w}$ is the mapping $(N \cup T)^* \rightarrow M(F, N)$ such that

$$\varepsilon \mapsto \varepsilon.$$

$$a_1 a_2 \dots a_k \mapsto a_1 \cdot a_2 \cdot a_3 \cdot \dots \cdot a_k,$$

where $a_1, \dots, a_k \in N \cup T$. Without loss of generality we can assume that $N = \{u_1, \dots, u_n\}$ and is ordered in this way.

Let \mathbf{M} be the F -magma with domain $\mathcal{P}(T^*)$, such that $+$ denotes the set union, \cdot denotes the product of languages, Ω denotes \emptyset , ε denotes $\{\varepsilon\}$ and a denotes $\{a\}$ for all a in T . Ordered by set inclusion, \mathbf{M} is ω -complete and by a result of Ginsburg and Rice [51] ([78] for another proof) the least solution of S_G in \mathbf{M} is the n -tuple of languages $(L(G, u_i))_{i \in [n]}$.

The system S_G is regular over F . The concatenation of words is explicitly introduced as the composition of functions was in Section 2.7. In Sections 10–18 we shall investigate the class of polynomial systems which abstracts from systems like S_G by working in an arbitrary powerset magma $\mathcal{P}(\mathbf{M})$ instead of the specific one $\mathcal{P}(T^*)$ (see Section 10 for the definition of $\mathcal{P}(\mathbf{M})$).

We conclude this chapter with some general definitions concerning transformations of regular systems.

2.9. Definitions: transformations of regular systems

By an *equivalence of regular systems* we mean an equivalence relation on the set of regular systems such that any two equivalent systems have the same set of unknowns. Examples of equivalences are $\approx_{\mathcal{E}}$ and $\sim_{\mathcal{E}}$.

By a *transformation* we mean a binary relation τ on the set of regular systems which is semi-decidable, i.e., such that the set of pairs of systems (S, S') such that $S\tau S'$ is recursively enumerable. Typical examples are **unf** (the classical transformation by unfolding, see Definition 4.1) and **rewr_g** (consisting in transforming the right-hand sides of a regular system by rewritings associated with \mathcal{E} , see Definition 4.1).

Let η be an equivalence of regular systems. A transformation τ is η -correct if $\tau \subseteq \eta$, i.e., if $S\eta S'$ whenever $S\tau S'$. A set of transformations \mathcal{T} is η -correct if its elements are η -correct. It is η -complete if $\eta = \mathcal{T}^*$, i.e., if it is η -correct and if, for S, S' such that $S\eta S'$, one has $S\mathcal{T}^* S'$, i.e., $S = S'$ or $S\tau_0 S_1 \tau_1 \cdots S_k \tau_k S'$ for some $k \geq 0$, some systems S_1, \dots, S_k , and some τ_0, \dots, τ_k in \mathcal{T} .

If \mathcal{T} and \mathcal{T}' are two sets of transformations, we say that \mathcal{T} is *strictly less powerful than* \mathcal{T}' (respectively *has the same power as* \mathcal{T}') if $\mathcal{T}^* \subseteq \mathcal{T}'^*$ (respectively if $\mathcal{T}^* = \mathcal{T}'^*$).

In the next sections we shall characterize the equivalences $\approx_{\mathcal{E}}$ and $\sim_{\mathcal{E}}$ and try to find sets of transformations which are correct and complete w.r.t. them.

Our completeness results will be obtained by the definition of a mapping $S \mapsto S_\eta$ (where η is some equivalence) such that

- (1) $S\eta S_\eta$,
- (2) $S\eta S'$ if and only if $S_\eta = S'_\eta$,
- (3) $S\mathcal{T}^* S_\eta$.

We summarize conditions (1) and (2) by saying that S_η is η -canonical. (Actually this notion refers to the mapping $S \mapsto S_\eta$.)

2.1. Proposition. *Let η be an equivalence of systems and \mathcal{T} be a set of η -correct transformations such that $\tau^{-1} \subseteq \mathcal{T}^*$ for each τ in \mathcal{T} . If S_η is η -canonical and $S\mathcal{T}^* S_\eta$ for all S , then \mathcal{T} is η -complete.*

Proof. If $S\eta S'$, then $S_\eta = S'_\eta$ and $S\tau_1 \tau_2 \cdots \tau_k S_\eta \tau'_1 \tau'_1^{-1} \cdots \tau'_1 \tau'_1^{-1} S'$ for some $\tau_1, \dots, \tau_k, \tau'_1, \dots, \tau'_l$ in \mathcal{T} . This easily yields $S\mathcal{T}^* S'$. \square

Remark. The renaming of unknowns of regular systems introduced in Section 2.5 is also a transformation, but is not η -correct since it modifies the sets of unknowns (see the end of Section 2.5).

3. Comparing regular systems with respect to their full sets of solutions

In this section we characterize the relation $\approx_{\mathcal{E}}$ and we obtain a transformation which is $\approx_{\mathcal{E}}$ -complete. Other transformations will be investigated in the next section. This characterization will deal with rewriting systems associated with S .

3.1. Definition. Let S be a regular system and \mathcal{E} be a set of equations, $\mathcal{E} \subseteq M(F, X) \times M(F, X)$. Let $U = \text{Unk}(S)$ (with $X \cap U = \emptyset$). We shall also denote by S the *ground* rewriting system $\{(u_i, t_i) \mid 1 \leq i \leq n\}$ on $M(F \cup U)$. Note that the elements of U are considered as constants and not as variables, as are those of X . Note that S is left-irreducible.

We shall also use the ground systems $S^{-1} = \{(t_i, u_i) \mid 1 \leq i \leq n\}$ and $R(S)$ defined as S^{-1} minus the pairs (u, u) for u in U .

We denote by \leftrightarrow_S the relation $\rightarrow_{S \cup S^{-1}}$ on $M(F \cup U)$, by $\rightarrow_{S, \mathcal{E}}$ the relation $\rightarrow_S \cup \leftrightarrow_{\mathcal{E}}$, and by $\leftrightarrow_{S, \mathcal{E}}$ the relation $\leftrightarrow_S \cup \leftrightarrow_{\mathcal{E}}$. (Note that the pairs of \mathcal{E} use variables from the set X (where $X \cap U = \emptyset$) hence, $\leftrightarrow_{\mathcal{E}}$ is *not* a ground rewriting relation.)

3.2. Theorem. *Let S and S' be two regular systems over F having the same set of unknowns U :*

- (1) *for t, t' in $M(F, U)$, $t \approx_{S, \mathcal{E}} t'$ if and only if $t \leftrightarrow_{S, \mathcal{E}}^* t'$.*
- (2) *$S \cong_{\mathcal{E}} S'$ if and only if $u \leftrightarrow_{S, \mathcal{E}}^* t'$ for every equation $u = t'$ of S' .*

Proof. (1) For every F -magma \mathbf{M} , for every $m = (m_1, \dots, m_n)$ in M^n , let $\mathbf{M}(m)$ be the $(F \cup U)$ -magma $\langle \mathbf{M}, \langle f \rangle_{f \in F}, \langle m_i \rangle_{u_i \in U} \rangle$. It is clear that m is a solution of S in \mathbf{M} iff $\mathbf{M}(m)$ satisfies S considered as a set of ground equations. Hence, $t \approx_{S, \mathcal{E}} t'$ iff $S \cup \mathcal{E} \models t = t'$. The result follows from Lemma 1.4.

For later reference, let us mention that the main step of the proof consists in the construction of $M(F, U)/\leftrightarrow_{S, \mathcal{E}}^*$ which belongs to $\mathcal{V}(\mathcal{E})$ and where S has a solution. See [6] for a more general use of this construction.

Part (2) follows from part (1) and fact (2.3.1) of Section 2.3. \square

These characterizations raise questions of decidability when \mathcal{E} is finite. We answer them in the following proposition.

3.3. Proposition. (1) *The properties $t \approx_S t'$, $S \cong S'$, $S \approx S'$ are decidable.*

(2) *The properties $t \approx_{S, \mathcal{E}} t'$, $S \cong_{\mathcal{E}} S'$, $S \approx_{\mathcal{E}} S'$ are undecidable in general (even if \mathcal{E} has a decidable word problem).*

Proof. (1) By Lemma 1.1, $t \leftrightarrow_S^* t'$ iff $t \rightarrow_S^* s$ and $t' \rightarrow_S^* s$ for some s . By classical techniques [16, 17, 50] one can construct a finite-state tree automaton recognizing the tree-language $L(S, t) = \{w \in M(F, U) \mid t \rightarrow_S^* w\}$ and similarly for $L(S, t')$. Hence, one can test whether $L(S, t) \cap L(S, t') \neq \emptyset$, i.e., whether $t \leftrightarrow_S^* t'$. The decidability of $S \cong S'$ and $S \approx S'$ follows from Theorem 3.2(2). Another proof that $S \approx S'$ is decidable will be given below (Proposition 4.13).

(2) Let F consist of one binary function symbol “.” (for which infix notation will be used), together with constants. Let \mathcal{E} consist of the single equation expressing that . is associative. It follows that $M(F, U)/\leftrightarrow_{\mathcal{E}}^*$ is the free semigroup generated by $F_0 \cup U$.

The problem of deciding whether $t \leftrightarrow_{S, \mathcal{E}}^* t'$ for a regular system S and two elements t and t' of $M(F, U)$ is exactly the word problem for a Thue system (on a free semigroup X^+) defined by a finite set of the form $\{(x, m_x) \mid x \in Y\}$, where $Y \subseteq X$ and $m_x \in X^+$ for all x in Y (the set U corresponds to Y , the set F_0 to $X - Y$, the function “.” to the concatenation of words). And this special case of the word problem for Thue systems has been shown undecidable by Book [15]. Hence, $t \approx_{S, \mathcal{E}} t'$ is undecidable in general.

The last undecidability results follow from Lemma 3.4 below. \square

Our main interest is the investigation of the relations $\approx_{\mathcal{T}}$ and $\sim_{\mathcal{T}}$. The relations $t \approx_{S, \mathcal{T}} t'$ and $t \sim_{S, \mathcal{T}} t'$ are technical tools to help in this study (see Section 2.3) and the following lemma shows that, vice versa, $\approx_{S, \mathcal{T}}$ can be characterized in terms of $\approx_{\mathcal{T}}$ (or $\cong_{\mathcal{T}}$) and similarly for $\sim_{S, \mathcal{T}}$.

3.4. Lemma. *Let S be a regular system over F , let $t, t' \in M(F, \mathbf{Unk}(S))$, and $\mathcal{T} \subseteq \mathcal{V}$. Let u and u' be new unknowns, not in $\mathbf{Unk}(S)$. Let $S' = S \cup \langle u = t, u' = t' \rangle$ and $S'' = S \cup \langle u = t, u' = t' \rangle$.*

- (1) *Then $t \approx_{S, \mathcal{T}} t'$ iff $S' \cong_{\mathcal{T}} S''$ iff $S' \approx_{\mathcal{T}} S''$.*
- (2) *If furthermore, $\mathcal{T} \subseteq \mathcal{V}^{\omega}$, then $t \sim_{S, \mathcal{T}} t'$ iff $S' \preceq_{\mathcal{T}} S''$ iff $S' \sim_{\mathcal{T}} S''$.*

Proof. (1) Let us assume that $t \approx_{S, \mathcal{T}} t'$. Let m be a solution of S' in \mathbf{M} for some \mathbf{M} in \mathcal{T} . Its restriction to $\mathbf{Unk}(S)$ defines a solution of S , hence, $t_{\mathbf{M}}(m) = t'_{\mathbf{M}}(m)$ and m is also a solution of S'' . Similarly, any solution of S'' in \mathbf{M} is a solution of S' . Hence, $S' \cong_{\mathcal{T}} S''$ and $S' \approx_{\mathcal{T}} S''$.

Conversely, if $S' \cong_{\mathcal{T}} S''$, then any solution of S in \mathbf{M} extends into a solution of S' which is also a solution of S'' hence, such that $t_{\mathbf{M}}(m) = t'_{\mathbf{M}}(m)$. Hence, $t \approx_{S, \mathcal{T}} t'$.

Part (2) is proven with a similar argument. \square

Proposition 3.3 leaves open the problem of finding conditions on $\leftrightarrow_{\mathcal{E}}^*$ (or on \mathcal{E}) insuring that the word problem for $S \cup \mathcal{E}$ is decidable (either for some given S or for all possible ones). Lemma 1.9 with $S' = S$, $R = \mathcal{E} \cup \mathcal{E}^{-1}$ may help to find such conditions.

We now derive from Theorem 3.2 the definition of an $\approx_{\mathcal{E}}$ -complete transformation.

3.5. Definition. Let $\mathbf{eq}_{\mathcal{E}}$ be the semidecidable relation on regular systems defined as follows for S and S' , respectively of the form $\langle u_i = t_i; i \in [n] \rangle$ and $\langle u_i = t'_i; i \in [n] \rangle$:

$$S \mathbf{eq}_{\mathcal{E}} S' \text{ iff for all } i \text{ in } [n], t_i \leftrightarrow_{S, \mathcal{E}}^* t'_i \text{ and } t_i \leftrightarrow_{S', \mathcal{E}}^* t'_i.$$

Note that this condition corresponds to saying that $S \cup \mathcal{E}$ and $S' \cup \mathcal{E}$ generate the same congruence on $M(F, U)$ (see Example 4.15). And Lemma 1.9 simplifies the expression of $\mathbf{eq}_{\mathcal{E}}$ if \mathcal{E} is linear.

Part (2) of Theorem 3.2 immediately yields the following corollary.

- 3.6. Corollary.** (1) $S \approx_{\mathcal{E}} S'$ iff $S \mathbf{eq}_{\mathcal{E}} S'$.
 (2) $\{\mathbf{eq}_{\mathcal{E}}\}$ is $\approx_{\mathcal{E}}$ -complete.

Although having $\mathbf{eq}_{\mathcal{E}}$ is better than nothing, we are not fully satisfied with it since it does not produce a sequence S_1, \dots, S_k of systems such that $S \approx_{\mathcal{E}} S_1 \approx_{\mathcal{E}} S_2 \approx_{\mathcal{E}} \dots \approx_{\mathcal{E}} S_k \approx_{\mathcal{E}} S'$, where each step $S \rightarrow S_1$, $S_1 \rightarrow S_2$, etc. can be considered as 'elementary'. In other words $\mathbf{eq}_{\mathcal{E}}$ is too global.

We shall try to find other transformation rules, based on the processes of folding, unfolding and rewriting modulo \mathcal{E} . Such transformations are commonly used in manipulations of recursive programs [19, 25, 63] and of context-free grammars (see Section 17). Hence, we think it to be important to study them at a theoretical level, in particular because they are not always correct (see [25, 63, 64]), so that they must be used with some caution.

3.7. Remark. The reader may ask what is the relation between $t \approx_{S, \mathcal{E}} t'$ and $t \approx_{S, \mathbf{M}} t'$ for some fixed \mathbf{M} in $\mathcal{V}(\mathcal{E})$, say, for instance, $\mathbf{M} = \mathbf{M}(F, X) / \leftrightarrow_{\mathcal{E}}^*$. Actually, the former implies the latter but not conversely. Take for example $S = \langle u = fu \rangle$, $t = u$, $t' = a$ (where a is any constant), $\mathcal{E} = \emptyset$. Then, $t \approx_{S, \mathcal{E}} t'$ since S has no solution in $\mathbf{M}(F, X)$.

The reason is that when there exists a homomorphism $h : \mathbf{M} \rightarrow \mathbf{M}'$, the image under h of a solution of S in \mathbf{M} is a solution of S in \mathbf{M}' , but S may have other solutions in \mathbf{M}' . Hence, $t \approx_{S, \mathbf{M}} t'$ does not imply $t \approx_{S, \mathbf{M}'} t'$. This fact has also been noted by Nelson [75].

4. Transformations by folding, unfolding and rewriting

Transformations of recursive programs by unfolding, folding and use of equations expressing the algebraic properties of the considered interpretations have been used by Burstall and Darlington [19]. But these transformations are not always correct, i.e., the program obtained is not always equivalent to the original one. Hence, after having used such a transformation, one must prove the equivalence of the program thus obtained with the original one.

Alternatively, syntactical restrictions insuring the correctness can be defined [25, 63, 64]. We shall apply these transformations to regular systems and define syntactical restrictions insuring their $\approx_{\mathcal{E}}$ -correctness. A completeness result will be proved when $\mathcal{E} = \emptyset$ by means of the transformation of an arbitrary system into a \approx -canonical equivalent one.

4.1. Definition. Let S and \mathcal{E} be as in Definition 3.1 and let $S' = \langle u_i = t'_i; 1 \leq i \leq n \rangle$. We introduce the following transformations (see Section 2.9 on system transformations in general):

- $S \text{ unf } S'$ iff for all i in $[n]$, $t_i \rightarrow_{\mathcal{E}}^* t'_i$ (*unfolding*),
- $S \text{ fld } S'$ iff for all i in $[n]$, $t_i \rightarrow_{\mathcal{E}}^{*-1} t'_i$ (*folding*),
- $S \text{ unfld } S'$ iff for all i in $[n]$, $t_i \leftrightarrow_{\mathcal{E}}^* t'_i$ (*folding-unfolding*),
- $S \text{ rewr}_{\mathcal{E}} S'$ iff for all i in $[n]$, $t_i \leftrightarrow_{\mathcal{E}}^* t'_i$ (*use of equational laws*).

Finally, the use of laws can be mixed with **unf**, **fld**, **unfld**, in the following transformations:

- $S \text{ unf}_{\mathcal{E}} S'$ iff for all i in $[n]$, $t_i \rightarrow_{\mathcal{E}}^* t'_i$,

and similarly for $\mathbf{fld}_{\mathcal{E}}$ and $\mathbf{ufld}_{\mathcal{E}}$. Note that $\mathbf{rewr}_{\mathcal{E}} \subseteq \mathbf{unf}_{\mathcal{E}} \subseteq \mathbf{ufld}_{\mathcal{E}}$ and that $\mathbf{rewr}_{\mathcal{E}} \subseteq \mathbf{fld}_{\mathcal{E}} \subseteq \mathbf{ufld}_{\mathcal{E}}$.

4.2. Example. Let $S = \langle u = fu \rangle$, $S' = \langle u = ffu \rangle$, and $S'' = \langle u = u \rangle$. It is clear that $S \mathbf{unf} S'$ and that $S \mathbf{fld} S''$.

These examples show that $\mathbf{unf}^{-1} \not\subseteq \mathbf{fld}$ and that $\mathbf{fld}^{-1} \not\subseteq \mathbf{unf}$.

4.3. Proposition. (1) *The transformation $\mathbf{unf}_{\mathcal{E}}$ is transitive.*

(2) $\mathbf{unf}_{\mathcal{E}} = \mathbf{unf} \cdot \mathbf{rewr}_{\mathcal{E}}$ if \mathcal{E} is linear.

(3) *The classes $\{\mathbf{unf}, \mathbf{rewr}_{\mathcal{E}}\}$ and $\{\mathbf{unf}_{\mathcal{E}}\}$ have the same power if \mathcal{E} is linear.*

Proof. (1) If $S \mathbf{unf}_{\mathcal{E}} S' \mathbf{unf}_{\mathcal{E}} S''$ with $S' = \langle u_i = t'_i; i \in [n] \rangle$ and $S'' = \langle u_i = t''_i; i \in [n] \rangle$, then $t_i \rightarrow_{S, \mathcal{E}}^* t'_i \rightarrow_{S', \mathcal{E}}^* t''_i$ for all $i = 1, \dots, n$. Since $u_i \rightarrow_{S, \mathcal{E}}^* t'_i \rightarrow_{S'} \subseteq \rightarrow_{S, \mathcal{E}}^*$ hence, $t_i \rightarrow_{S, \mathcal{E}}^* t''_i$. This shows that $S \mathbf{unf}_{\mathcal{E}} S''$.

Part (2) is an immediate consequence of Lemma 1.7.

Part (3) follows from parts (1) and (2). \square

The following example shows that the results of Proposition 4.3 do not hold for $\mathbf{fld}_{\mathcal{E}}$.

4.4. Example. We first show that \mathbf{fld} is not transitive by considering

$$S_1 = \langle u = ffu, v = gfw, w = fu \rangle,$$

$$S_2 = \langle u = fw, v = gfw, w = fu \rangle,$$

$$S_3 = \langle u = fw, v = gu, w = fu \rangle.$$

Hence, $S_1 \mathbf{fld} S_2 \mathbf{fld} S_3$, but $S_1 \mathbf{fld} S_3$ does not hold.

Let now $\mathcal{E} = \{fx = gfx\}$ and $S = \langle u = fu \rangle$. Let $S' = \langle u = gu \rangle$ so that $S \mathbf{fld}_{\mathcal{E}} S'$ since $fu \leftrightarrow_{\mathcal{E}} gfu \xrightarrow{S} gu$. It is easy to verify that $S\gamma S'$ does not hold for any γ in $\{\mathbf{fld}, \mathbf{rewr}_{\mathcal{E}}\}^*$. Hence, $\mathbf{fld}_{\mathcal{E}} \not\subseteq \{\mathbf{fld}, \mathbf{rewr}_{\mathcal{E}}\}^*$ and $\{\mathbf{fld}_{\mathcal{E}}\}$ is strictly more powerful than $\{\mathbf{fld}, \mathbf{rewr}_{\mathcal{E}}\}$.

4.5. Proposition. *The transformation $\mathbf{ufld}_{\mathcal{E}}$ is transitive.*

The proof is similar to that of Proposition 4.3(1).

Next, we examine the $\approx_{\mathcal{E}}$ -correctness of these transformations.

4.6. Proposition. (1) *If $S \mathbf{ufld}_{\mathcal{E}} S'$, then $S \cong_{\mathcal{E}} S'$.*

(2) *If $S \mathbf{rewr}_{\mathcal{E}} S'$, then $S \approx_{\mathcal{E}} S'$.*

Proof. (1) Let $\mathbf{M} \in \mathcal{V}(\mathcal{E})$, let $m = (m_1, \dots, m_n) \in \mathbf{Sol}_{\mathbf{M}}(S)$. Since $t'_i \leftrightarrow_{S, \mathcal{E}}^* t_i$, $t'_{i\mathbf{M}}(m) = t_{i\mathbf{M}}(m) = m_i$, hence, m is a solution of S' in \mathbf{M} .

(2) As for (1), but since $S \mathbf{rewr}_{\mathcal{E}} S'$ implies $S' \mathbf{rewr}_{\mathcal{E}} S$, one also has $S' \cong_{\mathcal{E}} S$, hence, $S \approx_{\mathcal{E}} S'$. \square

Example 4.2 shows that the inequality of Proposition 4.6(1) may be strict since neither $S \approx S'$ nor $S \approx S''$ hold (this follows from Theorem 3.2).

We now define restrictions of the transformations $\mathbf{unf}_{\mathcal{E}}$, $\mathbf{fld}_{\mathcal{E}}$, and $\mathbf{ufld}_{\mathcal{E}}$ which are $\approx_{\mathcal{E}}$ -correct. The main idea is to restrict $\mathbf{ufld}_{\mathcal{E}}$ into $\mathbf{rufld}_{\mathcal{E}}$ in such a way that

$$S \mathbf{rufld}_{\mathcal{E}} S' \text{ implies } S' \mathbf{rufld}_{\mathcal{E}} S$$

and this guarantees that $S' \approx_{\mathcal{E}} S$ as in the proof of Proposition 4.6(2).

4.7. Definition. Let S, S' and \mathcal{E} be as in Definition 4.1. Let T be a nonempty subset of $[n]$ (the set of indices of the unknowns of S and S') such that $T \neq [n]$. We write $S \mathbf{runf}_{\mathcal{E}}^{(T)} S'$ if, for all i in $[n]$, the following holds:

- (1) if $i \in T$, then $t'_i = t_i$;
- (2) if $i \notin T$, then $t_i \rightarrow_{S \upharpoonright T, \mathcal{E}}^* t'_i$ where $S \upharpoonright T = \{(u_j, t_j) \mid j \in T\}$.

In words, this means that $S \mathbf{unf}_{\mathcal{E}} S'$ with the restriction that only the equations of rank j , $j \notin T$, can be transformed and this by means of \mathcal{E} and the remaining equations (i.e., those with rank in T).

Similar definitions are given for $\mathbf{rfld}_{\mathcal{E}}^{(T)}$ and $\mathbf{rufld}_{\mathcal{E}}^{(T)}$ with $\rightarrow_{S \upharpoonright T^{-1}, \mathcal{E}}$ and $\leftrightarrow_{S \upharpoonright T, \mathcal{E}}$ instead of $\rightarrow_{S \upharpoonright T, \mathcal{E}}$.

It is also convenient to write $S \mathbf{rewr}_{\mathcal{E}}^{(T)} S'$ if $S \mathbf{rewr}_{\mathcal{E}} S'$ with $t'_i = t_i$ for all i in T . Hence, $\mathbf{rewr}_{\mathcal{E}}^{(T)} \subset \mathbf{unf}_{\mathcal{E}}^{(T)}, \mathbf{fld}_{\mathcal{E}}^{(T)}, \mathbf{ufld}_{\mathcal{E}}^{(T)}$.

In some cases and especially in examples, the elements of $U = \mathbf{Unk}(S)$ have no indices (i.e., $\mathbf{Unk}(S) = \{u, v, w\}$) and we shall use for T subsets of U instead of subsets of $[\mathbf{Card}(U)]$, in an obvious way.

Finally, we let

$$S \mathbf{runf}_{\mathcal{E}} S' \text{ if } S \mathbf{runf}_{\mathcal{E}}^{(T)} S',$$

$$S \mathbf{rfld}_{\mathcal{E}} S' \text{ if } S \mathbf{rfld}_{\mathcal{E}}^{(T)} S',$$

$$S \mathbf{rufld}_{\mathcal{E}} S' \text{ if } S \mathbf{rufld}_{\mathcal{E}}^{(T)} S'$$

for some T , and these transformations are called *restricted unfolding*, *restricted folding*, and *restricted folding–unfolding*, respectively.

4.8. Proposition

- (1) $\mathbf{runf}_{\mathcal{E}}^{(T)} = \mathbf{rfld}_{\mathcal{E}}^{(T)-1}$;
- (2) $\mathbf{runf}_{\mathcal{E}}^{(T)} = \mathbf{runf}_{\mathcal{E}}^{(T)} \cdot \mathbf{rewr}_{\mathcal{E}}^{(T)}$ if \mathcal{E} is linear;
- (3) $\mathbf{rfld}_{\mathcal{E}}^{(T)} = \mathbf{rewr}_{\mathcal{E}}^{(T)} \cdot \mathbf{rfld}_{\mathcal{E}}^{(T)}$ if \mathcal{E} is linear;
- (4) $\mathbf{rufld}_{\mathcal{E}}^{(T)} = \mathbf{runf}_{\mathcal{E}}^{(T)} \cdot \mathbf{rewr}_{\mathcal{E}}^{(T)} \cdot \mathbf{rfld}_{\mathcal{E}}^{(T)}$ if \mathcal{E} is linear;
- (5) $\mathbf{runf}_{\mathcal{E}}^{(T)}$, $\mathbf{rfld}_{\mathcal{E}}^{(T)}$, and $\mathbf{rufld}_{\mathcal{E}}^{(T)}$ are transitive and $\mathbf{rufld}_{\mathcal{E}}^{(T)}$ is symmetric.

Proof. (1) Let $S \mathbf{runf}_{\mathcal{E}}^{(T)} S'$. Then, $S \upharpoonright T = S' \upharpoonright T$, hence, $t_i \rightarrow_{S \upharpoonright T}^* t'_i$ iff $t'_i \rightarrow_{S' \upharpoonright T^{-1}}^* t_i$ (for $i \notin T$).

(2) Let $S \mathbf{runf}_{\mathcal{G}}^{(T)} S'$. We look for S'' such that $S \mathbf{runf}_{\mathcal{G}}^{(T)} S'' \mathbf{rewr}_{\mathcal{G}}^{(T)} S'$. If $t_i \rightarrow_{S \uparrow T, \mathcal{G}}^* t'_i$, then $t_i \rightarrow_{S \uparrow T}^* t''_i \leftrightarrow_{\mathcal{G}}^* t'_i$ by Lemma 1.7. Hence, the result follows with $S'' = \langle u_i = t''_i; 1 \leq i \leq n \rangle$ and $t''_i = t_i$ if $i \in T$, t''_i as above if $i \notin T$.

Part (3) follows from parts (1) and (2) and the fact that $\mathbf{rewr}_{\mathcal{G}}^{(T)}$ is symmetric.

Part (4) is proved as part (2), by using Lemma 1.9.

Part (5) is proved by simple verification. \square

Remark that $\mathbf{runf}_{\mathcal{G}}$, $\mathbf{rflid}_{\mathcal{G}}$, $\mathbf{ruflid}_{\mathcal{G}}$ are not transitive and that $\mathbf{ruflid}_{\mathcal{G}}$ is symmetric.

We now establish the $\approx_{\mathcal{G}}$ -correctness of these transformations.

4.9. Proposition. *If $S \mathbf{ruflid}_{\mathcal{G}} S'$, then $S \approx_{\mathcal{G}} S'$.*

Proof. By Proposition 4.6(1) and since $\mathbf{ruflid}_{\mathcal{G}}$ is symmetric, $S \cong_{\mathcal{G}} S'$ and $S' \cong_{\mathcal{G}} S$. Hence, $S \approx_{\mathcal{G}} S'$. \square

In other words, $\mathbf{rewr}_{\mathcal{G}}$ and $\mathbf{ruflid}_{\mathcal{G}}$ are $\approx_{\mathcal{G}}$ -correct, whereas $\mathbf{uflid}_{\mathcal{G}}$ is not.

We now prove the \approx -completeness of $\{\mathbf{ruflid}\}$.

4.10. Theorem. *Let S and S' be two regular systems. Then $S \approx S'$ iff $S \mathbf{ruflid}^* S'$.*

We shall prove this by defining a \approx -canonical system S_{\approx} associated with S such that $S \mathbf{ruflid}^* S_{\approx}$. The result will follow from Proposition 2.1. Some technical definitions are needed.

4.11. Definition. Let us fix a linear order \leq on the set $\mathbf{Unk}(S)$ which is not necessarily the same as the one of \mathcal{U} (see Section 2.1). We extend it to a partial order on $M(F, U)$ by the following recursive definition:

$$t \leq t' \\ \text{iff either } t, t' \in U \text{ and } t \leq t' \text{ (w.r.t. the given order on } \mathbf{Unk}(S)), \\ \text{or } t \in U, t' \notin U, \\ \text{or } t = f(t_1, \dots, t_n), t' = f(t'_1, \dots, t'_n) \text{ and } t_i \leq t'_i \text{ for } i = 1, \dots, n.$$

4.12. Proposition. *Let S be a regular system and \leq be a linear order on $\mathbf{Unk}(S)$. There exists a unique regular system S_{\approx} such that $S \approx S_{\approx}$ and $R(S_{\approx})$ is \leq -compatible and left-irreducible. Hence, S_{\approx} is \approx -canonical.*

Proof. We shall use some technical results proved in Appendix A.

Given S let \equiv be the congruence $\leftrightarrow_{\mathcal{G}}^*$ on $M(F \cup U)$. It is F -coherent and F -simplifiable by Proposition A.2. The regular system S_{\equiv} of Proposition A.7 is the unique one such that $R(S_{\equiv})$ is left-irreducible, is \leq -compatible, and generates \equiv (i.e., such that $S \approx S_{\equiv}$). Hence, we let $S_{\approx} = S_{\equiv}$.

Since S_{\approx} is defined from $\leftrightarrow_{\mathcal{S}}^*$, $S'_{\approx} = S_{\approx}$ if S' is another system such that $\leftrightarrow_{\mathcal{S}}^*$ and $\leftrightarrow_{\mathcal{S}'}^*$ are the same, i.e., such that $S' \approx S$. Hence, S_{\approx} is \approx -canonical. \square

The last assertion of Proposition A.7 shows that if one uses another linear order on $\mathbf{Unk}(S)$, say \leq' , the corresponding system S'_{\approx} associated with S and \leq' is just a renaming of S_{\approx} and hence, that the dependence of this construction upon \leq is inessential.

Hence, from now on and for the sake of simplicity, we shall take for \leq the restriction to $\mathbf{Unk}(S)$ of the order of \mathcal{U} , i.e., $u_i \leq u_j$ iff $i \leq j$.

4.13. Proposition. *Let S be a regular system. One can effectively construct a sequence of systems S_1, \dots, S_m such that*

$$S \text{ rufld } S_1 \text{ rufld } S_2 \cdots S_m \text{ rufld } S_{\approx}.$$

Hence, the \approx -equivalence of regular systems is decidable.

Proof. *First part.* Let $S = \langle u_i = t_i; 1 \leq i \leq n \rangle$. Note that $R(S)$ is \leq -compatible iff, for all l, j in $[n]$, $t_l = u_j \Rightarrow j \geq l$ iff $d(S) = 0$, where $d(S)$ is the sum of the numbers $l - j$ such that $1 \leq j < l \leq n$ and $t_l = u_j$. If $d(S) = 0$, then there is nothing to do. Otherwise, we shall construct a sequence of systems S_1, S_2, \dots, S_k such that $S \text{ rufld}^* S_1 \text{ rufld}^* S_2 \cdots \text{rufld}^* S_k$, $d(S) > d(S_1) > \cdots > d(S_k) = 0$ (whence $R(S_k)$ is \leq -compatible). Let j and l be such that $1 \leq j < l \leq n$, $t_l = u_j$, j is minimal such that there exists such an l .

We first assume that $t_j \neq u_j$.

Let S' and S'' be the two systems with set of unknowns U and right-hand sides t'_i, t''_i , $1 \leq i \leq n$ such that

$$\begin{aligned} t'_i &= t''_i = t_i & \text{for } i \neq j, i \neq l, \\ t'_j &= u_l, & t''_j &= t_j, & t'_l &= t''_l = t_j. \end{aligned}$$

It follows that

$$S \text{ rufld}^{(j)} S'' \text{ rfld}^{(l)} S',$$

where we write (j) for $(\{j\})$. This corresponds to the transformations of $\langle \dots, u_j = t_j, \dots, u_l = u_j, \dots \rangle$ into $\langle \dots, u_j = t_j, \dots, u_l = t_j, \dots \rangle$ and then into $\langle \dots, u_j = u_l, \dots, u_l = t_j, \dots \rangle$ by a restricted unfolding followed by a restricted folding. Note that $S'' = S'$ when $t_j = u_l$.

We show that $d(S') < d(S)$. This is clear if $t_j \notin U$. Otherwise, let $t_j = u_m$. By our choice of j , we only have to consider the two cases $m \geq l$ and $l > m > j$ for which we have, respectively

$$\begin{aligned} d(S') &= d(S) - (l - j), \\ d(S') &= d(S) - (l - j) + l - m = d(S) + j - m, \end{aligned}$$

so that $d(S') < d(S)$.

If $t_j = u_j$, then we use the transformations

$$S \text{ rfld}^{(l)} S'' \text{ runf}^{(j)} S'$$

so that $S = \langle \dots, u_j = u_j, \dots, u_l = u_j, \dots \rangle$ becomes $S'' = \langle \dots, u_j = u_l, \dots, u_l = u_j, \dots \rangle$ and then becomes $S' = \langle \dots, u_j = u_l, \dots, u_l = u_l, \dots \rangle$. It is clear that $d(S') = d(S) - (l - j) < d(S)$.

In both cases, $S \text{ rufld}^2 S'$ and $d(S') < d(S)$. Hence, this transformation of S into S' can be repeated finitely many times in order to yield S_k such that $R(S_k)$ is \leq -compatible.

Second part. We now have to construct a sequence of systems giving $S_k \text{ rufld}^* S_\infty$. In order to simplify the notations we identify S_k and S for the subsequent steps.

If $R(S)$ is left-irreducible, there is nothing to do. Otherwise, there exists l and $j \neq l$ in $[n]$ such that t_j is a subterm of t_l .

There are two cases. In the first case, $t_j \neq t_l$ (i.e., t_j is a proper subterm of t_l). We let t be the result of the substitution of u_j for some occurrence of t_j in t_l (i.e., $t_l \rightarrow_{R(S)} t$). Letting $S' = \langle u_i = t'_i; 1 \leq i \leq n \rangle$ with $t'_l = t$ and $t'_i = t_i$ for $i \neq l$, we have $S \text{ rfld}^{(j)} S'$. It is clear that $R(S')$ is still compatible with \leq . Furthermore $t < t_l$, so that $(t'_1, \dots, t'_n) < (t_1, \dots, t_n)$ ($<$ is the componentwise extension of $<$ to $M(F, U)^n$).

Let us now assume that $t_j = t_l$. Without loss of generality, we can assume that $j < l$. We let $S' = \langle u_i = t'_i; 1 \leq i \leq n \rangle$ be such that $t'_j = u_l$, $t'_i = t_i$ for $i \neq j$.

Hence, $S \text{ rfld}^{(l)} S'$, $R(S')$ is compatible with \leq since $R(S)$ is so and $t'_j < t_j$, hence, $(t'_1, \dots, t'_n) < (t_1, \dots, t_n)$.

Hence, this transformation of S into S' can be repeated finitely many times, yielding a system S'_k such that $R(S'_k)$ is compatible with \leq and left-irreducible.

Since we have only used restricted foldings and unfoldings, $S'_k \approx S$. By Proposition 4.12, $S'_k = S_\infty$. Hence, we have shown how to construct a sequence of transformations giving $S \text{ rufld}^* S_\infty$. \square

Theorem 4.10 is then an immediate consequence of Propositions 2.11 and 4.13 and the fact that **rufld** is symmetric.

We now illustrate Proposition 4.13 with an example.

4.14. Example. The given system S and its successive modifications are displayed in Table 1. The equations of a system that are not written are the same as in the preceding one. The star * indicates the equation that is used to transform the system.

The system $R(S_4)$ is \leq -compatible and is obtained by

$$S \text{ runf}^{(1)} S_1 \text{ rfld}^{(4)} S'_2 \text{ runf}^{(3)} S_2 \text{ runf}^{(5)} S'_3 \text{ rfld}^{(7)} S_3 \text{ runf}^{(6)} S'_4 \text{ rfld}^{(7)} S_4.$$

The subsequent transformations eliminate the critical pairs in $R(S_4)$ (between rules 1 and 2, and 5 and 6) by

$$S_4 \text{ rfld}^{(1)} S_5 \text{ rfld}^{(7)} S_6 \text{ rfld}^{(5)} S_7 \text{ rfld}^{(6)} S_8.$$

All cases of the construction of Proposition 4.13 have been used in this example.

Table 1.

S	S_1	S'_2	S_2	S'_3	S_3	S'_4
$u_1 = u_3^*$ $u_2 = f(u_1, u_3)$ $u_3 = u_1$ $u_4 = u_3$ $u_5 = u_6$ $u_6 = f(u_1, u_1)$ $u_7 = u_5$	$u_3 = u_3$ $*$	$u_3 = u_4^*$	$u_4 = u_4$ $*$		$u_5 = u_7$ $*$	$u_7 = f(u_1, u_1)^*$
S_4	S_5	S_6	S_7	S_8		
$u_1 = u_3^*$ $u_2 = f(u_1, u_3)$ $u_3 = u_4$ $u_4 = u_4$ $u_5 = u_7$ $u_6 = u_7$ $u_7 = f(u_1, u_1)$	$u_2 = f(u_1, u_1)$ $*$	$u_2 = u_7$ $*$	$u_2 = u_5$ $*$	$u_1 = u_3$ $u_2 = u_5$ $u_3 = u_4$ $u_4 = u_4$ $u_5 = u_6$ $u_6 = u_7$ $u_7 = f(u_1, u_1)$		

A natural question is then whether Theorem 4.10 extends to $\approx_{\mathcal{E}}$ and $\mathbf{ruffld}_{\mathcal{E}}$, i.e., whether $\{\mathbf{ruffld}_{\mathcal{E}}\}$ is $\approx_{\mathcal{E}}$ -complete. The answer is no, as shown by the following example.

4.15. Example. Let $S = \langle u = gu, v = f(u, v) \rangle$ and $S' = \langle u = gu, v = h(u, v) \rangle$. Let $\mathcal{E} = \{f(gx, y) = h(x, f(x, y)), h(gx, y) = f(x, h(x, y))\}$. It is easy to verify that $S \mathbf{eq}_{\mathcal{E}} S'$:

$$f(u, v) \xrightarrow{S} f(gu, v) \xrightarrow{\mathcal{E}} h(u, f(u, v)) \xrightarrow{S^{-1}} h(u, v)$$

and similarly $f(u, v) \leftrightarrow_{S', \mathcal{E}}^* h(u, v)$.

We claim that $S \mathbf{ruffld}_{\mathcal{E}}^* S'$ does not hold. Let us assume that $S \mathbf{ruffld}_{\mathcal{E}} S_1 \mathbf{ruffld}_{\mathcal{E}} S_2 \cdots S_k$ and consider the step $S \mathbf{ruffld}_{\mathcal{E}} S_1$.

Since the first equation of S can be modified neither by \mathcal{E} , nor by the second one nor by itself, it remains unchanged in S_1 . The same argument applies to S_1, S_2 , etc. so that our initial assumption implies that $f(u, v) \leftrightarrow_{\mathcal{E} \cup R}^* h(u, v)$, where R is the (ground) rewriting system $\{u \rightarrow gu\}$. In order to prove that this is impossible let us consider the least subset M of $M(F, U)$ such that

- (1) $f(g^n u, v) \in M$ for all $n \geq 0$,
- (2) $f(g^n u, t), h(g^n u, t) \in M$ for all t in M and all $n \geq 0$.

It is easy to verify that $f(u, v) \in M$, $h(u, v) \notin M$, and $t' \in M$ whenever $t \in M$ and $t \leftrightarrow_{\mathcal{E} \cup R} t'$. Whence the result.

This example leaves the following open problem.

4.16. Problem. Find conditions on \mathcal{E} insuring that $\{\mathbf{ruffd}_{\mathcal{E}}\}$ is $\approx_{\mathcal{E}}$ -complete.

It is easy to verify (by an adaptation of the proof of Theorem 4.10) that equations of the form $f(x, y) = f(y, x)$ expressing the commutativity of binary operators satisfy the completeness requirement of Problem 4.16. But the general situation remains to be investigated.

We conclude this section with a technical result, that we include for the sake of completeness.

4.17. Definition. Let S be a regular system and $U = \mathbf{Unk}(S)$. We define an increasing sequence $U_0 \subseteq U_1 \subseteq \dots \subseteq U_i \subseteq \dots \subseteq U$ by letting

$$U_0 = \emptyset, \quad U_{i+1} = U_i \cup \{u_j \in U \mid t_j \in M(F, U_i)\}.$$

The system S is *recursion-free* if $U = \bigcup \{U_i \mid i \geq 0\}$. It is *trivial* if $U = U_1$, i.e., if the unknowns do not occur in the right-hand sides of the equations.

4.18. Proposition. (1) *Let S be a regular system. The following properties are equivalent:*

- (i) *S is recursion-free,*
- (ii) *$S \mathbf{runf}^* \bar{S}$ for some trivial system \bar{S} ,*
- (iii) *$S \mathbf{unf} \bar{S}$ for some trivial system \bar{S} ,*
- (iv) *S has at most one solution in every F -magma,*
- (v) *S has one and only one solution in every F -magma.*

The system \bar{S} of (ii) and (iii) is uniquely defined.

(2) *If S is a Greibach system, these properties are equivalent to:*

- (vi) *S has at least one solution in every F -magma.*

Proof. (i) \Rightarrow (ii): Let S be recursion-free but not trivial. Let $h(S) = \mathbf{Card}(U - U_1)$ so that $h(S) > 0$; hence, in particular, $\mathbf{Card}(U_2) > 0$.

Let $S' = \langle u_i = t'_i; 1 \leq i \leq n \rangle$ be the system such that $t'_i = t_i$ if $u_i \in U_1$ and $t'_i = t_i[t_j/u_j; u_j \in U_1]$ if $u_i \notin U_1$. Hence, $S \mathbf{runf}^{(U_1)} S'$ and $h(S') = h(S) - \mathbf{Card}(U_2) < h(S)$. Note also that S' is recursion-free. This step can be iterated until one obtains a trivial system \bar{S} and one has $S \mathbf{runf}^* \bar{S}$.

(ii) \Rightarrow (iii): By Proposition 4.3(1) and Definition 4.7, this easily follows.

(iii) \Rightarrow (iv): It is clear that \bar{S} has at most one solution in any F -magma \mathbf{M} . Hence, the same holds for S since $\mathbf{Sol}_{\mathbf{M}}(S) \subseteq \mathbf{Sol}_{\mathbf{M}}(\bar{S})$ (by Proposition 4.6(1)).

The unicity of \bar{S} follows since if $\bar{S} = \langle u_i = \bar{t}_i; 1 \leq i \leq n \rangle$, the n -tuple $(\bar{t}_1, \dots, \bar{t}_n)$ is the solution of \bar{S} (and of S) in $M(F)$.

(iv) \Rightarrow (i): If S is not recursion-free, one can define an F -magma \mathbf{M} with domain $\{a, b, b'\}$ and two distinct solutions of S in \mathbf{M} . One lets $m = (m_1, \dots, m_n)$ with $m_i = a$

if $u_i \in U' = \bigcup \{U_j \mid j \geq 0\}$ and $m_i = b$ if $u_i \notin U'$, and one defines m' similarly with b' instead of b .

For defining \mathbf{M} it suffices to take:

$$f_{\mathbf{M}}(d_1, \dots, d_k) = \begin{cases} a & \text{if } k=0 \text{ or } d_1 = d_2 = \dots = d_k = a, \\ b & \text{if } d_i = b \text{ for some } i = 1, \dots, k, \\ b' & \text{if } d_i = b' \text{ for some } i \text{ and } d_j \in \{a, b'\} \text{ for all } j \neq i. \end{cases}$$

(v) \Rightarrow (iv): This implication is trivial.

(ii) \Rightarrow (v): This follows from Proposition 4.9 and the fact that \bar{S} has one and only one solution.

(2) Let S be a Greibach system.

(v) \Rightarrow (vi): This implication is trivial.

(vi) \Rightarrow (i): If S is not recursion-free, there exists a rewriting sequence $u_i \rightarrow_S^+ t$ for some u_i in U , some t in $F(M(F, U))$ having at least one occurrence of u_i . Hence, $u_i \approx_S t$. Hence, S cannot have any solution (m_1, \dots, m_n) in $M(F)$ since one would have for such a solution $|m_i| = |t[m_1/u_1, \dots, m_n/u_n]| > |m_i|$. Hence, (vi) does not hold. \square

This result should not have surprised anybody accustomed to manipulating context-free grammars and recursive program schemes. Its present formulation includes in particular [75, Proposition 1].

5. Comparing regular systems with respect to their least solutions

We now consider the relations $t \sim_{S, \mathcal{E}} t'$, $S \preceq_{\mathcal{E}} S'$, $S \sim_{\mathcal{E}} S'$ by which systems can be compared with respect to their least solutions in all ω -complete F -magmas satisfying some set \mathcal{E} of equations.

5.1. Definition. Let S be a regular system (of the general form of Section 2.1). For every ω -complete F -magma \mathbf{M} , this system has a least solution (m_1, m_2, \dots, m_n) in \mathbf{M}^n , denoted by $\mu\text{-Sol}_{\mathbf{M}}(S)$ and characterized as $\text{Sup}_{i \geq 0} S_{\mathbf{M}}^i(\perp_{\mathbf{M}}^n)$ (see Section 2.2). In the F -magma $\mathbf{M}_{\Omega}^{\infty}(F)$, this least solution is an n -tuple of trees, $T(S) = (T(S, u_1), \dots, T(S, u_n))$. These trees are *regular*, i.e., they only have finitely many distinct subtrees. See for instance [26] for a systematic study of regular trees.

Since $\mathbf{M}_{\Omega}^{\infty}(F)$ is the initial ω -complete F -magma [54], there exists for any ω -complete F -magma \mathbf{M} a unique ω -continuous homomorphism $h_{\mathbf{M}}: \mathbf{M}_{\Omega}^{\infty}(F) \rightarrow \mathbf{M}$. (The notation $t_{\mathbf{M}}$ will also be used for $h_{\mathbf{M}}(t)$.)

5.2. Proposition. For every regular system S as above, for every ω -complete F -magma \mathbf{M} , $\mu\text{-Sol}_{\mathbf{M}}(S) = h_{\mathbf{M}}(\mu\text{-Sol}_{\mathbf{M}_{\Omega}^{\infty}(F)}(S))$, i.e., $\mu\text{-Sol}_{\mathbf{M}}(S) = (h_{\mathbf{M}}(T(S, u_1)), \dots, h_{\mathbf{M}}(T(S, u_n)))$.

This proposition is just a special case of the following one, proved (as Lemma 5.3) in a slightly less general situation in [73] (see also Section 16.3).

5.3. Lemma. *Let S be a regular system over F . Let \mathbf{M} and \mathbf{M}' be two ω -complete F -magmas and $h: \mathbf{M} \rightarrow \mathbf{M}'$ a homomorphism of ω -complete F -magmas such that $h(\perp_{\mathbf{M}}) = \perp_{\mathbf{M}'}$. Then, $\mu\text{-Sol}_{\mathbf{M}'}(S) = h(\mu\text{-Sol}_{\mathbf{M}}(S))$. Hence, $t \sim_{S, \mathbf{M}} t'$ implies $t \sim_{S, \mathbf{M}'} t'$.*

Proof. It is easy to see that $h(S_{\mathbf{M}}(x)) = S_{\mathbf{M}'}(h(x))$ for all x in \mathbf{M}^n and since $h(\perp_{\mathbf{M}}) = \perp_{\mathbf{M}'}$, $h(S_{\mathbf{M}}^i(\perp_{\mathbf{M}}^n)) = S_{\mathbf{M}'}^i(\perp_{\mathbf{M}'}^n)$ for all i . Hence, by the continuity of h ,

$$\begin{aligned} \mu\text{-Sol}_{\mathbf{M}'}(S) &= \text{Sup}_i(S_{\mathbf{M}'}^i(\perp_{\mathbf{M}'}^n)) = \text{Sup}_i h(S_{\mathbf{M}}^i(\perp_{\mathbf{M}}^n)) \\ &= h\left(\text{Sup}_i(S_{\mathbf{M}}^i(\perp_{\mathbf{M}}^n))\right) = h(\mu\text{-Sol}_{\mathbf{M}}(S)). \end{aligned}$$

The second assertion immediately follows. Note the difference with Remark 3.7. \square

We can now state our characterizations of $t \sim_{S, \mathcal{E}} t'$ and $S \leq_{\mathcal{E}} S'$ (whence of $S \sim_{\mathcal{E}} S'$), where S' denotes a regular system of the form $\langle u_i = t'_i; 1 \leq i \leq n \rangle$ and s_i denotes $T(S, u_i)$ for all $i = 1, \dots, n$. For t in $M(F, \{u_1, \dots, u_n\})$, we denote by $T(S, t)$ the tree $t[s_1/u_1, \dots, s_n/u_n]$ (it is infinite in general). The free ω -complete F -magma satisfying \mathcal{E} is denoted by $\mathbf{M}_{\mathcal{E}}$ (its definition is recalled in Lemma 1.5).

