Axiomatizing Permutation Equivalence *

Cosimo Laneve   Ugo Montanari
Universitá di Bologna   Universitá di Pisa

May 1993, Revised Version: July 1994

Abstract

We axiomatize *permutation equivalence* in term rewriting systems and Klop's orthogonal Combinatory Reduction Systems [Klop 1980]. The axioms for the former ones are provided by the general approach proposed by Meseguer [Meseguer 1992]. The latter ones need extra axioms modeling the interplay between reductions and the operation of substitution.

As a consequence of this work, the definition of permutation equivalence is rid of residual calculi, which are heavy in general.

1 Introduction

1. What does permutation equivalence mean? A well-known syntactical property of the λ-calculus is the Church-Rosser theorem. It states that, if a term M reduces into N_1 and N_2 by firing two different redexes, then there exists a term P which is a reduct both of N_1 and N_2. Graphically:

$$\begin{tikzcd} & M \arrow[dl, "\mathbf{u}"'] \arrow[dr, "\mathbf{v}"] & \\ N_1 \arrow[dr, "\rho"'] & & N_2 \arrow[dl, "\sigma"] \\ & P & \end{tikzcd}$$

Actually the Church-Rosser property can be asserted in a stronger way. For this purpose, remark that the derivations ρ and σ are strictly related to the redexes v and u, respectively. In particular ρ (resp. σ) contracts *exactly* the residuals of v (resp. u) in N_1 (resp. N_2). That is, the computational contents of $\mathbf{u}; \rho$ and $\mathbf{v}; \sigma$ are equal: they reduce the redexes u and v in

*Partially supported by the ESPRIT Basic Research Project 6454 - CONFER.

M. More precisely, the derivations $\mathbf{u};\rho$ and $\mathbf{v};\sigma$ differ only in the order of the (independent) reductions.

The notion that equates those derivations which contract the same redexes, perhaps in different order, is *permutation equivalence*, precisely [Curry and Feys 1974, Lévy 1980, Boudol 1985]. Therefore, the Church-Rosser property can be stated as the existence of two derivations ρ and σ such that $\mathbf{u};\rho$ and $\mathbf{v};\sigma$ in the above picture are permutation equivalent. And the coincidence of the ending terms of $\mathbf{u};\rho$ and $\mathbf{v};\sigma$ becomes a consequence of the definition of permutation equivalence. Permutation equivalence has been at the basis of two important notions: the *family relation* in the theory of optimality [Lévy 1980] and the *concurrent semantics* of process calculi [Boudol and Castellani 1988].

2. On the definition of permutation equivalence. Let us focus on the concurrent semantics of process calculi since it has directly stimulated our research. In a concurrent scenario, where works are done by cooperating processes, computations are sequences of reductions (or events, in general). Define a suitable notion of permutation equivalence. Then consider as "the same abstract computation" those derivations that are permutation equivalent. This is a possible way (among others) of giving a so-called (true) concurrent semantics of the system.

The approach is strikingly simple, due to the plainnes of the definition of permutation equivalence for process calculi. Indeed, in concurrent systems, the residual of an event w.r.t. an *independent* one (or "*concurrent*" one, see [Boudol and Castellani 1988]) is *exactly one* event (its "individuality" does not change, see [Laneve 1994]). This is definitely false in rewriting systems, where determinating residuals is not so immediate because of the phenomena of duplication and erasing of redexes along reductions (for this reason, in the above discussion, ρ and σ are *derivations*, i.e. possible empty sequences of reductions). The standard examples are the residuals of the innermost redex w.r.t. the outermost one in the terms $(\lambda x.\, xx)((\lambda y.\, y)z)$ and $(\lambda x.\, y)((\lambda y.\, y)z)$.

In general, defining the residual of a redex u w.r.t. a reduction $\mathbf{v}$ requires the knowledge of the rewriting schema contracting v, that may be involved at will (see the definition in Section 5.1). Moreover, it may happen that residuals of a same redex are one inside the other (not *disjoint*, according to the terminology of Section 2). This situation is absent in the λ-calculus and complicates the definition of the derivation contracting the residuals of a redex.

3. The structural approach to concurrent semantics. The strict affinity between permutation equivalence and concurrent semantics encouraged us to investigate whether techniques developed in concurrency theory could be successfully applied to provide an alternative definition of permutation equivalence. In particular we considered a recent approach described in [Meseguer and Montanari 1990].

The basic idea in [Meseguer and Montanari 1990] is to exploit the structure of the system itself (defined by terms of a language) in order to express the reductions of a concurrent system. This allows one to recognize easily where the reduction is performed, i.e., the subsystem which actually moves. Hence, once the algebraic structure of terms is extended to derivations, it is rather simple and natural to add suitable axioms expressing the desired equivalence. Actually, it turns out that these axioms are often strongly suggested by the formal framework itself. This is the case when a categorical approach is taken: the so-called functoriality axioms are often such key axioms. They express distributivity of arrow composition (here computation concatenation) over the other available operations on computations.

Meseguer pursued this approach on *rewriting systems* (roughly term rewriting systems where the terms are taken modulo some axiomatization) [Meseguer 1992] (an alternative technique can be found in [Corradini and Montanari 1992]). Reductions of such systems are (intensionally) described through a language which is the free algebra of the terms over elementary rewritings. The semantics is defined through an axiomatization over the language of reductions in order to abstract away from the sequential nature of the syntactic description. In particular, the axioms turn the functions of the signature into functors of the category of computations, lift the axioms which underlie the terms of the rewriting system to axioms between functors and, finally, add an *exchange rule* stating the independence between rewritings in the arguments of a reduction and the reduction itself.

Meseguer does not provide any comparison between his semantics and permutation equivalence, even if a strong relation between the two semantics seems to exist. Indeed, the functorial axioms and the exchange axiom seem to capture the basic identifications yielded by permutation equivalence.

4. Our results. We prove that Meseguer's axioms completely define permutation equivalence in the case of term rewriting systems (which may have critical pairs). However, the axiomatization fails to be complete w.r.t. permutation equivalence when a larger class of rewriting systems is taken. In particular, when terms are taken up to some axiomatization. Indeed, in general, critical pairs may appear between axioms and proper rewritings, hiding subtle interplays among them. This is the case for the λ-calculus, that can be flattened to a term rewriting system by quotienting the expressions through axioms for α-conversion and substitution. It happens that α-conversion and the axiom dropping substitution inside application give rise to critical pairs with β-redexes. As a consequence, for example, Meseguer's axioms are not powerful enough for identifying a β-reduction with the one involving an α-equivalent abstraction.

We already proved that, in the λ-calculus case, Meseguer's axiomatization can be completed w.r.t. permutation equivalence by adding some simple axioms modeling the interplay between the operation of substitution and β-reduction [Laneve and Montanari 1992]. Here we generalize this result to generic rewriting systems with mechanisms of binding and substitution. More precisely, we study Klop's orthogonal Combinatory Reduction Systems (oCRS's, in the following). The restriction of orthogonality (no critical pair is admitted) is adopted for simplicity's sake, in order to keep distinct the problems due to the presence of critical pairs and those deriving from the mechanisms of binding and substitution.

The main consequence of our results is that permutation equivalence can be defined without mentioning residuals at all. More perspicuously, one can reason about derivations in a purely axiomatic way by means of a sound and complete deductive system.

5. The mechanisms of binding and substitution. Since binding and substitution are the reasons for the incompleteness of Meseguer's axioms, we wondered whether this failure can be repaired, at least for oCRS's, by adopting an alternative, cleaner description of such mechanisms. Up to our knowledge, there are two (algebraic) theories that have been recently examined: the theory of explicit substitution (with de Bruijn numbers) [Abadi, Cardelli, Curien and Lévy 1990] and the theory of binding structures [Talcott 1993].

In the theory of explicit substitutions, the operation of substitution appears explicitly in the language (rather than in the meta-language) and it is manipulated through axioms. In the λ-calculus case, one of these axioms (the one pushing substitution inside an application) gives rise to a critical pair with β-reduction, thus causing the same failure as before. We have discussed in detail this case in Section 4.

A similar failure can be shown in the theory of binding structures. In this theory, binding structures are defined through an algebra and a variety of operations on them are described by homomorphisms. In particular, the operation of substitution is performed by the composition of two homomorphisms ("adjustment" and "unbinding"). Again, in the λ-calculus case, a critical pair shows up as soon as these homomorphisms are turned into axioms of the algebra.

6. The organization of the paper. The paper is organized as follows. Section 2 introduces term rewriting systems, permutation equivalence and Meseguer's method. In Section 3 we prove the coincidence of Meseguer's axiomatization and permutation equivalence in the case of term rewriting systems. The failure of this coincidence in a more general setting is proved in Section 4 by means of a counterexample: the λ-calculus with explicit substitutions. In Section 5 we introduce the class of oCRS's, whilst in Section 6 we describe how to flatten a oCRS to a term rewriting system. The complete axiomatization of permutation equivalence for oCRS's is provided in Section 6.1.

In the paper some familiarity of the reader with basic notions about many-sorted algebras and many-sorted Birkhoff's deductive system is assumed: we refer the reader to [Meseguer and Goguen 1985].

2 Background

In this section we survey term rewriting systems (trs's, in brief) and Meseguer's method. Let us begin with some preliminary definitions.

Let S be a set of symbols called *sorts*. A *signature* Σ over sorts S is a collection $\{\Sigma_{w,s} \mid w \in S^*,\ s \in S\}$ where $\Sigma_{w,s}$ are sets of *operations* whose arity is w and *type* is s. As usual, T_Σ denotes the Σ-algebra of ground terms and $T_\Sigma(\mathsf{X})$ is the Σ-algebra of ground terms with variables in a family of sets X ranked by S. The function var gives the set of free variables in a term of $T_\Sigma(\mathsf{X})$. An *algebraic theory* is a pair (Σ, E) where Σ is a signature and E is a set of pairs in $T_\Sigma(\mathsf{X})$ called *equations*. The term algebra $T_{\Sigma,E}(\mathsf{X})$ represents the Σ-algebra of equivalence classes of Σ-terms according to the congruence $=_E$ derived by *Birkhoff's many sorted equational deductive system.*

A standard representation of terms is provided by *trees*. In this representation, subexpressions are denoted by the *access path* that leads from the root to the subexpression. Access paths will be ranged over by u, v, w, $\cdots$ and are partially ordered by the prefix order: $u \preceq w$ iff there exists v such that $u \cdot v = w$. If $u \not\preceq w$ and $w \not\preceq u$ then we call u and w *disjoint* and write $u|w$. As usual, we write $u \prec w$ if $u \preceq w$ and $u \neq w$. We will concatenate sets of access paths. If U is a set of access paths then $u \cdot U = \{u \cdot v \mid v \in U\}$. Notice that $u \cdot U$ is empty if $U = \emptyset$. Similarly, if V is also a set of access paths, $U \cdot V = \{u \cdot v \mid u \in U \text{ and } v \in V\}$.

2.1 Term rewriting systems and permutation equivalence

Definition 1 *A* (linear) term rewriting system *(trs, for short) is a finite set of rules $t_1 \to t_2$ where t_1 (the left-hand side of the rule, lhs for short) and t_2 (the right-hand side of the rule, rhs in brief) are terms in $T_\Sigma(\mathsf{X})$ and provided that*

1. $\mathsf{var}(t_2) \subseteq \mathsf{var}(t_1)$*;*
2. *t_1 is not a variable and*
3. *variables in t_1 occur linearly (i.e. every variable occurs at most once).*

We will assume that rules have a distinguishing label (ranged over by r, s) and we will refer to them by their label.

It is worth remarking that in trs's we may have *critical pairs* among rules. That is, given a trs (Σ, R), two different rules $t' \to t''$ and $t^+ \to t^\star$ in R have a *critical pair* if there exists an access path u such that the subexpression t'_u of t' at u is not a variable and there exist a pair of substitutions $\delta, \delta' : \mathsf{X} \to T_\Sigma(\mathsf{X})$ such that

$$\delta(t'_u) \; = \; \delta'(t^+).$$

Roughly, a *redex* is a subexpression whose shape matches the lhs of a rule; a *reduction* is the substitution of a redex with the rhs of the corresponding rule (appropriately instantiated). Usually redexes are denoted by the access path of the corresponding subexpression. However, due to the presence of critical pairs, this mechanism is no longer adequate to represent redexes uniquely, because the same expression may match with the lhs's of two different rules. Therefore, redexes and reductions will be denoted by the access path of the subexpression to be contracted *together with* the name of the contracting rule. We will use the notation u^r for redexes and $\mathbf{u}^r$ for reductions (remark that "u" is in bold for reductions and in italics for redexes), where u is the access path of u^r and r is the rule contracting the subexpression at u. As much as possible we will omit the superscript r. The meaning of a reduction is the standard one. Whenever it is not clear from the context we will explicitly give the initial and ending terms of $\mathbf{u}^r$ by using the notation $t \xrightarrow{u^r} t'$. A *derivation* is a possibly empty sequence $\mathbf{u}_1 \,;\, \mathbf{u}_2 \,;\, \ldots \,;\, \mathbf{u}_n$ of reductions such that the ending term of $\mathbf{u}_i$ is equal to the initial term of $\mathbf{u}_{i+1}$. Derivations will be ranged over by σ, ρ. The *empty reduction* from t to t is denoted by $\underline{\varepsilon}_t$ (we will omit the index t when it is clear from the context). As usual with strings, $\underline{\varepsilon}; \sigma = \sigma = \sigma; \underline{\varepsilon}$.

Critical pairs make the operation of residual a *partial* operation. That is, the residual of a redex after the firing of another redex yielding a critical pair with the first is no longer defined (the redex is disallowed without firing it or completely deleting it). The generalization of the residual calculus and permutation equivalence to trs's has been studied in detail by Boudol [Boudol 1985]. Let us recall here just the basic definitions.

Definition 2 (consistent redexes) *Two redexes u^r and v^s are* consistent, *written $u^r \| v^s$, if they are equal (i.e. $u = v$ and $r = s$), or disjoint, or $u \succeq v \cdot u'$, where u' is the access path of a variable in the lhs of s, or vice versa, $v \succeq u \cdot v'$, where v' is the access path of a variable in the lhs of r.*

A set U of redexes is consistent *if its elements are pairwise consistent.*

Definition 3 *Let t be a term in $T_\Sigma(\mathsf{X})$ and let u^r and v^s be two consistent redexes in t. The set $v^s/\mathbf{u}^r$ of* residuals *of v^s by $\mathbf{u}^r$ is the following subset of the ending expression of $\mathbf{u}^r$:*

$$v^s/\mathbf{u}^r \;=\; \begin{cases} \emptyset & \text{if } v^s = u^r \\ \{v^s\} & \text{if } u|v \ \mathsf{or}\ v \prec u \\ \{(u \cdot w_1 \cdot v_1)^s \mid t^2_{w_1} = x\} & \text{if } v = u \cdot w \cdot v_1 \ \mathsf{and}\ t^1_w = x \end{cases}$$

where t^1_w is the lhs of the rule r at occurrence w and $t^2_{w_1}$ is the rhs of the rule r at occurrence w_1.

It is important to remark that the residual $v^s/\mathbf{u}^r$ is a consistent set of redexes. The above definition can be generalized by replacing the contraction $\mathbf{u}^r$ with derivations. Indeed, this operation is inductively defined by:

1. $u/\underline{\varepsilon} = \{u\}$;
2. $u/(\sigma\,;\mathbf{v}) = \{w \mid w \in v'/\mathbf{v} \ \wedge\ v' \in u/\sigma\}$, provided that $v\|(u/\sigma)$.

Let U be a consistent set of redexes in a term t and $\sigma = \mathbf{u}_1\,;\mathbf{u}_2\,;\ldots$ be a derivation starting at t. We define $U/\sigma = \{u' \mid \exists u \in U.\ u' \in u/\sigma\}$. Moreover σ is *relative* to U iff for every $n \geq 1$, $u_n \in U/(\mathbf{u}_1\,;\cdots;\mathbf{u}_{n-1})$. The sequence σ is a *development* of U iff σ is relative to U and $U/\sigma = \emptyset$. That is, a development of a set U of redexes is a derivation always contracting redexes in U or residuals of them till there is no residual of U to reduce.

