Diss. ETH Nr. 8070

Equational Completion by Proof Transformation

WOLFGANG KÜCHLIN

SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZÜRICH

Zürich 1986

Equational Completion by Proof Simplification

Wolfgang Küchlin

ETH Mathematics
Report No. 86-02
May 1986

Abstract: We extend Buchberger's generalization of Newman's Diamond Lemma to rewrite relations modulo equations. Lifting this result to an efficient test on superpositions, we obtain an abstract framework for confluence criteria based on subconnectedness. An efficient specialization of the abstract test yields an improved version of the completion algorithm of Jouannaud and Kirchner, which now enforces the more general subconnectedness modulo E instead of local E-confluence. Rule-deletions and other intermediate reductions are succinctly justified by showing that reducible rules can only produce subconnected critical pairs. We offer a new view of Jouannaud's multiset induction technique in the form of Noetherian induction on equational proofs, which provides a well-structured completeness proof of our completion algorithm. As further applications of our method, we develop a subsumption criterion for resolution theorem proving, and a criterion for ground confluence of term-rewriting systems.

Acknowledgements

This is a reprint of my doctoral thesis (ETH Diss. # 8070), submitted to the Swiss Federal Institute of Technology (ETH) under the title "Equational Completion by Proof Transformation". I am indebted to Prof. Erwin Engeler for supervising it, and for providing an environment in which it could grow. Prof. Rüdiger Loos got me started in this area of research and was willing to serve as co-examiner. My colleagues of the Mathematical Institute helped through numerous discussions; I am especially grateful for the many counterexamples provided by Ronny Peikert, and for the mathematical advice of Gerhard Jäger. At various stages of the work Profs. Jieh Hsiang and Bruno Buchberger helped through discussions, suggestions, and, most importantly, through encouragement from outside. Norbert Eisinger's comments substantially corrected the proof of the subsumption criterion and improved its presentation. Hands-on experience with AC-completion was only possible through the help of the EUREKA group at CRIN, especially Prof. Jean-Pierre Jouannaud and Jalel Mzali.

Table of Contents

Summary

We study improvements of the Knuth-Bendix Completion Algorithm, a proof-procedure for the validity problem in equational varieties presented by a finite set *A* of equations. Our aim is twofold: First, we identify the KB Completion Algorithm as an instance of a transformation process on equational proofs. This yields a characterization of the output of completion as a fixedpoint of proof-transformation, and facilitates a simple and intuitive proof of correctness. Second, we present effective criteria to determine if a critical pair computed by the KB Algorithm is unnecessary for completion. Essentially, the criteria predict whether the proof-transformation exercised by the pair will eventually be accomplished implicitly through different critical pairs.

We treat the general case of completion modulo a subset *E* of *A* with finite equivalence classes, using Jouannaud and Kirchner's variant of the completion algorithm as a basis. For our theoretical developments, we construct a well-founded ordering on equational proofs modulo *E* which embeds the transformation process, and which for our correctness arguments facilitates the use of Noetherian induction on entire equational proofs as opposed to rewrite relations. For practical applications, we propose a specialization of the abstract algorithm and we discuss various refinements, based on some empirical results. The suggestions of Winkler and of Kapur et al. for confluence criteria also fall into our framework as (different) special cases. As theoretical applications, we develop a specific ground confluence criterion for inductive completion, and a subsumption criterion for resolution theorem proving.

