ABOUT THE IRREFLEXIVITY HYPOTHESIS FOR FREE LEFT DISTRIBUTIVE MAGMAS

PATRICK DEHORNOY *

Abstract. An important combinatorial statement about free left distributive structures, the irreflexivity hypothesis, has been proved by R. Laver using a large cardinal axiom. We discuss here another approach that could, if completed, lead to a new proof independent of any set theoretical assumption.

A left distributive magma—or LD-magma—will be any set endowed with a binary law satisfying the left distributivity identity

$$x(yz) = (xy)(xz).$$

The interest for (free) LD-magmas was emphasized by the study of the iterations of an elementary embedding of a rank into itself in set theory and the conjecture that the structure obtained in this way is actually a free (monogenic) LD-magma. This conjecture has been proved in 1989 by Richard Laver ([La]); an alternative proof in given in [De4]. Both proofs make an intensive use of the relation of being a left factor in LD-magmas.

DEFINITION. Let $\mathfrak{g}$ be a LD-magma, and x, y belong to $\mathfrak{g}$; write $x <_L^{\mathfrak{g}} y$ if, and only if, there exists a (positive) integer p and a finite sequence $z_1, z_2, \ldots, z_p$ in $\mathfrak{g}$ such that y is equal to $(\cdots((xz_1)z_2)\cdots)z_p$.

The statement we shall discuss here is the

IRREFLEXIVITY HYPOTHESIS (IH). *Let $\mathfrak{f}$ be the free monogenic LD-magma; then $<_L^{\mathfrak{f}}$ is an irreflexive relation.*

This property proved to be crucial in the study of free LD-magmas. In particular, the following was proved independently in [De2], and in [La1] (for the monogenic case):

PROPOSITION. *If IH is true, then for any set Σ, the word problem for the free LD-magma generated by Σ is decidable; also every free LD-magma admits left cancellation.*

* This work was supported in part by a CNRS grant PRC mathématiques et informatique.

The point in the proofs is that $<_L^{\mathfrak{f}}$ is a linear ordering on $\mathfrak{f}$. However the irreflexivity property is clearly preserved under projection, so that if $\mathfrak{g}$ is any LD-magma such that $<_L^{\mathfrak{g}}$ is irreflexive, then $<_L^{\mathfrak{f}}$ must be irreflexive too. It follows moreover that (if $\mathfrak{g}$ is monogenic) it must be free as well, and this is the way R. Laver proves that the iterations of an elementary embedding make a free LD-magma.

PROPOSITION (Laver). *Assume that j is an elementary embedding of a rank V_λ into itself; let $\mathfrak{a}^j$ be the structure generated by j using the operation $ik := \bigcup_{\alpha<\lambda} i(k{\restriction}V_\alpha)$; then $<_L^{\mathfrak{a}^j}$ is irreflexive—and therefore $\mathfrak{a}^j$ is free, and* IH *is true.*

Let EE be the large cardinal axiom "there exists an elementary embedding of a rank into itself". The irreflexivity hypothesis is thus proved under EE—and therefore such natural questions about free LD-magmas as decidability of the word problem or left cancellation are proved under EE. There is a surprising contrast between the (very) large set theoretical hypothesis EE and the algebraic and, more or less, finitistic properties of LD-magmas that are, up to now, established under EE too. Though no metamathematics is known to force it, it seems likely that the axiom EE could be dropped from the proofs—and, at first, from the proof of the key statement IH.

Owing to the preservation of irreflexivity under projection, the most natural way for proving IH would be to exhibit some particular LD-magma $\mathfrak{g}$ such that $<_L^{\mathfrak{g}}$ is irreflexive—or, at least, satisfies $x \not<_L^{\mathfrak{g}} x$ for sufficiently many x's. Unfortunately, little is known about monogenic LD-magmas : most of the (numerous) examples of LD-magmas are in fact idempotent, so they give rise only to trivial monogenic structures. In [De3], a nontrivial (infinite) monogenic LD-magma $\mathfrak{d}$ is constructed that satisfies "1-irreflexivity": $x = xz_1$ is impossible in $\mathfrak{d}$. But no extension to 2-irreflexivity ("$x = (xz_1)z_2$ is impossible") or more is known.

The aim of this paper is to develop the scheme of a proof for IH that is connected with the study of a certain structural monoid associated with the distributive structures. This proof is *not* complete, so that the conjecture is still open. Nevertheless we hope that the reduced form we obtain for IH in this way can be considered a progress toward a complete solution.

1. General framework.

The general setting will be the one of [De1]. We start with any nonempty set Σ (we shall assume that Σ has at least two elements), and let $\mathcal{T}(\Sigma)$ be the free magma generated by Σ, i.e., the set of all terms constructed from Σ using some fixed binary operator, say $*$. It will be convenient to use here the *right Polish notation*, so that the product of two terms S, T is denoted by $ST*$. Now the free LD-magma generated by Σ is the quotient of $\mathcal{T}(\Sigma)$ under the least congruence $\equiv$ that forces the left distributivity condition, i.e., that satisfies, for every S, T, U in $\mathcal{T}(\Sigma)$,

$$STU{*}{*} \equiv ST{*}SU{*}{*}.$$

The main tool introduced in [De1] to analyse this congruence $\equiv$ is a monoid ϑ generated by some elementary term transformations. To describe it easily in this nonassociative framework, it is convenient to think to terms as to *binary trees* (with leaves indexed by Σ): thus the subterms of a given term can be specified using any system of addresses in a binary tree, for instance finite sequences of 0's and 1's describing the path in the corresponding tree to reach the current node from the root of the tree (0 meaning "going to the left," 1 meaning "going to the right").

DEFINITION. Let $\mathbf{S}$ be the set of all finite sequences of 0's and 1's; for w in $\mathbf{S}$, and S in $\mathcal{T}(\Sigma)$, $S_{/w}$ denotes the subterm of S whose root has address w (if it exists); the set of all addresses w such that $S_{/w}$ exists is called the *support* of S and written $\mathbf{Supp}(S)$; the set of all addresses w such that $S_{/w}$ exists is denoted by $\mathbf{Supp}^+(S)$.

EXAMPLE. Let S be $abcd{*}{*}{*}$; then $S_{/0}$ is a, $S_{/1}$ is $bcd{*}{*}$; $\mathbf{Supp}(S)$ is $\{0, 10, 110, 111\}$, while $\mathbf{Supp}^+(S)$ is $\{0, 10, 110, 111, 11, 1, \Lambda\}$, where Λ denotes the empty sequence (the address of the root in any tree). Notice that $\mathbf{Supp}^+S$ is (in any case) the closure of $\mathbf{Supp}S$ under word prefixing.

DEFINITION. i) For w in $\mathbf{S}$, define a partial mapping w^+ of $\mathcal{T}(\Sigma)$ into itself by:

S is in $\mathbf{Dom}w^+$ if, and only if, $wu0, w10, w11$ are in $\mathbf{Supp}(S)$, and, in this case, the value of w^+ on S is obtained from S by replacing $S_{/w}$ (that is $S_{/w0}S_{/w10}S_{/w11}{*}{*}$) by $S_{/w0}S_{/w10}{*}S_{/w0}S_{/w11}{*}{*}$.

ii) The monoid generated by all w^+'s for w in $\mathbf{S}$ with reverse composition is denoted by $\boldsymbol{\vartheta}^+$. The inverse mapping of w^+ is denoted by w^-; the monoid generated by all w^+'s and w^-'s is denoted by $\boldsymbol{\vartheta}$.

The action of w^+ is clear: it consists in expanding according to left distributivity "at w." We use reverse composition to make reading more natural, and to avoid ambiguity write $\mathbf{val}(S, \varphi)$ to denote the image of S under φ (the value of φ at S).

EXAMPLE. A picture should make clear that $\mathbf{val}(abcd{*}{*}{*}, \Lambda^+)$ is $ab{*}acd{*}{*}{*}$, while $\mathbf{val}(abcd{*}{*}{*}, 1^+)$ is $abc{*}bd{*}{*}{*}$.

With this definition, $\boldsymbol{\vartheta}$ acts on $\mathcal{T}(\Sigma)$, and $\equiv$ is exactly the equivalence relation attached to this action: $S \equiv T$ holds if, and only if, T is the image of S under some element of $\boldsymbol{\vartheta}$. Notice that, owing to the above definition, $\boldsymbol{\vartheta}$ could depend on Σ; in fact it is proved in [De1] that it does not, at least if Σ has strictly more than one element, what we shall assume henceforth.