Theorem 1 *[Boudol 1985] Every development of a consistent set U of redexes is finite and ends at the same term. Moreover, if σ and ρ are two developments then, for every redex u consistent with U, $u/\sigma = u/\rho$.*

Therefore, the order according to which redexes of a consistent set are contracted is immaterial for both the final state and the effect upon other redexes. Consequently, the notion of parallel reduction contracting in one step a consistent set U of redexes (notation $\mathbf{U}$) can be defined unambiguously. In particular, the final expression of $\mathbf{U}$ is that reached by an arbitrary development of U and, similarly, when σ is a development of U, $u/\mathbf{U}$ is equal to u/σ. When $U \cup V$ is a consistent set of redexes, $V/\mathbf{U} = \{v/\mathbf{U} \mid v \in V\}$.

A simple consequence of Theorem 1 is that, when $U \cup V \cup W$ is a consistent set of redexes, then $\mathbf{U};\mathbf{V}/\mathbf{U}$ and $\mathbf{V};\mathbf{U}/\mathbf{V}$ end at the same term and $W/(\mathbf{U};\mathbf{V}/\mathbf{U}) = W/(\mathbf{V};\mathbf{U}/\mathbf{V})$. Furthermore $W/(\mathbf{V};\mathbf{U}/\mathbf{V})$ is a consistent set of redexes.

In the following we will consider derivations whose elementary steps are consistent sets of redexes (parallel derivations). We obtain the generalization of the residual operation to pairs of coinitial (parallel) derivations by applying the above method. The definition is given inductively over the sum of lengths of σ and ρ by

$$\sigma/\rho \;=\; \begin{cases} \underline{\varepsilon} & \textit{if } \sigma = \underline{\varepsilon} \\ (\sigma'/\rho);(\mathbf{U}/(\rho/\sigma')) & \textit{if } \sigma = \sigma';\mathbf{U} \;\; (U \text{ consistent}). \end{cases}$$

Notice that the notion of σ/ρ is partially defined, in general (U or a residual of U may not be consistent with some contraction along ρ/σ', for instance). Here is the definition of permutation equivalence.

Definition 4 Permutation equivalence *(notation $\equiv$) is the least equivalence relation on derivations satisfying:*

1. *If $U \cup V$ is a set of parwise consistent redexes then* $\mathbf{U};(\mathbf{V}\ \mathbf{U}) \equiv \mathbf{V};(\mathbf{U}/\mathbf{V})$*;*
2. $\underline{\varepsilon} \equiv \underline{\emptyset}$*;*
3. *if $\sigma \equiv \rho$, then $\tau;\sigma;\tau' \equiv \tau;\rho;\tau'$.*

We recall that derivations are always taken up to associativity of ";" and identity of $\underline{\varepsilon}$ w.r.t. ";".

Notice that $\equiv$ is a congruence w.r.t. composition of derivations. Indeed, if $\rho \equiv \rho'$ and $\sigma \equiv \sigma'$ then $\rho;\sigma \equiv \rho;\sigma' \equiv \rho';\sigma'$, by applying rule 3 twice. Permutation equivalence is also a congruence w.r.t. the algebraic operators.

NOTATION: Given a trs, $\mathcal{L}$ will be the structure whose objects are terms in $T_\Sigma(\mathsf{X})$ and whose arrows are derivations modulo $\equiv$, whose domain and codomain are the initial and ending expressions.

WARNING: in the notation $\mathcal{L}$, for simplicity, we will emphasize neither the signature of the trs nor the set of variables X. They will always be assumed fixed.

Observe that $\mathcal{L}$ is trivially a category.

2.2 Meseguer's concurrent semantics

In [Meseguer 1992], Meseguer defines a paradigm that allows endowing a rewriting system with a (concurrent) semantics. The idea underlying the method is to consider a rewriting system as a logical theory whose formulas are rewrite rules. In this view, formulas express how the system can *change*, contrary to the usual, Platonic meaning of formulas as expressing truths. Deductions in the logic describe how changes are computed, that is, how the simpler components of a system are involved in the transitions. So, by providing a syntax for deductions (i.e. by pursuing on a Curry-Howard correspondence), a notion of "structured transition" is obtained, that is, a transition whose syntactical structure describes the sub-systems that actually move. The *concurrent* semantics of the system is obtained by quotienting sequences of deductions through axioms. Let us go deeper into the details.

Definition 5 *An (unconditional)* rewrite theory $\mathcal{R}$ *is a 4-tuple* $\langle \Sigma, E, L, R \rangle$*, where* (Σ, E) *is an algebraic theory,* L *is a set of* labels *and* R *is a function* $R : L \to T_{\Sigma,E}(\mathsf{X}) \times T_{\Sigma,E}(\mathsf{X})$*, where* X *is a countable set of variables (indexed by sorts). The elements of* R *are called* rewrite rules *and will be denoted by*

$$\rho \ : \ t \longrightarrow t'$$

where ρ *is the label and* t, t' *stand for the congruence classes, according to the axioms in* E*. The terms* t *and* t' *are the initial and final terms of* ρ.

Compared with the definition in [Meseguer 1992], the above notion of rewrite theory is slightly simplified because here we assume that two distinct rewrite rules have different labels.

The next step relies on encoding the proofs of the logic in the terms of a language. Of course, in this way, proofs which are *essentially the same* are differentiated due to the rigidity of the intensional, syntactic description. Therefore a set of equations will be postulated. In this way, given a rewriting theory $\mathcal{R}$, we build up a model $\mathcal{T}_{\mathcal{R}}(\mathsf{X})$ which describes its *concurrent* semantics.

More formally, given a rewrite theory $\mathcal{R} = \langle \Sigma, E, L, R \rangle$, $\mathcal{T}_{\mathcal{R}}(\mathsf{X})$ is the category whose set of objects is $T_{\Sigma,E}(\mathsf{X})$ and whose arrows are equivalence classes of *proofs*, according to the axiomatization which follows. Proofs are terms generated by the following rules:

1. **Reflexivity**. $\forall t \in T_{\Sigma,E}(\mathsf{X})$

$$\frac{}{0_t \ : \ t \longrightarrow t}$$

2. Σ**-structure**. $\forall f \in \Sigma_{u_1,\cdots,u_n,u}$, π_i a proof of sort u_i:

$$\frac{\pi_1 \ : \ t_1 \longrightarrow t'_1 \ \ldots \ \pi_n \ : \ t_n \longrightarrow t'_n}{f(\pi_1, \ldots, \pi_n) \ : \ f(t_1, \ldots, t_n) \longrightarrow f(t'_1, \ldots, t'_n)}$$

where $f(\pi_1, \ldots, \pi_n)$ is a proof of sort u.

3. **Replacement**. $\forall\, \rho\, :\, t(x_1, \ldots, x_n) \longrightarrow t'(x_1, \ldots, x_n)\, \in R\, :$

$$\frac{\pi_1\, :\, t_1 \longrightarrow t'_1\, \ldots\, \pi_n\, :\, t_n \longrightarrow t'_n}{\rho(\pi_1, \ldots, \pi_n)\, :\, t(t_1/x_1, \ldots, t_n/x_n) \longrightarrow t'(t'_1/x_1, \ldots, t'_n/x_n)}$$

where π_i has the sort of x_i.

4. **Composition**

$$\frac{\pi\, :\, t_1 \longrightarrow t_2 \qquad \xi\, :\, t_2 \longrightarrow t_3}{\pi\, ;\, \xi\, :\, t_1 \longrightarrow t_3}$$

Notice that the rewrite rules play the role of extra constructors for building proofs, in addition to the function symbols in Σ.

WARNING: In the case of term rewriting systems, the notation $\rho : t(x_1, \cdots, x_n) \rightarrow t'(x_1, \cdots, x_n)$ wants to emphasize the set of free variables in the lhs of ρ (namely $\{x_1, \cdots, x_n\}$). By definition, the set of free variables in the rhs of ρ is a subset of $\{x_1, \cdots, x_n\}$. In general, the requirement $\mathsf{var}(t) \supseteq \mathsf{var}(t')$ is not imposed by Meseguer's method. So the most general assumption is $\{x_1, \cdots, x_n\} = \mathsf{var}(t) \cup \mathsf{var}(t')$.

Definition 6 *A proof is called an* elementary step *when it is derived by a finite application of rules 1, 2 and 3. A proof is a* step-derivation *when it is the sequential composition of elementary steps.*

The equations quotienting proofs are the following:

1. **Category**

$$Assoc)\;\; \forall \pi, \xi, \vartheta.\, (\pi\, ;\, \xi)\, ;\, \vartheta \;=\; \pi\, ;\, (\xi\, ;\, \vartheta) \qquad Id)\;\; \forall \pi\, :\, t \longrightarrow t'\, .\; 0_t\, ;\, \pi \;=\; \pi \;=\; \pi\, ;\, 0_{t'}$$

2. **Functoriality of the Σ-algebraic structure**. $\forall f \in \Sigma_{u_1, \cdots, u_n, u}$, π_i and ξ_i proofs of sort u_i

$$\begin{array}{ll} Comp) & f(\pi_1; \xi_1, \cdots, \pi_n; \xi_n) \;=\; f(\pi_1, \cdots, \pi_n)\, ;\; f(\xi_1, \cdots, \xi_n) \\ Ide) & f(0_{t_1}, \cdots, 0_{t_n}) \;=\; 0_{f(t_1, \cdots, t_n)} \end{array}$$

3. **Axioms** in E. For $t(x_1, \ldots, x_n) \;=\; t'(x_1, \ldots, x_n)$ an axiom in E, for all proofs $\pi_1, \ldots, \pi_n$, with π_i and x_i of the same sort,

$$t(\pi_1, \ldots, \pi_n) \;=\; t'(\pi_1, \ldots, \pi_n)$$

4. **Exchange**. $\forall\, \rho\, :\, t(x_1, \ldots, x_n) \longrightarrow t'(x_1, \ldots, x_n)\, \in R\, :$

$$\frac{\pi_1\, :\, t_1 \longrightarrow t'_1\, \ldots\, \pi_n\, :\, t_n \longrightarrow t'_n}{t(\pi_1, \ldots, \pi_n)\, ;\, \rho(0_{t'_1}, \ldots, 0_{t'_n}) \;=\; \rho(\pi_1, \ldots, \pi_n) \;=\; \rho(0_{t_1}, \ldots, 0_{t_n})\, ;\, t'(\pi_1, \ldots, \pi_n)}$$

We remark that, in order to increase the expressive power of the rewrite theory, open terms are also considered as states. In this way rewritings are *parametrized* transitions (i.e. procedures) that can be applied to every state obtained through a substitution of the left hand side of the rule.

Let us comment a little on Meseguer's axioms. The axioms of category follow from the fact that derivations are naturally equipped with the (partial) operation of concatenation which is associative and has identities. The functoriality of algebraic operations over terms expresses the independence of reductions of disjoint subexpressions. Let us illustrate this feature with an example.

Example 1 *Consider the term rewriting system whose signature Σ has three functions: a binary one, named f, a unary one called g and a nullary one, named h. The rewriting rule is*

$$r \,:\, g(x) \to x$$

Now, consider the term $t = f(g(h), g(h))$. Then, the two derivations starting at t and ending at $f(h, h)$

$$f(r(0_h),\, 0_{g(h)}));\, f(0_h,\, r(0_h))) \qquad\qquad f(0_{g(h)},\, r(0_h)));\, f(r(0_h),\, 0_h))$$

are equal according to the axioms of identity and functoriality. Notice that the equality expresses the fact that the two derivations can be performed in either order. Notice also that the above derivations are also equal to $f(r(0_h),\, r(0_h)))$, where both redexes are contracted at the same time.

There is another key axiom, besides functoriality: the *exchange axiom*. The exchange axiom captures the phenomena of duplication and erasing of redexes. For instance, add the following rule to the rewriting system of Example 1:

$$s \,:\, g(x) \to f(x,\, x)$$

(notice that r and s have a critical pair). Take the term $g(g(h))$. According to the exchange axiom, the following two derivations are equal:

$$g(r(0_h));\, s(0_h) \qquad\qquad s(0_{g(h)});\, f(r(0_h), r(0_h))\ .$$

In particular, in the derivation on the right, two copies of the reduction $r(0_h)$ are fired, according to the occurrences of the free variable x in the rhs of the rule s.

Remarks: (1) Observe that, if ρ is the name of a rule, then $\rho(\pi_1, \cdots, \pi_n)$ will denote a parametric reduction in Meseguer's method: it means the *parallel* reduction firing ρ and $\pi_1, \cdots, \pi_n$ at the same time. The interesting point is that, for every i, π_i is internal to the expression replacing the i-th variable of the rule. That is, the set of redexes represented by

ρ and $\pi_1, \cdots, \pi_n$ is consistent. The contrary also holds: a consistent set of redexes can be "algebraicized".

(2) For trs's, in the sense of Definition 1, the axioms E in the rewriting theory $\langle \Sigma, E, L, R \rangle$ are empty. However, such set E of axioms will play an essential role in the second part of the paper when we will instantiate the method to Combinatory Reduction Systems. In that case, expressions are quotiented by α-conversion and axioms modeling substitution.

The following lemma states a useful property of the derivations yielded by the above machinery.

Lemma 1 *[Meseguer 1992] Every derivation is equal to a sequence of elementary steps.*

Finally, we remark that the set of proofs does not have the structure of a (total) algebra, because of the presence of the partial operation ';'. However, the previous presentation, by writing $\pi : t \to t'$, uses a typing mechanism (see, for instance, [Manca and Salibra and Scollo 1990]) which allows ";" to be defined as a total operation over properly typed terms (types are the collection of pairs $t \to t'$). Typed algebraic theories have an initial model whose identifications are exactly those obtained by ground instantiations of a typed deductive system. In our case, since types have a free structure, the deductive system is the Birkhoff equational deductive system (with type information).

In the paper we are not fussy about types, assuming that sequential composition is always applied to correctly typed arguments.

NOTATION: We will call $\mathcal{M}$ the category yielded by Meseguer's paradigm and $=_M$ the corresponding equivalence relation between derivations. Again, remark that the notation leaves implicit the signature of the rewriting system and the set of free variables. Note also that, since we have assumed many-sorted signatures, there is in fact a category $\mathcal{M}_s$, for each sort s. However, in all the examples considered in this paper there will be a principal sort of interest p, and $\mathcal{M}$ then denotes $\mathcal{M}_p$.

3 The coincidence of $\equiv$ and Meseguer's semantics for trs's

Let (Σ, R) be a trs. We have two categories. The first, $\mathcal{L}$, is provided by permutation equivalence, the other, $\mathcal{M}$, by the method of the previous section (we assume the set of free variables is the same).

We want to show that $\mathcal{L}$ and $\mathcal{M}$ are the same category. Formally, we have to provide a pair of functors equating them. Let $\mathcal{F} : \mathcal{L} \to \mathcal{M}$ and $\mathcal{G} : \mathcal{M} \to \mathcal{L}$ be such that $\mathcal{F}$ and $\mathcal{G}$ are the identity function on the objects. As far as arrows are concerned, it is enough to define $\mathcal{F}$ over parallel reductions: its definition over derivations will follow by functoriality. That is, $\mathcal{F}(\mathbf{U}_1; \cdots; \mathbf{U}_n) = \mathcal{F}(\mathbf{U}_1); \cdots; \mathcal{F}(\mathbf{U}_n)$. $\mathcal{G}$ will be defined by induction over the structure of the arrows. The difficult part will be to show that $\mathcal{F}$ and $\mathcal{G}$ are well defined, i.e., that equal derivations on one side are mapped into equal derivations on the other side.