Zusammenfassung

Wir untersuchen Verbesserungen des Knuth-Bendix Vervollständigungsalgorithmus, einem Beweisverfahren für das Gültigkeitsproblem in Varietäten, die durch eine endliche Menge *A* von Gleichungen präsentiert sind. Wir verfolgen zwei Hauptzielsetzungen: Zum einen identifizieren wir den KB-Vervollständigungsalgorithmus als ein spezielles Transformationsverfahren für Beweisketten in Gleichungstheorien. Daraus ergibt sich die Charakterisierung des Ergebnisses einer Vervollständigung als ein Fixpunkt der Beweistransformation und somit ein vergleichsweise einfacher und einsichtiger Korrektheitsbeweis des Verfahrens. Zum anderen präsentieren wir effektive Kriterien zur Feststellung, ob ein vom KB-Algorithmus erzeugtes kritisches Paar für die Vervollständigung unnötig ist. Dabei sagen die Kriterien im wesentlichen voraus, ob die durch das Paar bewerkstelligte Beweistransformation letztlich auch implizit durch andere kritische Paare erreicht wird.

Wir behandeln hier den allgemeinen Fall der Vervollständigung modulo einer Teilmenge *E* von *A* mit endlichen Äquivalenzklassen, und wir benützen den Vervollständigungsalgorithmus in einer Variante von Jouannaud und Kirchner als Basis. Für unsere theoretischen Entwicklungen konstruieren wir eine wohlfundierte Ordnung auf gleichungserzeugten Beweisketten modulo *E*, in die der Transformationsprozess eingebettet ist, und die Noether'sche Induktion direkt auf ganzen Beweisketten statt nur auf Reduktionsrelationen zulässt. Für die Anwendung in der Praxis schlagen wir, basierend auf einigen empirischen Ergebnissen, eine Spezialisierung des abstrakten Algorithmus vor, und wir diskutieren verschiedene mögliche Verfeinerungen. Die Vorschläge von Winkler und von Kapur et al. für Konfluenzkriterien stellen innerhalb unseres abstrakten Rahmens andere Spezialfälle dar. Als Anwendungen theoretischer Natur entwickeln wir schliesslich ein Kriterium das spezifisch die Grundkonfluenz eines kritischen Paares testet und bei induktiver Vervollständigung eingesetzt werden kann, und des weiteren ein Subsumptionskriterium für Resolutionsbeweiser.

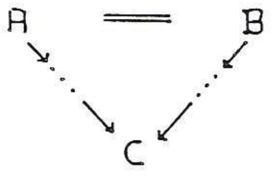
1 Introduction

1.1 Background

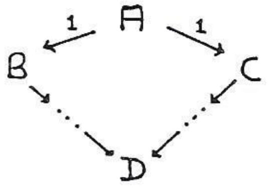
As a general framework, we are interested in theorem proving in equational varieties; i.e., we are presented with a finite set A of equations (axioms) between expressions (terms) in a universal algebra T, and we want to know whether some equality A = B holds true under A. The importance of such axiom-systems and the associated question of validity is evident from modern Algebra. From a Computer Science point of view, computability theory tells us that every computable function has a denotation as a finite set of equations. Therefore, equations provide a language that is general enough for the formulation of many interesting problems. Term equations have been used e.g. for software specification in the theory of algebraic abstract data types [G&H&M 78] and for the formulation of consistency problems in relational data-bases [Co&Ka 85]; there is also a natural "equational view" of first-order predicate logic and the proof procedure of resolution [Hs&De 83] [Pa 85], including the Prolog programming language [De&Jo 84]. [Hu&Op 80] gives a survey in a terminology that has become a virtual standard, and to which we shall adhere with minor variations.

The validity problem in equational varieties is of course undecidable in general, with the word problem in finitely presented groups being a special case. Intuitively speaking, the problem here is that the two sides of an equation may have different complexities, and each step in an equational proof can either increase or decrease the complexity of an intermediate result. Owing to the simultaneous presence of complexity increasing and decreasing derivation steps in general, there can be no upper bound on the complexity of intermediate results, and hence no way of telling when to abort some fruitless search for a proof.