The monoid $\boldsymbol{\vartheta}$ is closely connected with the infinite braid group B_∞. The existence of canonical operation of braid groups on distributive structures has already been noticed and used (see [Br]). The "structural" monoid $\boldsymbol{\vartheta}$ introduced above is in fact an extension of B_∞. Let us describe B_∞ as the group generated by an infinite family of generators $(\sigma_i)_{i=0,1,\ldots}$ under the relations

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$$

$$\sigma_i\sigma_j = \sigma_j\sigma_i \quad \text{if} \quad |i-j| \geq 2;$$

then the mapping π defined by

$$\pi(w^+) := \begin{cases} \sigma_i & \text{if } w \text{ is } 1^i \text{ for some } i \\ 1 & \text{otherwise} \end{cases} \qquad \pi(w^-) := \begin{cases} \sigma_i^{-1} & \text{if } w \text{ is } 1^i \text{ for some } i \\ 1 & \text{otherwise} \end{cases}$$

is an epimorphism of $\boldsymbol{\vartheta}$ onto B_∞. The process described below can be seen as extending some work about normal forms for the elements of B_∞: for instance, proposition 1 below extends the existence of Garside form (see for instance [Bi]). However $\boldsymbol{\vartheta}$ appears as much more complicated than B_∞ to handle, and the results in B_∞ that can be derived using π from the ones established here in $\boldsymbol{\vartheta}$ have in general (much) more simple direct proofs.

With the present notations, the left subterms of a term S are the various $S_{/0^p}$ for $p = 1, 2, \ldots$, and the irreflexivity conjecture can be stated as:

IRREFLEXIVITY HYPOTHESIS (IH′). *There cannot exist S in $\mathcal{T}(\Sigma)$, φ in $\boldsymbol{\vartheta}$ and a positive integer p such that φ maps S to $S_{/0^p}$.*

A first reduction of the question can be obtained by focusing on the positive terms in $\boldsymbol{\vartheta}$, i.e., the terms in $\boldsymbol{\vartheta}^+$. Let us introduce the following notations.

DEFINITION. For S, T in $\mathcal{T}(\Sigma)$, write $S \longrightarrow T$ (respectively, $S \longrightarrow^n T$) if, and only if, T is the image of S under some element of $\boldsymbol{\vartheta}^+$ (respectively, under the product of at most n successive w^+'s).

The main result about $\longrightarrow$ is its confluent character proved in [De1]; it immediately implies

PROPOSITION 1. *Let S, T be arbitrary terms in $\mathcal{T}(\Sigma)$; the following are equivalent:*
i) $S \equiv T$ holds;
ii) there exist U such that both $S \longrightarrow U$ and $T \longrightarrow U$ hold.

We can therefore rewrite IH as

IRREFLEXIVITY HYPOTHESIS (IH″) . *There cannot exist S, T in $\mathcal{T}(\Sigma)$ and a positive integer p such that both $S \longrightarrow T$ and $S_{/0^p} \longrightarrow T$ hold.*

2. Progressive sequences.

The main obstruction for a direct proof of conjecture IH″ is the *lack of uniqueness* in the writing of the elements in $\boldsymbol{\vartheta}^+$ as products of a sequence of w^+ transformations. For instance, the sequences $\Lambda^+1^+\Lambda^+$, $1^+\Lambda^+0^+1^+$ and $1^+\Lambda^+1^+0^+$ represent the same element of $\boldsymbol{\vartheta}^+$. The idea is to distinguish particular sequences that enjoy some uniqueness property, so that we reach a contradiction in assuming both $S \longrightarrow T$ and $S_{/0^p} \longrightarrow T$ because the canonical sequences witnessing for these relations should be both equal (by uniqueness) and different (since they represent 1-1 mappings having different arguments and the same image).

It will be convenient in the sequel to use as "atomic terms" no longer the w^+ transformations, but some simple products. Also we shall use an ordering on $\mathbf{S}$. So we put

NOTATION. i) For w in $\mathbf{S}$ and r a positive integer, set $w^{(r)} := w^+(w0)^+\cdots(w0^{r-1})^+$;
ii) $\prec$ is the natural linear ordering on $\mathbf{S}$ for which $0\prec 1\prec\Lambda$ holds, i.e., $u\prec v$ holds either if v is a prefix of u (that is $u = vw$ for some w) or u is on the left of v (that is $w0$ is a prefix of u and $w1$ is a prefix of v for some w);
iii) $\overline{\mathbf{S}}$ will be $\mathbf{S}$ enlarged with a new element 0^∞ that will be considered minimal for $\prec$.

The aim of this paper is to introduce the following refinement of the relation $\longrightarrow$.

DEFINITION. i) The relation $\Longrightarrow^1_\bullet$ on $\mathcal{T}(\Sigma)\times\overline{\mathbf{S}}$ is defined by:

$(S,u)\Longrightarrow^1_\bullet(T,v)$ holds if, and only if, for some w in $\mathbf{S}$ and some integer r one has $T = \mathbf{val}(S, w^{(r)}), u\preceq w10^r$ and $w0^r\preceq v$.

The reflexive-transitive closure of $\Longrightarrow^1_\bullet$ is denoted by $\Longrightarrow_\bullet$, and the projection of $\Longrightarrow_\bullet$ on $\mathcal{T}(\Sigma)$ is denoted by $\Longrightarrow$.
ii) A sequence $\langle w_1^{(r_1)}\dots w_n^{(r_n)}\rangle$ in $\boldsymbol{\vartheta}^+$ is said to be *progressive* if, and only if, $w_i0^{p_i}\preceq w_{i+1}10^{p_{i+1}}$ holds for $i = 0,1,\dots,n-1$. The elements of $\boldsymbol{\vartheta}^+$ that can be written (in at least one way) as the product of a progressive sequence are called *progressive*; the set of all progressive elements in $\boldsymbol{\vartheta}^+$ is written $\boldsymbol{\vartheta}^+_{\mathbf{prog}}$.

The connection between progressive transformations and $\Longrightarrow$ is easy: the second coordinate in $\Longrightarrow_\bullet$ is used to witness for the progressivity of the sequence of elementary transformations applied to the first coordinate, so that one has

LEMMA 1. *Let S,T belong to $\mathcal{T}(\Sigma)$; then $S\Longrightarrow T$ holds if, and only if, T is the image of S under some progressive element of $\boldsymbol{\vartheta}^+$.*

The set $\boldsymbol{\vartheta}^+_{\mathbf{prog}}$ is a strict subset of $\boldsymbol{\vartheta}^+$, i.e., $\Longrightarrow$ is a strict refinement of $\longrightarrow$. Indeed, while $\Longrightarrow_\bullet$ is designed to be transitive, $\Longrightarrow$ is *not* transitive: for instance, Λ^+ and 00^+ are in $\boldsymbol{\vartheta}^+_{\mathbf{prog}}$ (so is every atomic element $w^{(r)}$), but the product Λ^+00^+ is not (the sequence $\langle\Lambda^+,00^+\rangle$ does not satisfy the combinatorial criterion since $0\preceq 0010$ is false, and one can easily show that it is the only possible decomposition of Λ^+00^+ as a product of positive terms). Notice that the corresponding projections on B_∞ behave nicely and give rise to a simple "unique normal form" result: every positive term in B_∞ is progressive, and has exactly one progressive writing, since $\langle\sigma_i,\sigma_j\rangle$ satisfies the progressivity assumption exactly when $j\le i+1$ holds.

We prove now that progressive sequences enjoy the required uniqueness properties.

DEFINITION. i) Recall that the terms in $\mathcal{T}(\Sigma)$ are considered as finite sequences from $\Sigma\cup\{*\}$; we shall treat such a sequence say S as a mapping of the integer interval $1..|S|$ to $\Sigma\cup\{*\}$. Then we denote by $\mathbf{add}(.,S)$ the increasing bijection of $(1..|S|,<)$ onto $(\mathbf{Supp}^+S,\prec)$ (the *address* in S).
ii) Let S,T be two distinct terms in $\mathcal{T}(\Sigma)$; the *divergence* of S and T, written $\mathbf{div}(S,T)$, is the least integer p such that $S(p+1)$ and $T(p+1)$ are not equal (i.e., either both are defined and have different values, or one is defined while the other is not).

