PROOF-THEORETIC TECHNIQUES FOR TERM REWRITING THEORY

Nachum Dershowitz and Mitsuhiro Okada

Department of Computer Science
University of Illinois
Urbana, IL 61801, USA

Department of Computer Science
Concordia University
Montreal, Quebec H3G 1M8, CANADA

ABSTRACT

The purpose of this paper is to provide a bridge between term rewriting theory in computer science and proof theory in logic. It is shown that proof theoretic tools are very useful for analyzing two basic attributes of term rewriting systems, the termination property and the Church-Rosser property.

In section 1 we give the relationship between proof theoretic ordinals in logic and the ordering structures used in termination proof and in the Knuth-Bendix completion procedure of term rewriting theory. In section 2 we utilize the proof-theoretic normalization technique to analyze Church-Rosser property and completion procedure for conditional term rewriting theory. In the course of this study, we show that Knuth's Critical Pair Lemma does not hold for conditional rewrite systems, by presenting a counter-example. Then we present two restrictions on conditional systems under which the Critical Pair Lemma holds. One is considered a generalization of Bergstra-Klop's former result; the other is concerned with a generalization of Kaplan's and Jouannaud-Waldmann's systems.

1 PROOF-THEORETIC ORDINALS AND TERM REWRITING ORDERINGS

To show termination of a given rewrite system, the typical method is to embed the reduction ordering of the system into an abstract ordering structure known to be well-founded. In particular, if a rewrite system R consists of a set of (finite) rules (i.e., oriented equations between first-order terms) of the form $\{\ell_1 \to r_1, \ell_2 \to r_2, \ldots, \ell_n \to r_n\}$, then the induced "reduction" ordering $<_R$ is the smallest (strict partial) ordering such that $\ell_i\sigma >_R r_i\sigma$ for all $i \leq n$ and any substitution σ of terms for variables and which has the monotonicity property: if $s <_R t$, then $f(\ldots s\ldots) <_R f(\ldots t\ldots)$ for all operators f of R. In other words, $s >_R t$ if t may be obtained from s by one or more applications of rules in R to replace subterms matching a left-hand side ℓ_i with the corresponding right-hand side r_i. By T(F, C), we denote the set of variable-free terms constructed from constants in C and operators F. Thus, to show termination of a system R over a set of terms T(F, C) (i.e. that no infinite seqeunce of rewritings is possible and $<_R$ is well-founded), it is (necessary and) sufficient to show for some well-founded monotonic ordering $<T(F, C), \prec>$ on terms one has $\ell_i\sigma \succ r_i\sigma$ for all $i \leq n$ and for any substitution σ.

For this purpose various abstract ordering structures have been proposed and studied in the literature of term rewriting. Those include the *"recursive path ordering"* of [5], the *"path of subterms ordering"* [25], the *"recursive decomposition ordering"* [11], the *"path ordering"* [16], the *"lexicographic-path ordering"* [15], the *"semantic-path ordering"* [4], etc. However, the size of those orderings was not clear because of the lack of a suitable measure. Also there was no systematic method of generating larger and more general ordering structures, though such orderings are sometimes desirable. For example, one of the main causes of failures of the Knuth-Bendix completion procedure (cf. [10, 17]) (of a given equational system to a convergent rewrite system) is "incomparable terms", which is due to the lack of more general and larger orderings. Also for a termination proof of a rewrite system whose reduction ordering is incompatible with the subterm property, the existing abstract orderings in the literature of term rewriting theory do not work because virtually all of them are in the class of simplification orderings (cf. Dershowitz [4]) which have the subterm property. Here the subterm property is the condition: if s is a subterm of t then $s < t$ for any terms s and t.

The purpose of this section is to link proof theoretic ordinals with the orderings used in rewriting theory. We present a generalized system of Ackermann's ordinals [1] (i.e., a generalized constructive notational system for the Veblen hierarchy of set theoretic ordinals), and elucidate its relationship with the "precedence" orderings used in most implementations of the completion procedure to guarantee termination of systems it generates. (Precedence orderings are orderings on terms induced by an ordering on the operators of the underlying signature.)

* This work was partly supported by the National Science Foundation DCR85-13417. The second author was also partly supported by the Committee on Aid to Research Activity (Concordia University), Fonds pour la Formation de Chercheurs et l'Aide a la Recherche (Quebec) and the Natural Science and Engineering Research Council (Canada).

** This paper is based on a talk by the second author at the Computer Science - Logic Seminar of the Technical University of Munich, July 1987. The author wishes to express his thanks to Profs. Bauer, Brauer, Buchholz and Schwichtenberg for the opportunity.