In 1941, M. H. A. Newman [Ne 42] identified this as a recurring problem in, e.g., the theory of free groups, Church's λ-calculus, and combinatorial topology; we may add combinatory calculus and Chomsky-0 grammars to his list. In all these theories, some search space of theorems is given by a finite number of axioms together with two kinds of derivation rules or "moves" in Newman's terms, an undesirable, "negative", one that increases, and a desirable, "positive", one that decreases complexity. Newman's positive moves are what we now call *reductions*. Especially for an automated treatment of such theories it is desirable to know whether each theorem can be derived by a sequence of reductions only, i.e. whether for any equality A = B there is a common term C to which both A and B may be reduced. Newman went on to give an important characterization of this *Church-Rosser* or *confluence* property: a theory in which positive moves are embedded in a well-founded partial ordering > (i.e. sequences of reductions always terminate) is Church-Rosser iff it is locally confluent; where *local confluence* is the property that, for each B, C, derived by single positive moves from some common A, they can be further reduced to a common D (by an arbitrary number of positive moves).



a) Church-Rosser property



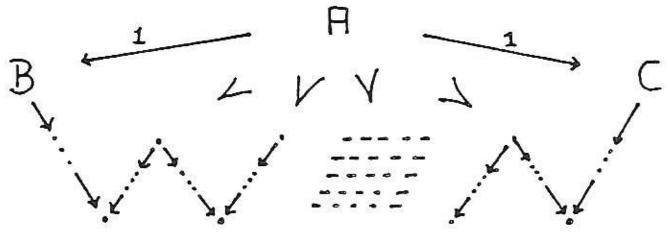
b) local confluence

In 1967, D. E. Knuth showed [Kn&Be 70] that for equational theories defined by a finite set of axioms over the usual term-algebras, Newman's local confluence can be "lifted" to a "most general" condition on the defining axioms alone (in contrast to the generated reduction relation), and is therefore decidable. Axiom systems whose associated reduction relation is Church-Rosser are called *complete*, because the reductions contain all information about the theory. Most importantly, Knuth developed a *completion process* which deals with the usual situation of incomplete reductions: it gradually enhances the basis of known facts in the search space by controlled application of negative moves until a theorem is provable from the augmented basis of facts by positive moves alone. This derivation process is called *complete*, if each valid theorem in the search space can be detected in finite time. Moreover, in the rare cases in which the process terminates it yields a complete basis of facts from which all other facts in the search space can be derived by reductions alone without further completion steps. If sequences of reductions are guaranteed to terminate, we then have a decision procedure for our theory by Newman's lemma.

1.2 Completion of Term-Rewriting Systems

Rephrased in the classical environment of free term-algebras, the Knuth-Bendix (KB-) completion procedure transforms a set A of term equations into a finitely and uniquely terminating set R of rewrite-rules with equal theorem-proving power. (Though it may not terminate it is usually still called an algorithm.) In general, many more rules are needed than there were equations, to make good the loss of computational power incurred by restricting the use of equations to one-sided application. At each iteration of the procedure, candidates for new rules are systematically computed as "critical pairs", which reflect most general situations where the local confluence property of R may be impaired; only those pairs must actually become rules that cannot yet be reduced to a common normal form. The method constitutes a semi-decision procedure for equality under A, viz. for any valid equality A = B it will eventually produce a rewrite system R which can prove A = B by mere reduction of A and B to a common normal form; if completion terminates, the final term-rewriting system alone is good for deciding each such equality in A (i.e. it has the Church-Rosser property).

In [Bu 84], Buchberger presented a generalization of the interesting direction of Newman's Lemma that allows to test for the more general *local pseudo-confluence* property instead of local confluence when showing that a rewrite system is Church-Rosser.



c) local pseudo-confluence

Although it was derived and proved in a different way (see [Bu 79], [Ba&Bu 80], [Wi&Bu 83]), pseudo-confluence (also called *subconnectedness*) is best explained in the light of the technique of multiset induction developed in [Jo&Ki 84]. The reduction ordering on terms induces via its multiset extension an ordering on equational proofs in which the purely reductional proofs are the least (simplest) elements. Pseudo confluence now demands that for each (minimal) equational proof containing a negative move there is also an alternative proof which is simpler. Thus enforcing the pseudo-confluence property amounts to performing a transformation process on equational proofs which replaces proofs by simpler proofs until purely reductional proofs are found. The completion procedure halts as soon as it detects a fixpoint of the transformation, which, by its very definition, enjoys the Church-Rosser property.

