FREE DISTRIBUTIVE GROUPOIDS*

Patrick DEHORNOY
Département de Mathématiques, Université de Caen, 14032 Caen, France

Communicated by A. Blass
Received 28 June 1988
Revised 19 October 1988

We study the free groupoids satisfying the identity $x\cdot(y\cdot z)=(x\cdot y)\cdot(x\cdot z)$ and show that the canonical congruence generating them as quotients of free algebras is associated with a confluent system of elementary transformations. Some properties of the monoid generated by these transformations are established.

Introduction

In this paper we investigate general left autodistributive groupoids, namely sets endowed with a binary operation, say $\cdot$, satisfying the following identity:

$$x\cdot(y\cdot z)=(x\cdot y)\cdot(x\cdot z).$$

Such structures will be called for short *distributive groupoids* in the sequel (we also propose to use the term '*clump*'). We concentrate on the properties of free distributive groupoids; standard arguments provide a description of such objects as quotients of free sets of terms (or magmas in the terminology of [1]) under the congruence $\leftrightarrow$ generated by the rewriting rule

$$x\cdot(y\cdot z)\rightarrow(x\cdot y)\cdot(x\cdot z).$$

This general framework does not solve however the numerous questions that can be raised about the free distributive groupoids and $\leftrightarrow$. In particular the word problem for $\leftrightarrow$, i.e. the problem of getting a procedure for deciding whether two given terms are equivalent for $\leftrightarrow$, seems to be difficult, and we cannot solve it for the moment. Nevertheless we establish in this paper several results that can be viewed as first steps in this direction. In particular, we prove the following:

Theorem. *Let $\rightarrow^*$ be the smallest transitive relation that is compatible with the binary operation and includes the rewriting rule $\rightarrow$ above, then $\rightarrow^*$ is a confluent relation.*

* This work was partially supported by a CNRS grant PRC mathématiques & informatique.

It follows that two terms are equivalent for ↔ if and only if they can be developed into a same third one using $\to^*$.

We think that the interest of such results is double. First, the basic rewriting rule → is not a linear one (the term 'x' is repeated twice), so all general arguments as in [9] fail to prove results like the confluency of $\to^*$ (in particular the local confluency is not sufficient for getting the global one), and therefore a rather precise study of the monoid ϑ generated by the transformation → and its translated copies is needed; we hope that some of the tools introduced here could have some intrinsic interest.

Secondly, the paper tries to give a better understanding of the free distributive groupoids (and, therefore, of the general ones). Special families of distributive groupoids have been intensively studied for several decades. In particular classification results and connections with various mathematical objects such as Moufang loops or Steiner triple systems have been established, but in those cases, additional axioms are generally requested, like idempotency [8], median axiom [12] or existence of inverses [13]. On the other hand, it seems that the most general autodistributive groupoids have not been much studied, probably because few examples of such structures appeared naturally. Our actual interest for them precisely originates in the recent appearance in set theory of a 'mysterious' distributive groupoid. One can present it roughly as follows.

When models of ZF are dealt with, the convenient notion corresponding to the homomorphisms in algebra is the notion of an elementary embedding. If M, M' are two models of ZF, an elementary embedding of M into M' is a mapping

$$j : M \to M'$$

such that, for every first-order formula $F(x_1, \dots, x_n)$ using $\in$ and every n-tuple $\langle a_1, \dots, a_n\rangle$ made by members of M, $F(a_1, \dots, a_n)$ is true in M iff $F(ja_1, \dots, ja_n)$ is true in M'. It follows that such a mapping is a homomorphism with respect to *every* operation or relation that is first-order definable from the membership relation $\in$, for instance equality ($a_1 = a_2$ holds in M iff $ja_1 = ja_2$ holds in M'), membership ($a_1 \in a_2$ holds in M iff $ja_1 \in ja_2$ holds in M'), but as well integer addition ($\langle a_1, a_2, a_3\rangle \in \mathbb{N}^3$ and $a_1 = a_2 + a_3$ hold in M iff $\langle ja_1, ja_2, ja_3\rangle \in \mathbb{N}^3$ and $ja_1 = ja_2 + ja_3$ hold in M') since integer addition is definable in ZF set theory, or application of a mapping to a member of its domain ('f is a mapping' and $b = f(a)$ hold in M iff 'jf is a mapping' and $jb = jf(ja)$ hold in M'). Notice that the last equality can be rewritten as

$$j(f(a)) = jf(ja), \tag{*}$$

that is typographically the left distributivity of the operation $x, y \to x(y)$; but, of course, in this formula, f and a are members of M while j is a mapping of M into M'.

When only one model M of ZF is studied, one naturally introduces the notion of an elementary embedding of M into itself. The identity mapping of M is trivially such an elementary embedding. It happens that nontrivial (i.e. distinct of identity) elementary embeddings need not exist for all models, but in fact the hypotheses asserting the existence of various kinds of elementary embeddings proved in the last two decades to be the most powerful tools in order to describe and to classify the models of ZF set theory, according to works by Silver, Jensen, Woodin, Martin and Steel in particular (see [11] or [10] for an introduction). One of the hypotheses above, that will be referred to as $(\mathscr{H})$, asserts the existence of an elementary embedding, say j, of a model M into itself that is a class for M, which means, roughly speaking, that j itself can be viewed as a member of M (in fact, in that case, M has to be restricted to be only a convenient part of a model of ZF). It follows that j can be applied to itself, providing a new object $j(j)$ that proves to be an elementary embedding of M into itself as well, and the construction can be repeated to get, for instance, new elementary embeddings $j(j(j))$ or $j(j)(j)$... Let $\mathfrak{j}$ denote the family of all elementary embeddings one gets in this way: the identity $(*)$ above applies in particular when its three entries are arbitrary members of $\mathfrak{j}$, and this means that $\mathfrak{j}$ is a distributive groupoid (generated by j). So, under the assumption $(\mathscr{H})$, one obtains a groupoid (or several ones, since it is not known whether different elementary embeddings give raise to isomorphic structures), and, as no other relation is known in $\mathfrak{j}$, it is rather natural to conjecture that $\mathfrak{j}$ is in fact a free distributive groupoid, but, up to now, few arguments corroborate this conjecture; precisely a natural way for attacking the problem is to show that the properties proved in $\mathfrak{j}$ also hold in the free distributive groupoid, and this paper is a preliminary step in this direction. In any case, the groupoid $\mathfrak{j}$ is quite a strange object (see [6]), and the above conjecture would imply a fascinating complexity for the free distributive groupoids. We can still mention that the above analysis has already been used in set theory, namely in [4] the purely algebraic framework developed in [3] is used to show that the determinacy property for coanalytic subsets of the real line essentially rests upon the groupoid structure of $\mathfrak{j}$.

Finally let us quote some other examples of monogenic distributive groupoids. First, three finite projections of $\mathfrak{j}$ with respectively 2, 4 and 8 elements are known (notice that the tables of these groupoids have been constructed using $\mathfrak{j}$, that is a purely hypothetic object – in particular Gödel's second incompleteness theorem dismisses any hope of even proving that its existence is not contradictory – but then these tables are finite, the distributivity axiom is easily verified and therefore the resulting groupoids do not have any more hypothetic character). Secondly, using some ideas from the definition of $\mathfrak{j}$, one can get a groupoid structure on the set $\mathfrak{I}_X$ of all one-one mappings of any set X into itself and construct in this way nontrivial examples of monogenic distributive groupoids [5].

The paper is divided into five sections. The first one sets notations and introduces the basic relation $\rightarrow^*$ and the structural monoid ϑ. In the second one, some commutation relations are proved in ϑ. In the third one, the confluence of $\rightarrow^*$ is established. The fourth section improves this result to an intrinsic relation in ϑ. The last section briefly discusses some further questions on the structure of $\rightarrow^*$ and ϑ.

1. Description of ϑ and $\rightarrow^*$

In order to handle easily with terms in non-associative structures, it will be useful to consider these terms as binary *trees* – exactly as, in the associative case, terms are represented by strings. A point in a tree will be specified by its address, consisting of a finite sequence of 0's and 1's. More precisely, our notations will be as follows· $\mathbb{S}$ denotes the set $\{0,1\}^*$ of all such finite sequences, the empty sequence in $\mathbb{S}$ is denoted by Λ; for u, v in $\mathbb{S}$, the product (concatenation) of u, v is denoted by uv, and $\mathbb{S}$ is endowed with the usual order $\subseteq$ defined by

$$u \subseteq v \quad \text{iff} \quad (\exists w)(v = uw).$$

We also use the notion of the left-right ordering on $\mathbb{S}$ that is defined in an obvious way for incomparable members of $\mathbb{S}$ (w.r. to $\subseteq$): for every u, v, w in $\mathbb{S}$, $u0v$ is on the left of $u1w$.

It will be convenient to consider a binary tree on Σ as a maximal finite set of pairwise incomparable members of $\mathbb{S}$ (w.r. to $\subseteq$) – the addresses of the leaves of the tree – together with a member of Σ associated to each of these addresses – i.e. a label in Σ for each leaf of the tree. Formally, this leads to the following recursive definition:

Definition 1.1. Let Σ be any set;

(i) assume that S, T are (partial) mappings of $\mathbb{S}$ into Σ; define a new mapping $S \wedge T$ as follows:

$$(S \wedge T)(u) = a \quad \text{iff} \quad (\exists v)((u = 0v \text{ and } S(v) = a) \text{ or } (u = 1v \text{ and } T(v) = a)).$$

(ii) $\mathscr{C}_\Sigma$, the set of all (binary) trees on Σ, is the smallest set of partial mappings of $\mathbb{S}$ into Σ that is closed under $\wedge$ and contains $\{(\Lambda, a)\}$ for every a in Σ.

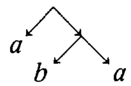
It immediately follows from this definition that, in order to prove that some property holds for every member of $\mathscr{C}_\Sigma$, it suffices to prove that the property is preserved under $\wedge$ and holds for all $\{(\Lambda, a)\}$ with a in Σ.

We shall identify, for a in Σ, the term a with the tree $\{(\Lambda, a)\}$, so $\mathscr{C}_\Sigma$ is nothing but the set of all terms constructed from Σ using the binary operator $\wedge$ (i.e. is a free magma generated by Σ in the terminology of [1]) – since every tree that is not in Σ can be written is a unique way as the product of two trees with smaller cardinalities of their domains. Now if we associate to each tree T a graph Γ_T such that, for a in S, Γ_a has only one point labelled a, and $\Gamma_{S \wedge T}$ is exactly

$$\begin{tikzcd} & {} \arrow[dl] \arrow[dr] & \\ \Gamma_S & & \Gamma_T, \end{tikzcd}$$

we get the usual geometrical representation of trees.