The definitions of the functor $\mathcal{F}$ will exploit the following function κ (U is a consistent set of redexes in t):

$$\kappa_t(\mathbf{U}) = \begin{cases} 0_t & \text{if } U = \emptyset \\ f(\kappa_{t_1}(\mathbf{U}_1), \cdots, \kappa_{t_n}(\mathbf{U}_n)) & \text{if } \varepsilon \notin U \ \textbf{and} \ t = f(t_1, \cdots, t_n) \\ r(\kappa_{t'_1}(\mathbf{V}_1), \cdots, \kappa_{t'_m}(\mathbf{V}_m)) & \text{if } \varepsilon^r \in U \end{cases}$$

where $U_i = \{u \mid i \cdot u \in U\}$ and $V_i = \{v \mid w_i \cdot v \in U\}$, where w_i is the access path of the i-th variable in the lhs of r. The expression t'_i is that at access path w_i in t. In order to define $\mathcal{G}$, we need some operations over (parallel) derivations:

(prefixing) $i \cdot (\mathbf{U}_1; \cdots; \mathbf{U}_n) = i \cdot \mathbf{U}_1; \cdots; i \cdot \mathbf{U}_n$;

(union) $\bigcup_{1 \le i \le m}(\mathbf{U}^i_1; \cdots; \mathbf{U}^i_{n_i}) = \left(\bigcup_{1 \le i \le m} \mathbf{U}^i_1\right) ; \cdots ; \left(\bigcup_{1 \le i \le m} \mathbf{U}^i_q\right)$, where $q = \mathbf{max}\{n_i \mid 1 \le i \le m\}$ and $U^i_k = \emptyset$ if $n_i < k$ (provided that every $\bigcup_{1 \le i \le m} \mathbf{U}^i_j$ is consistent);

(firing) $[r]_i(\mathbf{U}_1; \cdots; \mathbf{U}_n) = w_i \cdot \mathbf{U}_1; W_i \cdot \mathbf{U}_2; \cdots; W_i \cdot \mathbf{U}_n$, where w_i is the access path of the i-th variable in the lhs of the rule r and W_i is the set of access paths of the same variable in the rhs of r.

The only operator that is not intuitive is *firing*. The idea behind $[r]_i(\mathbf{U}_1; \cdots; \mathbf{U}_n)$ is that $\mathbf{U}_1; \cdots; \mathbf{U}_n$ is internal to the i-th variable of r and it is fired together with r. Notice that r is fired at the same time as $\mathbf{U}_1$.

Definition 7 *The mapping $\mathcal{F} : \mathcal{L} \to \mathcal{M}$ is defined as follows ($\mathbf{U}$ is a consistent set of redexes):*

$$\mathcal{F}(\mathbf{U}) = \kappa_t(\mathbf{U}) \qquad\qquad \mathcal{F}(\sigma; \rho) = \mathcal{F}(\sigma); \mathcal{F}(\rho)$$

The mapping $\mathcal{G} : \mathcal{M} \to \mathcal{L}$ is defined by induction over the syntactic structure of derivations in $\mathcal{M}$ by the following rules:

$$\begin{aligned} \mathcal{G}(0_t) &= \emptyset \\ \mathcal{G}(f(\pi_1, \cdots, \pi_n)) &= \textstyle\bigcup_{1 \le i \le n} i \cdot \mathcal{G}(\pi_i) \\ \mathcal{G}(r(\pi_1, \cdots, \pi_n)) &= \{\varepsilon^r\} \cup (\textstyle\bigcup_{1 \le i \le n} [r]_i \mathcal{G}(\pi_i)) \\ \mathcal{G}(\sigma; \rho) &= \mathcal{G}(\sigma); \mathcal{G}(\rho) \end{aligned}$$

Notice the choice made in the definition of $\mathcal{G}(r(\pi_1, \cdots, \pi_n))$ of firing the outermost together with those fired at the "first step". Other choices could be possible (firing ε^r as last reduction, for example), which, however, would invalidate the correspondence between elementary steps and consistent sets. The main motivation supporting our choice is Lemma 4.

Proposition 1 *U is a consistent set of redexes if and only if it can be "algebraicized" (i.e., $\mathcal{F}(\mathbf{U})$ is an elementary step).*

PROOF: Obvious consequence of definitions.

Let us embark on the proof of the isomorphism of $\mathcal{L}$ and $\mathcal{M}$. The first step consists in showing that the functors $\mathcal{F}$ and $\mathcal{G}$ are well-defined. That is:

(1) if σ and ρ are two derivations in $\mathcal{L}$, then $\sigma \equiv \rho$ implies that $\mathcal{F}(\sigma) =_M \mathcal{F}(\rho)$ (see Lemma 2);

(2) if σ and ρ are two derivations in $\mathcal{M}$ then $\sigma =_M \rho$ implies that $\mathcal{G}(\sigma) \equiv \mathcal{G}(\rho)$ (see Lemma 3),

As far as $\mathcal{F}$ is concerned, it is enough to check that the three basic axioms of "$\equiv$" can be proved from those of $=_M$ after the mapping. In the proof we will use two technical propositions (Proposition 2 and 3) that, to ease the exposition, will be proved at the end of the section. The $\mathcal{G}$ case is a bit harder, because, besides the axioms (of which there are more), we must verify that rules of the (typed) Birkhoff deductive system still produce permutation equivalent derivations.

Lemma 2 *If $\sigma \equiv \rho$, then $\mathcal{F}(\sigma) =_M \mathcal{F}(\rho)$.*

PROOF: It is enough to verify the basic axioms of $\equiv$. The remaining work will be done by the functoriality of $\mathcal{F}$ and the congruence of $\equiv$ w.r.t. ";". The non-trivial axiom is the first one in Definition 4. Let $U \cup V$ be a consistent set in t. We must prove that

$$\mathcal{F}(\mathbf{U}); \mathcal{F}(\mathbf{V}/\mathbf{U}) \quad =_M \quad \mathcal{F}(\mathbf{V}); \mathcal{F}(\mathbf{U}/\mathbf{V})$$

(we recall that $\mathbf{V}/\mathbf{U}$ and $\mathbf{U}/\mathbf{V}$ are consistent sets of redexes: see [Boudol 1985]).

We use double induction over the cardinality of $U \cup V$ and the structure of t. The basic case is immediate. Let us discuss the inductive step. Let $t = f(t_1, \cdots, t_n)$. There are two subcases: either $\varepsilon \in U \cup V$ or $\varepsilon \notin U \cup V$. We prove first the second case, which is simpler.

(case $\varepsilon \notin U \cup V$) If both U and V are internal to some t_i then the statement follows easily by induction. Therefore $U = \bigcup_{1 \le i \le n} i \cdot U_i$ and $V = \bigcup_{1 \le i \le n} i \cdot V_i$, where $U_i = \{u_i \mid i \cdot u_i \in U\}$ and $V_i = \{v_i \mid i \cdot v_i \in V\}$. Let $t' = f(t'_1, \cdots, t'_n)$ be the ending term of $\mathbf{U}$ and $t'' = f(t''_1, \cdots, t''_n)$ be the ending term of $\mathbf{V}$. By Proposition 2, $V/\mathbf{U} = \bigcup_{1 \le i \le n} i \cdot (V_i/\mathbf{U}_i)$. Therefore

$$\kappa_{t'}(\mathbf{V}/\mathbf{U}) \;=\; f(\kappa_{t'_1}(\mathbf{V}_1/\mathbf{U}_1), \cdots, \kappa_{t'_n}(\mathbf{V}_n/\mathbf{U}_n)) \,.$$

Then

$$\begin{array}{rcl}
\mathcal{F}(\mathbf{U}); \mathcal{F}(\mathbf{V}/\mathbf{U}) & = & \kappa_t(\mathbf{U}); \kappa_{t'}(\mathbf{V}/\mathbf{U}) \\
& = & f(\kappa_{t_1}(\mathbf{U}_1), \cdots, \kappa_{t_n}(\mathbf{U}_n)) \;;\; f(\kappa_{t'_1}(\mathbf{V}_1/\mathbf{U}_1), \cdots, \kappa_{t'_n}(\mathbf{V}_n/\mathbf{U}_n)) \\
& \overset{(\star)}{=}_M & f(\kappa_{t_1}(\mathbf{U}_1); \kappa_{t'_1}(\mathbf{V}_1/\mathbf{U}_1), \cdots, \kappa_{t_n}(\mathbf{U}_n); \kappa_{t'_n}(\mathbf{V}_n/\mathbf{U}_n)) \\
& \overset{(\star\star)}{=}_M & f(\kappa_{t_1}(\mathbf{V}_1); \kappa_{t''_1}(\mathbf{U}_1/\mathbf{V}_1), \cdots, \kappa_{t_n}(\mathbf{V}_n); \kappa_{t''_n}(\mathbf{U}_n/\mathbf{V}_n)) \\
& = & \mathcal{F}(\mathbf{V}) \;;\; \mathcal{F}(\mathbf{U}/\mathbf{V})
\end{array}$$

where $\stackrel{(\star)}{=}$ follows by functoriality of f and $\stackrel{(\star\star)}{=}$ by the inductive hypothesis.

(case $\varepsilon \in U \cup V$) Assume that $\varepsilon \in V$ and $\varepsilon \notin U$. Then, by Proposition 3, $V/\mathbf{U} = \{\varepsilon\} \cup (\bigcup_{w_i} w_i \cdot (V_i/\mathbf{U}_i))$, where w_i is the access path of the i-th variable in the lhs of the rule firing ε and $U_i = \{u \mid w_i \cdot u \in U\}$ and $V_i = \{v \mid w_i \cdot v \in V\}$. Let $r(x_1, \cdots, x_n)$ be the rule firing the redex at ε and $t^\star(x_1, \cdots, x_n)$ and $t^\bullet(x_1, \cdots, x_n)$ be its initial and final term, respectively.

Again, let $t' = f(t'_1, \cdots, t'_n)$ be the final term of $\mathbf{U}$. By definition of $\kappa_{t'}$, $\kappa_{t'}(\mathbf{V}/\mathbf{U}) = r(\kappa_{t'_1}(\mathbf{V}_1/\mathbf{U}_1), \cdots, \kappa_{t'_n}(\mathbf{V}_n/\mathbf{U}_n))$, where t'_i is the subterm at w_i in t'. By applying the Exchange axiom, we get

$$\begin{array}{rcl} r(\kappa_{t'_1}(\mathbf{V}_1/\mathbf{U}_1), \cdots, \kappa_{t'_n}(\mathbf{V}_n/\mathbf{U}_n)) & =_M & t^\star(\kappa_{t'_1}(\mathbf{V}_1/\mathbf{U}_1), \cdots, \kappa_{t'_n}(\mathbf{V}_n/\mathbf{U}_n))\ ; \\ & & \ r(0_{t''_1}, \cdots, 0_{t''_n}) \\ & =_M & r(0_{t'_1}, \cdots, 0_{t'_n})\ ; \\ & & t^\bullet(\kappa_{t'_1}(\mathbf{V}_1/\mathbf{U}_1), \cdots, \kappa_{t'_n}(\mathbf{V}_n/\mathbf{U}_n)) \end{array}$$

where t''_i is the final term of $\mathbf{V}_i/\mathbf{U}_i$. Now, let us consider $\mathbf{U};\mathbf{V}/\mathbf{U}$:

$$\begin{array}{rcl} \mathcal{F}(\mathbf{U});\mathcal{F}(\mathbf{V}/\mathbf{U}) & = & \kappa_t(\mathbf{U});\kappa_{t'}(\mathbf{V}/\mathbf{U}) \\ & =_M & t^\star(\kappa_{t_1}(\mathbf{U}_1), \cdots, \kappa_{t_n}(\mathbf{U}_n))\ ;\ t^\star(\kappa_{t'_1}(\mathbf{V}_1/\mathbf{U}_1), \cdots, \kappa_{t'_n}(\mathbf{V}_n/\mathbf{U}_n))\ ; \\ & & r(0_{t''_1}, \cdots, 0_{t''_n}) \\ & \stackrel{(\star)}{=}_M & t^\star(\kappa_{t_1}(\mathbf{U}_1);\kappa_{t'_1}(\mathbf{V}_1/\mathbf{U}_1), \cdots, \kappa_{t_n}(\mathbf{U}_n));\kappa_{t'_n}(\mathbf{V}_n/\mathbf{U}_n))\ ; \\ & & r(0_{t''_1}, \cdots, 0_{t''_n}) \\ & \stackrel{(\star\star)}{=}_M & t^\star(\kappa_{t_1}(\mathbf{V}_1);\kappa_{t^+_1}(\mathbf{U}_1/\mathbf{V}_1), \cdots, \kappa_{t_n}(\mathbf{V}_n);\kappa_{t^+_n}(\mathbf{U}_n/\mathbf{V}_n))\ ; \\ & & r(0_{t''_1}, \cdots, 0_{t''_n}) \\ & =_M & t^\star(\kappa_{t_1}(\mathbf{V}_1), \cdots, \kappa_{t_n}(\mathbf{V}_n))\ ;\ t^\star(\kappa_{t^+_1}(\mathbf{U}_1/\mathbf{V}_1), \cdots, \kappa_{t^+_n}(\mathbf{U}_n/\mathbf{V}_n))\ ; \\ & & r(0_{t''_1}, \cdots, 0_{t''_n}) \end{array}$$

where t^+_i is the final term of $\mathbf{V}_i$. The equality marked $(\star)$ follows from functoriality of $t^\star$ and that marked $(\star\star)$ is due to the inductive hypothesis. The set $U/\mathbf{V}$ is a consistent set in t^+, the final term of the reduction $\mathbf{V}$. Therefore, the Exchange axiom can be applied to $t^\star(\kappa_{t^+_1}(\mathbf{U}_1/\mathbf{V}_1), \cdots, \kappa_{t^+_n}(\mathbf{U}_n/\mathbf{V}_n))\ ;\ r(0_{t''_1}, \cdots, 0_{t''_n})$ yielding

$$r(0_{t^+_1}, \cdots, 0_{t^+_n})\ ;\ t^\bullet(\kappa_{t^+_1}(\mathbf{U}_1/\mathbf{V}_1), \cdots, \kappa_{t^+_n}(\mathbf{U}_n/\mathbf{V}_n)).$$

Notice that $t^\star(\kappa_{t_1}(\mathbf{V}_1), \cdots, \kappa_{t_n}(\mathbf{V}_n))\ ;\ r(0_{t^+_1}, \cdots, 0_{t^+_n})$ can be easily proved equal to $\mathcal{F}(\mathbf{V})$. Therefore, the statement of the lemma holds if $\mathcal{F}(\mathbf{U}/\mathbf{V}) = t^\bullet(\kappa_{t^+_1}(\mathbf{U}_1/\mathbf{V}_1), \cdots, \kappa_{t^+_n}(\mathbf{U}_n/\mathbf{V}_n))$. This latter equality is a simple consequence of Proposition 3 and the definition of κ.

Observe that the case where ε belongs both to U and V reduces to the previous one because $U/\mathbf{V} = (U \setminus \{\varepsilon\})/\mathbf{V}$.

Lemma 3 *If $\sigma =_M \rho$ then $\mathcal{G}(\sigma) \equiv \mathcal{G}(\rho)$.*

PROOF: We prove the statement by induction over the depth ℓ of the proof of $\sigma =_M \rho$. (**basic case**) When $\ell = 0$, as usual, there are two subcases: $\sigma =_M \rho$ is an axiom or an instance of the reflexivity rule. Reflexivity is an immediate consequence of the fact that $\equiv$ is an equivalence relation. When $\sigma =_M \rho$ is an axiom, there are three cases.

(Axioms of category) Obvious consequence of the functoriality of $\mathcal{G}$.

(Axioms of functoriality) They follow easily by definition of $\mathcal{G}$.