Thus, pseudo-confluence suggests itself as the natural property to enforce during completion. The only snag lies in the construction of this simpler equational proof, because it was our very problem in the beginning that we could not deal with proofs containing negative moves; when we restrict ourselves to finding proofs with only positive moves, we get the traditional local confluence as a special case of pseudo-confluence. Furthermore, for axiom-systems on free term-algebras, pseudo- confluence must be lifted to a condition on axioms, i.e. we need again a kind of Knuth-Bendix theorem. The first partial solution to this was found in 1983 by Winkler [Wi 83], who developed a sufficient criterion for subconnectedness, which was however difficult to handle in practice. Winkler's proposal was generalized and simplified in [Kü 85] and [Wi 85] to a sufficient criterion which is even necessary if $>$ is the reduction relation itself. Furthermore, practicality of completion for pseudo-confluence was demonstrated in [Kü 85] with an implementation and encouraging empirical results with the classical Knuth-Bendix examples related to the concept of free groups.

In [Wi 85], Winkler proved completeness for the completion algorithm with subconnectedness criterion with an algorithm organization and proof structure based on [Hu 81]. For a different algorithm organization based on the model of a producer-consumer process, completeness was proved in [Kü 86] with a simple proof-induction technique. In contrast to [Hu 81], the proof appeared rather easy and well structured, owing both to the stronger induction technique and to a concise justification of rule deletions made possible by pseudo confluence.

The basic completion method meets its limits where inherently unorientable equations are encountered, as e.g. the axioms of associativity and commutativity (AC) together. The idea for the solution of these cases is to split $A = E \cup R$ into the disjoint subsets E and R of unorientable and orientable equations, respectively, so that the application of the trouble-making axioms can be covered by an extended unification algorithm, and rewriting is performed with the extended relation of R modulo E which works on E-equivalence classes. After the solution of the important AC case ([Hu 80], [La&Ba 77], [Pe&St 81]), a framework for the general case of a set of unorientable equations with finite equivalence classes and finite and complete unification algorithm was presented in [Jo&Ki 84]: The R-confluence test is augmented by a test for E-coherence, and the two properties can again be localized, and lifted to a most general level by E-unification.

In the following we carry the results of [Kü 86] over to the general case of non-empty E, deriving an E-completion algorithm that contains the one of [Jo&Ki 84] as a special case. In Chapter 2, we give an introduction to the proof-induction method used in most of the proofs. Our proof ordering immediately suggests the definitions of pseudo-E-coherence and pseudo-E-confluence, which, by a generalization of the equational Buchberger-Newman Lemma, imply the Church-Rosser property. From this lemma we obtain a new Church-Rosser test for non-Noetherian term-rewriting systems. The special case where the reduction ordering $>$ embeds the rewrite relation $\rightarrow$ yields the equational form of the Buchberger-Newman Lemma and the foundation of our completion method. Chapter 3 renders an adaptation of the main theorem of [Jo&Ki 84], which specifies the sets of critical pairs whose pseudo-E-confluence and pseudo-E-coherence implies the global Church-Rosser property. In Chapter 4, we first give the abstract criteria on critical pairs which imply their subconnectedness modulo E. Furthermore, we show that reducible rules generate only subconnected critical pairs. We then present our version of the equational Knuth-Bendix Algorithm with a general framework for the utilization of the abstract criteria, of which, e.g., the proposals of [Wi 83] and [K&M&N 866] are special cases. The complete proof of correctness follows in Chapter 5. In Chapter 6, we suggest various ways in which the abstract test can be put to work in practice. We treat explicitly the special case of empty E, for which we have the most thorough computational experience. We discuss various strategy refinements suggested by the different specializations of the abstract criterion together with empirical results. Chapter 7 contains two immediate applications of the theory of subconnected completion: For resolution theorem proving, an analogue to the subconnectedness test gives a subsumption criterion which predicts whether a resolvent is eventually going to be subsumed by other clauses; for the method of inductionless induction proposed in [Jo&Ko 85] we develop a ground subconnectedness criterion which is a sufficient test for the subconnectedness of all ground instances of a critical pair without requiring subconnectedness on the general level.