Using this relationship we can express the size of the different orderings (in rewriting theory) in terms of ordinal numbers. It has sometimes been considered implicitly that the orderings used in rewriting theory are not that large (e.g. less than ϵ_0) and the canonical rewrite systems embeddable into those orderings have the expressive power of a relatively small class of the computational functions (such as the primitive recursive functions or the ϵ_0-ordinal recursive functions). Our results show, on the contrary, that the size of those orderings and hence the expressive power of such systems are much more than expected.

Since proof theory in logic provides various methods of generating larger and more general ordering structures (e.g. Backmann hierarchy, Howard ordinals, Feferman-Schütte ordinal notations, Takeuti's ordinal diagrams) than the Ackermann's ordinals, it is desirable to utilize such methods for term rewriting theory. Some examples of the use of such higher proof theoretic ordinals for termination proof of tree rewritings and term rewritings may be found in [23] and its references. In particular, one can expect the following benefits with more general and stronger orderings:

1. A reduction in frequency of failure of the completion procedure.
2. Termination proofs for a wider range of rewrite systems (particularly those whose reduction ordering is not compatible with the subterm property).
3. More powerful tools for proving termination and related properties of conditional rewrite systems (see §2 below).
4. Provision of stronger orderings on proofs (i.e., orderings of proof-rewriting, instead of term-rewriting) for theoretical analysis of confluence and of completion of term rewrite systems (cf. §2 for proof-rewriting with some term rewrite systems; see also [2]).

Now we introduce Ackermann's system [1] of ordinals based on partial ordered sets, (cf. [19]).

Definition (The set of generalized Ackermann terms $A_n(F, C)$). Let F be a set of operators, C a set of constants. Then

(1) if $c \in C$ then $c \in A_n(F, C)$.

(2) if $\alpha_1, \ldots, \alpha_n \in A_n(F, C)$, $f \in F$, then $f(\alpha_1, \ldots, \alpha_n) \in A_n(F, C)$, and

(3) if $\alpha_1, \ldots, \alpha_m \in A_n(F, C)$, then $\alpha_1 \#\ldots\# \alpha_m \in A_n(F, C)$.

A term of the form $f(\alpha_1, \ldots, \alpha_n)$ or c (for c in C) (as opposed to one of the form $\alpha_1\#\ldots\#\alpha_m$) is called a "connected" term; a term all of whose subterms are connected is called "purely connected"; $A^*(F, C)$ denotes the subset of purely connected terms in A(F, C).

Definition $\langle A_n(F, C), \succ\succ \rangle$ (The Ackermann ordering on $A_n(F, C)$.) Let F and C be well-founded by $<$.

Case 1 If $s, t \in C$, then $s \succ t$ if $s > t$ in C. If $s \in C$, $t \notin C$, then $s \prec t$ holds, but $s \succ t$ does not.

Case 2 Let $s \equiv f(s_1, \ldots, s_n)$, $t \equiv g(t_1, \ldots, t_n)$. Then $s \succ t$

if (1) $s_i \succeq t$ for some i $(1 \le i \le n)$,

or (2) $f > g$, $s \succ t_1, \ldots, s \succ t_n$,

or (3) $f = g$, $s_1 \approx t_1, \ldots, s_{i-1} \approx t_{i-1}, s_i \succ t_i, s \succ t_{i+1}, \ldots, s \succ t_n$, for some i, $1 \le i \le n$,

where $\approx$ means the permutative congruence.

Case 3 Let $s \equiv s_1 \#\ldots\# s_m$, $t \equiv t_1 \#\ldots\# t_\ell$. Then $s \succ t$ iff $\{s_1, \ldots, s_m\} \succ\succ \{t_1, \ldots, t_\ell\}$, where $\succ\succ$ is the multiset ordering induced by $\succ$, in the sense of Dershowitz-Manna [6]. More precisely,

(*) $X = \{s_1, \ldots, s_m\} \succ\succ \{t_1, \ldots, t_\ell\} = Y$ if

$$s_i \succ t_{j1}, t_{j2}, \ldots, t_{jk} \text{ for some i}$$

and

$$X - \{s_i\} \succeq\succeq Y - \{t_{j1}, t_{j2}, \ldots, t_{jk}\}.$$

Remark The ordering on multisets is essentially the same as the ordering of natural sums $\alpha_1\#\ldots\#\alpha_n$ for additive principal ordinal numbers α_i.

$A_n(F, C)$ is well-founded by $\succ$. If F and C are totally ordered by $\succ$ (hence well-orderings), $A_n(F, C)$ is also totally ordered, hence well ordered by $\succ$.

