CHURCH-ROSSER PROPERTIES OF WEAKLY TERMINATING TERM REWRITING SYSTEMS

Jean-Pierre Jouannaud (*) Helene Kirchner (*) and Jean-Luc Remy

CRIN et Greco de Programmation
Campus Scientifique BP 239
F54506 Vandoeuvre les Nancy Cedex

ABSTRACT

The well known Knuth and Bendix completion procedure computes a convergent term rewriting system from a given set of equational axioms. This procedure was extended to handle mixed sets of rules and equations in order to deal with axioms that cannot be used as rules without loosing the required termination property. The developed technique requires the termination property of the rules modulo the equations. We describe here an abstract model of computation, assuming the termination property of the set of rules only. We show that two abstract properties, "uniform confluence modulo" and "uniform coherence modulo" are both necessary and sufficient ones to compute with these models. We then give sufficient properties that can be checked on "parallel critical pairs", assuming the rules are left linear. These results allow to deal with sets of axioms including coramutativity, associativity and idempotency.

INTRODUCTION

Term Rewriting Systems (TRS in short) are used for a lot of Artificial Intelligence applications. TRS express computations based on directed equalities, whenever properties are satisfied. The well known Confluence property expresses roughly that the result of a computation does not depend on the choice of the rules to be applied. When a TRS is not confluent, it can be transformed into an "equivalent" confluent one, using the well known Knuth and Bendix completion procedure [K&B,70]. This procedure can be seen as a way to compile equational specifications into confluent sets of rules. Then these rules can be used as well as "PROLOG like" programs [DER,82].

During the ten past years, the Knuth and Bendix completion procedure was shown to be a major tool for a wide class of problems, mainly the word problem in universal algebras [K&B,70], equivalence proofs of sets of axioms in algebra [LES,83], unification in equational theories [JKK,83], proving consistency and assertions in algebraic specifications of data types [H&H,80], theorem proving in first order logic [H&D,83], program synthesis from specifications [DER,82] [H&P,82], computing with rewrite programs [DER,82]. The Knuth and Bendix completion procedure is based on using equations as rewrite rules and computing "critical pairs" when left members of rules overlap. If a critical pair has distinct irreducible forms, then a new rule must be added and the procedure recursively applies until it eventually stops. This procedure requires the termination property of the set of rules, which can be proved by various tools. A full implementation of these techniques is described in [LES,83].

The method was extended to handle the case of Equational Term Rewriting Systems (ETRS in short) i.e. sets A of axioms split into a set R of rules and a set E of equations, in order to allow axioms such as commutativity, which cannot be directed without loosing the termination property. A first approach by Lankford and Ballantyne [L&B,77] studies permutative axioms that generate finite E-congruence classes. The case of infinite E-congruence classes was studied by Peterson and Stickel [P&S,81] and Huet [HUE,77-&80]. These approaches are unified and generalized in [JOU,83], where two properties, E-confluence and E-coherence, are shown to be both necessary and sufficient ones to compute with ETRS. When an ETRS is not E-confluent and E-coherent, it can be transformed into an equivalent E-confluent and E-coherent one by computing "E-critical pairs". In addition to a complete E-unification algorithm, this E-completion procedure requires the termination of the relation induced by the rules in the E-congruence classes.

The termination of a set of rules can be checked by various tools such as the recursive path ordering [DER,79] and the recursive decomposition ordering [JLR,82]. On the contrary, checking the E-terrainations of a set of rules is actually an open problem except for the special case of associative and commutative equations.
Moreover, a set of rules can be terminating and not E-terminating as noticed by Jeanrond [JEA,80]. The following counterexample is extracted from a set theory or from a boolean ring theory:
Assume + is an idempotent function symbol and let l->r be any rule. Then 1 - 1+1 -> 1+r , which induces an infinite derivation even if the set of rules itself was terminating.

To solve this problem, Padawitz developed in [PAD,82] new techniques based on a so called "strong confluence" property, proved to be sufficient for a Church-Rosser property. However, it is rather complicated to express and carries on a lot of technical restrictions, in addition to the left linearity of the set of rules.

Our first goal in this paper is to give a well suited framework in order to simplify and

generalize Padawitz's results. This is achieved by describing an abstract model of computation in the same way as in [JOU,83J: It makes clear that two properties, "uniform confluence modulo" and "uniform coherence modulo" are both necessary and sufficient conditions for the Church-Rosser property that we need. Uniform confluence modulo ensures that the normal form of any term, using the rules of R, is unique up to the equality generated by the equations of E. Uniform coherence modulo says roughly that the uniqueness is also true if the reduction is applied to terms that are equal, up to the E-equality.