5.4. Theorem. (1) *For t, t' in $M(F, U)$, $t \sim_{S, \mathcal{E}} t'$ iff $t \sim_{S, \mathbf{M}_{\mathcal{E}}} t'$ iff $T(S, t) \equiv_{\mathcal{E}} T(S, t')$.*
 (2) *$S \leq_{\mathcal{E}} S'$ iff $S \leq_{\mathbf{M}_{\mathcal{E}}} S'$ iff $s_i \equiv_{\mathcal{E}} T(S, t'_i)$ for all $i = 1, \dots, n$.*

Proof. (1) Let $t \in M(F, U)$, let $\mathbf{M} \in \mathcal{V}^{\omega}(\mathcal{E})$ and (m_1, \dots, m_n) be the least solution of S in \mathbf{M} . It follows from Proposition 5.2 that $t_{\mathbf{M}}(m_1, \dots, m_n) = h_{\mathbf{M}}(t[s_1/u_1, \dots, s_n/u_n])$, where $h_{\mathbf{M}}$ is the unique ω -continuous homomorphism: $\mathbf{M}_{\Omega}^{\infty}(F) \rightarrow \mathbf{M}$. Hence, by taking $\mathbf{M} = \mathbf{M}_{\mathcal{E}}$, one gets

$$\begin{aligned} t \sim_{S, \mathbf{M}_{\mathcal{E}}} t' &\text{ iff } h_{\mathbf{M}_{\mathcal{E}}}(t[s_1, \dots, s_n]) = h_{\mathbf{M}_{\mathcal{E}}}(t'[s_1, \dots, s_n]) \\ &\text{ iff } t[s_1, \dots, s_n] \equiv_{\mathcal{E}} t'[s_1, \dots, s_n] \quad (\text{by Lemma 1.5}). \end{aligned}$$

It is clear that $t \sim_{S, \mathcal{E}} t'$ implies $t \sim_{S, \mathbf{M}_{\mathcal{E}}} t'$ and the converse holds by the second assertion of Lemma 5.3 since for every \mathbf{M} in $\mathcal{V}^{\omega}(\mathcal{E})$ there exists an ω -continuous homomorphism: $\mathbf{M}_{\mathcal{E}} \rightarrow \mathbf{M}$.

Part (2) immediately follows from part (1) and the definitions. \square

5.5. Proposition. (1) *The relations $t \sim_S t'$, $S \leq S'$, and $S \sim S'$ are decidable.*

(2) *The relations $t \sim_{S, \mathcal{E}} t'$, $S \leq_{\mathcal{E}} S'$, and $S \sim_{\mathcal{E}} S'$ are not semidecidable (hence, they are undecidable).*

Proof. (1) If $\mathcal{E} = \emptyset$, then $\equiv_{\mathcal{E}}$ is just the equality in $\mathbf{M}_{\Omega}^{\infty}(F)$ and properties $t \sim_S t'$ and $S \leq_S S'$ are decidable since the equality of two regular trees is decidable [26, 30].

(2) The undecidability of $t \sim_{S, \mathcal{E}} t'$ will be shown below (Proposition 13.8). The cases $S \leq_{\mathcal{E}} S'$ and $S \sim_{\mathcal{E}} S'$ follow from this one by Lemma 3.4. \square

Rather than on decidability questions, we shall concentrate our attention (in the next section) on $\sim_{\mathcal{E}}$ -correct transformations, and their possible $\sim_{\mathcal{E}}$ -completeness.

Theorem 5.4(2) yields the following characterization:

$$S \sim_{\mathcal{E}} S' \text{ iff } t_i[s_1, \dots, s_n] \equiv_{\mathcal{E}} t'_i[s_1, \dots, s_n] \text{ and} \\ t_i[s'_1, \dots, s'_n] \equiv_{\mathcal{E}} t'_i[s'_1, \dots, s'_n] \text{ for all } i = 1, \dots, n$$

(where $(s_1, \dots, s_n) = T(S)$ and $(s'_1, \dots, s'_n) = T(S')$) which is analogous to Corollary 3.6(1). But since $t \equiv_{\mathcal{E}} t'$ is not semidecidable in general (for regular trees t and t'), this characterization cannot be considered as defining a transformation rule as **eq** _{\mathcal{E}} did. Furthermore, Proposition 5.5(2) shows that there does not exist any recursively enumerable set of transformations which is $\sim_{\mathcal{E}}$ -complete (for arbitrary finite sets \mathcal{E}), otherwise, $\sim_{\mathcal{E}}$ would be semidecidable which is not the case.

We conclude this section with three technical results helping to establish some facts like $t \sim_{S, \mathcal{E}} t'$ or $S \sim_{\mathcal{E}} S'$. The first one is the so-called Scott's Induction Principle ([34, 58]; some works (e.g. [68]) attribute it also to De Bakker and Scott [5]).

5.6. Definition (Scott's Induction Principle). Let S be a regular system, $\mathbf{M} \in \mathcal{V}^{\omega}$ and $(m_1, \dots, m_n) = \mu\text{-Sol}_{\mathbf{M}}(S)$. Let $P(x_1, \dots, x_n)$ be an n -ary predicate on \mathbf{M} . We do not specify any logical calculus in which P is written; we only assume that, for all x_1, \dots, x_n in \mathbf{M} , $P(x_1, \dots, x_n)$ is either true or false.

We say that P is ω -continuous if, for every n -tuple $(d_1^{(j)}, \dots, d_n^{(j)})$ of increasing sequences in \mathbf{M} (i.e., $d_i^{(j)} \leq d_i^{(j')}$ for all $i \in [n]$, all $0 \leq j \leq j'$), it holds that if $P(d_1^{(j)}, \dots, d_n^{(j)})$ is true for all $j \geq 0$, then $P(d_1, \dots, d_n)$ is true, where $d_i = \text{Sup}_j d_i^{(j)}$.

We say that P is S -inductive if the following conditions hold in \mathbf{M} :

- (1) $P(\perp_{\mathbf{M}}, \dots, \perp_{\mathbf{M}})$,
- (2) $\forall x_1, \dots, x_n [P(x_1, \dots, x_n) \Rightarrow P(t_1, \dots, t_n)]$.

Condition (2) is just a short writing for

(2') For all x_1, \dots, x_n in M , if $P(x_1, \dots, x_n)$ is true, then so is $P(t_{1\mathbf{M}}(x_1, \dots, x_n), \dots, t_{n\mathbf{M}}(x_1, \dots, x_n))$.

Scott's Induction Principle is based on the following proposition and consists in establishing the validity of $P(m_1, \dots, m_n)$ by verifying that P is ω -continuous and S -inductive.

5.7. Proposition. *If P is ω -continuous and S -inductive, then $P(\mu\text{-Sol}_{\mathbf{M}}(S))$ holds.*

Proof. The hypothesis allows to prove by induction on j that $P(a_1^{(j)}, \dots, a_n^{(j)})$ holds for all $j \geq 0$, where $(a_1^{(j)}, \dots, a_n^{(j)}) = S_{\mathbf{M}}^j(\perp_{\mathbf{M}}, \dots, \perp_{\mathbf{M}})$.

Since $m_i = \text{Sup}_j (a_i^{(j)})$, the ω -continuity of P shows that $P(m_1, \dots, m_n)$ holds. \square

Our second technical result will allow us to define a new $\sim_{\mathcal{E}}$ -correct transformation. (It uses the notations of Section 1.6.)

5.8. Proposition. *Let \mathcal{E} be a set of equations, let $S = \langle u_i = t_i; 1 \leq i \leq n \rangle$ and $S' = \langle u_i = t'_i; 1 \leq i \leq n \rangle$ be two regular systems, let $q_i \in M(F, \text{Unk}(S))$ for all i in $[n]$. For all \mathbf{M} in \mathcal{V} and $m \in M^n$, let $q_{\mathbf{M}}(m) = (q_{1\mathbf{M}}(m), \dots, q_{n\mathbf{M}}(m))$.*

(1) *If $q_i[t_1/u_1, \dots, t_n/u_n] \leftrightarrow_{\mathcal{E}}^* t'_i[q_1/u_1, \dots, q_n/u_n]$ for all i in $[n]$, then $q_{\mathbf{M}}(m) \in \text{Sol}_{\mathbf{M}}(S')$ for all \mathbf{M} in $\mathcal{V}(\mathcal{E})$ and all m in $\text{Sol}_{\mathbf{M}}(S)$.*

Let us now assume that $\Omega \in F$ and that $\mathbf{M} \in \mathcal{V}^{\omega}(\mathcal{E})$.

(2) *If, for all i , $q_i[t_1/u_1, \dots, t_n/u_n] \equiv_{\mathcal{E}} t'_i[q_1/u_1, \dots, q_n/u_n]$ and $q_i[\Omega/u_1, \dots, \Omega/u_n] \leq_{\mathcal{E}}^0 t'_i{}^p[\Omega/u_1, \dots, \Omega/u_n]$ for some $p \geq 0$, then $q_{\mathbf{M}}(\mu\text{-Sol}_{\mathbf{M}}(S)) = \mu\text{-Sol}_{\mathbf{M}}(S')$.*

In this proposition, $t'_i{}^0 = u_i$ and $t'_i{}^{p+1} = t'_i[t'_1{}^p/u_1, \dots, t'_n{}^p/u_n]$ so that $S'^p = \langle u_i = t'_i{}^p; i \in [n] \rangle$ is the p th iterate of S' , $(S'^p)_{\mathbf{M}} = (S'_{\mathbf{M}})^p$ and $S'_{\mathbf{M}}{}^p(\perp_{\mathbf{M}}^n)$ is the so-called Kleene-sequence of S' in \mathbf{M} (see [56, 76]).

Proof of Proposition 5.8. Part (1) is easily verified from the hypotheses.

(2) From (1), we have $q_{\mathbf{M}}(\mu\text{-Sol}_{\mathbf{M}}(S)) \supseteq \mu\text{-Sol}_{\mathbf{M}}(S')$. For the opposite inequality, one can apply Scott's Induction Principle to the system S and the formula

$$q_{\mathbf{M}}(x_1, \dots, x_n) \leq \mu\text{-Sol}_{\mathbf{M}}(S').$$

The verifications are easy. \square

5.9. Remark. In Proposition 5.8(1), the inequality may be strict. Take for example: $S = \langle u = fu \rangle$, $S' = \langle u = hu \rangle$, \mathbf{M} with domain $M = \{a, b\}$, and $f_{\mathbf{M}}(a) = f_{\mathbf{M}}(b) = a$, $h_{\mathbf{M}}(a) = a$, $h_{\mathbf{M}}(b) = b$. Then, $\mathbf{M} \in \mathcal{V}(\mathcal{E})$, where $\mathcal{E} = \{ffx = hfx\}$. Let now $q = fu$. Then, $q[fu] \leftrightarrow_{\mathcal{E}} hq$. The unique solution of S in \mathbf{M} is a and $q_{\mathbf{M}}(a) = f_{\mathbf{M}}(a) = a$ is also a solution of S' . However, S' has another solution in \mathbf{M} , namely b .

In case (2), the second hypothesis cannot be omitted. It suffices to take $b = \Omega_{\mathbf{M}}$ in the above example. Then the least solution of S is a . Hence, $q_{\mathbf{M}}(\mu\text{-Sol}_{\mathbf{M}}(S)) = a$. And, clearly, $\mu\text{-Sol}_{\mathbf{M}}(S') = b$.

5.10. Definition. Let us assume that the systems S and S' of Proposition 5.8 have a common subset of equations $S'' = S \upharpoonright U'' = S' \upharpoonright U''$ for some $U'' \subseteq U$. Let $U' = U - U''$. In order to state in a simpler way the subsequent conditions, we assume without loss of generality that $U' = \{u_1, \dots, u_k\}$ and that $U'' = \{u_{k+1}, \dots, u_n\}$. Hence, $t'_i = t_i$ for all $i = k+1, \dots, n$. We also assume the following conditions for all i in $[k]$:

- (1) $t'_i \in M(F, \{u_1, \dots, u_k\})$,
- (2) $t_i[\Omega/u_1, \dots, \Omega/u_n] \leq_{\mathcal{E}}^0 t'_i{}^p[\Omega/u_1, \dots, \Omega/u_k]$ for some $p \geq 0$,
- (3) $t_i[t_1/u_1, \dots, t_n/u_n] \equiv_{\mathcal{E}} t'_i[t_1/u_1, \dots, t_k/u_k]$.

If all these conditions hold, up to a renaming of the unknowns, we write S $\text{redef}_{\mathcal{E}} S'$ and we say that S' is obtained by a *redefinition* of (certain unknowns of) S .

Actually, the equations $u_i = t'_i$ for $i = 1, \dots, k$ are satisfied by the least solution of S and are taken as new defining equations for u_1, \dots, u_k in S' .

5.11. Remark. This transformations can be used with $U'' = \emptyset$. Consider, for example,

$$S = \langle u = \Omega, v = f(v, \Omega) \rangle, \quad S' = \langle u = u, v = f(v, u) \rangle.$$

Then conditions (1), (2), and (3) hold with $U'' = \emptyset$ (and $\mathcal{E} = \emptyset$). This fact will be exploited in Proposition 5.16.

The following result is an easy corollary of Proposition 5.8.

5.12. Corollary. *If S redef $_{\mathcal{E}}$ S' , then $S \sim_{\mathcal{E}} S'$.*

Proof. We apply Proposition 5.8 with $q_i = t_i$ for $i = 1, \dots, n$.

The condition $q_i[t_1, \dots, t_n] \equiv_{\mathcal{E}} t'_i[q_1, \dots, q_n]$ of Proposition 5.8(2) is trivially satisfied if $i = k+1, \dots, n$ and it follows from condition (3) if $i \in [k]$.

Condition $q_i[\Omega, \dots, \Omega] \leq_{\mathcal{E}}^0 t'_i{}^p[\Omega, \dots, \Omega]$ of Proposition 5.8(2) follows from condition (2) and the definition of (q_1, \dots, q_n) .

Hence, Proposition 5.8(2) yields, if $(m_1, \dots, m_n) = \mu\text{-Sol}_{\mathbf{M}}(S)$, $(m'_1, \dots, m'_n) = \mu\text{-Sol}_{\mathbf{M}}(S')$,

$$q_{\mathbf{M}}(\mu\text{-Sol}_{\mathbf{M}}(S)) = \mu\text{-Sol}_{\mathbf{M}}(S'),$$

whence the result follows since $q_{\mathbf{M}}(\mu\text{-Sol}_{\mathbf{M}}(S)) = \mu\text{-Sol}_{\mathbf{M}}(S)$. \square

5.13. Remark. Let redef' $_{\mathcal{E}}$ be the transformation defined exactly as redef $_{\mathcal{E}}$ with $\leftrightarrow_{\mathcal{E}}^*$ instead of $\equiv_{\mathcal{E}}$ in Definition 5.10(3). Then, redef' $_{\mathcal{E}} \subseteq \text{ufld}_{\mathcal{E}}$. To see this, note that conditions (1) to (3) of Definition 5.10 (with $\leftrightarrow_{\mathcal{E}}^*$ instead of $\equiv_{\mathcal{E}}$) imply the following:

$$S = \langle u_1 = t_1, \dots, u_k = t_k, u_k = t_{k+1}, \dots \rangle,$$

$$S' = \langle u_1 = t'_1, \dots, u_k = t'_k, u_k = t_{k+1}, \dots \rangle,$$

and, for all i in $[k]$,

$$t_i \xrightarrow[S]{*} t_i[t_1/u_1, \dots, t_n/u_n] \xleftrightarrow[\mathcal{E}]{*} t'_i[t_1/u_1, \dots, t_k/u_k] \xleftarrow[S]{*} t'_i.$$

Hence, $S \text{ufld}_{\mathcal{E}} S'$ (but $S \text{rufld}_{\mathcal{E}} S'$ does not hold). Note also that $S \text{redef}_{\mathcal{E}} S'$ implies $S \text{ufld}_{\mathcal{E}'} S'$ where \mathcal{E}' is the restriction of $\equiv_{\mathcal{E}}$ to $M_{\Omega}(F, X)$.

Our third technical result concerns the powersingular unknowns of a regular system. The proof of the following proposition is another example of the use of Scott's Induction Principle.

Let us precise that F is a ranked alphabet which *does not* contain the special constant Ω . We denote by F_{Ω} the ranked alphabet $F \cup \{\Omega\}$.

5.14. Proposition. *Let S be a regular system over F and $u \in U = \mathbf{Unk}(S)$. The following properties are equivalent:*

- (1) $u \sim_S \Omega$;
- (2) u is powersingular;
- (3) there is no t in $F(M(F, U))$ such that $u \rightarrow_S^* t$.

Proof. (2) \Rightarrow (1): Let \mathbf{M} be an ω -complete F -magma. Let $P(x_1, \dots, x_n)$ be the following property

$$\bigwedge \{x_i = \perp_{\mathbf{M}} \mid u_i \in \mathbf{Psing}(S)\}.$$

Since $u_i \in \mathbf{Psing}(S)$ implies $t_i \in \mathbf{Psing}(S)$, the property P is S -inductive. It is also ω -continuous, hence, true. Since it is true for all \mathbf{M} , $u_i \sim_S \Omega$ if u_i is powersingular.

(3) \Rightarrow (2): This is proved by an easy argument.

(1) \Rightarrow (3): Let $t \in F(M(F, U))$ such that $u \rightarrow_S^* t$. Since $u \sim_S t$, $T(S, u) = T(S, t) \in F(M_\Omega^\infty(F))$. Hence, $T(S, u) \neq \Omega$ and $u \not\sim_S \Omega$. \square

5.15. Definition. Let S be a regular system S over F_Ω . We denote by $\mathbf{Unk}_\Omega^-(S)$ the set of unknowns u of $\mathbf{Unk}(S)$ such that $u \sim_S \Omega$ and by $\mathbf{Unk}_\Omega^+(S)$ the set $\mathbf{Unk}(S) - \mathbf{Unk}_\Omega^-(S)$.

The system S is \sim -reduced if, for all i in $[n]$,

- (1) $t_i \in M(F_\Omega, \mathbf{Unk}_\Omega^+(S))$,
- (2) $t_i = \Omega$ iff $u_i \in \mathbf{Unk}_\Omega^-(S)$.

With any system S we can associate a system $\mathbf{Red}_\Omega(S) = \langle u_i = t'_i; i \in [n] \rangle$ by letting $t'_i = t_i[\Omega/u; u \in \mathbf{Unk}_\Omega^-(S)]$.

5.16. Proposition. $S \text{ redef}^{-1} \mathbf{Red}_\Omega(S)$. Hence, $\mathbf{Red}_\Omega(S) \sim S$ and $\mathbf{Red}_\Omega(S)$ is \sim -reduced.

Proof. Let us verify conditions (1), (2), and (3) of Definition 5.10 with S for S' , $\mathbf{Red}_\Omega(S)$ for S , and $U'' = \emptyset$ (i.e., $k = n$). Condition (1) is trivially true, condition (2) holds with $p = 1$.

For every $s \in M_\Omega(F, \mathbf{Unk}(S))$, let $\bar{s} = s[\Omega/u; u \in \mathbf{Unk}_\Omega^-(S)]$. By using an induction on the structure of s , one can prove that

$$\bar{s}[t'_1/u_1, \dots, t'_n/u_n] = s[t'_1/u_1, \dots, t'_n/u_n]. \quad (1)$$

If $s \in \mathbf{Unk}_\Omega^-(S)$, then $\bar{s} = \Omega$ and $s = u_j$ with $t'_j = \Omega$, hence, (1) holds. If $s \in \mathbf{Unk}(S) - \mathbf{Unk}_\Omega^-(S)$, then $\bar{s} = s$, hence, (1) holds. The case $s = f(s_1, \dots, s_m)$, $f \in F_\Omega$ easily follows by induction. This proves (1).

Then one proves condition (3) of Definition 5.10 by taking for s the terms t_1, \dots, t_n (so that $\bar{t}_i = t'_i$ for all $i = 1, \dots, n$). \square

6. System transformations and \sim -equivalence

We already know several $\sim_{\mathcal{E}}$ -correct transformations of regular systems. We shall define another one, **eunf** called the extended unfolding. We shall also prove that **eunf** is $\sim_{\mathcal{E}}$ -correct.

Since the $\sim_{\mathcal{E}}$ -equivalence of regular systems is not semidecidable, there is no hope to find any finite (or even recursively enumerable) set of transformations (depending on \mathcal{E}) that would be $\sim_{\mathcal{E}}$ -complete. But we shall find one, namely $\{\mathbf{eunf}, \mathbf{eunf}^{-1}\}$, for the special case where $\mathcal{E} = \emptyset$ (recall that $S \sim S'$ is decidable).

The following proposition collects easy consequences of already proved results (Propositions 4.6(1), 4.9, and 5.12).

6.1. Proposition. *Let S, S' be two regular systems and let \mathcal{E} be a set of equations.*

- (1) *If $S \mathbf{rufld}_{\mathcal{E}} S'$, then $S' \sim_{\mathcal{E}} S$.*
- (2) *If $S \mathbf{ufld}_{\mathcal{E}} S'$, then $S \preceq_{\mathcal{E}} S'$, i.e., $\mu\text{-Sol}_{\mathbf{M}}(S') \leq \mu\text{-Sol}_{\mathbf{M}}(S)$ for \mathbf{M} in $\mathcal{V}^{\omega}(\mathcal{E})$.*
- (3) *If $S \mathbf{redef}_{\mathcal{E}} S'$, then $S' \sim_{\mathcal{E}} S$.*

Here is the new transformation.

6.2. Definition. Let S be a regular system of the usual form and $S' = \langle u_i = t'_i; 1 \leq i \leq n \rangle$. Let $I(S)$ be the ground rewriting system $\{(t_j, u_j) \mid j \in [n] \text{ and } t_j \in U\}$. We say that S' derives from S by *extended unfolding* if, for all $i = 1, \dots, n$,

- (1) $u_i \xrightarrow[S \cup I(S)]{*} t'_i$,
- (2) $\mathbf{PSing}(S') \subseteq \mathbf{PSing}(S)$.

We denote this by $S \mathbf{eunf} S'$.

By Lemma 1.8(2), condition (1) is equivalent to

$$u_i \xrightarrow[S]{*} t \xrightarrow[I(S)]{*} t'_i \quad \text{for some } t$$

and yields two cases:

- (1') $t_i \xrightarrow[S]{*} t \xrightarrow[I(S)]{*} t'_i$ for some t ,
- (1'') $u_i \xrightarrow[I(S)]{*} t'_i$.

Case (1') means that in addition to the usual unfoldings one uses some foldings associated with the non-Greibach equations. In case (1'') one only uses these foldings. Hence, clearly, $S \mathbf{eunf} S'$ implies $S \mathbf{ufld} S'$. But this does not guarantee that $S \sim S'$. Hence, we have introduced **eunf** separately.

Condition (2) is necessary to guarantee that $S' \sim S$. As a counterexample, consider

$$S = \langle u = v, v = w, w = gw \rangle, \quad S' = \langle u = v, v = u, w = gw \rangle$$

and note that condition (1) holds, but

$$\mathbf{Psing}(S) = \emptyset, \quad \mathbf{Psing}(S') = \{u, v\}$$

so that (by Proposition 5.14) S is not \sim -equivalent to S' .

Finally, condition (1) implies $\mathbf{Psing}(S) \subseteq \mathbf{Psing}(S')$, hence, $\mathbf{Psing}(S') = \mathbf{Psing}(S)$ if $S \mathbf{eunf} S'$.

6.3. Proposition. (1) *The transformation \mathbf{eunf} is \sim -correct.*

(2) *The transformation \mathbf{unf}_g is \sim_g -correct.*

Proof. (1) Let $S = \langle u_i = t_i; i \in [n] \rangle$ and $S' = \langle u_i = t'_i; i \in [n] \rangle$ be such that $S \mathbf{eunf} S'$. Then, $S \mathbf{ufld} S'$ and $S \preceq S'$ by Proposition 6.1(2), i.e., if $(m_1, \dots, m_n) = \mu\text{-Sol}_M(S)$ and $(m'_1, \dots, m'_n) = \mu\text{-Sol}_M(S')$ (for some ω -complete F -magma M), then $m'_i \leq_M m_i$ for all $i = 1, \dots, n$.

In order to establish the opposite inequalities, we let $P(x_1, \dots, x_n)$ denote the property defined by

$$(i) \quad \forall i \in [n], \forall w \in T_i: x_i \leq_M w_M(m'_1, \dots, m'_n),$$

where

$$\begin{aligned} T_i &= \left\{ w \in M(F, U) \mid u_i \xrightarrow[S \cup I(S)]{*} w \right\} \\ &= \left\{ w \in M(F, U) \mid u_i \xrightarrow[S]{*} w' \xrightarrow[I(S)]{*} w \text{ for some } w' \text{ in } M(F, U) \right\}, \end{aligned}$$

and $U = \{u_1, \dots, u_n\}$.

We want to establish the validity of $P(m_1, \dots, m_n)$ by Scott's Induction Principle (see Definition 5.6). It is clear that P is ω -continuous and that $P(\perp_M, \dots, \perp_M)$ holds. We verify that condition (2) of Definition 5.6 holds. Let $x_1, \dots, x_n \in M$ satisfy (i). We have to show that, for all i , all w in T_i ,

$$(ii) \quad t_{iM}(x_1, \dots, x_n) \leq_M w_M(m'_1, \dots, m'_n).$$

There are two cases:

Case 1: $u_i \rightarrow_S t_i \xrightarrow[S \cup I(S)]{*} w$. This means that $w \in t_i[\text{OI } T_1/u_1, \dots, T_n/u_n]$. Since, by (i), $x_j \leq_M w'_M(m'_1, \dots, m'_n)$ for all w' in T_j , we have

$$t_{iM}(x_1, \dots, x_n) \leq_M t_M(m'_1, \dots, m'_n),$$

for all t in $t_i[\text{OI } T_1/u_1, \dots, T_n/u_n]$, hence, in particular, for $t = w$. This establishes (ii).

Case 2: $u_i \xrightarrow[I(S)]{*} w = u_j$. This means that $u_j \xrightarrow[S]{*} u_i$. We must prove that

$$(iii) \quad t_{iM}(x_1, \dots, x_n) \leq_M m'_j = t'_{jM}(m'_1, \dots, m'_n).$$

There are two subcases.

Subcase 2.1: u_i and u_j belong to $\mathbf{Psing}(S') = \mathbf{Psing}(S)$. Then $m'_i = \perp_M$, whence $x_i = \perp$, for all u_i in $\mathbf{Psing}(S')$. Since $t_i \in \mathbf{Psing}(S') = \mathbf{Psing}(S)$, (iii) holds.

Subcase 2.2: u_i and u_j do not belong to $\mathbf{P}\text{sing}(S')$. This means that for some j_1, \dots, j_m in $[n]$ one has

$$(iv) \quad u_j = u_{j_1} \xrightarrow{S'} t'_{j_1} = u_{j_2} \xrightarrow{S'} t'_{j_2} = u_{j_3} \xrightarrow{S'} \cdots \xrightarrow{S'} t'_{j_m},$$

with t'_{j_m} not in U . Hence,

$$u_j = u_{j_1} \xrightarrow{S \cup I(S)^*} u_{j_2} \xrightarrow{S \cup I(S)^*} \cdots \xrightarrow{S \cup I(S)^*} u_{j_m} \xrightarrow{S \cup I(S)^*} t'_{j_m}$$

and, by a previous remark,

$$u_j \xrightarrow{S^*} t \xrightarrow{I(S)^*} t'_{j_m},$$

for some t , and t cannot be in U .

Since $u_j \xrightarrow{S^*} u_i$, one necessarily has $u_i \xrightarrow{S^+} t$, hence, $u_i \xrightarrow{S \cup I(S)^+} t'_{j_m}$. The proof of Case 1 gives

$$t_{iM}(x_1, \dots, x_n) \leq_M t'_{j_m M}(m'_1, \dots, m'_n).$$

From (iv) we have

$$m'_j = m'_{j_2} = \cdots = m'_{j_m} = t'_{j_m M}(m'_1, \dots, m'_n),$$

hence, (iii) is proved.

We have shown that P is S -inductive. Hence, $P(m_1, \dots, m_n)$ holds by Proposition 5.7. By taking $w = u_i$ in (i), one gets $m_i \leq_M m'_i$ for all i .

(2) Letting S and S' be as in part (1), we now assume that $S \text{ unif}_{\mathcal{E}} S'$ and we prove in a similar way that $S' \sim_{\mathcal{E}} S$.

We let $M \in \mathcal{V}^\omega(\mathcal{E})$, $(m_1, \dots, m_n) = \mu\text{-Sol}_M(S)$ and $(m'_1, \dots, m'_n) = \mu\text{-Sol}_M(S')$. As in (1), the inequality $\mu\text{-Sol}_M(S') \leq \mu\text{-Sol}_M(S)$ is immediate. In order to obtain the opposite inequality we consider the property $Q(x_1, \dots, x_n)$ defined as the conjunction of $Q_1(x_1, \dots, x_n)$:

$$\bigwedge \{x_i \leq t_{iM}(x_1, \dots, x_n) \mid 1 \leq i \leq n\}$$

and of $Q_2(x_1, \dots, x_n)$:

$$\bigwedge \{x_i \leq w_M(m'_1, \dots, m'_n) \mid 1 \leq i \leq n, w \in A_i\},$$

where $A_i = \{u_i\} \cup \{w \mid t_i \xrightarrow{S \cup \mathcal{E}} w\}$.

We shall prove by Scott's Induction Principle that $Q(m_1, \dots, m_n)$ holds. It is clear that Q is ω -continuous and that $Q(\perp_M^n)$ holds. We now verify condition (2) of Definition 5.6.

Let $x_1, \dots, x_n \in M$ and $x'_i = t_{iM}(x_1, \dots, x_n)$. We must prove that $Q(x_1, \dots, x_n)$ implies $Q(x'_1, \dots, x'_n)$. We first consider Q_1 :

$$\begin{aligned} x'_i &= t_{iM}(x_1, \dots, x_n) \\ &\leq t_{iM}(x'_1, \dots, x'_n) \quad (\text{by } Q_1 \text{ and the monotonicity of } t_{iM}) \end{aligned}$$

and this holds for all i in $[n]$.

Next we prove that

$$(v) \quad x'_i = t_{iM}(x_1, \dots, x_n) \leq w_M(x_1, \dots, x_n),$$

for all i , for all w such that $t_i \rightarrow_{S \cup \mathcal{G}}^k w$ for some k . We use an induction on k . If $k=0$, then $w = t_i$ and the result holds trivially. Otherwise, let $t_i \rightarrow_{S \cup \mathcal{G}}^{k-1} w' \rightarrow_{S \cup \mathcal{G}} w$. One can assume that $x'_i \leq w'_M(x_1, \dots, x_n)$. If $w' \leftrightarrow_{\mathcal{G}} w$, then $w_M(x_1, \dots, x_n) = w'_M(x_1, \dots, x_n)$. If $w' \rightarrow_S w$, then $w' = c[u_j/y]$ and $w = c[t_j/y]$ for some c in $M(F, \{u_1, \dots, u_n, y\})$. Hence, by Q_1 , $w'_M(x_1, \dots, x_n) = c_M(x_1, \dots, x_n, x_j) \leq c_M(x_1, \dots, x_n, x'_j) = w_M(x_1, \dots, x_n)$. Whence the result follows.

We now establish $Q_2(x'_1, \dots, x'_n)$. Let $w \in A_i$.

First case: If $t_i \rightarrow_{S \cup \mathcal{G}}^k w$, then

$$\begin{aligned} x'_i &\leq w_M(x_1, \dots, x_n) && \text{(by property (v) above)} \\ &\leq w_M(m'_1, \dots, m'_n) && \text{(by } Q_2 \text{ and the monotonicity of } w_M\text{)}. \end{aligned}$$

Second case: If $w = u_i$, then

$$\begin{aligned} x'_i &\leq t'_{iM}(x_1, \dots, x_n) && \text{(by the first case since } t_i \rightarrow_{S \cup \mathcal{G}}^k t'_i\text{)} \\ &\leq t'_{iM}(m'_1, \dots, m'_n) \\ &= m'_i && \text{(since } (m'_1, \dots, m'_n) \text{ is a solution of } S'\text{)} \\ &= w_M(m'_1, \dots, m'_n). \end{aligned}$$

Hence, $Q(m_1, \dots, m_n)$ holds.

It follows that $m_i \leq m'_i$ for all i in $[n]$ (by letting $w = u_i$ in Q_2). \square

6.4. Remarks and examples. (1) Let $S_0 = \langle u = fu \rangle$ and $S_1 = \langle u = u \rangle$. One has $S_0 \text{ fld } S_1$, but S_0 is strictly smaller than S_1 w.r.t. \leq since $u \sim_{S_1} \Omega$. This shows that **fld** is not \sim -correct (whereas **unf** is by Proposition 6.3).

(2) Consider now the two systems $S_2 = \langle u = g(v, w), v = f(v), w = f(w) \rangle$ and $S_3 = \langle u = g(w, v), v = f(v), w = v \rangle$. It is clear that $S_3 \sim S_2$. Remark that $S_3 \text{ eunf } S_2$ since

$$g(w, v) \xrightarrow{S_3} g(v, v) \xrightarrow{I(S_3)} g(v, w), \quad v \xrightarrow{S_3} f(v) \xrightarrow{I(S_3)} f(w).$$

We now prove that **rufld**, **unf**, and **unf**⁻¹ are insufficient to derive S_2 from S_3 , i.e., that the set of transformations $\{\text{rufld}, \text{unf}, \text{unf}^{-1}\}$ is not \sim -complete. Let \mathcal{C} be the set of all systems of the form $\langle u = g(f^n v, f^m w), v = f^p(v), w = f^q(w) \rangle$ for $n, m \geq 0, p, q \geq 1$. It is easy to verify that all these systems are \sim -equivalent to S_2 and that \mathcal{C} is the set of all systems S such that $S_2 \gamma S$ for some γ in $\{\text{rufld}, \text{unf}, \text{unf}^{-1}\}^*$. Our claim is proved since $S_3 \notin \mathcal{C}$.

This example shows that the extended unfolding adds power to the set $\{\text{rufld}, \text{unf}, \text{unf}^{-1}\}$.

(3) It would be natural to extend **eunf** into **eunf** _{\mathcal{G}} by taking $\rightarrow_{S \cup I(S) \cup \mathcal{G}}^*$ instead of $\rightarrow_{S \cup I(S)}^*$ in condition (1) of Definition 6.2. But this transformation is not $\sim_{\mathcal{G}}$ -correct

since the rewritings which use \mathcal{E} can destroy the effect of condition (2) of Definition 6.2. It suffices to have in \mathcal{E} the rule $fx = x$, and to consider S as in the counterexample following Definition 6.2 and $S'' = \langle u = v, v = fu, w = gw \rangle$. Then $S \text{ eunf}_{\mathcal{E}} S''$, but $S'' \not\sim_{\mathcal{E}} S$.

A rule like $fx = x$ looks stupid but a similar example could be built with the rule $x + x = x$, which we shall use in Section 10.

We shall prove the \sim -completeness of $\mathcal{C} = \{\text{eunf}, \text{eunf}^{-1}\}$ for the class of regular systems over F (not over F_{Ω} , an extension to systems over F_{Ω} will be given afterwards). We first construct for every system S over F a \sim -canonical system S_{\sim} and we shall prove that $S_{\sim} \text{ eunf } S$.

6.5. Definition (\sim -canonical systems). Let S be a regular system and $\text{Unk}(S) = U = \{u_1, \dots, u_n\}$. Let (s_1, \dots, s_n) be its least solution in $\mathbf{M}_{\Omega}^{\infty}(F)$ and $T(S) = \{s_1, \dots, s_n\}$. Hence, $k = \text{Card}(T(S)) \leq n$. Let us enumerate $T(S)$ as $\{s_{i_1}, \dots, s_{i_k}\}$ with $i_1, \dots, i_k \in [n]$.

Let $U' = \{u_{i_1}, \dots, u_{i_k}\}$ and \equiv be the congruence relation \sim_S on $\mathbf{M}(F, U')$, i.e. (by Theorem 5.4), $t \equiv t'$ iff $t[s_{i_1}/u_{i_1}, \dots, s_{i_k}/u_{i_k}] = t'[s'_{i_1}/u_{i_1}, \dots, s'_{i_k}/u_{i_k}]$. This congruence is F -coherent and F -simplifiable (see Definition A.1) and, furthermore, $u \not\equiv u'$ for $u, u' \in U'$, $u' \neq u$.

Let S' be the regular system associated with \equiv by Definition A.6 and let S_{\sim} be the system $S' \cup \langle u_i = u_j; u_i \in U - U', u_j \in U', s_i = s_j \rangle$. Its set of unknowns is U . It is clear that S_{\sim} is constructed from the set $T(S)$, the mapping: $U \rightarrow T(S)$ associating s_i with u_i , and the sequence i_1, \dots, i_k . For an other sequence i'_1, \dots, i'_k such that $T(S) = \{s_{i'_1}, \dots, s_{i'_k}\}$ one obtains a different system S_{\sim} but this system is just a renaming of the first one. In order to avoid this indeterminacy, we assume in the sequel that i_1, \dots, i_k is such that $s_i \neq s_j$ for all $j = 1, \dots, k$, all $i < i_j$.

The following lemma is an extension of Lemma A.7. It shows that $\rightarrow_{S_{\sim} \cup I(S_{\sim})}^*$ plays with respect to \sim_S the same role as $\rightarrow_{S_{\sim}}^*$ with respect to \equiv .

6.6. Lemma. *Let $t \in M(F, U)$ and $l \in [n]$. If $t \sim_S u_l$, then $u_l \rightarrow_{S_{\sim} \cup I(S_{\sim})}^* t$.*

Proof. We let $S_{\sim} = \langle u_i = t'_i; 1 \leq i \leq n \rangle$.

Case 1: $t \in U$, say $t = u_j$. Then, $s_l = s_j$. Let u_m be the unique element of U' such that $s_l = s_m$. There are several subcases:

Subcase 1.1: $l \neq m, j \neq m$. Then $t'_l = u_m, t'_j = u_m$, hence, $u_l \rightarrow_{S_{\sim} \cup I(S_{\sim})}^* t'_l \rightarrow_{I(S_{\sim})} u_j = t$.

Subcase 1.2: $l \neq m, j = m$. Then $t'_l = u_m$, hence, $u_l \rightarrow_{S_{\sim}}^* t'_l = u_j = t$.

Subcase 1.3: $l = m, j \neq m$. Then $t'_j = u_m$, hence, $u_l = t'_j \rightarrow_{I(S_{\sim})} u_j = t$.

Case 2: We now assume that $t \in F(M(F, U))$. Let $t' = t[u_j/u_i; u_j \in U', u_i \in U, s_i = s_j]$ so that $t' \rightarrow_{I(S_{\sim})}^* t$ by definition of S' .

Hence, it suffices to prove that $t'_l \rightarrow_{S_{\sim}}^* t'$. But $t'_l \equiv t'$. Hence, $t'_l \leq t'$ by Definition A.6. This fact follows then from Lemma A.7 applied to the subsystem S' of S_{\sim} . \square

6.7. Proposition. *Let S be a regular system over F . Then $S \sim S_-$ and S_- is \sim -canonical. Furthermore, $S_- \text{ eunf } S$.*

Proof. Since S_- is defined from $T(S)$, i.e., the n -tuple of trees (s_1, \dots, s_n) , the systems S_- and \bar{S}_- are equal if $T(S) = T(\bar{S})$, i.e., if $S \sim \bar{S}$, where \bar{S} is another system with the same unknowns as S . By Proposition 6.3, it suffices to prove that $S_- \text{ eunf } S$ to establish that $S_- \sim S$. (We shall use the notations of the proof of Lemma 6.6.)

Let $i \in [n]$. One has $t_i \sim_S u_i$, hence, Lemma 6.6 shows that $u_i \rightarrow_{S_- \cup I(S_-)}^* t_i$. We only have to verify that $\text{Psing}(S) \subseteq \text{Psing}(S_-)$. If $u_i \in \text{Psing}(S)$, then $s_i = \Omega$. Let m be such that $u_m \in U'$ and $s_m = \Omega$. The equivalence class of u_m modulo \equiv is reduced to u_m . Hence, $t'_m = u_m$. Furthermore, $t'_i = u_m$. Hence, $u_i \in \text{Psing}(S_-)$.

Hence, we have shown that $S_- \text{ eunf } S$. \square

6.8. Theorem. *The set of transformations $\{\text{eunf}, \text{eunf}^{-1}\}$ is \sim -complete for the class of regular systems over F .*

Proof. The \sim -correctness follows from Proposition 6.3.

Let $S \sim S'$. Then $S_- = S'_-$, hence, $S' \text{ eunf}^{-1} S_- \text{ eunf } S$ by Proposition 6.7. \square

6.9. Corollary. $\text{rufld} \subseteq \text{eunf}^{-1} \cdot \text{eunf}$.

It is clear that $\{\text{eunf}, \text{eunf}^{-1}\}$ is not \sim -complete for regular systems over F_Ω . It suffices to consider $S = \langle u = u \rangle$ and $S' = \langle u = \Omega \rangle$. They are \sim -equivalent, but since neither eunf nor eunf^{-1} can introduce Ω in any system over F to which they apply, S' cannot be reached from S by them. Nevertheless, we have the following proposition.

6.10. Proposition. *The class $\{\text{redef}, \text{redef}^{-1}, \text{eunf}, \text{eunf}^{-1}\}$ is \sim -complete for regular systems over F_Ω .*

Proof. Let S and S' be \sim -equivalent. Then $S_1 = \text{Red}_-(S)$ and $S'_1 = \text{Red}_-(S')$ are also \sim -equivalent. Furthermore, S_1 and S'_1 have no singular unknowns, and by Theorem 8.8 each of them has a unique solution in $M_\Omega^\infty(F)$. These solutions coincide with the least ones, hence, are equal since $S \sim S'$ and $S_1 \sim S$, $S'_1 \sim S'$. This means that Ω can be considered as an ordinary constant in S_1 and S'_1 . More precisely, if a is any new constant, then the systems S_2 and S'_2 where a is substituted for Ω everywhere in S_1 and S'_1 , are still \sim -equivalent. Hence, $S_2 \text{ eunf}^{-1} \cdot \text{eunf } S'_2$ by Theorem 6.8 and $S_1 \text{ eunf}^{-1} \cdot \text{eunf } S'_1$.

The result then follows from Proposition 5.16. \square

7. Subsystems and auxiliary unknowns

Many useful transformations of grammars and recursive program schemes involve the introduction of auxiliary unknowns (i.e., nonterminals for grammars and procedure symbols for recursive program schemes) or the elimination of unknowns and equations which are unnecessary (in some sense). The validation of such transformations in terms of $\approx_{\mathcal{E}}$ - or $\sim_{\mathcal{E}}$ -equivalence necessitates the comparison of two systems with different sets of unknowns. In this direction we already know that the renaming of unknowns can help (see Section 2.5), but further definitions are necessary.

7.1. Definition. Let S be a regular system and let W be a nonempty subset of $\text{Unk}(S) = \{u_1, u_2, \dots, u_n\}$; we assume that $W = \{u_{i_1}, \dots, u_{i_k}\}$ and that it is ordered in this way according to the order on \mathcal{U} (see Section 2.1). Let $\pi_W: M^n \rightarrow M^k$ be the mapping associating $(m_{i_1}, \dots, m_{i_k})$ with (m_1, \dots, m_n) . Let S' be another system such that $W \subseteq \text{Unk}(S) \cap \text{Unk}(S')$ and let \mathcal{C} be a class of F -magmas. We can compare S and S' by letting

$$S \approx_{\mathcal{C}, W} S' \text{ iff } \pi_W(\text{Sol}_{\mathbf{M}}(S)) = \pi_W(\text{Sol}_{\mathbf{M}}(S')) \text{ for all } \mathbf{M} \text{ in } \mathcal{C},$$

$$S \sim_{\mathcal{C}, W} S' \text{ iff } \pi_W(\mu\text{-Sol}_{\mathbf{M}}(S)) = \pi_W(\mu\text{-Sol}_{\mathbf{M}}(S')) \text{ for all } \mathbf{M} \text{ in } \mathcal{C}$$

(where $\mathcal{C} \subseteq \mathcal{V}^\omega$).

We replace \mathcal{C} by \mathbf{M} or \mathcal{E} , or omit it exactly as in Section 2.3.

Our purpose is to extend the results of Sections 3–6 to these equivalences.

7.2. Lemma. Let S' be a subsystem of S and $U' = \text{Unk}(S')$.

(1) $\pi_{U'}(\text{Sol}_{\mathbf{M}}(S)) \subseteq \text{Sol}_{\mathbf{M}}(S')$ for every F -magma \mathbf{M} .

(2) $\pi_{U'}(\mu\text{-Sol}_{\mathbf{M}}(S)) = \mu\text{-Sol}_{\mathbf{M}}(S')$ for every ω -complete F -magma \mathbf{M} , i.e., $S \sim_{U'} S'$.

Proof. Part (1) is clear. The inclusion may be strict since a solution of S' may have no extension into a solution of S . One does not have $S \approx_{U'} S'$ in general.

Part (2) follows from the Least Fixpoint Theorem. \square

Hence, if \mathcal{E} is a set of equations, if S and S' are two regular systems such that $S \text{ redef}_{\mathcal{E}} S'$, and if S'' is the subsystem $S' \upharpoonright U'$ of S' (where U' is as in Definition 5.10), then $S'' \sim_{\mathcal{E}, U'} S$. One can consider the transformation of S into S'' as a way to eliminate from S the unknowns of U' (see Definition 5.10).

The possibly strict inclusion in Lemma 7.2(1) points out a difficulty with $\approx_{\mathcal{E}, W}$ and actually we shall only investigate a restriction of $\approx_{\mathcal{E}, W}$, where W is such that one has an equality.

We first consider $\sim_{\mathcal{E}, W}$ for which things go more smoothly.

7.3. Definition. Let S be a regular system, $U = \text{Unk}(S)$, $W \subset U$, and $U' = U - W$. Let $F' = F \cup W$. Then $S \upharpoonright U'$ is a system over F' .

Let us assume that $W = \{u_{i_1}, \dots, u_{i_l}\}$ (enumerated in the order of \mathcal{U}). For every F -magma \mathbf{M} and every sequence (d_1, \dots, d_l) in M^l , one defines an F' -magma $\mathbf{M}' = \mathbf{M}(d_1, \dots, d_l)$ by letting $M' = M$, $f_{\mathbf{M}'} = f_{\mathbf{M}}$ for f in F and $u_{i_j \mathbf{M}'} = d_j$ for $j = 1, \dots, l$. With these notations we have the following lemma.

7.4. Lemma. *If \mathbf{M} is ω -complete, then $\mu\text{-Sol}_{\mathbf{M}'}(S \upharpoonright U') = \pi_{U'}(\mu\text{-Sol}_{\mathbf{M}}(S))$, where $\mathbf{M}' = \mathbf{M}(\pi_W(\mu\text{-Sol}_{\mathbf{M}}(S)))$.*

This lemma means that if one replaces in a system S some unknowns by their values (in the least solution), then the least solution of the system obtained in this way yields for the remaining unknowns the same values as S . This fact is currently used for proving properties of programs [34, 68, 82].

Proof of Lemma 7.4. Without loss of generality we can assume that $U' = \{u_1, \dots, u_k\}$ and $W = \{u_{k+1}, \dots, u_n\}$. Let $(m_1, \dots, m_n) = \mu\text{-Sol}_{\mathbf{M}}(S)$ and $(m'_1, \dots, m'_k) = \mu\text{-Sol}_{\mathbf{M}'}(S')$, where $S' = S \upharpoonright U'$. It is clear that (m_1, \dots, m_k) is a solution of S' in \mathbf{M}' , hence, $(m'_1, \dots, m'_k) \leq (m_1, \dots, m_k)$. In order to establish the opposite inequality, it suffices to prove that $P(m_1, \dots, m_n)$ holds, where

$$P(x_1, \dots, x_n) \Leftrightarrow x_1 \leq m'_1 \text{ and } \dots \text{ and } x_k \leq m'_k \\ \text{and } x_{k+1} \leq m_{k+1} \text{ and } \dots \text{ and } x_n \leq m_n,$$

and this can easily be done with Scott's Induction Principle (see Proposition 5.7) and by using the inequalities $m'_i \leq m_i$ for i in $[k]$. \square

7.5. Proposition. *Let S and S' be regular systems and W be a subset of $\text{Unk}(S) \cap \text{Unk}(S')$. Then $S \sim_{\mathcal{G}, W} S'$ iff there exists a renaming α and two regular systems S_1 and S_2 such that α is the identity on W , $\text{Unk}(\alpha(S)) \cap \text{Unk}(S') = W$, and*

$$\alpha(S) \subseteq S_1 \sim_{\mathcal{G}} S_2 \supseteq S'.$$

Proof. The 'if' part is an immediate consequence of Lemma 7.2(2) and Section 2.5.

For the 'only if' part, let $U = \text{Unk}(S)$, $U' = \text{Unk}(S')$. We first assume that $U \cap U' = W$ and for α we take the identity. We let $S = \langle u = t_u; u \in U \rangle$ and $S' = \langle u = t'_u; u \in U' \rangle$. We define

$$S_1 = S \cup \langle u = t'_u; u \in U' - U \rangle, \quad S_2 = S' \cup \langle u = t_u; u \in U - U' \rangle,$$

so that $\text{Unk}(S_1) = \text{Unk}(S_2) = U \cup U'$.

We have to prove that $S_1 \sim_{\mathcal{G}} S_2$. So let $\mathbf{M} \in \mathcal{V}^\omega(\mathcal{E})$. Remark that S_1 and S_2 only differ by the equations with left-handside in W , hence, $S_1 \upharpoonright U'' = S_2 \upharpoonright U''$, where $U'' = U \cup U' - W$. Let us denote by S'' this regular system (over $F \cup W$).

By Lemma 7.2(2),

$$\pi_W(\mu\text{-Sol}_M(S_1)) = \pi_W(\pi_U(\mu\text{-Sol}_M(S_1))) = \pi_W(\mu\text{-Sol}_M(S))$$

and similarly,

$$\pi_W(\mu\text{-Sol}_M(S_2)) = \pi_W(\mu\text{-Sol}_M(S')) = \pi_W(\mu\text{-Sol}_M(S_1)) \quad (2)$$

since $S \sim_{\mathcal{E}, W} S'$.

Let now $M' = M(\pi_W(\mu\text{-Sol}_M(S))) = M(\pi_W(\mu\text{-Sol}_M(S')))$. Then

$$\pi_{U''}(\mu\text{-Sol}_M(S_1)) = \mu\text{-Sol}_{M'}(S'')$$

by Lemma 7.4 and, similarly

$$\pi_{U''}(\mu\text{-Sol}_M(S_2)) = \mu\text{-Sol}_{M'}(S'') = \pi_{U''}(\mu\text{-Sol}_M(S_1)). \quad (3)$$

Hence, putting (2) and (3) together, we have $\mu\text{-Sol}_M(S_1) = \mu\text{-Sol}_M(S_2)$. This proves that $S_1 \sim_{\mathcal{E}} S_2$.