EXAMPLE. Let S be $abc{*}{*}$ and T be $ab{*}ac{*}{*}$; $|T|$ is 7, and one has e.g., $T(1) = a$, $T(3) = *$. Since the $\prec$-increasing enumeration of $\mathbf{Supp}(T)$ is $00, 01, 0, 10, 11, 1, \Lambda$, $\mathbf{add}(1,T)$ is 00 while $\mathbf{add}(3,T)$ is 0. Finally $\mathbf{div}(S,T)$ is 2, since $S(3)$ is a and $T(3)$ is $*$.

One will easily verify that $u = \mathbf{add}(p, S)$ means that p is the rank in S of the last occurrence of a character coming from the subterm $S_{/u}$.

LEMMA 2. *Assume $S \Longrightarrow T$; then the first term of any progressive sequence such that T is the image of S under the product of this sequence is $w^{(r)}$ where $w10^r$ is $\mathbf{add}(\mathbf{div}(S,T), S)$.*

Proof. A direct computation shows for $T = \mathbf{val}(S, w^{(r)})$ the following equalities

$$\mathbf{add}(\mathbf{div}(S,T), S) = w10^r$$
$$\mathbf{add}(\mathbf{div}(S,T) + 1, T) = w0^r.$$

It follows that if we start with a progressive sequence

$$(S_0, u_0) \Longrightarrow^1_\bullet (S_1, u_1) \Longrightarrow^1_\bullet \cdots \Longrightarrow^1_\bullet (S_n, u_n),$$

then the integers $\mathbf{div}(S_0, S_1), \mathbf{div}(S_1, S_2), \ldots, \mathbf{div}(S_{n-1}, S_n)$ make a strictly increasing sequence: indeed if $w_i^{(r_i)}$ maps S_{i-1} to S_i, then the inequality $\mathbf{div}(S_{i-1}, S_i) + 1 \leq \mathbf{div}(S_i, S_{i+1})$ is equivalent to $\mathbf{add}(\mathbf{div}(S_{i-1}, S_i) + 1, S_i) \preceq \mathbf{add}(\mathbf{div}(S_i, S_{i+1}), S_i)$, hence to $w_i 0^{r_i} \preceq w_{i+1} 10^{r_{i+1}}$, which is the progressivity assumption. It follows that $\mathbf{div}(S_0, S_n)$ is equal to $\mathbf{div}(S_0, S_1)$, and, therefore, that $\mathbf{add}(\mathbf{div}(S_0, S_n), S_0)$ is $w_1 10^{r_1}$, and this determines uniquely both w_1 and r_1. ∎

The preceding proof makes the notion of progressive sequence clear: a sequence is progressive when the divergences produced by successive application of its terms appear in strictly increasing order (from the left to the right). We deduce

LEMMA 3. *i) Every member of $\vartheta^+_{\mathrm{prog}}$ has exactly one progressive decomposition.*

ii) There cannot exist S, T in $\mathcal{T}(\Sigma)$ and a positive integer p such that both $S \Longrightarrow T$ and $S_{/0^p} \Longrightarrow T$ simultaneously hold.

Proof. i) is an obvious iteration of lemma 2. In fact, we get in this way an *algorithm* that produces when starting with two terms S, T the unique progressive sequence $\langle w_1^{(r_1)}, \ldots, w_n^{(r_n)} \rangle$ such that T is the image of S under $w_1^{(r_1)} \cdots w_n^{(r_n)}$ if such a sequence exists. Indeed start with S, get $w_1^{(r_1)}$ from $\mathbf{div}(S,T)$, replace S by $\mathbf{val}(S, w_1^{(r_1)})$ and loop until equality with T is obtained.

ii) Assume $S_{/0^p} \Longrightarrow T$: the algorithm above running on $S_{/0^p}$ and T provides φ in $\vartheta^+_{\mathrm{prog}}$ such that T is $\mathbf{val}(S_{/0^p}, \varphi)$. Now remember that $S_{/0^p}$ is just a prefix of S (when viewed as words on $\Sigma \cup \{*\}$): then for every $p < |S_{/0^p}|$, $\mathbf{add}(p, S)$ is $0^p \mathbf{add}(p, S_{/0^p})$, so that the same algorithm running on S and T will produce "$0^p\varphi$" (same as φ but add 0^p before each term) after scanning $S_{/0^p}$, and the current value of the first term at this step will be TX if S was $S_{/0^p}X$. It is then clearly impossible that the algorithm continues on TX and T and succeeds, since $\mathbf{add}(\mathbf{div}(TX, T), TX)$ is Λ: so $S \Longrightarrow T$ is impossible. ∎

Comparing lemma 3ii) with conjecture IH″ suggests a way for proving IH, namely to replace $\longrightarrow$ by its (strict) refinement $\Longrightarrow$ in the confluency results.

PROGRESSIVITY HYPOTHESIS (PH*). *Let S, T be arbitrary terms in $\mathcal{T}(\Sigma)$; the following are equivalent:*
i) $S \equiv T$ holds;
ii) there exist U such that both $S \Longrightarrow U$ and $T \Longrightarrow U$ hold.

It is clear that PH* implies IH. Due to the lack of transitivity of $\Longrightarrow$, it will be convenient to introduce a more technical statement that seems easier to prove than PH* and nevertheless implies IH. To do that, we shall first recall the construction of the derivation operation on $\mathcal{T}(\Sigma)$, which is the key tool for proving the confluency of $\longrightarrow$. The problem there lies in the fact that $\longrightarrow$ is not a noetherian relation, i.e., there are infinitely long nontrivial sequences $S_0 \longrightarrow S_1 \longrightarrow S_2 \longrightarrow \cdots$, and that therefore the easy local confluency does not imply the global one. The solution given in [De1] introduces a kind of "local noetherianity" by constructing for every term S an infinite sequence $S, \partial S, \partial^2 S, \ldots$, so that some lower bound phenomenon appears, from which proposition 1.1 easily follows.

DEFINITION. i) The binary operation **dist** on $\mathcal{T}(\Sigma)$ is inductively given by

$$\mathbf{dist}(S,T) := \begin{cases} ST* & \text{if } T \text{ is in } \Sigma, \\ \mathbf{dist}(S, T_{/0})\mathbf{dist}(S, T_{/1})* & \text{otherwise.} \end{cases}$$

ii) The unary operation ∂ on $\mathcal{T}(\Sigma)$ is inductively given by

$$\partial S := \begin{cases} S & \text{if } S \text{ is in } \Sigma, \\ \mathbf{dist}(\partial(S_{/0}), \partial(S_{/1})) & \text{otherwise.} \end{cases}$$

The operation **dist** is a "complete" distribution: $\mathbf{dist}(S, T)$ is obtained from T by replacing every variable a in T by $Sa*$; ∂ corresponds to recursively applying **dist** to every subterm of its argument. The key lemma for proving the confluency of $\longrightarrow$ is the following

LEMMA 4. *For any S, T in $\mathcal{T}(\Sigma)$ and any integer n, $S \longrightarrow^n T$ implies $T \longrightarrow \partial^n S$.*

The convenient refinement of this result we wish to set as a reachable conjecture is the following.

PROGRESSIVITY HYPOTHESIS (PH). *For any S, T in $\mathcal{T}(\Sigma)$ and any integer n, $S \longrightarrow^n T$ implies $T \Longrightarrow \partial^n S$.*

LEMMA 5. PH *implies* IH.

Proof. In order to prove IH″, assume that $S \longrightarrow T$ and $S_{/0^p} \longrightarrow T$ hold for some S, T and positive p. An easy induction on ϑ^+ shows that, if $S \longrightarrow T$ holds, then for every $p > 0$ (such that $S_{/0^p}$ exist) there exists $q \geq p$ such that $S_{/0^p} \longrightarrow T_{/0^q}$ holds. Let n be large enough so that $S_{/0^p} \longrightarrow^n T$ and $S_{/0^p} \longrightarrow^n T_{/0^q}$ hold. If PH is true, this implies $T \Longrightarrow \partial^n(S_{/0^p})$ and $T_{/0^q} \Longrightarrow \partial^n(S_{/0^p})$, a contradiction to lemma 3 since $q \geq p \geq 1$. ∎

NOTATION. Let PH_n, PH'_m be the following statements:

PH_n: For any S, T in $\mathcal{T}(\Sigma)$, $S \longrightarrow^n T$ implies $T \Longrightarrow \partial^n S$.