Applying then this abstract model to ETRS, we obtain easily a more general version of Padawitz's results as well as new ones. More precisely, we introduce sufficient conditions for uniform confluence modulo and uniform coherence modulo called local confluence in one step and local coherence in one step, that can be checked on critical pairs or on "parallel critical pairs" as in [PAD,82].

Section I is devoted to recall classical notions about TRS. A purely axiomatic approach working with arbitrary relations is developed in section II. Abstract results obtained in section II are applied to ETRS in section III. Equalities are used as usual in a first subsection, whereas they are used in a parallel way in a second one and in a recursive parallel way In a third one.

I-PRELIMINARIES

Definitions 1: Given a set X of variables and a graded set F of function symbols T(F,X) denotes the free algebra over X. Elements of T(F,X) are called terms. Terms may be viewed as labelled trees in the following way : a terra t is a partial application of N* into F X such that its domain D(t) satisfies:
(1) The empty word e is in D(t).
(2) iu is in D(f(... ti ...)) iff u is in D(t).
D(t) is the set of occurrences of t, 0(t) the subset of non variable occurrences of D(t), V(t) the set of variables of t and #(x,t) the number of occurrences of x in t. A term t is said to be linear iff //(x,t)*l for any x in V(t). Let t/u be the subterm of t at occurrence u and t[u<-t'] the terra obtained by replacing t/u by *t"* in t. []

Definations_2: Substitutions s are defined to be endomorphisms of T(F,X) with a finite domain D(s) - {x In X I s(x) 4 xj.
Composition of two substitutions s and s' is denoted by s s'.
The subsumption preorder < on T(F,X) is defined by: t < t' iff t'- s(t) for a substitution s called a match from t to t'. Given a subset V of X, we define s<s' [V] iff s(x) *4* s'(x) for all x in V, which is equivalent to s'=s'o s [V] for some substitution s". V is omitted if equal to X. A substitution s is a unifier of two terms t and t' iff s(t)=s(t'). For any unifiable terms t and t', there exists a minimum unifier of t and t' (for the ordering < [V(t)UV(t')]), called most general unifier (mgu for short) of t and t'. []

defination-2: we call axiom or equation any pair (t,t') of terms and write it t-t'. The A-equality -A (or |-*-|A) is the smallest congruence closed under instanciation and generated by a finite set A of axioms.
I — I A denotes one step of A-equality.
I —n—I A denotes n steps of A-equality. []

Many theoretical problems in equational theories (word problem,...) can be approached by using rewrite rules that is one-way equations. Working with rules requires good properties as shown by Knuth and Bendix [K&B,70],

Definitions 4: A term rewriting system R is a set of pairs g->d s.t. V(d)cV(g).
We say that a term t R-reduces at occurrence u to a terra t' using the rule g->d, and we write t ->R *t"* , iff there exists a match s from g to t/u and t' - tfu <- s(d)]. We may omit R.
A term rewriting system R is left (resp. right) linear if g (resp. d) is linear for all g->d in R.
-*->R is the reflexive transitive closure of ->R,
-+->R the transitive closure of ->R and
=R the generated equational theory.
An irreducible term' for -> is said in normal form, t! denotes a normal form of t, that is a term t" in normal form s.t. t -*-> t'.
A term rewriting system R is terminating (or noetherian) if there Is no infinite sequence of the form: tO ->R tl ->R ... tn ->R .... []

II.ABSTRACT PROPERTIES OF CONFLUENCE

From now on, we deal with weakly terminating Equational Term Rewriting Systems (ETRS in short), that is sets A of axioms split into a terminating TRS R and a set E of equations with a decidable E-equality. These ETRS are said to be weakly terminating because the relation -E ->R =E induced by ->R in the E-equivalence classes is not necessarily terminating as required in other works [HUE,77&80] [P&S.81] [JOU,83].

We start here using abstract relations: In this section, |-|E is any symetric relation whose reflexive transitive closure is -E , ->R is any relation and -A is the reflexive, symmetric and transitive closure of ->R U =E . This abstract approach allows us to generalize Padawitz's results and provides new ones by appropriate choices of the relation |-|E in section III.

To decide A-equality, the classical way is to require a Church-Rosser property, which allows to decide whether tl "A t2 or not by computing the normal forms of tl and t2 and checking for their E-equality. Two properties called confluence and coherence are needed to ensure the Church-Rosser property. The style of properties we use here is quite different from Jouannaud's [JOU,83] or Huet's [HUE,77&80], because we explicitely use normal forms in the definitions. This difference is quite important in the abstract part of the paper: it allows removing the so-called E-termination property of the set of rules. It will however carry on other restrictions in section III.