2 Abstract Subconnectedness Modulo E

We first concentrate on the set-theoretic part of our method where no knowledge of terms is required. In the following, let S be any non-empty set, and $t \in S$; we will be concerned with binary relations on $S \times S$.

DEFINITION: Let ${}_{R}{\rightarrow}$ be a relation on $S \times S$, called *reduction* to emphasize that it is non-symmetric. ${}_{R}{\leftarrow}$ denotes the inverse of ${}_{R}{\rightarrow}$, and ${}_{R}{\leftrightarrow} = {}_{R}{\rightarrow} \cup {}_{R}{\leftarrow}$. For simplicity we write $\rightarrow$ instead of ${}_{R}{\rightarrow}$ if no ambiguity arises. $\rightarrow^{+}$, $\rightarrow^{*}$, and $\leftrightarrow^{*}$ denote the transitive, and the reflexive and transitive, and reflexive, transitive and symmetric closure of $\rightarrow$, respectively. Let ${}_{E}{\leftrightarrow}$ be a symmetric relation on $S \times S$, whose reflexive transitive closure ${}_{E}{\leftrightarrow^{*}}$ is called *E-equivalence*. ${}_{R/E}{\rightarrow}$ is the relation ${}_{E}{\leftrightarrow^{*}} \circ {}_{R}{\rightarrow} \circ {}_{E}{\leftrightarrow^{*}}$ which corresponds to the relation induced by ${}_{R}{\rightarrow}$ in E-equivalence classes. Let ${}_{A}{\leftrightarrow} = {}_{E}{\leftrightarrow} \cup {}_{R}{\leftrightarrow}$; the reflexive-transitive closure ${}_{A}{\leftrightarrow^{*}}$ is correspondingly called *A-equivalence*.

DEF: Let $\blacktriangleright$ be a binary relation on $S \times S$. $\blacktriangleright$ is Noetherian, if there is no infinite sequence $t \blacktriangleright t' \blacktriangleright \ldots$. A binary Noetherian transitive relation is a well founded (and strict) partial ordering; for abbreviation, it will be called a *Noetherian ordering*.

Our overall goal is theorem proving in A, i.e. we want to infer relationships such as $t_1 \;{}_{A}{\leftrightarrow^{*}}\; t_2$. Now, working with A itself in an automated manner is difficult, because it is not Noetherian and hence derivations may e.g. run into cycles. The main idea in completion methods is to single out a subset $R \subseteq A$ such that $A = R \cup E$ and R/E is a Noetherian reduction relation, and then to complete R/E such that each theorem provable in A becomes provable in R/E through a finite number of reduction steps that can readily be automated.

DEF: $t \in S$ is *$\rightarrow$-reducible* if $\exists\, t' \in S : t \rightarrow t'$, otherwise t is *$\rightarrow$-irreducible* or in *$\rightarrow$-normal form*. A reduction ${}_{R}{\rightarrow}$ is *terminating* if it is Noetherian; it is *E-terminating*, or *terminating modulo E*, if ${}_{R/E}{\rightarrow}$ is Noetherian.

From now on, we will use the prefix *E-* and *modulo E* as synonyms. For brevity we often only define the general notions modulo E, and we will tacitly assume that whenever we omit E- or modulo E we refer to the corresponding property for the case of $E = \emptyset$.