Example. Assume that a, b are in Σ; then $\{(0,a),(10,b),(11,a)\}$ is a tree T_0 on Σ, and the corresponding term is $a\wedge(b\wedge a)$, while the associated graph is



In other words, T_0 has three leaves, whose addresses are 0, 10, 11, and the leaf 10 for instance is labelled 'b'.

Definition 1.2. Let T be any member of $\mathscr{C}_\Sigma$.

(i) The domain of T will be denoted by $|T|$ ($|T|$ is a subset of $\mathbb{S}$), and the set $\{u\in\mathbb{S}\colon (\exists v\in\mathbb{S}\setminus\{\Lambda\})(uv\in|T|)\}$ will be denoted by $|T|^\circ$ (the strict interior of $|T|$);

(ii) T is extended to a mapping of $|T|\cup|T|^\circ$ to $\mathscr{C}_\Sigma$ (still denoted by T) by defining, for u in $|T|^\circ$, $T(u)$ to be the subtree of T whose root is 'in u'.

For instance, if T_0 is the tree quoted above, $|T_0|$ is $\{0,10,11\}$, $|T_0|^\circ$ is $\{\Lambda,1\}$, $T_0(10)$ is b while $T_0(1)$ is $b\wedge a$. We notice that $T=T(\Lambda)$ always holds, and that $T=T(0)\wedge T(1)$ holds for every T such that $|T|$ is not $\{\Lambda\}$ (i.e. T is not in Σ). If a is in Σ, and T is in $\mathscr{C}_\Sigma$, every member of $T^{-1}(a)$ will be called an *occurrence* of a in T. In the example above, a has two occurrences in T, namely 0 and 11. The set of all members of Σ having at least one occurrence in T is exactly the image of T, written Im T.

We are now ready to introduce some rewriting rules on $\mathscr{C}_\Sigma$ in order to compel the wished autodistributivity conditions. Clearly we have to identify trees (i.e. terms) such that the second one is obtained by replacing in the first one some subtree with the form $x\wedge(y\wedge z)$ by the corresponding subtree $(x\wedge y)\wedge(x\wedge z)$. So we set:

Definition 1.3. Let Σ be any set;

(i) for u in $\mathbb{S}$, u_Σ^+ is the partial mapping of $\mathscr{C}_\Sigma$ into itself such that T is in Dom u_Σ^+ iff $u1$ is in $|T|^\circ$ and, in this case, the image Tu_Σ^+ of T under u_Σ^+ is determined by:

$$(Tu_\Sigma^+)(v) := \begin{cases} T(v) & \text{if } u \text{ and } v \text{ are incomparable (for } \subseteq), \\ (T(u0)\wedge T(u10))\wedge(T(u0)\wedge T(u11)) & \text{if } v \text{ is } u. \end{cases}$$

(ii) ϑ_Σ denotes the monoid generated by all u_Σ^+'s for u in $\mathbb{S}$ using reverse composition (we write $\varphi\psi$ for $\psi\circ\varphi$).

It is easy to verify that this definition makes sense; the effect of u_Σ^+ is distributing the left factor $T(u0)$ to each of the right factors $T(u10)$, $T(u11)$. For instance if T_0 is, as above, $a\wedge(b\wedge a)$, T_0 is in Dom Λ_Σ^+ and $T\Lambda_\Sigma^+$ is $(a\wedge b)\wedge(a\wedge a)$.

Now things are exactly as they should be, and standard arguments show:

Proposition 1.4. *Let Σ be any set; for S, T in $\mathscr{C}_\Sigma$ write $S\rightarrow_\Sigma T$ (resp. $S\rightarrow_\Sigma^* T$) if T*

is Su_Σ^+ *for some* u *in* $\mathbb{S}$ *(resp.* T *is* $S\varphi$ *for some* φ *in* ϑ_Σ*); let* $\leftrightarrow_\Sigma$ *be the equivalence relation generated by* $\rightarrow_\Sigma^*$*; then*

(i) $\rightarrow_\Sigma^*$ *is the reflexive transitive closure of* $\rightarrow_\Sigma$ *and is a partial ordering on* $\mathscr{C}_\Sigma$ *that is compatible with* $\wedge$;

(ii) $\leftrightarrow_\Sigma$ *is a congruence with respect to* $\wedge$, and $(\mathscr{C}_\Sigma/\leftrightarrow_\Sigma, \wedge/\leftrightarrow_\Sigma)$ *is a free distributive groupoid generated by (a copy of)* Σ.

Proof. (i) If φ is in ϑ_Σ and is not the identity mapping, the cardinality of $|T\varphi|$ is strictly larger than the cardinality of $|T|$ for every T in Dom φ, so $\rightarrow_\Sigma^*$ is antisymmetric (and the converse relation $\leftarrow_\Sigma^*$ is noetherian). Next we have for all trees S, T:

$$S\wedge(Tu_\Sigma^+)=(S\wedge T)(1u)_\Sigma^+, \qquad (Su_\Sigma^+)\wedge T=(S\wedge T)(0u)_\Sigma^+,$$

so $\rightarrow_\Sigma$ and then $\rightarrow_\Sigma^*$ are compatible with $\wedge$.

(ii) $S\leftrightarrow_\Sigma T$ holds iff there exists a finite sequence $\langle U_0, \ldots, U_{2k}\rangle$ such that S is U_0, T is U_{2k} and, for $i<k$, $U_{2i}\rightarrow_\Sigma^* U_{2i+1}$ and $U_{2i+2}\rightarrow_\Sigma^* U_{2i+1}$ hold. So the compatibility of $\rightarrow_\Sigma^*$ with $\wedge$ implies the same property for $\leftrightarrow_\Sigma$. Next for all S, T, U in $\mathscr{C}_\Sigma$ we have

$$(S\wedge T)\wedge(S\wedge U)=(S\wedge(T\wedge U))\Lambda_\Sigma^+,$$

hence

$$S\wedge(T\wedge U)\leftrightarrow_\Sigma(S\wedge T)\wedge(S\wedge U)$$

holds, and $\mathscr{C}_\Sigma/\leftrightarrow_\Sigma$ with $\wedge/\leftrightarrow_\Sigma$ is a distributive groupoid. Now, for a in Σ, a is in the domain of no u_Σ^+ so a is alone in its class under $\leftrightarrow_\Sigma$. Finally let $(\mathfrak{c}, \bullet)$ be any distributive groupoid and let π be any mapping of Σ into $\mathfrak{c}$; π is extended to $\mathscr{C}_\Sigma$ in the obvious way:

$$(S\wedge T)\pi := S\pi\bullet T\pi.$$

Certainly π is compatible with $\leftrightarrow_\Sigma$ since $(\mathfrak{c}, \bullet)$ is a distributive groupoid, therefore π induces a morphism of $\mathscr{C}_\Sigma/\leftrightarrow_\Sigma$ to $\mathfrak{c}$. This morphism is unique since Σ generates $\mathscr{C}_\Sigma$. □

Before going on, we notice that most of the notions introduced above are essentially independent of the choice of a particular set Σ:

Lemma 1.5. *Assume that* Σ *is included in* Σ';

(i) *for every* u *in* $\mathbb{S}$, u_Σ^+ *is* $u_{\Sigma'}^+\restriction\mathscr{C}_\Sigma$;

(ii) *for all* S, T *in* $\mathscr{C}_\Sigma$, $S\rightarrow_\Sigma T$ *(resp.* $S\rightarrow_\Sigma^* T$, $S\rightarrow_\Sigma T$*) holds iff* $S\leftrightarrow_{\Sigma'} T$ *(resp.* $S\rightarrow_{\Sigma'}^* T$, $S\leftrightarrow_{\Sigma'} T$*) holds.*

In order to control the geometrical behaviour of the transformations in ϑ_Σ, we introduce the following notion of inheritance:

Definition 1.6. (i) For u in $\mathbb{S}$, u^+ is the partial mapping of $\mathbb{S}$ into its powerset such that v is in Dom u^+ iff v is not included in $u1$, and, in this case, the image of v

under u^+, denoted by v/u^+ is defined by:

$$v/u^+ := \begin{cases} \{v\} & \text{if } u, v \text{ are incompatible (for } \subseteq\text{) or } v \text{ includes } u11; \\ \{u01w\} & \text{if } v \text{ is } u10w; \\ \{u00w, u10w\} & \text{if } v \text{ is } u0w. \end{cases}$$

This notation is extended to subsets of $\mathbb{S}$ by defining, for A included in $\mathbb{S}$, A/u^+ to be the union of all v/u^+ for v in A provided that v/u^+ is defined for *all* v in A.

(ii) ϑ denotes the monoid generated by all u^+'s for u in $\mathbb{S}$ using reverse composition; for φ in ϑ and v in $\mathbb{S}$, the members of v/φ are called the *heirs* of v under φ.

We also extend the notations in Definitions 1.3 and 1.6 to finite sequences from $\mathbb{S}$ as follows: if α is in $\mathbb{S}^*$ (the set of all finite sequences from $\mathbb{S}$) and is nonempty, say $\alpha = \langle u_1, \dots, u_k \rangle$, then α^+ (resp. α^+_Σ) denotes $u_1^+ \dots u_k^+$ (resp. $u^+_{1\Sigma} \dots u^+_{k\Sigma}$).