The above definition is essentially due to Ackermann [1], though he only considered the total order case, and only described A_3 explicitly. $A_2(\{0\}, \{0\})$ is the Feferman-Schütte system (cf. [29]) of ordinal notations less than Γ_0.

Theorem The multiset extension of the recursive path ordering Dershowitz [5] over $T(F \cup C)$ is the same as $A_1(F,C)$.

In other words, if we consider the connected terms of $A_1(F, C)$, the generalized Ackermann ordering is the same as the recursive path ordering, with a term $f(t_1, \ldots, t_m)$ in $T(F \cup C)$ interpreted as the connected term $f(t_1\#\ldots\#t_m)$ in $A_1(F, C)$.

In rewriting theory, one is mainly interested in finite sets F and C, because one usually deals only with finite rewrite systems. For any finite C and totally ordered F of cardinality n, the order type of $A_1(F, C)$ is $\varphi_n 0$ (of Feferman-Schütte's system [29]). From this, and the fact that the different precedence-based orderings share the same structure as the recursive path ordering for the same total ordering $\langle F \cup C; \prec \rangle$ (cf. Rusinowitch [27]), we have

Theorem The path of subterms ordering (Plaisted [25]), recursive path ordering (Dershowitz [5]), recursive decomposition ordering (Jouannaud-Lescanne-Reinig [11]), and path ordering (Kapur-Narendran-Sivakumar [16]), are of order type up to $\varphi_\omega 0$. In particular, for n distinct operators, the order type is bounded by $\varphi_n 0$.

The well-foundedness of these orderings is provable in the system of Implication-free Inductive Definition defined in Okada [22] §3, which is a subsystem of the usual system of (non-iterated) Inductive Definition, hence a subsystem of the second order arithmetic. Actually, the critical ordinal (i.e., the first unprovable ordinal) of this system is $\varphi_\omega 0$.

Theorem The recursive path ordering, extended to allow arbitrary terms as operators (as in [4]), is of order type Γ_0.

Now we extend the Ackermann ordering of $A_n(F, C)$ to one of $A_\omega(F, C)$. The set $A_\omega(F, C)$ of Ackermann terms is defined in the same way as $A_n(F, C)$, except that for each $f \in F$, f may have an unbounded, finite number of argument. In other words, we have terms $f(\alpha_1, ..., \alpha_m)$ for any m. The Ackermann ordering $\succ_r$ for $A_\omega(F, C)$ is defined in the same way as before, where when we compare $f(\alpha_1, ..., \alpha_n)$ with $g(\beta_1, ..., \beta_m)$ for $n < m$, we re-interpret $f(\alpha_1, ..., \alpha_n)$ as $f(\underbrace{0, ..., 0}_{m-n}, \alpha_1, ..., \alpha_n)$, then follow the definition before. $\succ_\ell$ is the same as $\succ_r$ but we re-interpret $f(\alpha_1, ..., \alpha_n)$ as $f(\alpha_1, ..., \alpha_n, 0, ..., 0)$. Here 0 is a minimal element of C.

$A^*_\omega(F, C)$ is defined in the same way as before, i.e., the set of purely connected terms.

The system $\langle A_\omega(\{0\}, \{0\}), \succ \rangle$ is essentially the same as the Schütte ordinals of §11 in [28].

Theorem The lexicographic path ordering (Kamin-Levy [15] over $T(F \cup C)$ is the same as $\langle A^*_\omega(F, C), \succ_\ell \rangle$.

Theorem Lescanne's ordering (Lescanne [18]) (which is obtained by combining the lexicographic ordering with the recursive path ordering) over $T(F \cup C)$ is the same as $\langle A_\omega(F, C), \succ_\ell \rangle$.

We note the following: $\langle A^*_\omega(F, C), \succ_\ell \rangle$ is not well-founded even for singleton F and C. However, $\langle A^*_n(F, C), \succ_\ell \rangle$ is well-founded for every n provided F and C are. In other words, the lexicographic path ordering is only well-founded when the number of arguments to each f is bounded. Also, $\langle A^*_n(F, C), \succ_\ell \rangle$ has the same order type as $\langle A_n(F, C), \succ_\ell \rangle$ for all $n \geq 3$ provided F and C are well-ordered, while $\langle A^*_2(F, C), \succ_r \rangle$ for any finite sets F, C has the order type ϵ_0.

We next relate Ackermann's ordering with special cases of the "semantic path ordering" of Plaisted [personal communication] and Kamin-Levy [15]. The following is the quasi-order version of the semantic path ordering.

Definition. (The semantic path ordering) Let $\succeq$ be a quasi ordering on $A_n(F, C)$.