PH'_m: For any S, T, U in $\mathcal{T}(\Sigma)$, $S \longrightarrow^1 T$ and $S \Longrightarrow^m U$ imply $T \Longrightarrow \partial U$ (where $\Longrightarrow_\bullet^m$ is the m-th power of $\Longrightarrow_\bullet^1$, and $\Longrightarrow^m$ the projection of $\Longrightarrow_\bullet^m$).

An immediate induction shows that, if PH'_m is true for every m, then PH_n is also true for every n, i.e., PH is true. The following section gives a proof of PH_1, that is also PH'_0. The best result presently proved in this direction is PH'_1. The main improvement brought by replacing IH by PH seems to be that IH is a negative statement while PH is positive and, due to the uniqueness of progressive decomposition, the "double arrow" whose existence is claimed is in fact completely determined, so that proving PH (if it is true!) appears as a kind of (very complicated) verification only.

3. A proof of PH_1.

In order to prove that $T \Longrightarrow \partial S$ holds for every T satisfying $S \longrightarrow^1 T$ (and, at first, that $S \Longrightarrow \partial S$ holds), it will be necessary to define a family of terms that contains S, ∂S, all T's satisfying $S \longrightarrow^1 T$, but also all intermediate terms appearing in the progressive transformations $T \Longrightarrow \partial S$.

DEFINITION. Assume that $\mathcal{X}$ is a subset of $\mathcal{T}(\Sigma)$;
i) write $(U,u) \overset{\mathcal{X}}{\Longrightarrow}_\bullet (V,v)$ whenever $(U,u) \Longrightarrow_\bullet (V,v)$ holds and all intermediate terms appearing in the progressive transformation (including U and V themselves) are in $\mathcal{X}$; use $U \overset{\mathcal{X}}{\Longrightarrow} V$ in the same way;
ii) say that $\mathcal{X}$ is *S-directed* if, and only if, $U \overset{\mathcal{X}}{\Longrightarrow} S$ holds for every U in $\mathcal{X}$.

For every S in $\mathcal{T}(\Sigma)$, $\{U \in \mathcal{T}(\Sigma); U \Longrightarrow S\}$ is the maximal S-directed set. Clearly a subset of $\mathcal{T}(\Sigma)$ can be S-directed for at most one term S. In order to describe the progressive transformations toward terms written as "**dist**," we introduce a machinery that controls partial distribution.

NOTATION. If f is any mapping with domain included in Σ and u is in Σ, write $f_{/u}$ for the new mapping defined by $f_{/u}(w) = x$ if, and only if, $f(uw) = x$. Also, we write $\mathbf{Dom}^+ f$ for the prefix closure of $\mathbf{Dom} f$: w is in $\mathbf{Dom}^+ f$ if, and only if, there is some v in $\mathbf{Dom} f$ such that w is a prefix of v.

DEFINITION. Assume that $\mathcal{X}$, $\mathcal{Y}$ are subsets of $\mathcal{T}(\Sigma)$ and T is any term in $\mathcal{T}(\Sigma)$;
i) an *$\mathcal{X}$-graft* is a mapping whose domain is a support (i.e., is $\mathbf{Supp}(S)$ for some term S in $\mathcal{T}(\Sigma)$), and whose range is included in $\mathcal{X}$; an $\mathcal{X}$-graft is said to be *T-suitable* if its domain is included in $\mathbf{Supp}^+ T$. If Γ is a T-suitable $\mathcal{X}$-graft, a new term $\langle \Gamma, T\rangle$ is defined inductively on $\mathbf{Dom}\Gamma$ by

$$\langle \Gamma, T \rangle := \begin{cases} \Gamma(\Lambda) T * & \text{if } \mathbf{Dom}\Gamma \text{ is } \{\Lambda\}, \\ \langle \Gamma_{/0}, T_{/0} \rangle \langle \Gamma_{/1}, T_{/1} \rangle * & \text{otherwise.} \end{cases}$$

ii) The set $\{\langle \Gamma, T\rangle; \Gamma \text{ is an } \mathcal{X}\text{-graft for } T\}$ is denoted by $\mathcal{D}\boldsymbol{ist}(\mathcal{X}, T)$, and $\bigcup_{T \in \mathcal{Y}} \mathcal{D}\boldsymbol{ist}(\mathcal{X}, T)$ by $\mathcal{D}\boldsymbol{ist}(\mathcal{X}, \mathcal{Y})$.

Point i) in the definition makes sense since if **Dom**Γ is not $\{\Lambda\}$, **Supp**T is not $\{\Lambda\}$, so that $T_{/0}$ and $T_{/1}$ exist and moreover **Dom**$(\Gamma_{/e})$ is included in $\mathbf{Supp}^+T_{/e}$ for $e = 0, 1$.

EXAMPLE. Let $\mathcal{X}$ be $\{a, ab*\}$ and T be $cde**$; set $\Gamma = \{(0, ab*), (1, a)\}$; then Γ is an T-suitable $\mathcal{X}$-graft, and $\mathbf{dist}(\Gamma, T)$ is $ab*c*ade***$: $\langle\Gamma, T\rangle$ is obtained from T by "grafting" some members from $\mathcal{X}$ in T at the places prescribed by **Dom**Γ.

The key result of this section will be the following

PROPOSITION 1. *Assume that $\mathcal{X}$ is S-directed and $\mathcal{Y}$ is T-directed; then $\mathcal{D}ist(\mathcal{X},\mathcal{Y})$ is $\mathbf{dist}(S, T)$-directed.*

LEMMA 2. *Assume that Γ is a T-suitable graft;*
i) for u in $\mathbf{Dom}^+\Gamma$, one has

$$\langle\Gamma, T\rangle_{/u} = \langle\Gamma_{/u}, T_{/u}\rangle;$$

ii) for u in **Dom**Γ *and w short enough, one has*

$$\langle\Gamma, T\rangle_{/u} = \langle\Gamma(u), T_{/u}\rangle \ ; \ \langle\Gamma, T\rangle_{/u0w} = \Gamma(u)_{/w} \ ; \ \langle\Gamma, T\rangle_{/u1w} = T_{/uw}.$$

The proof is an easy induction on **Dom**Γ. Notice that, for any terms S, T in $\mathcal{T}(\Sigma)$, $\mathbf{dist}(S, T)$ is $\langle\Gamma, T\rangle$ where Γ is the constant $\{S\}$-graft with domain **Supp**T and value S.

NOTATION. For u in Σ, we write $\{u\}^\sim$ for the least support that contains u: $\{u\}^\sim$ can be defined inductively by $\{\Lambda\}^\sim := \{\Lambda\}$, $\{0u\}^\sim := 0\{u\}^\sim \cup \{1\}$ and $\{1u\}^\sim := \{0\} \cup 1\{u\}^\sim$.

LEMMA 3. *Assume that u is in* **Supp**T*; the following are equivalent:*
i) the term U is $\langle\Gamma, T\rangle$ for some T-suitable $\mathcal{X}$-graft Γ such that u is in $\mathbf{Dom}^+\Gamma$;
ii) for every w in $\{u\}^\sim$, the term $U_{/w}$ is in $\mathcal{D}ist(\mathcal{X}, T_{/w})$.

Proof. Induction on u. If u is Λ, $\{u\}^\sim$ is $\{\Lambda\}$ and both i) and ii) say that U is in $\mathcal{D}ist(\mathcal{X}, T)$. Otherwise, assume $u = eu'$ with $e = 0$ or $e = 1$. Use $\overline{e}$ to mean 1 (respectively, 0) if e is 0 (respectively, 1). Assume i). As u is in $\mathbf{Dom}^+\Gamma$, hence in **Supp**T, T is not in Σ, and $\langle\Gamma, T\rangle$ is $\langle\Gamma_{/0}, T_{/0}\rangle\langle\Gamma_{/1}, T_{/1}\rangle*$. Now u' is in $\mathbf{Supp}^+(T_{/e})$, so $U_{/e_{/w}}$ must be in $\mathcal{D}ist(\mathcal{X}, T_{/e_{/w}})$ for every w in $\{u'\}^\sim$. Moreover, $U_{/\overline{e}}$ is in $\mathcal{D}ist(\mathcal{X}, T_{/\overline{e}})$, so ii) is proved. Now assume ii). Then $U_{/e_{/w}}$ is in $\mathcal{D}ist(\mathcal{X}, T_{/e_{/w}})$ for every w in $\{u'\}^\sim$, so (induction hypothesis) $U_{/e}$ is $\langle\Gamma_e, T_{/e}\rangle$ for some $\mathcal{X}$-graft Γ_e with $u' \in \mathbf{Dom}^+(\Gamma_e)$. Moreover $U_{/\overline{e}}$ is in $\mathcal{D}ist(\mathcal{X}, T_{/\overline{e}})$, i.e., is $\langle\Gamma_{\overline{e}}, T_{/\overline{e}}\rangle$ for some $\mathcal{X}$-graft $\Gamma_{\overline{e}}$. Then U is $\langle\Gamma, T\rangle$ where Γ is, with obvious notations, $0\Gamma_0 \cup 1\Gamma_1$, and u is in $\mathbf{Dom}^+\Gamma$. ∎

DEFINITION. i) For T in $\mathcal{T}(\Sigma)$ and u in **S**, write $\mathbf{Supp}_u T$ for $\{w \in \mathbf{Supp}T; w \preceq u\}$.
ii) Assume that $\mathcal{X}$ is S-directed; we say that Γ is a (T, u)-*complete* $\mathcal{X}$-graft whenever Γ is a T-suitable $\mathcal{X}$-graft, **Dom**Γ includes $\mathbf{Supp}_u T$, and for w in the latter set, $\Gamma(w)$ is equal to S.