When some transformation say α^+_Σ is performed on a tree S in $\mathscr{C}_\Sigma$, certain subtrees $S(v)$ of S are translated and/or several times copied, but not intrinsically modified: then v/α^+ is intended to be the set of the addresses in $S\alpha^+$ of these copies of $S(v)$. More precisely, one can show, using an easy induction on the length of α in $\mathbb{S}^*$:

Lemma 1.7. *Let α be in $\mathbb{S}^*$, and Σ be any set;*

(i) *if v/α^+ is defined, then, for every w in $\mathbb{S}$, $(vw)/\alpha^+$ is defined and is $(v/\alpha^+)w$ - where Aw stands for $\{uw: u \in A\}$;*

(ii) *for T in $\mathscr{C}_\Sigma$, T is in $\operatorname{Dom} \alpha^+_\Sigma$ iff $|T|$ is in $\operatorname{Dom} \alpha^+$; in that case, $|T\alpha^+_\Sigma|$ is $|T|/\alpha^+$, and, iff v is in $(|T| \cup |T|^\circ) \cap \operatorname{Dom} \alpha^+$, $(T\alpha^+_\Sigma)(w) = T(v)$ holds for every w in v/α^+;*

(iii) *v/α^+ is defined iff there exists some tree T such that $|T|$ contains v and $|T|/\alpha^+$ is defined.*

We immediately deduce:

Proposition 1.8. *If Σ has at least two members, then the monoid ϑ_Σ is isomorphic to the monoid ϑ.*

Proof. The mappings $\alpha \to \alpha^+$ and $\alpha \to \alpha^+_\Sigma$ are projections of $\mathbb{S}^*$ onto ϑ and ϑ_Σ respectively (we map of course the empty sequence on the identity mapping). Assume that $\alpha^+ = \beta^+$ holds: Lemma 1.7(ii) implies that $\operatorname{Dom} \alpha^+_\Sigma$ is equal to $\operatorname{Dom} \beta^+_\Sigma$; let T be in $\operatorname{Dom} \alpha^+_\Sigma$, by Lemma 1.7(ii) again, $|T\alpha^+_\Sigma|$ is equal to $|T\beta^+_\Sigma|$; finally let w be in $|T\alpha^+_\Sigma|$: there exists v in $|T|$ such that w is in v/α^+, whence

$$(T\alpha^+_\Sigma)(w) = T(v) = (T\beta^+_\Sigma)(w).$$

So $T\alpha^+_\Sigma$ and $T\beta^+_\Sigma$ coincide, and $\alpha^+_\Sigma = \beta^+_\Sigma$ holds. We get by factorization a projection of ϑ on ϑ_Σ in any case. Now assume moreover that Σ has at least two members, say

a and b, and assume that $\alpha_\Sigma^+ = \beta_\Sigma^+$ holds. Assume that υ/α^+ is defined. By Lemma 1.7(iii) we get T such that $|T|/\alpha^+$ and therefore $T\alpha_\Sigma^+$ are defined and υ is in $|T|$. If υ/β^+ were not defined, then $|T|/\beta^+$ could not be defined, so (by Lemma 1.7(ii)) $T\beta_\Sigma^+$ would not exist, a contradiction. So υ/β^+ exists. We may request moreover that υ be the only occurrence of a in T (all the other leaves of T are labelled b). As $T\alpha_\Sigma^+$ and $T\beta_\Sigma^+$ are equal, we get:

$$\upsilon/\alpha^+ = \{w \in |T\alpha_\Sigma^+|: T\alpha_\Sigma^+(w) = a\} = \upsilon/\beta^+,$$

so α^+ is equal to β^+, and the projection above is an isomorphism. □

A natural question is asking whether Proposition 1.8 holds when Σ has only one member. Some indications thereabout will be given in Section 5. For the moment, owing to Lemma 1.5 and Proposition 1.8, we shall drop the subscript Σ in the denotations of →, →*, ↔ and, assuming that Σ is a (fixed) infinite set, write α^+ for α_Σ^+.

We conclude this introductory section with the following remark: assume that $u_1^+ \dots u_k^+ = \upsilon_1^+ \dots \upsilon_m^+$ holds in ϑ, then, for every w in $\mathbb{S}$, $(wu)^+ \dots (wu_k)^+ = (w\upsilon_1)^+ \dots (w\upsilon_m)^+$ holds (use induction on w). Therefore there is no problem in defining, for φ in ϑ and w in $\mathbb{S}$, a new member $w\varphi$ of ϑ by $w\varphi := (wu_1)^+ \dots (wu_k)^+$ if φ is $u_1^+ \dots u_k^+$.

2. Commutation relations in ϑ

Our aim is now to prove the confluency of →*, i.e. to prove that, if $S \to^* T_1$ and $S \to^* T_2$ hold in $\mathscr{C}_\Sigma$, then $T_1 \to^* U$ and $T_2 \to^* U$ hold for some tree U. So, when α_1, α_2 are given in $\mathbb{S}^*$ and S in $\operatorname{Dom} \alpha_1^+ \cap \operatorname{Dom} \alpha_2^+$, we have to find β_1, β_2 such that

$$S\alpha_1^+\beta_1^+ = S\alpha_2^+\beta_2^+$$

holds. In other words, when α_1, α_2 are given in $\mathbb{S}^*$ and T in the image of $\operatorname{Dom} \alpha_2^+$ under α_1^+, we have to find β_1, β_2 such that

$$T\alpha_1^- \alpha_2^+ = T\beta_1^+\beta_2^-$$

holds, where α^- denotes the inverse mapping of α^+ (this makes sense as α^+ is one-one). So we wish to transform the sequence $\alpha_1^-\alpha_2^+$ where the 'negative' terms precede the 'positive' ones into a new sequence with inversed signs. To do that, we try to let the positive terms migrate to the left through the negative ones. In this approach, we need some commutation relations in ϑ, and the natural first step is to consider the case of sequences α_1, α_2 with lenght 1. This step is easily carried out.

Lemma 2.1. *If u, υ are incomparable members of $\mathbb{S}$, then u^+ and υ^+ commute in ϑ.*

The proof is straightforward, as u^+ and υ^+ act on disjoint subtrees of their argument. As a consequence, we notice that, if A is a (finite) set of *pairwise incom-*

parable elements of $\mathbb{S}$, the value of $u_1^+ \dots u_k^+$ of A does not depend on this enumeration; it will be denoted simply by A^+. This in particular applies to any set υ/φ, for an easy induction shows that the heirs of any point are (when defined) incomparable.

Lemma 2.2. *Assume that* υ/φ *is defined; then the following relation holds in* ϑ:

$$\upsilon^+\varphi = \varphi(\upsilon/\varphi)^+.$$

Proof. Represent φ as α^+ for some α in $\mathbb{S}^*$ and use induction on the length of α. For the basic step, i.e. $\varphi = u^+$ for some u in $\mathbb{S}$, a picture makes the formula clear. □

Proposition 2.3. *For every* u, υ, w *in* $\mathbb{S}$, *the following relations holds in* ϑ:

$$(u0\upsilon)^+(u1w)^+ = (u1w)^+(u0\upsilon)^+; \qquad u^+(u01w)^+ = (u10w)^+u^+;$$

$$u^+(u11w)^+ = (u11w)^+u^+; \qquad u^+(u00w)^+(u10w)^+ = (u0w)^+u^+;$$

$$u^+(u1)^+u^+ = (u1)^+u^+(u1)^+(u0)^+.$$

Proof. The first relation is a rewriting of Lemma 2.1, while the following three relations are particular cases of Lemma 2.2. The last one is more mysterious, but it should become more natural later and, for the moment, it can be directly verified. □

Corollary 2.4. (i) *For every* u, υ *in* $\mathbb{S}$, *there exist* φ, ψ *in* ϑ *such that* $u^+\varphi = \upsilon^+\psi$ *holds.*

(ii) *If* $S \to T_1$ *and* $S \to T_2$ *hold in* $\mathscr{C}_\Sigma$, *then* $T_1 \to^* U$ *and* $T_2 \to^* U$ *hold for some tree* U.

Proof. It suffices to notice that Proposition 2.3 provides a convenient relation for all possible mutual positions of u, υ in $\mathbb{S}$; indeed the last four relations cover all possible cases for $\upsilon \supset u$, namely $\upsilon \supseteq u10$, $\upsilon \supseteq u11$, $\upsilon \supseteq u11$, $\upsilon \supseteq u0$, and $\upsilon = u1$. The case $u \supset \upsilon$ is symmetric, the case $u = \upsilon$ is obvious, and finally the case of incomparable u, υ follows from the first relation. □

This first result is encouraging but we are far from being done. We have proved in fact the local confluency of $\to^*$, but of course the relation $\to^*$ is not noetherian and there is no reason why local confluency should imply a global one. The critical point is that the preceding corollary furnishes a method for commuting one positive term and one negative term in a sequence of transformations, but in doing so *several* new positive and negative terms can appear and the termination of an iterated application is quite problematic. However, easy experiments show that, even when starting with short expressions, very long sequences can appear: for instance the process succeeds in transforming $\Lambda^- 1^+ 1^+ 1^+ 1^+ 1^+$ into a $\beta_1^+ \beta_2^-$-sequence, but the resulting sequence has more than 10^3 terms.

So we shall in the sequel develop a new approach involving more powerful commutation relations in ϑ. This however does not dismiss any hope of a direct proof for the termination of the iterated process above - for instance by constructing some parameter with values in a well-ordered set that should decrease in the process, like in [9]. This point remains open.

Another open (and related) question is to know whether $\langle \mathbb{S}, \mathfrak{R} \rangle$ is an exact presentation of ϑ, where $\mathfrak{R}$ is the set of all relations quoted in Proposition 2.3.

We now introduce some more tools. The first one is the following natural and easy notion of an endomorphism.

Definition 2.5. (i) An *endomorphism* of $\mathscr{C}_\Sigma$ is any mapping σ of $\mathscr{C}_\Sigma$ into itself such that, for all S, T in $\mathscr{C}_\Sigma$, the following equality holds:

$$(S \wedge T)\sigma = S\sigma \wedge T\sigma;$$

the set of all endomorphisms of $\mathscr{C}_\Sigma$ will be denoted by End $\mathscr{C}_\Sigma$.

(ii) $\mathscr{C}_\Sigma^1$ denotes the subset of $\mathscr{C}_\Sigma$ made by all one-one trees (when viewed as mappings of $\mathbb{S}$ to Σ), i.e. trees with pairwise distinct labels.

Lemma 2.6. (i) *Every mapping of Σ into $\mathscr{C}_\Sigma$ can be extended to an endomorphism in a unique way*;

(ii) *if T is $S\sigma$ for some σ in* End $\mathscr{C}_\Sigma$, *then $|S|^\circ$ is included in $|T|^\circ$ and, for every v in $|S| \cup |S|^\circ$, $T(v)$ is $S(v)\sigma$; moreover, if $S\varphi$ is defined for some φ in ϑ, $T\varphi$ is defined as well and $T\varphi$ is equal to $S\varphi\sigma$*;

(iii) *conversely if S is in $\mathscr{C}_\Sigma^1$ and $|S|^\circ$ is included in $|T|^\circ$, then T is $S\sigma$ for some σ in* End $\mathscr{C}_\Sigma$;

(iv) *assume that σ, σ' are in* End $\mathscr{C}_\Sigma$ *and that for every s occuring in S there exists some φ_s in ϑ such that $s\sigma'$ is $s\sigma\varphi_s$; then the following equality holds*:

$$S\sigma' = S\sigma \prod_{s \in \operatorname{Dom} S} \left(\prod_{S(w)=s} w\varphi_s \right)$$

The proofs are easy (for (iv), use induction on S).

We introduce now a new binary operation on $\mathscr{C}_\Sigma$.

Definition 2.7. For S, T in $\mathscr{C}_\Sigma$, we let $S \otimes T$ be $T\sigma$, where σ is the endomorphism such that, for every s in Σ, $s\sigma$ is $S \wedge s$.