Case 2. Let $s = f(s_1, ..., s_n)$ and $t = g(t_1, ..., t_n)$. Then $s \geq_{spo} t$ if

(1) $s_i \geq_{spo} t$ for some i $(1 \leq i \leq n)$, or

(2) $s \succ t$ and $s >_{spo} t_j$ for all j $(1 \leq j \leq n)$, or

(3) $s \approx t$ and $\{s_1, ..., s_n\} \geq\geq_{spo} \{t_1, ..., t_n\}$.

Case 1 and Case 3 are the same as those in the definition of the Ackermann's ordering.

Consider the following three orderings.

(1) $f(s_1, ..., s_n) <_0 g(t_1, ..., t_n)$ on $A_n(F, C)$ iff $f < g$ in the precedence F.

(2) $f(s_1 \#...\# s_n) <_1 g(t_1 \#...\# t_m)$ on $A_1(F, C)$ iff

(i) $f < g$ in F, or

(ii) $f = g$ and $\{s_1, ..., s_n\} \leq\leq_{spo} \{t_1, ..., t_m\}$, where $\leq\leq_{spo}$ is the multiset extension of $\leq_{spo}$.

(3) $f(s_1, ..., s_n) <_{lex} g(t_1, ..., t_m)$ on $A_n(F, C)$ iff

(i) $f < g$ in F, or

(ii) $f = g$, $s_1 = t_1, ..., s_{i-1} = t_{i-1}$, $s_i <_{spo} t_i$, for some i $(1 \leq i \leq n)$, or

(iii) $f = g$, $s_1 = t_1, ..., s_n = t_n$, $n < m$.

Theorem.

(1) If we take $<_0$ for $\prec$, then $<_{spo}$ on $A^*_\omega(F, C)$ is the same as the recursive path ordering on $A_1(F, C)$.

(2) If we take $<_1$ for $\prec$, then $<_{spo}$ on $A_1(F, C)$ is the same as the recursive path ordering on $A_1(F, C)$.

(3) If we take $<_{lex}$ for $\prec$, then

(i) $<_{spo}$ on $A_\omega(F, C)$ is the same as the Ackermann ordering; therefore

(ii) $<_{spo}$ on $A^*_\omega(F, C)$ is the same as the lexicographic path ordering, and

(iii) $<_{spo}$ on $A_1(F, C)$ is the same as the recursive path ordering.

2 PROOF-NORMALIZATION AND REWRITE SYSTEMS

In this section, we first outline the correspondence between the paradigm of traditional proof theory and the paradigm of the "proof ordering" method (cf. Bachmair-Dershowitz-Hsiang [2]) used for analyzing "completion procedures" for (unconditional) rewrite systems (like the one in Knuth-Bendix [17]). Next we will show how the same paradigm can be applied to the theory of conditional rewriting.

Unless otherwise stated, rewrite systems are presumed to be terminating, i.e., their reduction ordering (the transitive closure of the rewrite relation) embeds in some well-founded structure. As discussed in the previous section, in most cases termination is established by embedding the given rewrite system in a segment of the generalized Ackermann ordinals.

Traditional proof theory is concerned with reduction procedures that transforms a given proof into a "normal proof". For that purpose, the following steps are employed:

(1) Assign a (proof-theoretic) ordinal to each proof.
(2) Define a "maximal formula" or an "essential cut" of a proof. (A proof without maximal formula or essential cut is called a "normal proof".)
(3) Define a reduction step which reduces one "maximal formula" or "essential cut".
(4) State a lemma, called the "existence lemma", showing theexistence of a reduction under certain circumstances.
(5) Show that each reduction step decreases the ordinal of the proof.

The simplest application of this paradigm in rewrite theory is in proving that a rewrite system has the Church-Rosser property (hence provides a decision procedure for the underlying word problem) if every critical pair (in the sense of Knuth-Bendix [17]) is "joinable", i.e. both terms in the pair rewrite to the identical terms.

Below, $s = t$ stands for the usual sense of equality in equatinal systems; $s \to t$ stands for one-step rewrite in a rewrite system; $s \to^* t$ is a reflexive-transitive closure of one-step rewriting; $s{\downarrow}t$ stands for the joinability relation, i.e. $s \to^* u \ ^*\!\leftarrow t$ for some u; $s =^* t$ means that there exist $u_1, \ldots, u_n$ such that $s{\downarrow}u_1{\downarrow}\ldots{\downarrow}u_n{\downarrow}t$.

$s =^* t$ in a rewrite system if and only if $s = t$ in the underlying equational system (considering every rule to be an equation). Actually, a switch of the direction of one rewrite $\to$ of a proof $s =^* t$ in a rewrite system corresponds to one use of the symmetric axiom for a proof of $s = t$ in the underlying equational system.