LEMMA 4. *Assume that $\mathcal{X}$ is S-directed and u is in* **Supp**T*; the following are equivalent:*

i) U is $\langle\Gamma, T\rangle$ for some (T,u)-complete $\mathcal{X}$-graft Γ;

ii) for every w in $\{u\}^{\sim}$, the term $U_{/w}$ is in $\boldsymbol{\mathcal{D}ist}(\mathcal{X}, T_{/w})$, and moreover it is equal to $\mathbf{dist}(S, T_{/w})$ *whenever $w \preceq u$ holds.*

Proof. Induction on u. If u is Λ, then Γ is (T,u)-complete if, and only if, $\mathbf{Dom}\Gamma$ is equal to $\mathbf{Supp}T$ and $\Gamma(w)$ is equal to S for every w in $\mathbf{Dom}\Gamma$, so if, and only if, $\langle\Gamma, T\rangle$ is $\mathbf{dist}(S,T)$. Otherwise let u be eu' with $e = 0$ or $e = 1$. Assume i). By lemma 3, we know that $U_{/w}$ is in $\boldsymbol{\mathcal{D}ist}(\mathcal{X}, T_{/w})$ for w in $\{u\}^{\sim}$. Assume $e = 0$. Then Γ is (T,u)-complete if, and only if, $\Gamma_{/0}$ is $(T_{/0}, u')$-complete, since $\mathbf{Supp}_u T$ is exactly $0\mathbf{Supp}_{u'}(T_{/0})$. This implies $U_{/0_{/w}} = \mathbf{dist}(S, T_{/0_{/w}})$ for w in $\mathbf{Supp}_{u'}(T_{/0})$, and proves ii). Conversely if ii) holds, then "ii) holds" as well for $U_{/0}$ with respect to u', so (induction hypothesis) $U_{/0}$ is $\langle\Gamma_0, T_{/0}\rangle$ for some $(T_{/0}, u')$-complete $\mathcal{X}$-graft Γ_0. Moreover $U_{/1}$ is assumed to be $\langle\Gamma_1, T_{/1}\rangle$ for some $T_{/1}$-suitable $\mathcal{X}$-graft Γ_1. So finally U is $\langle\Gamma, T\rangle$ where Γ is $0\Gamma_0 \cup 1\Gamma_1$, and Γ is (T,u)-complete. Now assume $e = 1$: $\mathbf{Dom}_u T$ is $0\mathbf{Supp}(T_{/0}) \cup 1\mathbf{Supp}_{u'}(T_{/1})$, so Γ is (T,u)-complete if, and only if, $\Gamma_{/0}$ is $(T_{/0}, \Lambda)$-complete and $\Gamma_{/1}$ is $(T_{/1}, u')$-complete, if, and only if, $\langle\Gamma_0, T_{/0}\rangle$ is $\mathbf{dist}(S, T_{/0})$ and $\langle\Gamma_1, T_{/1}\rangle_{/w} = \mathbf{dist}(S, T_{/1w})$ holds for $w \preceq u'$ in $\{u'\}^{\sim}$. This is exactly ii). The converse direction is proved as above. ■

LEMMA 5. *Assume that $\mathcal{X}$ is S-directed, that T' is* $\mathbf{val}(T, w^{(r)})$ *and Γ is a $(T, w10^r)$-complete $\mathcal{X}$-graft; then there exists a $(T', w0^r)$-complete $\mathcal{X}$-graft, say Γ', such that $\langle\Gamma', T'\rangle$ is* $\mathbf{val}(\langle\Gamma, T\rangle, w^{(r)})$*, and, therefore $(\langle\Gamma, T\rangle, w10^r) \Longrightarrow_{\bullet} (\langle\Gamma', T'\rangle, w0^r)$ holds.*

Proof. Let $u_1, \ldots, u_p$ (respectively, $v_1, \ldots, v_q$) be the elements of $\{w\}^{\sim}$ such that $u_i \prec w$ (respectively, $w \prec v_j$) holds. Let U' be $\mathbf{val}(\langle\Gamma, T\rangle, w^{(r)})$ (which exists since $w10^r$ is in $\mathbf{Supp}U$). By lemma 4, we get

$$\begin{aligned}
U'_{/x} &= U_{/x} = \mathbf{dist}(S, T_{/x}) = \mathbf{dist}(S, T'_{/x}) \qquad \text{for } x = u_1, \ldots, u_p,\\
U'_{/w0^r} &= U_{/w0} U_{/w10^r} *\\
&= \mathbf{dist}(S, T_{/w0}) \mathbf{dist}(S, T_{/w10^r}) *\\
&= \mathbf{dist}(S, T_{/w0} T_{/w10^r} *)\\
&= \mathbf{dist}(S, T'_{/w0^r}),\\
U'_{/x} &= U_{/x} \in \boldsymbol{\mathcal{D}ist}(\mathcal{X}, T_{/x}) = \boldsymbol{\mathcal{D}ist}(\mathcal{X}, T'_{/x}) \qquad \text{for } x = v_1, \ldots, v_q,\\
U'_{/w0^k1} &= U_{/w0} U_{/w10^k1} *\\
&\in \boldsymbol{\mathcal{D}ist}(\mathcal{X}, T_{/w0}) \boldsymbol{\mathcal{D}ist}(\mathcal{X}, T_{/w10^k1}) *\\
&\subseteq \boldsymbol{\mathcal{D}ist}(\mathcal{X}, T_{/w0} T_{/w10^k1} *)\\
&= \boldsymbol{\mathcal{D}ist}(\mathcal{X}, T'_{/w0^k1}) \qquad \text{for } k = 0, \ldots, r-1.
\end{aligned}$$

By lemma 4 again, this shows that U' is $\langle\Gamma', T'\rangle$ for some $(T', w0^r)$-complete $\mathcal{X}$-graft Γ'. ■

LEMMA 6. *Assume that $\mathcal{X}$ is S-directed, $\overline{S}$ is in $\mathcal{X}$ and 0^r is in* **Supp**T*; then there exists a $(T, 0^r)$-complete $\mathcal{X}$-graft Γ such that one has*

$$(\overline{S}T*, 0^{\infty}) \overset{\boldsymbol{\mathcal{D}ist}(\mathcal{X}, T)}{\Longrightarrow_{\bullet}} (\langle\Gamma, T\rangle, 0^r).$$

Proof. First $\overline{S} \overset{\mathcal{X}}{\Longrightarrow} S$ holds, and therefore $(\overline{S}T*, 0^\infty) \overset{\boldsymbol{Dist}(\mathcal{X},T)}{\Longrightarrow_\bullet} (ST*, 0)$ holds as well. Now 10^r is in $\mathbf{Supp}(ST*)$, so $ST*$ is in $\mathbf{Dom}\Lambda^{(r)}$. Let U be $\mathbf{val}(ST*, \Lambda^{(r)})$: we have $(ST*, 10^r) \overset{\boldsymbol{Dist}(\mathcal{X},T)}{\Longrightarrow_\bullet} (U, 0^r)$ and

$U_{/0^r} = S(T_{/0^r})* = \mathbf{dist}(S, T_{/0^r})$ (since $T_{/0^r}$ is in Σ)

$U_{/0^k 1} = S(T_{/0^k 1})* \in \boldsymbol{Dist}(\mathcal{X}, T_{/0^k 1})$ for $k = 0, \ldots, r-1$.