(Axiom of Exchange) Firstly, let us prove the case concerning elementary steps. Let $r(x_1, \cdots, x_n) : t(x_1, \cdots, x_n) \rightarrow t'(x_1, \cdots, x_n)$ be a rewriting rule. The axiom we must verify is $t(\pi_1, \cdots, \pi_n); r(0_{t'_1}, \cdots, 0_{t'_n}) = r(\pi_1, \cdots, \pi_n)$ (with π_i elementary steps). By definition $\mathcal{G}(t(\pi_1), \cdots, \pi_n)) = \bigcup_{w_i} w_i \cdot \mathcal{G}(\pi_i)$, where w_i is the access path of the variable x_i in $t(x_1, \cdots, x_n)$. Moreover $\mathcal{G}(r(0_{t'_1}, \cdots, 0_{t'_n})) = \{\underline{\varepsilon}^r\}$ and $\mathcal{G}(r(\pi_1, \cdots, \pi_n)) = \{\underline{\varepsilon}^r\} \cup (\bigcup_{w_i} w_i \cdot \mathcal{G}(\pi_i)$ because π_i are elementary steps. Now the equality follows by taking $\mathbf{V} = \{\underline{\varepsilon}^r\} \cup (\bigcup_{w_i} w_i \cdot \mathcal{G}(\pi_i)$ and $\mathbf{U} = \bigcup_{w_i} w_i \cdot \mathcal{G}(\pi_i)$. In order to show the other "half" $r(0_{t'_1}, \cdots, 0_{t'_n}); t'(\pi_1, \cdots, \pi_n) = r(\pi_1, \cdots, \pi_n)$, take $\mathbf{U} = \{\underline{\varepsilon}^r\}$ and $\mathbf{V}$ as before.

When π_i are not elementary steps, we prove the Exchange axiom by reducing the proof to the previous case. For instance, let $\pi_i = \zeta_1^i; \cdots; \zeta_{m_i}^i$. In order to show that

$$\begin{aligned}\mathcal{G}(r(\zeta_1^1; \cdots; \zeta_{m_1}^1, \cdots, \zeta_1^n; \cdots; \zeta_{m_n}^n)) &= \mathcal{G}(t(\zeta_1^1; \cdots; \zeta_{m_1}^1, \cdots, \zeta_1^n; \cdots; \zeta_{m_n}^n)) \,; \\ &\quad\ \mathcal{G}(r(0_{t'_1}, \cdots, 0_{t'_n}))\end{aligned}$$

holds, we must move the reduction $\{\underline{\varepsilon}^r\}$ to the end of the derivation yielded by the lhs of the above equality. The elementary steps of such operation exploit the basic case. This check is quite tedious: we leave it to the reader. The other half of the Exchange axiom is even simpler because, due to the definition of $\mathcal{G}$, the basic case must be applied exactly once (to the first step, in order to move the reduction $\underline{\varepsilon}^r$ to the front of the derivation).

(**inductive case**) Assuming that we have proved the statement of the lemma for $\ell = n$, the case $\ell = n + 1$ is immediate. For instance, when the last rule is the congruence (b_5), it follows by the fact that permutation equivalence is a congruence w.r.t. algebraic operators.

The following lemma states that $\mathcal{F}$ and $\mathcal{G}$ are inverse to each other when consistent set of redexes are considered. Theorem 2 will generalize Lemma 4 to derivations.

Lemma 4 *Let U be a consistent set of redexes in t, and let π be an elementary step. Then $\mathcal{G}(\mathcal{F}(\mathbf{U})) = \mathbf{U}$ and $\mathcal{F}(\mathcal{G}(\pi)) = \pi$.*

PROOF: The proof of $\mathcal{G}(\mathcal{F}(\mathbf{U})) = \mathbf{U}$ goes by induction over the cardinality of U; that of $\mathcal{F}(\mathcal{G}(\pi)) = \pi$ is by induction over the structure of π.

($(\mathcal{G}(\mathcal{F}(\mathbf{U})) = \mathbf{U})$) The non-trivial case is the inductive step. Assume that $\underline{\varepsilon}^r \in \mathbf{U}$ and let u_i be the access path of the i-th free variable in the lhs of r. Observe that, by definition of consistency, for each $\mathbf{u} \in \mathbf{U} \setminus \{\underline{\varepsilon}^r\}$, $u = u_i \cdot v_i$, for some u_i and v_i. Therefore

$$\begin{array}{rcl}\mathcal{G}(\mathcal{F}(\mathbf{U})) & = & \mathcal{G}(\kappa_t(\mathbf{U})) \\ & = & \mathcal{G}(r(\kappa_{t'_1}(\mathbf{V}_1), \cdots, \kappa_{t'_n}(\mathbf{V}_n))) \\ & = & \{\underline{\varepsilon}^r\} \cup (\bigcup_{1 \le i \le n} u_i \cdot \mathcal{G}(\kappa_{t'_i}(\mathbf{V}_i))) \\ & = & \mathbf{U}.\end{array}$$

where the notation is the same as in the definition of $\kappa_t(\mathbf{U})$.

When $\underline{\varepsilon} \notin \mathbf{U}$, then let $t = f(t_1, \cdots, t_n)$ and $U_i = \{u_i \mid i \cdot u_i \in U\}$. Then, we easily get $U = \bigcup_{1 \le i \le n} U_i$. If there exist i, j, $i \neq j$ with U_i, $U_j \neq \emptyset$, then we can apply the inductive hypothesis to them and get in a standard way the statement of the lemma. Otherwise, $U = U_i$, for some i. Then repeat the above reasoning over U_i. Eventually we will end up in one of the basic cases.

($(\mathcal{F}(\mathcal{G}(\pi)) = \pi)$) The case $\pi = 0_t$ is obvious. The case $\pi = f(\pi_1, \cdots, \pi_n)$ follows in a standard way from the inductive hypothesis. When $\pi = r(\pi_1, \cdots, \pi_n)$ then $\mathcal{F}(\mathcal{G}(\pi)) = k_t(\mathcal{G}(\pi)) = \kappa_t(\{\underline{\varepsilon}^r\} \cup (\bigcup_i u_i \cdot \mathcal{G}(\pi_i)) = r(\pi_1, \cdots, \pi_n)$, by definition of κ_t and the inductive hypothesis.

Theorem 2 *$\mathcal{L}$ and $\mathcal{M}$ are isomorphic categories.*

PROOF: The two mappings providing the isomorphism are $\mathcal{F}$ and $\mathcal{G}$. Indeed, Lemma 2 and Lemma 3 guarantee that they are well-defined. Moreover $\mathcal{F}$ and $\mathcal{G}$ are obviously functors. Let us show that $\mathcal{G}(\mathcal{F}(\sigma)) = \sigma$ and $\mathcal{F}(\mathcal{G}(\sigma)) = \sigma$. In the first equality, by definition, $\sigma = \mathbf{U}_1; \cdots; \mathbf{U}_n$. So the equality follows by functoriality of $\mathcal{F}$ and $\mathcal{G}$ and Lemma 4. For the second equality, take a derivation $\sigma = \pi_1; \cdots; \pi_n$ where the π_i are elementary steps (it exists by Lemma 1). Again, the equality $\mathcal{F}(\mathcal{G}(\pi_1; \cdots; \pi_n)) = \pi_1; \cdots; \pi_n$ follows by functoriality of $\mathcal{F}$ and $\mathcal{G}$ and Lemma 4.

3.1 Technical propositions

We devote this subsection to the proof of the two propositions that have been used to prove Lemma 2.

Proposition 2 *Let $t = f(t_1, \cdots, t_n)$ and let $U \cup V$ be a consistent set of redexes in t such that $\varepsilon \notin U \cup V$. Let $U_i = \{u_i \mid i \cdot u_i \in U\}$ and $V_i = \{v_i \mid i \cdot v_i \in V\}$; then $V_i/\mathbf{U}_i = \{v \mid i \cdot v \in V/\mathbf{U}\}$ and $V/\mathbf{U} = \bigcup_{1 \le i \le n} i \cdot (V_i/\mathbf{U}_i)$.*

PROOF: Let us show that $V_i/\mathbf{U}_i = \{v \mid i \cdot v \in V/\mathbf{U}\}$. By hypothesis $V = \bigcup_{1 \le i \le n} i \cdot V_i$. Observe that $(i \cdot V_i)/\mathbf{U} = (i \cdot V_i)/(i \cdot \mathbf{U}_i)$, because redexes in U_j, $i \neq j$, are disjoint w.r.t. those in $i \cdot V_i$ and, thus, can not affect them. By definition,

$$(i \cdot V_i)/(i \cdot \mathbf{U}_i) = \{(i \cdot v)/(i \cdot \mathbf{U}_i) \mid i \cdot v \in i \cdot V_i\}$$

and $(i \cdot v)/(i \cdot \mathbf{U}_i)$ is given in terms of a development $\sigma = \mathbf{w}_1; \cdots; \mathbf{w}_p$ of $i \cdot \mathbf{U}_i$. Therefore, $(i \cdot v)/(i \cdot \mathbf{U}_i) = \{i \cdot w \mid i \cdot w \in (i \cdot v)/\sigma\}$. It is simple to prove that σ is internal to the i-th argument of f, i.e. $w_j = i \cdot w'_j$.

The last step consists in showing $\{w \mid w \in (i \cdot v)/\sigma\} = i \cdot \{w' \mid w' \in v/\sigma'\}$, where $\sigma' = \mathbf{w}'_1; \cdots; \mathbf{w}'_p$. That is, we prove that

$$w \in (i \cdot v)/\sigma \quad \Leftrightarrow \quad w = i \cdot w' \text{ and } w' \in v/\sigma'$$

by induction over the length of σ. The basic case is immediate. For the inductive case, by definition,

$$(i \cdot v)/(\sigma; \mathbf{u}) \;=\; \{z \mid z \in w/\mathbf{u} \text{ and } w \in (i \cdot v)/\sigma\} \;.$$

By the inductive hypothesis, $w = i \cdot w'$ and $w' \in v/\sigma'$. Since $u = i \cdot u'$, $z \in (i \cdot v)/\sigma$ satisfies $z = i \cdot z'$. It is now easy to prove the proposition.

The fact that $V/\mathbf{U} = \bigcup_{1 \leq i \leq n} i \cdot (V_i/\mathbf{U}_i)$ is an immediate consequence of disjointness of V_i w.r.t. V_j, $i \neq j$, and the previous discussion.

Proposition 3 *Let $U \cup V$ be a consistent set of redexes in t such that $\varepsilon \in V$ and $\varepsilon \notin U$. Let w_i (resp. W_i) be the access path (resp. the set of access paths) of the i-th variable in the lhs (resp. rhs) of the rule firing ε and $U_i = \{u \mid w_i \cdot u \in U\}$ and $V_i = \{v \mid w_i \cdot v \in V\}$.*

Then $V/\mathbf{U} = \{\varepsilon\} \cup (\bigcup_{w_i} w_i \cdot (V_i/\mathbf{U}_i))$ and $U/\mathbf{V} = W_i \cdot (U_i/\mathbf{V}_i)$.

Proof: By definition of consistency, redexes in U and $V \setminus \{\varepsilon\}$ are of the form $w_i \cdot v$, where w_i is the access path of a variable in the lhs of the rule r firing ε. The equality $V/\mathbf{U} = \{\varepsilon\} \cup (\bigcup_{w_i} w_i \cdot (V_i/\mathbf{U}_i))$ follows by arguing as in Proposition 2, since $i \neq j$ implies $w_i \neq w_j$.

Let us prove that $U/\mathbf{V} = W_i \cdot (U_i/\mathbf{V}_i)$. By hypothesis, $\underline{\varepsilon}^r; \mathbf{V}/\underline{\varepsilon}^r$ is a development of V. By definition $V/\underline{\varepsilon}^r = \bigcup_i \{W_i \cdot v \mid w_i \cdot v \in V\}$, where w_i is the access path of the i-th variable in the lhs of r and W_i is the set of access paths of the i-th variable in the rhs of r. Similarly, $U/\underline{\varepsilon}^r = \bigcup_i \{W_i \cdot u \mid w_i \cdot u \in U\}$. Thus,

$$U/(\underline{\varepsilon}^r; \mathbf{V}/\underline{\varepsilon}^r) \;=\; (U/\underline{\varepsilon}^r)/(V/\underline{\varepsilon}^r)$$

and the statement of the proposition follows by substituting equals for equals.

4 A counterexample with a rewriting system modulo axioms

Theorem 2 does not hold when rewritings modulo axioms E are taken into consideration. More precisely, if terms are quotiented by axioms, it can happen that axioms interfere with the rewriting rules in a way that is not recognized by Meseguer's axiomatization. This is the case when we have a critical pair between a left-hand side of a rewriting rule and one side of an axiom. Let us see an example.

Example 2 *As an explanatory example, take the λ-calculus with explicit substitution [Abadi, Cardelli, Curien and Lévy 1990]. The language consists of the following syntax:*

$$\textbf{Terms} \qquad a \ ::= \ \mathtt{1} \ | \ ab \ | \ \lambda a \ | \ a\,[s]$$

$$\textbf{Substitutions} \qquad s \ ::= \ id \ | \ \uparrow \ | \ a \cdot s \ | \ s \circ t$$

Notice that there are no variable names (de Bruijn numbers are used, that allow giving up α-conversion) and substitutions are provided with a "syntactic status" by means of the operation $a\,[s]$. The operations over terms do not need further comments. The substitution id *is the identity substitution $[^{\mathtt{i}}/_{\mathtt{i}}]$, for all* $\mathtt{i}$*. The* shift *operation $\uparrow$ is the substitution $[^{\mathtt{i+1}}/_{\mathtt{i}}]$. For instance, the de Bruijn number $\mathtt{n}$ is represented by $\mathtt{1}[\uparrow^n]$, where $\uparrow^n$ is the composition of n* shifts*, $\uparrow \circ \cdots \circ \uparrow$. The* cons *$a \cdot s$ of a onto s means the substitution $[^{a}/_{\mathtt{1}},\ ^{s(i)}/_{\mathtt{i+1}}]$. The operation $s \circ t$ is the composition of s and t.*

From the operational point of view, making the substitutions explicit also means making explicit the computations of substitutions (they are considered internal *in the λ-calculus and Combinatory Reduction Systems). That is, explicit rules (or axioms) must be added in order to compute substitutions.*

The standard β-reduction is encoded by the following rule:

$$\beta(X,\,Y) \ \ : \ \ (\lambda X)Y \ \rightarrow \ X\,[Y \cdot id]$$

Terms are taken up to equivalence modulo the following axiomatization:

$$\begin{array}{ll}
\mathtt{1}[id] = \mathtt{1} & id \circ s = s \\
\mathtt{1}[a \cdot s] = a & \uparrow \circ id = \uparrow \\
(ab)[s] = (a[s])(b[s]) & \uparrow \circ (a \cdot s) = s \\
(\lambda a)[s] = \lambda(a[\mathtt{1} \cdot (s \circ \uparrow)]) & (a \cdot s) \circ t = a[t] \cdot (s \circ t) \\
a[s][t] = a[s \circ t] & (s_1 \circ s_2) \circ s_3 = s_1 \circ (s_2 \circ s_3)
\end{array}$$

where the axioms in the first column allow pushing substitutions inside λ-expressions, whilst those in the second column manage the composition of substitutions.

The interesting remark for what follows is the presence of a critical pair between the left hand side of the β-rule and the third axiom in the leftmost column (pushing substitutions inside applications).

Let us apply Meseguer's method. We have two categories generated by the sorts of λ-terms and of substitutions, respectively, modulo the above substitution axioms. The category of substitutions has no proper reduction: there are only identity arrows up to the axioms that come from the rightmost column above. So we will not care about this category. In the category of λ-terms we have the category axioms, the functoriality of λ and application, the lifting of the substitution axioms and the exchange axioms. Now, take the following two reductions:

$$\beta(0_{\mathtt{1}},\,0_{\mathtt{1}})[0_{\mathtt{1}[\uparrow]} \cdot id] \qquad\qquad \beta(0_{\mathtt{1}},\,0_{\mathtt{1}[\uparrow]})$$

These two reductions should be the same because they express the unique contraction in the term $(\lambda\mathtt{1})(\mathtt{1}[\uparrow])$, that is equivalent to $((\lambda\mathtt{1})\mathtt{1})[0_{\mathtt{1}[\uparrow]} \cdot id]$. There is no axiom provided by

Meseguer forcing such identifications. This is because the operators corresponding to proper rewriting rules (the "β", in this case) are introduced "freely" in the space of derivations, without taking into account possible interferences with axioms quotienting the syntax. In particular, in the above case, we should need an axiom like

$$\beta(a, b)[s] = \beta(a[\mathtt{1} \cdot (s \circ \uparrow)], b[s])$$

that is, pushing the substitution inside the β-constructor.