A proof of the form $s =^* t$ is called an equational proof. A proof of the form $s{\downarrow}t$ is called a normal proof. Transforming a proof P of the form $s =^* t$ to a proof P' of normal form $s{\downarrow}t$ is called "normalization". If every proof of the form $s =^* t$ is normalizable, the system is said to have the Church-Rosser property.

We are interested, then, in proving a theorem of the following form.

Normalization Theorem

For any equational proof, by successive reductions (regardless of choice of maximal term (peak)), one can reach a normal proof.

To achieve this, we need the following five steps:

(1) Ordinal assignment for proofs

The ordinal for an equational proof P is the multiset of terms occurring in P. Hence, if α is the order type of the reduction ordering, then proofs are assigned ordinals less than ω^α. (See Section 1 for the definition of the ordering on multisets.) E.g., if P is of the form $s_1 \to s_2 \leftarrow s_3 \to s_4 \to s_5 \leftarrow s_6$, then the multiset $\{s_1, s_2, \ldots, s_6\}$ is the ordinal of P.

(2) Maximal term

A "peak" or a "maximal term" in a rewrite proof is an occurrence of a term t in the form $s \leftarrow t \to u$.

(3) Reduction step

By a reduction of an equational proof we mean a replacement of a sub-proof of the form $s \leftarrow t \to u$ for a peak t by a sub-proof of the form $s \to^* v \ ^*\!\leftarrow t$ for some v (i.e., $s{\downarrow}t$) in the proof.

(4) Existence lemma

If every critical pair is joinable, every non-normal proof allows at least one reduction.

(A critical pair is a special kind of peak. A finite rewrite system has only a finite number of critical pairs.)

(5) Lemma (Decreasing Lemma)

For each reduction step, the ordinal of the proof decreases.

In proof theory, the system under consideration is fixed; hence the restriction in the Existence Lemma is also fixed. In rewrite theory, on the other hand, the system is dynamic; for this reason, completion procedures constantly generate new equational consequences to satisfy the requirements of the Existence Lemma. Completion typically includes the deletion of rules from the system under construction; this requires somewhat more subtle ordering assignments (cf. Bachmair et al [2]).

Our purpose in the remainder of this section is to show how this same paradigm applies to the theory of conditional rewriting. By a "conditional equational system", we mean a set of Horn clauses of the form

$$s_1 = t_1 \wedge \ldots \wedge s_n = t_n \Rightarrow \ell = r$$

A "standard conditional rewrite system" is a rewrite system whose rules are of the form

$$s_1{\downarrow}t_1, \ldots, s_n{\downarrow}t_n : \ell \to r$$

A "natural conditional" rewrite system is a rewrite system whose rules are of the form

$$s_1 =^* t_1, \ldots, s_n =^* t_n : \ell \to r$$

Table 1 COMPARISON OF SIMPLE EXAMPLES OF NORMALIZATION PARADIGM IN PROOF THEORY AND TERM REWRITING THEORY

	Peano Arithmetic (Gentzen)	Unconditional Rewrite System
ordinal assignment	ordinals less than ϵ_0	multiset extension of reduction ordering
maximal element	essential cut (maximal formula)	ordering peak (maximal term)
existence lemma	holds for proofs of Σ^0_1-formulae	holds if every critical pair is joinable

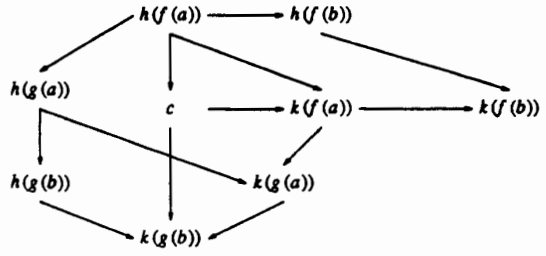
It is easily seen that if a conditional or natural conditional rewrite system R is convergent (or "canonical", i.e., has the termination and Church-Rosser properties) then it is equivalent to the corresponding equational system E, i.e., s↓t in R if and only if s = t in E. It is also easily seen that for any natural, not necessarily convergent, conditional rewrite system R and the corresponding equational system E, s $=^*$ t in R if and only if s = t in E. We follow the usual definitions of basic notions (including a "critical pair") for conditional rewrite theory (cf. [3, 7]).

However, first we remark that the condition for the existence lemma should be modified for standard conditional rewrite systems. Actually, if we keep the same condition, i.e., "every critical pair is joinable", then the existence lemma does not hold. In other words, the Critical Pair Lemma of Knuth-Bendix [17] and Huet [9] does not carry over to standard conditional systems, as can be seen from the following counter-example.