Assume we have $t_1 \leftrightarrow^{*} t_2$; then t_1 and t_2 are actually connected by a finite *chain* $C = \langle t_1 \leftrightarrow u_1 \leftrightarrow u_2 \leftrightarrow \ldots \leftrightarrow u_{n-1} \leftrightarrow u_n \leftrightarrow t_2 \rangle$, which proves that t_1 and t_2 are related in the reflexive-transitive closure of $\leftrightarrow$. In general there can be many different proofs of $t_1 \leftrightarrow^{*} t_2$; we shall use the notation $P = \langle t_1 \leftrightarrow^{*} t_2 \rangle$ to indicate that P is any (fixed) proof, whereas we refer to a specific proof $P = \langle t_1 \leftrightarrow u_1 \leftrightarrow u_2 \leftrightarrow \ldots \leftrightarrow u_{n-1} \leftrightarrow u_n \leftrightarrow t_2 \rangle$ by its connecting sequence $C = \langle u_1 \leftrightarrow u_2 \leftrightarrow \ldots \leftrightarrow u_{n-1} \leftrightarrow u_n \rangle$, which we abbreviate as $P = \langle t_1 \leftrightarrow_{C} t_2 \rangle$. Of course we identify C and $C^{\leftarrow} = \langle u_n \leftrightarrow u_{n-1} \leftrightarrow \ldots \leftrightarrow u_2 \leftrightarrow u_1 \rangle$.

DEF: By transitivity, proofs can be concatenated if the last element of one proof is the first of the other. So, if $P = \langle x \leftrightarrow^{*} y \rangle$ is a proof that x relates to y, and $Q = \langle y \leftrightarrow^{*} z \rangle$ is a proof that y relates to z, then $W = P.Q = \langle x \leftrightarrow^{*} z \rangle$ is a proof that x relates to z. Correspondingly, W contains P and Q as *subproofs*. We denote the *empty proof* by $\langle\rangle$; *trivial proofs* are of the form $\langle t \rangle$, and *elementary proofs* are of the form $\langle u_1 \leftrightarrow u_2 \rangle$.

Our notation $P = \langle x \leftrightarrow^{*} y \rangle$ alone makes no reference to the proof sequence. So several proofs denoted all by $\langle x \leftrightarrow^{*} y \rangle$ will in general have different connecting sequences. However, they all prove that x relates to y, and are hence called *equivalent proofs* for this fact; the corresponding equivalence relation on proofs is denoted by $\approx$.

DEF: Let $A = R \cup E$. $B(A) = (A; ., \langle\rangle)$ is the monoid of proof chains, i.e. the set of all proofs in the reflexive transitive symmetric closure of A, augmented by the empty proof; note that there is no cut rule. A proof $W = \langle x \; {}_{A}{\leftrightarrow}^{*} \; z\rangle$ is said to be in *V-form modulo E*, if $\exists$ P, Q $\in B(R)$, M $\in B(E)$, $P = \langle x \; {}_{R}{\rightarrow}^{*} \; y_1\rangle$, $M = \langle y_1 \; {}_{E}{\leftrightarrow}^{*} \; y_2\rangle$, $Q = \langle y_2 \; {}_{R}{\leftarrow}^{*} \; z\rangle$: $W = P.M.Q$. $Bv_E(A) \subseteq B(A)$ is the subset of *reductional proofs* in A, i.e. proofs that are in V-form modulo E; we write $Bv(A)$ if $E = \emptyset$.