So U is $\langle \Gamma, T \rangle$ for some $(T, 0^r)$-complete $\mathcal{X}$-graft Γ . We are done, since $0 \prec 10^r$ holds and $\overset{\boldsymbol{Dist}(\mathcal{X},T)}{\Longrightarrow_\bullet}$ is a transitive relation. ■

LEMMA 7. *Assume that $\mathcal{X}$ is S-directed, U is in $\boldsymbol{Dist}(\mathcal{X}, T)$ and 0^r is in* $\mathbf{Supp}T$; *then there exists a $(T, 0^r)$-complete $\mathcal{X}$-graft Γ such that one has*

$$(U, 0^\infty) \overset{\boldsymbol{Dist}(\mathcal{X},T)}{\Longrightarrow_\bullet} (\langle \Gamma, T \rangle, 0^r).$$

Proof. Either U is $\overline{S}T*$ for some $\overline{S}$ in $\mathcal{X}$, and lemma 6 applies, or U is $U_0 U_1 *$ with U_e in $\boldsymbol{Dist}(\mathcal{X}, T_{/e})$. If r is 0, only the first case may occur, so that the induction starts. Assume the second case. Since 0^{r-1} is in $\mathbf{Supp}(T_{/0})$, there exists by induction hypothesis some $(T_{/0}, 0^{p-1})$-complete $\mathcal{X}$-graft Γ_0 such that the following holds

$$(U_0, 0^\infty) \overset{\boldsymbol{Dist}(\mathcal{X},T_{/0})}{\Longrightarrow_\bullet} (\langle \Gamma_0, T_{/0} \rangle, 0^{r-1}),$$

and so does

$$(U, 0^\infty) \overset{\boldsymbol{Dist}(\mathcal{X},T)}{\Longrightarrow_\bullet} (\langle \Gamma_0, T_{/0} \rangle U_1 *, 0^r).$$

Since U_1 is in $\boldsymbol{Dist}(\mathcal{X}, T_{/1})$, by lemma 4 again, $\langle \Gamma_0, T_{/0} \rangle U_1 *$ is $\langle \Gamma, T \rangle$ for some $(T, 0^r)$-complete $\mathcal{X}$-graft Γ' ■

LEMMA 8. *Assume that $\mathcal{X}$ is S-directed, u, v are points in* $\mathbf{Supp}^+(T)$ *satisfying $u \preceq v$ and Γ is a (T, u)-complete $\mathcal{X}$-graft; then there exists a (T, v)-complete $\mathcal{X}$-graft Δ such that one has*

$$(\langle \Gamma, T \rangle, u) \overset{\boldsymbol{Dist}(\mathcal{X},T)}{\Longrightarrow_\bullet} (\langle \Delta, T \rangle, v).$$

Proof. If v is u, there is nothing to prove (take $\Delta := \Gamma$). Otherwise, by transitivity we can assume that v is the immediate successor of u in $\mathbf{Supp}^+T$ (with respect to $\prec$). If u is Λ, there is nothing to prove. If u is $w1$ for some w, then w is the successor of u, and (from lemma 4) the (T, u)-completeness of a graft implies its (T, w)-completeness. So assume $u = w0$. Then, for some positive integer r, v is $w10^r$, and, in this case, v is in $\mathbf{Supp}T$. We argue inductively on w. Assume $w = \Lambda$. Since Γ is $(T, 0)$-complete, $\langle \Gamma, T \rangle_{/0}$ is equal to $\mathbf{dist}(S, T_{/0})$ and $\langle \Gamma, T \rangle_{/1}$ is in $\boldsymbol{Dist}(\mathcal{X}, T_{/1})$. Applying lemma 7 to $T_{/1}$, we get a $(T_{/1}, 0^r)$-complete $\mathcal{X}$-graft Δ_1 such that

$$(\langle \Gamma, T \rangle_{/1}, 0^\infty) \overset{\boldsymbol{Dist}(\mathcal{X},T_{/1})}{\Longrightarrow_\bullet} (\langle \Delta_1, T_{/1} \rangle, 0^r)$$

holds, and so does

$$(\langle \Gamma, T \rangle, 0) \overset{\boldsymbol{Dist}(\mathcal{X},T)}{\Longrightarrow_\bullet} (\langle \Gamma, T \rangle_{/0} \langle \Delta_1, T_{/1} \rangle *, 10^r).$$

Since $\langle\Gamma, T\rangle_{/0}$ is equal to $\mathbf{dist}(S, T_{/0})$, lemma 4 guarantees that $\langle\Gamma, T\rangle_{/0}\langle\Delta_1, T_{/1}\rangle*$ is $\langle\Delta, T\rangle$ for some $(T, 10^r)$-complete $\mathcal{X}$-graft.

Assume now $w = ew'$ with $e = 0$ or $e = 1$; $\langle\Gamma, T\rangle$ is $\langle\Gamma_{/0}, T_{/0}\rangle\langle\Gamma_{/1}, T_{/1}\rangle*$, and Γ_e is $(T_{/e}, w')$-complete. So (induction hypothesis)

$$((\langle\Gamma_{/e}, T_{/e}\rangle, w'0) \overset{\mathcal{D}ist(\mathcal{X}, T_{/e})}{\Longrightarrow_\bullet} ((\langle\Delta_e, T_{/e}\rangle, w'10^r)$$

holds for some $(T_{/e}, w'10^r)$-complete $\mathcal{X}$-graft Δ_e. It follows that

$$((\langle\Gamma, T\rangle, w0) \overset{\mathcal{D}ist(\mathcal{X}, T)}{\Longrightarrow_\bullet} ((\langle\Delta, T\rangle, w10^r)$$

holds, where Δ is the $(T, w10^r)$-complete $\mathcal{X}$-graft defined by $\Delta = 0\Delta_0 \cup 1\Gamma_{/1}$ if e is 0, and by $\Delta = 0\Gamma_{/0} \cup 1\Delta_1$ if e is 1. ■

We are now ready to prove proposition 1. Let U be an arbitrary member of $\mathcal{D}ist(\mathcal{X}, \mathcal{Y})$: U is $\langle\Gamma_0, T_0\rangle$ for some T_0 in $\mathcal{Y}$ and some T_0-suitable $\mathcal{X}$-graft Γ_0. Let $T_0, T_1, \ldots, T_n = T$ be the intermediate terms witnessing for $T_0 \Longrightarrow T$. Introduce for $\ell = 1, \ldots, n$ the elements w_ℓ, r_ℓ such that $w_\ell^{(r_\ell)}$ maps $T_{\ell-1}$ to T_ℓ. Using lemma 7 to start, and then lemma 8, get a $(T_0, w_1 10^{r_1})$-complete $\mathcal{X}$-graft Δ_0 such that one has

$$((\langle\Gamma_0, T_0\rangle, 0^\infty) \overset{\mathcal{D}ist(\mathcal{X}, \mathcal{Y})}{\Longrightarrow_\bullet} ((\langle\Delta_0, T_0\rangle, w_1 10^{r_1})$$

Using lemma 5, get a $(T_1, w_1 0^{r_1})$-complete $\mathcal{X}$-graft Γ_1 such that one has

$$((\langle\Delta_0, T_0\rangle, w_1 10^{r_1}) \overset{\mathcal{D}ist(\mathcal{X}, \mathcal{Y})}{\Longrightarrow_\bullet} ((\langle\Gamma_1, T_1\rangle, w_1 0^{r_1})$$

Using lemma 8, get a $(T_0, w_1 10^{r_1})$-complete $\mathcal{X}$-graft Δ_1 such that one has

$$((\langle\Gamma_1, T_1\rangle, w_1 0^{r_1}) \overset{\mathcal{D}ist(\mathcal{X}, \mathcal{Y})}{\Longrightarrow_\bullet} ((\langle\Delta_1, T_1\rangle, w_2 10^{r_2})$$

Using alternatively lemma 5 and lemma 8, one continues and finally gets some $(T_n, w_n 0^{r_n})$-complete $\mathcal{X}$-graft Γ_n. A last call to lemma 8 provides a (T_n, Λ)-complete $\mathcal{X}$-graft Δ_n such that one has

$$((\langle\Gamma_n, T_n\rangle, w_n 0^{r_n}) \overset{\mathcal{D}ist(\mathcal{X}, \mathcal{Y})}{\Longrightarrow_\bullet} ((\langle\Delta_n, T_n\rangle, \Lambda),$$

and, by transitivity, one deduces

$$((\langle\Gamma_0, T_0\rangle, 0^\infty) \overset{\mathcal{D}ist(\mathcal{X}, \mathcal{Y})}{\Longrightarrow_\bullet} ((\langle\Delta_n, T_n\rangle, \Lambda).$$

But T_n is T, and the Λ-completeness of Δ_n means that $\langle\Delta_n, T_n\rangle$ is $\mathbf{dist}(S, T)$. So the proof is complete. ■

It is now very easy to conclude this section.