Counter-example (A):

h(f(a)) → c
h(x) → k(x)
c → k(f(a))
a → b
c → k(g(b))
k(g(b))↓h(f(x)) : f(x) → g(x)

Here a peak k(g(a)) ← k(f(a)) → k(f(b)) allows no reduction. On the other hand, as easily seen, every critical pair is joinable. (See [8] for further discussion on the counter-example.)



Hence our aim is to provide suitable additional conditions for the existence lemma. Here we give two such examples. The first one is a generalization of Bergstra-Klop's result [3]; the second one is concerned with a generalization of Kaplan's simplification systems [13] and of Jouannaud-Waldmann's reductive system [12].

Definition (depth of a proof)

(1) The depth of a proof of s→t is 0 if s→t is the result of an application of an unconditional rule.
(2) The depth of a proof of s → t is one more than the maximum depth of subproofs for conditions $u_1\downarrow v_1$, ..., $u_n\downarrow v_n$ if s→t is the result of an application of a conditional rule which has a substitution instance of the form $u_1\downarrow v_1$, ..., $u_n\downarrow v_n$: $\ell \to r$.
(3) The depth of a proof of $s \to s_1 \to s_2 \to \dots \to s_m \to v \leftarrow t_n \leftarrow t_1 \leftarrow t$ is the maximum depth of subproofs for $s \to s_1$, $s_1 \to s_2$, ..., $s_m \to v$, $t_n \to v$, ..., $t_1 \to t_2$, $t \to t_1$.

Definition For a critical pair (s, t) and overlap u of the form s ← u → t such that u → s has depth n and u → t has depth m, the critical pair is "shallow joinable" if there exists a term v such that t $\to^*$ v is provable with depth less than or equal to n and s $\to^*$ v is provable with depth less than or equal to m.

For a normal form (i.e., irreducible term) N and a term s, a condition of the form s↓N is called a "normal condition" ora "Bergstra-Klop condition". A conditional rewrite system in which every conditional rule is of the form $s_1\downarrow N_1$, ..., $s_n\downarrow N_n$: $\ell \to r$, for normal conditions $s_i\downarrow N_i$, is called a "normal conditional system".

Normal conditional systems were introduced by Bergstra-Klop [3]. First we consider extensions of the following Theorem in Bergstra-Klop [3]. A "left-linear" system is a system in which a left-hand side ℓ of a rule C : $\ell \to r$ allows only one occurrence for any variable.

Bergstra-Klop's Theorem [3]. For every left-linear (not necessarily terminating) normal conditional system with no critical pair, every proof is normalizable.

We can relax the "no critical pair" condition of Bergstra-Klop, at the expense of insisting on termination, as follows.

Existence Lemma For any left-linear normal conditional system, if every critical pair is shallow joinable then every non-normal proof has a reduction.

The Existence Lemma is obtained via the following lemma.

Substitution Lemma If $N\downarrow r(s)$ is provable with depth n, and if $s \rightarrow t$ is provable, then $N\downarrow r(t)$ is also provable with depth at most n, where N is an irreducible term.

The proof is carried out by double induction on (n+m, r(s)), where m is the depth for $s \rightarrow t$. (See [8] for details.)

Theorem For any left-linear normal conditional system, if every critical pair is shallow joinable then every proof of this system is normalizable. Hence such a system has the Church-Rosser property.

Here we can take the same (multiset) ordinal assignment for unconditional systems.

Next we consider an alternative restriction to give an existence lemma. By the reduction ordering, we mean the transitive closure of finite reductions in a given system.

A conditional system is called a "decreasing" system if there exists a well-founded extension $<$ of the reduction ordering which satisfies the following properties:

(1) For each conditional rule of the form $s_1\downarrow t_1, \ldots, s_n\downarrow t_n : \ell \rightarrow r$, $s_i\sigma < \ell\sigma$ and $t_i\sigma < \ell\sigma$ for all i ($1 \leq i \leq n$) and for all substitutions σ.

(2) $<$ has the subterm property, i.e., if s is a proper subterm of t then $s < t$.

Then a decreasing system has the following properties:

1. the system is terminating
2. the basic notions are decidable, i.e., for any terms s and t, one step reduction $s \rightarrow t$, a finite reduction $s \rightarrow^* t$, $s\downarrow t$, "s is a normal form" are all decidable.

We can readily see that Kapaln's simplification systems [13] and Jouannaud-Waldmann's reductive systems [12] are special cases of our decreasing systems.

The following "critical pair" lemma can be proved by essentially the same argument as used by the above authors.