If $W \subset U \cap U'$, one can define $U'' \subseteq \mathcal{U}$ and a bijection $\alpha: U \rightarrow U''$ such that $W = U \cap U''$ and α is the identity on W . The above proof can then be applied to $\alpha(S)$ instead of S . \square

By means of Theorem 6.8, this proposition gives a characterization of \sim_W in terms of transformations by renamings, extended unfoldings, and restriction to subsystems.

We now consider $S \approx_{\mathcal{E}, W} S'$, but only in a special case, when W is ‘large enough’. This necessitates some more definitions.

7.6. Definition. Let S be a regular system and W be a subset of U . Let $W_0 \subseteq W_1 \subseteq \dots \subseteq W_i \subseteq U$ be such that $W_0 = W$, $W_{i+1} = W_i \cup \{u_j \in U \mid \text{Var}_U(t_j) \subseteq W_i\}$ and let $\bar{W} = \bigcup \{W_i \mid i \geq 0\}$. We say that W is a *base of S* if $\bar{W} = U$.

Note that S is *recursion-free* (see Definition 4.17) iff \emptyset is a base of S and that W is a base of S iff the system $S \upharpoonright (U - W)$ (over $F \cup W$) is recursion-free. Hence, it follows from Proposition 4.18 that W is a base of S iff, for all u in $U' = U - W$, there exists t in $M(F, W)$ such that $u \rightarrow_{S \upharpoonright U'}^* t$.

7.7. Remark. Let G be the directed graph associated with S , having U as set of nodes and having an arc from u_i to u_j iff u_j occurs in t_i . Then W is a base of S iff W is a base of G in the sense of Braquelaire and Courcelle [18], i.e., if W is a set of nodes of G such that any loop in G has at least one node in W .

We say that S is a *large subsystem* of S' (we denote this by $S \subseteq_{\ell} S'$) if $S \subseteq S'$ and $\text{Unk}(S)$ is a base of S' .

7.8. Proposition. *Let S be a regular system, let W be a subset of $\text{Unk}(S)$, and $U' = \text{Unk}(S) - W$. Then W is a base of S iff there exist two systems S' and S'' such that $\text{Unk}(S') = \text{Unk}(S)$, $\text{Unk}(S'') = W$, and $S \text{ runf}^{(U')} S' \cong_{\ell} S''$. If this is the case, then S' and S'' exist in a unique way.*

Proof. Let $U = \text{Unk}(S)$. Since $S \upharpoonright U'$ is recursion-free, it follows from Proposition 4.18 that, for all u_i in U' , there exists s_i in $M(F, W)$ such that $u_i \rightarrow_{S \upharpoonright U'}^* s_i$. Let $t'_i = t_i[s_j/u_j; u_j \in U']$ for u_i in W and $t'_i = t_i$ if $u_i \in U'$.

The systems $S' = \langle u_i = t'_i; i \in [n] \rangle$ and $S'' = S' \upharpoonright W$ satisfy the requirements.

Conversely, if $S'' \subseteq_{\ell} S'$, then $\text{Unk}(S'')$ is a base of S' .

Let us remark that, for any two systems S_1 and S_2 , if $S_1 \text{ unf } S_2$ and W_1 is a base of S_2 , then W_1 is a base of S_1 : if $u \in \text{Unk}(S_1) - W_1$, there exists a t in $M(F, W_1)$ such that $u \rightarrow_{S_2}^* t$, hence, $u \rightarrow_{S_1}^* t$. Hence, if $S \text{ runf}^{(U')} S'$, W is a base of S .

Finally, it follows from the unicity results of Proposition 4.18(1) that S' (whence S'') exists in a unique way. \square

The transformation of S into S'' can be considered as the *elimination* of the unknowns of $U' = \text{Unk}(S) - W$. However, this is possible only if the unknowns of U' are ‘auxiliary’ in some sense, i.e., precisely if W is a base.

The above properties of bases and large subsystems are syntactical. We now consider their semantical properties. The following lemma is the counterpart of Lemma 7.4 and is stated with the same notations.

7.9. Lemma. *If W is a base of S , if $U' = \text{Unk}(S) - W$, and m is a solution of S in \mathbf{M} , then $S \upharpoonright U'$ has a unique solution in $\mathbf{M}(\pi_W(m))$ and this solution is $\pi_{U'}(m)$. Hence, the mapping $\pi_W : \text{Sol}_{\mathbf{M}}(S) \rightarrow M^{\text{Card}(W)}$ is one-to-one.*

This result could be written as follows:

$$\text{Sol}_{\mathbf{M}'}(S \upharpoonright U') = \{\pi_{U'}(m)\},$$

where $m \in \text{Sol}_{\mathbf{M}}(S)$ and $\mathbf{M}' = \mathbf{M}(\pi_W(m))$ in order to stress the similarity with Lemma 7.4.

Proof of Lemma 7.9. $\pi_{U'}(m)$ is clearly a solution of $S \upharpoonright U'$ in $\mathbf{M}(\pi_W(m))$ and this solution is the only one since $S \upharpoonright U'$ is recursion-free (Proposition 4.18).

Let $m, m' \in \text{Sol}_{\mathbf{M}}(S)$ be such that $\pi_W(m) = \pi_W(m')$. Since $S \upharpoonright U'$ has a unique solution in $\mathbf{M}(\pi_W(m))$ (by Proposition 4.18), $\pi_{U'}(m)$ and $\pi_{U'}(m')$ which are solutions of this type are equal. Hence, $m = m'$. \square

7.10. Proposition. *If $S' \subseteq_{\ell} S$, then $S' \approx_{\text{Unk}(S')} S$.*

Proof. Let $U = \text{Unk}(S)$ and $W = \text{Unk}(S')$. By Lemma 7.2(1), one has $\pi_W(\text{Sol}_{\mathbf{M}}(S)) \subseteq \text{Sol}_{\mathbf{M}}(S')$.

In order to establish the equality, let m' be a solution of S' in \mathbf{M} . The system $S \upharpoonright (U - W)$ has a unique solution in $\mathbf{M}' = \mathbf{M}(m')$, call it m_1 . Merging m' and m_1 gives a solution m of S in \mathbf{M} such that $\pi_W(m) = m'$ and $\pi_{U-W}(m) = m_1$. Hence, $m' \in \pi_W(\text{Sol}_{\mathbf{M}}(S))$.

Note that π_W is a bijection of $\text{Sol}_{\mathbf{M}}(S)$ onto $\text{Sol}_{\mathbf{M}}(S')$. \square

Hence, for large enough subsystems, the inequality of Lemma 7.2(1) becomes an equality.

The following proposition is similar to Proposition 7.5.

7.11. Proposition. *Let S, S' be regular systems and let \mathcal{E} be a set of equations. Let $W \subseteq \text{Unk}(S) \cap \text{Unk}(S')$ be a base for both S and S' . Then $S \approx_{\mathcal{E}, W} S'$ if and only if there exist four systems S_1, S_2, S_3, S_4 such that $\text{Unk}(S_2) = \text{Unk}(S_3) = W$, and*

$$S \text{ ruf} S_1 \supseteq_{\ell} S_2 \approx_{\mathcal{E}} S_3 \subseteq_{\ell} S_4 \text{ ruf}^{-1} S'.$$

Proof. Let us assume that $S \approx_{\mathcal{E}, W} S'$. Let $U = \text{Unk}(S)$ and $U' = \text{Unk}(S')$. The existence of S_1, S_2, S_3, S_4 such that $S \text{ ruf} S_1 \supseteq_{\ell} S_2$ and $S' \text{ ruf} S_4 \supseteq_{\ell} S_3$ follows from Proposition 7.8. By Proposition 4.9 and Proposition 7.10, the hypothesis $S \approx_{\mathcal{E}, W} S'$ implies $S_2 \approx_{\mathcal{E}, W} S_3$, hence, $S_2 \approx_{\mathcal{E}} S_3$.

The 'if' direction follows from the definitions in Section 2.5, Proposition 4.9, and Proposition 7.10. \square

Note the difference with Proposition 7.5: the systems S_2 and S_3 are smaller than S and S' (one takes some kind of intersection) whereas in Proposition 7.5, the systems S_1 and S_4 which play a similar role are larger than S and S' , respectively and correspond to some kind of union.

In the case $\mathcal{E} = \emptyset$, one obtains with the help of Theorem 4.10 a characterization of \approx_W in terms of \subseteq_{ℓ} and **rufld**.

Here we give an application to the *uniformization* of regular systems. At the cost of introducing extra unknowns, one can transform an arbitrary system into a quasi-uniform one (respectively, a Greibach system into a uniform one). More precisely stated, we have the following proposition.

7.12. Proposition. *For every regular system S one can construct a quasi-uniform system $\text{Ufm}(S)$ such that $S \subseteq_{\ell} S'' \text{ rufld} \text{Ufm}(S)$ (for some system S''). Hence, $\text{Ufm}(S) \approx_{\text{Unk}(S)} S$. If S is a Greibach system, then $\text{Ufm}(S)$ is uniform.*

Proof. Let $S = \langle u_i = t_i; 1 \leq i \leq n \rangle$ and $U = \text{Unk}(S)$. Let R be the set of proper sub-terms of t_1, \dots, t_n which are not in U . We can enumerate R as $\{s_1, \dots, s_k\}$. If $R = \emptyset$, then S is quasi-uniform and one takes $\text{Ufm}(S) = S$. Otherwise, one defines $\text{Ufm}(S) = S'$ by letting $U' = \{u_{n+1}, \dots, u_{n+k}\} \subseteq \mathcal{U}$ (hence, U' is disjoint from U) and by letting

$t \mapsto \bar{t}$ be the partial mapping $M(F, U) \rightarrow U \cup F(U \cup U')$ defined as follows:

$$\begin{aligned} \bar{t} &= t && \text{if } t \in U, \\ \bar{t} &= f(u_{i_1}, \dots, u_{i_l}) && \text{if } t = f(w_1, \dots, w_l), w_1, \dots, w_l \in M(F, U) \text{ and,} \\ &&& \text{for all } j = 1, \dots, l, \text{ either } w_j = u_{i_j} \text{ or } w_j = s_{i_j-n}. \end{aligned}$$

Note that $\bar{t} = t$ if $t \in F(U)$ and that \bar{t} is defined whenever $t \in \{t_1, \dots, t_n, s_1, \dots, s_k\}$.

Finally, the system $S' = \langle u_i = t'_i; i \in [n+k] \rangle$ with $t'_i = \bar{t}_i$ for $i \in [n]$ and $t'_i = \bar{s}_{i-n}$ for $i \in \{n+1, \dots, n+k\}$ satisfies the required properties. It is not difficult to verify that $\bar{t}_i \rightarrow_{S' \uparrow U}^* t_i$ for all i in $[n]$, but we omit these technical details. \square

7.13. Example. Let $S = \langle u_1 = u_2, u_2 = f(u_1, g(u_2, f(u_1, u_2))) \rangle$. Then $R = \{g(u_2, f(u_1, u_2)), f(u_1, u_2)\}$ and $U' = \{u_3, u_4\}$. The system $\text{Ufm}(S)$ is then

$$\langle u_1 = u_2, u_2 = f(u_1, u_3), u_3 = g(u_2, u_4), u_4 = f(u_1, u_2) \rangle.$$

8. Regular systems having a unique solution

When a recursive applicative program scheme (considered as a system of equations) has a unique solution in some interpretation, a proof method which generalizes the one of McCarthy [70] and which is simpler than Scott's Induction Principle can be used to prove the equivalence of two systems (i.e., their \sim -equivalence in some interpretation). This proof method has been investigated in [25], under the name of *Unique Fixpoint Principle*. This method is also applicable to certain context-free grammars [78] in order to prove that a given grammar generates some given language. Examples will be given later (see Section 17).

Hence, we investigate conditions insuring that $\text{Sol}_{\mathbf{M}}(S)$ is a singleton. It follows from Proposition 4.18 that the systems such that $\text{Sol}_{\mathbf{M}}(S)$ is a singleton for all \mathbf{M} in \mathcal{V} are not very interesting. Hence, we shall formulate this unicity property with respect to special subclasses of \mathcal{V} .

8.1. Definition. Let \mathbf{M} be an F -magma. A regular system S is \mathbf{M} -univocal if S has one and only one solution in \mathbf{M} . If \mathcal{C} is a class of F -magmas, then S is \mathcal{C} -univocal if S is \mathbf{M} -univocal for all \mathbf{M} in \mathcal{C} .

The following proposition is an easy consequence of the definitions.

8.2. Proposition. Let $\mathbf{M} \in \mathcal{V}(\mathcal{E})$. Let S and S' be two regular systems such that $S \text{ ufld}_{\mathcal{E}} S'$.

- (1) If S has a solution in \mathbf{M} and if S' is \mathbf{M} -univocal, then S is \mathbf{M} -univocal and S and S' have the same solution in \mathbf{M} (hence, $S \approx_{\mathbf{M}} S'$).
- (2) If S' is \mathbf{M} -univocal and $\mathbf{M} \in \mathcal{V}(\mathcal{E})$, then $S' \sim_{\mathbf{M}} S$.

Let us recall that \mathbf{ufl}_g is not \sim_g -correct, i.e., that $S \mathbf{ufl}_g S'$ does not imply $S' \sim_g S$. However, this implication does hold if S' is $\mathcal{V}^\omega(\mathcal{E})$ -univocal. This idea has been developed in [25] for recursive applicative program schemes. We do not recall the rather technical results obtained there.

A simple topological condition will be used here to insure the univocality of Greibach regular systems. It has been used in [1, 2, 10, 12, 14, 24, 26].

3.3. Definition ([26]). Let E be a metric space with distance d . The distance d is extended to E^k by $d((x_1, \dots, x_k), (x'_1, \dots, x'_k)) = \mathbf{Max}\{d(x_i, x'_i) \mid i \in [k]\}$.

If α is a mapping $E^k \rightarrow E$, we let

$$\|\alpha\| = \mathbf{Sup}\{d(\alpha(x), \alpha(x'))/d(x, x') \mid x, x' \in E^k, x \neq x'\}.$$

Hence, $\|\alpha\|$ belongs to the real interval $[0, +\infty]$.

The mapping α is *contracting* if $\|\alpha\| < 1$. This condition is equivalent to the existence of a real number c , $0 \leq c < 1$ such that

$$d(\alpha(x_1, \dots, x_k), \alpha(x'_1, \dots, x'_k)) \leq c \cdot \mathbf{Max}\{d(x_i, x'_i) \mid i \in [k]\}.$$

An F -magma $\mathbf{M} = \langle M, \langle f_{\mathbf{M}} \rangle_{f \in F} \rangle$ is *semicontracting* if

- (1) M is a complete metric space with distance $d_{\mathbf{M}}$;
- (2) $d_{\mathbf{M}}(x, y) \leq 1$ for all x, y in M ;
- (3) $\|f_{\mathbf{M}}\| \leq 1$ for all f in F .

It is *contracting* if, furthermore,

- (4) $\mathbf{Sup}\{\|f_{\mathbf{M}}\| \mid f \in F\} < 1$.

Let \mathcal{Sctr} (respectively \mathcal{Ctr}) be the class of semicontracting (respectively contracting) magmas.

8.4. Lemma. (1) If $t \in M(F, X)$ and $\mathbf{M} \in \mathcal{Sctr}$, then $\|t_{\mathbf{M}}\| \leq 1$.

- (2) If $t \in M(F, X) - X$ and $\mathbf{M} \in \mathcal{Ctr}$, then $\|t_{\mathbf{M}}\| < 1$.

Note that $\|t_{\mathbf{M}}\|$ may be < 1 even if \mathbf{M} is not contracting. This justifies the following definition (where \mathbf{M} is any F -magma such that M is a metric space): A regular system S is \mathbf{M} -*contracting* if $\|t_{i\mathbf{M}}\| < 1$ for all $i = 1, \dots, n$. It is \mathbf{M} -*semicontracting* if $\|t_{i\mathbf{M}}\| \leq 1$ for all $i = 1, \dots, n$.

We recall a well-known lemma which justifies our interest in contracting mappings.

8.5. Lemma (Fixpoint Lemma). *Let E be a complete metric space. Every contracting mapping $\alpha : E \rightarrow E$ has a unique fixpoint.*

The proof is easy (it is given in [26]). For extensions of this lemma, see [62]. In particular, it suffices that α^h is contracting for some $h \geq 1$ to obtain the same result.

8.6. Proposition. (1) *Let \mathbf{M} be an F -magma such that M is a complete metric space. If a regular system is \mathbf{M} -contracting, it is \mathbf{M} -univocal.*

- (2) *A Greibach system is \mathcal{Ctr} -univocal.*

Proof. Part (1) is proved by application of Lemma 8.5 to $E = M^k$ and $\alpha = S_M$.

Part (2) is an immediate consequence of part (1) and Lemma 8.4(2). \square

8.7. Definition ($M_\Omega^\infty(F)$ as a metric space [1, 2, 10, 26]). For any two elements t and t' of $M_\Omega^\infty(F)$, let $h(t, t')$ be the first level at which they differ ($h(t, t') = 0$ if they differ at the root, $h(t, t') = \infty$ if $t = t'$). Then we let

$$d(t, t') = \begin{cases} 0 & \text{if } t = t', \\ 2^{-h(t, t')} & \text{if } t \neq t'. \end{cases}$$

It is easy to show that d is a distance on $M_\Omega^\infty(F)$ making it into a complete metric space. This distance is even ultrametric. It is essentially the same as the distance that one puts on the ring of formal power series. Note that $d(t, t') \leq 1$ for all t, t' in $M_\Omega^\infty(F)$.

It can be shown that $M_\Omega^\infty(F)$ is compact if and only if F is finite, that $M_\Omega(F)$, the set of finite trees is a dense subset of $M_\Omega^\infty(F)$ and that $M_\Omega^\infty(F)$ is the topological completion of $M_\Omega(F)$ [2, 74]. Finally, $M_\Omega^\infty(F)$ is a contracting F -magma.

In the following proposition we assume that F is large enough so that $M_\Omega(F)$ is infinite. And we denote by S^h , $h \geq 1$, the regular system $\langle u_i = t_i^h; i \in [n] \rangle$, where $t_i^1 = t_i$ and $t_i^{h+1} = t_i[t_1^h/u_1, \dots, t_n^h/u_n]$. It is clear that $S \text{ unif } S^h$.

The following theorem encompasses and reformulates in the present framework some results of Bloom et al. [11, Proposition 2.8] and Nelson [75, Proposition 2].

8.8. Theorem. *Let S be a regular system. The following conditions are equivalent:*

- (1) S is $\mathcal{C}tr$ -univocal,
- (2) S is $M_\Omega^\infty(F)$ -univocal,
- (3) S has no singular unknowns,
- (4) $S \text{ runf}^* S'$ for some Greibach system S' ,
- (5) S^h is a Greibach system for some $h \geq 1$.
- (6) There exists h such that, for all $M \in \mathcal{C}tr$, S_M^h is contracting.

Proof. (1) \Rightarrow (2) since $M_\Omega^\infty(F) \in \mathcal{C}tr$.

(2) \Rightarrow (3): Let u_k be singular and let t be any finite tree in $M_\Omega(F) - T(S)$ (notation of Definition 6.5). Let S' be the system $\langle u_i = t'_i; 1 \leq i \leq n \rangle$ such that $t'_i = t$ if $u_i \rightarrow_S^* u_k$ and $t'_i = t_i$ otherwise. The least solution of S' is also a solution of S and differs from the least one. Hence, S is not $M_\Omega^\infty(F)$ -univocal.

(3) \Rightarrow (4): If $\text{Psing}(S) = \emptyset$ and S is not a Greibach system, there exist i, j such that $t_i = u_j$ and $t_j \in F(M(F, U))$, $j \neq i$. The system S'_1 obtained by replacing in S the equation $u_i = t_i$ by $u_i = t_j$ is such that $S \text{ runf } S_1$ and $\text{Psing}(S_1) = \emptyset$. By iterating this construction one obtains a Greibach system S' such that $S \text{ runf}^* S'$.

(4) \Rightarrow (1) since $S' \approx S$ and S' is $\mathcal{C}tr$ -univocal by Proposition 8.6.

(5) \Rightarrow (1) is proved by Proposition 8.2(1) with $\mathcal{E} = \emptyset$, Proposition 8.6, and the fact that $S \text{ unif } S^h$.

(3) \Rightarrow (5): Let $h = 1 + \text{Max}\{m \mid u \rightarrow_S^m u', u, u' \in \text{Unk}(S)\}$. Since $\text{Psing}(S) = \emptyset$, $h \leq n$ and S^h is a Greibach system.

(5) \Rightarrow (6): This easily follows from Lemma 8.4(2).

(6) \Rightarrow (1): The above-mentioned extension of Lemma 8.5 shows that $S_{\mathbf{M}}$ has a unique fixed point in \mathbf{M}^n , hence, that S is \mathbf{M} -univocal. \square

Let us finally mention that Courcelle [24] and Nelson [75] have investigated the class of all F -magmas where every regular system without singular unknowns has a unique solution.

9. Recursive applicative program schemes as regular systems

In this section we formalize the ideas sketched in Section 2.8. The example presented there was only involving binary functions, either base functions or recursively defined ones. Hence, one only had to deal with objects of a single type, namely the binary functions.

In the presence of functions of various arities, several composition operators (like **comp**) are needed. This can be conveniently handled by means of *sorts*. The introduction of sorts in the formalism of regular systems is straightforward. We did not use sorts in the initial definitions to have simpler notations.

We need some definitions and notations concerning sorts. All results of the preceding sections extend in an obvious way.

9.1. Sorts and signatures

Let \mathcal{S} be a set of sorts. An \mathcal{S} -sorted signature (or simply an \mathcal{S} -signature) is a set F (of function symbols) given with two mappings:

- $\alpha : F \rightarrow \mathcal{S}^*$ ($\alpha(f)$ is called the *arity* of f),
- $\sigma : F \rightarrow \mathcal{S}$ ($\sigma(f)$ is called the *sort* of f).

The length of $\alpha(f)$ is called the *rank* of f and is denoted by $\rho(f)$ as before. If $\alpha(f) = \varepsilon$ (we denote by ε the empty word of any free monoid X^*), then we say that f is a constant.

Let F be an \mathcal{S} -signature. We define an heterogeneous F -magma as an object

$$\mathbf{M} = \langle \langle M_s \rangle_{s \in \mathcal{S}}, \langle f_{\mathbf{M}} \rangle_{f \in F} \rangle,$$

where M_s is a set, the carrier of sort s and $f_{\mathbf{M}}$ a total mapping:

$$M_{s_1} \times \cdots \times M_{s_n} \rightarrow M_s, \quad \text{where } \alpha(f) = s_1 \dots s_n \text{ and } \sigma(f) = s.$$

If X is an \mathcal{S} -sorted set of variables (each x in X has the arity ε and a sort in \mathcal{S}) one can also define $\mathbf{M}(F, X)$, the free F -magma generated by X , and $M(F, X)_s$ is identified with the set of well-formed terms written with F and X and which are of sort s .

An ω -complete F -magma is an object $\mathbf{M} = \langle \langle M_s \rangle_{s \in \mathcal{S}}, \langle \perp_s \rangle_{s \in \mathcal{S}}, \langle \leq_s \rangle_{s \in \mathcal{S}}, \langle f_{\mathbf{M}} \rangle_{f \in F} \rangle$, where \leq_s is an ω -complete partial order on M_s with least element \perp_s and the $f_{\mathbf{M}}$'s are ω -continuous as usual.

The concepts of congruences, quotients, ideal completion, and rewriting systems extend in an obvious way. See [28, 53, 54] for a formal treatment of some of them.

9.2. Derived signatures

Derived signatures have been used in [28, 39, 45, 48]. For every ranked alphabet F which does not contain the special constant Ω , $\partial(F)$ denotes the *derived signature* of F which is defined as follows.

Let $K \geq \mathbf{Max}\{\rho(f) \mid f \in F\}$; the set $\mathcal{S} = \{1, \dots, K\}$ is taken as set of sorts. The signature $\partial(F)$ consists of $F \cup H$, where every element f of F_k , $k \geq 0$ is considered as a constant of sort k .

The set H consists of the following symbols:

- the new constant Ω_k of sort k for all k in \mathcal{S} ,
- the new constant $\pi_{j,k}$ of sort k for $1 \leq k \leq K$ and $1 \leq j \leq k$,
- the new function symbols \mathbf{comp}_k^n for n, k in \mathcal{S} ; its arity is $nkk \dots k$ (with n times k) and its sort is k .

Hence, all these definitions depend on K , but we do not make this dependence explicit in order to simplify the notations. We assume that K is chosen as large as needed.

With an ω -complete F -magma $\mathbf{D} = \langle D, \perp, \leq, \langle f_{\mathbf{D}} \rangle_{f \in F} \rangle$, we associate an ω -complete $\partial(F)$ -magma $\mathbf{M} = \langle \langle M_k \rangle_{k \in \mathcal{S}}, \langle \perp_k \rangle_{k \in \mathcal{S}}, \langle \leq_k \rangle_{k \in \mathcal{S}}, \langle f_{\mathbf{M}} \rangle_{f \in \partial(F)} \rangle$ as follows:

- $M_k = (D^k \rightarrow D)$ is the set of ω -continuous functions $D^k \rightarrow D$ (with $M_0 = D$);
- $\alpha \leq_k \alpha'$ iff $\alpha(d_1, \dots, d_k) \leq \alpha'(d_1, \dots, d_k)$ for all d_1, \dots, d_k in D ;
- $\perp_k = \Omega_{k\mathbf{M}}$ is the constant function $D^k \rightarrow D$ whose value is everywhere \perp ;
- $f_{\mathbf{M}} = f_{\mathbf{D}}$ if $f \in F$ (recall that f is a constant in $\partial(F)$ and that $f_{\mathbf{M}} \in M_k$ if $f \in F_k$);
- $\pi_{j,k\mathbf{M}}$ is the j th projection $D^k \rightarrow D$ ($\pi_{j,k\mathbf{M}}$ belongs to M_k),
- $\mathbf{comp}_{k\mathbf{M}}^n(\alpha, \beta_1, \dots, \beta_n) = \alpha \circ (\beta_1, \dots, \beta_n)$ for α in $(D^n \rightarrow D)$, β_1, \dots, β_n in $(D^k \rightarrow D)$.

This definition also applies when $n = 0$, $k \geq 0$, ($\mathbf{comp}_{k\mathbf{M}}^0(\alpha)$ denotes the constant function $D^k \rightarrow D$ yielding the value α , i.e., \mathbf{comp}_k^0 is the natural inclusion $M_0 \rightarrow M_k$), and when $k = 0$, $n \neq 0$, ($\mathbf{comp}_{0\mathbf{M}}^n(\alpha, \beta_1, \dots, \beta_n) = \alpha(\beta_1, \dots, \beta_n)$).

It is classical (and anyway easy to verify) that \mathbf{M} is ω -complete. It is called the *derived magma* of \mathbf{D} and is denoted by $\partial(\mathbf{D})$.

We denote by $\partial\mathcal{V}^\omega$ the class $\{\partial(\mathbf{D}) \mid \mathbf{D} \in \mathcal{V}^\omega\}$ (for some fixed alphabet F) and by $\partial\mathcal{V}^\omega(\mathcal{E})$ the class $\{\partial(\mathbf{D}) \mid \mathbf{D} \in \mathcal{V}^\omega(\mathcal{E})\}$.

9.1. Remark. All these definitions can be restricted to the unordered case by omitting Ω_k (and then $\partial_0(F)$ denotes $\partial(F)$ minus the constants Ω_k), \perp_k , \leq_k and taking for M_k the set $[D^k \rightarrow D]$ of total functions: $D^k \rightarrow D$. Doing so one defines for every F -magma \mathbf{D} a $\partial_0(F)$ -magma denoted by $\partial_0(\mathbf{D})$. We denote by $\partial_0\mathcal{V}$ the class of all such derived magmas and by $\partial_0\mathcal{V}(\mathcal{E})$ the class $\{\partial_0(\mathbf{D}) \mid \mathbf{D} \in \mathcal{V}(\mathcal{E})\}$.

Since our purpose here is to deal with recursive program schemes, we have introduced the ω -complete case first. All results of Sections 9.3 and 9.4 can be restricted to the unordered case and yield interesting corollaries. We shall not mention them each time.

9.3. \mathbf{beta} and its inverse

The elements of $M^\infty(\partial(F))_k$ may be considered as denotations for terms in $M_\Omega^\infty(F, X_k)$. The mapping $\mathbf{beta}_k: M(\partial(F))_k \rightarrow M_\Omega(F, X_k)$ associates a term with its abstract denotation. (It is called *yield* in many papers [36, 37, 39, 45], but the present terminology is chosen to recall its similarity with the β -reduction in λ -calculus.)

We shall define an inverse for \mathbf{beta}_k and call it \mathbf{comb}_k , because the elements of $M(\partial(F))_k$ can be considered as terms of a certain combinatory logic (this notation is used in [36, 37, 45, 48]).

Let $\mathbf{beta}_k: M(\partial(F))_k \rightarrow M_\Omega(F, X_k)$ be defined as follows:

$$\begin{aligned} \mathbf{beta}_k(\Omega_k) &= \Omega, & \mathbf{beta}_k(\pi_{j,k}) &= x_j, \\ \mathbf{beta}_k(f) &= f(x_1, \dots, x_k) \quad \text{for } f \text{ in } F_k, \\ \mathbf{beta}_k(\mathbf{comp}_k^n(t, t_1, \dots, t_n)) &= \mathbf{beta}_n(t)[\mathbf{beta}_k(t_1)/x_1, \dots, \mathbf{beta}_k(t_n)/x_n]. \end{aligned}$$

This function is monotone, hence, extends by ω -continuity into $\mathbf{beta}_k: M^\infty(\partial(F))_k \rightarrow M_\Omega^\infty(F, X_k)$.

We also define $\mathbf{comb}_k: M_\Omega(F, X_k) \rightarrow M(\partial(F))_k$ by

$$\begin{aligned} \mathbf{comb}_k(\Omega) &= \Omega_k, & \mathbf{comb}_k(x_j) &= \pi_{j,k}, \\ \mathbf{comb}_k(f(t_1, \dots, t_l)) &= \mathbf{comp}_k^l(f, \mathbf{comb}_k(t_1), \dots, \mathbf{comb}_k(t_l)) \end{aligned}$$

and extend it by ω -continuity into $\mathbf{comb}_k: M_\Omega^\infty(F, X_k) \rightarrow M^\infty(\partial(F))_k$.

9.2. Lemma. (1) For all t in $M_\Omega^\infty(F, X_k)$, $\mathbf{beta}_k(\mathbf{comb}_k(t)) = t$.

(2) For every ω -complete F -magma \mathbf{D} and all t in $M^\infty(\partial(F))_k$, $t_{\partial(\mathbf{D})} = \mathbf{beta}_k(t)_{\mathbf{D}}$.

Proof. Both assertions can be proved in the same way. They are first established for finite t 's by structural induction and the equalities extend to infinite t 's by ω -continuity. \square

Since \mathbf{comp}_n^k and $\pi_{j,k}$ receive a fixed interpretation, they satisfy some laws. We precise them in the next section.

9.4. Properties of \mathbf{comp}_k^n

We aim to characterize the congruence on $M^\infty(\partial(F))$ defined by $\partial \mathcal{V}^\omega \models t = t'$.

Let $\mathcal{A} \subseteq M(\partial(F), Y) \times M(\partial(F), Y)$ be the set of equations:

$$\begin{aligned} (9.4.1) \quad \mathbf{comp}_n^k(\Omega_k, x_1, \dots, x_k) &= \Omega_n, \\ (9.4.2) \quad \mathbf{comp}_n^k(\pi_{j,k}, x_1, \dots, x_k) &= x_j, \end{aligned}$$

$$(9.4.3) \quad \mathbf{comp}_n^n(f, \pi_{1,n}, \dots, \pi_{n,n}) = f,$$

$$(9.4.4) \quad \mathbf{comp}_n^k(\mathbf{comp}_k^m(z, y_1, \dots, y_m), x_1, \dots, x_k) \\ = \mathbf{comp}_n^m(z, \dots, \mathbf{comp}_n^k(y_i, x_1, \dots, x_k), \dots),$$

for all f in F_n , all k, m, n in \mathcal{S} . One assumes that $Y = \{z, x_1, \dots, y_1, \dots\}$ and that in each equation as above, z is of sort m , y_1, \dots, y_m are of sort k , and x_1, \dots, x_k are of sort n .

From the definition of $\partial(\mathbf{D})$ it is clear that the equations of \mathcal{A} are valid in every derived magma $\partial(\mathbf{D})$. Hence, $t \equiv_{\mathcal{A}} t'$ implies $\partial\mathcal{V}^\omega \models t = t'$. (The relation $\equiv_{\mathcal{A}}$ has been defined in Section 1.6.)

Let $\mathcal{E} = \bigcup \{\mathcal{E}_k \mid k \geq 0\}$ be a set of equations, $\mathcal{E}_k \subseteq M(F, X_k) \times M(F, X_k)$. We define $\partial(\mathcal{E})$ as the set of *ground* equations $\{\mathbf{comb}_k(t) = \mathbf{comb}_k(t') \mid k \geq 0, (t, t') \in \mathcal{E}_k\}$. It is clear by Lemma 9.2 that the equations of $\partial(\mathcal{E})$ hold in every derived magma $\partial(\mathbf{D})$ for \mathbf{D} in $\mathcal{V}^\omega(\mathcal{E})$. Hence, $t \equiv_{\mathcal{A} \cup \partial(\mathcal{E})} t'$ implies $\partial\mathcal{V}^\omega(\mathcal{E}) \models t = t'$. We aim to prove the converse which is not trivial since $\partial\mathcal{V}^\omega(\mathcal{E})$ is a proper subclass of $\mathcal{V}^\omega(\mathcal{A} \cup \partial(\mathcal{E}))$.

9.3. Lemma. *If $t \in M^\infty(\partial(F))_k$, then $\mathbf{comp}_k^k(t, \pi_{1,k}, \dots, \pi_{k,k}) \equiv_{\mathcal{A}} t$.*

Proof. We prove that $\mathbf{comp}_k^k(t, \pi_{1,k}, \dots, \pi_{k,k}) \leftrightarrow_{\mathcal{A}}^* t$ for all t in $M(\partial(F))_k$ by structural induction on t . The various cases to examine are $t = \Omega_k$, $t = \pi_{j,k}$, $t \in F_k$ and the results follow respectively from (9.4.1), (9.4.2), (9.4.3), and $t = \mathbf{comp}_k^m(t', s_1, \dots, s_m)$ and the result follows from (9.4.4) and the induction hypothesis for s_1, \dots, s_m .

By taking the limit of an increasing sequence, one gets the desired result for t in $M^\infty(\partial(F))_k$. \square

We could have added the equations

$$(9.4.5) \quad \mathbf{comp}_k^k(x, \pi_{1,k}, \dots, \pi_{k,k}) = x$$

to our set \mathcal{A} , of which (9.4.3) is just a special case. But they are not necessary. Lemma 9.3 shows that the equations (9.4.5) belong to the *inductive ω -theory* of \mathcal{A} (we do not define this concept formally but only appeal to the intuition of the reader who knows [52, 60, 77], where the inductive theory of a set of equations is investigated).

9.4. Theorem. *For t, t' in $M^\infty(\partial(F))$, $\partial\mathcal{V}^\omega(\mathcal{E}) \models t = t'$ iff $\mathcal{A} \cup \partial(\mathcal{E}) \models_\omega t = t'$ (iff $t \equiv_{\mathcal{A} \cup \partial(\mathcal{E})} t'$).*

Proof. The ‘if’ part follows from the remark that $\partial\mathcal{V}^\omega(\mathcal{E}) \subseteq \mathcal{V}^\omega(\mathcal{A} \cup \partial(\mathcal{E}))$.

For the ‘only if’ part, we construct, for every $m \geq 0$, an F -magma \mathbf{D} in $\mathcal{V}^\omega(\mathcal{E})$ such that, for all t, t' in $M^\infty(\partial(F))_m$, if $t_{\partial(\mathbf{D})} = t'_{\partial(\mathbf{D})}$, then $t \equiv_{\mathcal{A} \cup \partial(\mathcal{E})} t'$.

Let $\mathcal{A}' = \mathcal{A} \cup \partial(\mathcal{E})$ and m be fixed. Let \mathbf{E} be the ω -complete $\partial(F)$ -magma $[\mathbf{M}(\partial(F)) / \leq_{\mathcal{A}'}^0]^\infty$ (see Lemma 1.5, the presence of sorts does not create any difficulty). Hence, $t \mapsto t_{\mathbf{E}}$ is the canonical $\partial(F)$ -homomorphism $\mathbf{M}^\infty(\partial(F)) \rightarrow \mathbf{E}$. Let us recall from Lemma 1.5 that if $t, t' \in M^\infty(\partial(F))_k$, then $t_{\mathbf{E}} = t'_{\mathbf{E}}$ iff $t \equiv_{\mathcal{A}'} t'$.

We define an ω -complete F -magma \mathbf{D} by letting its domain D be $E_m = [M(\partial(F))_m / \leq_{\mathcal{A}'}^0]^\infty$ and $f_{\mathbf{D}}$ be defined by

$$(9.4.6) \quad f_{\mathbf{D}}(d_1, \dots, d_k) = \mathbf{comp}_{m\mathbf{E}}^k(f_{\mathbf{E}}, d_1, \dots, d_k),$$

for $f \in F_k$, $k \geq 0$. This function is ω -continuous since $\mathbf{comp}_{m\mathbf{E}}^k$ is, hence, \mathbf{D} is an ω -complete F -magma.

The following result is an extension of (9.4.6).

Claim 1. For every k , every t in $M_\Omega^\infty(F, X_k)$, every d_1, \dots, d_k in $D (= E_m)$,

$$t_{\mathbf{D}}(d_1, \dots, d_k) = \mathbf{comp}_{m\mathbf{E}}^k(\mathbf{comb}_k(t)_{\mathbf{E}}, d_1, \dots, d_k).$$

Proof. This can be proved for $t \in M_\Omega(F, X_k)$ by induction on the structure of t . We only consider the case $t = f(t_1, \dots, t_l)$ and we let $\vec{d} = (d_1, \dots, d_k)$:

$$\begin{aligned} t_{\mathbf{D}}(\vec{d}) &= f_{\mathbf{D}}(t_{1\mathbf{D}}(\vec{d}), \dots, t_{l\mathbf{D}}(\vec{d})) \\ &= \mathbf{comp}_{m\mathbf{E}}^l(f_{\mathbf{E}}, t_{1\mathbf{D}}(\vec{d}), \dots, t_{l\mathbf{D}}(\vec{d})) \\ &= \mathbf{comp}_{m\mathbf{E}}^l(f_{\mathbf{E}}, \mathbf{comp}_{m\mathbf{E}}^k(\mathbf{comb}_k(t_1)_{\mathbf{E}}, \vec{d}), \dots) \quad (\text{by induction}) \\ &= \mathbf{comp}_{m\mathbf{E}}^k(\mathbf{comp}_{k\mathbf{E}}^l(f_{\mathbf{E}}, \mathbf{comb}_k(t_1)_{\mathbf{E}}, \dots, \mathbf{comb}_k(t_l)_{\mathbf{E}}), \vec{d}) \\ &\quad (\text{since } \mathbf{E} \text{ satisfies (9.4.4)}), \end{aligned}$$

but $\mathbf{comp}_{k\mathbf{E}}^l(f_{\mathbf{E}}, \mathbf{comb}_k(t_1)_{\mathbf{E}}, \dots, \mathbf{comb}_k(t_l)_{\mathbf{E}}) = \mathbf{comb}_k(t)_{\mathbf{E}}$ from the definition of \mathbf{comb}_k , whence the result. This result extends to t in $M_\Omega^\infty(F, X_k)$ by ω -continuity. \square

Claim 2. $\mathbf{D} \in \mathcal{V}^\omega(\mathcal{E})$.

Proof. This claim is an immediate consequence of Claim 1 and the fact that $\mathbf{E} \in \mathcal{V}^\omega(\partial(\mathcal{E}))$. \square

Hence, $\partial(\mathbf{D}) \in \mathcal{V}^\omega(\mathcal{A}')$.

Claim 3. For every n , every s in $M^\infty(\partial(F))_n$, every t_1, \dots, t_n in $M^\infty(\partial(F))_m$:

$$\mathbf{comp}_m^n(s, t_1, \dots, t_n)_{\mathbf{E}} = \mathbf{beta}_n(s)_{\mathbf{D}}(t_{1\mathbf{E}}, \dots, t_{n\mathbf{E}}).$$

Proof. Note that $t_{1\mathbf{E}}, \dots, t_{n\mathbf{E}} \in D$, hence, the right-hand side of the equality to be established is well-defined. As in Claim 1, we prove Claim 3 for finite s 's first and then for infinite ones by ω -continuity.

The case $s = f \in F_n$ is an immediate consequence of (9.4.6). Let $s = \mathbf{comp}_n^k(s', s_1, \dots, s_k)$. Then

$$\begin{aligned}
\mathbf{comp}_m^n(s, t_1, \dots, t_n)_E &= \mathbf{comp}_m^n(\mathbf{comp}_n^k(s', s_1, \dots, s_k), t_1, \dots, t_n)_E \\
&= \mathbf{comp}_m^k(s', \mathbf{comp}_m^n(s_1, t_1, \dots, t_n), \dots)_E \\
&= \mathbf{beta}_k(s')_D(\mathbf{comp}_m^n(s_1, t_1, \dots, t_n)_E, \dots) \\
&= \mathbf{beta}_k(s')_D(\mathbf{beta}_n(s_1)_D(t_{1E}, \dots, t_{nE}), \dots) \\
&= \mathbf{beta}_k(s')[\mathbf{beta}_n(s_1), \dots, \mathbf{beta}_n(s_k)]_D(t_{1E}, \dots, t_{nE}) \\
&= \mathbf{beta}_n(\mathbf{comp}_n^k(s', s_1, \dots, s_k))_D(t_{1E}, \dots, t_{nE}) \\
&= \mathbf{beta}_n(s)_D(t_{1E}, \dots, t_{nE}).
\end{aligned}$$

The other cases are easier. \square

Proof of Theorem 9.4 (continued). Let $t, t' \in M^\infty(\partial(F))_m$ such that $\partial \mathcal{V}^\omega(\mathcal{E}) \models t = t'$. Claim 2 yields $t_{\partial(D)} = t'_{\partial(D)}$, hence,

$$\begin{aligned}
t_{\partial(D)}(\pi_{1, m_E}, \dots, \pi_{m, m_E}) &= \mathbf{beta}(t)_D(\pi_{1, m_E}, \dots, \pi_{m, m_E}) \\
&= \mathbf{comp}_m^m(t, \pi_{1, m}, \dots, \pi_{m, m})_E \quad (\text{by Claim 3}) \\
&= t_E \quad (\text{by Lemma 9.3}).
\end{aligned}$$

The same computation for t' gives $t_E = t'_E$ since $t_{\partial(D)} = t'_{\partial(D)}$, hence $t \equiv_{\mathcal{A}} t'$. \square

By restricting this proof to the unordered case one obtains the following corollary (with \mathcal{A}_0 being \mathcal{A} minus equation (9.4.1)).

9.5. Corollary. (1) For t, t' in $M(\partial_0(F))$, $\partial_0 \mathcal{V}(\mathcal{E}) \models t = t'$ iff $\mathcal{A}_0 \cup \partial(\mathcal{E}) \models t = t'$ iff $t \leftrightarrow_{\mathcal{A}_0 \cup \partial(\mathcal{E})}^* t'$.

(2) For every t, t' in $M(F, X_m)$, $t \leftrightarrow_{\mathcal{E}}^* t'$ iff $\mathbf{comb}_m(t) \leftrightarrow_{\mathcal{A}_0 \cup \partial(\mathcal{E})}^* \mathbf{comb}_m(t')$.

Proof. Part (1) is proved by inspecting the proof of Theorem 9.4.

Part (2) follows from part (1) and the remark that $t \leftrightarrow_{\mathcal{E}}^* t'$ iff $\mathcal{E} \models t = t'$ iff $\partial_0 \mathcal{V}(\mathcal{E}) \models \mathbf{comb}_m(t) = \mathbf{comb}_m(t')$ (by the restriction to the unordered case of Lemma 9.2). \square

The second part of Corollary 9.5 says that one can simulate an arbitrary rewriting system by a ground one and a fixed set of nonground rewriting rules. The consequences of this fact remain to be explored.

We now go back to the main purpose of this section.

9.5. Recursive applicative program schemes

9.5.1. Definitions

We recall the basic definitions of these program schemes investigated in various works [10, 25, 47, 56, 76, 82], to mention a few.

Let F and Φ be ranked alphabets with rank function ρ such that $F \cap \Phi = \emptyset$, $\Phi = \{\psi_1, \dots, \psi_n\}$. One lets $k_i = \rho(\psi_i)$ for all i .

An *algebraic system over F with set of unknowns Φ* is an n -tuple of equations $\Sigma = \langle \psi_1(x_1, \dots, x_{k_1}) = m_1, \dots, \psi_n(x_1, \dots, x_{k_n}) = m_n \rangle$ such that $m_i \in M(F \cup \Phi, X_{k_i})$ for all $i = 1, \dots, n$.

A *recursive applicative program scheme* is a pair (Σ, m) consisting of a system Σ as above and an element m of $M(F \cup \Phi, X_k)$ for some $k \geq 0$.

Let \mathbf{D} be an F -magma. An n -tuple $\bar{\Phi} = (\bar{\psi}_1, \dots, \bar{\psi}_n)$ of functions $\bar{\psi}_i: D^{k_i} \rightarrow D$ is a solution of Σ if, for all i in $[n]$, $\bar{\psi}_i = m_{i\mathbf{D}}$, where $\bar{\mathbf{D}}$ is the $(F \cup \Phi)$ -magma $\langle D, \langle f_{\mathbf{D}} \rangle_{f \in F}, \langle \bar{\psi} \rangle_{\psi \in \Phi} \rangle$. There may exist no solution for Σ in \mathbf{D} . If \mathbf{D} is ω -complete, then Σ has a least solution $\Phi_{\mathbf{D}} = (\psi_{1\mathbf{D}}, \dots, \psi_{n\mathbf{D}})$ in \mathbf{D} (where the $\psi_{i\mathbf{D}}$'s are ω -continuous).

If $m \in M(F \cup \Phi, X_k)$, then the *function defined by (Σ, m) in \mathbf{D}* is $m_{\mathbf{D}'}: D^k \rightarrow D$, where \mathbf{D}' is the $(F \cup \Phi)$ -magma associated with $\Phi_{\mathbf{D}}$ as $\bar{\mathbf{D}}$ was with $\bar{\Phi}$.

Finally, if m, m' are both in $M(F \cup \Phi, X_k)$ and \mathcal{E} is a set of equations, then $m \sim_{\Sigma, \mathcal{E}} m'$ if $m_{\mathbf{D}'} = m'_{\mathbf{D}'}$ for all \mathbf{D} in $\mathcal{V}^\omega(\mathcal{E})$. This relation means that (Σ, m) and (Σ, m') are equivalent in every interpretation satisfying \mathcal{E} . Its characterization is a basic result of the theory.

9.5.2. Construction

We now show how to associate a regular system S with Σ as above. Let $\mathcal{S} = \{1, \dots, K\}$ be a set of sorts with $K \geq \mathbf{Max}\{\rho(f) \mid f \in F \cup \Phi\}$. We let Φ be the set of unknowns of S . If ψ is of rank k in Φ , it is of sort k as an unknown of S .

We wish to define S in such a way that the least solution of Σ in \mathbf{D} , namely $\langle \psi_{1\mathbf{D}}, \dots, \psi_{n\mathbf{D}} \rangle$ (recall that $\psi_{i\mathbf{D}}$ is a continuous mapping: $D^{\rho(\psi_i)} \rightarrow D$), be also the least solution of S in $\mathbf{M} = \partial(\mathbf{D})$. We define S as the set of *regular* equations $\langle \psi_i = \mathbf{comb}_{k_i}(m_i); 1 \leq i \leq n \rangle$. Hence, S is a regular system over $\partial(F)$ with set of unknowns Φ . We denote it by $\partial(\Sigma)$. With these notations we have the following proposition.

9.6. Proposition. (1) *Let \mathbf{D} be an F -magma. An n -tuple $\bar{\Phi}$ as in Section 9.5.1 is a solution of Σ in \mathbf{D} iff it is a solution of $\partial(\Sigma)$ in $\partial(\mathbf{D})$.*

(2) *If \mathbf{D} is ω -complete the least solution of Σ in \mathbf{D} is also the least solution of $\partial(\Sigma)$ in $\partial(\mathbf{D})$.*

Proof. Part (1) is an immediate consequence of Lemma 9.2 and the definitions.

Part (2) is an immediate consequence of part (1). \square

9.7. Corollary. *Let Σ be an algebraic system as in Section 9.5.1, let $t, t' \in M(F \cup \Phi, X_k)$, let \mathcal{E} be a set of equations. Then $t \sim_{\Sigma, \mathcal{E}} t'$ iff $\mathbf{comb}_k(t) \sim_{\partial(\Sigma), \mathcal{A} \cup \partial(\mathcal{E})} \mathbf{comb}_k(t')$.*

This corollary shows that the investigation of the relation $\sim_{\Sigma, \mathcal{E}}$ for an algebraic system Σ reduces to that of the analogous relation for a regular system and for a different set of equations, namely $\mathcal{A} \cup \partial(\mathcal{E})$. It does not modify the difficulty of the decision problem for $\sim_{\Sigma, \mathcal{E}}$ (its decidability is open in the case $\mathcal{E} = \emptyset$ (see [22, 26]) and it is undecidable in general (see Proposition 13.8)), but it may help to define correct program transformations in a simpler and more powerful way than in [25, 63, 64]. This last aspect remains unexplored.

10. Powerset magmas

We have seen in Section 2.8 that context-free grammars can be considered as regular systems to be solved in $\mathcal{P}(X^*)$ equipped with the operation of union together with an operation of concatenation which is inherited from X^* . Following Mezei and Wright [73] we want to generalize this situation to the case of $\mathcal{P}(\mathbf{M})$, where \mathbf{M} is an arbitrary F -magma (possibly assumed to be in some $\mathcal{V}(\mathcal{E})$) and $\mathcal{P}(\mathbf{M})$ is also equipped with set union (denoted by $+$) together with F -operations inherited from \mathbf{M} in a standard way.

Hence, our purpose is to investigate the regular systems of which the right-hand sides are *polynomials*, i.e., terms of the form $t_1 + t_2 + \dots + t_k$, where $t_1, t_2, \dots, t_k \in M(F, U)$ (and U is the set of unknowns), their sets of solutions and their least solutions in the powerset magmas $\mathcal{P}(\mathbf{M})$ for \mathbf{M} in some variety $\mathcal{V}(\mathcal{E})$. Most of the results of Sections 2 to 7 will be applicable and new results will appear corresponding to the specific properties of set-union in $\mathcal{P}(\mathbf{M})$.