The effect of $\otimes$ on (S, T) is to distribute S in T as many times as possible (while Λ^+ distributes only once). For instance if S_0 is d and T_0 is $a \wedge (b \wedge a)$, $S_0 \otimes T_0$ is $(d \wedge a) \wedge ((d \wedge b) \wedge (d \wedge a))$. It should be clear that $S \wedge T \to^* S \otimes T$ holds; we shall describe precisely the way for getting $S \otimes T$ from $S \wedge T$.

Lemma 2.8. *For T in $\mathscr{C}_\Sigma$, define inductively T^+ in ϑ by*

$$T^+ := \begin{cases} \mathrm{id} & \textit{if } T \textit{ is in } \Sigma; \\ \Lambda^+(0T(0)^+)(1T(1)^+) & \textit{otherwise}; \end{cases}$$

(i) *for all T, U in $\mathscr{C}_\Sigma$, U is in* $\mathrm{Dom}\, T^+$ *iff $|T|^\circ$ is included in $|U(1)|^\circ$.*
(ii) *for all S, T in $\mathscr{C}_\Sigma$, one has*

$$S \otimes T = (S \wedge T)T^+.$$

Proof. Use induction on T. If T is in Σ, (i) and (ii) are obvious. Assume the results proved for $T(0)$ and $T(1)$; then:

$$\begin{aligned} & U \in \mathrm{Dom}\, T^+ \\ & \text{iff} \quad U \in \mathrm{Dom}\, \Lambda^+ \text{ and } U\Lambda^+ \in \mathrm{Dom}(0T(0)^+)(1T(1)^+) \\ & \text{iff} \quad 1 \in |U|^\circ \text{ and } U\Lambda^+(0) \in \mathrm{Dom}\, T(0)^+ \text{ and } U\Lambda^+(1) \in \mathrm{Dom}\, T(1)^+ \\ & \text{iff} \quad \lambda \in |U(1)|^\circ \text{ and } |T(0)|^\circ \subseteq |U\Lambda^+(0)(1)|^\circ \text{ and } |T(1)|^\circ \subseteq |U\Lambda^+(1)(1)|^\circ \\ & \text{iff} \quad \Lambda \in |U(1)|^\circ \text{ and } |T(0)|^\circ \subseteq |U(10)|^\circ \text{ and } |T(1)|^\circ \subseteq |U(11)|^\circ \\ & \text{iff} \quad |T|^\circ \subseteq |U(1)|^\circ. \end{aligned}$$

$$\begin{aligned} S \otimes T &= T\sigma \quad (\text{where } s\sigma = S \wedge s \text{ for } s \text{ in } \Sigma) \\ &= T(0)\sigma \wedge T(1)\sigma = (S \otimes T(0)) \wedge (S \otimes T(1)) \\ &= (S \wedge T(0))T(0)^+ \wedge (S \wedge T(1))T(1)^+ \\ &= (S \wedge T(0)) \wedge (S \wedge T(1))(0T(0)^+)(1T(1)^+) \\ &= (S \wedge (T(0) \wedge T(1)))\Lambda^+(0T(0)^+)(1T(1)^+) \\ &= (S \wedge T)T^+. \qquad \square \end{aligned}$$

We notice that T^+ corresponds to enumerating all points of $|T|^\circ$ using the linear ordering on $\mathbb{S}$ that extends both the inclusion and the left-right partial orderings (of course any linear extension of the inclusion would be convenient since the order of points that are incomparable with respect to $\subseteq$ does not matter owing to Lemma 2.1). In the example above, $|T_0|$ is $\{\Lambda, 1\}$, so T_0^+ is Λ^+1^+.

We are now ready to extend the results of Proposition 2.3.

Lemma 2.9. *Assume that φ, ψ are in ϑ and T is in* $\mathrm{Dom}\, \psi$; *then the following equalities hold*:

(i) $$T^+ \prod_{w \in |T|} (w0\varphi) = (0\varphi)T^+;$$

(ii) $$T^+\psi = (1\psi)(T\psi)^+.$$

Proof. (i) We apply Lemma 2.2. An easy induction shows that, for every T, the set $0/T^+$ is defined and is equal to $|T|0$ (i.e. to $\{w0\colon w \in |T|\}$): this is however natural as the intended effect of T^+ is to distribute the left factor '0' to the left of each leaf of T. By Lemma 1.7(i), we conclude that for every u, $(0u)/T^+$ is defined and is equal to $|T|0u$. So Lemma 2.2 yields

$$(0\varphi)T^+ = (0u_1)^+ \dots (0u_{k-1})^+ T^+ \prod_{w \in |T|} (w0u_k)^+.$$

So iterating the process, we get

$$(0\varphi)T^+ = T^+ \prod_{w \in |T|} (w0u_1)^+ \dots \prod_{w \in |T|} (w0u_k)^+.$$

Finally we notice that the members of $|T|$, and therefore their successors in $\mathbb{S}$, are pairwise incomparable, so applying Lemma 2.1 we may group the terms that correspond to the same w in $|T|$, getting the desired formula.

(ii) The principle is as follows: distributing the left factor everywhere in T and afterwards applying ψ is the same as first applying ψ to the right factor and then distributing the left factor at the corresponding places, i.e. in $T\psi$. Going into some detail is perhaps preferable. Let U be any member of $\operatorname{Dom} T^+\psi$. We can assume w.l.o.g. that T is in $\mathscr{C}_\Sigma^1$ (since only $|T|$ is really used), so by Lemma 2.6(iii) and 2.8(i) we know that U is $(a \wedge T)\sigma$ for some σ in $\operatorname{End} \mathscr{C}_\Sigma$ and some a in Σ with no occurrence in T. We then get, applying Lemmas 2.6(ii), 2.8(ii) and Definition 2.7,

$$UT^+ = (a \wedge T)\sigma T^+ = (a \wedge T)T^+\sigma = (a \otimes T)\sigma = T\tau\sigma,$$

where τ is defined by $s\tau := a \wedge s$ for s in Σ. So we have:

$$\begin{aligned}
UT^+\psi &= T\tau\sigma\psi = T\psi\tau\sigma \quad \text{(by Lemma 2.6(ii))} \\
&= (a \otimes T\psi)\sigma \quad \text{(by Definition 2.7)} \\
&= (a \wedge T\psi)(T\psi)^+\sigma \quad \text{(by Lemma 2.8(ii))} \\
&= (a \wedge T)(1\psi)(T\psi)^+\sigma \\
&= (a \wedge T)\sigma(1\psi)(T\psi)^+ \quad \text{(by Lemma 2.6(ii))} \\
&= U(1\psi)(T\psi)^+,
\end{aligned}$$

so U is in $\operatorname{Dom}(1\psi)(T\psi)^+$ and the desired equality holds. On the other hand, if U is in $\operatorname{Dom}(1\psi)(T\psi)^+$, $U(1)$ must be in $\operatorname{Dom}\psi$ and $U(1\psi)$ must be in $\operatorname{Dom}(T\psi)^+$, i.e. $|T\psi|^\circ$ is included in $|U(1\psi)(1)|^\circ$, that is $|U(1)\psi|^\circ$. This implies that $|T|^\circ$ is included in $|U(1)|^\circ$ (for ψ preserves inclusion), so U is in $\operatorname{Dom} T^+$. Next UT^+ is $T\sigma$ for some σ, and therefore UT^+ is in $\operatorname{Dom}\psi$: finally U is in $\operatorname{Dom} T^+\psi$, and the proof is complete. □

With Lemma 2.9, we are able to commute sequences with the three particular types T^+, 0φ and 1ψ (and therefore to transform any sequence $T^-(0\varphi)$ or $T^-(1\psi)$ into a $\beta_1^+\beta_2^-$-sequence using the terminology introduced at the beginning of this section). This however is not yet sufficient to transform an arbitrary sequence.

3. Derivation

We introduce now the key notion of the confluency proof: for every tree T, we prove the existence of a canonical sequence of trees $\langle \partial^k T; k \in \mathbb{N}\rangle$ such that $\partial^k T$ is an upper bound (w.r. to $\to^*$) of all images $T\alpha^+$'s with length(α) at most equal to k.

Definition 3.1. The mapping ∂ ('derivation') of $\mathscr{C}_\Sigma$ into itself is defined by the following inductive clauses:

$$\partial T := \begin{cases} T & \text{if } T \text{ is in } \Sigma, \\ \partial T(0) \otimes \partial T(1) & \text{otherwise} \end{cases}$$

(where $\partial T(u)$ denotes $\partial(T(u))$).

We write $\partial^k T$ for $\partial \dots \partial T$, k terms. For instance one will verify that $\partial(a \wedge (b \wedge (c \wedge d)))$ is $((a \wedge b) \wedge (a \wedge c)) \wedge ((a \wedge b) \wedge (a \wedge d))$. We shall prove the following:

Proposition 3.2. *If T is in* $\operatorname{Dom} \alpha^+$ *and k is at least the length of α, then $T\alpha^+ \to^* \partial^k T$ holds.*

Corollary 3.3. (i) *The relation $\to^*$ is confluent.*

(ii) *$T_1 \leftrightarrow T_2$ holds iff $T_1 \to^* U$ and $T_2 \to^* U$ hold for some U.*

Proof. Let α_1, α_2 be arbitrary members of $\mathbb{S}^*$ and assume that S is in $\operatorname{Dom} \alpha_1^+ \cap \operatorname{Dom} \alpha_2^+$; let k be the supremum of the lengths of α_1, α_2. By Proposition 3.2, $S\alpha_1^+ \to^* \partial^k S$ and $S\alpha_2^+ \to^* \partial^k S$ hold, and Corollary 3.3 is proved. □

The proof of Proposition 3.2 will be split into four lemmas.