Existence Lemma

For any decreasing system, if every critical pair is joinable then every non-normal proof allows a reduction.

It should be remarked that the existence lemma does not hold in general if we omit the second condition, the "sub-term property", in our definition of decreasing systems. In particular, counter-example (A) above satisfies all the properties of decreasing systems, except for the subterm property.

Now we show this. For this purpose, we utilize systems of proof theoretic ordinals in logic, which provide various well-founded orderings without the sub-term property. Here we actually consider an embedding of our counter-example into Takeuti's system O(2, 1) of ordinal diagrams, which is one of the two major systems of proof theoretic ordinals.

The reduction ordering of this system is embeddable into the ordering $<_\infty$ in O(2, 1) (see eg. Okada [20] or Okada-Takeuti [21] for the definitions $<_\infty$ and O(2, 1)), by the following embedding o:

o(h(t)) = (0, o(t)#2)
o(f(t)) = (1, o(t))
o(c) = (0, (1, 1)#1)
o(k(t)) = (0, o(t))
o(a) = 1
o(b) = 0
o(g(t)) = (0, o(t))

Also, $<_\infty$ satisfies the additional condition for the decreasingness, i.e., each condition term d and h(f(x)) is less than the left-hand side f(x) of the last rule in the sense of $<_\infty$.

If we consider a decreasing system in which every critical pair is joinable, then the same proof for the Normalization Theorem holds, as before. Moreover, with a decreasing system, we can extend the Normalization and Church-Rosser properties further. We introduce a stronger form of Normalization and the Church-Rosser properties to analyze conditional rewrite systems.

1. By a "fully normal" proof of $s =^* t$ in a given natural conditional system, we mean a normal proof $s\downarrow t$ such that every subproof $s_i\sigma =^* t_i\sigma$ used in establishing the conditions needed for $s\downarrow t$ is fully normal.
2. If for a given proof P of $s =^* t$ in a natural conditional system R there is a fully normal proof P' (of $s\downarrow t$) in R, we say the proof P is fully normalizable. If every proof (of the form $s =^* t$) is fully normalizable, the system is said to have the "strong" Church-Rosser property.

A decreasing natural system is a natural conditional system which satisfies all the above conditions for a decreasing system.

Theorem (Full Normalization Theorem cf. [24])

For any decreasing natural system, if every critical pair is joinable, then every proof is fully normalizable. Hence such a system has the strong Church-Rosser property.

The full normalization is carried out by successive normalizations from the surface proof to the deepest levels. More precisely, first we normalize the surface proof of $s =^* t$ to a normal form $s\downarrow t$ in the given natural system. Then we consider the immediate conditions $c_1 =^* d_1, \ldots,$

$c_n =^* d_n$ used for the proof $s \downarrow t$, and normalize the surface proof of each of those to $c_i \downarrow d_i$. We repeat this process. Each normalization procedure is exactly the same as the case for unconditional systems before: For the ordinal assignment of a given conditional proof, we use the multiset of terms occurring in the surface proof. We use the following Existence Lemma for a natural conditional system.

Existence Lemma For any (not necessarily decreasing) natural conditional system, if critical pair is joinable, then every surface proof which is not normal allows a reduction.

It should be remarked that the above successive normalization processes stop in finite steps because of the decreasingness property (1).

The following corollary is a direct consequence of the Full Normalization Theorem.

Corollary If a decreasing natural conditional system (with conditions of the form $s =^* t$) is convergent (canonical), then the corresponding standard conditional system (with conditions of the form $s \downarrow t$) is also a convergent (canonical) decreasing system.

It should also be remarked that the converse of this corollary is obvious for general case, i.e., if a standard conditional system is convergent then the corresponding natural conditional system is also convergent (without any assumption of decreasingness).

Further techniques for full normalization of conditional equational proofs are studied in [24].

REFERENCES

[1] Ackermann, W., "Konstruktiver Aufbau eines Abschnitts der zweiten Cantorischen Zahlenklasse," Math. Z. 53, 403-413, 1951.

[2] Bachmair, L., N. Dershowitz and J. Hsiang, "Orderings for equational proofs," Proceedings of the Symposium on Logic in Computer Science, Cambridge, MA, 346-357, June 1986.

[3] Bergstra, J. A. and W. Klop, "Conditional rewrite rules: Confluence and termination", Report IW 198/82 MEI, Mathematische Centrum, Amsterdam, 1982.

[4] Dershowitz, N., "Termination of rewriting," Report 85-1220, Department of Computer Science, University of Illinois, Urbana, 1985; the revised version is in Journal of Symbolic Computation 3, 69-116, 1987.