Definition 5: R is said to be:
Uniformly Church-Rosser modulo E iff ∀t1,t2 s.t. t1 =A t2 , then t1! =E t2! .
Uniformly confluent modulo E iff ∀t,t1,t2 s.t. t1 <-*- t -*-> t2 , then t1! =E t2!.
Uniformly coherent modulo E iff ∀t,t1,t2 s.t. t1 <- t =E t2 , then t1! =E t2! []

Notice that under these hypotheses, a term may have several different normal forms. Therefore, each upper formula t1! =E t2! is existencially quantified and must read: there exist t1! and t2! such that t1! =E t2!. On the other hand, the property of uniform confluence modulo E implies obviously that different normal forms of a same term are E-equal, avoiding the drawback of having to choose each time the good one. Therefore, normal forms are universally quantified as well as existencially quantified!

Lemma 1: Let R be uniformly confluent modulo E. Then R is uniformly coherent modulo E iff t =E t' implies t! =E t'! . []

Proposition 1: R is uniformly Church-Rosser modulo E iff R is uniformly confluent modulo E and uniformly coherent modulo E.

Proof: The "only if" part is obvious. The "if" part is proved by induction on the length of the A-equality with the help of lemma 1. []

As usually, we now reduce global properties to local ones.

Definitions 6: R is said to be:
locally uniformly confluent modulo E iff ∀t,t1,t2 s.t. t1 <-t-> t2, then t1! =E t2! .
locally uniformly coherent modulo E iff ∀t,t1,t2 s.t. t1 |-|E t ->t2, then t1! =E t2! []

Proposition 2: Assume R is noetherian. Then R is uniformly confluent modulo E and uniformly coherent modulo E iff R is locally uniformly confluent modulo E and locally uniformly coherent modulo E.

Proof : The "only if" part is obvious . For the "if" part, we first prove that local uniform confluence modulo E implies uniform confluence modulo E by noetherian induction on ->:
Let t -> t1 -*->t' and t ->t2 -*-> t" .
t1! =E t2! by uniform local confluence hypothesis.
t'! =E t1! by induction hypothesis applied to t1.
t"! =E t2! by induction hypothesis applied to t2.
Therefore, t'! =E t"! achieving the first part.
We now prove that local uniform coherence modulo E implies uniform coherence modulo E, by induction on n if t |-n-|E t1. The case n=0 is obvious. For the case n+1, let assume t |-|E t' |-n-| t1 . Applying first local uniform coherence modulo E, we then discuss the two following cases:
- if t' is irreducible and t1 is reducible into t" the result is obtained by induction hypothesis.
- if t' is reducible, the result is obtained by induction hypothesis and the already proved uniform confluence modulo E property. []

It should be noticed that, on the contrary to Huet's approach [HUE,77&80], the termination property of R is sufficient here, because we compute normal forms for closing the diagrams.

Unfortunately, these local properties cannot be of any help, because they don't carry on an easy check on the rewriting system. Against this drawback, we introduce two new local properties which carry on sufficient conditions only.

Definition 7: We write t |-ℓ-|E t' iff either t=t' or t |-|E t'. A pair (p,q) is confluent in one step modulo E and we write p !0,1!E q iff there exist two terms t and t' such that p -*-> p' |- ℓ -|E q' <-*- q.
R is locally confluent in one step iff ∀t,t1,t2 s.t. t1 <- t -> t2 , then t1 !0,1!E t2 .
R is locally coherent in one step iff ∀t,t1,t2 s.t. t1 <- t |-|E t2 , then t1 !0,1! t2 . []

We now show that these new local properties imply the previous local ones:

Proposition 3: Assume R is noetherian, locally confluent in one step and locally coherent in one step. Then R is both:
a) locally uniformly coherent modulo E
b) locally uniformly confluent modulo E

Proof : we prove a) using a noetherian induction on the pairs of terms, then b).
Let us define the relation ==> by :
(x,y)==>(x',y') iff either (1) x-+->x' and y-*->y'
or (2) x-+->y' and y-*->x'
As R is terminating, cases 1 and 2 are separately noetherian. As case 1 steps can be incorporated into case 2 steps, ==> is also noetherian.
Let now go back to the main proof of:
- a). Let t2 <- t |-| t1. Using local coherence modulo E in one step, there exist u1 and u2 s.t. t1 -*-> u1, t2 -*-> u2 and u1 |-ℓ-|E u2 .
If neither u1 nor u2 is reducible, or if u1 and u2 are equal, then we are done. Else assume u1 reduces to u1': The result is obtained by applying the induction hypothesis a) to the pair (u1,u2) which is a proper son of the pair (t,t1) for ==>.
- b). Let t1 <- t -> t2 . Using local confluence modulo E in one step, there exist u1 and u2 s.t. t1 -*-> u1, t2 -*-> u2 and u1 |-ℓ-|E u2 .
The result now follows from property a). []

III. APPLICATION TO EQUATIONAL, REWRITING SYSTEMS

From now on, we assume that =E is the equality generated by a set of axioms E and |—|E is one step of some relation whose transitive closure is equal to -E. This relation will first be we step of E-equality, then one step of parallel E-equality, finally one step of recursive parallel E-equality. In each case, a pair (p,q) is said to be confluent in one step |-|E, iff there exists terms p" and q' such that:
p -*-> p' |-.e "|E q' <-*- q.