Lemma 3.4. *For every T in $\mathscr{C}_\Sigma$, $T \to^* \partial T$ holds, and, moreover, if T is in* $\operatorname{Dom} \Lambda^+$, *there exists α such that ∂T is $T\alpha^+$ and Λ is the first term of α.*

Proof. Induction on T; if T is in Σ, the result is clear; assume that $\partial T(0)$ is $T(0)\varphi_0$ and $\partial T(1)$ is $T(1)\varphi_1$ for some φ_0, φ_1 in ϑ. We get

$$\begin{aligned} \partial T &= \partial T(0) \otimes \partial T(1) \\ &= (\partial T(0) \wedge \partial T(1))(\partial T(1))^+ \quad \text{(Lemma 2.8(ii))} \\ &= (T(0)\varphi_0 \wedge T(1)\varphi_1)(\partial T(1))^+ = T(0\varphi_0)(1\varphi_1)(\partial T(1))^+ \\ &= T\varphi, \end{aligned}$$

where φ is $(0\varphi_0)(1\varphi_1)(\partial T(1))^+$. If T is in $\operatorname{Dom} \Lambda^+$, $T(1)$ is not in Σ, so $(T(1))^+$ is not the identity mapping. We can therefore apply Lemma 2.9: as $\partial T(1)$ is $T(1)\varphi_1$, we get

$$\varphi = (0\varphi_0)(T(1))^+\varphi_1 = (T(1))^+ \prod_{w\in|T|} (w0\varphi_0)\cdot\varphi_1,$$

and we are done, since the first term of $T(1)^+$ is precisely Λ^+. □

Lemma 3.5. *If T in* $\mathrm{Dom}\, u^+$, *then $Tu^+ \to^* \partial T$ holds.*

Proof. Induction on (the length of) u. If u is Λ, the result was proved in Lemma 3.4. Assume that u is $0v$ and the result holds for v. Let T belong to $\mathrm{Dom}\, u^+$: certainly T is not in Σ, and $T(0)$ is in $\mathrm{Dom}\, v^+$, so $T(0)v^+ \to^* \partial T(0)$ follows from the induction hypothesis. Now we get, applying the compatibility of $\to^*$ with $\wedge$, Lemma 2.8(ii) and Lemma 3.4:

$$\begin{aligned} Tu^+ &= T(0)v^+ \wedge T(1) \to^* \partial T(0) \wedge T(1) \to^* \partial T(0) \wedge \partial T(1) \to^* \partial T(0) \otimes \partial T(1) \\ &= \partial T. \end{aligned}$$

The proof is analogous when u is $1v$. □

We are done for one-step transformations. Getting further still requests some more work.

Lemma 3.6. *If T in* $\mathrm{Dom}\,\Lambda^+$, *then $\partial T \to^* \partial(T\Lambda^+)$ holds.*

Proof. Set $U := \partial T(0)$, $V := \partial T(10)$, $W = \partial T(11)$ and define endomorphisms σ, τ, θ by $s\sigma := U \wedge s$, $s\tau := V \wedge s$, $s\theta := (U \otimes V) \wedge s$ for s in Σ. We have

$$\begin{aligned} \partial T &= U \otimes (V \otimes W) = W\tau\sigma, \\ \partial(T\Lambda^+) &= (U \otimes V) \otimes (U \otimes W) = W\sigma\theta. \end{aligned}$$

Owing to Lemma 2.6(iv), it suffices, in order to prove $\partial T \to^* \partial(T\Lambda^+)$, i.e. $W\tau\sigma \to^* W\sigma\theta$, to show that, for every s in Σ, $s\tau\sigma \to^* s\sigma\theta$ holds. Now this follows from a direct computation:

$$\begin{aligned} s\sigma\theta &= (U \wedge s)\theta = U\theta \wedge s\theta = ((U \otimes V) \wedge U)U^+ \wedge ((U \otimes V) \wedge s) \\ &= (V\sigma \wedge U)U^+ \wedge (V\sigma \wedge s) = (V\sigma \wedge U) \wedge (V\sigma \wedge s)(0U^+) \\ &= (V\sigma \wedge (U \wedge s))\Lambda^+(0U^+) = (V\sigma \wedge s\sigma)\Lambda^+(0U^+) = s\tau\sigma\Lambda^+(0U^+). \end{aligned}$$

So the proof is complete. □

Lemma 3.7. *The mapping ∂ is increasing with respect to $\to^*$.*

Proof. It suffices to show that, if T is in $\mathrm{Dom}\, u^+$, then $\partial T \to^* \partial(Tu^+)$ holds. This is proved using induction on the length of u. If u is Λ, the result has been proved in Lemma 3.6. Assume that u is $0v$ and the result is proved for v. Let T belong to $\mathrm{Dom}\, u^+$: $T(0)$ is in $\mathrm{Dom}\, v^+$, $\partial T(0) \to^* \partial(T(0)v^+)$ follows from the induction hypothesis. Now ∂T is $\partial T(1)\sigma$ and $\partial(Tu^+)$ is $\partial T(1)\tau$ where σ and τ are defined by $s\sigma := \partial T(0) \wedge s$, $s\tau := \partial(T(0)\upsilon^+) \wedge s$ for s in Σ. As $s\sigma \to^* s\tau$ holds for every s, $\partial T \to^* \partial(Tu^+)$ follows from Lemma 2.6(iv). Likewise, if u is 1υ and T is in $\operatorname{Dom} u^+$, ∂T is $\partial T(1)\sigma$ while $\partial(Tu^+)$ is $\partial(T(1)\upsilon^+)\sigma$ where $s\sigma := \partial T(0) \wedge s$, so $\partial T \to^* \partial(Tu^+)$ follows from $\partial T(1) \to^* \partial(T(1)\upsilon^+)$ and Lemma 2.6(ii). □

It is now straightforward to prove Proposition 3.2 inductively on the length of α: assume that α is $\beta^\frown\langle u\rangle$ and k is at least the length of α; if T is in $\operatorname{Dom}\alpha^+$, T is certainly in $\operatorname{Dom}\beta^+$, and $T\beta^+ \to^* \partial^{k-1}T$ implies

$$T\alpha^+ = T\beta^+u^+ \to^* \partial(T\beta^+) \to^* \partial(\partial^{k-1}T) = \partial^k T.$$

Remarks 3.8. (i) Starting from α_1, α_2 and S in $\operatorname{Dom}\alpha_1^+ \cap \operatorname{Dom}\alpha_2^+$, we get sequences β_1, β_2 such that

$$S\alpha_1^+\beta_1^+ = S\alpha_2^+\beta_2^+ = \partial^k S$$

hold, where k is the supremum of the lengths of α_1, α_2. Of course we cannot claim that the sequences β_1, β_2 constructed in this way are the shortest possible ones (they are not unique however...), but we get an upper bound for the minimal possible lengths of the 'commuting sequences'. First the (minimal) length of the α's such that ∂T is $T\alpha^+$ is approximately bounded by $(\#|T|)^2$ (where $\#A$ denotes the cardinality of A). Now the bounds for $\#|\partial T|$ are

$$\#|T| \le \#|\partial T| \le 2^{\#|T|-1}$$

and these bounds are reached (for arbitrary large trees). So the only upper bound we can expect for the lengths of the α's such that $\partial^k T$ is $T\alpha^+$ is a tower of k exponentials. These values are coherent with the 'experimental' ones.

(ii) It is natural to ask whether $\partial^k T$ is exactly a *least* upper bound for all $T\alpha^+$'s with length (α) at most k: this is not true in general.

4. Uniform confluency of $\to^*$

We proved in the preceding section that, for all φ_1, φ_2 in ϑ, and S in $\operatorname{Dom}\varphi_1 \cap \operatorname{Dom}\varphi_2$, there exist ψ_1, ψ_2 in ϑ such that $S\varphi_1\psi_1$ is equal to $S\varphi_2\psi_2$. We will now show that ψ_1 and ψ_2 above can be chosen is an uniform way that does not depend on the particular tree S. So we can enounce the following neat result (diamond property for ϑ):

Theorem 4.1. *For all φ_1, φ_2 in ϑ, there exist ψ_1, ψ_2 in ϑ such that $\varphi_1\psi_1 = \varphi_2\psi_2$ holds and, moreover,* $\operatorname{Dom}\varphi_1\psi_1$ *is exactly* $\operatorname{Dom}\varphi_1 \cap \operatorname{Dom}\varphi_2$.

The proof uses two auxiliary results. The first one is easy and provides a characterization of $\operatorname{Dom}\varphi$ for φ in ϑ.

Lemma 4.2. *For every φ in ϑ, there exists a tree S_φ in $\mathscr{C}_\Sigma$ such that T is in* Dom φ *iff $|S_\varphi|^\circ$ is included in $|T|^\circ$.*

Proof. We represent φ and α^+ and use induction on the length of α. The basic step follows from the following observation: for A included in $\mathbb{S}$ and u in $\mathbb{S}$, there exists B such that, for every T in $\operatorname{Dom} u^+$, A is included in $|Tu^+|^\circ$ iff B is included in $|T|^\circ$. This in turn is proved inductively on the length of u. □

Proposition 4.3. *If T is in $\mathscr{C}_\Sigma^1$, the mapping $\varphi \to T\varphi$ is one-one on $\{\varphi \in \vartheta$: $T \in \operatorname{Dom} \varphi\}$.*

Let us prove Theorem 4.1 from Lemma 4.2 and Proposition 4.3. By Lemma 4.2, we get trees S_1, S_2 such that T is in $\operatorname{Dom} \varphi_1 \cap \operatorname{Dom} \varphi_2$ iff $|S_1|^\circ$ and $|S_2|^\circ$ are included in $|T|^\circ$. It is easy to construct another tree S such that $|S|^\circ$ is $|S_1|^\circ \cup |S_2|^\circ$. We moreover request that S be in $\mathscr{C}_\Sigma^1$ (recall that Σ is infinite). So we are sure (by Lemma 2.6(iii)) that T is in $\operatorname{Dom} \varphi_1 \cap \operatorname{Dom} \varphi_2$ iff T is $S\sigma$ for some endomorphism σ. By Corollary 3.3, ψ_1, ψ_2 exist in ϑ such that $S\varphi_1\psi_1 = S\varphi_2\psi_2$ holds. Using Proposition 4.3, we get $\varphi_1\psi_1 = \varphi_2\psi_2$. Moreover if T is $S\sigma$, certainly T is in $\operatorname{Dom} \varphi_1\psi_1$, so $\operatorname{Dom} \varphi_1 \cap \operatorname{Dom} \varphi_2$ is included in $\operatorname{Dom} \varphi_1\psi_1$. The converse inclusion is clear, and Theorem 4.1 is proved.

We now turn to the proof of Proposition 4.3 and, first, introduce some convenient notions. The proof below is rather tedious, but no other one is known. The point is to get a criterion to prove that some particular relation $S \to^* T$ does *not* hold. Therefore we try to control certain properties that are preserved under $\to^*$.

Definition 4.4. Assume that $\mathscr{U}$ is a subset of $\mathscr{C}_\Sigma$;

(i) $\mathscr{U}$ is said to be *stable* if the following three implications hold:

(#) $S \wedge T \in \mathscr{U}$ implies $S \wedge (T \wedge U) \in \mathscr{U}$;

(##) $S \wedge T \in \mathscr{U}$ implies $S \wedge (U \wedge T) \in \mathscr{U}$;

(###) $T \in \mathscr{U}$ and $S \to^* T$ imply $S \in \mathscr{U}$;

(ii) for υ in $\mathbb{S}$ in $\mathscr{C}_\Sigma$, we say that υ is *$\mathscr{U}$-good* for T if υ is in $|T|$ and there exists w in $\mathbb{S}$ and l in $\mathbb{N}$ such that $l \geq 1$, $\upsilon = w0^l$ and $T(w) \in \mathscr{U}$ hold.