This section is devoted to algebraic preliminaries concerning powerset magmas.

10.1. Definition. Let F be a ranked alphabet which *does not* contain the special constant Ω . We denote by F_+ the ranked alphabet $F \cup \{+, \Omega\}$, where $+$ is binary (we shall always use the infix notation for it) and Ω is nullary (it will be used as in Section 1.5).

A *distributive* F -magma \mathbf{P} is an F_+ -magma satisfying the following set \mathcal{D} of equations:

$$\begin{aligned} x_1 + (x_2 + x_3) &= (x_1 + x_2) + x_3, & x_1 + x_2 &= x_2 + x_1, \\ x_1 + \Omega &= x_1, & x_1 + x_1 &= x_1, \\ f(x_1, x_2, \dots, \Omega, \dots, x_k) &= \Omega, \\ f(x_1, x_2, \dots, x_i + x'_i, \dots, x_k) &= f(x_1, \dots, x_k) + f(x_1, \dots, x_{i-1}, x'_i, \dots, x_k) \\ & \text{(for all } k \geq 1, \text{ all } f \in F_k). \end{aligned}$$

If A is a finite subset $\{a_1, \dots, a_n\}$ of the domain of \mathbf{P} , we use $\sum A$ as an abbreviation of $a_1 + a_2 + \dots + a_n$ (due to the associativity and commutativity of $+$ the order in which A is enumerated is irrelevant). If $A = \emptyset$, then $\sum A$ stands for $\Omega_{\mathbf{P}}$.

Let $\mathbf{M} = \langle M, \langle f_{\mathbf{M}} \rangle_{f \in F} \rangle$ be an F -magma. Its powerset F -magma is the F_+ -magma $\mathbf{P} = \langle \mathcal{P}(M), +_{\mathbf{P}}, \Omega_{\mathbf{P}}, \langle f_{\mathbf{P}} \rangle_{f \in F} \rangle$ such that, for all $A_1, \dots, A_k \subseteq M$, $A_1 +_{\mathbf{P}} A_2 = A_1 \cup A_2$, $\Omega_{\mathbf{P}} = \emptyset$, $f_{\mathbf{P}}(A_1, \dots, A_k) = \{f_{\mathbf{M}}(a_1, \dots, a_k) \mid a_1 \in A_1, \dots, a_k \in A_k\}$ for $f \in F_k$, $k \geq 1$ and $f_{\mathbf{P}} = \{f_{\mathbf{M}}\}$ for $f \in F_0$.

It is easy to verify that \mathbf{P} is a distributive F -magma. We shall denote it by $\mathcal{P}(\mathbf{M})$ in order to emphasize its dependence on \mathbf{M} .

We shall also use $\mathcal{P}_f(M)$ (where $\mathcal{P}(M)$ is replaced by $\mathcal{P}_f(M)$, the set of finite subsets of M) and $\mathcal{P}_\omega(M)$ (where $\mathcal{P}(M)$ is replaced by $\mathcal{P}_\omega(M)$ the set of countable subsets of M).

We shall denote by \mathcal{PV} the class of all powerset F -magmas and by $\mathcal{PV}(\mathcal{E})$ the class of all powerset F -magmas $\mathcal{P}(\mathbf{M})$ for \mathbf{M} in $\mathcal{V}(\mathcal{E})$. The notations $\mathcal{P}_f\mathcal{V}$, $\mathcal{P}_f\mathcal{V}(\mathcal{E})$, $\mathcal{P}_\omega\mathcal{V}$, $\mathcal{P}_\omega\mathcal{V}(\mathcal{E})$ will also be used (their meaning is clear).

10.2. Definition. Let X be a set of variables. A *monomial* is an element of $M(F, X)$. We assume that $M(F, X)$ is linearly ordered by a strict order $<$ in a fixed way such that $t < t'$ whenever $t \in X$ and $t' \in F(M(F, X))$. (This technical assumption will be used in Lemma 14.13.)

A *polynomial* is an element of $M(F_+, X)$ of the two possible forms Ω or $t_1 + \dots + t_n$ with $t_1, \dots, t_n \in M(F, X)$ and $t_1 < t_2 < \dots < t_n$.

We denote by $M^+(F, X)$ the set of polynomials.

If A is a finite subset of $M(F, X)$, we denote by $\sum A$ the polynomial $t_1 + t_2 + \dots + t_k$, where $A = \{t_1, \dots, t_k\}$ with $t_1 < t_2 < \dots < t_k$, and the polynomial Ω if $A = \emptyset$.

Every term t of $M(F_+, X)$ can be transformed into a polynomial by means of the following mapping \mathbf{Dev} associating with t a finite subset $\mathbf{Dev}(t)$ of $M(F, X)$, as follows

$$\begin{aligned} \mathbf{Dev}(\Omega) &= \emptyset, & \mathbf{Dev}(f) &= \{f\} \quad \text{if } f \in F_0 \cup X, \\ \mathbf{Dev}(t_1 + t_2) &= \mathbf{Dev}(t_1) \cup \mathbf{Dev}(t_2), \\ \mathbf{Dev}(f(t_1, \dots, t_k)) &= f(\mathbf{Dev}(t_1), \dots, \mathbf{Dev}(t_k)) \\ &= \{f(w_1, \dots, w_k) \mid w_1 \in \mathbf{Dev}(t_1), \dots, w_k \in \mathbf{Dev}(t_k)\}. \end{aligned}$$

We denote by $\mathbf{Pol}(t)$ the polynomial $\sum \mathbf{Dev}(t)$. The mapping \mathbf{Dev} corresponds to the development of a factorized expression.

10.3. Lemma. For t, t' in $M(F_+, X)$, the following holds

- (1) $t \leftrightarrow_{\mathfrak{D}}^* \mathbf{Pol}(t)$,
- (2) $t \leftrightarrow_{\mathfrak{D}}^* t'$ if and only if $\mathbf{Dev}(t) = \mathbf{Dev}(t')$ if and only if $\mathbf{Pol}(t) = \mathbf{Pol}(t')$.

Proof. Part (1) is proved by easy formal manipulations.

(2) One can prove that $t \leftrightarrow_{\mathcal{D}} t'$ implies $\mathbf{Dev}(t) = \mathbf{Dev}(t')$ by induction on the structure of t . The result now follows. \square

A consequence of this lemma is that the word problem for \mathcal{D} is decidable.

10.4. Definition. A distributive F -magma \mathbf{P} can be *canonically ordered* as follows:

$$d \leq d' \Leftrightarrow d' = d + d'.$$

This condition is equivalent to

$$\exists d'' \in P, d' = d + d''$$

since, for given such d'' , we have

$$d + d' = d + d + d'' = d + d'' = d'.$$

It is easy to verify that \leq is a partial order with least element $\Omega_{\mathbf{P}}$ and that the $f_{\mathbf{P}}$'s are monotone. Note that \mathbf{P} is not necessarily ω -complete. If \mathbf{P} is $\mathcal{P}_f(\mathbf{M})$, $\mathcal{P}_{\omega}(\mathbf{M})$, or $\mathcal{P}(\mathbf{M})$, this ordering is nothing else than set inclusion and \mathbf{P} is ω -complete in the last two cases.

We conclude these preliminaries by noting that the mapping $\mathbf{Dev}: M(F_+, X) \rightarrow \mathcal{P}(M(F, X))$ (Definition 10.2) is monotone, i.e., that $t < t'$ implies $\mathbf{Dev}(t) \subseteq \mathbf{Dev}(t')$ (this is easy to prove by induction on the structure of t). Hence, \mathbf{Dev} extends to $M^{\infty}(F_+, X)$ by ω -continuity, i.e., by $\mathbf{Dev}(t) = \bigcup \{\mathbf{Dev}(t') \mid t' < t, t \text{ is finite}\}$. Note in particular that $\mathbf{Dev}(t) = \emptyset$ if $t \in M_{\Omega}^{\infty}(F, X) - M(F, X)$ since every finite term t' such that $t' < t$ has at least one occurrence of Ω which yields $\mathbf{Dev}(t') = \emptyset$.

If \mathbf{M} is an F -magma and $t \in M(F, X_k)$, we also denote by $t_{\mathbf{M}}$ the extension of $t_{\mathbf{M}}$ to sets, i.e., if $A_1, \dots, A_k \subseteq M$,

$$t_{\mathbf{M}}(A_1, \dots, A_k) = \{t_{\mathbf{M}}(a_1, \dots, a_k) \mid a_1 \in A_1, \dots, a_k \in A_k\}.$$

10.5. Lemma. Let $\mathbf{P} = \mathcal{P}(\mathbf{M})$ or $\mathcal{P}_{\omega}(\mathbf{M})$, let A_1, \dots, A_k be subsets of M , let $t \in M^{\infty}(F_+, X_k)$:

- (1) $t_{\mathbf{P}}(A_1, \dots, A_k) = \bigcup \{s_{\mathbf{P}}(A_1, \dots, A_k) \mid s \in \mathbf{Dev}(t)\}$.
- (2) If $\mathbf{M} = \mathbf{M}(F)$, then $t_{\mathbf{P}}(A_1, \dots, A_k) = \mathbf{Dev}(t)[_{\text{OI}}A_1/x_1, \dots, A_k/x_k]$.
- (3) If $t \in M_{\Omega}^{\infty}(F, X_k) - M(F, X_k)$, then $t_{\mathbf{P}}(A_1, \dots, A_k) = \emptyset$.
- (4) If $t \in M(F, X_k)$ and if, for all $i = 1, \dots, k$,
 - (i) $\text{Card}(A_i) = 0$ implies $|t|_{x_i} > 0$,
 - (ii) $\text{Card}(A_i) \geq 2$ implies $|t|_{x_i} \leq 1$,

then

- (iii) $t_{\mathbf{P}}(A_1, \dots, A_k) = t_{\mathbf{M}}(A_1, \dots, A_k)$.

Assertion (4) also holds if $\mathbf{P} = \mathcal{P}_f(\mathbf{M})$ and A_1, \dots, A_k are finite.

Since if $\mathbf{M} = \mathbf{M}(F)$, $t_{\mathbf{M}}(A_1, \dots, A_k) = t_{[\text{IO}A_1/x_1, \dots, A_k/x_k]}$, part (4) of this lemma states conditions under which the IO-substitution and the OI-substitution give the same result.

Proof of Lemma 10.5. (1) The property follows from Lemma 10.3(1) for t in $M(F_+, X_k)$. It extends by continuity to the case where t is infinite.

(3) If $t \in M_{\Omega}^{\infty}(F, X_k) - M(F, X_k)$, then $\text{Dev}(t) = \emptyset$, hence, $t_{\mathbf{P}}(A_1, \dots, A_k) = \emptyset$ by (1).

(2) If $t \in M(F, X_k)$, then $t_{\mathbf{P}}(A_1, \dots, A_k) = t_{[\text{OI}A_1/x_1, \dots, A_k/x_k]}$ (by structural induction on t and the definition of OI-substitution). The result then follows from (1).

(4) We first assume that $A_i \neq \emptyset$ for all i . It is easy to prove that $t_{\mathbf{P}}(A_1, \dots, A_k) \supseteq t_{\mathbf{M}}(A_1, \dots, A_k)$ for all t in $M(F, X_k)$ even if (ii) does not hold.

We now prove that (ii) \Rightarrow (iv), where

$$(iv) \quad t_{\mathbf{P}}(A_1, \dots, A_k) \subseteq t_{\mathbf{M}}(A_1, \dots, A_k),$$

by induction on t . If $t \in X_k \cup F_0$, then (ii) and (iv) both hold (since $A_i \neq \emptyset$ for all i). Let $t = f(t_1, \dots, t_n)$ be such that (ii) holds. Hence, (ii) holds for t_1, \dots, t_n , hence, so does (iv) by the induction hypothesis.

So let $a \in t_{\mathbf{P}}(A_1, \dots, A_k)$. This means that $a = f_{\mathbf{M}}(a_1, \dots, a_n)$ for some a_1, \dots, a_n with $a_i \in t_{i\mathbf{P}}(A_1, \dots, A_k)$ for all i . By the induction hypothesis, $a_i \in t_{i\mathbf{M}}(A_1, \dots, A_k)$, hence,

$$(v) \quad a_i = t_{i\mathbf{M}}(a_1^i, \dots, a_k^i) \quad \text{for some } a_1^i \text{ in } A_1, \dots, a_k^i \text{ in } A_k.$$

If $\text{Card}(A_j) = 1$, then $a_j^i = a_j^1$ for i in $[n]$.

If $\text{Card}(A_j) > 1$, then x_j occurs in at most one of the t_i 's, say t_{i_j} , hence, one can replace a_j^i by $a_j^{i_j}$ in the equalities of form (v), i.e., one can assume that $a_j^i = a_j^1$ for all i in $[n]$. Hence, $a_i = t_{i\mathbf{M}}(a_1^1, \dots, a_k^1)$ for all i in $[n]$ and $a = t_{\mathbf{M}}(a_1^1, \dots, a_k^1)$. Since $a_i^1 \in A_i$, for $i = 1, \dots, k$, $a \in t_{\mathbf{M}}(A_1, \dots, A_k)$ and we are done.

Let us now assume that $A_i = \emptyset$ for some i . Hence, $t_{\mathbf{M}}(A_1, \dots, A_k) = \emptyset$. By condition (i), x_i occurs in t , hence, $t_{\mathbf{P}}(A_1, \dots, A_k) = \emptyset$ since $f_{\mathbf{P}}(\dots, \emptyset, \dots) = \emptyset$ for all f in F . Hence, (iii) also holds in this case. \square

Our purpose is to solve polynomial systems (formally defined in the next section) in powerset magmas $\mathcal{P}(\mathbf{M})$ for \mathbf{M} in $\mathcal{V}(\mathcal{E})$. In order to use the results of Sections 2 to 8, we want to consider a polynomial system to be solved in $\mathcal{P}(\mathbf{M})$ for \mathbf{M} in $\mathcal{V}(\mathcal{E})$ as a regular system to be solved in a magma belonging to $\mathcal{V}^{\omega}(\mathcal{E}')$ for some set of equations \mathcal{E}' , in such a way that \mathcal{E}' describes $\mathcal{P}(\mathbf{M})$ as well as possible. A natural candidate is clearly $\mathcal{E}' = \mathcal{D} \cup \mathcal{E}$, but this only works if $\mathcal{P}(\mathbf{M}) \in \mathcal{V}(\mathcal{E})$ for all \mathbf{M} in $\mathcal{V}(\mathcal{E})$. The following result due to Gautam [49] (see also [79]) shows that \mathcal{E} cannot be arbitrary.

10.6. Proposition. *Let \mathcal{C} be a variety. Then $\mathcal{P}(\mathbf{M}) \in \mathcal{C}$ for all \mathbf{M} in \mathcal{C} iff $\mathcal{C} = \mathcal{V}(\mathcal{E})$ for some set \mathcal{E} of linear and balanced equations.*

Proof. We shall only need the ‘if’ part which is an immediate consequence of Lemma 10.5(4). See [79] for the ‘only if’ part of the statement. \square

10.7. Examples. The variety of monoids ($F = \{., e\}$ and $\mathcal{E} = \{(x.y).z = x.(y.z), x.e = x, e.x = x\}$) and the variety of monadic algebras (F consists of unary symbols and a constant e , $\mathcal{E} = \emptyset$) are two useful examples in language theory (see Sections 2.8, 11.4.1, and 11.4.2).

The variety of monoids with a zero a such that $x.a = a$ and $a.x = a$ or the variety of groups are not closed by the powerset operation. (In the case of monoids with zero one has $\emptyset.\{a\} = \emptyset$ so that the equation $x.\{a\} = \{a\}$ is not valid as it should be if this variety were closed under powerset.)

Our next purpose is to characterize the relation $\mathcal{PV}(\mathcal{E}) \models t = t'$. For a set \mathcal{E} of linear and balanced equations, we shall prove that $\mathcal{PV}(\mathcal{E}) \models t = t'$ iff $\mathcal{V}^\omega(\mathcal{D} \cup \mathcal{E}) \models t = t'$, i.e., that the ω -equational theory of $\mathcal{PV}(\mathcal{E})$ is the same as that of $\mathcal{V}^\omega(\mathcal{D} \cup \mathcal{E})$ although $\mathcal{PV}(\mathcal{E})$ is strictly included in $\mathcal{V}^\omega(\mathcal{D} \cup \mathcal{E})$. This proof needs some technical definitions.

For every t in $M_\Omega(F, X)$ we denote by $[t]_{\mathcal{E}}$ the equivalence class of t modulo $\leftrightarrow_{\mathcal{E}}^*$ and for $T \subseteq M_\Omega(F, X)$, we denote by $[T]_{\mathcal{E}}$ the set $\{[t]_{\mathcal{E}} \mid t \in T\}$. In the following proposition we omit the subscript \mathcal{E} .

10.8. Proposition. *Let \mathcal{E} be a set of linear and balanced equations. For all t, t' in $M(F_+, X)$,*

$$(1) \quad t \leftrightarrow_{\mathcal{E} \cup \mathcal{D}}^* t' \text{ iff } [\mathbf{Dev}(t)] = [\mathbf{Dev}(t')],$$

$$(2) \quad t \leq_{\mathcal{E} \cup \mathcal{D}}^0 t' \text{ iff } [\mathbf{Dev}(t)] \subseteq [\mathbf{Dev}(t')].$$

For t, t' in $M^\infty(F_+, X)$,

$$(3) \quad t \leq_{\mathcal{E} \cup \mathcal{D}} t' \text{ iff } [\mathbf{Dev}(t)] \subseteq [\mathbf{Dev}(t')],$$

$$(4) \quad t \equiv_{\mathcal{E} \cup \mathcal{D}} t' \text{ iff } [\mathbf{Dev}(t)] = [\mathbf{Dev}(t')].$$

Proof. (1) If $[\mathbf{Dev}(t)] = [\mathbf{Dev}(t')]$, then $t \leftrightarrow_{\mathcal{D}}^* \mathbf{Pol}(t) \leftrightarrow_{\mathcal{E} \cup \mathcal{D}}^* \mathbf{Pol}(t') \leftrightarrow_{\mathcal{D}}^* t'$, hence, $t \leftrightarrow_{\mathcal{E} \cup \mathcal{D}}^* t'$.

Conversely, if $t \leftrightarrow_{\mathcal{E} \cup \mathcal{D}} t'$, then $\mathbf{Dev}(t) = \mathbf{Dev}(t')$.

Let us consider the case of $t \leftrightarrow_{\mathcal{E}} t'$. We do the proof by induction on the structure of t .

Case 1: $t = f(t_1, \dots, t_k)$, $t' = f(t'_1, \dots, t'_k)$ and $t_i \leftrightarrow_{\mathcal{E}} t'_i$ for some i , say $i = 1$, and $t_j = t'_j$ for $j = 2, \dots, k$. Then

$$\begin{aligned} [\mathbf{Dev}(t)] &= \{[w] \mid w \in f(\mathbf{Dev}(t_1), \dots, \mathbf{Dev}(t_k))\} \\ &= \{f_{\mathbf{M}}([w_1], \dots, [w_k]) \mid w_1 \in \mathbf{Dev}(t_1), \dots, w_k \in \mathbf{Dev}(t_k)\} \\ &= f_{\mathcal{D}(\mathbf{M})}([\mathbf{Dev}(t_1)], \dots, [\mathbf{Dev}(t_k)]), \end{aligned}$$

where $\mathbf{M} = \mathbf{M}(F) / \leftrightarrow_{\mathcal{E}}^*$.

From a similar characterization of $[\mathbf{Dev}(t')]$ and the equality $[\mathbf{Dev}(t_1)] = [\mathbf{Dev}(t'_1)]$, one gets $[\mathbf{Dev}(t)] = [\mathbf{Dev}(t')]$.

If $t = t_1 + t_2$, $t' = t'_1 + t'_2$ with t_i, t'_i as above, the proof is similar.

Case 2: $t = s[t_1, \dots, t_k]$, $t' = s'[t_1, \dots, t_k]$ for some $(s, s') \in \mathcal{E}$ (with $\mathbf{Var}(s) = \mathbf{Var}(s') = X_k$) and some t_1, \dots, t_k in $M(F_+, X)$. It is easy to prove that

$$\mathbf{Dev}(t) = \{s[w_1, \dots, w_k] \mid w_1 \in \mathbf{Dev}(t_1), \dots, w_k \in \mathbf{Dev}(t_k)\}$$

(this uses the linearity of s and the fact that $\mathbf{Var}(s) = X_k$) and similarly for t' . This gives the desired equality: $[\mathbf{Dev}(t)] = [\mathbf{Dev}(t')]$.

(2) If $[\mathbf{Dev}(t)] \subseteq [\mathbf{Dev}(t')]$, then $t \leftrightarrow_{\mathcal{D}}^* \mathbf{Pol}(t) + \Omega$ ($\langle \cup \leftrightarrow_{\mathcal{D} \cup \mathcal{E}}^* \mathbf{Pol}(t') \leftrightarrow_{\mathcal{D}}^* t'$). Hence, $t \leq_{\mathcal{D} \cup \mathcal{E}}^0 t'$. Conversely, if $t \leq_{\mathcal{E} \cup \mathcal{D}}^0 t'$, then one shows that $[\mathbf{Dev}(t)] \subseteq [\mathbf{Dev}(t')]$ by an extension of the proof of part (1) using the extra case where $t = \Omega$ for which $\mathbf{Dev}(t) = \emptyset \subseteq \mathbf{Dev}(t')$, whatever t' might be.

Parts (3) and (4) easily follow from (2) and the various definitions. \square

10.9. Example. We show that Proposition 10.8(1) is false if \mathcal{E} is not linear or not balanced. Let $\mathcal{E} = \{g(x) = a\}$. Then $a \leftrightarrow_{\mathcal{E}} g\Omega \leftrightarrow_{\mathcal{D}} \Omega$ and $[\mathbf{Dev}(a)] = \{[a]\} \neq \emptyset$, whereas $[\mathbf{Dev}(\Omega)] = \emptyset$. If $\mathcal{E}' = \{f(x, x) = gx\}$, then

$$t = g(a+b) \leftrightarrow_{\mathcal{E}'} f(a+b, a+b) = t',$$

$$[\mathbf{Dev}(t)] = \{[ga], [gb]\},$$

$$[\mathbf{Dev}(t')] = \{[f(a, a)], [f(b, b)], [f(a, b)], [f(b, a)]\} \supsetneq \mathbf{Dev}(t)$$

since $[f(a, b)] = \{f(a, b)\}$, hence, does not belong to $[\mathbf{Dev}(t)]$.

The following is a corollary of Proposition 10.8.

10.10. Corollary. (1) $M(F_+, X) / \leftrightarrow_{\mathcal{D} \cup \mathcal{E}}^*$ is isomorphic to $\mathcal{P}_f(M(F, X) / \leftrightarrow_{\mathcal{E}}^*)$.

(2) $M^\infty(F_+, X) / \equiv_{\mathcal{D} \cup \mathcal{E}}$ is isomorphic to $\mathcal{P}_\omega(M(F, X) / \leftrightarrow_{\mathcal{E}}^*)$.

Proof. (1) Let h be the mapping $M(F_+, X) \rightarrow \mathcal{P}_f(M(F, X) / \leftrightarrow_{\mathcal{E}}^*)$ such that $h(t) = [\mathbf{Dev}(t)]$. By Proposition 10.8(1), $h(t) = h(t')$ iff $t \leftrightarrow_{\mathcal{E} \cup \mathcal{D}}^* t'$. Hence, h factors through $M(F_+, X) / \leftrightarrow_{\mathcal{E} \cup \mathcal{D}}^*$ and this defines the required isomorphism.

(2) Similar argument with $h': M^\infty(F_+, X) \rightarrow \mathcal{P}_\omega(M(F, X) / \leftrightarrow_{\mathcal{E}}^*)$ such that $h'(t) = [\mathbf{Dev}(t)]$ by using Proposition 10.8(4). For the surjectivity, let $A = \{[w_1], [w_2], \dots, [w_n], \dots\}$ be a countable subset of $M(F, X) / \leftrightarrow_{\mathcal{E}}^*$, let $a = w_1 + w_2 + \dots + w_n + \dots$ (a is an element of $M^\infty(F_+, X)$). Hence, $h'(a) = A$. \square

10.11. Theorem. Let \mathcal{E} be a set of linear and balanced equations.

(1) For t, t' in $M(F_+, X)$ the following conditions are equivalent:

- (i) $\mathcal{PV}(\mathcal{E}) \models t = t'$,
- (ii) $\mathcal{P}_f\mathcal{V}(\mathcal{E}) \models t = t'$,
- (iii) $\mathcal{D} \cup \mathcal{E} \models t = t'$,
- (iv) $t \leftrightarrow_{\mathcal{D} \cup \mathcal{E}}^* t'$.

(2) For t, t' in $M^\infty(F_+, X)$, the following conditions are equivalent:

- (i) $\mathcal{P}\mathcal{V}(\mathcal{E}) \models t = t'$,
- (ii) $\mathcal{P}_\omega \mathcal{V}(\mathcal{E}) \models t = t'$,
- (iii) $\mathcal{D} \cup \mathcal{E} \models_\omega t = t'$,
- (iv) $t \equiv_{\mathcal{D} \cup \mathcal{E}} t'$.

Proof. (1) (i) \Rightarrow (ii) since $\mathcal{P}_f(\mathbf{M})$ is a subobject of $\mathcal{P}(\mathbf{M})$ with respect to the structure of a distributive F -magma.

(ii) \Rightarrow (iv): Let $\mathbf{M} = \mathbf{M}(F, X) / \leftrightarrow_{\mathcal{E}}^*$ and $\mathbf{M}' = \mathcal{P}_f(\mathbf{M})$. Let $\bar{x}_i = \{[x_i]\}$ for all i (note that $\bar{x}_i \in \mathbf{M}'$). By Lemma 10.5, one has, for all s in $M(F, X_k)$,

$$s_{\mathbf{M}'}(\bar{x}_1, \dots, \bar{x}_k) = s_{\mathbf{M}}(\bar{x}_1, \dots, \bar{x}_k) = \{s_{\mathbf{M}}([x_1], \dots, [x_k])\} = \{[s]\}.$$

If $t \in M(F_+, X_k)$, then

$$\begin{aligned} t_{\mathbf{M}'}(\bar{x}_1, \dots, \bar{x}_k) &= \bigcup \{s_{\mathbf{M}'}(\bar{x}_1, \dots, \bar{x}_k) \mid s \in \mathbf{Dev}(t)\} \\ &= \bigcup \{\{[s]\} \mid s \in \mathbf{Dev}(t)\} = [\mathbf{Dev}(t)]. \end{aligned}$$

If $t, t' \in M(F_+, X_k)$ and $\mathcal{P}_f \mathcal{V}(\mathcal{E}) \models t = t'$, then $t_{\mathbf{M}'} = t'_{\mathbf{M}'}$ and $[\mathbf{Dev}(t)] = [\mathbf{Dev}(t')]$. Hence, $t \leftrightarrow_{\mathcal{D} \cup \mathcal{E}}^* t'$ by Proposition 10.8(1).

(iv) \Leftrightarrow (iii) is proved by Lemma 1.4.

(iii) \Rightarrow (i) follows from Proposition 10.6.

(2) The proof is similar. For the implication (ii) \Rightarrow (iv), one takes $\mathbf{M}' = \mathcal{P}_\omega(\mathbf{M})$ instead of $\mathcal{P}_f(\mathbf{M})$, and one uses Proposition 10.8(4) to conclude that $t \equiv_{\mathcal{D} \cup \mathcal{E}} t'$ if $[\mathbf{Dev}(t)] = [\mathbf{Dev}(t')]$. \square

11. Polynomial regular systems

We now define the polynomial (regular) systems and the relations associated with them.

11.1. Definition of polynomial systems

11.1. Definition. A *polynomial regular system of equations over F* (or more shortly a *polynomial system*) is a regular system over F_+ , $S = \langle u_i = t_i; 1 \leq i \leq n \rangle$ such that each t_i is a polynomial.

Regular systems over F_+ will be more shortly called *+regular systems*. It follows from Lemma 10.3 that for every +regular system S there exists a unique polynomial system S' such that $S \text{ rewr}_{\mathcal{D}} S'$. We shall denote it by $\mathbf{Pol}(S)$. It is clear that $\mathbf{Pol}(S) \approx_{\mathcal{D}} S$, hence, since polynomial and +regular systems will always be solved in distributive magmas, there is nearly no difference between them. Nevertheless the distinction will be useful for making precise statements (and proofs) concerning transformations of systems in Sections 12, 13, 14 below.

The generic polynomial system will be $S = \langle u_i = p_i; 1 \leq i \leq n \rangle$, where p_i is a polynomial in $M^+(F, \text{Unk}(S))$. If S is a $+$ -regular system and \mathbf{M} is an F -magma, we denote by $\mathbf{Psol}_{\mathbf{M}}(S)$ the set of all its solutions in $\mathcal{P}(\mathbf{M})$. Since $\mathcal{P}(\mathbf{M})$ is ω -complete, S also has a least solution denoted by $\mu\text{-Psol}_{\mathbf{M}}(S)$. Such least solutions have been investigated in [41, 73]. A subset A of M is *equational* if it is a component of $\mu\text{-Psol}_{\mathbf{M}}(S)$ for some polynomial system S (or equivalently, some $+$ -regular system S) (some results concerning equational sets can be found in [67] and the articles cited there).

11.2. Polynomial systems of special types

In Definition 11.1, we consider a polynomial system as a regular system over an alphabet of a special type, to be solved in a restricted class of magmas (namely \mathcal{PV}). We can also consider a regular system as a polynomial system, where neither $+$ nor Ω occurs. But the class of magmas where a regular system is solved, namely \mathcal{V} or \mathcal{V}^ω is larger than \mathcal{PV} . Hence, this latter point of view is purely syntactical. It will nevertheless guide the following definitions which extend the one given in Section 2.1.

11.2. Definition. Let S be a polynomial system $\langle u_i = p_i; 1 \leq i \leq n \rangle$, let $U = \{u_1, \dots, u_n\}$. It is *uniform* if $\text{Dev}(p_i) \subseteq F(U)$ for all i . It is *quasi-uniform* if $\text{Dev}(p_i) \subseteq F(U) \cup U$ for all i . It satisfies the *Greibach condition* (or is a *Greibach system*) if $\text{Dev}(p_i) \subseteq F(M(F, U))$ for all i .

Hence, in the first two cases, S is not necessarily uniform or quasi-uniform as a regular system over F_+ .

11.3. Equivalences and preorders on $+$ -regular systems

Let S and S' be two $+$ -regular systems with the same set of unknowns U and let \mathcal{C} be a class of F -magmas. We shall investigate the following relations:

$$t \approx_{\mathcal{S}, \mathcal{C}}^p t' \quad \text{iff} \quad t_{\mathcal{P}(\mathbf{M})}(m) = t'_{\mathcal{P}(\mathbf{M})}(m) \quad \text{for all } \mathbf{M} \text{ in } \mathcal{C} \text{ and all } m \in \mathbf{Psol}_{\mathbf{M}}(S),$$

$$S \leq_{\mathcal{C}}^p S' \quad \text{iff} \quad \mathbf{Psol}_{\mathbf{M}}(S) \subseteq \mathbf{Psol}_{\mathbf{M}}(S') \quad \text{for all } \mathbf{M} \text{ in } \mathcal{C},$$

$$S \approx_{\mathcal{C}}^p S' \quad \text{iff} \quad \mathbf{Psol}_{\mathbf{M}}(S) = \mathbf{Psol}_{\mathbf{M}}(S') \quad \text{for all } \mathbf{M} \text{ in } \mathcal{C}.$$

The superscript p recalls that one deals with $+$ -regular systems to be solved in *powerset* magmas.

Similar definitions can be given for least solutions:

$$t \sim_{\mathcal{C}}^p t' \quad \text{iff} \quad t_{\mathcal{P}(\mathbf{M})}(\mu\text{-Psol}_{\mathbf{M}}(S)) = t'_{\mathcal{P}(\mathbf{M})}(\mu\text{-Psol}_{\mathbf{M}}(S')) \quad \text{for all } \mathbf{M} \text{ in } \mathcal{C},$$

$$S \leq_{\mathcal{C}}^p S' \quad \text{iff} \quad \mu\text{-Psol}_{\mathbf{M}}(S) \in \mathbf{Psol}_{\mathbf{M}}(S') \quad \text{for all } \mathbf{M} \text{ in } \mathcal{C}, \text{ i.e.,}$$

$$\text{iff } \mu\text{-Psol}_{\mathbf{M}}(S') \subseteq \mu\text{-Psol}_{\mathbf{M}}(S) \quad \text{for all } \mathbf{M} \text{ in } \mathcal{C},$$

$$S \sim_{\mathcal{C}}^p S' \quad \text{iff} \quad \mu\text{-Psol}_{\mathbf{M}}(S) = \mu\text{-Psol}_{\mathbf{M}}(S') \quad \text{for all } \mathbf{M} \text{ in } \mathcal{C}$$

$$\text{(i.e., iff } S \leq_{\mathcal{C}}^p S' \text{ and vice versa).}$$

As before we replace the subscript \mathcal{C} by \mathbf{M} , by \mathcal{E} , or delete it if $\mathcal{C} = \{\mathbf{M}\}$, $\mathcal{C} = \mathcal{V}(\mathcal{E})$ or $\mathcal{C} = \mathcal{V}$, respectively.

As for $\approx_{\mathcal{E}}$, $\leq_{\mathcal{E}}$, $\sim_{\mathcal{E}}$, and $\cong_{\mathcal{E}}$ some implications immediately follow from the definitions:

$$(11.3.1) \quad t \approx_{S, \mathcal{C}}^p t' \text{ implies } t \sim_{S, \mathcal{C}}^p t',$$

$$(11.3.2) \quad S \cong_{\mathcal{C}}^p S' \text{ implies } S \leq_{\mathcal{C}}^p S',$$

$$(11.3.3) \quad S \approx_{\mathcal{C}}^p S' \text{ implies } S \sim_{\mathcal{C}}^p S',$$

$$(11.3.4) \quad S \cong_{\mathcal{C}}^p S' \text{ iff } p_i \approx_{S, \mathcal{C}}^p p'_i \text{ for all } i = 1, \dots, n,$$

$$(11.3.5) \quad S \leq_{\mathcal{C}}^p S' \text{ iff } p_i \sim_{S, \mathcal{C}}^p p'_i \text{ for all } i = 1, \dots, n.$$

If we now assume that \mathcal{E} is a set of linear and balanced equations, then

$$(11.3.6) \quad t \approx_{S, \mathcal{E} \cup \mathcal{E}} t' \text{ implies } t \approx_{S, \mathcal{E}}^p t',$$

$$(11.3.7) \quad S \cong_{\mathcal{E} \cup \mathcal{E}} S' \text{ implies } S \cong_{\mathcal{E}}^p S',$$

and similarly for $\approx_{\mathcal{E} \cup \mathcal{E}}$, $\sim_{S, \mathcal{E} \cup \mathcal{E}}$, $\leq_{\mathcal{E} \cup \mathcal{E}}$, and $\sim_{\mathcal{E} \cup \mathcal{E}}$. This means that every transformation which is correct w.r.t. $\approx_{\mathcal{E} \cup \mathcal{E}}$ (respectively $\sim_{\mathcal{E} \cup \mathcal{E}}$) is correct w.r.t. $\approx_{\mathcal{E}}^p$ (respectively $\sim_{\mathcal{E}}^p$).

The completeness of such rules w.r.t. $\approx_{\mathcal{E}}^p$ (or $\sim_{\mathcal{E}}^p$) depends on the converse implications of (11.3.6) and (11.3.7) which are not obvious either. These questions will be the subject of the next sections. We now define several algebraic structures allowing to apply these notions to finite state automata and context-free grammars.

11.4. Examples

11.4.1. Finite-state automata

With every finite alphabet T we associate the ranked alphabet $T_u = T \cup \{e\}$ with $\rho(a) = 1$ for a in T and $\rho(e) = 0$. We let U_T denote the T_u -magma with domain T^* , ε as value of e and the function $u \rightarrow ua$ as the unary function associated with a for a in T . Actually U_T is isomorphic to $\mathbf{M}(T_u)$.

We define an automaton over T as a 4-tuple $\langle T, Q, \tau, Q_I \rangle$, where Q is the finite set of states, $Q_I \subseteq Q$ is the set of initial states and $\tau \subseteq Q \times (T \cup \{\varepsilon\}) \times Q$ is the transition table. For every q in Q , we denote by $L(A, q)$ the language of all words of T^* corresponding to some computation of A starting at some state in Q_I and ending at q . The language accepted by (A, Q_F) , where $Q_F \subseteq Q$ is a set of final states, is $L(A, Q_F) = \bigcup \{L(A, q) \mid q \in Q_F\}$.

With an automaton A as above we associate a polynomial system S_A defined as follows. Its set of unknowns is $U = \{u_q \mid q \in Q\}$. Its equations are $u_q = \sum P_q$, where P_q is the set of all terms of the following three forms:

- (i) $a(u_{q'})$ for all $a \in T$, $q' \in Q$ such that $(q', a, q) \in \tau$,
- (ii) $u_{q'}$ for all $q' \in Q$ such that $(q', \varepsilon, q) \in \tau$,
- (iii) e whenever $q \in Q_I$.

It is a classical result that the least solution of S_A in $\mathcal{P}(U_T)$ is nothing else than the $\mathbf{Card}(Q)$ -tuple $(L(A, q))_{q \in Q}$ (where $L(A, q)$ is the value of u_q).

It is clear that a polynomial system over T_u is of the form S_A for some automaton A (respectively for some automaton A without ε -transition) iff it is quasi-uniform (respectively uniform).

11.4.2. Context-free grammars

With every finite alphabet T (such that $\varepsilon \notin T$), we associate the ranked alphabets $T_s = T \cup \{.\}$ and $T_m = T_s \cup \{\varepsilon\}$. We let \mathcal{E}_s be the set of equations $\{(x.y).z = x.(y.z)\}$ and $\mathcal{E}_m = \mathcal{E}_s \cup \{x.\varepsilon = x, \varepsilon.x = x\}$. Hence, $\mathcal{V}(\mathcal{E}_s)$ is the variety of semigroups and $\mathcal{V}(\mathcal{E}_m)$ is the variety of monoids. We denote by \mathbf{T}^+ (respectively by \mathbf{T}^*) the free semigroup (respectively the free monoid) generated by T .

We have shown in Section 2.8 how a +-regular system can be associated with a context-free grammar $G = \langle N, T, P \rangle$. From now on, we shall denote by S_G the unique polynomial system corresponding to this regular system as explained in Section 11.1. It is clear that G has no ε -rule iff S_G is a polynomial system over T_s .

The N -tuple $L(G, u)_{u \in N}$ of languages generated by G is the least solution of S_G in $\mathcal{P}(\mathbf{T}^*)$ (or in $\mathcal{P}(\mathbf{T}^+)$ if G has no ε -rule). Hence, $L(G, u) = L(G, u')$ if and only if $u \sim_{S_G, \mathcal{P}(\mathbf{T}^*)} u'$.

Conversely, let $S = \langle u = t_u; u \in N \rangle$ be a +-regular system over T_m (respectively over T_s). There exists a unique context-free grammar (respectively a unique ε -free context-free grammar) G such that $S_G = \mathbf{Pol}(S)$.

Hence, all our results concerning +-regular systems and their solutions in $\mathcal{P}(\mathbf{T}^*)$ (or $\mathcal{P}(\mathbf{T}^+)$) or, more generally, in $P(\mathbf{M})$ for \mathbf{M} in $\mathcal{V}(\mathcal{E}_m)$ (or \mathbf{M} in $\mathcal{V}(\mathcal{E}_s)$) can be formulated in terms of context-free grammars. In Section 17 we shall show that, conversely, many results on context-free grammars can be conveniently reformulated and proved in terms of polynomial systems and transformations of such systems.

12. Polynomial systems and their sets of solutions

Most of this chapter will be devoted to the proof of the following theorem.

12.1. Theorem. *Let S be a polynomial regular system and t, t' belong to $M(F_+, \mathbf{Unk}(S))$. Then $t \approx_S^p t'$ if and only if $t \approx_{S, \mathcal{Q}} t'$ iff $t \leftrightarrow_{S \cup \mathcal{Q}}^* t'$.*

Although this theorem is similar to Theorem 3.2(1), its proof is much more difficult. The reason is that the F_+ -magma $\mathbf{M}(F_+, U) / \leftrightarrow_{\mathcal{Q}, S}^*$ is *not* a powerset F -magma. Hence, the proof method of Theorem 3.2(1) does not apply.

Our proof will use several steps, each of them needing technical constructions and lemmas. Let us immediately mention that our proof does not extend so as to prove that $t \approx_{S, \mathcal{Z}}^p t'$ iff $t \leftrightarrow_{S \cup \mathcal{Z} \cup \mathcal{Q}}^* t'$. The characterization of the relation $t \approx_{S, \mathcal{Z}}^p t'$ remains an open question (see Question 12.22).

We begin with the notion of a polynomial system which is reduced w.r.t. the relation \approx^P . Another one, relative to the relation \sim^P , will be defined later (see Definition 14.3).

12.2. Definition. Let S be a polynomial system (as in Section 11.1). We denote by $\mathbf{Unk}_{\approx}^0(S)$ the set of unknowns u of S such that $u \approx_{\mathcal{P}}^0 \Omega$, i.e., the value of which is \emptyset for all solution of S (in a power-set F -magma). We let $\mathbf{Unk}_{\approx}^+(S) = \mathbf{Unk}(S) - \mathbf{Unk}_{\approx}^0(S)$. A more precise notation would have been $\mathbf{Unk}_{\approx^P}^0(S)$ (or equivalently, $\mathbf{Unk}_{\approx^0}^0(S)$) since $\mathbf{Unk}_{\approx}^0(S)$ does not denote the same set according to whether S is considered as a regular system or as a polynomial one. But this simplification in notations will not cause any ambiguity in the sequel.

We say that S is \approx -reduced if, for all i in $[n]$, $p_i \in M^+(F, \mathbf{Unk}_{\approx}^+(S))$, and $p_i = \Omega$ iff $u_i \in \mathbf{Unk}_{\approx}^0(S)$.

We now give an algorithm to compute $\mathbf{Unk}_{\approx}^0(S)$ and to \approx -reduce the system S . Let $U_0 = \emptyset$, $U_{i+1} = U_i \cup \{u_j \mid \text{every monomial in } p_j \text{ has at least one unknown in } U_i\}$ (note that $U_1 = \{u_j \mid p_j = \Omega\}$). Let $U_{\infty} = U_0 \cup U_1 \cup U_2 \cup \dots \cup U_i \cup \dots$. Since U is finite, U_{∞} is computable.

Let $S' = \langle u_i = p'_i; i \in [n] \rangle$, where $p'_i = \Omega$ if $u_i \in U_{\infty}$ and $p'_i = \sum (\text{Dev}(p_i) \cap M(F, U - U_{\infty}))$ if $u_i \notin U_{\infty}$. We shall denote S' by $\text{Red}_{\approx}(S)$. With these notations we have the following proposition.

12.3. Proposition. (1) $U_{\infty} = \mathbf{Unk}_{\approx}^0(S)$.

(2) The system S' is \approx -reduced and $S \text{ runf}_{\mathcal{P}}^* S'$ (hence, $S' \approx^P S$).

Proof. (1) It is easy to establish by induction on i the validity of the following claim.

Claim. For all $i \geq 0$, for all u_j in U_i , for every powerset F -magma \mathbf{P} , for every solution $m = (m_1, \dots, m_n)$ of S in \mathbf{P} , $m_j = \emptyset$.

Hence, $u \in U_{\infty}$ implies $u \approx_{\mathcal{P}}^0 \Omega$.

To prove the converse, let \mathbf{M} denote the trivial F -magma reduced to a single element a and let $\mathbf{P} = \mathcal{P}(\mathbf{M})$. Then let $m = (m_1, \dots, m_n)$, where $m_j = \emptyset$ if $u_j \in U_{\infty}$ and $m_j = \{a\}$ if $u_j \notin U_{\infty}$. It is easy to check that m is a solution of S in \mathbf{P} . Hence, $u \not\approx_{\mathcal{P}}^0 \Omega$ if $u \notin U_{\infty}$.

(2) Let $d(S) = \text{Card}(\mathbf{Unk}_{\approx}^0(S) - U_1)$ so that if S is \approx -reduced, then $d(S) = 0$. If $d(S) \neq 0$, let $S_1 = \langle u_i = p_i^{(1)}; 1 \leq i \leq n \rangle$, where $p_i^{(1)} = \text{Pol}(p_i[\Omega/u; u \in U_1])$. It is clear that $S \text{ runf. rewr}_{\mathcal{P}} S_1$ and that $d(S_1) < d(S)$. Hence, this transformation can be repeated and gives after at most $d(S)$ steps a \approx -reduced system S' such that $S \text{ runf}_{\mathcal{P}}^* S'$. \square

In terms of context-free grammars, this transformation consists in eliminating certain useless productions. Note that we do not eliminate the useless unknowns

since we want to obtain a system S' which is \approx -equivalent to S , hence, which has the same set of unknowns. The \approx^P -correctness of this transformation is insured by its expression in terms of $\text{runf}_{\mathcal{D}}$.

Remark. Proposition 12.3 is valid with respect to the class of all distributive F -magmas and not only with respect to \mathcal{PV} . More precisely, $U_{\infty} = \{u \in \text{Unk}(S) \mid u \approx_{S, \mathcal{D}} \Omega\}$ and $\text{Red}_{\approx}(S) \approx_{\mathcal{D}} S$.

The following definition and lemma will only be used in the proof of Proposition 12.8 below.

12.4. Definition. Given a polynomial system S we define its h -th iterate S^h for $h \geq 1$ as follows:

$$\begin{aligned} S^h &= \langle u_i = \text{Pol}(p_i^h); 1 \leq i \leq n \rangle, \\ p_i^1 &= p_i \quad \text{for all } i \in [n] \quad (\text{hence, } S^1 = S), \\ p_i^{h+1} &= p_i[p_1^h/u_1, \dots, p_n^h/u_n]. \end{aligned}$$

It is clear that $p_i \rightarrow_{S, \mathcal{D}}^* p_i^h$ for all i , hence, that $S \text{unf}_{\mathcal{D}} S^h$ for all $h \geq 1$.

12.5. Lemma. Let S be a polynomial system. There exists an integer h such that, for all u_i in $\text{Unk}(S)$,

$$u_i \in \text{Unk}_{\approx}^0(S) \quad \text{iff} \quad p_i^h \leftrightarrow_{\mathcal{D}}^* \Omega.$$

Proof. Let h be the smallest $j \geq 1$ such that $U_j = \text{Unk}_{\approx}^0(S)$. Note that $j \leq n$. We show by induction on j that, for all $j \geq 1$,

$$u_i \in U_j \quad \text{implies} \quad p_i^{j'} \leftrightarrow_{\mathcal{D}}^* \Omega \quad \text{for all } j' \geq j.$$

By the associativity of substitution,

$$p_i^{j+1} = p_i^j[p_1^j/u_1, \dots, p_n^j/u_n],$$

hence, $p_i^j \leftrightarrow_{\mathcal{D}}^* \Omega$ implies $p_i^{j'} \leftrightarrow_{\mathcal{D}}^* \Omega$ for $j' \geq j$ and it suffices to do the proof for $j' = j$. This is clear for $j = 1$. Let us consider the case $j + 1$. Let $u_i \in U_{j+1}$ and $p_i = t_1 + \dots + t_k$ for $t_1, \dots, t_k \in M(F, \text{Unk}(S))$. Since every t_m has an occurrence of some $u_{i'}$ in U_j ,

$$\begin{aligned} t_m[p_1^j/u_1, \dots, p_n^j/u_n] &\xleftrightarrow[\mathcal{D}]{*} t_m[p_1^j/u_1, \dots, \Omega/u_{i'}, \dots] \\ &\xleftrightarrow[\mathcal{D}]{*} \Omega. \end{aligned}$$

Hence, $p_i^{j+1} \leftrightarrow_{\mathcal{D}}^* \Omega$.

Conversely, let j be any integer such that $p_i^j \leftrightarrow_{\mathcal{D}}^* \Omega$. Then $u_i \approx_S^{p_j} \Omega$. Since every solution of S is a solution of S^j , $u_i \approx_S^p \Omega$, hence, $u_i \in \text{Unk}_{\approx}^0(S)$. \square

Note that S^h is not \approx -reduced in general and is not \approx^P -equivalent to S .

12.6. Definition. A polynomial system S (as in Section 11.1) is *deterministic* if it is uniform and $\mathbf{Dev}(p_i) \cap \mathbf{Dev}(p_j) = \emptyset$ for all $i, j \in [n]$ such that $i \neq j$.

It is *complete deterministic* if, furthermore, $F(U) = \bigcup \{\mathbf{Dev}(p_i) \mid 1 \leq i \leq n\}$ (where $U = \mathbf{Unk}(S)$).

This terminology can be understood with the help of the example in Section 11.4.1: the polynomial system S_A associated with a finite automaton A is deterministic iff A is deterministic (i.e., A has only one initial state, has no ε -transition, and its transition relation $\tau \subseteq Q \times T \times Q$ is functional w.r.t. its first two arguments); it is complete deterministic iff A is (i.e., if A is deterministic and, for all q in Q , a in T , then there exists q' in Q such that $(q, a, q') \in \tau$). The complete deterministic systems are called ‘deterministic’ in [73] and the deterministic ones have no special name in this paper.

We can now start the proof of Theorem 12.1. The following proposition is a just special case of it.

12.7. Proposition. *Let S be a complete deterministic polynomial system. Let $A, A' \subseteq \mathbf{Unk}^+(S)$ and $t = \sum A$, $t' = \sum A'$. Then $t \approx_S^P t'$ if and only if $A = A'$, i.e., iff $t = t'$.*

For later use, note that the stated conditions on t, t' could be formulated as $t, t' \in M^+(\emptyset, \mathbf{Unk}^+(S))$.

Proof of Proposition 12.7. We define an F -magma \mathbf{M} with domain $M = U = \mathbf{Unk}(S)$ and operations defined as follows:

$$f_{\mathbf{M}}(u_{i_1}, \dots, u_{i_k}) = u_i \text{ iff } f(u_{i_1}, \dots, u_{i_k}) \in \mathbf{Dev}(p_i).$$

Since S is complete deterministic, this properly defines $f_{\mathbf{M}}$ for all f in F .

It is easy to verify that the n -tuple $m = (m_1, \dots, m_n)$, where $m_i = \emptyset$ if $u_i \in \mathbf{Unk}^0(S)$ and $m_i = \{u_i\}$ if $u_i \in \mathbf{Unk}^+(S)$, is a solution of S in $\mathcal{P}(\mathbf{M})$ and that, for t, t' as in the statement, $t_{\mathcal{P}(\mathbf{M})}(m) = A = \mathbf{Dev}(t)$ and similarly for t' . Hence, $t \approx_S^P t'$ implies $t_{\mathcal{P}(\mathbf{M})}(m) = t'_{\mathcal{P}(\mathbf{M})}(m)$, hence, $A = A'$ and $t = t'$.