III.1. E=EQUALITY

In this section, |—|K is one step of E-

equality. In the case of left and right linear rewrite rules, we show how to check our local properties on classical critical pairs.

Definition 8: A term t' overlaps a term t at occurrence u in O(t), with a substitution s iff s is a mgu of t' and t/u. Given two pairs (g,d) and (g',d') s.t. V(g)∩V(g') = ∅ and g overlaps g' at occurrence u with a substitution s, (p=s(d'), q=s(g'[u<-d])) is a critical pair of (g,d) on (g',d') at occurrence u. Let SCP(R) be the set of all critical pairs of rules of R on rules of R, SCP(E,R) the set of all critical pairs of equations of E (oriented both sides) on rules of R and SCP(R,E) the set of all critical pairs of rules of R on equations of E. []

With the concept of critical pair is associated the so called:

Critical pairs lemma [HUE,77&80]: Assume that t ->[e,g->d] t1 and t ->[v,l->r] t2 with v in O(g). Then, there exists a critical pair (p,q) and a substitution s such that t1 = s(p) and t2 = s(q).
The pair (p,q) is in SCP(R) if g->d and l->r are rules of R, in SCP(E,R) if g=d is an equation of E and l->r a rule of R and in SCP(R,E) if g->d is a rule of R and l=r an equation of E. []

The following propositions are modified versions of lemmas 3.1 and 3.5 of [HUE,77&80]. The proofs are based on the critical pairs lemma.

Proposition 4: R is locally confluent in one step |-|E iff all critical pairs of R are confluent in one step |-|E. []

Proposition 5: Assume R is right and left linear. Then R is locally coherent in one step |-|E iff all critical pairs in SCP(R,E) and SCP(E,R) are confluent in one step |-|E.

Proof : Let us prove the non obvious "if" part:
Assume t |-|E t1 using axiom g1=d1 at occurrence u with a match s1 and t -> t2 using rule g2->d2 at occurrence v with a match s2.
Three cases must be distinguished :
1. u and v are disjoint occurrences: then rule and axiom commute.
2. u ≤ v , with two subcases, assuming u=e without loss of generality:
   subcase 1: v is not in O(g1).
   Then, there exists a variable x such that s1(x) is reducible by g2->d2 and local coherence in one step is proved as usually (see [JOU,83]).
   subcase 2: v is in O(g1).
   From critical pair lemma, a critical pair (p,q) in SCP(R,E) and a substitution s exist s.t. t2=s(p), t1=s(q) and p -*->p' |-£-|E q'<-*- q . Therefore, t2 -*-> s(p') |-£-|E s(q') <-*- t1 .
3. v < u , with two subcases, assuming v=e without loss of generality:
   subcase 1: v is not in O(g2).
   Then a variable x exists s.t. the axiom g1=d1 applies to a subterm of s2(x) at occurrence w.
   Define s'2 by s'2(x)= s2(x)[w<-s1(d1)]
   s'2(y)= s2(y) if y is distinct of x.
   Then t2=s2(d2) <- t=s2(g2) |-|E s'2(g2)=t1 and since g2 and d2 are both linear,
   t2 = s2(d2) |-|E s'2(d2) <- s'2(g2) = t1 .
   subcase 2: v is in O(g2).
   Using the critical pairs lemma, there exists a critical pair of SCP(E,R), and the proof is achieved as in case 2, subcase 2. []

As a corollary of these two propositions and propositions 1, 2 and 3:

Theorem 1: Let R be a right and left linear, terminating term rewriting system and E a set of axioms such that =E is decidable. Then R is uniformly Church-Rosser modulo E if all critical pairs (p,q) in SCP(R), SCP(R,E) and SCP(E,R) are confluent in one step |-|E. []

Examples: The following sets of rules and axioms satisfy these conditions:

1. R = { h(x+y) -> h(x)+h(y) ; f(f(x)) -> x }
   E = { (x+y)+z = x+(y+z) ; x+y = y+x ; x+x = x }
2. idempotent groups:
   R = { x*e -> x ; e*x -> x ; i(e) -> e ;
   i(i(x)) -> x ; i(x*y) -> i(y)*i(x) }
   E = { x*y = y*x ; x*(y*z) = (x*y)*z ; x*x = x }