We notice that, for any distinct w, w' in $\mathbb{S}$ (and α in $\mathbb{S}^*$), the sets w/α^+ and w'/α^+ are disjoint when defined, so, for every υ, there exists at most one w such that υ is in w/α^+: such a w will be denoted by υ/α^- if it exists.

Lemma 4.5. *Assume that $\mathscr{U}$ is stable and υ is $\mathscr{U}$-good for $T\alpha^+$; then υ/α^- exists and is $\mathscr{U}$-good for T.*

Proof. It suffices to prove the result for α in $\mathbb{S}$, say $\alpha = \langle u \rangle$. As υ is in $|Tu^+|$, we know (Lemma 1.7(ii)) that υ/u^- exists and is in $|T|$. Write υ' for υ/u^- and choose

w, l witnessing for the $\mathcal{U}$-goodness of v for Tu^+. Now define w' by:

$$w' := \begin{cases} w/u^- & \text{if } w \supset u0 \text{ or } w \supset u1 \text{ or } u, w \text{ are incomparable,} \\ u & \text{if } w = u0 \text{ or } w = u1, \\ w & \text{if } w \subseteq u. \end{cases}$$

Notice that w' is always defined in this way. We claim that, for some $l' \leq l$, v' is $w'0^{l'}$ and $T(w')$ is in $\mathcal{U}$.

Case 1. w/u^- is defined. Then w is in w'/u^+, so $T(w')$ is equal to $(Tu^+)(w)$, and therefore is in $\mathcal{U}$, while $w0^l/u^-$ is $w'0^l$ (using Lemma 1.7(i)), so v' is exactly $w'0^l$.

Case 2. $w = u0$. Then $T(w')$ is $T(u)$, that is $(Tu^+)(w0) \wedge ((Tu^+)(w1) \wedge T(u11))$; $(Tu^+)(w0) \wedge (Tu^+)(w1)$ is assumed to be in $\mathcal{U}$, so (#) implies that $T(u)$ is in $\mathcal{U}$ as well. Moreover, v' is $u0^{l-1}$, i.e. $w'0^l$.

Case 3. $w = u1$. Then $T(w')$ is $T(u)$, that is $(Tu^+)(w0) \wedge (T(u10) \wedge (Tu^+)(w1))$ and, as above, we conclude that $T(u)$ is in $\mathcal{U}$ using (##). Moreover, v' is $u0^l$, i.e. $w'0^l$.

Case 4. u is wu_0 for some u_0. Then $(Tu^+)(w)$ is $(T(wu_0)^+)(w)$, that is $T(w)u_0^+$, so $T(w) \to^* (Tu^+)(w)$ holds. By (###) we conclude that $T(w)$ (i.e. $T(w')$) is in $\mathcal{U}$. Next we notice that either v is incomparable with u or v includes $u00$ (because v is in $|Tu^+|$ and v is $w0^l$ with $l \geq 1$). In the first case, we have $v' = v = w0^l = w'0^l$; in the second one, we have $v' = w0^{l-1} = w'0^{l-1}$. So the proof is complete.

Now the point is the following technical result:

Lemma 4.6. *Let φ be any member of ϑ; assume that for some σ in* End $\mathcal{C}_\Sigma$ *the tree $S\sigma$ is in $\mathcal{C}_\Sigma^1 \cap$* Dom φ *and that $S\sigma\varphi$ is in the image of σ; then S itself must lie in* Dom φ.

Proof. We assume that $S\sigma$ is in $\mathcal{C}_\Sigma \cap \operatorname{Dom} \varphi$ but S is not in $\operatorname{Dom} \varphi$, and prove that $S\sigma\varphi$ cannot be in the image of σ provided that $a\sigma$ is in $\mathcal{C}_\Sigma^1$ for every a in $\operatorname{Im} S$. First choose a decomposition $\alpha^+ u^+ \beta^+$ of φ such that S is in $\operatorname{Dom} \alpha^+$ but $S\alpha^+$ is not in $\operatorname{Dom} u^+$: $S\sigma\varphi$ is equal to $S\alpha^+\sigma u^+\beta^+$ (Lemma 2.6(ii)), and the pair $(S\alpha^+, u^+\beta^+)$ satisfies the same hypotheses as the pair (S, φ), so we may replace S by $S\alpha^+$ and φ by $u^+\beta^+$. In other words, we may assume without loss of generality that α^+ is the identity. Now $S\sigma$ is certainly in $\operatorname{Dom} u^+$ (for $S\sigma$ is in $\operatorname{Dom} \varphi$), while S is not: hence $u1$ lies in $|S\sigma|^\circ \setminus |S|^\circ$. Let w be the unique member of $|S|$ that is included in $u1$, and let a be $S(w)$. Let l, m be the integers (>0) such that $u10^l$ and $u1^{m+1}$ are in $|S\sigma|$, and let b, c be the values of $S(u10^l)$, $S(u1^{m+1})$ respectively (see Fig. 1).

The assumption of $a\sigma$ being in $\mathcal{C}_\Sigma^1$ implies that b and c must be distinct, and that moreover c occurs neither in $S\sigma(u10)$ nor in $S\sigma(u0)$. It follows that c does not occur in $S\sigma u^+(u0)$, so, if we let $\mathcal{U}$ be the set of all trees in which c occurs at least once, $u010^{l-1}$ is an occurrence of b in $S\sigma u^+$ that is not $\mathcal{U}$-good for $S\sigma u^+$. Clearly $\mathcal{U}$ is stable, so Lemma 4.5 implies that at least one occurrence of b in $S\sigma u^+\beta^+$ cannot

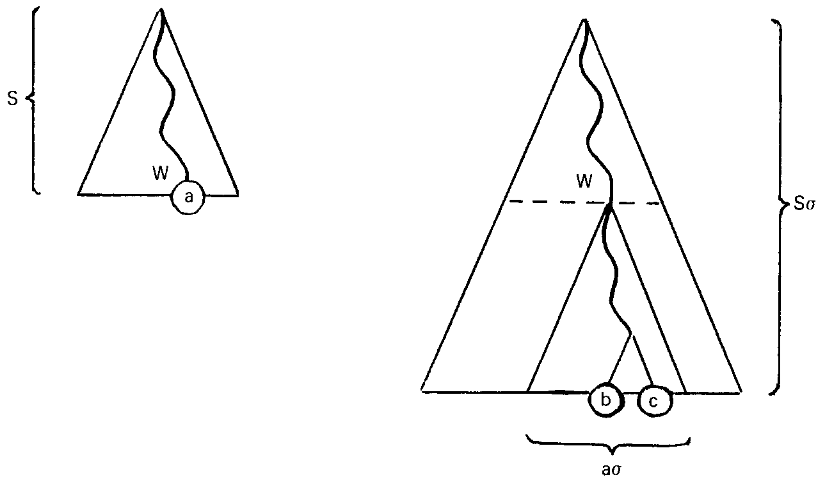


Fig. 1.

be $\mathscr{U}$-good for $s\sigma u^+\beta^+$. But this prevents $S\sigma u^+\beta^+$ from being in the image of σ since any occurrence of b in a tree $U\sigma$ with Im U included in Im S appears in fact in a subtree equal to $a\sigma$ (for b does not occur in any other $s\sigma$ with s occuring in S) and therefore is $\mathscr{U}$-good for $U\sigma$. □

We can now establish Proposition 4.3. Assume that T is in $\mathscr{C}^1_\Sigma \cap \operatorname{Dom}\varphi \cap \operatorname{Dom}\psi$ and $T\varphi = T\psi$ holds. By Lemma 4.2, we get S in $\mathscr{C}^1_\Sigma$ such that, for every U in $\mathscr{C}_\Sigma$, $u\varphi$ is defined iff $|S|^\circ$ is included in $|U|^\circ$, i.e. (Lemma 2.6(iii)) iff U is $S\tau$ for some endomorphism τ. So in particular T must be $S\sigma$ for some σ and we get (Lemma 2.6(ii))

$$S\sigma\varphi = T\varphi = T\psi = S\sigma\psi = S\psi\sigma.$$

So, as $S\sigma$ is in $\mathscr{C}^1_\Sigma$, Lemma 4.6 forces S itself to be in Dom φ, and then we get $S\varphi\sigma = S\psi\sigma$.

Now we are sure that Im $s\sigma$ and Im $s'\sigma$ are disjoint for distinct s, s' occuring in S; an easy induction shows that in this case $S\varphi\sigma = S\psi\sigma$ implies $S\varphi = S\psi$. Finally, if U is any member of Dom ψ, U is $S\tau$ for some τ, so U is in Dom φ and we have

$$U\varphi = S\tau\varphi = S\varphi\tau = S\psi\tau = S\tau\psi = U\psi.$$

A symmetric proof would show that Dom ψ is included in Dom φ, so the equality holds, and we are done.

5. Getting φ from T and $T\varphi$

It seems that the word problem for ↔ is a difficult question. The aim of this last section is to discuss the connection between various natural questions about ↔, $\rightarrow^*$

and ϑ that could be viewed as first steps toward this word problem. These questions are related with the problem of recognizing a member φ of ϑ when only a single pair $(T, T\varphi)$ is given.

Lemma 5.1. *The following statements are equivalent*:

($\mathrm{C_i}$) *If* $|T_1|$ *and* $|T_2|$ *are equal, then* $T_1 \leftrightarrow T_2$ *holds* (*if and*) *only if* T_1 *and* T_2 *are equal*;

($\mathrm{C_{ii}}$) *For any* T *in* $\mathscr{C}_\Sigma$, *the mapping* $\varphi \to |T\varphi|$ *is one-one on* $\{\varphi \in \vartheta\colon T \in \mathrm{Dom}\,\varphi\}$;

($\mathrm{C_{iii}}$) *For any* T *in* $\mathscr{C}_\Sigma$, *the mapping* $\varphi \to T\varphi$ *is one-one on* $\{\varphi \in \vartheta\colon T \in \mathrm{Dom}\,\varphi\}$;

($\mathrm{C_{iv}}$) *For any nonempty set* Σ, *the monoid* ϑ_Σ *is isomorphic to* ϑ.