The converse is obvious. \square

We now use this result to establish another special case of Theorem 12.1, which includes this one.

12.8. Proposition. *Let S be uniform and $t, t' \in M^+(\emptyset, \mathbf{Unk}(S))$. Then $t \approx_S^P t'$ if and only if $t \leftrightarrow_{S, \emptyset}^* t'$.*

The proof of this proposition rests upon a construction of Mezei and Wright [73] which associates with a uniform system a complete deterministic one and which generalizes the classical determinization algorithm for finite-state automata.

Construction: Let S be a uniform polynomial system, as in Section 11.1 and let $U = \{u_1, \dots, u_n\} = \text{Unk}(S)$. We introduce a new set of unknowns \bar{U} in bijection with $\mathcal{P}(U)$. We denote by $\bar{\alpha}$ the element of \bar{U} associated with $\alpha \subseteq U$. We do not identify $\{u_i\}$ with u_i . Further, we assume that $\bar{U} \subseteq \mathcal{U}$ for every finite subset U of \mathcal{U} .

For every $k \geq 0$, every f in F_k , every u_{i_1}, \dots, u_{i_k} in U , we let $\bar{f}(u_{i_1}, \dots, u_{i_k})$ denote $\{u_i \in U \mid f(u_{i_1}, \dots, u_{i_k}) \in \text{Dev}(p_i)\}$. This mapping extends in a standard way to $\mathcal{P}(U)^k$ by

$$\bar{f}(\alpha_1, \dots, \alpha_k) = \bigcup \{\bar{f}(u_{i_1}, \dots, u_{i_k}) \mid u_{i_1} \in \alpha_1, \dots, u_{i_k} \in \alpha_k\}.$$

We let $\bar{S} = \langle \bar{\alpha} = p_{\bar{\alpha}}; \bar{\alpha} \in \bar{U} \rangle$, where

$$p_{\bar{\alpha}} = \sum \{f(\bar{\alpha}_1, \dots, \bar{\alpha}_k) \mid \bar{\alpha}_1, \dots, \bar{\alpha}_k \in \bar{U}, \bar{f}(\alpha_1, \dots, \alpha_k) = \alpha\}.$$

Equivalently, $f(\bar{\alpha}_1, \dots, \bar{\alpha}_k) \in \text{Dev}(p_{\bar{\alpha}})$ iff $\alpha = \{u_i \in U \mid f(u_{i_1}, \dots, u_{i_k}) \in \text{Dev}(p_i) \text{ for some } u_{i_1} \in \alpha_1, \dots, u_{i_k} \in \alpha_k\}$. It is clear that \bar{S} is complete deterministic (but not necessarily \approx -reduced). Let also S'' denote the set of equations $\langle u_i = q_i; 1 \leq i \leq n \rangle$, where $q_i = \sum \{\bar{\alpha} \mid \bar{\alpha} \in \bar{U}, u_i \in \alpha\}$, and $S' = \bar{S} \cup S''$. It is clear that \bar{S} is a (large) subsystem of S' .

12.9. Lemma. $S' \text{ redef}_{\mathcal{D}}(S \cup \bar{S})$. Hence, for every \mathbf{P} in $\mathcal{V}(\mathcal{D})$, $\pi_U(\text{Sol}_{\mathbf{P}}(S')) \subseteq \text{Sol}_{\mathbf{P}}(S)$.

Proof. We verify conditions (1)–(3) of Definition 5.10. Condition (1) holds since it reads $p_i \in M(F_+, U)$, for all i in $[n]$.

Condition (2) holds since

$$q_i[\Omega/\bar{\alpha}; \bar{\alpha} \in \bar{U}] \xleftrightarrow[\mathcal{D}]{*} \Omega.$$

Condition (3) reads:

$$q_i[p_{\bar{\alpha}}/\bar{\alpha}; \bar{\alpha} \in \bar{U}] \xleftrightarrow[\mathcal{D}]{*} p_i[q_1/u_1, \dots, q_n/u_n]$$

(since $\equiv_{\mathcal{D}}$ coincides with $\leftrightarrow_{\mathcal{D}}^*$) and we shall verify its validity:

$$\begin{aligned} & \text{Dev}(q_i[p_{\bar{\alpha}}/\bar{\alpha}; \bar{\alpha} \in \bar{U}]) \\ &= \bigcup \{\text{Dev}(p_{\bar{\alpha}}) \mid u_i \in \alpha \subseteq U\} \\ &= \{f(\bar{\alpha}_1, \dots, \bar{\alpha}_k) \mid \alpha_1, \dots, \alpha_k \subseteq U, u_i \in \bar{f}(\alpha_1, \dots, \alpha_k)\}. \end{aligned}$$

On the other hand,

$$\begin{aligned}
& \mathbf{Dev}(p_i[q_1/u_1, \dots, q_n/u_n]) \\
&= \bigcup \{ \mathbf{Dev}(f(q_{i_1}, \dots, q_{i_k})) \mid k \geq 0, f \in F_k, \\
&\quad i_1, \dots, i_k \in [n], f(u_{i_1}, \dots, u_{i_k}) \in \mathbf{Dev}(p_i) \} \\
&= \{ f(\bar{\alpha}_1, \dots, \bar{\alpha}_k) \mid k \geq 0, f \in F_k, \text{ there exist } i_1, \dots, i_k \text{ such that} \\
&\quad f(u_{i_1}, \dots, u_{i_k}) \in \mathbf{Dev}(p_i) \text{ and } u_{i_1} \in \alpha_1, \dots, u_{i_k} \in \alpha_k \} \\
&= \mathbf{Dev}(q_i[p_{\bar{\alpha}}/\bar{\alpha}; \bar{\alpha} \in \bar{U}]),
\end{aligned}$$

by the definition of \bar{f} . Hence, condition (3) holds and $S' \text{ redef}_{\mathcal{D}}(S \cup \bar{S})$.

The second assertion follows from Remark 5.13 and Proposition 4.6(1). \square

In [73], the construction of \bar{S} is immediately followed by the deletion of all unknowns $\bar{\alpha}$ such that $\bar{\alpha} \sim_{\bar{S}}^p \Omega$: we shall do this in Definition 14.3.

In the following lemma we denote by $M_h(F, X)$ the subset of $M(F, X)$ defined by

$$M_0(F, X) = X, \quad M_{h+1}(F, X) = F(M_h(F, X)).$$

Note that $M_1(F, X) = F(X)$ and $F_0 \subseteq M_h(F, X)$ for all $h \geq 1$.

12.10. Lemma. *Let S be a uniform polynomial system, let $U = \mathbf{Unk}(S)$, let $S^h = \langle u_i = q_i^h; i \in [n] \rangle$ be its h -th iterate. If S is complete deterministic, then $\{ \mathbf{Dev}(q_i^h) \mid i \in [n], \mathbf{Dev}(q_i^h) \neq \emptyset \}$ is a partition of $M_h(F, U)$.*

The lemma is proved by induction on h . We omit the details.

12.11. Lemma. *Let S be uniform, let $U = \mathbf{Unk}(S)$, let $\bar{S} = \langle \bar{\alpha} = p_{\bar{\alpha}}; \bar{\alpha} \in \bar{U} \rangle$ be the complete deterministic system associated with S as above. Let $S^h = \langle u_i = \mathbf{Pol}(p_i^h); i \in [n] \rangle$ and $\bar{S}^h = \langle \bar{\alpha} = \mathbf{Pol}(p_{\bar{\alpha}}^h); \bar{\alpha} \in \bar{U} \rangle$ be the h -th iterates of S and \bar{S} respectively.*

For all t in $M_h(F, X_k)$ which is X_k -linear, for all $\bar{\alpha}, \bar{\alpha}_1, \dots, \bar{\alpha}_k$ in \bar{U} the following conditions are equivalent:

- (1) $t[\bar{\alpha}_1/x_1, \dots, \bar{\alpha}_k/x_k] \in \mathbf{Dev}(p_{\bar{\alpha}}^h)$,
- (2) $\alpha = \{ u_i \in U \mid t[u_i/x_1, \dots, u_i/x_k] \in \mathbf{Dev}(p_i^h) \}$

for some u_{i_1} in α_1, \dots, u_{i_k} in α_k .

This lemma states that \bar{S}^h is ‘something like’ the complete deterministic system associated with S^h . However, we cannot write $\bar{S}^h = \overline{(S^h)}$ since, for $h \geq 2$, S^h is not uniform, hence, the above construction does not apply. We only want to point out the similarity between Lemma 12.11 and the definition of $p_{\bar{\alpha}}$.

Proof of Lemma 12.11. The proof is by induction on h . The result is trivial if $h = 1$.

Let us establish the result for $h > 1$ by assuming that it holds for $h - 1$. Let $t \in M_h(F, X_k)$ be X_k -linear.

(1) \Rightarrow (2): If $t[\bar{\alpha}_1, \dots, \bar{\alpha}_k] \in \mathbf{Dev}(p_{\bar{\alpha}}^h)$, then $t = f(t_1, \dots, t_l)$ and there exist β_1, \dots, β_l in $\mathcal{P}(U)$ such that $f(\bar{\beta}_1, \dots, \bar{\beta}_l) \in \mathbf{Dev}(p_{\bar{\alpha}})$ and $t_j[\bar{\alpha}_1, \dots, \bar{\alpha}_k] \in \mathbf{Dev}(p_{\bar{\beta}_j}^{h-1})$ for all $j = 1, \dots, l$. By the induction hypothesis,

$$\beta_j = \{u_i \in U \mid t_j[u_{i_1}, \dots, u_{i_k}] \in \mathbf{Dev}(p_{\bar{\beta}_j}^{h-1}) \text{ for some } u_{i_1} \text{ in } \alpha_1, \dots, u_{i_k} \text{ in } \alpha_k\}. \quad (4)$$

If $u_m \in \alpha$, then $f(u_{j_1}, \dots, u_{j_l}) \in \mathbf{Dev}(p_m)$ for some u_{j_1} in β_1, \dots, u_{j_l} in β_l . Hence, $f(t_1, \dots, t_l)[u_{i_1}, \dots, u_{i_k}] \in \mathbf{Dev}(p_m^h)$ for some u_{i_1} in α_1, \dots, u_{i_k} in α_k , by (4) and the linearity of t . Hence, we have proved the \subseteq -part of (2).

To prove the other inclusion of (2), let u_i belong to the right-hand side of (2) and u_{i_1}, \dots, u_{i_k} be the associated elements of $\alpha_1, \dots, \alpha_k$. Then $f(u_{j_1}, \dots, u_{j_l}) \in \mathbf{Dev}(p_i)$ for some u_{j_1}, \dots, u_{j_l} such that $t_m[u_{i_1}, \dots, u_{i_k}] \in \mathbf{Dev}(p_{j_m}^{h-1})$ for all $m = 1, \dots, l$. Hence, $u_{j_1} \in \beta_1, \dots, u_{j_l} \in \beta_l$. Hence, $u_i \in \alpha$ since $f(\bar{\beta}_1, \dots, \bar{\beta}_l) \in \mathbf{Dev}(p_{\bar{\alpha}})$ (and by the definition of \bar{S}). Hence, we have shown the \supseteq -part of (2).

(2) \Rightarrow (1): Let us assume (2) and prove that $t[\bar{\alpha}_1/x_1, \dots, \bar{\alpha}_k/x_k] \in \mathbf{Dev}(p_{\bar{\alpha}}^h)$.

By Lemma 12.10, $t[\bar{\alpha}_1, \dots, \bar{\alpha}_k]$ belongs to $\mathbf{Dev}(p_{\bar{\beta}}^h)$ for some $\bar{\beta}$ in \bar{U} . With the help of the first part of the proof one obtains $\alpha = \beta$. \square

Proof of Proposition 12.8. Let us assume that $t = u_{i_1} + \dots + u_{i_k}$ and that $t' = u_{j_1} + \dots + u_{j_l}$. Let us also assume that we have proved that

$$u_{i_m} + t' \xleftrightarrow[S, \mathcal{D}]^* t' \quad \text{for all } m = 1, \dots, k,$$

$$u_{j_m} + t \xleftrightarrow[S, \mathcal{D}]^* t \quad \text{for all } m = 1, \dots, l.$$

It is easy to prove (by using \mathcal{D}) that $t + t' \leftrightarrow_{S, \mathcal{D}}^* t'$ and $t' + t \leftrightarrow_{S, \mathcal{D}}^* t$, whence $t \leftrightarrow_{S, \mathcal{D}}^* t'$. Hence, it suffices to establish Proposition 12.8 for $t = u_{i_1} + t'$ and $t' = u_{j_1} + \dots + u_{j_l}$. If $i_1 \in \{j_1, \dots, j_l\}$, then $t \leftrightarrow_{\mathcal{D}}^* t'$.

We shall assume, without loss of generality, that $t = u_1 + u_2 + \dots + u_k$, $t' = u_2 + \dots + u_k$. We also assume that $t \approx_S^p t'$. For $i \in [n]$, let $\bar{U}_i = \{\bar{\alpha} \in \bar{U} \mid u_i \in \alpha \text{ and } \bar{\alpha} \in \mathbf{Unk}_{\approx}^+(\bar{S})\}$. Let $m = (m_{\bar{\alpha}})_{\bar{\alpha} \in \bar{U}}$ be an arbitrary solution of \bar{S} in $\mathcal{P}(\mathbf{M})$ for some \mathbf{M} in \mathcal{V} .

It uniquely extends to a solution m' of S' since \bar{S} is a large subsystem of S' . Its projection $m'' = \pi_U(m')$ defines (by Lemma 12.9) a solution of S , namely $m'' = (m''_1, \dots, m''_n)$ with $m''_i = \sum \{m_{\bar{\alpha}} \mid \bar{\alpha} \in \bar{U}_i\}$. Hence, $t_{\mathcal{P}(\mathbf{M})}(m') = \sum \{m_{\bar{\alpha}} \mid 1 \leq i \leq k, \bar{\alpha} \in \bar{U}_i\}$. Similarly, $t'_{\mathcal{P}(\mathbf{M})}(m') = \sum \{m_{\bar{\alpha}} \mid 2 \leq i \leq k, \bar{\alpha} \in \bar{U}_i\} = t_{\mathcal{P}(\mathbf{M})}(m')$. Hence,

$$\sum \{\bar{\alpha} \mid 1 \leq i \leq k, \bar{\alpha} \in \bar{U}_i\} \approx_S^p \sum \{\bar{\alpha} \mid 2 \leq i \leq k, \bar{\alpha} \in \bar{U}_i\}$$

since $(m_{\bar{\alpha}})_{\bar{\alpha} \in \bar{U}}$ is an arbitrary solution of \bar{S} .

Hence, by Proposition 12.7,

$$\bar{U}_1 \subseteq \bar{U}_2 \cup \bar{U}_3 \cup \dots \cup \bar{U}_k.$$

This means that $\bar{\alpha} \approx_S^p \Omega$ for all $\alpha \in A$, where $A = \{\alpha \subseteq U \mid u_1 \in \alpha \text{ and } u_i \notin \alpha \text{ for all } i = 2, \dots, k\}$.

Let h be the integer associated with \bar{S} by Lemma 12.5. It follows that $p_{\bar{\alpha}}^h \leftrightarrow_{S, \mathcal{D}}^* \Omega$ for all α in A . From this, we now prove that

$$\mathbf{Dev}(p_1^h) \subseteq \mathbf{Dev}(p_2^h) \cup \dots \cup \mathbf{Dev}(p_k^h). \quad (5)$$

Let $t \in M_h(F, X_I)$ be X_I -linear and let $t[u_{i_1}, \dots, u_{i_r}]$ belong to $\mathbf{Dev}(p_1^h)$. Assume that it does not belong to the right-hand side of (5) and consider $t[\{\bar{u}_{i_1}\}, \dots, \{\bar{u}_{i_r}\}]$ which belongs to $\mathbf{Dev}(p_{\bar{\beta}}^h)$ for some $\beta \subseteq U$ by Lemma 12.10. Lemma 12.11 shows that $u_1 \in \beta$ and that $u_2, \dots, u_k \notin \beta$. Hence, $\beta \in A$ and $\mathbf{Dev}(p_{\bar{\beta}}^h) \neq \emptyset$, which is a contradiction.

Note that $u_i \rightarrow_S^* p_i^h$ for all $i = 1, \dots, k$. Hence, it follows from (5) that

$$u_1 + \dots + u_k \xrightarrow[S, \mathcal{D}]^* p_1^h + \dots + p_k^h \xleftarrow[\mathcal{D}]^* p_2^h + \dots + p_k^h \xleftarrow[S, \mathcal{D}]^* u_2 + \dots + u_k,$$

hence, $t \longleftrightarrow_{S, \mathcal{D}}^* t'$ as was to be shown.

Note that instead of the integer h of Lemma 12.5 it suffices to take

$$h = \mathbf{Min}\{i \mid p_{\bar{\alpha}}^i = \Omega \text{ for all } \alpha \text{ in } A\},$$

which is smaller in general. \square

We illustrate this complicated proof by an example.

12.12. Example. Let S be the following system:

$$u = a + b + gu + gv + gw, \quad v = a + gx,$$

$$w = b + gv + gw + gx, \quad x = gu + gv.$$

We shall prove that $u + v + w \approx_S^p v + w$ and that $u + v + w \leftrightarrow_{S, \mathcal{D}}^* v + w$. To do so, we construct \bar{S} :

$$\bar{u}\bar{v} = a, \quad \bar{u}\bar{w} = b + g\bar{w}, \quad \bar{u}\bar{x} = g\bar{u},$$

$$\bar{v}\bar{w} = g\bar{x}, \quad \bar{u}\bar{v}\bar{w} = g\bar{w}\bar{x},$$

$$\bar{u}\bar{w}\bar{x} = g\bar{v} + g\bar{u}\bar{v} + g\bar{u}\bar{w} + g\bar{v}\bar{w} + g\bar{u}\bar{v}\bar{w},$$

$$\bar{u}\bar{v}\bar{w}\bar{x} = g\bar{u}\bar{x} + g\bar{v}\bar{x} + g\bar{u}\bar{v}\bar{x} + g\bar{u}\bar{w}\bar{x} + g\bar{v}\bar{w}\bar{x} + g\bar{u}\bar{v}\bar{w}\bar{x},$$

$$\bar{\emptyset} = g\bar{\emptyset}.$$

To simplify the notations we have used $\bar{u}\bar{v}$ for $\{\bar{u}, \bar{v}\}$, etc. and omitted the equations with right-hand side Ω .

Since $\bar{u} \approx_S^p \Omega$, $\bar{u}\bar{x} \approx_S^p \Omega$, it follows that $\bar{\alpha} \approx_S^p \Omega$ for all $\alpha \subseteq \{u, v, w, x\}$ such that $u \in \alpha$ and $v, w \notin \alpha$. Hence, $u + v + w \approx_S^p v + w$. Note that $p_{\bar{u}} = \Omega$, $\mathbf{Pol}(p_{\bar{u}\bar{x}}) \neq \Omega$, but $\mathbf{Pol}(p_{\bar{u}\bar{x}}^2) = \Omega$. It follows that $h = 2$ suffices in the proof of Proposition 12.8 (see the final remark).

Let us verify (5):

$$\mathbf{Dev}(p_u^2) = \{a, b, ga, gb, ggu, ggv, ggw, ggx\},$$

$$\mathbf{Dev}(p_v^2) = \{a, ggu, ggv\},$$

$$\mathbf{Dev}(p_w^2) = \{b, ga, ggx, gb, ggv, ggw, ggx, ggu\}.$$

Hence, $\mathbf{Dev}(p_u^2) \subseteq \mathbf{Dev}(p_v^2) \cup \mathbf{Dev}(p_w^2)$, whereas $\mathbf{Dev}(p_u)$ is not included in $\mathbf{Dev}(p_v) \cup \mathbf{Dev}(p_w)$. Hence, $u + v + w \leftrightarrow_{\mathcal{S}, \emptyset}^* p_u^2 + p_v^2 + p_w^2 \leftrightarrow_{\emptyset}^* p_v^2 + p_w^2 \leftrightarrow_{\mathcal{S}, \emptyset}^* v + w$, and $u + v + w \leftrightarrow_{\mathcal{S}, \emptyset}^* v + w$.

We now extend Proposition 12.8 to the class of quasi-uniform polynomial systems. The proof will be based on a construction of independent interest (see Lemma 14.13) that we shall present separately.

12.13. Definition. Let S be a polynomial system (as in Section 11.1). Let us associate with S a binary relation \rightarrow on $\mathbf{Unk}(S)$ defined as follows:

$$u_i \rightarrow u_j \text{ iff } u_j \in \mathbf{Dev}(p_i).$$

We say that u is *cyclic* if $u \rightarrow^+ u$ and we denote by $\mathbf{Cycl}(S)$ the set of cyclic unknowns. We say that S is *cycle-free* if $\mathbf{Cycl}(S) = \emptyset$. We associate with S a system S' as follows. We let $q_i = \sum (\mathbf{Dev}(p_i) \cap U)$, $r_i = \sum (\mathbf{Dev}(p_i) \cap F(M(F, U)))$ and $S' = \langle u_i = \mathbf{Pol}(q'_i + r'_i); 1 \leq i \leq n \rangle$, where

$$(1) \quad q'_i = \sum \{u_j \in \mathbf{Cycl}(S) \mid u_i \rightarrow^* u_j\},$$

$$(2) \quad r'_i = \sum \{r_j \mid j \in [n], u_i \rightarrow^* u_j\}.$$

12.14. Lemma. $S \mathbf{runf}_{\emptyset}^* S'$. Hence, $S' \approx^P S$.

Proof. For every j in $[n]$ we shall define a transformation γ_j on polynomial systems with set of unknowns $U = \{u_1, \dots, u_n\}$ such that

$$(1) \quad \gamma_j \subseteq \mathbf{runf}_{\emptyset},$$

$$(2) \quad S\gamma_1\gamma_2 \cdots \gamma_n S'.$$

Letting S be as in Definition 12.13, and $\bar{S} = \langle u_i = \bar{p}_i; 1 \leq i \leq n \rangle$, we write $S\gamma_j\bar{S}$ iff the following conditions hold

$$(3) \quad \bar{p}_j = p_j,$$

$$(4) \quad \bar{p}_i = \mathbf{Pol}(q_i[p'_j/u_j] + r_i) \quad \text{if } i \neq j,$$

where $p'_j = p_j$ if $u_j \notin \mathbf{Cycl}(S)$ and $p'_j = p_j + u_j$ if $u_j \in \mathbf{Cycl}(S)$.

It is not difficult to verify that $\gamma_j \subseteq \mathbf{runf}_{\emptyset}^{(j)}$ (with the notation of the proof of Proposition 4.13) which proves (1).

Assertion (2) could be proved by an adaptation of the correctness proof of the classical $O(n^3)$ -algorithm for transitive closure. We omit the technical details, but below we shall give a representative example.

The statements of Lemma 12.14 immediately follow from (1) and (2). \square

12.15. Example. In Table 2, we display S_i such that $S\gamma_1\gamma_2\cdots\gamma_i S_i$ for $i = 1, \dots, 5$. We need not specify r_1, \dots, r_5 which are arbitrary elements of $M^+(F(M(F, U)))$. The cyclic unknowns are u_1, u_2, u_3, u_5 . As in Example 4.14, if an equation of S_{i+1} is not written, this means that it is exactly as in S_i .

12.16. Proposition. *If S is quasi-uniform, if $t, t' \in M^+(\emptyset, U)$ and $t \approx_S^P t'$, then $t \leftrightarrow_{S, \emptyset}^* t'$.*

Proof. Let S' be associated with S by Definition 12.13. Without loss of generality, we can assume that $\text{Cycl}(S) = \{u_1, \dots, u_k\}$ for some $k \leq n$. Let $C = \{c_1, \dots, c_k\}$ be a set of new constants, let $F' = F \cup C$.

If $S' = \langle u_i = \text{Pol}(q'_i + r'_i); 1 \leq i \leq n \rangle$ as in Definition 12.13, we let $S'' = \langle u_i = \text{Pol}(q''_i + r'_i); 1 \leq i \leq n \rangle$, with $q''_i = q'_i[c_1/u_1, \dots, c_k/u_k]$ for all i in $[n]$. Note that S and S'' are two polynomial systems over F' with the same set of unknowns.

Claim. $S'' \cong^P S$.

This means that every solution of S'' in $\mathcal{P}(\mathbf{M})$, where \mathbf{M} is an F' -magma, is a solution of S , equivalently of S' by Lemma 12.14.

Proof of Claim. Let $m = (m_1, \dots, m_n)$ be a solution of S'' in $\mathcal{P}(\mathbf{M})$, i.e.,

$$m_i = q''_i(m) \cup r'_i(m) \quad \text{for all } i$$

(instead of $q''_{i\mathbf{M}}(m)$ we write $q''_i(m)$ for simplicity). We have to prove that $m_i = q'_i(m) \cup r'_i(m)$.

For the inclusion \supseteq it suffices to prove that $q''_i(m) \subseteq q'_i(m)$. If $d \in q''_i(m)$, then $d = c_{j\mathbf{M}}$ for some j in $[k]$ such that $u_i \rightarrow^* u_j$. However, $c_j \in \text{Dev}(q''_j)$, hence, $d \in m_j$. And $m_j \subseteq q'_j(m)$ since $u_j \in \text{Dev}(q'_j)$. Hence, $d \in q'_j(m)$.

Table 2.

S	S_1	S_2
$u_1 = u_2 + r_1$ $u_2 = u_3 + u_4 + r_2$ $u_3 = u_1 + r_3$ $u_4 = u_5 + r_4$ $u_5 = u_5 + r_5$	$u_3 = u_1 + u_2 + r_1 + r_3$	$u_1 = u_2 + u_3 + u_4 + r_1 + r_2$ $u_3 = u_1 + u_2 + u_3 + u_4 + r_1 + r_2 + r_3$
S_3	S_4	$S_5 = S'$
$u_1 = u_1 + u_2 + u_3 + u_4$ $+ r_1 + r_2 + r_3$ $u_2 = \text{idem}$ $u_3 = \text{idem}$	$u_1 = u_1 + u_2 + u_3 + u_5$ $+ r_1 + r_2 + r_3 + r_4$ $u_2 = \text{idem}$ $u_3 = \text{idem}$	$u_1 = u_1 + u_2 + u_3 + u_5$ $+ r_1 + r_2 + r_3 + r_4 + r_5$ $u_2 = \text{idem}$ $u_3 = \text{idem}$ $u_4 = u_5 + r_4 + r_5$ $u_5 = u_5 + r_5$

For the reverse inclusion \supseteq , it suffices to prove that $q'_i(m) \subseteq q''_i(m) \cup r'_i(m)$. Let $d \in q'_i(m)$. Hence, $d \in m_j$ for some j in $[k]$ such that $u_i \rightarrow^* u_j$. Hence, $d \in q''_j(m) \cup r'_j(m)$.

Since $u_i \rightarrow^* u_j$ and by the definition of S' , $\mathbf{Dev}(r'_j) \subseteq \mathbf{Dev}(r'_i)$ and $\mathbf{Dev}(q''_j) \subseteq \mathbf{Dev}(q''_i)$. This concludes the proof of the claim. \square

Proof of Proposition 12.16 (continued). Let now $t, t' \in M^+(\emptyset, U)$ be such that $t \approx_S^p t'$. It follows from the claim that $t \approx_{S''}^p t'$. However, S'' is uniform since the cyclic unknowns of S' have been replaced by constants. Hence, $t \leftrightarrow_{S'', \emptyset}^* t'$ by Proposition 12.8; let $\gamma: t \leftrightarrow_{S'', \emptyset} t_1 \leftrightarrow_{S'', \emptyset} t_2 \leftrightarrow_{S'', \emptyset} \dots \leftrightarrow t'$ be a sequence of rewritings. Let $\theta: M(F_+ \cup C, U) \rightarrow M(F_+, U)$ be the substitution such that $\theta(w) = w[u_1/c_1, \dots, u_k/c_k]$.

It is easy to prove that $w \leftrightarrow_{S''} w'$ implies $\theta(w) \leftrightarrow_{S''} \theta(w')$ and that $w \rightarrow_{S''} w'$ implies $\theta(w) \rightarrow_{S''} \theta(w')$. Hence, this gives

$$t \xleftrightarrow{S'', \emptyset} \theta(t_1) \xleftrightarrow{S'', \emptyset} \theta(t_2) \xleftrightarrow{S'', \emptyset} \dots \xleftrightarrow{S'', \emptyset} t'.$$

By Lemma 12.14 and Proposition 4.3, $S \mathbf{unf}_{\emptyset} S'$, hence, $u_i \rightarrow_{S, \emptyset}^* q'_i + r'_i$ for all i . Hence, $w \leftrightarrow_{S'} w'$ implies $w \leftrightarrow_{S, \emptyset}^* w'$. And this shows that $t \leftrightarrow_{S, \emptyset}^* t'$. \square

The last step of the proof of Theorem 12.1 will use a construction which transforms an arbitrary polynomial system into a quasi-uniform (polynomial) one. This construction is an obvious extension of the one of Proposition 7.12 and as we did there, we denote by $\mathbf{Ufm}(S)$ the result of the construction applied to S . Since we want $\mathbf{Ufm}(S)$ to be polynomial and not simply $+$ -regular, some reorderings of the monomials may be necessary. Hence, we obtain the following proposition.

12.17. Proposition. *For every polynomial system S , one can construct a quasi-uniform polynomial system $\mathbf{Ufm}(S)$ such that $S \subseteq_{\ell} S' \mathbf{rfl}_{\emptyset} \mathbf{Ufm}(S)$ (for some polynomial system S'). Hence, $S \approx_{\mathbf{Unk}(S), \emptyset} \mathbf{Ufm}(S)$. If S is a Greibach system, then $\mathbf{Ufm}(S)$ is uniform.*

To give an example, the system

$$S = \langle u_1 = u_2 + f(u_1, g(u_2, f(u_1, u_2))), u_2 = a + h(u_2, f(u_1, u_2)) \rangle$$

is transformed into

$$\begin{aligned} \mathbf{Ufm}(S) = \langle u_1 = u_2 + f(u_1, u_3), u_2 = a + h(u_2, u_4), u_3 = g(u_2, u_4), \\ u_4 = f(u_1, u_2) \rangle. \end{aligned}$$

Letting $S' = \mathbf{Ufm}(S)$, we have the following lemma.

12.18. Lemma. *If, $w, w' \in M(F_+, \mathbf{Unk}(S))$, $w \leftrightarrow_{S', \emptyset}^* w'$ implies $w \leftrightarrow_{S, \emptyset}^* w'$.*

Proof. Let $U = \mathbf{Unk}(S)$ and $U' = \mathbf{Unk}(S') = \{u_1, \dots, u_m\}$, $m \geq n$. For u in $U' - U$, let \bar{u} be the unique element of $M(F, U)$ such that $u \rightarrow_{S', (U' - U)}^* \bar{u}$.

Let $\theta: M(F_+, U') \rightarrow M(F_+, U)$ be the substitution such that $\theta(s) = s[\bar{u}/u; u \in U' - U]$. As in the proof of Proposition 12.16, we show that θ transforms a sequence of rewritings $s \leftrightarrow_{S', \mathcal{D}}^* s'$ into one of the form $\theta(s) \leftrightarrow_{S, \mathcal{D}}^* \theta(s')$ (note that $\theta(w) = w$ and $\theta(w') = w'$).

If $s \leftrightarrow_{\mathcal{D}} s'$, then $\theta(s) \leftrightarrow_{\mathcal{D}} \theta(s')$; this is clear since $\leftrightarrow_{\mathcal{D}}$ is closed under substitutions.

If $s \rightarrow_{S'} s'$, then $\theta(s) \rightarrow_{S, \mathcal{D}}^* \theta(s')$; this is not so clear since S and S' are ground rewriting relations and since θ modifies the elements of U' . In fact, it suffices to do the proof in the following two cases by letting $S' = \langle u_i = p'_i; i \in [m] \rangle$.

Case 1: $s = u_i, s' = p'_i, 1 \leq i \leq n$. In this case, $\theta(s) = u_i$ and $\theta(s') \leftrightarrow_{\mathcal{D}}^* p_i$ so that $u_i = \theta(s) \rightarrow_{S, \mathcal{D}}^* \theta(s')$.

Case 2: $s = u_i, s' = p'_i, i \in \{n+1, \dots, m\}$. In this case, $\theta(s) = \theta(s')$ so that the result trivially holds. \square

We can finally prove the main result of this section.

Proof of Theorem 12.1. Let S be a polynomial system (as usual) and $U = \text{Unk}(S)$. Let $t, t' \in M(F_+, U)$ be such that $t \approx_S^P t'$. Let S' be the system $S \cup \langle u_{n+1} = \text{Pol}(t), u_{n+2} = \text{Pol}(t') \rangle$, where u_{n+1} and u_{n+2} are two new unknowns. It is clear that $u_{n+1} \approx_{S'}^P u_{n+2}$. If $u_{n+1} \leftrightarrow_{S', \mathcal{D}}^* u_{n+2}$, then $\text{Pol}(t) \leftrightarrow_{S, \mathcal{D}}^* \text{Pol}(t')$ (it suffices to substitute $\text{Pol}(t)$ for u_{n+1} and $\text{Pol}(t')$ for u_{n+2} everywhere in the sequence of rewritings transforming u_{n+1} into u_{n+2}), hence $t \leftrightarrow_{S, \mathcal{D}}^* t'$.

Hence, it suffices to do the proof of Theorem 12.1 for t, t' in U . Without loss of generality we can assume that $t = u_1$ and $t' = u_2$.

If S is quasi-uniform, the result follows from Proposition 12.16. Otherwise, let S' be the quasi-uniform system associated with S by Proposition 12.17. Since $S' \approx_U^P S$, one has $t \approx_{S'}^P t'$. Hence, $t \leftrightarrow_{S', \mathcal{D}}^* t'$ by Proposition 12.16 and $t \leftrightarrow_{S, \mathcal{D}}^* t'$ by Lemma 12.18. \square

Fact (11.3.4) yields the following characterizations of the relations $S \cong_S^P S'$ and $S \approx_S^P S'$.

12.19. Corollary. *For every two polynomial systems S and S' with the same set of unknowns U , for every t, t' in $M(F_+, U)$,*

- (1) $t \approx_S^P t'$ iff $t \approx_{S, \mathcal{D}} t'$,
- (2) $S \cong_S^P S'$ iff $S \cong_{\mathcal{D}} S'$,
- (3) $S \approx_S^P S'$ iff $S \approx_{\mathcal{D}} S'$.

12.20. Corollary. *The condition $t \leftrightarrow_{S, \mathcal{D}}^* t'$ is decidable. Hence, $t \approx_S^P t', S \cong_S^P S'$, and $S \approx_S^P S'$ are decidable.*

Proof. Let us examine all steps of the proof of Theorem 12.1, and, in particular, the characterizations of $t \approx_S^P t'$. That of Proposition 12.7, namely $\mathbf{Dev}(t) = \mathbf{Dev}(t')$, is decidable. The condition (4) of the proof of Lemma 12.11 is also decidable and the integer h can be computed.

These two conditions are used to characterize $t \approx_S^P t'$ in the proofs of Proposition 12.16 and Theorem 12.1 by means of effective transformations of systems. Hence, the property $t \approx_S^P t'$ is decidable. \square

The results of Corollaries 12.19 and 12.20 also hold for +-regular systems. They show that the class of distributive F -magmas and its subclass consisting only of powerset F -magmas yield the same relations on polynomial systems, as well as on polynomials.

Another consequence is that the transformation rule $\mathbf{eq}_{\mathcal{D}}$ (introduced in Definition 3.5) is correct and complete w.r.t. the \approx^P -equivalence of polynomial systems.

But this result raises a few (probably difficult) questions (for which we do not make any conjecture).

12.21. Question. The transformation $\mathbf{rufld}_{\mathcal{D}}$ is \approx^P -correct; is it \approx^P -complete, or equivalently, is it $\approx_{\mathcal{D}}$ -complete?

Next comes the investigation of $\approx_{\mathcal{E}}^P$, in the case where \mathcal{E} is linear and balanced. The proof of Theorem 12.1 does not positively answer the following question (where $t, t' \in M(F_+, \mathbf{Unk}(S))$).

12.22. Question. Is it true that $t \approx_{S, \mathcal{E}}^P t'$ iff $t \leftrightarrow_{S, \mathcal{D} \cup \mathcal{E}}^* t'$? If not, find an alternative characterization of the relation $t \approx_{S, \mathcal{E}}^P t'$. Is it semidecidable?

In order to establish the validity of the ‘iff’ it suffices to establish it for all uniform systems S and for all t, t' in $M^+(\emptyset, \mathbf{Unk}(S))$ since the last steps of the proof of Theorem 12.1 can easily be extended to $\approx_{\mathcal{E}}^P$ and $\leftrightarrow_{S, \mathcal{D} \cup \mathcal{E}}$.

A positive answer to the following question would yield a positive answer to Question 12.22. As before \mathcal{E} is linear and balanced.

12.23. Question. Is the $\approx_{\mathcal{E}}^P$ -correct transformation $\mathbf{rufld}_{\mathcal{D} \cup \mathcal{E}}$ also $\approx_{\mathcal{E}}^P$ -complete? If not, find a $\approx_{\mathcal{E}}^P$ -complete set of transformations.

Concerning undecidability we have the following results, which come from the case of regular systems since a regular system over F can be considered as a polynomial system over F with no occurrence of $+$.

12.24. Proposition. *Let \mathcal{E} be a set of linear and balanced equations, let S be a regular system over F and $w, w' \in M(F, \mathbf{Unk}(S))$. Then $w \approx_{S, \mathcal{E}}^P w'$ iff $w \leftrightarrow_{S, \mathcal{D} \cup \mathcal{E}}^* w'$ iff $w \leftrightarrow_{S, \mathcal{E}}^* w'$. Hence, the relations $t \approx_{S, \mathcal{E}}^P t'$ and $t \leftrightarrow_{S, \mathcal{D} \cup \mathcal{E}}^* t'$ are undecidable (where \mathcal{E} is a finite set as above, S is a polynomial system, and t, t' are in $M(F_+, \mathbf{Unk}(S))$).*

Proof. Since $w \leftrightarrow_{S, \mathcal{E}}^* w'$ implies $w \leftrightarrow_{S, \mathcal{E} \cup \mathcal{E}}^* w'$ which implies $w \approx_{S, \mathcal{E}}^P w'$, it suffices to prove that the latter implies $w \leftrightarrow_{S, \mathcal{E}}^* w'$. So let us assume that $w \approx_{S, \mathcal{E}}^P w'$, $U = \text{Unk}(S)$, and consider $\mathbf{M} = \mathbf{M}(F, U) / \leftrightarrow_{S \cup \mathcal{E}}^*$. Since \mathcal{E} is linear and balanced, $\mathbf{P} = \mathcal{P}(\mathbf{M})$ belongs to $\mathcal{V}(\mathcal{E})$. Assuming that $U = \{u_1, \dots, u_n\}$, the n -tuple $([u_1], \dots, [u_n])$ is a solution of S in \mathbf{M} . Hence, the n -tuple $m = (\{[u_1]\}, \dots, \{[u_n]\})$ is a solution of S in \mathbf{P} . Hence $w_{\mathbf{P}}(m) = w'_{\mathbf{P}}(m)$. But Lemma 10.5(2) gives us $w_{\mathbf{P}}(m) = w_{\mathbf{M}}(m) = \{w_{\mathbf{M}}([u_1], \dots, [u_n])\} = \{[w]\}$, and similarly for w' so that $[w] = [w']$. Hence, $w \leftrightarrow_{S \cup \mathcal{E}}^* w'$. The second part of the proposition follows then from the undecidability result of Proposition 3.3. \square

Note that this proposition is consistent with positive answers to Questions 12.21 and 12.22.

12.25. Remark. Let us consider the special case of context-free grammars, i.e., of polynomial systems over T_m in the context of \mathcal{E}_m (see Section 11.4.2).

(1) If G and G' are two grammars having the same set of nonterminals, then

$$S_G \approx_{\mathcal{E}_m}^P S_{G'} \text{ implies } S_G \approx_{\mathcal{P}(T^*)}^P S_{G'},$$

i.e., the former implies that the systems associated with the two grammars have the same n -tuples of languages over T as solutions. The converse is not true (although T^* is the free monoid for the reasons given in Remark 3.7).

Consider $S_G = \langle u = au + b \rangle$ and $S_{G'} = \langle u = aau + ab + b \rangle$. They have the same (unique) solution, namely a^*b in $\mathcal{P}(\{a, b\}^*)$. But it is not difficult to construct a monoid \mathbf{M} where their sets of solutions are distinct. Since $S_G \text{ unfnf}_{\mathcal{E}} S_{G'}$, this shows that the transformation $\text{unfnf}_{\mathcal{E}}$ is not \approx^P -correct.

(2) On the other hand, Berstel has shown in [8, Theorem 1.7] that if in a polynomial system S one replaces an unknown by the right-hand side of its defining equation at only one of its occurrences in a right-hand side, then the system S' that one obtains and the system S have the same solutions in $\mathcal{P}(T^*)$.

One might conjecture that the same holds in the slightly more general situation where $S \text{ unfnf}_{\mathcal{E}_m} S'$. However, this is not the case as shown by the example of $S = \langle u = v + a, v = u + b \rangle$ and $S' = \langle u = u + a + b, v = v + a + b \rangle$ since $(\{a, b\}, \{a, b\}^*)$ is a solution of S' which is not a solution of S .

13. Polynomial systems and their least solutions

Our aim is now to characterize the relations $t \sim_{S, \mathcal{E}}^P t'$, $S \leq_{\mathcal{E}}^P S'$ and $S \sim_{\mathcal{E}}^P S'$, where \mathcal{E} is a set of equations. The characterizations we shall obtain will be based on the following theorem of Mezei and Wright [73] that we have already stated in a more general form for regular systems (Lemma 5.3).

13.1. Proposition. *Let S be a polynomial system, \mathbf{M} and \mathbf{M}' be two F -magmas and h be a homomorphism $\mathbf{M} \rightarrow \mathbf{M}'$. Then $\mu\text{-Psol}_{\mathbf{M}'}(S) = h(\mu\text{-Psol}_{\mathbf{M}}(S))$, i.e., the least solution of S in $\mathcal{P}(\mathbf{M}')$ is the image under h of its least solution in $\mathcal{P}(\mathbf{M})$.*

Proof. Let us extend h into a mapping $\mathcal{P}(\mathbf{M}) \rightarrow \mathcal{P}(\mathbf{M}')$ by $h(A) = \{h(a) \mid a \in A\}$ for $A \subseteq M$. Then h is a homomorphism of distributive F -magmas which is ω -continuous. Since $h(\emptyset) = \emptyset$ and $h(p_{\mathbf{M}}(A_1, \dots, A_n)) = p_{\mathbf{M}'}(h(A_1), \dots, h(A_n))$, for every p in $M(F_+, X_n)$, the conditions of Lemma 5.3 are satisfied and the result immediately follows. \square

13.2. Definition. Let S be a polynomial system with $U = \text{Unk}(S) = \{u_1, \dots, u_n\}$. Its least solution in $\mathcal{P}(M(F))$ is an n -tuple of subsets of $M(F)$ (i.e., of sets of trees) that we denote by $L(S)$ or by $(L(S, u_1), \dots, L(S, u_n))$. For $L \subseteq M(F)$ and \mathbf{M} in \mathcal{V} we denote by $L_{\mathbf{M}}$ the set $\{t_{\mathbf{M}} \mid t \in L\}$, where $t_{\mathbf{M}}$ is the value of t in \mathbf{M} (or, equivalently, $t \mapsto t_{\mathbf{M}}$ is the unique homomorphism $M(F) \rightarrow \mathbf{M}$).

The following proposition is an immediate consequence of Proposition 13.1.

13.3. Proposition. $\mu\text{-Psol}_{\mathbf{M}}(S) = (L(S, u_1)_{\mathbf{M}}, \dots, L(S, u_n)_{\mathbf{M}})$.

For t in $M(F_+, U)$, we denote by $L(S, t)$ the set of trees $t_{\mathcal{P}(M(F))}(L(S))$. We now characterize this set in terms of rewriting sequences. In addition to the ground rewriting system S on $M(F_+ \cup U)$ we associate with S (as in Section 11.1) a ground rewriting system on $M(F \cup U)$ defined as the set of pairs:

$$\text{Dev}(S) = \{(u_i, t) \mid i \in [n], t \in \text{Dev}(p_i)\}.$$

The following lemma states a relation between \rightarrow_S and $\rightarrow_{\text{Dev}(S)}$.

13.4. Lemma. Let $t \in M(F_+, U)$ and $w' \in M(F, U)$. Then $w' \in \text{Dev}(t')$ for some t' such that $t \rightarrow_S^* t'$ iff there exists a w in $\text{Dev}(t)$ such that $w \rightarrow_{\text{Dev}(S)}^* w'$.

We omit the proof which can be done by standard techniques.

The following result is nothing else than an adaptation to the present case of the theorem of Ginsburg and Rice [51] recalled in Section 2.8.

13.5. Proposition. For t in $M(F_+, U)$, $L(S, t) = \{w' \in M(F) \mid w \rightarrow_{\text{Dev}(S)}^* w' \text{ for some } w \text{ in } \text{Dev}(t)\}$. Hence, $L(S, t) = \{w' \in M(F) \mid w' \in \text{Dev}(t') \text{ for some } t' \text{ in } M(F_+, U) \text{ such that } t \rightarrow_S^* t'\}$.

The first equality is in fact a corollary of the theorem of Ginsburg and Rice since if one represents the elements of $M(F, U)$ as words written with the Polish prefix notation, $\text{Dev}(S)$ is a context-free grammar (in the usual sense) with set of nonterminals U . Nevertheless, we shall indicate the main steps of the proof for the sake of completeness.

For w in $M(F, U)$ and $k \geq 0$ we let $L^k(w) = \{w' \in M(F) \mid w \rightarrow_{\text{Dev}(S)}^m w', m \leq k\}$ and $L(w) = \bigcup \{L^k(w) \mid k \geq 0\}$.

13.6. Lemma. *Let $w \in M(F, U)$. Then, for all $k \geq 0$, $L^k(w) \subseteq w[_{\text{OI}}L^k(u_1)/u_1, \dots, L^k(u_n)/u_n]$ and $L(w) = w[_{\text{OI}}L(u_1)/u_1, \dots, L(u_n)/u_n]$.*

Proof. One proves the first assertion by induction on k , simultaneously for all w . The inclusion \subseteq of the second assertion follows. The inclusion \supseteq can be easily proved by structural induction on w . \square

Proof of Proposition 13.5. By Lemmas 10.5(2) and 13.6, $(L(u_1), \dots, L(u_n))$ is a solution of S in $\mathcal{P}(M(F))$.

Let (L_1, \dots, L_n) be an arbitrary solution of S in $\mathcal{P}(M(F))$. By using Lemmas 13.6, 10.5(2) again, one can prove that $L^k(u_i) \subseteq L_i$ for all $k \geq 0$, all i in $[n]$, by induction on k . Hence, $L(u_i) \subseteq L_i$ and $(L(u_1), \dots, L(u_n))$ is the least solution of S , i.e., $L(u_i) = L(S, u_i)$ for all i . Hence, for t in $M(F_+, U)$,

$$\begin{aligned} L(S, t) &= t_{\mathcal{P}(M(F))}(L(S, u_1), \dots, L(S, u_n)) \\ &= \mathbf{Dev}(t)_{\text{OI}}[L(S, u_1), \dots, L(S, u_n)] \quad (\text{by Lemma 10.5(2)}) \\ &= \bigcup_{\text{OI}} \{w[L(S, u_1), \dots, L(S, u_n)] \mid w \in \mathbf{Dev}(t)\} \\ &= \bigcup \{L(w) \mid w \in \mathbf{Dev}(t)\} \quad (\text{by Lemma 13.6}) \\ &= \left\{ w' \in M(F) \mid w \xrightarrow[\mathbf{Dev}(S)]{*} w' \text{ for some } w \text{ in } \mathbf{Dev}(t) \right\}. \end{aligned}$$

The second equality follows from Lemma 13.4. \square

Proposition 13.5 shows that one can recognize the set of trees $L(S, t)$ by a nondeterministic, finite-state, bottom-up tree-automaton (see [16, 44, 50]); it is *recognizable*. It follows, in particular, that properties like $L(S, t) = L(S, t')$ or $L(S, t) \cap L(S, t') = \emptyset$ are decidable.

We now want to characterize the relation $t \sim_{S, \mathcal{E}}^p t'$. Let \mathcal{E} be a fixed set of equations. We shall use the following notations:

- $[w]$ for $\{w' \in M(F) \mid w \leftrightarrow_{\mathcal{E}}^* w'\}$, $w \in M(F)$,
- $[L]$ for $\{[w] \mid w \in L\}$, $L \subseteq M(F)$,
- $[L(S)]$ for $([L(S, u_1)], \dots, [L(S, u_n)])$,
- $\mathbf{M}_{\mathcal{E}}^0$ for $M(F) / \leftrightarrow_{\mathcal{E}}^*$.

13.7. Theorem. *Let S be a polynomial system, let \mathcal{E} be a set of equations, let t, t' be in $M(F_+, U)$. Then $t \sim_{S, \mathcal{E}}^p t'$ if and only if $t \sim_{S, \mathbf{M}_{\mathcal{E}}^0}^p t'$ if and only if $[L(S, t)] = [L(S, t')]$.*

Proof. Let $\mathbf{M} \in \mathcal{V}(\mathcal{E})$, let h and h^0 be the canonical homomorphisms $\mathbf{M}_{\mathcal{E}}^0 \rightarrow \mathbf{M}$ and $M(F) \rightarrow \mathbf{M}_{\mathcal{E}}^0$ respectively. The same notations will be used for their respective

extensions to $\mathcal{P}(\mathbf{M}_{\mathcal{E}}^0)$ and $\mathcal{P}(\mathbf{M}(F))$. Hence,

$$\begin{aligned}\mu\text{-Psol}_{\mathbf{M}_{\mathcal{E}}^0}(S) &= h^0(L(S)) \quad (\text{by Proposition 13.1}) \\ &= [L(S)],\end{aligned}$$

and

$$t_{\mathcal{P}(\mathbf{M}_{\mathcal{E}}^0)}(\mu\text{-Psol}_{\mathbf{M}_{\mathcal{E}}^0}(S)) = h^0(t_{\mathcal{P}(\mathbf{M}(F))}(L(S))) = h^0(L(S, t)) = [L(S, t)].$$

Hence, $t \sim_{S, \mathbf{M}_{\mathcal{E}}^0}^p t'$ iff $[L(S, t)] = [L(S, t')]$. It is clear that $t \sim_{S, \mathcal{E}}^p t'$ implies $t \sim_{S, \mathbf{M}_{\mathcal{E}}^0}^p t'$. Since $t_{\mathcal{P}(\mathbf{M})}(\mu\text{-Psol}_{\mathbf{M}}(S)) = h(t_{\mathcal{P}(\mathbf{M}_{\mathcal{E}}^0)}(\mu\text{-Psol}_{\mathbf{M}_{\mathcal{E}}^0}(S)))$ (by Proposition 13.1), the converse also holds. \square

Characterizations of $S \preceq_{\mathcal{E}}^p S'$ and $S \sim_{\mathcal{E}}^p S'$ immediately follow, but they are undecidable in general.