As the reader may expect, the problem of λ-calculus with explicit substitution is also present in the setting of Combinatory Reduction Systems. We devote the remaining part of the paper to describing how the incompleteness of Meseguer's axiomatization w.r.t. permutation equivalence can be solved in the case of CRS's. We will avoid dealing with explicit substitutions, preferring to remain at the abstraction level of CRS's (namely we shall have variable names and *implicit* substitutions). The price we pay is that the axiomatization quotienting the expressions is countably infinite, due to the presence of axiom schemata for α-conversion and substitutions, but we gain the advantage of having a presentation more readable by (most) humans.

5 Orthogonal Combinatory Reduction Systems

A *Combinatory Reduction System* (shortened into CRS) is defined by a *signature* Σ and a set of *rewriting rules* R.

(**The signature**) The signature Σ consists of a countable set of *variables* and a set of *forms*. Forms will be ranged over by $\mathbf{f}$, $\mathbf{g}$, etc. Variables will be ranged over by x, y, z, $\cdots$, possibly indexed. Vectors of variables will be denoted by $\vec{x}_i^j$ where j is used to discriminate between vectors and i states the length of the vector. Thus, we assume that $\langle x_1^j, \cdots, x_i^j \rangle$ is the vector corresponding to $\vec{x}_i^j$. We will often omit the index i, and vectors of length 1 will be denoted by the variable name (without any bracket in this case). For simplicity, we will assume that variables inside a vector are pairwise different. Moreover, with a bit of inaccuracy, we will use set-theoretic operations over vectors: in those cases vectors are to be considered as the set of elements they have.

Each form can work as a binder. This means that in the arity of the form we must specify not only the number of arguments, but also, for each argument, the number of variables it is supposed to bind. Thus, the *arity* of a form $\mathbf{f}$, is a finite (possibly empty) sequence of naturals (and not, as usual, a natural!).

Ground expressions (or, simply, expressions), ranged over by $t, t_1, \cdots$, are inductively generated by the two rules below:

a. every variable is an expression;

b. if $\mathbf{f}$ is a form of arity $k_1 \cdots k_n$ and $t_1, \cdots, t_n$ are expressions then $\mathbf{f}(\vec{x}^1_{k_1}.t_1, \cdots, \vec{x}^n_{k_n}.t_n)$ is an expression.

Free and bound occurrences of variables are defined in the obvious way. Terms that differ only by the name of bound variables will be identified. That is, we assume that CRS-expressions are quotiented by the axiom of α-conversion.

(The rewriting rules) Rewriting rules are described by using schemas or *metaexpressions*. A metaexpression is an expression built up with *metavariables*. Metavariables will be ranged over by X, Y, $\cdots$, possibly indexed.

A *rewriting rule* of a CRS is a pair of metaexpressions without free variables, written $\mathsf{H} \to \mathsf{K}$, where H is built according to the following syntax

$$\mathsf{H} \ ::= \ X \ \mid \ \mathbf{f}(\vec{x}^{\,1}_{a_1}.\,\mathsf{H}, \cdots, \vec{x}^{\,j}_{a_j}.\,\mathsf{H})$$

and K is obtained by the syntax below:

$$\mathsf{K} \ ::= \ x \ \mid \ \mathbf{f}(\vec{x}^{\,1}_{a_1}.\,\mathsf{K}, \cdots, \vec{x}^{\,j}_{a_j}.\,\mathsf{K}) \ \mid \ X[^{\mathsf{K}}/_{x_1}, \cdots, ^{\mathsf{K}}/_{x_n}]$$

where x stands for a generic variable and $\mathbf{f}$ is a form of arity $a_1 \cdots a_j$. Moreover H and K are constrained by the following items:

1. H is not a metavariable and metavariables appearing in H are pairwise different (*left linearity*);
2. every variable x in K is bound;
3. the metavariables in K are a subset of those occurring in H and the proviso for the substitution $X[^{\mathsf{K}_1}/_{x_1}, \cdots, ^{\mathsf{K}_n}/_{x_n}]$ is that $\langle x_1, \cdots, x_n \rangle.\,X$ occurs in the lhs.

Notice that lhs's are substitution free. A CRS is *orthogonal* (notation oCRS) if there is no critical pair between rewriting rules.

The *meta-operation* of substitution $t[^{t_1}/_{x_1}, \cdots, ^{t_n}/_{x_n}]$ is defined as usual by induction on the structure of t and taking care of variable clashes (see the axioms $\vartheta_A, \vartheta_B, \vartheta_C$ in the next section).

Example 3 *It should be quite evident that the λ-calculus is an oCRS. In this case we have two forms: @ and λ having arity 00 and 1, respectively, and the schema of β-reduction is:*

$$@(\lambda(x.\,X), Y) \ \to \ X[^{Y}/_{x}].$$

Other oCRS's can be defined by enriching the λ-calculus. For instance, it is possible to enrich the λ-calculus with an if-then-else *operator* $\natural$*. Let* t *and* f *be two (new) forms of arity* ε *and let* $\natural$ *be an operator of arity* 000*. The rules modeling the conditional behaviour are due to the interactions between* $\natural$ *and* t *or* f *as shown below:*

$$\natural(\mathsf{t}, X, Y) \to X$$

$$\natural(\mathsf{f}, X, Y) \to Y$$

Another form is the recursion operator μ*, of arity* 0*. Similarly for @, the dual operator of* μ *is* λ*: the interaction between* μ *and* λ *is stated by the following rule:*

$$\mu(\lambda(x.\,X)) \to X[^{\mu(\lambda(y.\,X[^{y}/_{x}]))}/_{x}]$$

Let us define what an *instance of a rewriting rule* is. Let t be an expression of an oCRS; t has a *redex* of the rule $\mathsf{H} \to \mathsf{K}$ if there exists a subexpression t' of t such that $t' = \mathsf{H}\varphi$, where φ is an operation that replaces the metavariables in H with ground expressions (namely expressions without metavariables). The term t^+ obtained from t by reducing the redex at t' is defined replacing the subterm t' with $t'' = \mathsf{K}\varphi$ (and performing the substitutions according to the rules $\vartheta_A, \vartheta_B, \vartheta_C$ of Section 6).

REMARK: (*Aczel-Klop notation*) The above notation for rewriting rules is slightly different from that used by Aczel [Aczel 1978] and Klop [Klop 1980] (see also [Klop and van Oostrom and van Raamsdonk 1993]). In these papers, metavariables are forms with arities that are sequences of 0 (i.e. not performing any binding) and, for example, H and K are defined by the following rules:

$$\mathsf{H} \;::=\; X(x_1, \cdots, x_n) \;\mid\; \mathbf{f}(\vec{x}^{\,1}_{a_1}.\,\mathsf{H}, \cdots, \vec{x}^{\,j}_{a_j}.\,\mathsf{H})$$

$$\mathsf{K} \;::=\; x \;\mid\; \mathbf{f}(\vec{x}^{\,1}_{a_1}.\,\mathsf{K}, \cdots, \vec{x}^{\,j}_{a_j}.\,\mathsf{K}) \;\mid\; X(\mathsf{K}, \cdots, \mathsf{K})$$

The metaexpressions H and K are constrained as in Section 5. Just the last proviso, that constraining the substitution $X[{}^{\mathsf{K}_1}/_{x_1}, \cdots, {}^{\mathsf{K}_n}/_{x_n}]$ to the occurrence of $\langle x_1, \cdots, x_n\rangle.\,X$ in the lhs, is omitted because implicit in the notation $X(\mathsf{K}_1, \cdots, \mathsf{K}_n)$.

Our notation has been chosen both because it makes first-order representations easier (in view of the flattening of an oCRS given in the next section) and because it is closer to the standard notation in the λ-calculus.

5.1 Residuals and permutation equivalence

The residual calculus is particularly heavy in the case of oCRS's, due to the mechanisms of binding and substitution. In view of the definition of residual, let $o_x(t)$ be the set of occurrences of the free variable x inside an expression t defined by structural induction over t as follows

$$o_x(y) = \begin{cases} \{\varepsilon\} & \textit{if } x = y \\ \emptyset & \textit{otherwise} \end{cases}$$

$$o_x(\mathbf{f}(\vec{x}^{\,1}.\,t_1, \cdots, \vec{x}^{\,n}.\,t_n)) = \bigcup_{\substack{1\le i\le n\\ x\notin \vec{x}^{\,i}}} i \cdot o_x(t_i)$$

Definition 8 *Let $t \xrightarrow{u} t'$ be a reduction of an oCRS (Σ, R) and let v be a redex in t. The set $v/\mathbf{u}$ of* residuals *after the reduction $\mathbf{u}$ (whose contracting schema is r) is a set of redex occurrences inside t' defined by cases as follows:*

$$v/\mathbf{u} = \begin{cases} \emptyset & \textit{if } u = v \\ \{v\} & \textit{if } u|v \text{ or } v \prec u \\ \mathcal{O}^t_{u,v}(\mathsf{K}) & \textit{if } v = u\cdot w \text{ and } \mathsf{K} \text{ is the rhs of } r \end{cases}$$

where the set $\mathcal{O}^t_{u,v}(\mathsf{K})$ is defined by induction over the structure of K by the following rules (notice that v has to occur inside the instance of a metavariable of r):

1. $\mathcal{O}^t_{u,v}(\mathsf{K}) = \emptyset$ *when* $\mathsf{K} = x$, *for every variable* x;

2. $\mathcal{O}^t_{u,v}(\mathsf{K}) = \bigcup_i i \cdot \mathcal{O}^t_{u,v}(\mathsf{K}_i)$ *when* $\mathsf{K} = \mathbf{f}(\vec{x}^{\,1}.\,\mathsf{K}_1, \cdots, \vec{x}^{\,n}.\,\mathsf{K}_n)$;

3. $\mathcal{O}^t_{u,v}(\mathsf{K}) = S \cup \left(\bigcup_i o_{x_i}(t_j) \cdot \mathcal{O}^t_{u,v}(H_i)\right)$, *when* $\mathsf{K} = X_j[{}^{\mathsf{K}_1}/_{x_1}, \cdots, {}^{\mathsf{K}_n}/_{x_n}]$ *and where* $S = \emptyset$ *if* v *does not occur inside* t_j *(the subterm of* t *which replaces* X_j *in the instance of* r*) or* $S = \{v''\}$ *if* $v = u \cdot v' \cdot v''$ *and* v' *is the access path of the variable* X_j *in the lhs of* r.

In order to gain confidence with the the above definition, we suggest the reader to instantiate it to some oCRS. For instance, take the case of the λ-calculus.

The notion of development is similar to that in Section 2.1 (notice that now every set of redexes is consistent). In particular, Theorem 1 holds for oCRS's too (remove the constraint of consistency: see [Klop 1980] for more details). Therefore a *parallel derivation* can be defined in the same standard way. Let us rephrase the definition of permutation equivalence.

Definition 9 Permutation equivalence *(notation* $\equiv$*) is the least equivalence relation satisfying:*

1. $\mathbf{U};(\mathbf{V}/\mathbf{U}) \;\equiv\; \mathbf{V};(\mathbf{U}/\mathbf{V})$;

2. $\underline{\varepsilon} \equiv \underline{\emptyset}$;

3. *if* $\sigma \equiv \rho$ *then* $\tau;\sigma;\tau' \equiv \tau;\rho;\tau'$.

6 The flattening of an oCRS to a trs

In this section we begin our investigation of axiomatizing permutation equivalence in orthogonal CRS's. Even if oCRS's are not term rewriting systems, they can be converted into (term) rewriting systems whose terms are quotiented by a (countable) equational axiomatization and where substitution is given the status of an algebraic operation. This is what we are going to show in this section. Once this "flattening" has been provided, Meseguer's machinery can be applied (since it is defined for the whole class of rewriting systems), yielding in this way a "concurrent" semantics. The resulting semantics exhibits the same problem already found in the $\lambda\sigma$-calculus, namely it does not match any more with permutation equivalence. This problem will be the subject of the next section.

Take an oCRS (Σ, R). The signature of the *flattened* oCRS $(\Sigma^\flat, R^\flat)$ consists of the sort $\mathcal{E}$ of expressions and a countable set of sorts $\mathcal{V}^n$, for each n, corresponding to an n-tuple of variables (we are assuming the existence of a countable set of variables). The operations of $\Sigma^\flat$ are the following:

$\langle x_1, \cdots, x_n\rangle : \;\to \mathcal{V}^n$	variables are pairwise different
$- \;:\; \mathcal{V} \to \mathcal{E}$	variables are expressions
$\mathbf{f} \;:\; \coprod_{1 \le i \le n}(\mathcal{V}^{j_i} \times \mathcal{E}) \to \mathcal{E}$	if the arity of $\mathbf{f}$ is $j_1 \cdots j_n$
$-[^-/_-]_n \;:\; \mathcal{E} \times \mathcal{E}^n \times \mathcal{V}^n \to \mathcal{E}$	*substitution*

where $\mathcal{V}^0 \times \mathcal{E} = \mathcal{E}$. Observe that, for each n, there is a distinguished operation of substitution. In the following we will omit the index n. We use the sorts $\mathcal{V}^n$ in order to guarantee that variables in $\langle x_1, \cdots, x_n \rangle$ are pairwise different. The general case should require further axioms in order to implement substitution correctly. Notice that, in the flattened oCRS, the operation of substitution may appear *explicitly* in the ground terms.

Below we define the axioms of α-conversion and those for substitution. The abbreviation $[{}^{\vec{t}}/_{\vec{x}}]$ stays for the vector of substitutions $[{}^{t_1}/_{x_1}, \cdots, {}^{t_n}/_{x_n}]$ (as usual, the variables x_i are taken pairwise distinct)

(α) $\mathbf{f}(\cdots, \vec{x}_n.\, t, \cdots) \;=\; \mathbf{f}(\cdots, \vec{y}_n.\, t[{}^{y_1}/_{x_1}, \cdots, {}^{y_n}/_{x_n}], \cdots)$, provided that $\vec{y}_n \cap \mathsf{var}(t) = \emptyset$;

(ϑ_A) $x[{}^{\vec{t}}/_{\vec{x}}] = t_i$, if $x = x_i$;

(ϑ_B) $y[{}^{\vec{t}}/_{\vec{x}}] = y$, if $y \notin \vec{x}$;

(ϑ_C) $\mathbf{f}(\vec{x}^{\,1}.\, t'_1, \cdots, \vec{x}^{\,k}.\, t'_k)[{}^{\vec{t}}/_{\vec{x}}] \;=\; \mathbf{f}(\vec{y}^{\,1}.\, t''_1, \cdots, \vec{y}^{\,n}.\, t''_n)$, where $\vec{x}^{\,i}$ and $\vec{y}^{\,i}$ have the same length and

- $\vec{y}^{\,i} = \vec{x}^{\,i}$ and $t''_i = t'_i$ whenever $\vec{x} \subseteq \vec{x}^{\,i}$;
- $\vec{y}^{\,i} = \vec{x}^{\,i}$ and $t''_i = t'_i[{}^{\vec{t}}/_{\vec{x}}]$, whenever $\vec{x} \cap \vec{x}^{\,i} = \emptyset$ and ($\vec{x} \cap \mathsf{var}(t'_i) = \emptyset$ or $\mathsf{var}(\vec{t}) \cap \vec{x}^{\,i} = \emptyset$);
- $t''_i = t'_i[{}^{\vec{y}^{\,i}}/_{\vec{x}^{\,i}}][{}^{\vec{t}}/_{\vec{x}}]$, whenever one of the following holds
  - *i.* $\vec{x} \cap \vec{x}^{\,i} = \emptyset$ and $\vec{x} \cap \mathsf{var}(t'_i) \neq \emptyset$ and $\mathsf{var}(\vec{t}) \cap \vec{x}^{\,i} \neq \emptyset$ and $\vec{y}^{\,i} \cap (\mathsf{var}(t'_i) \cup \mathsf{var}(\vec{t})) = \emptyset$,
  - *ii.* $\vec{x} \cap \vec{x}^{\,i} \neq \emptyset$ and $\vec{x} \not\subseteq \vec{x}^{\,i}$ and $\vec{y}^{\,i} \cap (\mathsf{var}(t'_i) \cup \mathsf{var}(\vec{t})) = \emptyset$.

where $\mathsf{var}(\vec{t}) = \bigcup_i \mathsf{var}(t_i)$.