DEFINITION. For S in $\mathcal{T}(\Sigma)$, define $\mathcal{E}xt S$ inductively by

$$\mathcal{E}xt S := \begin{cases} \{S\} & \text{if } S \text{ is in } \Sigma, \\ \mathcal{D}ist(\mathcal{E}xt(S_{/0}), \mathcal{E}xt(S_{/1})) & \text{otherwise.} \end{cases}$$

PROPOSITION 9. *For every S in $\mathcal{T}(\Sigma)$, $\mathcal{E}xt S$ is ∂S-directed.*

Proof. Induction on S. If S is in Σ, S is the only member of $\mathcal{E}xt S$, and is equal to ∂S. Otherwise, assuming that $\mathcal{E}xt(S_{/e})$ is $\partial(S_{/e})$-directed, we apply proposition 1 to conclude that $\mathcal{E}xt S$ is $\mathbf{dist}(\partial(S_{/0}), \partial(S_{/1}))$-directed, that is ∂S-directed. ■

Corollary. *The statement* PH_1 *is true.*

Proof. Assume $S \longrightarrow^1 T$ (or even $S \Longrightarrow^1 T$): we claim that T is in $\mathcal{E}xt S$, and this, by the latter proposition, implies that $T \Longrightarrow \partial S$ holds. So assume that $w^{(r)}$ maps S to T. We argue inductively on S, and then, for a given S, inductively on w. If S is in Σ, the result is vacuously true. Assume it proved for $S_{/e}$ ($e = 0, 1$). If w is Λ, then T is in $\mathcal{D}ist(\{S_{/0}\}, \{S_{/1}\})$, hence in $\mathcal{E}xt S$. And if w is ew', $T_{/e}$ is in $\mathcal{E}xt(S_{/e})$ (induction hypothesis), while $T_{/\bar{e}}$ is $S_{/\bar{e}}$, therefore belongs to $\mathcal{E}xt(S_{/\bar{e}})$: so T is in $\mathcal{E}xt(S_{/0})\mathcal{E}xt(S_{/1})*$, hence in $\mathcal{D}ist(\mathcal{E}xt(S_{/0}), \mathcal{E}xt(S_{/1}))$, that is $\mathcal{E}xt S$. ∎

4. The syntactical approach.

All statements considered so far deal in fact with the study of particular expressions for the members of ϑ. For instance, the confluency of $\longrightarrow$ (proposition 1.1) can be stated as the equality $\vartheta = \vartheta^+\vartheta^-$ since it claims that every member of ϑ has an expression made by a block of positive generators followed by a block of negative generators. In the same way, the statement PH^* can be stated as $\vartheta = \vartheta^+_{\mathrm{prog}}\vartheta^-_{\mathrm{prog}}$ (with the obvious meaning of $\vartheta^-_{\mathrm{prog}}$), and analog forms exist for PH, PH_n and PH'_m. In each case, the point is to prove that certain terms in ϑ are progressive, i.e., can be written as the products of progressive sequences.

Such results have been established above in a *semantical* way, in so far as we used the operation of ϑ on $\mathcal{T}(\Sigma)$, and proved the progressivity of a given term φ by showing that $S \Longrightarrow \mathbf{val}(S, \varphi)$ holds for some (any) term S in $\mathcal{T}(\Sigma)$. Another approach consists in directly guessing a progressive sequence and proving that φ can be written as the product of this sequence by means of the commutation relations that are known to hold in ϑ^+. This type of argument can be called *syntactical* since it only uses the relations in ϑ, but not the operation of ϑ on $\mathcal{T}(\Sigma)$.

Definition. Let $(\mathbf{S}^*, \bullet)$ be the free monoid generated by $\mathbf{S}$, and denote by $\approx$ the congruence on $\mathbf{S}^*$ generated by the following pairs:
- all pairs $(u0v{\bullet}u1w\,,\ u1w{\bullet}u0v)$ ("$\perp$-pairs");
- all pairs $(u1{\bullet}u{\bullet}u0{\bullet}u1\,,\ u{\bullet}u1{\bullet}u)$ ("1-pairs");
- all pairs $(u0v{\bullet}u\,,\ u{\bullet}u00v{\bullet}u10v)$ ("0-pairs");
- all pairs $(u10v{\bullet}u\,,\ u{\bullet}u01v)$ ("10-pairs");
- all pairs $(u11v{\bullet}u\,,\ u{\bullet}u11v)$ ("11-pairs").

It is easily verified that the pairs above correspond to equal elements in ϑ^+, so that if ρ is the canonical projection of $\mathbf{S}^*$ onto ϑ^+ that maps w to w^+, ρ factorizes through $\approx$. Therefore any relation involving $\approx$ yields an equality when projected to ϑ^+. We quote below a few results in this direction; the proofs are rather painful, so they will be omitted.

Definition. i) For w in $\mathbf{S}$, and $e = 0, 1$, we let $|w|_e$ be the number of e's occurring in w; we let $|w|^{\mathrm{fin}}_e$ be the number of *final* e's in w, i.e., the maximal integer r such that w can be written as $w'e^r$; finally set $|w|^{\mathrm{nfin}}_e = |w|_e - |w|^{\mathrm{fin}}_e$.

ii) Let w be in $\mathbf{S}$ and n be an integer; put

$$w^{[n]} := \begin{cases} w{\bullet}w0{\bullet}\cdots{\bullet}w0^{n-1} & \text{if } n>0, \\ \varepsilon & \text{otherwise,} \end{cases} \qquad w^{\times} := w'^{[r]},$$

$$w^{!} := \begin{cases} (0^p1^{q-1})^{[r]}{\bullet}(0^p1^{q-2})^{[r]}{\bullet}\cdots{\bullet}(0^p)^{[r]} & \text{if } q\geq 1, \\ \varepsilon & \text{otherwise,} \end{cases}$$

where $p := |w|_0^{\mathrm{nfin}}, q := |w|_1, r := |w|_0^{\mathrm{fin}}, w = w'0^r$ and ε is the empty sequence in $\mathbf{S}^*$.

iii) For A included in $\mathbf{S}$, we set

$$A^{\times} := \overset{\prec}{\prod_{w\in A}} w^{\times} \quad \text{and} \quad A^{!} := \overset{\prec}{\prod_{w\in A}} w^{!}.$$

EXAMPLE. Let w be 101100; then the parameters p, q, r are respectively 1,3,2, so that $w^{\times}$ is 1011•10110 and $w^!$ is 011•0110•01•010•0•00.

Two important technical results are the following

LEMMA 1. *Assume that α is in $\mathbf{S}^*$ and that $\rho\alpha$ maps S to T; then one has*

$$(\mathbf{Supp}S)^{\times}{\bullet}\alpha \approx 1\alpha{\bullet}(\mathbf{Supp}T)^{\times},$$

where for any sequence $\alpha = w_1{\bullet}\cdots{\bullet}w_n$, $u\alpha$ means $uw_1{\bullet}\cdots{\bullet}uw_n$.

LEMMA 2. *Assume that A is a support and w is in $\mathbf{S}$; then one has*

$$(wA)^! \approx w^!{\bullet}0^m1^{q-1}A^{\times}{\bullet}0^m1^{q-2}A^{\times}{\bullet}\cdots{\bullet}0^mA^{\times}{\bullet}0^mA^!,$$

where m is $|w|_0$ and q is $|w|_1$.