13.8. Proposition. *The relations $t \sim_{S, \mathcal{E}}^p t'$, $S \preceq_{\mathcal{E}}^p S'$, and $S \sim_{\mathcal{E}}^p S'$ are undecidable in general, even if the word problem for \mathcal{E} is decidable. They are decidable if $\mathcal{E} = \emptyset$.*

Proof. Let $F = T_m$ and $\mathcal{E} = \mathcal{E}_m$ define the theory of monoids, and assume that t and t' belong to $\mathbf{Unk}(S)$. By Theorem 13.7, $t \sim_{S, \mathcal{E}}^p t'$ is equivalent to $[L(S, t)] = [L(S, t')]$. And this is equivalent to the equality of the context-free languages $L(G, t)$ and $L(G, t')$ if G is the context-free grammar such that $\mathbf{Pol}(S) = S_G$ (see Section 11.4.2). Hence, the problem of deciding whether $L(G, u) = L(G, u')$ for a context-free grammar and two of its nonterminals u and u' (which is undecidable) reduces to the problem of deciding whether $t \sim_{S, \mathcal{E}}^p t'$. The latter problem is undecidable, too.

The undecidability results concerning $S \preceq_{\mathcal{E}}^p S'$ and $S \sim_{\mathcal{E}}^p S'$ follow from Lemma 3.4.

If $\mathcal{E} = \emptyset$, deciding whether $t \sim_{S, \mathcal{E}}^p t'$ reduces to deciding whether $L(S, t) = L(S, t')$ and this is decidable since $L(S, t)$ and $L(S, t')$ are both recognizable sets of trees. \square

Our next purpose is to compare the relation $t \sim_{S, \mathcal{E}}^p t'$ with the relation $t \sim_{S, \mathcal{D} \cup \mathcal{E}} t'$. Clearly, we shall need to assume that \mathcal{E} is linear and balanced (this was *not* necessary in Theorem 13.7).

Let us recall from Section 5 that we denote by $(T(S, u_1), \dots, T(S, u_n))$ the least solution of S (which is a *regular* system over F_+) in $\mathbf{M}^\infty(F_+)$, and by $T(S, t)$ (if $t \in M(F_+, U)$) the tree $t[T(S, u_1)/u_1, \dots, T(S, u_n)/u_n]$ which is equal to $t_{\mathbf{M}^\infty(F_+)}(\mu\text{-Sol}_{\mathbf{M}^\infty(F_+)}(S))$.

Since \mathbf{Dev} is the unique ω -continuous homomorphism: $\mathbf{M}^\infty(F_+) \rightarrow \mathcal{P}(\mathbf{M}(F))$, it follows from Proposition 5.2 that $\mathbf{Dev}(T(S, u_i)) = L(S, u_i)$ for all $i \in [n]$, hence, that $\mathbf{Dev}(T(S, t)) = L(S, t)$. With the notations of Theorem 13.7 we have the following corollary.

13.9. Corollary. *Let \mathcal{E} be a set of linear and balanced equations. Let S be a polynomial system and $t, t' \in M(F_+, \text{Unk}(S))$. Then the following properties are equivalent:*

- (i) $t \sim_{S, \mathcal{E}}^P t'$,
- (ii) $t \sim_{S, \mathcal{D} \cup \mathcal{E}} t'$,
- (iii) $[L(S, t)] = [L(S, t')]$,
- (iv) $T(S, t) \equiv_{\mathcal{D} \cup \mathcal{E}} T(S, t')$.

Proof. (ii) \Rightarrow (i) follows by the properties stated in Section 11.3 since \mathcal{E} is linear and balanced.

(ii) \Leftrightarrow (iv) follows from Theorem 5.4.

(i) \Leftrightarrow (iii) is a consequence of Theorem 13.7.

(iii) \Leftrightarrow (iv) follows from Proposition 10.8(4) (using the fact that \mathcal{E} is linear and balanced) and the above remark that $\text{Dev}(T(S, t)) = L(S, t)$. \square

14. Transformations of polynomial systems and \sim -equivalence

Following our general program, we now investigate the $\sim_{\mathcal{E}}^P$ -correctness of system transformations.

Up to now we know that the following transformations are $\sim_{\mathcal{D} \cup \mathcal{E}}$ -correct: **rufld** $_{\mathcal{D} \cup \mathcal{E}}$, **unf** $_{\mathcal{D} \cup \mathcal{E}}$, **redef** $_{\mathcal{D} \cup \mathcal{E}}$, **eunf**.

If \mathcal{E} is linear and balanced, $\sim_{\mathcal{E}}^P$ coincides with $\sim_{\mathcal{D} \cup \mathcal{E}}$ and these transformations are $\sim_{\mathcal{E}}^P$ -correct. However, by Proposition 13.8, this set of transformations is not $\sim_{\mathcal{E}}^P$ -complete. Moreover, there cannot exist in general any recursively enumerable $\sim_{\mathcal{E}}^P$ -complete set of transformations since the relation $\sim_{\mathcal{E}}^P$ is not recursively enumerable.

If $\mathcal{E} = \emptyset$, this negative argument breaks down; hence, one can try to find a \sim^P -complete set of transformations, but we shall not be able to provide any. We shall prove a \sim^P -completeness result where the restriction to a subsystem is used in addition to the above transformations. And the proof of this result will use a notion of \sim^P -canonical system based on the determinization introduced in the proof of Proposition 12.8.

We first introduce a new $\sim_{\mathcal{D}}$ -correct transformation that will help us to transform a polynomial system into a cycle-free one.

14.1. Definition (elimination of cycles). Let S be a polynomial system (as in Section 11.1). Let $j \in [n]$ be such that $u_j \in \text{Dev}(p_j)$ and let S' be the system $\langle u_i = p'_i; 1 \leq i \leq n \rangle$, where $p'_i = p_i$ if $i \neq j$ and $\text{Dev}(p'_j) = \text{Dev}(p_j) - \{u_j\}$. We then write $S \text{ ncycl } S'$. It is clear that $\text{Cycl}(S') \subseteq \text{Cycl}(S)$.

14.2. Proposition. *If S ncycl S' , then $S' \sim_{\mathcal{D}} S$ (hence, $S' \sim^P S$).*

Proof. If S ncycl S' , then $S' \text{fld}_{\mathcal{D}} S$ since, for any equation of S' of the form $u = p$, one has $p \leftrightarrow_{\mathcal{D}} p + p_{S'} \leftarrow u + p$.

Hence, $\mu\text{-Sol}_{\mathbf{P}}(S) \leq \mu\text{-Sol}_{\mathbf{P}}(S')$, but this does not prove the equality since $\text{fld}_{\mathcal{D}}$ is not $\sim_{\mathcal{D}}$ -correct in general (and for this reason we have introduced ncycl as a separate transformation).

However, since $p'_{i\mathbf{P}} \leq p_{i\mathbf{P}}$ for all i , $S'_{\mathbf{P}} \leq S_{\mathbf{P}}$ and $S'_{\mathbf{P}}^h(\perp_{\mathbf{P}}^n) \leq S_{\mathbf{P}}^h(\perp_{\mathbf{P}}^n)$ for all $h \geq 0$. Hence, $\mu\text{-Sol}_{\mathbf{P}}(S') \leq \mu\text{-Sol}_{\mathbf{P}}(S)$ and the equality holds. \square

We now consider the \sim -reduction of polynomial systems, which extends the results at the end of Section 5.

14.3. Definition. Let S be a polynomial system. Let $\text{Unk}_{\sim}^0(S) = \{u \in \text{Unk}(S) \mid u \sim_S^P \Omega\}$ and $\text{Unk}_{\sim}^+(S) = \text{Unk}(S) - \text{Unk}_{\sim}^0(S)$. We say that S is \sim -reduced if, for every u_i in $\text{Unk}(S)$, $p_i \in M^+(F, \text{Unk}_{\sim}^+(S))$ and $u_i \in \text{Unk}_{\sim}^0(S)$ iff $p_i = \Omega$.

We let $S' = \langle u_i = p'_i; i \in [n] \rangle$ be the system such that $p'_i = \text{Pol}(p_i[\Omega/u; u \in \text{Unk}_{\sim}^0(S)])$ if $u_i \in \text{Unk}_{\sim}^+(S)$ and $p'_i = \Omega$ otherwise. It is also denoted by $\text{Red}_{\sim}(S)$.

These definitions generalize those of Definition 5.15 for regular systems and are fully similar to the ones given in Definition 12.2 with respect to \approx_S^P . As in definition 12.2, a more precise notation would have been $\text{Unk}_{\sim^P}^0(S)$ or $\text{Unk}_{\sim^P}^+(S)$, but the remarks made there apply here as well.

As in Definition 12.2, we can compute the set $\text{Unk}_{\sim}^0(S)$. Let $U = \text{Unk}(S)$ and let

$$U_0 = \emptyset, \quad U_{i+1} = U_i \cup \{u_j \in U \mid \text{Dev}(p_j) \cap M(F, U_i) \neq \emptyset\}.$$

Hence, U_1 is the set of unknowns u such that $u \rightarrow_{\text{Dev}(S)} w$ for some w in $M(F)$ (in the case of context-free grammars, this corresponds to the left-hand sides of terminal productions). In words, U_{i+1} is the set of unknowns u_j such that $u_j \in U_i$ or there exists a monomial in p_j with all its unknowns in U_i .

Let $U_{\infty} = \bigcup \{U_i \mid i \geq 0\}$. Since $U_0 \subseteq U_1 \subseteq \dots \subseteq U_i \subseteq \dots \subseteq U$ and U is finite, $U_{\infty} = U_i$ for some i and U_{∞} can be effectively computed.

14.4. Proposition. (1) $\text{Unk}_{\sim}^+(S) = U_{\infty}$.

(2) $S \text{redef}_{\mathcal{D}}^{-1} \text{Red}_{\sim}(S)$. Hence, $\text{Red}_{\sim}(S) \sim_{\mathcal{D}} S$ and $\text{Red}_{\sim}(S)$ is \sim -reduced.

Proof. (1) It is clear that $u \in U_{\infty}$ implies $L(S, u) \neq \emptyset$, hence, $u \in \text{Unk}_{\sim}^+(S)$.

One can apply Scott's Induction Principle to the property P such that

$$P(x_1, \dots, x_n) \Leftrightarrow \bigwedge \{x_i = \emptyset \mid u_i \in \text{Unk}(S) - U_{\infty}\}.$$

This shows that $u \notin \text{Unk}_{\sim}^+(S)$ if $u \notin U_{\infty}$.

Part (2) is proved by an easy adaptation of the proof of Proposition 5.16. \square

This transformation corresponds to the usual reduction step of context-free grammars consisting in the deletion of nonterminals which do not generate any word. Here we do not delete the nonterminals since we want to compare the new grammar to the given one by means of an equivalence relation which concerns pairs of regular systems having the same unknowns.

We now prove some properties of deterministic polynomial system, for they will play a crucial role in the construction of a \sim^P - (or $\sim_{\mathcal{D}}$ -) canonical system, and this construction will give us a \sim^P - (or $\sim_{\mathcal{D}}$ -) completeness result.

14.5. Lemma. *If S is a deterministic polynomial system, if $u, u' \in \text{Unk}(S)$, and $u' \neq u$ then $L(S, u) \cap L(S, u') = \emptyset$.*

Proof. Let us recall from Section 13 that $L(S, u) = \{t \in M(F) \mid u \rightarrow_{\text{Dev}(S)}^* t\}$ for every polynomial system S . Let S be deterministic. Then the ground rewriting system $R = \text{Dev}(S)^{-1}$ has no critical pair (hence, is confluent) and is Noetherian. Hence every t in $M(F, U)$ (where $U = \text{Unk}(S)$) has a unique R -normal form $\text{nf}_R(t)$ and $L(S, u) = \{t \in M(F) \mid \text{nf}_R(t) = u\}$. Since $\text{nf}_R(t)$ is uniquely defined, one cannot have simultaneously t in $L(S, u)$ and in $L(S, u')$ if $u' \neq u$. \square

14.6. Lemma. *Let S and S' be two \sim -reduced deterministic polynomial systems. Then $S \sim_{\mathcal{D}} S'$ iff $S = S'$.*

Proof. Let us consider S . Let s belong to $F(U)$, say $s = f(u_{i_1}, \dots, u_{i_k})$, and let $i \in [n]$

Claim. $s \in \text{Dev}(p_i)$ iff $u_{i_1}, \dots, u_{i_k} \in \text{Unk}^+(S)$ and $f(L(S, u_{i_1}), \dots, L(S, u_{i_k})) \subseteq L(S, u_i)$

Proof. The ‘only if’ part immediately follows from the definitions.

Conversely, let $u_{i_1}, \dots, u_{i_k} \in \text{Unk}^+(S)$ be such that $f(L(S, u_{i_1}), \dots, L(S, u_{i_k})) \subseteq L(S, u_i)$. For each $j = 1, \dots, k$, let t_j be an element of $L(S, \tilde{u}_{i_j})$ and $t = f(t_1, \dots, t_k)$. Hence, $t \in L(S, u_i)$.

By the proof of Lemma 14.5, $t_j \rightarrow_R^* u_{i_j}$ for all j , hence, $t \rightarrow_R^* f(u_{i_1}, \dots, u_{i_k})$. Since R is confluent and Noetherian, $f(u_{i_1}, \dots, u_{i_k}) \rightarrow_R^* \text{nf}_R(t) = u_i$. In fact (since S is uniform), $f(u_{i_1}, \dots, u_{i_k}) \rightarrow_R u_i$, i.e., $f(u_{i_1}, \dots, u_{i_k}) \in \text{Dev}(p_i)$. This proves the claim. \square

Proof of Lemma 14.6 (continued). Let S and S' be deterministic, \sim -reduced, and $\sim_{\mathcal{D}}$ -equivalent (S is as in Section 11.1 and $S' = \langle u_i = p'_i; 1 \leq i \leq n \rangle$). For all i in $[n]$, $p_i = \Omega$ iff $p'_i = \Omega$ (since $S' \sim^P S$ and they are both \sim -reduced). If $p_i \neq \Omega$, then $\text{Dev}(p_i) \neq \emptyset$. The claim and the hypothesis that $S' \sim_{\mathcal{D}} S$ (whence $L(S', u_j) = L(S, u_j)$ for all j in $[n]$) prove that $\text{Dev}(p_i) \subseteq \text{Dev}(p'_i)$. By symmetry, the equality holds. Hence, $S = S'$. (We have an equality since the polynomials in the right-hand side of S and S' are ordered in a canonical way.) \square

14.7. Definition. A polynomial system S is *quasi-deterministic* if there exist U_0 and U_1 such that:

- (1) $\mathbf{Unk}(S) = U_0 \cup U_1, U_0 \cap U_1 = \emptyset,$
- (2) $U_1 \subseteq \mathbf{Unk}^+(S),$
- (3) $S \upharpoonright U_1$ is a subsystem of S and is deterministic,
- (4) $p_i \in M^+(\emptyset, U_1)$ for all u_i in U_0 .

Hence, a quasi-deterministic system is quasi-uniform and has no cyclic unknown.

It is easy to verify whether a given system is quasi-deterministic (the verification of condition (2) uses Proposition 14.4) and there exists at most one pair (U_0, U_1) satisfying conditions (1)–(4). Note that by conditions (2) and (4), $S \upharpoonright U_1$ and S are necessarily \sim -reduced.

We now modify the construction in Section 12 in order to associate a quasi-deterministic system with a uniform system S .

Construction. Let S be a uniform system, let \bar{S} be the associated deterministic system (cf. the construction in Section 12). Let now $\bar{U}_+ = \mathbf{Unk}^+(\bar{S})$ and \bar{S}_+ be the system $\mathbf{Red}_\sim(\bar{S}) \upharpoonright \bar{U}_+$. Let S'' be the set of equations $\langle u_i = q_i; 1 \leq i \leq n \rangle$, where $q_i = \sum \{\bar{\alpha} \mid \bar{\alpha} \in \bar{U}_+, u_i \in \alpha\}$ for i in $[n]$ and let $S' = S'' \cup \bar{S}_+$. The system S' is quasi-deterministic (for the partition (U, \bar{U}_+) of its set of unknowns). Let us denote S' by $\mathbf{Qdet}(S)$. With these notations, we have the following proposition.

14.8. Proposition. *Let S be a uniform polynomial system. Then $\mathbf{Qdet}(S) \mathbf{redef}_\emptyset(S \cup \bar{S}_+)$ and $S \sim_{\emptyset, \mathbf{Unk}(S)} \mathbf{Qdet}(S)$.*

Proof. We verify conditions (1)–(3) of Definition 5.10 as in the proof of Lemma 12.9, where \bar{S}_+ is the subsystem which is common to $\mathbf{Qdet}(S)$ and $(S \cup \bar{S}_+)$.

Condition (1) holds from the definition of $\mathbf{Qdet}(S)$ and so does condition (2), exactly as in the proof of Lemma 12.9.

The computations done in the proof of Lemma 12.9 for proving condition (3) can be adapted as follows (with $\bar{S}_+ = \langle \bar{\alpha} = p_{\bar{\alpha}}; \bar{\alpha} \in \bar{U}_+ \rangle$):

$$\begin{aligned} & \mathbf{Dev}(q_i[p_{\bar{\alpha}}/\bar{\alpha}; \bar{\alpha} \in \bar{U}_+]) \\ &= \bigcup \{f(\bar{\alpha}_1, \dots, \bar{\alpha}_k) \mid \bar{\alpha}_1, \dots, \bar{\alpha}_k \in \bar{U}_+ \text{ and } u_i \in \alpha, \bar{\alpha} \in \bar{U}_+, \\ & \quad \text{where } \alpha = \bar{f}(\alpha_1, \dots, \alpha_k)\}, \end{aligned}$$

$$\begin{aligned} & \mathbf{Dev}(p_i[q_1/u_1, \dots, q_n/u_n]) \\ &= \{f(\bar{\alpha}_1, \dots, \bar{\alpha}_k) \mid k \geq 0, f \in F_k, \text{ there exist } i_1, \dots, i_k \text{ such that} \\ & \quad f(u_{i_1}, \dots, u_{i_k}) \in \mathbf{Dev}(p_i), u_{i_1} \in \alpha_1, \dots, u_{i_k} \in \alpha_k \text{ and } \bar{\alpha}_1, \dots, \bar{\alpha}_k \in \bar{U}_+\} \\ &= \mathbf{Dev}(q_i[p_{\bar{\alpha}}/\bar{\alpha}; \bar{\alpha} \in \bar{U}_+]), \end{aligned}$$

by the definition of $\bar{f}(\alpha_1, \dots, \alpha_k)$ (see the construction in Section 12) and the fact that $\bar{\alpha}_1, \dots, \bar{\alpha}_k \in \bar{U}_+$ and $\alpha = \bar{f}(\alpha_1, \dots, \alpha_k)$ implies $\bar{\alpha} \in \bar{U}_+$ (this follows from the definition of \bar{S}). Hence, condition (3) holds and $\mathbf{Qdet}(S) \text{ redef}_{\mathcal{D}}(S \cup \bar{S}_+)$. The second assertion follows from Corollary 5.12. \square

The following lemma will help us to prove that $\mathbf{Qdet}(S)$ is nearly \sim^P -canonical (it is not exactly since $\mathbf{Qdet}(S)$ is not \sim^P -equivalent to S since their sets of unknowns are different; furthermore, $\mathbf{Qdet}(S)$ is defined only if S is uniform).

14.9. Lemma. *For every $\bar{\alpha}$ in \bar{U} , $L(\bar{S}, \bar{\alpha}) = \bigcap \{L(S, u) \mid u \in \alpha\} \cap \bigcap \{M(F) - L(S, u) \mid u \in \text{Unk}(S) - \alpha\}$*

Proof. From Lemma 12.9, it follows that

$$L(S, u) = \bigcup \{L(\bar{S}, \bar{\alpha}) \mid \bar{\alpha} \in \bar{U}, u \in \alpha\}.$$

Hence,

$$L(\bar{S}, \bar{\alpha}) \subseteq \bigcap \{L(S, u) \mid u \in \alpha\}$$

and since $L(\bar{S}, \bar{\alpha}) \cap L(\bar{S}, \bar{\beta}) = \emptyset$, for $\bar{\beta} \in \bar{U}$, $\bar{\beta} \neq \bar{\alpha}$,

$$L(S, u) \cap L(\bar{S}, \bar{\beta}) = \emptyset$$

whenever $\beta \subseteq U$, $u \notin \beta$.

Hence,

$$L(\bar{S}, \bar{\alpha}) \subseteq \bigcap \{L(S, u) \mid u \in \alpha\} \cap \bigcap \{M(F) - L(S, u) \mid u \notin \alpha\}. \quad (6)$$

The collection of all sets $L(\bar{S}, \bar{\alpha})$ for $\alpha \subseteq U$ forms a partition of $\bigcup \{L(S, u) \mid u \in \text{Unk}(S)\}$ and so do the right-hand sides of the inequalities of the form (6) (for all $\alpha \subseteq U$). Hence, the equality holds in (6) for all $\alpha \subseteq U$. \square

14.10. Proposition. *Let S and S' be uniform. Then $S \sim_{\mathcal{D}} S'$ iff $\mathbf{Qdet}(S) = \mathbf{Qdet}(S')$.*

Proof. Let S and S' be uniform systems such that $S \sim_{\mathcal{D}} S'$ (and let $U = \text{Unk}(S) = \text{Unk}(S')$). They have the same least solution in $\mathbf{M}(F)$, i.e., $L(S, u) = L(S', u)$ for all u in U . Hence, $L(\bar{S}, \bar{\alpha}) = L(\bar{S}', \bar{\alpha})$ for all $\alpha \subseteq U$ (by Lemma 14.9), hence, $\bar{S} \sim_{\mathcal{D}} \bar{S}'$. It follows that $\bar{S}_+ \sim_{\mathcal{D}} \bar{S}'_+$. Since they are \sim -reduced, they are equal by Lemma 14.6. Hence, $\mathbf{Qdet}(S) = \mathbf{Qdet}(S')$. \square

14.11. Example. Let $S = \langle u = fu + a + b, v = fv + a \rangle$ and $S' = \langle u = fu + fv + a + b, v = fv + a \rangle$. The system \bar{S} is (with the notational convention of Example 12.12)

$$\bar{S} = \langle \bar{u} = f\bar{u} + b, \bar{u}\bar{v} = f\bar{u}\bar{v} + a, \bar{v} = f\bar{v}, \bar{\emptyset} = f\bar{\emptyset} \rangle.$$

One then obtains (after the \sim -reduction step)

$$\mathbf{Qdet}(S) = \langle u = \bar{u} + \bar{u}\bar{v}, v = \bar{u}\bar{v}, \bar{u} = f\bar{u} + b, \bar{u}\bar{v} = f\bar{u}\bar{v} + a \rangle.$$

For S' one obtains

$$\bar{S}' = \langle \bar{u} = f\bar{u} + b, \bar{u}\bar{v} = f\bar{u}\bar{v} + f\bar{v} + a, \bar{v} = \bar{\emptyset}, \bar{\emptyset} = f\bar{\emptyset} \rangle$$

(note that $\bar{S}' \neq \bar{S}$), but after the \sim -reduction steps which eliminates \bar{v} and $\bar{\emptyset}$, one obtains $\mathbf{Qdet}(S') = \mathbf{Qdet}(S)$. This shows that $S \sim_{\mathcal{D}} S'$.

The following corollary of Proposition 14.10 shows the \sim^P -completeness (in a limited sense) of the set of transformations $\{\mathbf{redef}_{\mathcal{D}}, \mathbf{redef}_{\mathcal{D}}^{-1}\}$.

14.12. Corollary. *Let S and S' be two uniform polynomial systems having the same set of unknowns. Then $S \sim_{\mathcal{D}} S'$ iff there exist two quasi-uniform systems S_1 and S_2 such that*

$$S \subseteq S_1 \mathbf{redef}_{\mathcal{D}}^{-1} \cdot \mathbf{redef}_{\mathcal{D}} S_2 \supseteq S'.$$

Proof. Let $U = \mathbf{Unk}(S) = \mathbf{Unk}(S')$. If S_1 and S_2 are as in the statement, then $S_1 \sim_{\mathcal{D}} S_2$, hence, $S_1 \sim_{\mathcal{D}, U} S_2$ and $S \sim_{\mathcal{D}, U} S'$, i.e., $S \sim_{\mathcal{D}} S'$.

Conversely, if $S \sim_{\mathcal{D}} S'$, then one can take $S_1 = S \cup \bar{S}'_+$ and $S_2 = S' \cup \bar{S}'_+$. Proposition 14.10 shows that $\mathbf{Qdet}(S_1) = \mathbf{Qdet}(S_2)$ and the result follows from Proposition 14.8. \square

14.13. Lemma. *Let S be a polynomial system. One can construct a system R and a uniform system T such that $S \subseteq R\mathcal{T}_0^*T$, where $\mathcal{T}_0 = \{\mathbf{rflld}_{\mathcal{D}}, \mathbf{ncycl}\}$.*

Proof. The proof will use two main steps by which S is successively transformed into a quasi-uniform system S_1 and then into a uniform system T .

First step: For the first step we let $S_1 = \mathbf{Ufm}(S)$ so that there exists R such that $S \subseteq_{\ell} R \mathbf{rflld}_{\mathcal{D}} S_1$ and $S_1 \approx_{\mathcal{D}, U} S$ by Proposition 12.17.

Second step: Let S'_1 be the system associated with S_1 by Definition 12.13 and such that $S_1 \mathbf{runf}_{\mathcal{D}}^* S'_1$ (by Lemma 12.14). Its set of unknowns is U' and, for every two equations $u = p$ and $u' = p'$ such that $u \rightarrow_{\mathbf{Dev}(S'_1)}^+ u' \rightarrow_{\mathbf{Dev}(S'_1)}^+ u$, one has $p = p'$ (since polynomials are ordered in a canonical way).

Let U'_1 be a subset of $\mathbf{Cycl}(S'_1)$ of the form $U'_1 = \{u' \mid u' \rightarrow_{\mathbf{Dev}(S'_1)}^+ u \rightarrow_{\mathbf{Dev}(S'_1)}^+ u'\}$ for some u in $\mathbf{Cycl}(S'_1)$ and such that $\mathbf{Card}(U'_1) \geq 2$. Without loss of generality we can assume that $U'_1 = \{u_1, \dots, u_k\}$ and $S'_1 = \langle u_i = p_i; 1 \leq i \leq n \rangle$. Hence, $p_2 = \dots = p_k = p_1$ and $p_1 = u_1 + u_2 + \dots + u_k + r$ for some r in $M^+(F, U)$ such that $\mathbf{Dev}(r) \cap U'_1 = \emptyset$.

We have $S'_1 \mathbf{rflld} T_1 \mathbf{runf}_{\mathcal{D}} T'_1$, where T_1 is as S'_1 except that the equation $u_i = u_1$ replaces the equation $u_i = p_i$ for every $i = 2, 3, \dots, k$ and where T'_1 is as T_1 except that the equation $u_1 = \mathbf{Pol}(u_1 + r[u_1/u_2, \dots, u_1/u_k])$ replaces the equation $u_1 = p_1$. Hence, $S'_1 \mathbf{rflld}_{\mathcal{D}}^* T'_1$.

This transformation can be applied to T'_1 yielding T'_2 such that $T'_1 \mathbf{rflld}_{\mathcal{D}}^* T'_2$ and to T'_2 , etc., until one obtains a system T'_k where all sets like U'_1 above are singletons. Let $S''_1 = T'_k$ so that $S'_1 \mathbf{rflld}_{\mathcal{D}}^* S''_1$ and, in S''_1 , an unknown u_i is cyclic iff $u_i \in \mathbf{Dev}(p)$,

where p is the right-hand side of its defining equation in S_1'' . Hence, there exists a cycle-free system S_1''' such that $S_1'' \text{ncycl}^* S_1'''$ (the cyclic unknowns of S_1'' are made noncyclic by several applications of **ncycl**). An obvious adaptation of the proof of (3) \Rightarrow (4) of Theorem 8.8 to polynomial systems yields a uniform system T such that $S_1''' \text{runf}_{\mathcal{D}}^* T$.

To summarize, we have

$$S_1 \text{rufld}_{\mathcal{D}}^* . \text{ncycl}^* . \text{runf}_{\mathcal{D}}^* T$$

(hence $T \sim_{\mathcal{D}} S_1$, but due to the presence of **ncycl**, $T \not\sim_{\mathcal{D}} S_1$ in general). Hence, we have $S \subseteq R\mathcal{T}_0^* T$. \square

We shall now extend Corollary 14.12 to pairs of polynomial systems which are not uniform. It will not be more difficult to formulate this extension for systems S and S' such that $S \sim_{\mathcal{D}, W} S'$ for some $W \subseteq \text{Unk}(S) \cap \text{Unk}(S')$ so that we shall also obtain an extension of Proposition 7.5.

14.14. Theorem. *Let S and S' be two polynomial systems and W be a subset of $\text{Unk}(S) \cap \text{Unk}(S')$. Then $S \sim_{\mathcal{D}, W} S'$ if and only if there exist a renaming α and two polynomial systems R and R' such that α is the identity on W , $\text{Unk}(\alpha(S)) \cap \text{Unk}(S') = W$, and $\alpha(S) \subseteq R\mathcal{T}^* R' \supseteq S'$, where $\mathcal{T} = \{\text{rufld}_{\mathcal{D}}, \text{ncycl}, \text{ncycl}^{-1}, \text{redef}_{\mathcal{D}}, \text{redef}_{\mathcal{D}}^{-1}\}$.*

Proof. The ‘if’ part is an immediate consequence of various preceding results. We only prove the other direction.

Let S and S' be such that $S \sim_{\mathcal{D}, W}^P S'$. We first assume that $W = \text{Unk}(S) \cap \text{Unk}(S')$ and we let α be the identity. By Lemma 14.13, there exist systems S_1, S_2, S'_1, S'_2 such that S_2 and S'_2 are uniform and

$$S \subseteq S_1 \mathcal{T}_0^* S_2, \quad S' \subseteq S'_1 \mathcal{T}_0^* S'_2, \quad \text{Unk}(S_2) \cap \text{Unk}(S'_2) = W,$$

(where \mathcal{T}_0 is as in Lemma 14.13). This implies that $S_2 \sim_{\mathcal{D}, W} S'_2$.

The construction of Proposition 7.5 can be applied to S_2 and S'_2 and produces uniform systems S_3 and S'_3 such that

$$S_2 \subseteq S_3 \quad (\text{say, } S_3 = S_2 \cup T_2),$$

$$S'_2 \subseteq S'_3 \quad (\text{say, } S'_3 = S'_2 \cup T'_2),$$

$$S_3 \sim_{\mathcal{D}} S'_3.$$

From Propositions 14.10 and 14.8, it follows that

$$\text{Qdet}(S_3) = \text{Qdet}(S'_3),$$

$$\text{Qdet}(S_3) \text{redef}_{\mathcal{D}}(S_3 \cup T_3) \quad (\text{where } T_3 = \bar{S}_{3+} \text{ (cf. the construction)}),$$

$$\text{Qdet}(S'_3) \text{redef}_{\mathcal{D}}(S'_3 \cup T'_3) \quad (\text{where } T'_3 = \bar{S}'_{3+}).$$

Hence,

$$S \subseteq (S_1 \cup T_2 \cup T_3) \mathcal{T}_0^* (S_2 \cup T_2 \cup T_3) \text{redef}_{\mathcal{D}}^{-1} \text{Qdet}(S_3)$$

and similarly for S' so that the result holds with $R = S_1 \cup T_2 \cup T_3$ and $R' = S'_1 \cup T'_2 \cup T'_3$.

If $W \subset \text{Unk}(S) \cap \text{Unk}(S')$ one defines α as in the proof of Proposition 7.5 and the above proof works with $\alpha(S)$ instead of S . \square

14.15. Open problem. Is the set consisting of the transformations rufld_\varnothing , unf_\varnothing , eunf , redef_\varnothing , ncycl , and their inverses \sim_\varnothing - (equivalently \sim^P -) complete? If it is, this means that if $S \sim^P S'$, one can transform S into S' by using these transformations and without introducing auxiliary unknowns as we do in Theorem 14.14, even if $W = \text{Unk}(S) = \text{Unk}(S')$. If it is not, the problem is to find another one which is.

15. Polynomial systems having a unique solution

We shall give sufficient conditions insuring that a polynomial system has a unique solution in some powerset magma $\mathcal{P}(\mathbf{M})$. We shall obtain necessary and sufficient conditions for the cases where $\mathbf{M} = \mathbf{T}^*$ and $\mathbf{M} = \mathbf{T}^+$ which arise from the study of context-free grammars.

15.1. Definitions. Let M be a set and \mathcal{F} be a set of total polyadic operations on M . Let \rightarrow be the binary relation on M such that

$$m \rightarrow m' \text{ iff } m = \alpha(m_1, \dots, m_i, m', m_{i+1}, \dots, m_k)$$

for some k -ary α in \mathcal{F} and some m_1, \dots, m_k .

We say that M is *well-founded with respect to* \mathcal{F} if there is no infinite sequence $m_1 \rightarrow m_2 \rightarrow \dots \rightarrow m_n \rightarrow m_{n+1} \dots$.

Let $S = \langle u_i = p_i; 1 \leq i \leq n \rangle$ be a polynomial system over F and \mathbf{M} be an F -magma.

For every element t of $M(F, U)$, let \bar{t} be the unique element of $M(F, X_k)$ such that

- (i) $\text{Var}(\bar{t}) = X_k$ and \bar{t} is X_k -linear,
- (ii) $t = \bar{t}[u_{i_1}/x_1, \dots, u_{i_k}/x_k]$ for some i_1, \dots, i_k ,
- (iii) x_i is to the left of x_{i+1} in \bar{t} (assumed to be linearly written) for $1 \leq i < k$.

Note that $k = |t|_U$. By \bar{t}_M we mean the total mapping: $M^k \rightarrow M$, associated with \bar{t} . Hence, the arity of \bar{t}_M is equal to $|t|_U$.

Let $\mathcal{F}(\mathbf{M}, S) = \{\bar{t}_M \mid t \in \text{Dev}(p_i), i \in [n]\}$. We say that \mathbf{M} is *well-founded with respect to* S if M is well-founded with respect to $\mathcal{F}(\mathbf{M}, S)$. These definitions are motivated by the following result:

15.2. Proposition. *Let S be a polynomial system over F , let \mathbf{M} be an F -magma which is well-founded w.r.t. S . Then S is $\mathcal{P}(\mathbf{M})$ -univocal.*

Proof. Let (A_1, \dots, A_n) be the least solution of S in $\mathcal{P}(\mathbf{M})$. Let us assume the existence of another solution (B_1, \dots, B_n) of S in $\mathcal{P}(\mathbf{M})$. Necessarily, $A_i \subseteq B_i$ for all i in $[n]$.

Assume that for some i there exists an m in $B_i - A_i$. There exists a t in $\text{Dev}(p_i)$ such that

$$\begin{aligned} m &= \bar{t}_{\mathbf{M}}(m'_1, \dots, m'_k), \\ m'_j &\in B_{i_j} \quad \text{for all } j = 1, \dots, k, \end{aligned}$$

where (i_1, \dots, i_k) is such that

$$t = \bar{t}[u_{i_1}/x_1, \dots, u_{i_k}/x_k].$$

For at least one j in $[k]$, $m'_j \in B_{i_j} - A_{i_j}$, otherwise, $m \in A_i$ contradicting the initial assumption. Hence, if one lets $m_1 = m'_j$ for such a j , one has

$$\begin{aligned} m_1 &\in B_{i'} - A_{i'} \quad \text{for some } i' \in [n], \\ m &\rightarrow m_1, \end{aligned}$$

where \rightarrow is defined over M with respect to $\mathcal{F}(\mathbf{M}, S)$.

The same argument can be repeated for m_1 instead of m yielding m_2 and then for m_2 , etc. so that one gets an infinite sequence:

$$m \rightarrow m_1 \rightarrow m_2 \rightarrow \dots \rightarrow m_i \rightarrow \dots$$

contradicting the hypothesis that \mathbf{M} is well-founded w.r.t. S .

Hence, $A_i = B_i$ for all i in $[n]$, i.e., the least solution of S in $\mathcal{P}(\mathbf{M})$ is the only one. \square

An F -magma $\mathbf{M} = \langle M, \langle f_{\mathbf{M}} \rangle_{f \in F} \rangle$ is *well-founded* if \mathbf{M} is well-founded with respect to $\{f_{\mathbf{M}} \mid f \in F\}$. We denote by \mathcal{W} the class of well-founded F -magmas and by \mathcal{PW} the class $\{\mathcal{P}(\mathbf{M}) \mid \mathbf{M} \in \mathcal{W}\}$.

15.3. Proposition. *Every Greibach polynomial system is \mathcal{PW} -univocal.*

Proof. It is easy to verify that if \mathbf{M} is well-founded, then it is well-founded with respect to $\{t_{\mathbf{M}} \mid k \geq 0, t \in F(M(F, X_k)), \text{Var}(t) = X_k\}$.

The result then follows from Proposition 15.2. \square

Here is an important class of well-founded magmas:

15.4. Definition. Let $\mathbf{M} = \langle M, \langle f_{\mathbf{M}} \rangle_{f \in F} \rangle$ be such that every m in M has a length $|m| \geq 0$. We say that a mapping $\alpha : M^k \rightarrow M$ is *spanning* if $|\alpha(m_1, m_2, \dots, m_k)| > |m_i|$ for all i in $[k]$, all m_1, \dots, m_k in M . We say that \mathbf{M} is *spanning* if each $f_{\mathbf{M}}$ is spanning.

It is clear that M is well-founded w.r.t. any set \mathcal{F} of spanning functions, and that \mathbf{M} is well-founded if it is spanning. Hence, a Greibach system is $\mathcal{P}(\mathbf{M})$ -univocal if \mathbf{M} is spanning. This result can also be established as a corollary of Proposition 8.6(2) as follows.

One defines a distance on $\mathcal{P}(\mathbf{M})$ by letting, for $A, A' \subseteq M$,

$$d(A, A') = 2^{-n} \quad \text{where } n = \mathbf{Min}\{|m| \mid m \in (A - A') \cup (A' - A)\}.$$

One can prove that $\mathcal{P}(\mathbf{M})$ is complete and that if \mathbf{M} is spanning, every Greibach polynomial system is $\mathcal{P}(\mathbf{M})$ -contracting, hence, has a unique solution. This proof technique has been used in [14, 78] for polynomial systems associated with context-free grammars. See also Examples 15.7 and 15.9.

If \mathbf{M} is spanning, then, for all m ,

$$h(m) = \mathbf{Max}\{n \mid m \xrightarrow{n} m' \text{ for some } m' \in M\} \leq |m|.$$

Hence, \mathbf{M} is well-founded. Conversely, if \mathbf{M} is well-founded and is such that $h(m)$ is finite for all m in M , then it is spanning w.r.t. the mapping $h: M \rightarrow \mathbb{N}$ taken as a length. However, \mathbf{M} may be well-founded without h being finite, i.e., without being spanning. Hence, Proposition 15.3 is more powerful than the topological argument.

15.5. Remark. A polynomial system may be $\mathcal{P}(\mathbf{M})$ -univocal without \mathbf{M} being well-founded w.r.t. it. It suffices to consider the system $S = \langle u = fu + a \rangle$ and \mathbf{M} with domain $\{a, b, c\}$ such that $f_{\mathbf{M}}(a) = b$ and $f_{\mathbf{M}}(b) = f_{\mathbf{M}}(c) = a$. The unique solution of S is $\{a, b\}$, but $a \rightarrow b \rightarrow a \rightarrow b \rightarrow \dots$.

The following theorem is similar to Theorem 8.8 and most steps of its proof will be adapted from the corresponding ones in that of Theorem 8.8.

15.6. Theorem. *Let S be a polynomial system and \mathbf{M} be a well-founded F -magma such that M contains at least one element outside the components of $\mu\text{-Psol}_{\mathbf{M}}(S)$. The following conditions are equivalent:*

- (1) S is \mathcal{PW} -univocal,
- (2) S is $\mathcal{P}(\mathbf{M})$ -univocal,
- (3) S has no cyclic unknowns,
- (4) $S \mathbf{runf}_{\mathcal{D}}^* S'$ for some Greibach polynomial system S' ,
- (5) S^h is a Greibach polynomial system for some $h \geq 1$.

Proof. (1) \Rightarrow (2) is trivial.

(2) \Rightarrow (3): This is easily adapted from Theorem 8.8. Let u_k be cyclic and let $d \in M$ be outside all components of $\mu\text{-Psol}_{\mathbf{M}}(S)$. Let $m = (m_1, \dots, m_n)$ be such that $m_j = \{d\}$ whenever $u_j \rightarrow_{\mathcal{D}}^* u_k$ and $m_j = \emptyset$ otherwise. It is easy to verify that $m \subseteq S_{\mathcal{P}(\mathbf{M})}(m)$. Hence, the sequence $S_{\mathcal{P}(\mathbf{M})}^i(m)$, $i \geq 0$, is increasing and its least upper bound defines a solution of S in $\mathcal{P}(\mathbf{M})$ which differs from the least one, which gives a contradiction.

(3) \Rightarrow (4): This is an easy adaptation from the corresponding case of Theorem 8.8.

(4) \Rightarrow (1): This follows from Proposition 15.3 and the fact that $S \text{runf}_{\mathcal{D}}^* S'$ implies $S' \approx^P S$.

(5) \Rightarrow (1): This follows from Proposition 8.2(1) with $\mathcal{E} = \mathcal{D}$, from Proposition 15.3 and the fact that $S \text{unf}_{\mathcal{D}} S^h$.

(3) \Rightarrow (5): This is proved as in Theorem 8.8 with $h = 1 + \text{Max}\{m \mid u \rightarrow_{\text{Dev}(S)}^m u', u, u' \in \text{Unk}(S)\}$. \square

15.7. Example (proper context-free grammars). We use the notations of Section 11.4.2. We consider ε -free context-free grammars, with which polynomial systems over T_s are associated. These systems are solved in $\mathcal{P}(\mathbf{T}^+)$.

A grammar $G = \langle N, T, P \rangle$ is *proper* if, for every rule $u \rightarrow m$ in P , the word m belongs to $(N \cup T)^+ - N$. Hence, G is proper iff S_G is a Greibach system over T_s .

It is clear that \mathbf{T}^+ is spanning (w.r.t. the usual length), hence, well-founded. Hence, Theorem 15.6 has the following immediate corollary (to state it, we denote by G^h , for $h \geq 2$, the unique context-free grammar G' such that $S_{G'} = (S_G)^h$).

15.8. Corollary. *Let G be an ε -free context-free grammar. The following conditions are equivalent:*

- (1) S_G is $\mathcal{P}(\mathbf{T}^+)$ -univocal,
- (2) $S_G \text{runf}_{\mathcal{D} \cup \mathcal{E}_s}^* S_{G'}$, for some proper context-free grammar G' ,
- (3) the grammar G^h is proper for some $h \geq 1$.

For example, if $G = \langle u \rightarrow aub, u \rightarrow v, v \rightarrow av, v \rightarrow b \rangle$, the grammar G^2 is $\langle u \rightarrow aaubbb, u \rightarrow avb, u \rightarrow av, u \rightarrow b, v \rightarrow aav, v \rightarrow ab, v \rightarrow b \rangle$ and it is proper.

Note that the grammar $G' = \langle u = u. u + a \rangle$ has a unique solution in $\mathcal{P}(\mathbf{T}^+)$ (provided $a \in T$) but several solutions in $\mathcal{P}(\mathbf{T}^*)$: namely a^+ (the least one), a^* , and T'^* for all $T' \subseteq T$ such that $a \in T'$. Note also that G'^h is not proper since it contains the production rule $u \rightarrow u^{2^h}$ for all $h \geq 1$.

15.9. Example (strict context-free grammars). We now consider context-free grammars with ε -rules. Following Berstel [8], we say that $G = \langle N, T, P \rangle$ is *strict* if, for every rule $u \rightarrow m$ in P , either $m = \varepsilon$ or m contains a terminal symbol.

The T_m -magma \mathbf{T}^* is not well-founded since $\varepsilon.w = w$ so that $w \rightarrow w \rightarrow w \rightarrow \dots$. However, if G is strict, then \mathbf{T}^* is well-founded w.r.t. S_G because of the presence of a terminal symbol in each nonconstant monomial (actually, S_G is contracting w.r.t. the usual length of words). Hence, S_G has a unique solution in $\mathcal{P}(\mathbf{T}^*)$. We cannot apply Theorem 15.6. Nevertheless, a similar result can be independently established.

For every context-free grammar $G = \langle N, T, P \rangle$, we let $N_\varepsilon = \{u \in N \mid \varepsilon \in L(G, u)\}$. This set can be computed (see Section 16.6).

Let $N_0 \subseteq N_1 \subseteq \dots \subseteq N_i \subseteq \dots \subseteq N$ be the increasing sequence such that

$$N_0 = \emptyset,$$

$$N_{i+1} = N_i \cup \{u \in N \mid \text{for every production rule } u \rightarrow m \text{ in } P,$$

$$m \in N_i^* \cup (N \cup T)^*(N_i \cup T - N_\varepsilon)(N \cup T)^*\},$$

and $N_\infty = \bigcup \{N_i \mid i \geq 0\}$, $N' = N - N_\infty$. It is clear that N_∞ and N' can be computed.

Fact. For all u in N' , there exists a production rule $u \rightarrow m$ in P such that $m \in (N_\varepsilon \cup N')^* N' (N_\varepsilon \cup N')^*$.

Proof. Let h be the least integer such that $N_\infty = N_{h+1} = N_h$. Let $m \in (N \cup T)^* - (N_\varepsilon \cup N')^* N' (N_\varepsilon \cup N')^*$. Then either $m = \varepsilon$ or m contains a terminal symbol or $m \in N^+$ but m contains a nonterminal in $N - N' - N_\varepsilon$ (which is equal to $N_h - N_\varepsilon$) or $m \in (N_\varepsilon - N')^+ \subseteq N_h^+$. In all cases, $m \in N_h^* \cup (N \cup T)^*(N_h \cup T - N_\varepsilon)(N \cup T)^*$. Hence, if u is such that, for every production rule $u \rightarrow m$ in P , $m \notin (N_\varepsilon \cup N')^* N' (N_\varepsilon \cup N')^*$, then $u \in N_{h+1} = N_\infty$. \square

Note that G is strict iff $N_\infty = N_1$.

In the following proposition, we assume that T is large enough so that $T^* - (L(G, u_1) \cup \dots \cup L(G, u_n)) \neq \emptyset$.

15.10. Proposition. Let G be a context-free grammar. The following conditions are equivalent:

- (1) S_G is $\mathcal{P}(T^*)$ -univocal,
- (2) $N' = \emptyset$,
- (3) $S_G \text{ runf}_{\emptyset \cup \mathcal{E}_m}^* S_{G'}$, for some strict context-free grammar G' ,
- (4) G^h is strict for some $h \geq 1$.

Proof. (1) \Rightarrow (2): Let us assume that $N' \neq \emptyset$. Let w be a word which does not belong to $L(G, u_i)$, $i \in [n]$. Let $L = (L_1, \dots, L_n)$ be the n -tuple of languages such that:

$$L_i = \begin{cases} \{w, \varepsilon\} & \text{if } u_i \in N', \\ \{\varepsilon\} & \text{if } u_i \in N_\varepsilon - N', \\ \emptyset & \text{otherwise, i.e., if } u_i \in N - N' - N_\varepsilon. \end{cases}$$

We first prove that $L \subseteq S_G(L)$, i.e., that $L_i \subseteq p_i(L)$ (where $S_G = \langle u_i = p_i; i \in [n] \rangle$). This is clearly true if $u_i \in N - N' - N_\varepsilon$. If $u_i \in N_\varepsilon - N'$, there exists a production rule of the form $u_i \rightarrow m$ with m in N_ε^* , hence, $\varepsilon \in p_i(L)$ by the definition of L . If $u_i \in N'$, there exists a production rule of the form $u \rightarrow mu_j m'$ with $u_j \in N'$ and $m, m' \in (N_\varepsilon \cup N')^*$. Hence, $\varepsilon \in m(L)$, $\varepsilon \in m'(L)$, and $\{w, \varepsilon\} \subseteq m(L) \cdot \{w, \varepsilon\} \cdot m'(L)$. Hence, $\{w, \varepsilon\} \subseteq p_i(L)$ as was to be shown.

Hence, $S_G^i(L) \subseteq S_G^{i+1}(L)$ for all i and $\bigcup\{S_G^i(L) \mid i \geq 0\}$ is a solution of S_G which differs from the least one since at least one of its components contains w . Hence, S_G is not $\mathcal{P}(\mathbf{T}^*)$ -univocal.

(2) \Rightarrow (3): Let us define $d(G) = \mathbf{Card}(N_\infty - N_1)$ so that G is strict iff $d(G) = 0$ and $N' = \emptyset$. Let G be such that $N' = \emptyset$ and $d(G) \neq 0$. Let $u_j \in N_2 - N_1$. Let $G^{(1)}$ be the grammar such that $S_{G^{(1)}} = \langle u_i = p'_i; 1 \leq i \leq n \rangle$, where $S_G = \langle u_i = p_i; 1 \leq i \leq n \rangle$ and $p'_i = p_i$ if $i \neq j$, $p'_j = \mathbf{Pol}(p_j[p_i/u_i; u_i \in N_1])$. It is clear that $S_G \mathbf{runf}_{\mathcal{D} \cup \mathcal{E}_m} S_{G^{(1)}}$, that the subset $N_\infty^{(1)}$ of N , associated with $G^{(1)}$ as N_∞ is associated with G , is equal to N and that $d(G^{(1)}) < d(G)$. Hence, the transformation of G into $G^{(1)}$ can be applied to $G^{(1)}$ and repeated until a grammar $G^{(k)}$ is obtained such that $d(G^{(k)}) = 0$. Letting $G' = G^{(k)}$ one then has

$$S_G \mathbf{runf}_{\mathcal{D} \cup \mathcal{E}_m}^* S_{G'}$$

and G' is strict.

(3) \Rightarrow (1): $S_{G'}$ is $\mathcal{P}(\mathbf{T}^*)$ -univocal since G' is strict. And S_G is $\mathcal{P}(\mathbf{T}^*)$ -univocal since $S_G \approx_{\mathcal{E}_m}^p S_{G'}$.

(4) \Rightarrow (1): This is proven by a similar argument with the help of Proposition 8.2(1).