We will call $=_{CRS}$ the above countable set of axioms.

Remark: Observe that each axiom in $=_{CRS}$ is a pair of ground expressions. In general, the axioms of an algebraic theory are pairs of terms with variables (not to be confused with the nullary operations of the sort $\mathcal{V}$!).

Expressions that have been built up without the operation of substitution will be called *substitution-free*. A useful property of the axioms ϑ_A, ϑ_B and ϑ_C is that they turn every ground expression into an equivalent substitution-free one.

Proposition 4 *For every ground expression t in $\mathcal{E}$, there exists another substitution-free ground expression $\tilde{t}$ such that $t \;=\; \tilde{t}$.*

Now that substitution has an "algebraic status", rewriting rules in $R^\flat$ are just pairs of open expressions in $\Sigma^\flat$. In particular, we call $\mathsf{T}[\;, \cdots, \;]$ a *primitive context* with n holes if it is built up with forms in Σ and the nullary operation $\Box_i$ $(1 \leq i \leq n)$ standing for a generic $\vec{x}.\, X$. It's clear that every lhs H of a rewriting rule in oCRS's can be written as $\mathsf{T}[\vec{x}^{\,1}.\, X_1, \cdots, \vec{x}^{\,n}.\, X_n]$, for some primitive context $\mathsf{T}[\ ,\cdots,\ ]$ (we are just singling out all the pairs $\vec{x}.X$ occurring in H). Then, if $\mathsf{T}[\vec{x}^1.X_1,\cdots,\vec{x}^n.X_n] \to \mathsf{K}$ is a rule r in R,

$$r_{\mathsf{T}}(\vec{x}^1.X_1,\cdots,\vec{x}^n.X_n) : \mathsf{T}[\vec{x}^1.X_1,\cdots,\vec{x}^n.X_n] \to \mathsf{K}$$

belongs to $R^\flat$ (we will omit the index T in r_{T} as much as possible). Notice that, for each choice of $\vec{x}^i$, we have a different rule $r_{\mathsf{T}}(\vec{x}^1.X_1,\cdots,\vec{x}^n.X_n)$.

There is a subtle problem: the definition of the set of redexes in a (ground) expression. We have to guarantee that two equal expressions have the same set of redexes. In CRS's, where substitution is a metaoperation, there is no danger because expressions are always substitution-free and the unique axiom is α-conversion (therefore we have to prove that α-conversion does not damage the set of redexes: we remedy this in Proposition 5 below). The idea is to exploit Proposition 4.

Definition 10 *The* set of redexes *of a ground expression in a flattened oCRS is that of the equivalent expression that is substitution-free.*

In this way, redexes are addressed as in Section 5.1. Notice that, if $t[^{t'}/_x]$ is a ground expression and u is a redex of t', it is possible that u is not a redex of $t[^{t'}/_x]$ because x may not occur freely in t (for the same reason u could be copied).

Let us guarantee the soundness of Definition 10 w.r.t. axiom α, namely that α-conversion does not modify the set of redex occurrences in an expression.

Proposition 5 *Let t and t' be two ground expressions. If $\{\alpha\} \vdash t = t'$ then the set of redexes of t and t' are equal.*

Proof: Standard induction over the depth of the proof of $t = t'$ in the Birkhoff deductive system.

6.1 The rewrite theory of an oCRS

The rewrite theory $\mathcal{R}$ of an oCRS (Σ, R) is $\langle \Sigma^\flat, =_{CRS}, L, R^\flat \rangle$, where L is a set of labels that identify uniquely rewriting rules.

We remark that Meseguer's machinery gives us a countable set of categories, one for each sort in $\Sigma^\flat$. However, the categories corresponding to sorts $\mathcal{V}^n$ are *discrete* (arrows are identities) and do not play any role in the development which follows. So we will call $\mathcal{M}(\mathsf{X})$ the category corresponding to expressions $\mathcal{E}$, without caring at all about the variables $\mathcal{V}^n$. Moreover, for notational convenience, reductions of $\mathcal{M}(\mathsf{X})$ will be written as

$$r(\vec{x}^1.\pi_1,\cdots,\vec{x}^n.\pi_n), \qquad \text{or} \qquad \mathbf{f}(\vec{x}^1.\pi_1,\cdots,\vec{x}^n.\pi_n), \qquad \text{or} \qquad \pi[^\xi/_x]$$

instead of $r(\zeta_1.\pi_1,\cdots,\zeta_n.\pi_n)$, or $\mathbf{f}(\zeta_1.\pi_1,\cdots,\zeta_n.\pi_n)$, or $\pi[^\xi/_{0_x}]$, since, as said before, the ζ_i are always identities $0_{\vec{x}^i}$. The axioms which quotient arrows of $\mathcal{M}(\mathsf{X})$ and come from the axiomatization $\alpha, \vartheta_A, \vartheta_B, \vartheta_C$ (those of group 3, according to Meseguer's arrangement of Section 2.2) are:

3. **Axioms in** $=_{CRS}$:

(α^σ) $\mathbf{f}(\cdots,\,\vec{x}_n.\,\pi,\,\cdots) \;=\; \mathbf{f}(\cdots,\,\vec{y}_n.\,\pi[{}^{0_{y_1}}/_{x_1},\,\cdots,\,{}^{0_{y_n}}/_{x_n}],\,\cdots)$, provided that $\vec{y}_n \cap \mathsf{var}(t) = \emptyset$, where t is the initial expression of π;

(ϑ^σ_A) $0_x[{}^{\vec{\pi}}/_{\vec{x}}] = \pi_i$, if $x = x_i$;

(ϑ^σ_B) $0_y[{}^{\vec{\pi}}/_{\vec{x}}] = 0_y$, if $y \notin \vec{x}$;

(ϑ^σ_C) $\mathbf{f}(\vec{x}^{\,1}.\,\rho_1,\,\cdots,\,\vec{x}^{\,n}.\,\rho_n)\,[{}^{\vec{\pi}}/_{\vec{x}}] \;=\; \mathbf{f}(\vec{y}^{\,1}.\,\rho'_1,\,\cdots,\,\vec{y}^{\,n}.\,\rho'_n)$, where $\vec{x}^{\,i}$ and $\vec{y}^{\,i}$ have the same length and

(1) $\vec{y}^{\,i} = \vec{x}^{\,i}$ and $\rho'_i = \rho_i$, whenever $\vec{x} \subseteq \vec{x}^{\,i}$;

(2) $\vec{y}^{\,i} = \vec{x}^{\,i}$ and $\rho'_i = \rho_i[{}^{\vec{\pi}}/_{\vec{x}}]$, whenever $\vec{x} \cap \vec{x}^{\,i} = \emptyset$ and ($\vec{x} \cap \mathsf{var}(t_i) = \emptyset$ or $\mathsf{var}(\vec{\pi}) \cap \vec{x}^{\,i} = \emptyset$);

(3) $\rho'_i = \rho_i[{}^{\vec{\zeta}}/_{\vec{x}^{\,i}}][{}^{\vec{\pi}}/_{\vec{x}}]$ (where $\vec{\zeta} = \vec{0}_{\vec{y}^{\,i}}$), whenever one of the following holds:

i. $\vec{x} \cap \vec{x}^{\,i} = \emptyset$ and $\vec{x} \cap \mathsf{var}(t_i) \neq \emptyset$ and $\mathsf{var}(\vec{\pi}) \cap \vec{x}^{\,i} \neq \emptyset$ and $\vec{y}^{\,i} \cap (\mathsf{var}(t_i) \cup \mathsf{var}(\vec{\pi})) = \emptyset$.

ii. $\vec{x} \cap \vec{x}^{\,i} \neq \emptyset$ and $\vec{x} \not\subseteq \vec{x}^{\,i}$ and $\vec{y}^{\,i} \cap (\mathsf{var}(t_i) \cup \mathsf{var}(\vec{\pi})) = \emptyset$.

where t_i is the initial expression of ρ_i and $\mathbf{var}(\vec{\pi})$ is the set of free variables in the initial expressions of the derivations in $\vec{\pi}$.

Example 4 (λ-calculus) *The rewrite theory of the λ-calculus has a single rewriting rule*

$$\beta(x.\,X,\,Y) \;:\; @(\lambda(x.\,X),\,Y) \longrightarrow X[{}^{Y}/_{x}]\,.$$

Now, take Meseguer's category of λ-expressions. Let $t = @(\lambda(x.\,@(x,\,x)),\,@(\mathbf{I},\,x))$. The following two derivations starting at t and ending at $@(x,\,x)$ are equal:

$$\beta(x.\,0_{@(x,x)},\,\beta(x.\,0_x,\,0_x)) \qquad \beta(x.\,0_{@(x,x)},\,0_{@(\mathbf{I},x)})\,;\,@(\beta(x.\,0_x,\,0_x),\,\beta(x.\,0_x,\,0_x))$$

6.2 Problems of completeness and the CRS-axioms

Meseguer's axiomatization does not match with permutation equivalence. There are essentially two reasons:

1. two reductions which act over two α-equivalent expressions are not equated,
2. substitutions should be "pushed into" reductions $r(\vec{x}^{\,1}.\,\pi_1,\cdots,\,\vec{x}^{\,n}.\,\pi_n)$.

The following example will clarify the point.

Example 5 *Take the rewriting theory of the λ-calculus as described in Example 4 and consider the following two reductions:*

$$\beta(x.\,0_x,0_z) \qquad\qquad \beta(y.\,0_y,0_z)$$

These two contractions describe the same reduction in the (equivalence class of the) λ-expression $@(\mathbf{I}, z)$, because they are the same "up to the axiom α". Therefore, syntactically, there is no reason for the two proofs not being equated. However, the expected equivalence cannot be derived by the axiomatization above. Indeed, the axiom responsible for such work should be α^σ recalled before. But it is not powerful enough to work over functions which are not in the signature Σ (and this is the case for β, since it is a new operator over derivations).

Similarly, consider the following reduction over a ground expression:

$$\beta(x.\,\pi,\,\xi)[^{\zeta}/_{y}]$$

One expects that it must be possible to execute the substitution, namely, to move the substitution operator deeper and deeper inside the proof tree until the actual occurrences of y are eventually replaced. This is what happens in the expressions of the λ-calculus thanks to the axioms $=_{CRS}$. However, since the rewrite rule is introduced as a free *proof operator, there is no way, by using axioms 1-4, to simplify the above reduction. Again, this would be possible if β were a function symbol in Σ (ϑ^σ_C would do the work). For this reason, $\beta(x.\,0_x, 0_y)$ and $\beta(x.\,0_x, 0_z)[^{0_y}/_{z}]$ are kept apart by Meseguer's axioms.*

It should be clear now what are the axioms to be added: we must lift axioms α^σ and ϑ^σ_C to rewriting rules. We will call these new axioms *lifted CRS-axioms*.

5. **Lifted CRS-axioms**. For every rewriting rule r in $R^\flat$:

(α^r) $r(\cdots,\,\vec{x}_n.\,\pi,\,\cdots) \;=\; r(\cdots,\,\vec{y}_n.\,\pi[^{0_{y_1}}/_{x_1},\,\cdots,\,^{0_{y_n}}/_{x_n}],\,\cdots)$, provided that $\vec{y}_n \cap \mathsf{var}(t) = \emptyset$, where t is the initial expression of π;

(ϑ^r_C) $r(\vec{x}^{\,1}.\,\rho_1,\,\cdots,\,\vec{x}^{\,n}.\,\rho_n)\,[^{\vec{\pi}}/_{\vec{x}}] \;=\; r(\vec{y}^{\,1}.\,\rho'_1,\,\cdots,\,\vec{y}^{\,n}.\,\rho'_n)$, where $\vec{x}^{\,i}$ and $\vec{y}^{\,i}$ have the same lengths and

- **(1)** $\vec{y}^{\,i} = \vec{x}^{\,i}$ and $\rho'_i = \rho_i$, whenever $\vec{x} \subseteq \vec{x}^{\,i}$;
- **(2)** $\vec{y}^{\,i} = \vec{x}^{\,i}$ and $\rho'_i = \rho_i[^{\vec{\pi}}/_{\vec{x}}]$, whenever $\vec{x} \cap \vec{x}^{\,i} = \emptyset$ and ($\vec{x} \cap \mathsf{var}(t_i) = \emptyset$ or $\mathsf{var}(\vec{\pi}) \cap \vec{x}^{\,i} = \emptyset$);
- **(3)** $\rho'_i = \rho_i[^{\vec{\zeta}}/_{\vec{x}^{\,i}}][^{\vec{\pi}}/_{\vec{x}}]$ (where $\vec{\zeta} = \vec{0}_{\vec{y}^{\,i}}$), whenever one of the followings holds:
  - *i.* $\vec{x} \cap \vec{x}^{\,i} = \emptyset$ and $\vec{x} \cap \mathsf{var}(t_i) \neq \emptyset$ and $\mathsf{var}(\vec{\pi}) \cap \vec{x}^{\,i} \neq \emptyset$ and $\vec{y}^{\,i} \cap (\mathsf{var}(t_i) \cup \mathsf{var}(\vec{\pi})) = \emptyset$.
  - *ii.* $\vec{x} \cap \vec{x}^{\,i} \neq \emptyset$ and $\vec{x} \not\subseteq \vec{x}^{\,i}$ and $\vec{y}^{\,i} \cap (\mathsf{var}(t_i) \cup \mathsf{var}(\vec{\pi})) = \emptyset$.

where t_i is the initial expression of ρ_i and $\mathbf{var}(\vec{\pi})$ is the set of free variables in the initial expressions of the derivations in $\vec{\pi}$.

Notice that, as for axioms $\alpha^\sigma, \vartheta^\sigma_A, \vartheta^\sigma_B, \vartheta^\sigma_C$, the above axioms equate ground derivations only. The category resulting by quotienting $\mathcal{M}(\mathsf{X})$ by α^r and ϑ^r_C, for every r, will be called $\mathcal{M}^\flat(\mathsf{X})$; the equality over arrows obtained by combining Meseguer's axioms 1, 2, 3 and 4 and lifted CRS-axioms will be denoted by $=^\flat$. In the next section we will prove that the ground subcategory of $\mathcal{M}^\flat(\mathsf{X})$ is isomorphic to that obtained by taking derivations of oCRS's up to permutation equivalence.

The axiomatization $=^\flat$ lets us lift Proposition 4 to derivations in $\mathcal{M}^\flat$ (i.e. the subcategory of ground expressions and ground derivations in $\mathcal{M}(\mathsf{X})$). Let us call substitution-free those derivations that have been built without using the operation of substitution.

Proposition 6 *For every derivation ρ in $\mathcal{M}^\flat$, there exists a substitution-free derivation σ such that $\rho =^\flat \sigma$.*

Proof: We sketch the proof because it is quite standard. Firstly, take $\rho = \rho'[^{\vec{\pi}}/_{\vec{x}}]$ where ρ' and every derivation in $\vec{\pi}\,'$ is substitution-free. Let us show that there exists a σ satisfying the thesis for such a ρ. The proof is by induction over the structure of ρ'. When ρ' is an identity of a variable apply axioms ϑ^σ_A or ϑ^σ_B. When ρ' has an outermost form $\mathbf{f}$, apply axiom ϑ^σ_C in order to drop $[^{\vec{\pi}}/_{\vec{x}}]$ inside $\mathbf{f}$. Similarly, when ρ' has an outermost rewriting rule use the axiom ϑ^r_C. When $\rho' = \rho_1;\rho_2$ apply functoriality of the substitution.

Let us show the general case. We prove, by induction over the structure of ρ, the existence of a σ that is substitution-free and show that $\rho =^\flat \sigma$. The interesting case is when $\rho = \rho'[^{\vec{\pi}}/_{\vec{x}}]$. By the inductive hypothesis there is a substitution-free derivation σ' such that $\rho' =^\flat \sigma'$. Similarly for derivations in the vector $\vec{\pi}$ (let $\vec{\xi}$ the vector of the equivalent substitution free derivations). Then, since $=^\flat$ is a congruence, $\rho'[^{\vec{\pi}}/_{\vec{x}}] =^\flat \sigma'[^{\vec{\xi}}/_{\vec{x}}]$. Now apply the previous result in order to prove the proposition.