[5] Dershowitz, N., "A note on simplification orderings," Inf. Proc. Lett. 9, 212-215, 1979.

[6] Dershowitz, N. and Z. Manna, "Proving termination with multiset orderings," Commun. ACM 22, 465-476, 1979.

[7] Dershowitz, N. and D. A. Plaisted, "Equational programming," in Machine Intelligence 11, 1987.

[8] Dershowitz, N., M. Okada and G. Sivakumar, "Confluence of conditional term rewriting systems," Proceedings of Workshop on Conditional Rewrite Systems, Orsay, France, July 1987, Springer Lecture Notes in Computer Science, to appear.

[9] Huet, G., "Confluent reductions: Abstract properties and applications to term rewriting systems," J. Assoc. Comp. Mach. 27, 797-821, 1980. (Previous version in Proceedings of the Symposium on Foundations of Computer Science, Providence, RI, 30-45, (October 1977).)

[10] Huet, G. and D. C. Oppen, "Equations and rewrite rules: A survey," in Formal Language Theory: Perspectives and Open Problems, ed. R. Book, Academic Press, New York, 349-405, 1980.

[11] Jouannaud, J.-P., P. Lescanne and F. Reinig, "Recursive decomposition ordering," Proceedings of the Second IFIP Workshop on Formal Description of Programming Concepts, Garmisch-Partenkirchen, West Germany, 331-348, 1982.

[12] Jouannaud, J. P. and B. Waldmann, "Reductive conditional term rewriting systems," Proc. of the Third IFIP Working Conference on Formal Description of Programming Concepts, 1986.

[13] Kaplan, S. "Conditional rewrite rules," Theoretical Computer Science 33, 175-193, 1984.

[14] Kaplan, S., "Fair conditional term rewritingsystems: Unification, termination and confluency," Laboratoire de Recherche en Informatique, Université de Paris-Sud, Orsay, France, November 1984.

[15] Kamin, S. and J.-J. Lévy, "Two generalizations of the recursive path ordering," Unpublished note, Department of Computer Science, University of Illinois, Urbana, IL, 1980.

[16] Kapur, D., P. Narendran and G. Sivakumar, "A path ordering for proving termination of term rewriting systems," Proceedings of the Tenth Colloquium on Trees in Algebra and Programming, Berlin, West Germany, Springer Lec. Notes Comp. Sci., 185, 173-185, 1985.

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

[18] Lescanne, P., "Uniform termination of term-rewriting systems: Recursive decomposition ordering with status," Proceedings of the Ninth Colloquium on Trees in Algebra and Programming, 181-194, Bordeaux, France. Cambridge: Cambridge University Press, 1984.

[19] Okada, M., "Ordering structures of term rewriting theory and theory of proof theoretic ordinals," Report 86 SF 20-1, Information Processing Society of Japan, 1-8, 1987.

[20] Okada, M., "A simple relationship between Buchholz's new system of ordinal notations and Takeuti's system of ordinal diagrams," Journal of Symbolic Logic 52, 577-581, 1987.

[21] Okada, M. and G. Takeuti, "On the theory of quasi-ordinal diagrams," in Logic and Combinatorics, ed. S. Simpson, Contemporary Mathematics 65, 295-308, 1987.

[22] Okada, M., "A theory of weak implications," Journal of Symbolic Logic 53, No. 1, 1988. To appear.

[23] Okada, M., "Note on a proof of the extended Paris-Kirby game for labeled finite trees," European Journal of Combinatorics, to appear, 1988.

[24] Okada, M., "A logical analysis for the theory of conditional rewriting," Proceedings of Workshop on Conditional Rewrite Systems, Orsay, France, July 1987, Springer Lecture Notes in Computer Science, to appear.

[25] Plaisted, D. A., "A recursively defined ordering for proving termination of term rewriting systems,"

Report R-78-943, Department of Computer Science, University of Illinois, Urbana, IL, 1978b.
[26] Remy, J.-L. and H. Zhang, "Reveur 4: a system for validating conditional algebraic specifications of abstract data types," Report 54506, Centre de Recherche en Informatique de Nancy, France, 1984.
[27] Rusinowitch, M., "Plaisted ordering and recursive decomposition ordering revisited," Proc. Conference on Rewrite Techniques and Application, Dijion, 1985.
[28] Schütte, K., Beweistheorie, Springer, 1960.
[29] Schütte, K., Proof Theory, Springer, 1978.
[30] Zhang, H. and J. L. Remy, "Contextual rewriting," Proceedings of First International Conference on Rewriting Techniques and Applications, Dijon, France (May 1985), Lecture Notes in Computer Science 202, Springer, Berlin, 46-62, 1985.