(2) \Rightarrow (4): Let h be the least integer such that $N_\infty = N_h$. We prove that G^h is strict. For every $i \in [n]$, $j \geq 1$, let $P_{i,j}$ be the set of words m such that $u_i \rightarrow m$ is a production rule of G^j . It is easy to prove that for $j, k \geq 1$, $P_{i,j+k}$ is the result of the (language) substitution of $P_{1,k}, \dots, P_{n,k}$ for u_1, \dots, u_n in $P_{i,j}$. We denote this by $P_{i,j+k} = P_{i,j}[P_{1,k}, \dots, P_{n,k}]$. Let us prove that, for all $i \in [n]$, $j \geq 1$,

$$u_i \in N_j \Rightarrow P_{i,j} \subseteq A, \tag{7}$$

where $A = \{\varepsilon\} \cup (N \cup T)^* T (N \cup T)^*$.

The proof is by induction on j . If $j = 1$, then (7) obviously holds. Let us prove (7) for $j + 1$ by assuming it to hold for j . Let $u_i \in N_{j+1}$. If $u_i \in N_j$, then $P_{i,j} \subseteq A$:

$$\begin{aligned} P_{i,j+1} &= P_{i,j}[P_{1,1}, \dots, P_{n,1}] \\ &\subseteq A[P_{1,1}, \dots, P_{n,1}] \\ &\subseteq A \quad (\text{by the definition of } A). \end{aligned}$$

Otherwise, let $u_i \in N_{j+1} - N_j$. For every m such that $u_i \rightarrow m$ is a production rule of P , either $m \in N_j^*$ and since $P_{i,j} \subseteq A$ for u_i in N_j :

$$\begin{aligned} m[P_{1,j}, \dots, P_{n,j}] &\subseteq (\bigcup\{P_{i,j} \mid u_i \in N_j\})^* \\ &\subseteq A^* = A, \end{aligned}$$

or $m \in (N \cup T)^* T (N \cup T)^*$ and clearly,

$$m[P_{1,j}, \dots, P_{n,j}] \subseteq A,$$

or $m \in (N \cup T)^*\{u_i\}(N \cup T)^*$ for some u_i in $N_j - N_\varepsilon$, whence $P_{i',j} \subseteq A - \{\varepsilon\}$ and then

$$m[P_{1,j}, \dots, P_{n,j}] \subseteq (N \cup T)^*(A - \{\varepsilon\})(N \cup T)^* \subseteq A.$$

This shows that $P_{i,j+1} = P_{i,1}[P_{1,j}, \dots, P_{n,j}] \subseteq A$. Hence, if $N = N_\infty$, $P_{i,h} \subseteq A$ for all i in $[n]$, i.e., G^h is strict. \square

16. Grammars on arbitrary magmas

Mezei and Wright have shown in [73] that context-free languages and finite-state languages are two instances of a same concept, that of an *equational set* defined with respect to two different algebraic structures equipping the set of words T^* (see Sections 11.4.1 and 11.4.2). This idea has not been developed very much and one of the purposes of this paper is to fill up this lack. Our results concerning polynomial systems and their least solutions contribute to this task. Further theoretical developments are presented in this section together with applications to attribute grammars and tree grammars.

16.1. Definition. A *grammar* is a pair $G = (S, \mathbf{M})$ consisting of a polynomial system S over some ranked alphabet F and an F -magma \mathbf{M} . If necessary, we shall precise that G is an \mathbf{M} -*grammar*. We shall also say in a loose way that S 'is' an \mathbf{M} -grammar.

Such a grammar is said to *define*, for every u in $\mathbf{Unk}(S)$, a subset of M , $L(G, u) = \{t_{\mathbf{M}} \mid t \in L(S, u)\}$. This set is also the component corresponding to u of the least solution of S in $\mathcal{P}(\mathbf{M})$, hence, is equational (see Section 13) with respect to the algebraic structure on M specified by \mathbf{M} , and every equational subset of M is of this form.

If $t \in L(S, u)$ and $m = t_{\mathbf{M}}$, then t is called a *grammatical denotation* of m . Note that $L(G, u) = \emptyset$ iff $L(S, u) = \emptyset$.

A context-free grammar G over the terminal alphabet T is nothing else than a T^* -grammar (see Section 11.4.2) and the notation $L(G, u)$ means the same thing in this definition and in the classical one.

Here is a simple example of a (word) grammar defining a non-context-free language.

16.2. Example. Let H be the ranked alphabet $T_m \cup \{s\}$ (see Section 11.4.2) and s is a new unary function symbol. Let \mathbf{M} be the H -magma consisting of T^* extended with the *squaring operation*

$$s_{\mathbf{M}}(w) = ww$$

for all w in T^* .

The M -grammar consisting of the system reduced to the equation $u = a + s(u)$ generates the non-context-free language $L = \{a^{2^n} \mid n \geq 0\}$ (more precisely, $L(S, u) = \{s^n(a) \mid n \geq 0\}$ and $L(S, u)_M = L$).

Other more complicated examples can be found in [21].

The notion of a grammar always incorporates that of a *structured description* of objects. And the structure of an object is represented by a tree, called the *derivation tree*. This classical concept easily extends to the present grammars.

16.1. Derivation trees

Let S be a polynomial system $\langle u_i = t_i; 1 \leq i \leq n \rangle$ such that $t_i = p_{i,1} + \dots + p_{i,n_i}$ for some $p_{i,j}$ in $M(F, U)$ with $U = \text{Unk}(S)$. If $t_i = \Omega$, then $n_i = 0$. Let us consider U as a set of sorts (cf. Section 9). We associate with S a U -sorted signature Q as follows:

$$Q = \{q_{i,j} \mid 1 \leq i \leq n, 1 \leq j \leq n_i\},$$

$$\sigma(q_{i,j}) = u_i, \quad \alpha(q_{i,j}) = u_{i_1} u_{i_2} \dots u_{i_k},$$

where u_{i_1}, \dots, u_{i_k} is the list of unknowns (of S) occurring in $p_{i,j}$ from left to right in this order, or, more precisely, $\alpha(q_{i,j}) = \text{Lvar}_U(p_{i,j})$, where Lvar_U is the mapping $M(F, U) \rightarrow U^*$ defined by

$$\begin{aligned} \text{Lvar}_U(p) &= \varepsilon \quad \text{if } p \in F_0, \\ \text{Lvar}_U(u) &= u \quad \text{if } u \in U, \\ \text{Lvar}_U(f(p_1, \dots, p_k)) &= \text{Lvar}_U(p_1) \dots \text{Lvar}_U(p_k). \end{aligned}$$

Let now θ be the mapping $M(Q) \rightarrow M(F)$ defined as follows (this is a second-order substitution [26]):

$$\begin{aligned} \theta(q_{i,j}) &= p_{i,j} \quad \text{if } \alpha(q_{i,j}) = \varepsilon, \text{ i.e., if } p_{i,j} \in M(F), \\ \theta(q_{i,j}(w_1, \dots, w_k)) &= \bar{p}_{i,j}[\theta(w_1)/x_1, \dots, \theta(w_k)/x_k], \end{aligned}$$

where $\bar{p}_{i,j}$ is the unique term in $M(F, X)$ such that (as in Definition 15.1)

$$\begin{aligned} p_{i,j} &= \bar{p}_{i,j}[u_{i_1}/x_1, \dots, u_{i_k}/x_k], \\ \text{Lvar}_X(\bar{p}_{i,j}) &= x_1 x_2 \dots x_k. \end{aligned}$$

16.3. Proposition. *For all u in U , $\theta(M(Q)_u) = L(S, u)$.*

Sketch of proof. One can prove that $\theta(w) \in L(S, \sigma(w))$ for all w in $M(Q)$ by induction on the structure of w . One can prove that every t in $L(S, u)$ is of the form $\theta(w)$ for some w in $M(Q)_u$ by induction on the length of a rewriting sequence $u \rightarrow_{\text{Dev}(S)}^* t$ (this result will be improved in Proposition 16.5). \square

Note as a corollary that $M(Q)_u \neq \emptyset$ iff $L(S, u) \neq \emptyset$.

If $w \in M(Q)_u$ and $m = \theta(w)_M$, we say that w is a *u -derivation tree of m with respect to G* (or of the grammatical denotation $\theta(w)$ of m). This allows us to define an

\mathbf{M} -grammar G as above as *nonambiguous* if, for all u in U , an element m of M has at most one u -derivation tree. The system S is defined as *nonambiguous* if, for all u , $\theta \upharpoonright M(Q)_u$ is injective and this is equivalent to saying that the grammar $(S, \mathbf{M}(F))$ is nonambiguous.

In the special case of finite-state automata considered as grammars (cf. Section 11.4.1), the canonical homomorphism $\mathbf{M}(T_u) \rightarrow \mathbf{T}^*$ is a bijection. Hence, roughly speaking, a word coincides with its denotation by a term in $M(T_u)$.

In the case of context-free grammars (cf. Section 11.4.2), \mathbf{T}^* is isomorphic to $\mathbf{M}(T_m)/\leftrightarrow_{\mathcal{E}_m}^*$, hence, a same word has several (actually, infinitely many) distinct denotations in $M(T_m)$. However, derivations are usually defined in $M(T_m, U)/\leftrightarrow_{\mathcal{E}_m}^*$ which is in bijection with $(T_m \cup U)^*$ and not in $M(T_m, U)$ (see Proposition 16.9 for general conditions insuring such a possibility).

Hence (and as in the case of finite state automata), there is no need for distinguishing between a word in $L(G, u)$ and its grammatical denotation. The need for such a distinction is clear in Example 16.2 in the case of IO-context-free tree languages examined in Section 16.2, or in the examples considered in [21].

We now examine the case where the derivation trees and the grammatical denotations coincide.

16.4. Definition. Let $G = (S, \mathbf{M})$ be a grammar as in Section 16.1. If S is uniform and if no symbol of F occurs in more than one monomial $p_{i,j}$, then Q is in bijection with a subset F' of F . This means that the mapping θ of Proposition 16.3 is a mere relabelling, hence, roughly speaking, this means that a derivation tree coincides with the corresponding grammatical denotation. If this is the case we shall say that S is an *abstract polynomial system* and that G is an *abstract grammar*.

Note nevertheless that Q is U -sorted and that F' is not. Hence, θ is a bijection $M(Q)_u \rightarrow L(S, u)$ and not $M(Q)_u \rightarrow M(F')$.

The following construction shows how an arbitrary polynomial system can be transformed into an abstract one. Let S be as in Section 16.1. Let \hat{S} be the polynomial system over Q , $\hat{S} = \langle u_i = \sum \{\hat{q}_{i,j} \mid 1 \leq j \leq n_i\}; i \in [n] \rangle$ such that for all i, j , $\hat{q}_{i,j} = q_{i,j}(u_{i_1}, \dots, u_{i_k})$, where $\alpha(q_{i,j}) = u_{i_1} u_{i_2} \dots u_{i_k}$. Let $\hat{\mathbf{M}}$ be the heterogeneous Q -magma with domains $M_u = M$ for all u in U and such that $q_{i,j\hat{\mathbf{M}}} = \bar{p}_{i,j\hat{\mathbf{M}}}$. Let $\hat{G} = (\hat{S}, \hat{\mathbf{M}})$. It follows from the definitions that $\hat{S}_{\hat{\mathbf{M}}} = S_{\mathbf{M}}$, hence, that $L(\hat{G}, u) = L(G, u)$ for all u in U , and it is clear that \hat{G} is an abstract grammar. This construction is just a generalization of the classical algebraic presentation of context-free grammars used in [20, 23, 27, 28, 54].

In the following proposition, θ is as in Section 16.1, with $\theta(u) = u$ for u in U .

16.5. Proposition. For all u in U , all t in $M(F)$, and for all derivations of the form

$$\gamma : u \xrightarrow{\text{Dev}(S)} t_1 \xrightarrow{\text{Dev}(S)} t_2 \xrightarrow{\text{Dev}(S)} \dots \xrightarrow{\text{Dev}(S)} t_k = t,$$

there exists a derivation

$$\hat{\gamma}: u \xrightarrow{\text{Dev}(\hat{S})} t'_1 \xrightarrow{\text{Dev}(\hat{S})} t'_2 \xrightarrow{\text{Dev}(\hat{S})} \cdots \xrightarrow{\text{Dev}(\hat{S})} t'_k = t'$$

such that $t' \in M(Q)_u$ and $\theta(t'_1) = t_1, \dots, \theta(t'_k) = t_k$. It is unique if $v \rightarrow_{\text{Dev}(S)} v$ for no v in $\text{Unk}(S)$.

The tree t' is called *the derivation tree of γ* .

Sketch of proof. If $v \rightarrow_{\text{Dev}(S)} v$ for no v in $\text{Unk}(S)$, the comparison of t_i and t_{i+1} defines in a unique way the pair of $\text{Dev}(S)$ which is used, and the occurrence where it is used in the transformation of t_i into t_{i+1} . This occurrence is the image of a unique occurrence in t'_i . Hence, t'_{i+1} exists in a unique way. \square

We now examine whether and how context-free tree grammars can be considered as grammars in our sense.

16.2. Context-free tree grammars: the IO case

Engelfriet and Schmidt [45] have shown that IO- and OI-context-free tree-languages can be characterized as components of the least solutions of certain regular systems in appropriate ω -complete magmas the domain of which is in both cases $\mathcal{P}(M(F, X))$. This construction uses derived alphabets exactly as the one of Section 9. A connection between recursive program schemes and IO- and OI-tree languages can be found in the fundamental paper of Damm [36].

In this section and the next one, we only provide examples, in order to illustrate the definitions of this chapter. The reader will find general definitions and proofs in [45].

Let G be the context-free tree grammar with terminal (ranked) alphabet $F = \{f, a\}$, nonterminal (ranked) alphabet $\Phi = \{\psi\}$, and a set of productions P as follows:

$$\begin{aligned} \psi(x_1, x_2) &\rightarrow a, & \psi(x_1, x_2) &\rightarrow x_2, \\ \psi(x_1, x_2) &\rightarrow f(x_1, x_1), & \psi(x_1, x_2) &\rightarrow \psi(\psi(x_2, x_1), x_1). \end{aligned}$$

Two different languages can be defined, namely,

$$\begin{aligned} L_{\text{OI}}(G, \psi(x_1, x_2)) &= \{t \in M(F, X_2) \mid \psi(x_1, x_2) \xrightarrow{P}^* t\}, \\ L_{\text{IO}}(G, \psi(x_1, x_2)) &= \{t \in M(F, X_2) \mid \psi(x_1, x_2) \xrightarrow{P, \text{IO}}^* t\}, \end{aligned}$$

where \rightarrow_P^* is the classical rewriting relation on $M(F \cup \Phi, X)$ associated with P and $\rightarrow_{P, \text{OI}}^*$ is the restriction of \rightarrow_P^* such that $\psi(t_1, t_2)$ rewrites into $s[t_1/x_1, t_2/x_2]$ for some s such that $\psi(x_1, x_2) \rightarrow s$ is a production rule in P only if t_1 and t_2 are both in $M(F, X)$.

Hence, $L_{\text{IO}}(G, \psi(x_1, x_2)) \subset L_{\text{OI}}(G, \psi(x_1, x_2))$ and the inclusion is strict since $f(a, x_1)$ belongs to $L_{\text{OI}}(G, \psi(x_1, x_2))$ but not to $L_{\text{IO}}(G, \psi(x_1, x_2))$.

Let H be the ranked alphabet $\{a, f, \pi_1, \pi_2, c\}$, where c is of arity three and the other symbols of arity zero. Let \mathbf{M} be the H -magma with domain $M = M(F, X_2)$ and such that

$$\begin{aligned} a_{\mathbf{M}} &= a, & f_{\mathbf{M}} &= f(x_1, x_2), \\ \pi_{1\mathbf{M}} &= x_1, & \pi_{2\mathbf{M}} &= x_2, \\ c_{\mathbf{M}}(t_0, t_1, t_2) &= t_0[t_1/x_1, t_2/x_2]. \end{aligned}$$

Let $\mathbf{P} = \mathcal{P}(\mathbf{M})$. Note that, by the definitions of Section 1,

$$c_{\mathbf{P}}(T_0, T_1, T_2) = T_0 \underset{\text{IO}}{[T_1/x_1, T_2/x_2]},$$

for $T_0, T_1, T_2 \in M(F, X_2)$.

Let now S be the regular system consisting of the unique equation

$$\psi = a + \pi_2 + c(f, \pi_1, \pi_1) + c(\psi, c(\psi, \pi_2, \pi_1), \pi_1).$$

It follows from [45, Theorem 4.9] that $L_{\text{IO}}(G, \psi(x_1, x_2))$ is the least solution of S in $\mathcal{P}(\mathbf{M})$ and that $L_{\text{IO}}(G, \psi(x_1, x_2)) = L(S, \psi)_{\mathbf{M}} = \{t_{\mathbf{M}} \mid t \in L(S, \psi)\}$. Note that $L(S, \psi) \subseteq M(H)$.

The mapping $t \mapsto t_{\mathbf{M}}: M(H) \rightarrow M(F, X_2)$ is called YIELD in [45] and so is the mapping $L \mapsto L_{\mathbf{M}}: \mathcal{P}(M(H)) \rightarrow \mathcal{P}(M(F, X_2))$ which is its extension to subsets of $M(H)$.

Of course, this result extends to arbitrary context-free tree grammars (and their IO-languages) provided one uses a derived alphabet (namely $\partial_0(F)$ introduced in Section 9) which also needs the introduction of sorts. This is formally done in [45]. And the IO-context-free tree languages can be characterized as equational subsets of $\mathcal{P}(\mathbf{M}(\partial_0(F)))$.

The above example is chosen so as to only use one sort (as was the example of Section 2.9).

As an example, we display some elements of $L(S, \psi)$, their values in $M(F, X_2)$, and their derivation trees (letting $Q = \{q_1, q_2, q_3, q_4\}$ in an obvious way).

$$\begin{array}{lll} q_2 & \pi_2 & x_2 \\ q_4(q_3, q_2) & c(c(f, \pi_1, \pi_1), c(\pi_2, \pi_2, \pi_1), \pi_1) & f(x_1, x_1) \\ q_4(q_4(q_2, q_2), q_1) & c(c(\pi_2, c(\pi_2, \pi_2, \pi_1), \pi_1), c(a, \pi_2, \pi_1), \pi_1) & a \end{array}$$

16.3. Context-free tree grammars: the OI case

An OI-context-free tree language can be characterized as the least solution of a regular system in an ω -complete magma with domain $\mathcal{P}(\mathbf{M}(F, X))$ but *which is not a powerset magma*.

Let G, S , and \mathbf{M} be as in Section 16.2. Let \mathbf{P}' be the H_+ -magma with domain $\mathbf{P}' = \mathcal{P}(\mathbf{M})$ and such that

$$\begin{aligned} g_{\mathbf{P}'} &= \{g_{\mathbf{M}}\} \quad \text{for all } g \in \{a, f, \pi_1, \pi_2\}, \\ \Omega_{\mathbf{P}'} &= \emptyset, \quad c_{\mathbf{P}'}(T_0, T_1, T_2) = T_0 \underset{\text{OI}}{[} T_1/x_1, T_2/x_2], \\ T_0 +_{\mathbf{P}'} T_1 &= T_0 \cup T_1, \end{aligned}$$

for $T_0, T_1, T_2 \subseteq M$. It can be shown that \mathbf{P}' is ω -complete with respect to the set inclusion as ordering. Hence, the equation S has a least solution in \mathbf{P}' and this least solution is precisely $L_{\text{OI}}(G, \psi(x_1, x_2))$. Once again this result extends to arbitrary OI-context-free tree grammars with help of the derived alphabet $\partial_0(F)$.

Let us note that \mathbf{P}' is not distributive since $c_{\mathbf{P}'}(T_0, T_1 \cup T'_1, T_2)$ properly includes $c_{\mathbf{P}'}(T_0, T_1, T_2) \cup c_{\mathbf{P}'}(T_0, T'_1, T_2)$ in general (take $T_0 = \{f(x_1, x_1)\}$). It follows that OI-context-free tree languages are not defined by grammars (in the sense of Definition 16.1) and that they are not equational subsets of $M(F, X)$ for any structure of $\partial_0(F)$ -magma on this set.

Hence, to summarize, IO-context-free tree grammars can be investigated in terms of polynomial systems solved in powerset magmas, whereas OI-context-free tree grammars cannot. Instead, they can be in the more general framework of regular systems solved in ω -complete magmas. (Actually, an intermediate class of structures lying between powerset magmas and ω -complete ones is used in [45] for the OI case).

Going back to the example, let us examine how the tree $f(a, x_1)$ which belongs to $L_{\text{OI}}(G, \psi(x_1, x_2)) - L_{\text{IO}}(G, \psi(x_1, x_2))$ comes in as an element of $L(S, \psi)_{\mathbf{P}'}$. We are obliged to go back to the infinite tree $T(S, \psi) \in M^\omega(H_+)$ which can be written in a loose, but hopefully clear way

$$\begin{aligned} T(S, \psi) &= a + \pi_2 + c(f, \pi_1, \pi_1) + c((a + \pi_2 + c(f, \pi_1, \pi_1) + \dots), \\ &\quad c((a + \pi_2 + c(f, \pi_1, \pi_1) + \dots), \pi_2, \pi_1), \pi_1). \end{aligned}$$

Since $c_{\mathbf{P}'}(T_0 \cup T'_0, T_1, T_2) = c_{\mathbf{P}'}(T_0, T_1, T_2) \cup c_{\mathbf{P}'}(T'_0, T_1, T_2)$, one gets

$$\begin{aligned} T(S, \psi)_{\mathbf{P}'} &= \dots \cup c(c(f, \pi_1, \pi_1), c((a + \pi_2 + \dots), \pi_2, \pi_1), \pi_1)_{\mathbf{P}'} \\ &= \dots \cup \{f(x_1, x_1)\} \underset{\text{OI}}{[} c(a, \pi_2, \pi_1)_{\mathbf{P}'} \cup c(\pi_2, \pi_2, \pi_1)_{\mathbf{P}'} \cup \dots / x_1, \{x_1\}/x_2] \\ &= \dots \cup \{f(x_1, x_1)\} [\{a, x_1, \dots\}/x_1, \{x_1\}/x_2] \ni f(a, x_1). \end{aligned}$$

Letting q_1, q_2, q_3, q_4 be as in Section 16.2, one can consider the tree $t = q_4(q_3, q_1 + q_2) \in M(Q_+)$ as a derivation tree of $f(a, x_1)$. However, t is also a derivation tree of $f(a, a)$, $f(x_1, x_1)$, and $f(x_1, a)$ since its value in \mathbf{P}' is $\{f(a, x_1), f(a, a), f(x_1, x_1), f(x_1, a)\}$. This idea will be developed in a forthcoming paper.

16.4. Derivation sequences

Let $G = (S, \mathbf{M})$ be a grammar. It follows from the results of Section 13 that $L(G, u) = L(S, u)_{\mathbf{M}} = \{t_{\mathbf{M}} \mid u \rightarrow_{\text{Dev}(S)}^* t, t \in M(F)\}$. In other words, an element m of

$L(G, u)$ can be defined in two steps, the first step consists in producing a grammatical denotation t and the second one in evaluating t into $m = t_{\mathbf{M}}$.

Let us now assume that $\mathbf{M} \in \mathcal{V}(\mathcal{E})$ for some set of equations \mathcal{E} . It is a natural idea to interleave derivation steps (i.e., $\rightarrow_{\text{Dev}(S)}$) with rewriting steps according to \mathcal{E} (i.e., with $\leftrightarrow_{\mathcal{E}}$). In fact, such an interleaving is done in the usual situation of context-free grammars where one rewrites $\alpha u \beta$ into $\alpha \varepsilon \beta$ if there exists an ε -rule $u \rightarrow \varepsilon$. This corresponds to a rewriting of $\alpha u \beta$ into $\alpha \varepsilon \beta$ followed by a rewriting of $\alpha \varepsilon \beta$ into $\alpha \beta$, corresponding to a use of the equation $\varepsilon.x = x$. (Actually, the derivations of context-free grammars will be more precisely described by Proposition 16.9.)

For every (oriented) rewriting system $R \subseteq M(F, X) \times M(F, X)$, we let $L(S, R, u) = \{t \in M(F) \mid u \rightarrow_{\text{Dev}(S) \cup R}^* t\}$ and we say that t is obtained by an R -derivation. It is clear that if $R \subseteq \leftrightarrow_{\mathcal{E}}^*$, $L(G, u) \subseteq L(S, R, u)_{\mathbf{M}}$, but the equality does not necessarily hold. In Example 16.2 it suffices to take $R = \{(s(x), x.x)\}$ and then to consider the R -derivation

$$u \xrightarrow[\text{Dev}(S)]{} s(u) \xrightarrow[R]{} u.u \xrightarrow[\text{Dev}(S)]{}^* a.s(a),$$

which yields a^3 which is not in $L(G, u)$. The difficulty comes from the nonlinearity of R .

We say that the R -derivations are *correct* for a grammar $G = (S, \mathbf{M})$ if $L(G, u) = L(S, R, u)_{\mathbf{M}}$ for all u in $\text{Unk}(S)$.

16.6. Proposition. *Let \mathbf{M} be an F -magma and R be a rewriting system $\subseteq M(F, X) \times M(F, X)$ such that $\mathbf{M} \in \mathcal{V}(R)$.*

(1) *If R is right-linear and $\text{Var}_X(t) \subseteq \text{Var}_X(t')$ for all (t, t') in R , then the R -derivations are correct for every \mathbf{M} -grammar.*

(2) *If R is right-linear, then the R -derivations are correct for every grammar (S, \mathbf{M}) such that $L(S, u) \neq \emptyset$ for all u in $\text{Unk}(S)$.*

Proof. (1) Let $u \rightarrow_{\text{Dev}(S) \cup R}^* t$ be an R -derivation. By Lemma 1.7 there exists a t' such that $u \rightarrow_{\text{Dev}(S)}^* t' \xrightarrow[R]{}^* t$. By the second condition on R , $t' \in M(F)$, hence, $t'_{\mathbf{M}} \in L(G, u)$. Since $\mathbf{M} \in \mathcal{V}(R)$, $t_{\mathbf{M}} = t'_{\mathbf{M}}$. Hence, $t_{\mathbf{M}} \in L(G, u)$. This proves that $L(S, R, u)_{\mathbf{M}} \subseteq L(G, u)$, hence, that the equality holds.

(2) As in (1), there exists a t' in $M(F, \text{Unk}(S))$, but we cannot conclude that $t' \in M(F)$. Let s_i be an element of $L(S, u_i)$ for each u_i in $\text{Unk}(S)$. Then $t' \xrightarrow[\text{Dev}(S)]{}^* t'[s_1/u_1, \dots, s_n/u_n]$. Hence, $t'_{\mathbf{M}}(s_{1\mathbf{M}}, \dots, s_{n\mathbf{M}}) \in L(G, u)$. Since $t' \xrightarrow[R]{}^* t$ and $\mathbf{M} \in \mathcal{V}(R)$, $t'_{\mathbf{M}}(s_{1\mathbf{M}}, \dots, s_{n\mathbf{M}}) = t_{\mathbf{M}}(s_{1\mathbf{M}}, \dots, s_{n\mathbf{M}}) = t_{\mathbf{M}}$. Hence, $t_{\mathbf{M}} \in L(G, u)$ and this proves that $L(S, R, u)_{\mathbf{M}} = L(G, u)$. \square

16.5. Derivation sequences in $M(F, U) / \leftrightarrow_{\mathcal{E}}^*$

An immediate consequence of Proposition 16.6 is that if \mathcal{E} is linear and balanced, the $(\mathcal{E} \cup \mathcal{E})^{-1}$ -derivations are correct for the \mathbf{M} -grammars such that $\mathbf{M} \in \mathcal{V}(\mathcal{E})$ and Lemma 1.6 yields the following fact.

16.7. Fact. For all s, t, t' in $M(F, U)$, if $s \leftrightarrow_{\mathcal{E}}^* t \rightarrow_{\text{Dev}(S)} t'$, there exists an s' such that $s \rightarrow_{\text{Dev}(S)} s' \leftrightarrow_{\mathcal{E}}^* t'$.

We can define a relation $\Rightarrow_{\text{Dev}(S)}$ on $M(F, U)/\leftrightarrow_{\mathcal{E}}^*$ by

$$[t]_{\mathcal{E}} \xrightarrow[\text{Dev}(S)]{\Rightarrow} [t']_{\mathcal{E}} \text{ iff } t \xrightarrow[\text{Dev}(S)]{\rightarrow} t'' \text{ for some } t'' \text{ in } M(F, U) \text{ such that } t' \leftrightarrow_{\mathcal{E}}^* t''$$

iff (by Fact 16.7) for every s in $[t]_{\mathcal{E}}$

$$\text{there exists an } s' \text{ such that } s \xrightarrow[\text{Dev}(S)]{\rightarrow} s' \leftrightarrow_{\mathcal{E}}^* t'.$$

The following fact is an immediate consequence of this definition.

16.8. Fact. Let $\alpha_1, \dots, \alpha_k \in M(F, U)/\leftrightarrow_{\mathcal{E}}^*$ and $t_1 \in \alpha_1$. Then $\alpha_1 \Rightarrow_{\text{Dev}(S)} \alpha_2 \Rightarrow_{\text{Dev}(S)} \dots \Rightarrow_{\text{Dev}(S)} \alpha_k$ iff there exist $t_2 \in \alpha_2, \dots, t_k \in \alpha_k$ such that $t_1 \rightarrow_{\text{Dev}(S)} t_2 \rightarrow_{\text{Dev}(S)} t_3 \rightarrow_{\text{Dev}(S)} \dots \rightarrow_{\text{Dev}(S)} t_k$.

Since if $t, t' \in M(F, U)$ and $t \leftrightarrow_{\mathcal{E}}^* t'$, $t \in M(F)$ iff $t' \in M(F)$, one can define:

$$L_{\mathcal{E}}(S, u) = \left\{ \alpha \mid \alpha \in M(F)/\leftrightarrow_{\mathcal{E}}^*, [u] \xrightarrow[\text{Dev}(S)]{\rightarrow} \alpha \right\}.$$

If $\mathbf{M} \in \mathcal{V}(\mathcal{E})$ and h denotes the unique homomorphism: $M(F)/\leftrightarrow_{\mathcal{E}}^* \rightarrow \mathbf{M}$, the following proposition holds.

16.9. Proposition. If \mathcal{E} is linear and balanced, if $\mathbf{M} \in \mathcal{V}(\mathcal{E})$ and S is a polynomial system, then

- (1) $L_{\mathcal{E}}(S, u) = [L(S, u)]_{\mathcal{E}}$ for all $u \in \text{Unk}(S)$;
- (2) $L(G, u) = h(L_{\mathcal{E}}(S, u))$.

Proof. Part (1) is an immediate consequence of Fact 16.8.

Part (2) follows from part (1). \square

This result is especially interesting if one knows syntactical objects playing the role of canonical representatives of the equivalence classes of $M(F, U)$ with respect to $\leftrightarrow_{\mathcal{E}}^*$. And one possible situation is when $\leftrightarrow_{\mathcal{E}}^*$ is equal to \leftrightarrow_R^* for some Noetherian and confluent rewriting system R . In this latter case, $\Rightarrow_{\text{Dev}(S)}$ can be defined as a rewriting relation on the set of R -normal forms of terms in $M(F, U)$. And this is the case for context-free grammars (with $\mathcal{E} = \mathcal{E}_m$ defined in Section 11.4.2).

Another example will be given later in Example 16.11.

16.10. Remark. In Fact 16.8 and if $t_1 \in U$, any derivation tree of the derivation sequence $t_1 \rightarrow_{\text{Dev}(S)} t_2 \rightarrow_{\text{Dev}(S)} \dots \rightarrow_{\text{Dev}(S)} t_k$ can be considered as a derivation tree

of the sequence $[t_1] \Rightarrow_{\text{Dev}(S)} [t_2] \Rightarrow_{\text{Dev}(S)} \cdots \Rightarrow_{\text{Dev}(S)} [t_k]$. But even if $u \rightarrow_{\text{Dev}(S)} u$ for no u in $\text{Unk}(S)$, there may exist several derivation trees.

Take for example the context-free grammar $G = \langle u \rightarrow uu, u \rightarrow a \rangle$ with Q consisting of q (of arity two) and q' (of arity zero). Then the derivation $u \rightarrow uu \rightarrow uuu \rightarrow auu \rightarrow aau \rightarrow aaa$ has the two derivation trees $q(q', q(q', q'))$ and $q(q(q', q'), q')$.

16.11. Example. The nondeterministic, two-tape automata introduced by Elgot and Mezei [43] can be defined as nondeterministic transition graphs with a set of initial nodes, a set of final nodes, and arrows labelled by pairs of words (w_1, w_2) on some alphabet T (the input alphabet). Such an automaton A defines a subset $L(A)$ of $T^* \times T^*$.

We shall assume that T is partitioned into $T_1 \cup T_2$ and that $w_1 \in T_1^*$ and $w_2 \in T_2^*$ for every pair (w_1, w_2) so that $L(A) \subseteq T_1^* \times T_2^*$. Let $F = T \cup \{e\}$ with $F_0 = \{e\}$, $F_1 = T$ and let \mathcal{E} be the set of all equations of the form $a(b(x)) = b(a(x))$ for a in T_1 and b in T_2 . Let \mathbf{M} be the F -magma with domain $T_1^* \times T_2^*$ and operations

$$a_{\mathbf{M}}((w_1, w_2)) = (w_1 a, w_2) \quad \text{if } a \in T_1,$$

$$b_{\mathbf{M}}((w_1, w_2)) = (w_1, w_2 b) \quad \text{if } b \in T_2,$$

$$e_{\mathbf{M}} = (\varepsilon, \varepsilon).$$

It is clear that $\mathbf{M} \in \mathcal{V}(\mathcal{E})$ and, moreover, that the canonical homomorphism $\mathbf{M}(F)/\leftrightarrow_{\mathcal{E}}^* \rightarrow \mathbf{M}$ is an isomorphism. By replacing in A every label (w_1, w_2) by $w_1 w_2$, one defines a finite-state, one-tape automaton \bar{A} such that $L(A) = [L(\bar{A})]_{\mathcal{E}}$ (we identify $M(F)$ with T^* and $M(F)/\leftrightarrow_{\mathcal{E}}^*$ with $T_1^* \times T_2^*$). And this allows to characterize the subsets of $T_1^* \times T_2^*$ definable by nondeterministic, two-tape automata as the equational subsets of $T_1^* \times T_2^*$ (w.r.t. the algebraic structure defined by \mathbf{M}).

An \mathbf{M} -grammar G can be associated with every automaton A (cf. Section 11.4.2, we omit the technical construction) and since \mathcal{E} is linear and balanced, the derivation sequences of G can be defined in $M(F \cup U)/\leftrightarrow_{\mathcal{E}}^*$. Note that $M(F \cup U)/\leftrightarrow_{\mathcal{E}}^*$ is in an obvious bijection with

$$(T_1^* \times T_2^* \times U) \cup (T_1^* \times T_2^*),$$

i.e., with the set of *configurations* of A since U is in bijection with the set of states of A . And the derivation sequences of G in $M(F \cup U)/\leftrightarrow_{\mathcal{E}}^*$ correspond to the computation sequences of A , defined as sequences of configurations in a usual way.

We now present in a unified way a family of algorithms on grammars called *iterative algorithms* which amount to solving by straightforward iteration the underlying regular systems in a magma which is finite or has a property insuring termination.

16.6. Iterative algorithms

Let $G = (S, \mathbf{M})$ be a grammar. Let A be a finite set and $h: M \rightarrow A$ be a mapping. For every u in U the set $h(L(G, u))$ is finite. Hence, one may wish to compute it in some effective way. The *iterative algorithms* presented below (at a theoretical level) allow to do this.

16.12. Algorithm. Let us assume that, for every $k \geq 0$, every f in F_k , one can define a computable mapping $f_A: A^k \rightarrow A$, hence, an F -magma \mathbf{A} with domain A , in such a way that h is a homomorphism $\mathbf{M} \rightarrow \mathbf{A}$. It then follows from Proposition 13.1 that $h(L(G, u)) = L(G', u)$, where G' is the grammar (S, \mathbf{A}) .

Since A is finite the increasing sequence $S_{\mathcal{P}(A)}^i(\emptyset^n)$ stabilizes after finitely many iterations, i.e., $\mu\text{-Psol}_{\mathbf{A}}(S) = S_{\mathcal{P}(A)}^{i_0}(\emptyset^n)$, where i_0 is the first i such that $S_{\mathcal{P}(A)}^{i+1}(\emptyset^n) = S_{\mathcal{P}(A)}^i(\emptyset^n)$. Since the f_A 's are computable, this sequence and i_0 are computable. Whence the results since $\mu\text{-Psol}_{\mathbf{A}}(S) = (h(L(G, u_1)), \dots, h(L(G, u_n)))$.

We sketch an example concerning context-free grammars. Let $\mathbf{M} = T^*$, $A = \{0, 1\}$ and $h: T^* \rightarrow A$ be such that $h(\varepsilon) = 0$, $h(u) = 1$ if $u \in T^+$. We make A into a monoid \mathbf{A} by letting \cdot be the Boolean 'and'. If G is a context-free grammar (S, \mathbf{M}) , one can compute $h(L(G, u))$ by the above method which gives us

$$\begin{aligned} L(G, u) \neq \emptyset &\text{ iff } h(L(G, u)) \neq \emptyset, \\ \varepsilon \in L(G, u) &\text{ iff } 0 \in h(L(G, u)). \end{aligned}$$

This is just a reformulation of the classical algorithms for deciding whether $L(G, u) = \emptyset$ and whether $L(G, u)$ contains the empty word. Here the two things can be done simultaneously.

Another example concerning IO-context-free tree languages will be given later (see Section 16.7).

We now present an improvement of Algorithm 16.12.

16.13. Algorithm. Let G , A , and h be as before. In some cases, it is not possible to define an F -magma structure on A such that h is a homomorphism because A is too small. A possible remedy to this situation consists in defining a finite set B and two mappings $h': M \rightarrow B$ and $k: B \rightarrow A$ such that $h = k \circ h'$ and k is computable. If Algorithm 16.12 is applicable to B and h' in place of A and h , then we can compute $h(L(G, u))$ since $h(L(G, u)) = k(h'(L(G, u))) = k(L(G', u))$, where $G' = (S, \mathbf{B})$.

A slight variant of this algorithm (or of the first one) consists in applying it to the grammar \hat{G} constructed in Definition 16.4 rather than to G .

Another extension concerns sorted systems. In this case, one must use families $(A_s)_{s \in \mathcal{S}}$, $(h_s)_{s \in \mathcal{S}}$, $(B_s)_{s \in \mathcal{S}}$, etc., where \mathcal{S} is the set of sorts. This extension is straightforward and we need not do it formally.

As an illustration, we shall reformulate the noncircularity test for attribute grammars as an instance of Algorithm 16.13 (see Section 16.8). However, we first consider a third algorithm dealing with a slightly different situation (which includes actually the one of Algorithm 16.12).

16.14. Algorithm. Let S be a regular system over F , let \mathbf{M} be an ω -complete F -magma, h be a mapping $\mathbf{M} \rightarrow A$, where A is some countable set. Without loss of generality, we can assume that A is a subset of \mathbb{N} .

The problem is to compute $(h(m_1), \dots, h(m_n))$, where $(m_1, \dots, m_n) = \mu\text{-Sol}_{\mathbf{M}}(S)$. For doing this it suffices to define the following:

- an ordering \leq_A on A such that $\perp_A = h(\perp_{\mathbf{M}}) \leq_A a$ for all a in A and A has no infinite strictly increasing chain,
- computable functions $f_A: A^{\rho(f)} \rightarrow A$ such that $\mathbf{A} = \langle A, \leq_A, \perp_A, \langle f_A \rangle_{f \in F} \rangle$ is an ω -complete F -magma and $h: \mathbf{M} \rightarrow \mathbf{A}$ is an ω -continuous homomorphism.

If \mathbf{A} has been so defined, then Lemma 5.3 shows that $(h(m_1), \dots, h(m_n)) = \mu\text{-Sol}_{\mathbf{A}}(S)$. Since A has no strictly increasing chains, the increasing sequence $S_{\mathbf{A}}^i(\perp_{\mathbf{A}}^n)$ is constant beyond some finite i_0 and $S_{\mathbf{A}}^{i_0}(\perp_{\mathbf{A}}^n) = \mu\text{-Sol}_{\mathbf{A}}(S)$. Since the f_A 's are computable so are this sequence and $\mu\text{-Sol}_{\mathbf{A}}(S)$.

As before, if A is too small, one may replace it by some larger set B . And the extension to the many-sorted case is straightforward.

A good example for this algorithm is the determination of the length of a shortest word of a context-free language. For this purpose one uses $A = \mathbb{N} \cup \{\infty\}$ ordered in the following way:

$$\infty \leq_A a,$$

$$a \leq_A b \text{ iff } b \leq a,$$

for all $a, b \in \mathbb{N}$. The appropriate mapping is $h: \mathcal{P}(T^*) \rightarrow A$ such that

$$h(\emptyset) = \infty,$$

$$h(L) = \mathbf{Min}\{|w| \mid w \in L\} \quad \text{if } L \neq \emptyset.$$

The definitions of $+_{\mathbf{A}}$ and $\cdot_{\mathbf{A}}$ follow from the remarks that

$$h(L_1 \cup L_2) = \mathbf{Min}\{h(L_1), h(L_2)\}, \quad h(L_1 \cdot L_2) = h(L_1) + (L_2)$$

(with $\infty + a = a + \infty$ for all a in A)

$$h(\{\varepsilon\}) = 0, \quad h(\{a\}) = 1.$$

Hence, $+_{\mathbf{A}}$ is defined as \mathbf{Min} and $\cdot_{\mathbf{A}}$ as the addition (on A).

All the verifications are left to the reader. Note that the computation of $\mu\text{-Sol}_{\mathbf{A}}(S_G)$ also allows us to decide whether $L(G, u) = \emptyset$ and whether $L(G, u)$ contains the empty word.

16.7. The occurrences of variables in IO-context-free tree languages

This section is the continuation of Section 16.2. We fix $X = \{x_1, x_2, \dots, x_n, \dots\}$ (with $X_k = \{x_1, \dots, x_k\}$) as a set of variables and for $t \in M(F, X)$, we let $\mathbf{Var}(t) = \mathbf{Var}_X(t)$. For $T \subseteq M(F, X)$ we let $\mathbf{VAR}(T) = \{\mathbf{Var}(t) \mid t \in T\}$. For every subset T of $M(F, X_k)$ the set $\mathbf{VAR}(T)$ is a finite set of finite sets that one may wish to compute from a finitary definition of T by a grammar or an automaton. Let us assume here that T is an IO-context-free tree language ($\subseteq M(F, X_k)$). It can be defined as $L(G, \psi)$ for some M-grammar G , where \mathbf{M} is as in Section 16.2 (or is a $\partial_0(F)$ -magma in the general case).

The following facts are clear:

$$\mathbf{Var}(x) = \{x\} \quad \text{if } x \in X,$$

$$\mathbf{Var}(f(t_1, \dots, t_k)) = \mathbf{Var}(t_1) \cup \dots \cup \mathbf{Var}(t_k),$$

$$\begin{aligned} \mathbf{Var}(t[t_1/x_1, \dots, t_k/x_k]) &= \bigcup \{\mathbf{Var}(t_i)/x_i \in \mathbf{Var}(t)\} \quad (\text{if } t \in M(F, X_k)) \\ &= \gamma_{k,n}(\mathbf{Var}(t), \mathbf{Var}(t_1), \dots, \mathbf{Var}(t_n)), \end{aligned}$$

where $\gamma_{k,n}$ is such that if $\alpha \subseteq X_k, \beta_1, \dots, \beta_k \subseteq X_n$,

$$\gamma_{k,n}(\alpha, \beta_1, \dots, \beta_k) = \bigcup \{\beta_i \mid x_i \in \alpha\}.$$

Hence, if $c_{k,n}$ is the operation symbol such that $c_{k,n}^{\mathbf{M}}(t, t_1, \dots, t_k) = t[t_1/x_1, \dots, t_k/x_k]$ for $t \in M(F, X_k), t_1, \dots, t_k \in M(F, X_n)$, then the operations on \mathbf{A} will be defined by

$$\pi_{i\mathbf{A}} = \{x_i\}, \quad a_{\mathbf{A}} = \emptyset \quad \text{if } a \in F_0,$$

$$f_{\mathbf{A}} = \{x_1, \dots, x_k\} \quad \text{if } f \in F_k,$$

$$c_{k,n\mathbf{A}} = \gamma_{k,n}$$

Hence, $\mathbf{VAR}(L_{\text{IO}}(G, \psi(x_1, \dots, x_n))) = L((S_G, \mathbf{A}), \psi)$, where S_G is the polynomial system associated with the grammar G as explained in Section 16.2 (and formally done in [45]).

16.8. The noncircularity test for attribute grammars

Rather than the noncircularity of usual attribute grammars, we shall consider a more general property, the noncircularity of *attribute dependency schemes*. These objects have been introduced in [27]. Every attribute grammar has an underlying attribute dependency scheme which is noncircular iff the attribute grammar is. Below, we shall redefine attribute dependency schemes. They are so close to attribute grammars that the reader will not have any difficulty to make the correspondence, especially if (s)he knows [20, 23, 28].

Let \mathbf{Attr} be a finite set of symbols called *attributes*. Let $\mathcal{A} = \mathcal{P}(\mathbf{Attr})$. If $\alpha_0, \dots, \alpha_k \in \mathcal{A}$, we denote by $H_{(\alpha_1 \dots \alpha_k \alpha_0)}$ the set of all (isomorphism classes of) finite graphs with $\mathbf{Card}(\alpha_0) + \dots + \mathbf{Card}(\alpha_k)$ distinguished vertices called *sources*. To be precise,

these graphs are of the form $g = \langle V, E, s_0, \dots, s_k \rangle$, where V is the finite set of vertices, E is the finite set of edges, and s_i is a mapping $\alpha_i \rightarrow V$ such that, for all i, j, a, b , $s_i(a) = s_j(b)$ iff $i = j$ and $a = b$. We also denote by H_α the set $H_{(\varepsilon, \alpha)}$.

If $g \in H_{(\alpha_1, \dots, \alpha_k, \alpha_0)}$, $g_1 \in H_{\alpha_1}, \dots, g_k \in H_{\alpha_k}$, we denote by $g[g_1, \dots, g_k]$ the graph $\langle V', E', s' \rangle$ in H_α defined as follows. By taking suitable copies of g_1, \dots, g_k , one can assume that

$$\begin{aligned} g_i &= \langle V_i, E_i, s_i \rangle, \quad i \in [k], \\ V_i \cap V_j &= \emptyset \quad \text{if } 1 \leq i < j \leq k, \\ g &= \langle V, E, s, t_1, \dots, t_k \rangle, \\ s_i(a) &= t_i(a) \quad \text{for all } a \in \alpha_i, \text{ all } i \in [k], \\ V \cap V_i &= \{s_i(a) \mid a \in \alpha_i\} \quad \text{for all } i \in [k]. \end{aligned}$$

And then one takes $V' = V \cup V_1 \cup \dots \cup V_k$, $E' = E \cup E_1 \cup \dots \cup E_k$ and $s' = s$.

An *attribute dependency scheme* is an object $T = \langle N, P, \text{Attr}, D \rangle$ consisting of

- a finite set of sorts $N = \{u_1, \dots, u_n\}$,
- a finite N -signature P ,
- a finite set of attributes Attr and a mapping θ associating with every u in N a subset $\theta(u)$ of Attr , a mapping D associating with p in P of arity $u^{(1)} \dots u^{(k)}$ and of sort u (with $u^{(1)}, \dots, u^{(k)}, u \in N$), a graph $D(p)$ in $H_{(\theta(u^{(1)}), \dots, \theta(u^{(k)}), \theta(u))}$.

With T as above we associate a P -magma $\mathbf{T} = \langle \langle T_u \rangle_{u \in N}, \langle p_{\mathbf{T}} \rangle_{p \in P} \rangle$, where

- $T_u = H_{\theta(u)}$,
- if $p \in P_{(u^{(1)} \dots u^{(k)}, u)}$ and $g_i \in H_{\theta(u^{(i)})}$ for all $i = 1, \dots, k$, then $p_{\mathbf{T}}(g_1, \dots, g_k) = D(p)[g_1, \dots, g_k]$.

Hence, there corresponds to every t in $M(P)_u$ a graph $t_{\mathbf{T}}$ in $H_{\theta(u)}$.

Letting S be the system $\langle u = \sum \{p(u^{(1)}, \dots, u^{(k)}) \mid p \in P, \sigma(p) = u, \alpha(p) = u^{(1)} \dots u^{(k)}\}; u \in N \rangle$, then $G = (S, \mathbf{T})$ is a grammar which defines for every u in N a set of graphs $L(G, u) \subseteq H_{\theta(u)}$.

The *noncircularity problem* consists in deciding whether there exists in $L(G, u)$ a graph having a cycle. To formulate this problem in the terms of Section 16.6, we define, for all u in N , $A_u = \{0, 1\}$ and $h_u: H_{\theta(u)} \rightarrow A_u$ by letting $h_u(g) = 0$ if g has no cycle and $h_u(g) = 1$ if g has a cycle. It is not possible (except in some very special cases) to define $p_{\mathbf{A}}$ for $p \in P$ such that the family of mappings $h = (h_u)_{u \in N}$ defines a homomorphism $\mathbf{T} \rightarrow \mathbf{A}$.

Algorithm 16.13 of Section 16.6 suitably extended to a system with sorts is applicable if one defines

$$\begin{aligned} B_u &= A_u \times \mathcal{P}(\theta(u) \times \theta(u)), \\ h'_u(g) &= (h_u(g), (g^+)_{\theta(u)}). \end{aligned}$$

By g^+ we mean the transitive closure of g and by $(g^+)_{\theta(u)}$ the restriction of g^+ to the set of sources of g (this set is in bijection with $\theta(u)$). Since the multiplicity of edges from a vertex a to a vertex b does not matter here (only the existence

matters), we can consider $(g^+)_{\theta(u)}$ as a binary relation on $\theta(u)$, i.e., as a subset of $\mathcal{P}(\theta(u) \times \theta(u))$.

We need only define $p_{\mathbf{B}}: B_{u^{(1)}} \times \cdots \times B_{u^{(k)}} \rightarrow B_{u^{(0)}}$ (for p in $P_{(u^{(1)}, \dots, u^{(k)}, u^{(0)})}$) such that, for all g_1 in H_{α_1}, \dots, g_k in H_{α_k} (where $\alpha_i = \theta(u^{(i)})$, $i = 0, \dots, k$),

$$p_{\mathbf{B}}(h'_{u^{(1)}}(g_1), \dots, h'_{u^{(k)}}(g_k)) = h'_{u^{(0)}}(p_{\mathbf{T}}(g_1, \dots, g_k)).$$

It suffices to take

$$p_{\mathbf{B}}((j_1, r_1), \dots, (j_k, r_k)) = (j_0, r_0)$$

with

$$r_0 = ((D(p)[r_1, \dots, r_k])^+)_{\alpha_0}$$

and

$$j_0 = \begin{cases} 1 & \text{if } D(p)[r_1, \dots, r_k] \text{ has a cycle or } \mathbf{Max}\{j_1, \dots, j_k\} = 1, \\ 0 & \text{otherwise.} \end{cases}$$

The proof that h' is a homomorphism reduces to the mere remark that if $p \in P_{(u^{(1)}, \dots, u^{(k)}, u^{(0)})}$ and, for all $i = 1, \dots, k$, g_i is a graph in H_{α_i} , then:

- (1) $D(p)[g_1, \dots, g_k]$ has a cycle iff $D(p)[(g_1^+)_{\alpha_1}, \dots, (g_k^+)_{\alpha_k}]$ has one,
- (2) $(D(p)[g_1, \dots, g_k])^+_{\alpha} = ((D(p)[(g_1^+)_{\alpha_1}, \dots, (g_k^+)_{\alpha_k}])^+_{\alpha}$,

which is straightforward to prove by going back to the definitions.