III.2. PARALLEL E-EQUALITY

In order to drop out the right linearity restriction, we are now going to apply several steps of E-equality at the same time. More formally, we define the parallel E-equality |=|E, whose reflexive transitive closure is also =E :

Definition 9: The parallel E-equality relation |=|E is defined as follows:
t |=|E t' iff there exist disjoint occurrences v1, ... ,vn in O(t), axioms gi=di in E and substitutions si s.t. t/vi = si(gi) for any i in [1..n] and t' = t[v1<-s1(d1)] ... [vn<-sn(dn)]. []

Working with this new equality requires new critical pairs [PAD,82]:

Definition 10: Terms g1,g2,..., gn are said to overlap the term g at disjoint occurrences v1,v2,...,vn in O(g) with the substitution s iff s is the most general unifier of the set of pairs {(g/v1, g1),..., (g/vn, gn)}.
The pair (p=s(d), q=s(g[v1<-d1]...[vn<-dn])) is said to be a parallel critical pair of the axioms g1=d1,...,gn=dn on the rule g->d at occurrences v1,...,vn in O(g) iff g1,...,gn overlap g at these occurrences with the substitution s.
Let SPCP(E,R) be the set of all parallel critical pairs of E on R obtained by all possible overlappings of sets of axioms of E on rules of R. []

Notice that a critical pair is a particular case of a parallel critical pair. With parallel critical pairs is associated the so called:

Parallel critical pairs lemma: Let t=s(g) for g->d in R and for any i in [1..n] t/vi=si(gi) with vi disjoint occurrences in O(g) and gi=di or di=gi in E. Then there exist

a parallel critical pair (p,q) and a substitution r s.t. s(d) = r(p)
and s(g)[v1<-s1(d1)]...[vn<-sn(dn)] = r(q).

Proof: as Huet's proof of critical pair lemma. []

An easy generalization of proposition 4 gives first :

Proposition 6: R is locally confluent modulo E in one step |=|E iff all critical pairs of R are confluent in one step |=|E. []

Using now parallel critical pairs, we get:

Proposition 7: A left linear TRS R is locally coherent in one step |=|E if:
- all critical pairs of R in E are confluent in one step |=|E.
- all parallel critical pairs of E in R are confluent.

Proof : Assume that t |=|E t1 at occurrences v1,...,vn with substitutions s1,...sn and axioms g1=d1,...,gn=dn and that t -> t2 at occurrence u with the rule g->d and the substitution s0.
Three cases are to be distinguished:

1. u is disjoint from all the vi, i=1,...,n. Then -> and |=|E commute.
2. vi≤u for an i. Then the proof works as the corresponding case 2 in propoaition 5.
3. Let J be the subset of [1,n] such that u<vi for i in J. Without loss of generality, we assume that J=[1,m'=m-1]. Let now K be the subset of J such that vi is in O(g) for any i in K. Let us assume that K=[1,k'=k-1]. The proof consists of sharing the step t |=|E t1 in three parts:
   t |=|E t' |=|E t" |=|E t1 with
   t' = t[v1<-s1(d1)] ... [vk'<-sk'(dk')]
   t" = t'[vk<-sk(dk)] ... [vm'<-sm'(dm')]
   t1 = t"[vm<-sm(dm)] ... [vn<-sn(dn)]

   1st part : applying the parallel critical pair lemma, there exist a critical pair (p,q) in SPCP(E,R) and a substitution s such that:
   t2 = t[u<-s(p)] and t'= t[u<-s(q)].
   As p and q reduce both to a given term, say pq, t2 and t' reduce both to t'2 = t2[u<-s(pq)].

   2nd part: for any j in K, there exists a variable x in V(g) and an occurrence wj such that s0(x)/wj is an instance of gj. Let Z be the set of all these variables. As g is linear, the terms s0(x) do not change in t'. Furthermore any variable x in Z is a variable of q and satisfies s0(x)=s(x).
   Let us now define the substitution s' :
   s'(x) = s(x) if x is in V(q)\Z and
   s'(x) = s0(x)[wj<-sj(dj)] if x is in Z.
   Then t"= t[u<-s'(q)] -*-> t"2 = t[u<-s'(p')] and s(q') |=|E s'(q') , therefore t'2 |=|E t"2 at occurrences which are suffixes of u.

   3rd part: As t" -*-> t"2 and t" |=|E t1 at disjoint occurrences, t1 -*-> t'1 |=|E t"2.

Finally t'2 |=|E t"2 |=|E t'1 at disjoint sets of occurrences, therefore t'2 |=|E t'1. []

As a corollary of Propositions 1, 2, 3, 6 and 7, we obtain now:

Theorem 2: Let R be a left linear and terminating term rewriting system, and E a set of axioms such that =E is decidable. Then R is uniformly Church-Rosser if:
- all critical pairs in SCP(R) are confluent modulo E in one step |=|E
- all critical pairs in SCP(R,E) are confluent modulo E in one step |=|E
- all parallel critical pairs in SPCP(E,R) are confluent.