Proof. ($\mathrm{C_i}$) $\Rightarrow$ ($\mathrm{C_{ii}}$). Assume $|T\varphi_1| = |T\varphi_2|$. Choose S in $\mathscr{C}_\Sigma^1$ such that $|S|$ is equal to $|T|$. Then $S\varphi_1, S\varphi_2$ are defined and clearly we have $|S\varphi_1| = |T\varphi_1| = |T\varphi_2| = |S\varphi_2|$ and $S\varphi_1 \leftrightarrow S\varphi_2$. So by ($\mathrm{C_i}$) we deduce $S\varphi_1 = S\varphi_2$ and by Proposition 4.3 we conclude $\varphi_1 = \varphi_2$.

($\mathrm{C_{ii}}$) $\Rightarrow$ ($\mathrm{C_{iii}}$). Obvious.

($\mathrm{C_{iii}}$) $\Rightarrow$ ($\mathrm{C_{iv}}$). Owing to Proposition 1.8, the only interesting case is when Σ has only one member, say a. So assume $\alpha_\Sigma^+ = \beta_\Sigma^+$. Choose T in $\mathscr{C}_\Sigma \cap \mathrm{Dom}\,\alpha^+ \cap \mathrm{Dom}\,\beta^+$; then we get

$$T\alpha^+ = T\alpha_\Sigma^+ = T\beta_\Sigma^+ = T\beta^+,$$

so by ($\mathrm{C_{iii}}$) we have $\alpha^+ = \beta^+$, i.e. $\alpha^+ \to \alpha_\Sigma^+$ is one-one, and ϑ_Σ is isomorphic to ϑ.

($\mathrm{C_{iv}}$) $\Rightarrow$ ($\mathrm{C_i}$). Assume that T_1, T_2 are in some $\mathscr{C}_\Sigma$, and that $|T_1| = |T_2|$ and $T_1 \leftrightarrow T_2$ hold; there exist φ_1, φ_2 in ϑ_Σ such that $T_1\varphi_1$ and $T_2\varphi_2$ are equal. Choose any a in Σ, and define σ to map every member of Σ to a: $T_1\sigma$ and $T_2\sigma$ are equal, as well as $T_1\sigma\varphi_1$ and $T_2\sigma\varphi_2$. It follows that $\varphi_1 \restriction \mathscr{C}_{\{a\}}$ and $\varphi_2 \restriction \mathscr{C}_{\{a\}}$ are equal, so, if ($\mathrm{C_{iv}}$) is assumed and therefore $\vartheta_{\{a\}}$ is isomorphic to ϑ_Σ, φ_1 and φ_2 itself are equal, and finally T_1, T_2 are equal, i.e. ($\mathrm{C_i}$) holds. □

Although we conjecture that ($\mathrm{C_i}$)–($\mathrm{C_{iv}}$) are true, we are not able to prove them presently; we shall only establish a very paradoxical consequence of their negation.

Proposition 5.2. *If* ($\mathrm{C_i}$)–($\mathrm{C_{iv}}$) *are false, then there exists two trees* S, T *and an integer* $l \geq 1$ *such that* $S \to^* T$, $S \to^* T(0^l)$, *and therefore* $T \leftrightarrow T(0^l)$ *hold.*

The only known fact is that $l = 1$ is impossible in the formula above (the proof uses an auxiliary groupoid, see [5]). Before proving Proposition 5.2, we state two lemmas:

Lemma 5.3. *If* $S \to^* T$ *holds, then for every* k *such that* $S(0^k)$ *is defined, there exists* $l \geq k$ *such that* $S(0^k) \to^* T(0^l)$ *holds.*

Lemma 5.4. *For every* v *in* $\mathbb{S}$, *there exists* φ *in* ϑ *such that*

(i) *υ/φ exists and is $\{0^k1^l\}$ for some k, l;*

(ii) *for w on the left of υ, w/φ exists and contains exactly one point on the left of 0^k1^l; moreover the left-right ordering of various such w's is the same as the left-right ordering of their left heirs mentioned above;*

(iii) *for w on the right of υ, w/φ exists and contains no point on the left of 0^k1^l.*

Proof. Use induction on the number of inversions in υ, i.e. the number of pairs $\dots1\dots0\dots$ that can be extracted from υ. If υ is $\upsilon'10\upsilon''$, applying υ'^+ leads to $\upsilon/\upsilon'^+ = \{\upsilon'01\upsilon''\}$, and $\upsilon'01\upsilon''$ has one inversion less than υ. Moreover, conditions (ii) and (iii) are preserved under the action of υ'^+, so we can iterate the process. □

We turn to the proof of Proposition 5.2. Assume that (C$_\text{l}$) is false, and choose S_1, S_2 in $\mathscr{C}_\Sigma$ such that $|S_1| = |S_2|$, $S_1 \leftrightarrow S_2$ and $S_1 \neq S_2$ holds. Let υ be the leftmost point in $|S_1|$ such that $S_1(\upsilon)$, say a_1, is not $S_2(\upsilon)$, say a_2. Using Lemma 5.4, we get

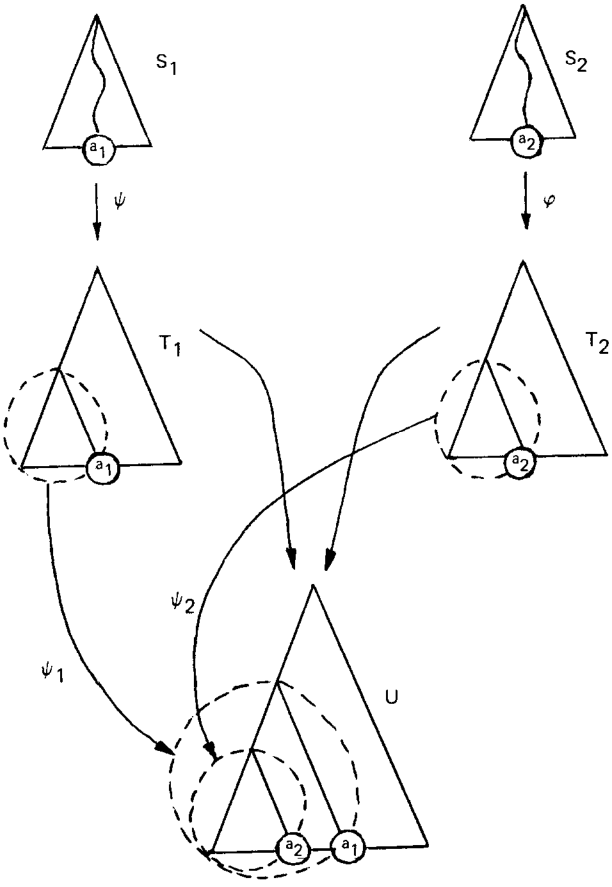


Fig. 2.

φ in ϑ such that v/φ is $\{0^k1^l\}$ and (ii), (iii) hold. Set $T_1 := S_1\varphi$, $T_2 := S_2\varphi$. Clearly we have $|T_1| = |T_2|$, $T_1 \leftrightarrow T_2$, $T_1 \neq T_2$ and the leftmost discrepancy between T_1 and T_2 is at 0^k1^l, for all points on the left of 0^k1^l come from points on the left of v in S. It follows that the only discrepancy between $T_1(0^k)$ and $T_2(0^k)$ is their rightmost label, namely a_1 for $T_1(0^k)$ and a_2 for $T_2(0^k)$ (Fig. 2).

Now $T_1 \leftrightarrow T_2$ holds so there exists some U such that $T_1 \to^* U$ and $T_2 \to^* U$ hold. According to Lemma 5.3, there exist ψ_1, ψ_2 in ϑ and l_1, l_2 in $\mathbb{N}$ such that $U(0^{l_i})$ is $T_i(0^k)\psi_i$ for $i = 1, 2$. Notice that $l_1 = l_2$ is impossible, for it implies $T_1(0^k) \leftrightarrow T_2(0^k)$ and this contradicts the fact that $T_1(0^k)$ and $T_2(0^k)$ have distinct rightmost labels and that the rightmost labels of the trees are preserved under $\to^*$ and therefore under $\leftrightarrow$. We assume $l_1 < l_2$, set $S := T_2(0^k)$ and let T be the result of replacing in $U(0^{l_1})$ the rightmost occurrence of a_1 by a_2. Certainly $U(0^{l_2})$ is $T(0^l)$, where l is $l_2 - l_1$, so we have $T(0^l) = S\psi_2$. Finally, we deduce $T = S\psi_1$ from $U(0^{l_1}) = T_1(0^k)\psi_1$ for the only changes between these equalities of trees concern the rightmost labels. So $S \to^* T$ and $S \to^* T(0^l)$ are proved, and the proof of Proposition 5.2 is carried out.

We conclude this paper with the proof of a particular case of ($\mathrm{C_{ii}}$). Instead of considering restrictions to particular trees as in Proposition 4.3 (which proves the instances of ($\mathrm{C_i}$) and ($\mathrm{C_{iii}}$) that correspond to trees in $\mathscr{C}^1_\Sigma$), we consider now restrictions to particular subsets of ϑ.

Definition 5.5. Let ϑ_1 be the submonoid of ϑ generated by all $(1^k)^+$'s for $k \geq 0$ (1^0 denotes Λ).

The family ϑ_1 is interesting because any member of ϑ can be written as a product of terms in ϑ_1 and in incomparable translated copies of ϑ_1.

Lemma 5.6. (i) *Any member of ϑ can be written as $\varphi(0\varphi_0)(10\varphi_1)\dots(1^n0\varphi_n)$ with φ in ϑ_1 (and $\varphi_0, \dots, \varphi_k$ in ϑ)*;

(ii) *Any member of ϑ_1 can be written as $(1^{k_1})^+ \dots (1^{k_n})^+$ with $k_i \leq k_{i+1} + 1$ for every i.*

Of course in (i), $\varphi_0, \dots, \varphi_n$ can in turn be written using ϑ_1. Notice that the writing may not be unique, for $\Lambda^+1^+\Lambda^+$ and $(1^+\Lambda^+1^+)0^+$ are two writings of the same member of ϑ in the form above.

Proof. (i) Start with any nonempty sequence α; our aim is to let the terms $(1^k)^+$ migrate to the left in α^+. We just have to cross terms like $(1^j0w)^+$, and therefore we use the following relations (established in 2.3):

$$(1^j0w)^+(1^k)^+ = \begin{cases} (1^k)^+(1^j0w)^+ & \text{if } j \geq k+2 \text{ or } j < k, \\ (1^k)^+(1^k01w)^+ & \text{if } j = k+1, \\ (1^k)^+(1^k00w)^+(1^{k+1}0w)^+ & \text{if } j = k. \end{cases}$$

The migrating term $(1^k)^+$ is not multiplied, so the process terminates, and one gets $\alpha^+ = \varphi\beta^+$ for some φ in ϑ_1 and β such that every term in β contains at least one zero. Using Lemma 2.1, it is then easy to group the terms of β in the wished form.