The iterative algorithm that one deduces from these remarks in the case of a attribute dependency scheme associated with an attribute grammar is *exactly the classical* noncircularity algorithm (see [40] for this algorithm and its possible improvements). We just wanted to show its similarity with the classical iterative algorithms on grammars as the ones taken in examples in Section 16.6.

17. Applications to context-free grammars

In this chapter we formulate some classical transformations of context-free grammars in terms of the $\sim_{\mathcal{D} \cup \mathcal{E}_m}$ -correct basic transformations used in Section 14. This formulation establishes their validity as an immediate corollary of the $\sim_{\mathcal{D} \cup \mathcal{E}_m}$ -correctness of the basic transformations. In classical books on context-free languages (for instance [57]) their validity is separately proved for each of them by inductive arguments on the length of derivations.

Let us recall from Section 11.4.2 that there is a one-to-one correspondence between context-free grammars and polynomial systems which associates with $G = \langle N, T, P \rangle$ (terminal alphabet, nonterminal alphabet, set of production rules) a polynomial system S_G over T_m with set of unknowns N .

17.1. Deletion of nonterminals which define no word

If $G = \langle N, T, P \rangle$ and $N_+ = \{u \in N \mid L(G, u) \neq \emptyset\}$, then one defines $G_+ = \langle N_+, T, P_+ \rangle$ by letting P_+ be the set of production rules $u \rightarrow m$ in P such that $u \in N_+$ and

$m \in (N_+ \cup T)^*$. This construction is effective since N_+ can be computed (see Section 16.6).

It follows from Definitions 14.3 and 16.1 that $N_+ = \mathbf{Unk}^+(S_G)$ and that $S_{G_+} = \mathbf{Red}_\sim(S_G) \upharpoonright N_+$. Hence, by Proposition 14.4,

$$S_{G_+} \subseteq \mathbf{Red}_\sim(S_G) \mathbf{redef}_{\emptyset} S_G$$

and this establishes that

$$S_{G_+} \sim_{N_+, \emptyset \cup \mathcal{E}_m} S_G,$$

whence,

$$L(G_+, u) = L(G, u) \quad \text{for all } u \text{ in } N_+.$$

17.2. Deletion of useless nonterminals

We first give a few definitions. If $G = \langle N, T, P \rangle$ and $G' = \langle N', T, P' \rangle$ are two grammars such that $N' \subseteq N$ and $P' \subseteq P$, one says that G' is a *subgrammar* of G .

If, for every rule $u \rightarrow m$ in P with $u \in N'$, the word m belongs to $(N' \cup T)^*$ and P' is the set of all such rules, then we say that G' is a *full subgrammar* of G . Hence, G' is a full subgrammar of G iff $S_{G'}$ is a subsystem of S_G and in this case, since

$$S_{G'} \sim_{N'} S_G,$$

it follows that

$$L(G', u) = L(G, u) \quad \text{for all } u \text{ in } N'.$$

Let s be a fixed nonterminal of G (usually called the *axiom* or *start symbol*); the set $N_s = \{u \in N \mid s \rightarrow_G^* wuw' \text{ for some } w, w' \text{ in } (N \cup T)^*\}$ can be easily computed.

The set of equations $S_G \upharpoonright N_s$ is a subsystem of S_G , hence, corresponds to a full subgrammar G_s of G . In G_s every nonterminal u appears in some derivation sequence starting from s and $L(G_s, u) = L(G, u)$ from the above observation.

A classical construction called *reduction* associates with (G, s) a grammar G' by $G' = (G_+)_s$. For every nonterminal u of G' there exists a derivation $s \rightarrow_G^* wuw' \rightarrow_G^* w''$ for some w'' in T^* and $L(G', s) = L(G, s)$. This last fact follows the observation that

$$S_{G'} \subseteq \mathbf{Red}_\sim(S_G) \mathbf{redef}_{\emptyset} S_G.$$

17.3. Elimination of ε -rules

Let $G = \langle N, T, P \rangle$ be a context-free grammar. Let $N_\varepsilon \subseteq N$ be the set of nonterminals u such that $\varepsilon \in L(G, u)$. We know from Section 16.6 how to compute N_ε .

Let $G' = \langle N, T, P' \rangle$ be the context-free grammar such that $u \rightarrow w'$ is a rule in P' iff $w' \neq \varepsilon$ and there exists in P a rule of the form $u \rightarrow w$ with $w = \alpha_1 u_1 \alpha_2 u_2 \dots u_k \alpha_{k+1}$, $k \geq 0$ such that $u_1, \dots, u_k \in N_\varepsilon$, $\alpha_1, \dots, \alpha_{k+1} \in (N \cup T)^*$, and $w' = \alpha_1 \alpha_2 \dots \alpha_k$. Since $k = 0$ is allowed, every rule $u \rightarrow w$ in P with $w \neq \varepsilon$ is also in P' .

Hence, G' has no ε -rule, i.e., no rule of the form $u \rightarrow \varepsilon$. We say that it is ε -free. By using an induction on derivation sequences, one can prove (see [57, p. 99]) that

$$(1) \quad L(G', u) = L(G, u) \quad \text{if } u \in N - N_\varepsilon,$$

$$(2) \quad L(G', u) = L(G, u) - \{\varepsilon\} \quad \text{if } u \in N_\varepsilon.$$

Our purpose is to formulate the transformation of G into G' in terms of our basic $\sim_{\mathcal{D} \cup \mathcal{E}_m}$ -correct transformations and obtain (1) and (2) immediately. Let $\bar{N} = \{\bar{u} \mid u \in N\}$ (hence $\bar{N} \cap N = \emptyset$), let α be the renaming which replaces u by \bar{u} and let $\bar{S} = \alpha(S_{G'})$. Let S be the set of equations:

$$u = \bar{u} \quad \text{for } u \in N - N_\varepsilon,$$

$$u = \bar{u} + \varepsilon \quad \text{for } u \in N_\varepsilon.$$

Claim. $(S \cup \bar{S}) \text{ redef}_{\mathcal{D} \cup \mathcal{E}_m} (S_G \cup \bar{S})$.

This claim yields $S_G \sim_{N, \mathcal{D} \cup \mathcal{E}_m} S \cup \alpha(S_{G'})$ which immediately implies (1) and (2).

Proof of the claim. For the verification of conditions (1) to (3) of Definition 5.10 we shall use the following notations:

$$S_G = \langle u = p_u \mid u \in N \rangle, \quad \bar{S} = \langle \bar{u} = q_{\bar{u}} \mid \bar{u} \in \bar{N} \rangle,$$

$$S = \langle u = r_u \mid u \in N \rangle.$$

Condition (1) reduces to the condition: p_u has its unknowns in N for all u in N , which holds from the definitions.

Condition (2) reduces to:

$$r_u[\Omega/\bar{u}; \bar{u} \in \bar{N}] \leq_{\mathcal{D} \cup \mathcal{E}_m}^0 p_u^h[\Omega/u; u \in N] \quad \text{for some } h \geq 0.$$

The only nontrivial case is when $u \in N_\varepsilon$ since then the left-hand side is $\leftrightarrow_{\mathcal{D} \cup \mathcal{E}_m}^*$ -equivalent to ε . (Otherwise, it collapses to Ω). But in this case, $\varepsilon \in L(G, u)$, hence, $\varepsilon \in \text{Dev}(p_u^h[\Omega/u; u \in N])$ for some large enough h by the theorem of Ginsburg and Rice (see our Proposition 13.5) and the Least Fixed Point Lemma (see Section 2.2)).

Condition (3) reduces to

$$(3a) \quad q_{\bar{u}} \equiv_{\mathcal{D} \cup \mathcal{E}_m} p_u[r_u/u; u \in N] \quad \text{if } u \in N - N_\varepsilon,$$

$$(3b) \quad q_{\bar{u}} + \varepsilon \equiv_{\mathcal{D} \cup \mathcal{E}_m} p_u[r_u/u; u \in N] \quad \text{if } u \in N_\varepsilon.$$

For every w in $(N \cup T)^*$, let P'_w be the set of words obtained by erasing in w some occurrences of elements of N_ε . Let \bar{P}'_w be $\alpha(P'_w)$, i.e., the result of the replacement of \bar{u} for u in all the words of P'_w . We also identify words in $(N \cup \bar{N} \cup T)^*$ with monomials in $M(T_m, N \cup \bar{N})$ in an obvious way. It follows that $\bar{P}'_w = \text{Dev}(w[r_u/u; u \in N])$. Note also that $q_{\bar{u}} = \sum (Q_u - \{\varepsilon\})$, where $Q_u = \bigcup \{\bar{P}'_w \mid u \rightarrow w \text{ is a production of } P\}$. Note finally that $\varepsilon \in Q_u$ iff $u \in N_\varepsilon$. These remarks immediately entail conditions (3a) and (3b). And this completes the proof of the Claim. \square

17.4. Elimination of chain-rules

A production rule of the form $u \rightarrow u'$, where u' is a nonterminal is called a *chain-rule*. A grammar is *chain-free* if it has no chain rule.

17.1. Definition. For every context-free grammar $G = \langle N, T, P \rangle$ which is ε -free the following classical construction (see [57, p. 101]) defines an equivalent chain-free grammar $G' = \langle N, T, P' \rangle$: P' is the set of rules of the form $u \rightarrow w$ where $w \notin N$, $u \rightarrow_G^* u'$, and $u' \rightarrow w$ is in P for some u' in N .

This definition is effective since the set of pairs (u, u') such that $u \rightarrow_G^* u'$ is the transitive and reflexive closure of the relation $P \cap (N \times N)$, hence, can be computed.

It is easy to verify, by adapting the second step of the proof of Lemma 14.13, to the present case, that

$$S_G \text{ rufld}_{\mathcal{D}}^* \text{ ncycl}^* \text{ runf}_{\mathcal{D}}^* S_{G'}.$$

Hence $S_G \sim_{\mathcal{D}} S_{G'}$, i.e.,

$$L(G', u) = L(G, u) \quad \text{for all } u \text{ in } N.$$

If G is cycle-free, then $S_G \text{ runf}_{\mathcal{D}}^* S_{G'}$ and $S_G \approx_{\mathcal{D}} S_{G'}$.

17.5. Chomsky normal form

A context-free grammar $G = \langle N, T, P \rangle$ is in *Chomsky normal form* if, for every rule $u \rightarrow w$ in P , either $w \in N^2$ or $w \in T$. This implies in particular that G is ε -free. It is clear that an ε -free grammar G is in Chomsky normal form iff S_G is uniform.

A classical construction (see [57, p. 104]) associates with $G = \langle N, T, P \rangle$ assumed to be ε -free, a grammar $G' = \langle N', T, P' \rangle$ in Chomsky normal form such that $N \subseteq N'$ and $L(G', u) = L(G, u)$ for all u in N .

Actually, there are several slightly different ways to do that which all consist in introducing auxiliary nonterminals and production rules. In all cases, S_G is the result of the elimination in $S_{G'}$ of the unknowns of $N' - N$, as explained in Proposition 7.8. Hence, there exists an S' such that

$$S_G \subseteq_{\ell} S' \text{ rfld } S_{G'}.$$

Hence, $S_G \approx_{\mathcal{D} \cup \mathcal{E}_{m,N}} S_{G'}$, i.e., S_G and $S_{G'}$ have the same set of solutions in $\mathcal{P}(T^*)$ (and even in $\mathcal{P}(M)$ for every monoid M such that $T \subseteq M$). One possible way to construct G' is by letting

$$S_{G'} = \text{Ufm}(S_G),$$

where Ufm is the uniformization of systems used in Proposition 12.17.

17.6. Invertible grammars

A context-free grammar G is *invertible* [57, p. 101] if, for any two production rules $u \rightarrow m$ and $u' \rightarrow m'$, $m = m'$ implies $u = u'$.

One can transform an arbitrary context-free grammar into an invertible one by means of an algorithm [57, p. 101] which extends the one given in [71] for parenthesis grammars and is essentially the construction of a quasi-deterministic system given in the construction of Section 14, which is actually due to Mezei and Wright [73].

17.7. Greibach normal form

The construction which transforms an arbitrary context-free grammar G into an equivalent one G' in Greibach normal form is more complicated. We conjecture that it cannot be expressed in terms of the basic transformations that we have defined as are the transformations described in Sections 17.1 to 17.6.

We now want to show that the main step in the transformation of G into G' can be fairly easily validated by the unique fixed-point technique. This main step is the following one, formulated in terms of $+$ -regular systems over T_s (i.e., it concerns ε -free grammars)

17.2. Lemma. *If $S = \langle u = u.p + q, v_1 = r_1, \dots, v_n = r_n \rangle$ and $S' = \langle u = q.u' + q, u' = p.u' + p, v_1 = r_1, \dots, v_n = r_n \rangle$, where p, q, r_1, \dots, r_n are polynomials over T_s such that $q, r_1, \dots, r_n \notin U = \{u, v_1, \dots, v_n\}$, then $S \sim_{T^+, U} S'$.*

Its proof will use the following lemma.

17.3. Lemma. *Let A, B be two subsets of T^+ . If $A = BA \cup B$, then $AB = BA$.*

Proof. Consider the equation

$$L = BL \cup BB. \quad (8)$$

Its solution in $\mathcal{P}(T^+)$ is unique since $\mathcal{P}(T^+)$ is spanning and since equation (8) is contracting (recall that $\varepsilon \notin B$). Let L_0 be this solution. From the hypothesis $A = BA \cup B$, one obtains $AB = BAB \cup BB$. Hence, $AB = L_0$. Similarly $BA = BBA \cup BB$. Hence, $BA = L_0$ and $AB = BA$. \square

Proof of Lemma 17.2. Let (L, L', L_1, \dots, L_n) be the least solution of S' . Clearly, L, L', L_1, \dots, L_n are subsets of T^+ . We prove that (L, L_1, \dots, L_n) is a solution of S . The last n equations of S obviously hold, so that we need only prove that

$$L = L.\bar{p} \cup \bar{q},$$

i.e., that

$$\bar{q}.L' \cup \bar{q} = \bar{q}.L'.\bar{p} \cup \bar{q}.\bar{p} \cup \bar{q}, \quad (9)$$

where \bar{p} denotes $p_{T^+}(L, L_1, \dots, L_n)$ and similarly for \bar{q} .

Since $L' = \bar{p}.L' \cup \bar{p}$, it follows that $\bar{p}.L' = L'.\bar{p}$, hence, the right-hand side of (9) evaluates to $\bar{q}.\bar{p}.L' \cup \bar{q}.\bar{p} \cup \bar{q} = \bar{q}.(L'.\bar{p}) \cup \bar{q} = \bar{q}L' \cup \bar{q}$ which proves (9). From the hypothesis on q, r_1, \dots, r_n , the system S corresponds to a proper grammar,

hence, has a unique solution in $\mathcal{P}(\mathbf{T}^+)$. Hence, (L, L_1, \dots, L_n) is its least (and unique) solution. \square

18. More general grammars

Rather than new results, this section introduces some generalizations of the concept of grammar defined in Section 16 and presents informally some forthcoming developments.

18.1. Definitions. Starting with the definition of a grammar as a pair (S, \mathbf{M}) we can generalize Definition 16.1 by allowing in \mathbf{M} :

Case 1: partial functions $f_{\mathbf{M}}: M^{\rho(f)} \rightarrow M$,

Case 2: multivalued functions defined as total functions $f_{\mathbf{M}}: M^{\rho(f)} \rightarrow \mathcal{P}(M)$,

Case 3: nonstrict partial functions $f_{\mathbf{M}}$ which possibly yield a value when some of their arguments are undefined.

In all these cases, S is solved in the ω -complete F_+ -magma $\mathbf{P} = \mathcal{P}(\mathbf{M})$, where $f_{\mathbf{P}}$ is defined as the canonical extension of $f_{\mathbf{M}}$ to $\mathcal{P}(\mathbf{M})^{\rho(f)}$.

There is still another generalization.

Case 4: The $f_{\mathbf{P}}$'s are defined as monotone functions $\mathcal{P}(\mathbf{M})^{\rho(f)} \rightarrow \mathcal{P}(M)$ so that it may happen that $f_{\mathbf{P}}(\{d, d'\})$ is strictly larger than $f_{\mathbf{P}}(\{d\}) \cup f_{\mathbf{P}}(\{d'\})$.

It is clear that Case 4 includes Cases 1 to 3, and that Case 2 includes Case 1. Some examples of Case 2 have been considered in [21], and the systems associated with OI-context-free tree grammars are examples of Case 4 (see Section 16.3).

Let \mathcal{V}_p be the class of *partial* F -magmas (of Case 1), \mathcal{V}_m be the class of *multivalued* F -magmas (of Case 2) and \mathcal{V}_{ns} be the class of *nonstrict* F -magmas (of Case 3).

18.2. Proposition. *If $\mathbf{M} \in \mathcal{V}_p$ or $\mathbf{M} \in \mathcal{V}_m$, then $\mathcal{P}(\mathbf{M})$ is a distributive F -magma.*

The proof can be done by easy verification.

If $\mathbf{M} \in \mathcal{V}_{ns}$, $\mathcal{P}(\mathbf{M})$ satisfies all equations of \mathcal{D} except

$$f(\dots, \Omega, \dots) = \Omega$$

(if $f_{\mathbf{M}}$ is nonstrict).

In Case 4, \mathbf{P} satisfies the equations of \mathcal{D} concerning $+$, but neither

$$f(\dots, \Omega, \dots) = \Omega$$

nor the distributivity

$$f(\dots, x + x', \dots) = f(\dots, x, \dots) + f(\dots, x', \dots).$$

Letting \approx_p^p, \sim_p^p , (respectively \approx_m^p, \sim_m^p) be the equivalences on polynomial systems associated with partial magmas in an obvious way (respectively with multivalued magmas) the following holds.

18.3. Proposition. (1) *Every transformation of polynomial systems which is $\approx_{\mathcal{D}}$ -correct (or $\sim_{\mathcal{D}}$ -correct) is \approx_p^p - and \approx_m^p -correct (or \sim_p^p -correct and \sim_m^p -correct).*

(2) *For polynomial systems S and S' ,*

$$S \approx_{\mathcal{D}} S' \text{ iff } S \approx_m^p S' \text{ iff } S \approx_p^p S' \text{ iff } S \approx^p S',$$

$$S \sim_{\mathcal{D}} S' \text{ iff } S \sim_m^p S' \text{ iff } S \sim_p^p S' \text{ iff } S \sim^p S'.$$

Proof. Part (1) is an immediate consequence of Proposition 18.2.

(2) $S \approx_{\mathcal{D}} S'$ implies $S \approx_m^p S'$ (by Proposition 18.2)

implies $S \approx_p^p S'$ (since $\mathcal{V}_m \supset \mathcal{V}_p$)

implies $S \approx^p S'$ (since $\mathcal{V}_p \supset \mathcal{V}$)

implies $S \approx_{\mathcal{D}} S'$ (by Theorem 12.1).

A similar argument works for $\sim_{\mathcal{D}}$ with the help of Theorem 13.7. \square

18.4. Remarks. Here are some remarks concerning derivation trees and grammatical denotations, which will be developed in a forthcoming paper.

Case 1: Derivations trees and grammatical denotations are defined as in Section 16 but some grammatical denotations have no value.

Case 2: As in Case 1 except that a grammatical denotation may have a (possibly empty) set of values.

Case 3: Derivation trees must be defined in $M(Q \cup \{\Omega\})$, grammatical denotations in $M(F \cup \{\Omega\})$ and they have at most one value.

Case 4: Derivation trees must be defined in $M(Q_+)$ (cf. the end of Section 16.3) and grammatical denotations in $M(F_+)$. Each of them denotes a (possibly empty) set of values.

Appendix A. Coherent and simplifiable congruences

We prove some technical properties of rewriting systems associated with regular systems which were needed in Sections 4 and 6. We present them in a self-contained chapter (depending only on Sections 1 and 2.1, and Definition 4.11), because we think that they are interesting by themselves.

A.1. Definitions. Let F be a finite ranked alphabet and $U = \{u_1, \dots, u_n\}$ be a finite set of constants disjoint from F . An equivalence relation \equiv on $M(F \cup U)$ is *F-coherent* if $f(s_1, \dots, s_l) \equiv g(s'_1, \dots, s'_m)$ with $f, g \in F$ (l and/or m may be zero) implies $f = g$. It is *F-simplifiable* if $f(s_1, \dots, s_l) \equiv f(s'_1, \dots, s'_l)$ implies $s_i \equiv s'_i$ for all $i = 1, \dots, l$.

A.2. Proposition. *The congruence \leftrightarrow_S^* on $M(F \cup \text{Unk}(S))$ associated with a regular system S is F-coherent and F-simplifiable.*

Proof. Let $s = f(s_1, \dots, s_l)$ and $s' = g(s'_1, \dots, s'_m)$ such that $s \leftrightarrow_S^* s'$. We show that $g = f$ and that $s_i \leftrightarrow_S^* s'_i$ for all $i = 1, \dots, l = m$.

We do the proof by induction on k , where k is the smallest integer such that $s \leftrightarrow_S^k s'$. The case $k = 0$ means that $s' = s$. The conclusion follows trivially.

Let $k \geq 1$. One has

$$s = f(s_1, \dots, s_m) \leftrightarrow_S s'' \leftrightarrow_S^{k-1} s'.$$

From the definition of a regular system, one only has two cases to consider:

Case 1: $s'' = f(s''_1, \dots, s''_l)$, $s_i \leftrightarrow_S^* s''_i$ and the result follows by induction.

Case 2: $s'' = u_i$ and $s = t_i$. The sequence $s \leftrightarrow_S^k s'$ is one of the following two possible forms (with u_i, u_{i_j} in $\text{Unk}(S)$):

$$s \xleftarrow[S]{} u_i \xleftarrow[S]{} u_{i_1} \xleftarrow[S]{} u_{i_2} \xleftarrow{\dots} \dots \xleftarrow[S]{} \dots \xleftarrow[S]{} u_{i_{k-1}} = s'$$

or

$$s \xleftarrow[S]{} u_i \xleftarrow[S]{} u_{i_1} \xleftarrow{\dots} \dots \xleftarrow[S]{} u_{i_{k-1}} \xleftarrow[S]{} u_{i_k} \xrightarrow[S]{} u_{i_{k-1}} \xleftrightarrow[S]^* s'.$$

The first one is impossible since s' is not in $\text{Unk}(S)$ and the second one is not of shortest length, so is impossible too. Hence, the result is proved. \square

A.3. Definition. By an *s.c. equivalence* (respectively *s.c. congruence*) on $M(F \cup U)$ we mean an equivalence (respectively congruence) which is *F-simplifiable* and *F-coherent*.

Let us now fix a linear order \leq on U and associate with it a partial order \leq on $M(F, U)$ as defined in Definition 4.11. Let $<$ be the associated strict partial order. It is clear that $|t| \leq |t'|$ whenever $t \leq t'$. It is easy to prove that $<$ is well-founded, i.e., that there is no infinite sequence in $M(F \cup U)$ such that $t_1 > t_2 > t_3 > \dots > t_i > \dots$.

Let now \equiv be an s.c. congruence on $M(F \cup U)$. Let δ be the mapping associating with s, s' in $M(F \cup U)$ such that $s \equiv s'$ an element $\delta(s, s')$ of $M(F \cup U)$ defined as

follows:

- (1) $\delta(f(s_1, \dots, s_m), f(s'_1, \dots, s'_m)) = f(\delta(s_1, s'_1), \dots, \delta(s_m, s'_m))$,
- (2) $\delta(s, s') =$ the smallest of s, s' w.r.t. \leq if at least one of s, s' belongs to U .

Since \equiv is assumed to be F -coherent, there is no other case to consider; since it is assumed F -simplifiable (and by induction), the terms $\delta(s_i, s'_i)$, $i = 1, \dots, m$ of clause (1) are well-defined. By the definition of \leq , s and s' are comparable in clause (2).

A straightforward induction on the computation of δ can show that the following lemma holds.

A.4. Lemma. *If \equiv is an s.c. congruence on $M(F \cup U)$, if $s, s' \in M(F \cup U)$ and $s \equiv s'$, then $\delta(s, s') \equiv s$ and $\delta(s, s')$ is the greatest lower bound of $\{s, s'\}$ w.r.t. \leq .*

Let $<_0$ be the relation on $M(F, U)$ defined by

$$t <_0 t' \text{ iff } t < t', t \equiv t' \text{ and, for all } s \text{ such that } s \equiv t \text{ and } t \leq s \leq t', \text{ either } s = t \text{ or } s = t'.$$

A.5. Lemma. *If \equiv is an s.c. congruence, if $u \in U$ and if there exists $t \equiv u$ such that $u < t$, then there exists a unique s such that $u <_0 s$.*

Proof. Let $C = \{t \in M(F, U) \mid u < t \text{ and } u \equiv t\}$. This set is nonempty. Let C' be the set of elements of C of minimal size. It is finite, hence, it has (by Lemma A.4) a greatest lower bound s . Hence, $u \leq s$. If $s \neq u$, then s is the desired object, and its unicity follows.

If $C \cap U \neq \emptyset$, then s is the least element of $C \cap U$ by the definition of \leq , $s \in U$ and $s \neq u$.

If $C \subseteq F(M(F, U))$, then the greatest lower bound of any pair of elements of C is in $F(M(F, U))$, hence, s is so and $s \neq u$. Note that s is the least element of C' , hence, also of C . \square

A.6. Definition. We associate with a s.c. congruence \equiv a regular system $S_{\equiv} = \langle u_i = t_i; 1 \leq i \leq n \rangle$ by the following requirements where $U = \{u_1, \dots, u_n\}$ and $C_i = \{t \mid u_i < t, u_i \equiv t\}$.

- (1) $t_i = u_i$ if $C_i = \emptyset$,
- (2) $t_i = \mathbf{Min}(C_i)$ if $C_i \neq \emptyset$ (i.e., t_i is the term s associated with u_i by Lemma A.5).

Note that if the equivalence class of u_i is included in U , then there exists a sequence i_1, \dots, i_k such that $t_i = u_{i_1}$, $t_{i_1} = u_{i_2}$, \dots , $t_{i_{k-1}} = u_{i_k}$, $t_{i_k} = u_{i_k}$, where u_{i_k} is the maximal element of this class w.r.t. \leq .

A.7. Lemma. *If $t \leq t'$ and $t \equiv t'$, then $t \rightarrow_{S_{\equiv}}^* t'$.*

Proof. The lemma is proved by induction on the structure of t' . (We let $S = S_{\equiv}$).

Case 1: $t' \in U$. Then $t \in U$. There exists a finite sequence $t <_0 t_1 <_0 t_2 <_0 \cdots <_0 t_k <_0 t'$ (by Lemma A.5) and necessarily $t_1, t_2, \dots, t_k \in U$. By the definition of S , $t \rightarrow_S t_1 \rightarrow_S t_2 \rightarrow_S \cdots \rightarrow_S t'$.

Case 2: $t, t' \in F(M(F, U))$. Hence, $t = f(t_1, \dots, t_k)$, $t' = f(t'_1, \dots, t'_k)$ for some t_i, t'_i such that $t_i \leq t'_i$ and $t_i \equiv t'_i$. The induction hypothesis shows that $t_i \rightarrow_S^* t'_i$. Hence, $t \rightarrow_S^* t'$.

Case 3: $t \in U$, $t' \in F(M(F, U))$. There exists (as in Case 1) a finite sequence $t = u_{i_0} <_0 u_{i_1} <_0 u_{i_2} <_0 \cdots u_{i_k} <_0 t''$, where $t'' \in F(M(F, U))$ and $t'' \leq t'$. Since $t'' \equiv t'$, the proof of Case 2 gives $t'' \rightarrow_S^* t'$ and, as in Case 1, $t \rightarrow_S u_{i_1} \rightarrow_S u_{i_2} \rightarrow_S \cdots \rightarrow_S u_{i_k} \rightarrow_S t''$.

Hence, $t \rightarrow_S^* t'$ as was to be proved. \square

A.8. Theorem. (1) *Let \equiv be a s.c. congruence on $M(F \cup U)$ and \leq be a linear order on U . Then S_{\equiv} is the unique regular system S such that $\text{Unk}(S) = U$, $R(S)$ is left-irreducible, \leq -compatible and such that \equiv is the congruence generated by S .*

(2) *Let \leq' be another linear order on U and S'_{\equiv} be the unique regular system associated with \equiv and \leq' by (1). There exists a renaming α such that $\alpha(S_{\equiv}) = S'_{\equiv}$.*

Proof. (1) Let $S = S_{\equiv}$. By construction, $R(S)$ is \leq -compatible and included in \equiv . If $R(S)$ is not left-irreducible, there exists an i such that $t_i \rightarrow_{R'} t$ with $R' = R(S) - \{(t_i, u_i)\}$. There are two cases.

Case 1: $t \in U$. Hence, $t = u_j$ and $t_i = t_j$ for some $j \neq i$. This implies $u_i \leftrightarrow_S^* u_j$, hence, $u_i \equiv u_j$. Either $u_i \in C_j$ or $u_j \in C_i$. In both cases one cannot have $\text{Min}(C_i) = \text{Min}(C_j)$. Hence, $t_i \neq t_j$.

Case 2: $t \in F(M(F, U))$. Hence, $t < t_i$, $t \equiv t_i$ since S is included in \equiv . Hence, $u_i < t < t_i$ and this contradicts the definition of t_i .

Hence, $R(S)$ is left-irreducible.

We now prove that \equiv is included in \leftrightarrow_S^* . Let $s \equiv s'$ and $s'' = \delta(s, s')$. By Lemma A.3, $s'' \leq s$, $s'' \leq s'$, and $s'' \equiv s \equiv s'$. Lemma A.7 shows that $s \leftarrow_S^* s'' \rightarrow_S^* s'$. Hence, $s \leftrightarrow_S^* s'$. Hence, we have shown that \equiv is the congruence generated by S_{\equiv} (equivalently by $R(S_{\equiv})$).

In order to prove the unicity result, let $S = \langle u_i = t_i; 1 \leq i \leq n \rangle$ be a regular system such that $R(S)$ is left-irreducible, \leq -compatible and such that \equiv is \leftrightarrow_S^* .

We must show that, for all i , either $u_i <_0 t_i$ or $t_i = u_i$ and $\{t \mid u_i < t, t \equiv u_i\} = \emptyset$. If $t_i \neq u_i$, then, since $R(S)$ is \leq -compatible, we have $u_i < t_i$ and $t_i \equiv u_i$. Let us assume that $u_i < s \equiv u_i$ for some s . Since $R(S)$ is confluent and Noetherian, s and t_i have the same normal form w.r.t. $R(S)$. Hence, there are two sequences (where \rightarrow represents $\rightarrow_{R(S)}$):

$$\begin{aligned} t_i &\rightarrow u_i \rightarrow w_k \rightarrow w_{k-1} \rightarrow \cdots \rightarrow w_1, \\ s &\rightarrow s_l \rightarrow s_{l-1} \rightarrow \cdots \rightarrow s_1 = w_1. \end{aligned}$$

By the \leq -compatibility of $R(S)$, we have

$$t_i > u_i > w_k > w_{k-1} > \cdots > w_1,$$

$$s > s_l > s_{l-1} > \cdots > s_1$$

and by the definition of \leq , $w_1, \dots, w_k \in U$.

Hence, $s_1 \in U$ and since S is a regular system, $s_2 = w_2$, hence, $s_2 \in U$, $s_3 = w_3$, etc. By going on, one arrives at u_i . Let us compare k and l . If $l \leq k$, then $s \in \{u_i, w_k, w_{k-1}, \dots, w_1\}$, but this contradicts the assumption that $u_i < s$. Hence, $k < l$. This means that $t_i \in \{s, s_l, s_{l-1}, \dots\}$ and that $t_i \leq s$. This shows that $u_i <_0 t_i$.

Hence, S coincides with the system S_{\equiv} .

(2) Let \leq' be another linear order on U . There exists a unique bijection $\alpha : U \rightarrow U$ such that:

$$(i) \quad u \leq u' \text{ iff } \alpha(u) \leq' \alpha(u'),$$

$$(ii) \quad \alpha(u) \equiv u,$$

for all u, u' in U such that $u \equiv u'$.

Consider now the system $S' = \alpha(S_{\equiv})$. Then $R(S')$ is \leq' -compatible by (i) and since $R(S_{\equiv})$ is \leq -compatible, it is left-irreducible since $R(S_{\equiv})$ is and α is a bijection. It follows from (ii) that $\leftrightarrow_{S'}^*$ is included in \equiv . If $u, u' \in U$ and $u \equiv u'$, then $\alpha^{-1}(u) \equiv \alpha^{-1}(u')$, hence, $\alpha^{-1}(u) \leftrightarrow_{S'}^* \alpha^{-1}(u')$. And $u \leftrightarrow_{S'}^* u'$ since $S' = \alpha(S_{\equiv})$. It follows from this that $u \rightarrow_{S_{\equiv}} t$ implies $u \leftrightarrow_{S'}^* t$.

Hence, the congruences \equiv , $\leftrightarrow_{S_{\equiv}}^*$, and $\leftrightarrow_{S'}^*$ are the same. By the unicity result of (1), S' is equal to S'_{\equiv} . \square

A.9. Corollary. *Let \equiv be an s.c. congruence on $M(F \cup U)$ and \leq be a linear order on U . There is a unique ground rewriting system which is proper, \leq -compatible and which generates \equiv .*

Proof. The rewriting system $R(S_{\equiv})$ is not necessarily right-irreducible. By replacing each of its right-hand sides by its normal form w.r.t. $R(S_{\equiv})$, one obtains a rewriting system R which is left- and right-irreducible, \leq -compatible and which generates \equiv (this is a special case of [72, Theorem 7]). By Proposition 1.2, R is the only one having the required properties. \square

As in Theorem A.8, if one uses another linear order \leq' on U , then the unique system R' associated with it is a renaming of R associated with \leq .

A.10. Example. Let $S = \langle u_1 = u_3, u_2 = u_1, u_3 = f(u_2, g(u_4, u_1)), u_4 = g(u_4, u_2) \rangle$ and \equiv be the congruence $\leftrightarrow_{S'}^*$. One has $u_1 <_0 u_2 <_0 u_3 <_0 f(u_1, u_4)$ and $u_4 <_0 g(u_4, u_1)$ (since

$u_1 \equiv u_2 \equiv u_3$ and $u_4 \not\equiv u_1$). Hence, the regular system S_{\equiv} is

$$\langle u_1 = u_2, u_2 = u_3, u_3 = f(u_1, u_4), u_4 = g(u_4, u_1) \rangle.$$

The rewriting system R associated with S_{\equiv} by Corollary A.9 is

$$R = \{u_2 \rightarrow u_1, u_3 \rightarrow u_1, f(u_1, u_4) \rightarrow u_1, g(u_4, u_1) \rightarrow u_4\}$$

and is not $R(S')$ for any regular system S' .

A.11. Proposition. *Let R be a ground rewriting system on $M(F, U)$. One can decide whether the congruence \leftrightarrow_R^* is F -coherent and F -simplifiable. If it is the regular system, $S_{\leftrightarrow_R^*}$ can be effectively constructed.*

Proof. We first recall that Brainerd has shown in [17] that the congruence class of t in $M(F, U)$ modulo \leftrightarrow_R^* is a regular tree language, for which a tree automaton can be constructed. Hence, the word problem is decidable (since the nonemptiness of the intersection of two classes can be decided).

We also recall that the existence of a substitution $\sigma: U \rightarrow M^\infty(F, U)$ in $\text{Unif}^\infty(R)$, i.e., such that $\sigma(\alpha) = \sigma(\beta)$ for all (α, β) in R can be decided [26, Proposition 4.9.5]. This corresponds to the existence of a first-order unifier (in $M^\infty(F, U)$) for R considered as a set of equations.

With every (t, t') in $M(F, U) \times M(F, U)$, we associate a subset $\theta(t, t')$ of $U \times M(F, U)$ as follows:

$$\theta(t, t') = \begin{cases} \{(t, t')\} & \text{if } t \in U, \\ \{(t', t)\} & \text{if } t \notin U, t' \in U, \\ \theta(t_1, t'_1) \cup \dots \cup \theta(t_k, t'_k) & \text{if } t = f(t_1, \dots, t_k), \\ & t' = f(t'_1, \dots, t'_k), \\ \text{undefined} & \text{if } t = f(t_1, \dots, t_k), t' = g(t'_1, \dots, t'_l) \text{ and } f \neq g. \end{cases}$$

We let $R' = \bigcup \{\theta(\alpha, \beta) \mid (\alpha, \beta) \in R\}$.

We now claim that \leftrightarrow_R^* is s.c. iff:

- (1) $\theta(\alpha, \beta)$ is defined for all (α, β) in R ,
- (2) $t \leftrightarrow_R^* t'$ for all (t, t') in R' ,
- (3) $\text{Unif}^\infty(R') \neq \emptyset$.

Let us assume that \leftrightarrow_R^* is s.c. Then (1) holds by the F -coherence, (2) holds by the F -simplifiability, (3) holds by [26, Proposition 4.9.5].

The converse similarly holds.

These three properties are decidable by the two results recalled at the beginning of the proof. Since the word problem is decidable, the construction of Definition A.6 is effective. \square

References

- [1] A. Arnold and M. Nivat, Metric interpretations of infinite trees and semantics of nondeterministic recursive programs, *Theoret. Comput. Sci.* **11** (1980) 181–205.
- [2] A. Arnold and M. Nivat, The metric space of infinite trees. Algebraic and topological properties, *Fund. Inform.* **III**(4) (1980) 445–476.
- [3] J. Backus, Can programming be liberated from the Von Neumann style? A functional style and its algebra of programs, *Comm. ACM* **21** (1978) 613–641.
- [4] J. de Bakker, Least fixed points revisited, *Theoret. Comput. Sci.* **2** (1976) 155–181.
- [5] J. de Bakker and D. Scott, A theory of programs, 1969, unpublished.
- [6] D. Benson and I. Guessarian, Algebraic solutions to recursion schemes, Rept. CS-81-079, Washington State University, Pullman, WA, 1981.
- [7] G. Berry and J.-J. Lévy, Minimal and optimal computations of recursive programs, *J. ACM* **26** (1979) 148–175.
- [8] J. Berstel, *Transductions and Context-free Languages* (Teubner, Stuttgart, 1979).
- [9] G. Birkhoff, On the structure of abstract algebras, *Proc. Cambridge Philos. Soc.* **29** (1935) 433–454.
- [10] S. Bloom, All solutions of a system of recursion equations in infinite trees and other contraction theories, *J. Comput. System Sci.* **27** (1983) 225–255.
- [11] S. Bloom, C. Elgot and J. Wright, Solutions of the iteration equation and extensions of the scalar iteration operation, *SIAM J. Comput.* **9** (1980) 25–45.
- [12] S. Bloom and R. Tindell, Compatible orderings on the metric theory of trees, *SIAM J. Comput.* **9** (1980) 683–691.
- [13] S. Bloom and R. Tindell, Varieties of ‘if-then-else’, *SIAM J. Comput.* **12** (1983) 677–707.
- [14] V. Bodnarchuk, The metrical space of events, *Kibernetika* **1** (1) (1965) 24–27 and (4) (1965) 22–30 (in English).
- [15] R. V. Book, The undecidability of a word problem: On a conjecture of Strong, Maggiolo-Schettini and Rosen, *Inform. Process. Lett.* **12** (1981) 121–122.
- [16] W. Brainerd, The minimalization of tree automata, *Inform. and Control* **13** (1968) 484–491.
- [17] W. Brainerd, Tree generating regular systems, *Inform. and Control* **14** (1969) 217–231.
- [18] J.P. Braquelaire and B. Courcelle, The solutions of two star-height problems for regular trees, *Theoret. Comput. Sci.* **30** (1984) 205–239.
- [19] R. Burstall and J. Darlington, A transformation system for developing recursive programs, *J. ACM* **24** (1977) 44–67.
- [20] L. Chirica and D. Martin, An order-algebraic definition of Knuthian semantics, *Math. Systems Theory* **13** (1979) 1–27.
- [21] L. Chottin, Etude syntaxique de certains langages solutions d’équations avec opérateurs, *Theoret. Comput. Sci.* **5** (1977) 51–84.
- [22] B. Courcelle, A representation of trees by languages, *Theoret. Comput. Sci.* **6** (1978) 255–279 and **7** (1978) 25–55.
- [23] B. Courcelle, Attribute grammars: Definitions, analysis of dependencies, proof methods, in: B. Lorho ed., *Methods and Tools for Compiler Construction* (Cambridge University Press, 1984).
- [24] B. Courcelle, Arbres infinis et systèmes d’équations, *RAIRO Inform. Théor.* **13** (1979) 31–48.
- [25] B. Courcelle, Infinite trees in normal form and recursive equations having a unique solution, *Math. Systems Theory* **13** (1979) 131–180.
- [26] B. Courcelle, Fundamental properties of infinite trees, *Theoret. Comput. Sci.* **25** (1983) 95–169.
- [27] B. Courcelle and P. Deransart, Proofs of partial correctness for attribute grammars and recursive procedures, INRIA Rept. 322, 1984, submitted for publication.
- [28] B. Courcelle and P. Franchi-Zannettacci, Attribute grammars and recursive program schemes, Parts I–II, *Theoret. Comput. Sci.* **17** (1982) 163–191; 235–257.

- [29] B. Courcelle and I. Guessarian, On some classes of interpretations, *J. Comput. System Sci.* **17** (1978) 388-413.
- [30] B. Courcelle, G. Kahn and J. Vuillemin, Algorithmes d'équivalence et de réduction à des expressions minimales, dans une classe d'équations récursives simples, *2nd Internat. Coll. on Automata, Languages and Programming*, Saarbrücken 1974, Lecture Notes in Computer Science **14** (Springer, Berlin, 1974) 200-213.
- [31] B. Courcelle and M. Nivat, Algebraic families of interpretations, *17th Ann. Symp. on Foundations of Computer Science*, Houston, TX (1976) 137-146.
- [32] B. Courcelle and M. Nivat, The algebraic semantics of recursive program schemes, *Math. Found. of Comput. Sci.* **78**, Lecture Notes in Computer Science **64** (Springer, Berlin, 1978) 16-30.
- [33] B. Courcelle and J. C. Raoult, Completions of ordered magmas, *Fund. Inform.* **III**(1) (1980) 105-116.
- [34] B. Courcelle and J. Vuillemin, Completeness results for the equivalence of recursive schemes, *J. Comput. System Sci.* **12** (1976) 179-197.
- [35] G. Cousineau, An algebraic definition for control structures, *Theoret. Comput. Sci.* **12** (1980) 175-192.
- [36] W. Damm, The IO- and OI-hierarchies, *Theoret. Comput. Sci.* **20** (1982) 95-207.
- [37] W. Damm, Languages defined by higher program schemes, *Lecture Notes in Computer Science* **52** (Springer, Berlin, 1977) 164-179.
- [38] W. Damm and E. Fehr, On the power of self-application and higher-type recursion, *Proc. 4th Internat. Coll. on Automata, Languages and Programming*, Udine, Italy, Lecture Notes in Computer Science **62** (Springer, Berlin, 1978) 177-191.
- [39] W. Damm, E. Fehr and K. Indermark, Higher type recursion and self-application as control structures, in: E. Neuhold, ed., *Formal Descriptions of Programming Concepts* (North-Holland, Amsterdam, 1978) 461-487.
- [40] P. Deransart et al., Speeding up circularity tests for attribute grammars, *Acta Inform.* **20** (1984) 375-391.
- [41] S. Eilenberg and J. Wright, Automata in general algebras, *Inform. and Control* **11** (1967) 52-70.
- [42] C. Elgot, Monadic computation and iterative algebraic theories, in: H. E. Rose and J. C. Shepherdson, eds., *Logic Colloquium '73* (North-Holland, Amsterdam, 1975) 175-230.
- [43] C. Elgot and F. Mezei, On relations defined by generalized finite automata, *IBM J. Res. Develop.* **9** (1965) 47-68.
- [44] J. Engelfriet, Bottom-up and top-down tree transformations, a comparison, *Math. Systems Theory* **9** (1975) 198-231.
- [45] J. Engelfriet and E. Schmidt, IO and OI, *J. Comput. System Sci.* **15** (3) (1977) 328-353 and **16** (1) (1978) 67-99.
- [46] J. H. Gallier, Nondeterministic flowchart programs with recursive procedures, semantics and correctness II, *Theoret. Comput. Sci.* **13** (3) (1981) 239-270.
- [47] J. H. Gallier, Recursion closed algebraic theories, *J. Comput. System Sci.* **23** (1981) 69-105.
- [48] J. H. Gallier, *N*-rational algebras, I: Basic properties and free algebras; II: Varieties and the logic of inequalities, *SIAM J. Comput.* **13** (1984) 750-794.
- [49] N. Gautam, The validity of equations of complex algebras, *Arch. Math. Logik, Grundlag.* **3** (1957) 117-124.
- [50] F. Gecseg and M. Steinby, *Tree-automata* (Akademiai Kiado, Budapest, 1984).
- [51] S. Ginsburg and H. Rice, Two families of languages related to ALGOL, *J. ACM* **9** (1962) 350-371.
- [52] J. Goguen, How to prove algebraic inductive hypotheses without induction, *5th Conf. on Automated Deduction*, Les Arcs, Lecture Notes in Computer Science **87** (Springer, Berlin, 1980) 356-373.
- [53] J. Goguen, J. Thatcher and E. Wagner, An initial algebra approach to the specification, correctness and implementation of abstract data types, in: R. Yeh, ed., *Current Trends in Programming Methodology* (Prentice-Hall, Englewood Cliffs, NJ, 1978) 80-149.
- [54] J. Goguen, J. Thatcher, E. Wagner and J. Wright, Initial algebra semantic and continuous algebras, *J. ACM* **24** (1977) 68-95.
- [55] I. Guessarian, Program transformations and algebraic semantics, *Theoret. Comput. Sci.* **9** (1979) 39-65.
- [56] I. Guessarian, *Algebraic Semantics*, Lecture Notes in Computer Science **99** (Springer, Berlin, 1981).
- [57] M. A. Harrison, *Introduction to Formal Language Theory* (Addison-Wesley, Reading, MA, 1978).
- [58] P. Hitchcock and D. Park, Induction rules and proofs of termination, *Proc. 1st Coll. on Automata Languages and Programming* (North-Holland, Amsterdam, 1973) 225-251.

- [59] G. Huet, Confluent reductions: Abstract properties and applications to term rewriting systems, *J. ACM* **27** (1980) 797–821.
- [60] G. Huet and J. M. Hullot, Proofs by induction in equational theories with constructors, *Proc. 21st Symp. on Foundations of Computer Science*, Syracuse, NY (1980) 96–107.
- [61] G. Huet and D. Oppen, Equations and rewrite rules, in: R. V. Book, ed., *Formal Languages, Perspectives and Open Problems* (Academic Press, New York/London, 1980). 349–405.
- [62] V. Istratescu, *Fixed Point Theory* (Reidel, Dordrecht, 1981).
- [63] L. Kott, About transformation systems, a theoretical study, in: B. Robinet, ed., *Transformations de Programmes* (Dunod, Paris, 1978) 232–247.
- [64] L. Kott, Unfold/fold program transformations, *Proc. Sem. on the Application of Algebra to Language Definition and Compilation*, Fontainebleau, 1982 (Cambridge University Press, 1985).
- [65] J.-L. Lassez, V. Nguyen and E. Sonenberg, Fixed points theorems and semantics: A folk tale, *Inform. Process. Lett.* **14** (1982) 112–116.
- [66] P. Lescanne, Equivalence entre la famille des ensembles réguliers et la famille des ensembles algébriques, *RAIRO Inform. Théor.* **10** (1976) 57–81.
- [67] P. Lescanne, Modèles non déterministes de types abstraits, *RAIRO Inform. Théor.* **16** (1982) 225–244.
- [68] Z. Manna and J. Vuillemin, Fixpoint approach to the theory of computation, *Comm. ACM* **15** (1972) 528–536.
- [69] G. Markowsky and B. Rosen, Bases for chain-complete posets, *IBM J. Res. Develop.* **20** (1976) 138–147.
- [70] J. McCarthy, A basis for a mathematical theory of computation, in: P. Braffort and D. Hirschberg, eds., *Computer Programming and Formal Systems* (North-Holland, Amsterdam, 1963) 33–70.
- [71] R. McNauthton, Parenthesis grammars, *J. ACM* **14** (1967) 490–500.
- [72] Y. Métivier, About the rewriting systems produced by the Knuth–Bendix completion algorithm, *Inform. Process. Lett.* **16** (1983) 31–34.
- [73] J. Mezei and J. Wright, Algebraic automata and context-free sets, *Inform. and Control* **11** (1967) 3–29.
- [74] J. Mycielski and W. Taylor, A compactification of the algebra of terms, *Algebra Universalis* **6** (1976) 159–163.
- [75] E. Nelson, Iterative algebras, *Theoret. Comput. Sci.* **25** (1983) 67–94.
- [76] M. Nivat, On the interpretation of recursive polyadic program schemes, *Symposia Mathematica* **15** (Academic Press, New York/London, 1975) 255–281.
- [77] E. Paul, Proof by induction in equational theories with relations between constructors, in: B. Courcelle, ed., *Proc. 9th Coll. on Trees in Algebra and Programming*, Bordeaux (Cambridge University Press, London, 1984) 211–225.
- [78] M. Schützenberger, On context-free languages and push-down automata, *Inform. and Control* **6** (1963) 246–264.
- [79] A. Shafaat, On varieties closed under the construction of power algebras, *Bull. Austral. Math. Soc.* **11** (1974) 213–218.
- [80] R. Tennent, The denotational semantics of programming languages, *Comm. ACM* **19** (1976) 437–453.
- [81] J. Vuillemin, Correct and optimal implementations of recursion in a simple programming language, *J. Comput. System. Sci.* **9** (1974) 332–354.
- [82] J. Vuillemin, *Syntaxe, Sémantique et Axiomatique d'un Langage de Programmation Simple* (Birkhäuser Verlag, Basel/Stuttgart, 1975).
- [83] J. Wright, J. Thatcher, E. Wagner and J. Goguen, Rational algebraic theories and fixed point solutions, *17th Symp. on Foundations of Computer Science*, Houston, TX (1976) 147–158.
- [84] J. Wright, E. Wagner and J. Thatcher, A uniform approach to inductive posets and inductive closure, *Theoret. Comput. Sci.* **7** (1978) 57–77.