Example: Removing the right linearity hypothesis on the rules allows to deal with rules like distributivity. The following ETRS satisfies theorem 2:
R = { z*(x+y)->(z*x)+(z*y) ; z*(x+y)->(z*y)+(z*x);
z+0 -> z ; 0+z -> z ; z*0 -> 0 ; 0*z -> 0 }
E = { x+y = y+x }

III.3. RECURSIVE PARALLEL E-EQUALITY

In this section, we use the recursive parallel equality introduced by Padawitz [PAD,82], in order to allow parallel critical pairs of E in R to be confluent in one step of this equality.

Definition 11: The recursive parallel E-equality is defined by: t |=rec=|E t' iff there exist disjoint occurrences v1,v2,...,vn in D(t), axioms (g1=d1),...,(gn=dn) in E, substitutions s1,s2,...,sn and s'1,s'2,...,s'n s.t. t/v1 = s1(g1),...,t/vn = sn(gn),
s'i(x) |=rec=|E si(x) or s'i(x) = si(x) for any i and any variable x
and t' = t[v1<-s'1(d1)] ... [vn<-s'n(dn)]. []

Example: With E = { x+y = y+x }
(a+b)+(c+d) |=rec=|E (d+c)+(b+a).

Notice that equality steps do not overlap in |=rec=|E and let us point out some easy properties of |=rec=|E, freely used in what follows:

a) For any terms t,t1,...,tn,t'1,...,t'n and any disjoint occurrences v1,..., vn in D(t), if t1 |=rec=|E t'1,..,tn |=rec=|E t'n, then t[v1<-t1]...[vn<-tn] |=rec=|E t[v1<-t'1]...[vn<-t'n] (compatibility).
b) For any terms t, t' and any substitution s, t |=rec=|E t' implies s(t) |=rec=|E s(t')
c) For any term t and any substitutions s and s' such that s(x) |=rec=|E s'(x) for any x in V(t), then s(t) |=rec=|E s'(t) .

Composition lemma: For any terms t,t' such that t |=rec=|E t' and substitutions s,s' s.t. s(x) |=rec=|E s'(x) for any x, then s(t) |=rec=|E s'(t'). []

Proof: We say that a relation is closed by recursive application if, for any axiom g=d and any substitutions s,s', s(g) and s'(d) are related when s(x) and s'(x) are related for any variable. Clearly |=rec=|E is the smallest relation on terms closed by recursive application and compatible

with the operations of the algebra.
For two substitutions s and s', let us now define the relation COMP(s,s') on any terms t, t' by:
t COMP(s,s') t' iff s(t) |=rec=|E s'(t').
It is now easy to prove that Comp is compatible with the operations of the algebra and closed by recursive application.
Therefore |=rec=|E is included into COMP(s,s'). []

Again, the property of local confluence modulo E in one step |=rec=|E is an easy generalization of proposition 4:

Proposition 8: R is locally confluent modulo E in one step |=rec=|E iff all critical pairs of R are confluent in one step |=rec=|E. []

The property of local coherence modulo E in in one step |=rec=|E is more difficult to ensure. It is possible to define recursive parallel critical pairs of E in R; however, in addition to a complex formalism, tricky cases can appear. According to Padawitz, we therefore prefer to add conditions on the rewrite rules and axioms in order to avoid these problems and keep parallel critical pairs of E in R only:

- Hypothesis 1: There is no superposition of rules into axioms except at occurrence e. It's not too restrictive for abstract data types, where top symbols of rules are usually new symbols, distinct from constructors.
- Hypothesis 2: Rules are left linear. Again, this is not too restrictive for data types, because definitions of functions use different variables.
- Hypothesis 3: For any parallel critical pair of E in R, say (p,q), obtained by superposition of axioms gi=di into g, the most general unifier s of the pairs {(g/vi,gi)} is a match from g/vi to gi. As a consequence, variables of gi are instanciated and belong to V(q).

The proof of local coherence modulo E in one step |=rec=|E consists of two steps: we show first that local coherence modulo E in one step |=rec=|E holds when rewriting t at the top of t, assuming hypotheses 2, 3 and a closure property on the parallel critical pairs of E in R. Then we are able to prove local coherence in the general case, assuming hypothesis 1.

Lemma 2: Assume that hypotheses 2 and 3 are true and all parallel critical pairs of E in R are confluent modulo E in one step |=rec=|E. Then, for any terms t, t1 and t2, such that
t=s0(g) -> t1=s0(d) and t |=rec=|E t2, then
t2 -*-> t'2 |=rec=|E t'1 <-*- t1.