The above fact, together with Lemma 1, allows all derivations to be written as sequential compositions of elementary steps that are substitution-free.

7 The correspondence between the two semantics

The proof of the coincidence of $\equiv$ and $=^\flat$ follows the same pattern as that of the analogous proof in Section 3: we must define two mappings which make the two representations isomorphic.

Let (Σ, R) be an oCRS. Let $\mathcal{L}^g$ be the category whose objects are ground expressions of Σ and whose arrows are derivations up to permutation equivalence. The subcategory of $\mathcal{M}^\flat(\mathsf{X})$ of (canonical representatives of) ground expressions and ground reductions will be called $\mathcal{M}^\flat$. The definition of the two mappings $\mathcal{F}^\flat : \mathcal{L}^g \to \mathcal{M}^\flat$ and $\mathcal{G}^\flat : \mathcal{M}^\flat \to \mathcal{L}^g$ is similar to that provided in Section 3: some care is needed for bindings and substitutions. Notice that the constraint of consistency can be removed in oCRS's, since redexes never overlap. Indeed, now the definition of κ_t is:

$$\kappa_t(\mathbf{U}) = \begin{cases} 0_t & \text{if } U = \emptyset \\ \mathbf{f}(\vec{x}^{\,1}.\, \kappa_{t_1}(\mathbf{U}_1), \cdots, \vec{x}^{\,n}.\, \kappa_{t_n}(\mathbf{U}_n)) & \text{if } \varepsilon \notin U \text{ and } t = \mathbf{f}(\vec{x}^{\,1}.\, t_1, \cdots, \vec{x}^{\,n}.\, t_n) \\ r(\vec{x}^{\,1}.\, \kappa_{t'_1}(\mathbf{V}_1), \cdots, \vec{x}^{\,n}.\, \kappa_{t'_n}(\mathbf{V}_n)) & \text{if } \varepsilon^r \in U \end{cases}$$

with the provisos that $U_i = \{u \mid i \cdot u \in U\}$ and $V_i = \{v \mid w_i \cdot v \in U\}$, where w_i is the access path of the i-th metavariable in the lhs of r. The expression t'_i is that at access path w_i in t.

The definition of the mapping $\mathcal{G}$ in Section 3 was provided by structural induction. We have to generalize it to the operation of substitution. However, the step that deserves much care is that when the outermost operator is a rewriting rule. Actually, in Section 3, we relied on the fact that occurrences of variables in the rhs's of rewriting rules were disjoint. This is definitely false in oCRS's, due to the role played by substitution. Let us see an example.

Example 6 *Take the λ-calculus and the expression $t = @(\lambda(x.\, @(\lambda(y.\, z),\, x)),\, \Omega)$, where $\Omega = @(\lambda(x.\, @(x,\, x)),\, \lambda(x.\, @(x,\, x)))$. Now take the following derivation starting at t:*

$$\pi \;=\; \beta(x.\, \beta(y.\, 0_z,\, 0_x),\, \rho)$$

where $\rho = \beta(x.\, 0_{@(x,x)},\, 0_{@(x,x)}); \beta(x.\, 0_{@(x,x)},\, 0_{@(x,x)})$. The computation of $\mathcal{G}(\pi)$, according to Definition 7, gives the derivation:

$$\{\varepsilon,\, 1\cdot 1,\, 2\}\;;\;\{1\cdot 1\cdot 2\}$$

that is clearly wrong because, after the firing of $\{\varepsilon,\, 1\cdot 1,\, 2\}$, there is no occurrence of x at all.

It should be evident that the firing operator cannot work separately over every proof replacing metavariables and that substitutions in the rhs of rewriting rules must be computed at "run time" as the derivation progresses. The new definition of firing takes as arguments the instances of the metavariables in the rewriting rule. So

$$[r](\vec{x}^{\,1}.\, \mathbf{U}_1; \rho_1, \cdots, \vec{x}^{\,n}.\, \mathbf{U}_n; \rho_n) \;=\; \bigcup_i w_i \cdot \mathbf{U}_i \;;\; \mathsf{K}(\vec{x}^{\,1}.\, \rho_1, \cdots, \vec{x}^{\,n}.\, \rho_n)$$

where w_i is the occurrence in the lhs of r of the i-th metavariable and K is the rhs of r. The notation $\mathsf{K}(\vec{x}^{\,1}.\, \rho_1, \cdots, \vec{x}^{\,n}.\, \rho_n)$ represents the instance of the rhs of r where metavariables and variables in K are replaced by the corresponding values.

The operation of substitution over derivations in $\mathcal{L}$ is defined in terms of the following operator $\mho$:

$$\begin{array}{rcl}
\mho(\underline{\emptyset}_t[\vec{\rho}/\vec{x}]) & = & \bigcup_{x_i}(o_{x_i}(t)\cdot \rho_i) \\
\mho(\sigma[{}^{0_{y_1}}/_{x_1}, \cdots, {}^{0_{y_n}}/_{x_n}]) & = & \sigma \\
\mho((\mathbf{U};\sigma)[\vec{\rho}/\vec{x}]) & = & \mathbf{U} \cup (\bigcup_{x_i}(o_{x_i}(t)\cdot \mathbf{V}^i))\;;\;\mho(\sigma[\vec{\rho}\,'/\vec{x}])
\end{array}$$

where $\vec{\rho} = \langle \rho_1, \cdots, \rho_n\rangle$, $\rho_i = \mathbf{V}^i; \rho'_i$, $\vec{\rho}\,' = \langle \rho'_1, \cdots, \rho'_n\rangle$, t is the initial expression of the derivation $\mathbf{U};\sigma$ and the function $o_{x_i}(t)$ is that defined in Section 5.1. Notice that we have used the proviso that, if $\rho_i = \underline{\emptyset}$, then $\rho'_i = \underline{\emptyset}$.

Definition 11 *The mapping $\mathcal{F}^\flat : \mathcal{L}^g \to \mathcal{M}^\flat$ is defined as follows (U is a set of redexes):*

$$\mathcal{F}^\flat(\mathbf{U}) \;=\; \kappa_t(\mathbf{U}) \qquad\qquad \mathcal{F}^\flat(\sigma;\rho) \;=\; \mathcal{F}^\flat(\sigma);\mathcal{F}^\flat(\rho)$$

The mapping $\mathcal{G}^\flat : \mathcal{M}^\flat \to \mathcal{L}^g$ is defined by induction over the syntactic structure of derivations in $\mathcal{M}^\flat$ by the following rules:

$$
\begin{array}{rcl}
\mathcal{G}^\flat(0_t) & = & \emptyset \\
\mathcal{G}^\flat(f(\vec{x}^1.\,\pi_1,\,\cdots,\,\vec{x}^n.\,\pi_n)) & = & \bigcup_{1\le i\le n} i\cdot\mathcal{G}^\flat(\pi_i) \\
\mathcal{G}^\flat(r(\vec{x}^1.\,\mathcal{G}^\flat(\pi_1),\,\cdots,\,\vec{x}^n.\,\mathcal{G}^\flat(\pi_n))) & = & \{\varepsilon^r\}\cup[r](\vec{x}^1.\,\pi_1,\,\cdots,\,\vec{x}^n.\,\pi_n) \\
\mathcal{G}^\flat(\pi[^{\vec{\rho}}/_{\vec{x}}]) & = & \mho(\mathcal{G}^\flat(\pi)[^{\mathcal{G}^\flat(\vec{\rho})}/_{\vec{x}}]) \\
\mathcal{G}^\flat(\sigma;\rho) & = & \mathcal{G}^\flat(\sigma);\mathcal{G}^\flat(\rho)
\end{array}
$$

where W_i is the set of occurrences of the variable x_i in the initial expression of π and $\mathcal{G}^\flat(\vec{\rho}) = \langle\mathcal{G}^\flat(\rho_1),\cdots,\mathcal{G}^\flat(\rho_n)\rangle$.

In the case of term rewriting systems the proof that $\mathcal{F}^\flat$ is well-defined used Propositions 2 and 3. The first proposition can be generalized easily to the case of oCRS's. The generalization of Proposition 3 is less immediate because the rhs of rules have expressions involving the operation of substitution. The proof needs a preliminary proposition.

Proposition 7 *Let $U\cup\{\varepsilon\}$ be a set of redexes in t. Let $r(\vec{x}^1.\,X_1,\cdots,\vec{x}^n.\,X_n) : \mathsf{T}[\vec{x}^1.\,X_1,\cdots,\vec{x}^n.\,X_n] \to \mathsf{K}$ be the rule firing the redex at ε. Then*

$$\mathcal{F}^\flat(\mathbf{U}/\underline{\varepsilon}) =^\flat \mathsf{K}(\vec{x}^1.\,\kappa_{t_1}(\mathbf{U}_1),\cdots,\,\vec{x}^n.\,\kappa_{t_n}(\mathbf{U}_n))$$

where $U_i = \{u \mid w_i\cdot u\in U\}$, w_i is the access path of the metavariable X_i in the lhs of r and t_i is the expression replacing X_i along $\underline{\varepsilon}$.

Proof: Notice that on the lhs of the equation there is a substitution-free elementary step, whilst on the rhs we can have substitutions. Without loss of generality we can assume that $\varepsilon\notin U$. Then, $U = \bigcup_i w_i\cdot U_i$ and, by definition of residual (see Section 5.1): $U/\underline{\varepsilon} = \bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K})$. Therefore, $\mathcal{F}^\flat(U/\underline{\varepsilon}) = \kappa_t(\bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K}))$. The proof is by induction over the structure of K.

(case $\mathsf{K} = x$) Notice that $U/\underline{\varepsilon} = \emptyset$ (because x is a variable created by the rule). The equality is immediate.

(case $\mathsf{K} = \mathbf{f}(\vec{x}^1.\,\mathsf{K}_1,\cdots,\,\vec{x}^m.\,\mathsf{K}_m)$) By definition of residual, $\bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K}) = \bigcup_{1\le i\le m} i\cdot(\bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K}_i))$. Therefore,

$$
\begin{array}{rcl}
\mathcal{F}^\flat(\bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K})) & = & \mathcal{F}^\flat(\bigcup_{1\le i\le m} i\cdot(\bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K}_i))) \\
& \stackrel{(\star)}{=} & \mathbf{f}(\cdots,\,\vec{x}^i.\,\mathcal{F}^\flat(\bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K}_i)),\cdots) \\
& \stackrel{(\star\star)}{=^\flat} & \mathbf{f}(\cdots,\,\vec{x}^i.\,\mathsf{K}_i(\vec{x}^1.\,\kappa_{t_1}(\mathbf{U}_1),\cdots,\,\vec{x}^n.\,\kappa_{t_n}(\mathbf{U}_n)),\cdots)
\end{array}
$$

where $(\star)$ follows by definition and $(\star\star)$ is a consequence of the inductive hypothesis.

(**case** $\mathsf{K} = X_j[^{\mathsf{K}_1}/_{z_1},\cdots,^{\mathsf{K}_m}/_{z_m}]$) Notice that

$$\bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K}) = U_j\cup\left(\bigcup_{1\le i\le m}\left(o_{z_i}(t_j)\cdot\bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K}_i)\right)\right).$$

On the other hand, $\mathsf{K}(\vec{x}^{\,1}.\,\kappa_{t_1}(\mathbf{U}_1), \cdots, \vec{x}^{\,n}.\,\kappa_{t_n}(\mathbf{U}_n)) = \kappa_{t_j}(\mathbf{U}_j)[{}^{\mathsf{K}_1^\star}/_{z_1}, \cdots, {}^{\mathsf{K}_m^\star}/_{z_m}]$, where $\mathsf{K}_i^\star = \mathsf{K}_i(\vec{x}^{\,1}.\,\kappa_{t_1}(\mathbf{U}_1), \cdots, \vec{x}^{\,n}.\,\kappa_{t_n}(\mathbf{U}_n))$. By induction assume that $\mathcal{F}^\flat(\bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K}_i)) = \mathsf{K}_i^\star$.

Now we use a further induction over the structure of $\kappa_{t_j}(\mathbf{U}_j)$ (notice that it is substitution-free).

(case $\kappa_{t_j}(\mathbf{U}_j) = 0_x$) If $x \in \langle z_1, \cdots, z_m\rangle$, let us say that $x = z_r$, then $\kappa_{t_j}(\mathbf{U}_j)[{}^{\mathsf{K}_1^\star}/_{z_1}, \cdots, {}^{\mathsf{K}_m^\star}/_{z_m}] = \mathsf{K}_r^\star$ by axiom ϑ^σ_A. On the other hand, $U_j = \emptyset$ and $o_{z_i}(t_j) = \emptyset$, for every $i \neq r$. Therefore, $\bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K}_r)$. The equality with $\mathsf{K}_r^\star$ follows by induction. If $x \notin \langle z_1, \cdots, z_m\rangle$ then, by axiom ϑ^σ_B, $\mathcal{F}^\flat(\mathbf{U}/\underline{\varepsilon})$ is equal to 0_x, which is equal to the rhs of the Proposition.

(case $\kappa_{t_j}(\mathbf{U}_j) = \mathbf{f}(\vec{x}^{\,1}.\,\kappa_{t_j^1}(\mathbf{U}_j^1), \cdots, \vec{x}^{\,p}.\,\kappa_{t_j^p}(\mathbf{U}_j^p)))$ ($U_j^i = \{u \mid i\cdot u \in U_j\}$ and $t_j = \mathbf{f}(\vec{x}^{\,1}.\,t_j^1, \cdots, \vec{x}^{\,p}.\,t_j^p)$) By axiom ϑ^σ_C, we can push substitutions inside the form $\mathbf{f}$. Thus we obtain:

$$\mathbf{f}(\vec{x}^{\,1}.\,\kappa_{t_j^1}(\mathbf{U}_j^1), \cdots, \vec{x}^{\,p}.\,\kappa_{t_j^p}(\mathbf{U}_j^p))[{}^{\mathsf{K}_1^\star}/_{z_1}, \cdots, {}^{\mathsf{K}_m^\star}/_{z_m}] \;=^\flat\; \mathbf{f}(\vec{y}^{\,1}.\,\pi_1', \cdots, \vec{y}^{\,p}.\,\pi_p')$$

On the other hand, $U_j = \bigcup_{1\le k\le p} k\cdot U_j^i$. Then $o_{z_i}(t_j) = \bigcup_{1\le k\le p} k\cdot o_{z_i}(t_j^k)$. Therefore:

$$\bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K}) \;=\; \bigcup_{1\le k\le p} k\cdot\left(U_j^k \cup \left(\bigcup_{1\le i\le m}\left(o_{x_i}(t_j^k)\cdot\bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K}_i)\right)\right)\right)\;.$$

Let $W_j^k = U_j^k \cup \left(\bigcup_{1\le i\le m}\left(o_{z_i}(t_j^k)\cdot\bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K}_i)\right)\right)$. Hence, $\mathcal{F}^\flat(\bigcup_{u\in U}\mathcal{O}^t_{\varepsilon,u}(\mathsf{K})) = \mathbf{f}(\cdots, \vec{x}^{\,r}.\,\mathcal{F}^\flat(W_j^r), \cdots)$. That is, we have to show that $\pi_r' = \mathcal{F}^\flat(W_j^r)$. This is proved by checking each case of the axiom ϑ^σ_C. The most interesting case is the third one (the first is immediate, and the second follows by induction). Let us look at the subcase when $\vec{x}^{\,r} \cap \langle z_1, \cdots, z_m\rangle = \emptyset$, the other is similar. Due to the format of the rhs of the rule r, the initial expression of $\mathcal{F}^\flat(\mathbf{U}/\underline{\varepsilon})$ will be the substitution-free expression equivalent to $\mathbf{f}(\vec{x}^{\,1}.\,t_j^1, \cdots, \vec{x}^{\,p}.\,t_j^p)[{}^{t_1^\star}/_{z_1}, \cdots, {}^{t_m^\star}/_{z_m}]$, where $t_i^\star$ is the expression obtained by computing K_i. In order to push the substitution inside the form $\mathbf{f}$, according to the method above, we must rename the bound variables of the r-th argument (we are discusing the case of the r-th argument only). Hence, the initial expression of $\mathcal{F}^\flat(\mathbf{U}/\underline{\varepsilon})$ will be something like

$$\mathbf{f}(\cdots, \vec{y}.\,t_j^r[{}^{\vec{y}}/_{\vec{x}^{\,r}}][{}^{t_1^\star}/_{z_1}, \cdots, {}^{t_m^\star}/_{z_m}], \cdots)$$

where $\vec{y}$ is a vector of fresh variables of the same length as $\vec{x}^{\,r}$. Notice that, by axiom α^σ:

$$\kappa_{t_j}(\mathbf{U}_j) \;=\; \mathbf{f}(\cdots, \vec{y}.\,\kappa_{t_j^r}(\mathbf{U}_j^r)[{}^{\vec{\zeta}}/_{\vec{x}^{\,r}}], \cdots)$$

where $\vec{\zeta} = \langle 0_{y_1}, \cdots, 0_{y_q}\rangle$ and q is the length of $\vec{x}^{\,r}$.