A typical (and self-contained) step toward the proof of such results is the following

CLAIM. *For $k\geq 1$ and $m\geq 0$, $\Lambda^{[k]}{\bullet}1^{[m+1]}{\bullet}\Lambda \approx 1{\bullet}\Lambda^{[k+1]}{\bullet}1^{[k]}{\bullet}01^{[m]}$ holds.*

Proof. Induction on $m\geq 0$. Assume $m=0$ and use induction on $k\geq 1$. For $k=1$, we have $\Lambda{\bullet}1{\bullet}\Lambda \approx 1{\bullet}\Lambda^{[2]}{\bullet}1$ since the two members make a 1-pair. Now assume $k>1$, we have:

$$\begin{aligned}
\Lambda^{[k]}{\bullet}1{\bullet}\Lambda &= \Lambda^{[k-1]}{\bullet}0^{k-1}{\bullet}1{\bullet}\Lambda \\
&\approx \Lambda^{[k-1]}{\bullet}1{\bullet}0^{k-1}{\bullet}\Lambda && (\perp\text{-pair}) \\
&\approx \Lambda^{[k-1]}{\bullet}1{\bullet}\Lambda{\bullet}0^{k}{\bullet}10^{k-1} && (0\text{-pair}) \\
&\approx 1{\bullet}\Lambda^{[k]}{\bullet}1^{[k-1]}{\bullet}0^{k}{\bullet}10^{k-1} && (\text{induction hypothesis}) \\
&\approx 1{\bullet}\Lambda^{[k]}{\bullet}0^{k}{\bullet}1^{[k-1]}{\bullet}10^{k-1} && (\perp\text{-pair}) \\
&= 1{\bullet}\Lambda^{[k+1]}{\bullet}1^{[k]}.
\end{aligned}$$

Now suppose $m\geq 1$ and the formula is proved for $m-1$ (and all k); we have:

$$\begin{aligned}
\Lambda^{[k]}{\bullet}1^{[m+1]}{\bullet}\Lambda &= \Lambda^{[k]}{\bullet}1^{[m]}{\bullet}10^{m}{\bullet}\Lambda \\
&\approx \Lambda^{[k]}{\bullet}1^{[m]}{\bullet}\Lambda{\bullet}010^{m-1} && (10\text{-pair}) \\
&\approx 1{\bullet}\Lambda^{[k+1]}{\bullet}1^{[k]}{\bullet}01^{[m-1]}{\bullet}010^{m-1} && (\text{induction hypothesis}) \\
&= 1{\bullet}\Lambda^{[k+1]}{\bullet}1^{[k]}{\bullet}01^{[m]}. \ \blacksquare
\end{aligned}$$

From lemmas 1 and 2, one deduces

PROPOSITION 3. *For any S in $\mathcal{T}(\Sigma)$, $\rho(\mathbf{Supp}S)^!$ maps S to ∂S.*

Proof. First, an induction on T shows that $\rho(\mathbf{Supp}T)^\times$ maps (for every term S) $ST*$ to $\mathbf{dist}(S,T)$. If T is in Σ, $ST*$ is equal to $\mathbf{dist}(S,T)$, and $\rho\Lambda^\times$ is the identity mapping. Otherwise, T is $T_{/0}T_{/1}*$, and the definition of $w^\times$ yields

$$(\mathbf{Supp}T)^\times = (0\mathbf{Supp}T_{/0})^\times \bullet (1\mathbf{Supp}T_{/1})^\times = \Lambda \bullet 0(\mathbf{Supp}T_{/0})^\times \bullet 1(\mathbf{Supp}T_{/1})^\times.$$

So, if $\rho(\mathbf{Supp}T_{/e})^\times$ maps $ST_{/e}*$ to $\mathbf{dist}(S,T_{/e})$, $\rho(\mathbf{Supp}T)^\times$ maps $ST*$ to

$$\mathbf{val}(ST_{/0}*, \rho(\mathbf{Supp}T_{/0})^\times)\mathbf{val}(ST_{/1}*, \rho(\mathbf{Supp}T_{/1})^\times)*,$$

that is $\mathbf{dist}(S,T_{/0})\mathbf{dist}(S,T_{/1})*$, i.e., $\mathbf{dist}(S,T)$.

Now we argue inductively on S. The result is obvious for S in Σ. Otherwise, we have $(\mathbf{Supp}S)^! = (0\mathbf{Supp}S_{/0})^! \bullet (1\mathbf{Supp}S_{/1})^!$, and lemma 2 gives $(0\mathbf{Supp}S_{/0})^! \approx 0(\mathbf{Supp}S_{/0})^!$ and $(1\mathbf{Supp}S_{/1})^! \approx (\mathbf{Supp}S_{/1})^\times \bullet (\mathbf{Supp}S_{/1})^!$. Assume (induction hypothesis) that $\rho(\mathbf{Supp}S_{/e})^!$ maps $S_{/e}$ to $\partial S_{/e}$. Then by lemma 1 we have

$$(\mathbf{Supp}S_{/1})^\times \bullet (\mathbf{Supp}S_{/1})^! \approx 1(\mathbf{Supp}S_{/1})^! \bullet (\mathbf{Supp}\partial(S_{/1}))^\times,$$

so that we deduce

$$(\mathbf{Supp}S)^! \approx 0(\mathbf{Supp}S_{/0})^! \bullet 1(\mathbf{Supp}S_{/1})^! \bullet (\mathbf{Supp}\partial(S_{/1}))^\times.$$

Now starting from S, i.e., $S_{/0}S_{/1}*$, $\rho(0(\mathbf{Supp}S_{/0})^!)$ maps S to $(\partial S_{/0})S_{/1}*$, then $\rho(1(\mathbf{Supp}S_{/1})^!)$ maps this term to $(\partial S_{/0})(\partial S_{/1})*$, and, finally, $\rho((\mathbf{Supp}\partial(S_{/1}))^\times)$ maps this later term to $\mathbf{dist}(\partial S_{/0}, \partial S_{/1})$, that is ∂S. ■

Since it is easily verified that, for any support A, $A^\times$ and $A^!$ are progressive sequences, we conclude from the proposition above that $S \Longrightarrow \partial S$ holds, and, moreover, we get the explicit progressive sequence witnessing for this property: this expression evaluates the exact contribution of each point w in $\mathbf{Supp}S$ to this sequence, namely the terms denoted by $\rho w^!$. Further computations could be made, for instance toward a syntactical proof of PH_1.

As a last question, let us mention the "completeness conjecture" that claims that $\boldsymbol{\vartheta}^+$ is in fact isomorphic to $\mathbf{S}^*/\approx$, i.e., that the set of pairs used in the definition of $\approx$ is exactly a presentation of $\boldsymbol{\vartheta}^+$. If this conjecture is true, any semantical proof can be converted into a syntactical proof. However, it seems likely that any proof of the completeness conjecture will require a lot of results about $\approx$ first, and therefore the computations above are not useless in any case.

References

[Bi] Birman, J., *Braids, links, and mapping class groups*, Annals of Math. Studies **82**, Princeton Univ. Press (1975).

[Br] Brieskorn, E., *Automorphic sets and braids and singularities*, Braids, Contemporary Math. **78**, Amer. Math. Soc. (1988) 45–117.

[De1] Dehornoy, P., *Free distributive groupoids*, Journal of Pure and Applied Algebra, **61** (1989) 123–146.

[De2] Dehornoy, P., *Sur la structure des gerbes libres*, Comptes-rendus de l'Acad. des Sciences de Paris, **309-I** (1989) 143–148.

[De3] Dehornoy, P., *Algebraic properties of the shift mapping*, Proc. Amer. Math. Soc., **106-3** (1989) 617–623.

[De4] DEHORNOY, P., *An alternative proof of Laver's results on the algebra generated by elementary embeddings*, preprint 1989.

[De5] DEHORNOY, P., *Preuve de la conjecture d'irréflexivité pour les structures distributives libres*, Comptes-rendus de l'Acad. des Sciences des Paris, **314-I** (1992) 333–336.

[Do] DOUGHERTY, R., *On critical points of elementary embeddings*, preprint 1988.

[Ke] KEPKA, P., *Notes on left distributive groupoids*, Acta universitatis Carolinae, Mathematica et physica, **22-2** (1981) 23–37.

[Jo] JOYCE, D., *A classifying invariant of knots: the knot quandle*, Journal of Pure and Applied Algebra, **23** (1982) 37–65.

[La1] LAVER, R., *On the left distributive law and the freeness of an algebra of elementary embeddings*, Advances in Mathematics, **91-2** (1992), 209–231.

[La2] LAVER, R., *A division algorithm for the free left distributive algebra*, this volume.

Groupe de recherche algorithmique et logique
Université de Caen
14032 Caen-cédex, France
dehornoy@geocub.greco-prog.fr