Proof: Let v1,...,vn the smallest (for the prefix ordering) occurrences of D(t) where the recursive parallel E-equality applies. Let us first distinguish the subset K of [1,n] such that for any i in K, vi belongs to O(g) and assume, without loss of generality that K=[1,k].
The recursive parallel equality step from t to t1 is shared into two steps t |=|E t'1 |=rec=|E t1 such that t'1 is obtained from t by applying the axioms of E at occurrences v1,...,vn.

Applying the parallel critical pairs lemma, there exist a parallel critical pair (p,q) and a substitution s such that t2=s(p) and t'1=s(q). Since p and q reduce to p' and q' s.t. p' |=rec"C-=|E q', t2=s(p) -*-> s(p') |-rec-e-|E s(q') <-*- s(q)=t'1. Let now Z be the set of variables x in V(g) s.t. sO(x) contains a subterm si(gi) at some occurrence wi, for i in [k+1.-n]. Since g is linear, such variables are not instanciated in the critical pair, belong to V(q) and satisfy sO(x) = s(x). On the other hand, with the hypothesis 3 on parallel critical pairs, for any y in V(d1), y belongs to V(q)\Z and satisfies s(y)=s1(y).
Let us finaly define the substitution s' by:
for any x in V(d1):
s'(x) = s'1(x) |=rec=|E s1(x) = s(x)
for any x in Z:
s'(x) = s0(x)[w<-s'1(di)] |=rec=|E s0(x) = s(x)
for any x in V(q)\V(d1): s'(x) = s(x).
Applying finally the composition lemma, we obtain the desired result s(p') |=rec=|E s'(q'). []

Proposition 9: Let us assume hypotheses 1,2 and 3. Then R is locally coherent in one step |=rec=|E iff all parallel critical pairs of E in R are confluent modulo E in one step |=rec=|E.

Proof : Let us prove the non obvious "if" part.
Let v1,...,vn be as previously the smallest occurrences where parallel recursive equalities apply and u the occurrence in D(t) where the rule applies with the substitution s0.
We prove the property by induction on the depth d(u,t |=rec=|E t2) of the occurrence u in the recursive equality, defined as follows:
IF t=t2 or u is not a suffix of some vi
THEN d(u, t|=rec=|E t2) = 0
ELSE an unique vi (say v1) is a prefix of u;
As there is no superposition of any rule into an axiom, there exists an occurrence w of g1 such that g1(w) is a variable x and u=v1.w.u' . Let d(u,t |=rec=|E t2) = 1+d(u',s1(x) |=rec=|E s'1(x)).

-Assume d(u,t |=rec=|E t2)=0: the result is either obvious or results from lemma 2 if u is a prefix of some of the vi.

-Assume d(u,t |=rec=|E t2)=n: let v1, w, u' and x be as in the definition of the depth, g1=d1 the axiom applied at occurrence v1, s1 and s'1 the substitutions used and t"= s1(x)[u'<-s0(d)].
As d(u,s1(x) |=rec=|E s'1(x)) is less than n, by induction hypothesis there exist two terms t"2 and t"1 s.t. t" -*-> t"2 |=rec=|E t"1 <-*-s'1(x).

Let us now define the substitutions s2 and s'2, respectively equal to s1 and s'1 except for the variable x where s2(x)=t"2 and s'2(x)=t"1. Of course, s2(z) |=rec=|E s'2(z) for any variable. Therefore:
s1(g1)[w<-t"]-*->s2(g1) |=rec=|E s'2(d1)<-*-s'1(d1)
Futhermore, the occurrence v1 being disjoint from the occurrences v2,...,vn , we can apply property (a) of compatibility to achieve the proof. []

As a corollary of propositions 1, 2, 3, 8 and 9:

Theorem 3: Let E be a set of axioms such that =E is decidable and R a left linear

and terminating term rewriting system. Then R is uniformly Church-Rosser modulo E if:
- all critical pairs in SCP(R) are confluent in one step |=rec=|E,
- there is no superposition of the rules into axioms except at occurrence e.
- for any parallel critical pair of SPCP(E,R), obtained by superposition of the axioms {gi=di} into g, the most general unifier s of the pairs (g/vi,gi) is a match from g/vi to gi and (p,q) is confluent in one step |=rec=|E. []

Examples:

1. E = {x+y = y+x, (x+y)+z = x+(y+z), x+x = x}
   R = {x*(y+z) -> (x*y)+(x*z)}

2. A specification of integers with constructors 0, 1, +, OPP :
   E = {x+y=y+x, (x+y)+z = x+(y+z), x+OPP(x) = 0,
        x+0 = x, OPP(x+y) = OPP(y)+OPP(x),
        OPP(OPP(x)) = x, OPP(0) = 0}
   R = {0*x ->0, 1*x -> x, x*(y+z) -> (x*y)+(x*z),
        x*OPP(y) ->OPP(x*y)}