Therefore, we must prove that

$$\mathcal{F}^\flat(W_j^r) \;=^\flat\; \kappa_{t_j^r}(\mathbf{U}_j^r)[{}^{\vec{\zeta}}/_{\vec{x}^{\,r}}][{}^{H_1^\star}/_{z_1}, \cdots, {}^{H_m^\star}/_{z_m}]$$

This follows by applying the inductive hypothesis, provided that we can first show that $\kappa_{t_j^r}(\mathbf{U}_j^r)[^{\vec{\zeta}}/_{\vec{x}^r}] = \kappa_{t^+}(\mathbf{U}_j^r)$, where $t^+ = t_j^r[^{\vec{y}}/_{\vec{x}^r}]$. This equality follows by an easy induction over the structure of t_j^r.
(case $\kappa_{t_j}(\mathbf{U}_j) = r(\vec{x}^1.\, \kappa_{t_j^1}(\mathbf{U}_j^1), \cdots, \vec{x}^p.\, \kappa_{t_j^p}(\mathbf{U}_j^p)))$ Similar to the previous case: use α^r and ϑ_C^r instead of α^σ and ϑ_C^σ.

Proposition 8 *Let U and V be two sets of redexes in t such that $\varepsilon \in V$ and $\varepsilon \notin U$. Let $r(\vec{x}^1.\, X_1, \cdots, \vec{x}^n.\, X_n) : \mathbf{d}(\mathbf{c}(\vec{x}^1.\, X_1, \cdots) \cdots, \vec{x}^n.\, X_n) \to \mathsf{K}$ be the rule firing the redex at ε. Then*

$$\mathcal{F}^\flat(\mathbf{U}/\mathbf{V}) =^\flat \mathsf{K}(\vec{x}^1.\, \kappa_{t_1}(\mathbf{U}_1/\mathbf{V}_1), \cdots,\ \vec{x}^n.\, \kappa_{t_n}(\mathbf{U}_n/\mathbf{V}_n))$$

where $U_i = \{u \mid w_i{\cdot}u \in U\}$ and $V_i = \{v \mid w_i{\cdot}v \in V\}$, w_i is the access path of the metavariable X_i in the lhs of r and t_i is the expression replacing X_i along $\underline{\varepsilon}$.

Proof: Observe that $U/\mathbf{V} = (U/\mathbf{V}')/\underline{\varepsilon}$, where $V' = V \setminus \{\varepsilon\}$. Then, by arguing similarly to Proposition 2, $U/\mathbf{V}' = \bigcup_i w_i \cdot (U_i/\mathbf{V}_i)$. Now apply Proposition 7 and the result follows.

Lemma 5 *If $\sigma \equiv \rho$ then $\mathcal{F}^\flat(\sigma) =^\flat \mathcal{F}^\flat(\rho)$.*

Proof: Similar to the proof of Lemma 2. Use Proposition 8 instead of Proposition 3.

Lemma 6 *If $\sigma =^\flat \rho$ then $\mathcal{G}^\flat(\sigma) \equiv \mathcal{G}^\flat(\rho)$.*

Proof: The proof strategy is similar to that of Lemma 3. We omit the cases discussed there and focus on the axioms in $=_{CRS}$ and the lifted CRS-axioms.

(Axioms in $=_{CRS}$) Axiom α^σ and ϑ_A^σ and ϑ_B^σ are immediate consequences of the definition of $\mho$. Axiom ϑ_C^σ is less evident. Let us discuss the case when $\mathbf{f}$ has a unique argument: the general case will be sketched afterwards. So we must show that:

$$\mathcal{G}^\flat(\mathbf{f}(\vec{x}.\, \rho)[^{\vec{\pi}}/_{\vec{y}}]) \ = \ \mathcal{G}^\flat(\mathbf{f}(\vec{z}.\, \rho')$$

This is proved by considering the different possible cases of the axiom ϑ_C^σ.

1. In this case $\vec{x} = \vec{z}$ and $\rho = \rho'$. Let $\mathcal{G}^\flat(\mathbf{f}(\vec{x}.\, \rho)) = \mathbf{U}_1; \cdots; \mathbf{U}_n$, $\vec{\pi} = \langle \pi_1, \cdots, \pi_r \rangle$ and $\mathcal{G}^\flat(\mathbf{f}(\pi_i) = \mathbf{V}_1^i; \cdots; \mathbf{V}_{k_i}^i$. Let us show that $\mathcal{G}^\flat(\mathbf{f}(\vec{x}.\, \rho)[^{\vec{\pi}}/_{\vec{y}}]) = \mathbf{U}_1; \cdots; \mathbf{U}_n$. Easy unfoldings of the definition of $\mathcal{G}^\flat$ yield the following equalities:

$$\begin{array}{rcl} \mathcal{G}^\flat(\mathbf{f}(\vec{x}.\, \rho)[^{\vec{\pi}}/_{\vec{y}}]) & = & \mho((\mathbf{U}_1; \cdots; \mathbf{U}_n)[^{\mathcal{G}^\flat(\vec{\pi})}/_{\vec{y}}]) \\ & = & \mathbf{U}_1 \cup (\bigcup_{y_i} o_{y_i}(\mathbf{f}(\vec{x}.\, t)) \cdot V_1^i) \ ; \ \mho((\mathbf{U}_2; \cdots; \mathbf{U}_n)[^{\mathcal{G}^\flat(\vec{\pi}\,')}/_{\vec{y}}]) \end{array}$$

   where $\vec{\pi}\,' = \langle \mathbf{V}_2^1; \cdots; \mathbf{V}_{k_1}^1, \cdots,\ \mathbf{V}_2^r; \cdots; \mathbf{V}_{k_r}^r \rangle$ and t is the initial expression of ρ. Observe that, according to the hypothesis, $o_{y_i}(\mathbf{f}(\vec{x}.\, t)) = \emptyset$. Thus, $\mathbf{U}_1 \cup (\bigcup_{y_i} o_{y_i}(\mathbf{f}(\vec{x}.\, t)) \cdot V_1^i) = \mathbf{U}_1$. Similarly at every successive step. Hence the lemma.

2. The hypotheses are $\vec{y} \cap \vec{x} = \emptyset$, and that when $\vec{y} \cap \mathsf{var}(t) \neq \emptyset$, then there is no clash of bound variables and free variables in the initial expressions of $\vec{\pi}$ (as in the previous item, t represents the initial expression of ρ). Thus, $\vec{z} = \vec{x}$ and $\rho' = \rho[^{\vec{\pi}}/_{\vec{y}}]$. Observe that:

$$\begin{array}{rcl} \mathcal{G}^\flat(\mathbf{f}(\vec{x}.\,\rho)[^{\vec{\pi}}/_{\vec{y}}]) & = & \mho((\mathbf{U}_1;\cdots;\mathbf{U}_n)[^{\mathcal{G}^\flat(\vec{\pi})}/_{\vec{y}}]) \\ & = & \mho(1\cdot(\mathbf{U}'_1;\cdots;\mathbf{U}'_n)[^{\mathcal{G}^\flat(\vec{\pi}\,')}/_{\vec{y}}]) \end{array}$$

where the U'_i are defined in the obvious way starting from the U_i. Furthermore, at each step, $o_{y_i}(\mathbf{f}(\vec{x}.\,t)) = 1\cdot W$, for some W. This ensures that it is always possible to factorize 1. The thesis follows by definition of prefixing (see Section 3).

3. Similar to item 2 because, by definition, the redex occurrences in $\mathcal{G}^\flat(\mathbf{f}(\vec{z}.\,\rho)[^{\vec{\zeta}}/_{\vec{x}}])$ (where $\vec{\zeta}$ is a vector of identities) and $\mathcal{G}^\flat(\mathbf{f}(\vec{x}.\,\rho))$ are the same (just the expression changes).

In the general case we have $\mathbf{f}(\vec{x}^{\,1}.\,\rho_1,\cdots,\,\vec{x}^{\,p}.\,\rho_p)$. It is easy to prove that we can write each step of $\mathcal{G}^\flat(\mathbf{f}(\vec{x}^{\,1}.\,\rho_1,\cdots,\,\vec{x}^{\,p}.\,\rho_p)[^{\vec{\pi}}/_{\vec{y}}])$ as

$$\bigcup_{1\le j\le p} j\cdot\left(\mathbf{U}^j \cup \left(\bigcup_{y_i} o_{y_i}(t_j)\cdot\mathbf{V}_i\right)\right)\ .$$

This lets us consider one argument at a time.

(Lifted CRS-Axioms) Follows the same pattern as the axioms in $=_{CRS}$.

Finally, notice that the inductive rule of congruence in the Birkhoff deductive system follow from the fact that, in oCRS's, permutation equivalence is a congruence w.r.t. the algebraic operators.

Lemma 4 can be strengthened to deal with a substitution-free elementary step. The proof is similar to that of Lemma 4 and, thus, omitted.

Lemma 7 *Let U be a set of redexes in t and π be a substitution-free elementary step. Then $\mathcal{G}^\flat(\mathcal{F}^\flat(\mathbf{U})) = \mathbf{U}$ and $\mathcal{F}^\flat(\mathcal{G}^\flat(\pi)) = \pi$.*

Theorem 3 *$\mathcal{L}^g$ and $\mathcal{M}^\flat$ are isomorphic categories.*

Proof: The two mappings providing the isomorphism are $\mathcal{F}^\flat$ and $\mathcal{G}^\flat$. Indeed, Lemma 2 and Lemma 3 guarantee that they are well-defined. $\mathcal{F}^\flat$ and $\mathcal{G}^\flat$ are obviously functors. Let us show that $\mathcal{G}^\flat(\mathcal{F}^\flat(\sigma)) \equiv \sigma$ and $\mathcal{F}^\flat(\mathcal{G}^\flat(\sigma)) =^\flat \sigma$. In the first equality, by definition, $\sigma = \mathbf{U}_1;\cdots;\mathbf{U}_n$. So the equality follows by functoriality of $\mathcal{F}^\flat$ and $\mathcal{G}^\flat$ and Lemma 7. As far as the latter equality is concerned, take the derivation $\sigma = \pi_1;\cdots;\pi_n$ where the π_i are elementary steps and substitution-free (it exists by Lemma 1 and Proposition 6). The equality $\mathcal{F}^\flat(\mathcal{G}^\flat(\pi_1;\cdots;\pi_n)) =^\flat \pi_1;\cdots;\pi_n$ follows by functoriality of $\mathcal{F}^\flat$ and $\mathcal{G}^\flat$ and Lemma 7.

8 Conclusions

We have axiomatized permutation equivalence in the case of term rewriting systems and orthogonal Combinatory Reduction Systems. This has the advantages of freeing permutation equivalence from the residual calculus, thus providing a more "uniform" and algebraic approach to permutation equivalence. We have proved that the axiomatization proposed by Meseguer [Meseguer 1992] is complete in the case of term rewriting systems but needs further axioms in the case of oCRS's.

A more orthodox approach to make the axiomatization complete in the case of CRS's should be founded, in our opinion, on a deep analysis of the algebraic properties of the mechanisms of binding and substitution. The underlying slogan in Meseguer's methodology is "a correct algebraicization yields a complete axiomatization of permutation equivalence". That is, broadly speaking, Meseguer's formulation should be a touchstone for the algebraicization of a formal system.

For instance, Meseguer's equivalence should turn out complete w.r.t. $\equiv$ in the case of combinatory logic (where the mechanisms of binding and substitution disappear). But this formal system lies at a lower abstraction level than the λ-calculus. The question that remains open is whether it is possible to provide an alternative description of CRS's where variables are still present, and substitutions are not implemented by simpler operations, such that Meseguer's axioms are complete w.r.t. $\equiv$.

Acknowledgements: Many thanks to José Meseguer for his careful reading of the paper and his suggestions. We also thank an anonymous referee whose comments have helped us improve the exposition.

References

[Abadi, Cardelli, Curien and Lévy 1990] M. Abadi, L. Cardelli, P. L. Curien, and J. J. Lévy (1990) Explicit substitutions. In *Proceedings* 17^{th} *ACM Symposium on Principles of Programmining Languages*, pages 59 – 71.

[Aczel 1978] P. Aczel (1978) A general Church-Rosser theorem. Draft, Manchester.

[Boudol 1985] G. Boudol (1985) Computational semantics of term rewriting systems. In M. Nivat and J. C. Reynolds, editors, *Algebraic Methods in Semantics*, pages 169 – 236. Cambridge University Press.

[Boudol and Castellani 1988] G. Boudol and I. Castellani (1988) A non-interleaving semantics for CCS based on proved transitions. *Fundamenta Informaticae*, 11(4):433–452.

[Corradini and Montanari 1992] A. Corradini and U.Montanari (1992) An algebraic semantics for structured transition systems and its application to logic programs. *Theoretical Computer Science*, 103:51 – 106.

[Curry and Feys 1974] H.B. Curry and R. Feys (1974) *Combinatory Logic*, volume 1. North-Holland.

[Klop 1980] J. W. Klop (1980) *Combinatory Reduction System.* PhD thesis, Mathematisch Centrum, Amsterdam.

[Klop and van Oostrom and van Raamsdonk 1993] J. W. Klop and V. van Oostrom and F. van Raamsdonk (1993) Combinatory Reduction System: introduction and survey. *Theoretical Computer Science*, 121:279 – 308, 1993.

[Laneve 1994] C. Laneve (1994) Distributive Evaluations of λ-calculus. *Fundamenta Informaticae*, 20(4):333–352.

[Laneve and Montanari 1992] C. Laneve and U. Montanari (1992) Axiomatizing permutation equivalence in the λ-calculus. In 3^{th} *Int. Conf. on Algebraic and Logic Programming*, volume 632 of *Lecture Notes in Computer Science*, pages 350 – 363. Springer-Verlag.

[Lévy 1980] J.J. Lévy.(1980) Optimal reductions in the lambda-calculus. In J.P. Seldin and J.R. Hindley, editors, *To H.B. Curry, Essays on Combinatory Logic, Lambda Calculus and Formalism*, pages 159 – 191. Academic Press.

[Manca and Salibra and Scollo 1990] V. Manca and A. Salibra and G. Scollo (1990) Equational type logic. *Theoretical Computer Science*, 77:131 – 159, 1990.

[Meseguer 1992] J. Meseguer (1992) Conditional rewriting logic as a unified model of concurrency. *Theoretical Computer Science*, 96:73 – 155, 1992.

[Meseguer and Goguen 1985] J. Meseguer and J.A. Goguen (1985) Initiality, Induction and Computability. In M. Nivat and J. C. Reynolds, editors, *Algebraic Methods in Semantics*, pages ??? – ???. Cambridge University Press.

[Meseguer and Montanari 1990] J. Meseguer and U. Montanari (1990) Petri nets are monoids. *Information and Computation*, 88:155 – 164.

[Talcott 1993] C. Talcott (1993) A theory of binding structures and applications to rewritings. *Theoretical Computer Science*, 112:99 – 143.