(ii) Represent $(1^{k_1})^+ \dots (1^{k_n})^+$ by the sequence $\langle k_1, \dots, k_n\rangle$ in $\mathbb{N}^*$ and let ϱ_i be the partial mapping of $\mathbb{N}^*$ into itself defined by

$$\varrho_i\langle k_1 \dots k_n\rangle = \langle k_1, \dots, k_{i-1}, k_{i+1}, k_i, k_{i+2}, \dots, k_n\rangle \quad \text{if } n \geq i+1 \text{ and } k_i \geq k_{i+1}+2.$$

Let ↲ be the reflexive transitive closure of the union of all ϱ_i's for $i \geq 0$. Then ↲ is a noetherian relation on $\mathbb{N}^*$, for the parameter ν defined by $\nu\langle k_1 \dots k_n\rangle = \sum (n-i)k_i$ decreases under ↲. Next ↲ is a confluent relation: it suffices to verify local confluency. Now ϱ_i and ϱ_j commute if $|i-j|$ is at least 2. The only nontrivial case concerns ϱ_i and ϱ_{i+1}, for instance ϱ_0 and ϱ_1. If $\langle k_0, k_1, k_2, \dots\rangle$ is in $\operatorname{Dom}\varrho_0 \cap \operatorname{Dom}\varrho_1$, certainly $k_1 \geq k_2+2$ and $k_0 \geq k_1+2$ hold, and one verifies that $\varrho_1\varrho_0\varrho_1 = \varrho_0\varrho_1\varrho_0$ holds. So (as in Sections 2 and 3 for $\to^*$) we conclude that the relation ↲ is confluent. Therefore it satisfies the Church–Rosser property and we get for every sequence a normal form $\langle k_1, \dots, k_n\rangle$ with $k_i \leq k_{i+1}+1$ for every $i<n$. This reduction translates to ϑ_1, since $(1^k)^+(1^{k'})^+ = (1^{k'})^+(1^k)^+$ holds whenever k' is $\geq k+2$. □

Proposition 5.7. *For any T in $\mathscr{C}_\Sigma$, the mapping $\varphi \to |T\varphi|$ is one-one on $\{\varphi \in \vartheta_1: T \in \operatorname{Dom}\varphi\}$;*

In fact, we shall prove the following technical form:

Lemma 5.8. *Let ϑ_1^- be the submonoid of ϑ_1 made by all terms whose reduced writing (in the sense of Lemma 5.6(ii)) ends with Λ^+; then the mappings:*

$$\varphi \to |T\varphi| \ \textit{on} \ \{\varphi \in \vartheta_1: T \in \operatorname{Dom}\varphi\}$$

and

$$\varphi \to |(T\varphi)(0)| \ \textit{on} \ \{\varphi \in \vartheta_1^-: T \in \operatorname{Dom}\varphi\}$$

are one-one.

Proof. We first establish some auxiliary formulas. Assume that φ is in ϑ_1; then the reduced writing of φ (according to Lemma 5.6(ii)) has the following form:

$$\varphi = (1\varphi_0)\Lambda^+(1\varphi_1)\Lambda^+ \dots \Lambda^+(1\varphi_n)$$

where $\varphi_0, \dots, \varphi_{n-1}$ are in ϑ_1^- and φ_n is in ϑ_1; moreover φ is in ϑ_1^- iff φ_n is the identity mapping. Assume that $T\varphi$ is defined, and put:

$$T_0 := T; \qquad T_{i+1} := T_i(1\varphi_i)\Lambda^+ \quad \text{for } 0 \leq i < n;$$

we claim that the following holds:

$$T\varphi(0^{n+1}) = T(0); \qquad T\varphi(0^{n-1}1) = (T_i(1)\varphi_i) \quad \text{for } 0 \leq i < n;$$

$$T\varphi(1) = T_n(1)\varphi_n.$$

These formulas are proved inductively on n. If n is 0, i.e. φ is $1\varphi_0$, then clearly $T\varphi(0)$ is $T(0)$ and $T\varphi(1)$ is $T(1)\varphi_0$. Now assume the formula proved for ψ with corresponding parameter $\leq n-1$ and let φ be as above. Let ψ be $(1\varphi_0)\Lambda^+ \dots \Lambda^+(1\varphi_{n-1})$. If T is in $\operatorname{Dom}\varphi$, certainly T is in $\operatorname{Dom}\psi$ and, for $0 \leq i < n-1$, the associated T_i's coincide. As $T\varphi$ is $T\psi\Lambda^+(1\varphi_n)$, we get using the induction hypothesis:

$$
\begin{aligned}
&T\varphi(0^{n+1}) = T\psi\Lambda^+(0^{n+1}) = T\psi(0^n) = T(0),\\
&T\varphi(0^{n-i}1) = T\psi\Lambda^+(0^{n-i}1) = T\psi(0^{n-1-i}1) = (T_i(1)\varphi_i)(0) \quad \text{for } 0 \leq i < n-1,\\
&T\varphi(01) = T\psi\Lambda^+(01) = T\psi(10) = T\psi(1)(0) = (T_{n-1}(1)\varphi_{n-1})(0),\\
&T\varphi(1) = T_n(1\varphi_n)(1) = T_n(1)\varphi_n.
\end{aligned}
$$

So the claim is proved. Now we shall prove that, starting from T and $|T\varphi|$, we are able to find the value of φ, i.e. the values of n and $\varphi_0, \dots, \varphi_n$ as above. The proof uses induction on $\lambda(T)$, defined to be the length of the rightmost branch of T. First we recall that λ is invariant under $\rightarrow$ (and therefore under $\rightarrow^*$). If $\lambda(T)$ is 0 or 1, T is in the domain of no φ in ϑ, so there is nothing to prove. In any case, we notice that Λ^+ increments the length of the leftmost branch and, therefore, when $|T|$ and $|T\varphi|$ (or only $|T(0)|$ and $|T\varphi(0)|$) are given, the integer n above is exactly the difference between the lengths of the left branches of $T\varphi(0)$ and $T(0)$. It follows that the result is proved for $\lambda(T) = 2$, for in that case the only φ's in ϑ such that $T\varphi$ is defined are precisely the Λ^{+n}'s.

Assume that the result of the lemma is proved for all S with $\lambda(S) < \lambda(T)$, and assume that T and $|T\varphi|$ are given. First n is computed as above. Next, using the formulas established at the beginning, we get:

$$|(T(1)\varphi_0)(0)| = |T\varphi(0^n 1)|.$$

As $T(1)$ and $|T\varphi(0^n 1)|$ are known, and φ_0 is in ϑ_1^-, the induction hypothesis asserts that φ_0 is determined, for $\lambda(T(1))$ is $\lambda(T) - 1$. The formulas also give:

$$|(T_1(1)\varphi_1)(0)| = |T\varphi(0^{n-1}1)|.$$

But now, as φ_0 is known, T_1 is determined, $|T\varphi(0^{n-1}1)|$ is given, and φ_1 is in ϑ_1^-, so the induction hypothesis asserts that φ_1 is determined, for $\lambda(T_1(1))$ is still $\lambda(T) - 1$. And the process goes on.... At the end, φ_{n-1} is determined from T_{n-1} and $|T\varphi(01)|$. Finally, $T\varphi(1)$ is $T_n(1)\varphi_n$, so φ_n is determined from T_n and $|T\varphi(1)|$. If φ is in ϑ_1^-, the last step is avoided, and therefore only $|T\varphi(0)|$ is used in the algorithm above. So the proof is complete. □

The previous proof is surprising for it does not only establish that $\varphi \rightarrow T\varphi$ is one-one on ϑ_1 but it also provides an *effective* algorithm that computes φ from $|T|$ and $|T\varphi|$. The existence of such an algorithm in the general case is a fascinating question. A possible recursive approach could try to compute from $|T|$ and $|T\psi|$ a member φ of ϑ_1 such that φ is (the) left factor of ψ as provided in Lemma 5.6(i).

We just notice that the *length* of such a φ is easily determined. For, define $\mu : \mathscr{C}_\Sigma \to \mathbb{N}$ by

$$\mu(T) := \begin{cases} 0 & \text{if } T \text{ is in } \Sigma, \\ \lambda(T(0)) + \mu(T(1)) & \text{otherwise.} \end{cases}$$

It will be immediately proved that $\mu(Tu^+)$ is $\mu(T)+1$ if u^+ is in ϑ_1, and is $\mu(T)$ otherwise. So μ is a counter for the number of transformations of ϑ_1 that are performed (and therefore in the writing of Lemma 5.6(i) the length of φ is uniquely determined).

Note added in proof. Further results on the word problem in free distributive groupoids are announced in P. Dehornoy, Sur la structure des gerbes libres, C.R. Acad. Sci. Paris Sér. I 309 (1989) 143–148.

References

[1] N. Bourbaki, Algèbre I (Hermann, Paris, 1970).

[2] R. Bruck, A Survey of Binary Systems (Springer, Berlin, 1958).

[3] P. Dehornoy, Infinite products in monoids, Semigroup Forum 34 (1986) 21–68.

[4] P. Dehornoy, Π_1^1-complete families of elementary embeddings, Ann. Pure Appl. Logic 3 (1988) 257–287.

[5] P. Dehornoy, Algebraic properties of the shift mapping, Proc. Amer. Math. Soc., submitted.

[6] R. Dougherty, Notes on critical points of elementary embeddings, Circulated notes, 1988.

[7] D. Joyce, A classifying invariant of knots, the knot quandle, J. Pure Appl. Algebra 23 (1982) 37–66.

[8] T. Kepka, Notes on left distributive groupoids. Acta Univ. Carolinae Math. Phys. 22 (1981) 23–37.

[9] D.E. Knuth and P.B. Bendix, Simple word problems in universal algebras, in: J. Leech, ed., Computational Problems in Abstract Algebra (Pergamon Press, Oxford, 1970) 263–297.

[10] Y. Moschovakis, Descriptive Set Theory (North-Holland, Amsterdam, 1980).

[11] R. Solovay, W. Reinhardt and A. Kanamori, Strong axioms of infinity and elementary embeddings, Ann. Math. Logic. 13 (1978) 73–116.

[12] J-P. Soublin, Etude algébrique de la notion de moyenne, J. Math. Pures Appl. 50 (1971) 253–264.

[13] S. Stein, Left distributive quasigroups, Proc. Amer. Math. Soc. 10 (1959) 577–578.