Remark that there are no parallel critical pairs here, but only classical ones. Notice that some critical pairs are not confluent, but confluent in one step, which was not allowed in section III.2 . For instance, in example 1:

$$x*(y+z) \;|=|E\; x*(z+y)$$
$$\downarrow \qquad\qquad \downarrow$$
$$(x*y)+(x*z) \;|=|E\; (x*z)+(x*y)$$

CONCLUSION

Local confluence in one step and local coherence in one step are defined in an abstract way for arbitrary symmetric relations.
Three different relations are then used with their corresponding critical pairs, that carry on sufficient conditions to be checked on critical pairs.
Simple equality is classical, as also the associated notion of critical pair. The corresponding theorem requires the rules to be left and right linear.
Parallel equality requires parallel critical pairs and allows to remove the condition of right linearity. However, critical pairs resulting from the superposition of equational axioms on rules have to be confluent, without any step of parallel equality.
This restriction can be simply explained. Consider an instanciation of a parallel critical pair which affects a variable that is not used in the superposition. By the way of rewritings, this variable can be mixed with the other variables. As a consequence, the term substituted for this variable can be embedded in a member of the parallel equality. Replacement of this term by an equivalent one introduces one more step of equality.
An elegant way of solving this problem is to define a recursive one step equality as Padawitz. Indeed we obtain a strictly more powerfull result without any more restriction on the equational axioms and we can deal with Padawitz's examples and also with a lot of other ones. An interesting point is that we do not define recursive critical pairs. Instead, we require equational axioms to superpose on rules only by the way of a matching of subterms of these rules: recursive equalities occur only outside of parallel critical pairs.

Finally, as confluence and coherence in one step are checked on critical pairs, a Knuth and Bendix like completion algorithm can be hoped from these results.

REFERENCES

[1] [DER,79&82] DERSHOWITZ N. : "Orderings for term rewriting systems" Proc 20th FOCS. pp 123-131 (1979) and TCS 17-3 (1982).

[2] [DER,82] DERSHOWITZ N. : "Computing with term rewriting systems" to be published.

[3] [H&D,83] HSIANG J. DERSHOWITZ N. : "Using rewrites methods for clausal and non clausal theorem proving" Proc. 10th ICALP.

[4] [H&H,80] HUET G. HULLOT J.M.: "Proofs by induction in equational theories with constructors" Proc. 21th FOCS (1980) and JCSS 25-2 (1982).

[5] [H&P,82] HSIANG J. PLAISTED D.A.: "Deriving automatically programs from proofs of specifications" to be published.

[6] [HUE,77&80] HUET G.: "Confluent reductions: abstract properties and applications to term rewriting systems" Proc. 18th. FOCS (1977) and JACM 27-4 pp 797-821 (1980).

[7] [JEA,80] JEANROND H.J.: "Deciding unique termination of permutative rewriting systems: choose your terra algebra carefully" Proc. 5th CADE. Les Arcs.

[8] [JOU,83] JOUANNAUD J.P.: "Confluent and Coherent Equational Term Rewriting Systems. Application to proofs in data types" Proc. 8th CAAP. L'aquila, Italy.

[9] [JKK,83] JOUANNAUD J.P. KIRCHNER C. and H.: "Incremental construction of unification algorithms in equationnal theories" Proc. 10th ICALP.

[10][JLR,82] JOUANNAUD J.P. LESCANNE P. REINIG F.: "Recursive decomposition ordering" in "Formal description of programming; concepts 2" Ed. BJORNER D. , North Holland

[11][K&B,70] KNUTH D. BENDIX P.: "Simple word problems in universal algebras" in "Computational problems in abstract algebra" Leech J. ed., Pergamon Press.

[12][L&B,77] LANKFORD D.S. BALLANTYNE A.M.: "Decision procedures for simple equational theories with permutative axioms: complete sets of permutative reductions" Rep. ATP-37, DCS, U. of Texas at Austin.

[13][LES,83] LESCANNE P:"Computer experiments with the REVE term rewriting system generator" Proc. 10th POPL conference.

[14][PAD,82] PADAWITZ P.: "Equational data type specification and recursive program scheme" in "Formal Description of Programming Concepts 2" Ed. BJORNER D.

[15][P&S,81] PETERSON G.E. STICKELM.E.: "Complete set of reductions for equational theories with complete unification algorithms" JACM 28. no.2, pp 233-264 .

[16][STI,81] STICKELM.E.: "A unification algorithm for associative commutative functions" JACM 28-3, pp 423-434.