Our overall goal being automatic deduction techniques for valid relationships in equivalence relations, we are interested in producing simple proofs for these relationships, transforming complicated into simple proofs, if necessary. The key concepts for proof orderings are the following:

DEF: For a given set S, a *multiset M(S)* is a collection of elements from S that may have multiple occurrences of identical elements. For a partially ordered set $(S, \succ)$, the *multiset ordering* $\gg$ on $M(S)$ is defined as follows: For $M, N \in M(S)$, $M \gg N$ iff $\exists X, Y \in M(S)$, $\emptyset \neq X \subseteq M$, Y finite: $N = (M - X) \cup Y$ and $\forall y \in Y \; \exists x \in X$: $x \succ y$. I.e., $M \gg N$ if we can replace a number of elements in M with a finite number of elements in Y, each of which must be less (in terms of $\succ$) than some replaced element.

LEMMA: (Dershowitz, Manna 1979)
Let $(S, \succ)$ be a partially ordered set. Then $(M(S), \gg)$ is a partially ordered set whose ordering $\gg$ is well founded iff $\succ$ is well founded.

PROOF: By Kōnig's lemma, see [De&Ma 79] □

We are now in a position where we can (partially) order our proofs, if we are only given an ordering on S, because $\gg$ immediately induces an ordering on proofs when we take as multisets the sets of intermediate results. We will say that proof $N = \langle u_1 \leftrightarrow u_2 \leftrightarrow \ldots \leftrightarrow u_{n-1} \leftrightarrow u_n\rangle$ is *simpler* than proof $M = \langle t_1 \leftrightarrow t_2 \leftrightarrow \ldots \leftrightarrow t_m\rangle$, iff $M = \{t_1, t_2, \ldots, t_m\} \gg N = \{u_1, u_2, \ldots, u_n\}$. Because of this 1-1 correspondence, we will also write $M \gg N$ (or $N \ll M$ if that is more convenient). In our applications, we shall take for $\succ$ a superset of the well-founded termination ordering for ${}_{R/E}{\rightarrow}$ that is needed anyway to keep reductions Noetherian. For the remainder of this section, we simply assume that $\succ$ is a Noetherian partial ordering on E-equivalence classes.

PROPOSITION 1: Let $P = w_1.p.w_2$ and q be proofs, $q \approx p$, $q \ll p$. Then $w_1.q.w_2 \ll w_1.p.w_2$ □

DEF: R is *Church-Rosser modulo E* (*A* is *Church-Rosser in R/E* $\cup$ *E*) iff $\forall$ W $\in B(A)$ $\exists$ V $\in Bv_E(R/E)$: $V \approx W$.

The Church-Rosser property for a reduction relation requires that for each (complicated) proof in the symmetric closure there are also two reduction chains in the relation itself, which constitute an equivalent simpler proof. If we can decide E-equivalence, and if R is Church-Rosser modulo E, then we can decide A-equivalence by purely reductional proofs in R/E, and a single E-equivalence test. Unfortunately, it turns out to be in general impracticable to work with the ${}_{R/E}{\rightarrow}$ relation itself, because of the arbitrary location of implicit ${}_{E}{\leftrightarrow}$-steps involved. The idea is now to contain occurrences of these E-subproofs in such a way that they can be built into the application procedure (matching) for ${}_{R}{\rightarrow}$-steps. I.e., effectively we compute with some relation ${}_{R'}{\rightarrow}$, where ${}_{R}{\rightarrow} \subseteq {}_{R'}{\rightarrow} \subseteq {}_{R/E}{\rightarrow}$ (we set $A' = R' \cup E$). So we are interested in more specific connecting sequences which must still be in V-form but use only R' reductions. Consequently, our notation must be capable of expressing that the subconnecting sequence belongs to a specific subset of proofs.

DEF: R is *R'-Church-Rosser modulo E* (*Church-Rosser modulo E in R'*) iff $\forall$ W $\in B(A)$ $\exists$ V $\in Bv_E(R')$: $V \approx W$.

We are mainly interested in transforming proofs into simpler, but still equivalent ones. Furthermore, our transformations will be applied locally, hence the following definitions.

DEF: $P \boldsymbol{<}\!\approx Q$ (P is *simpler, but equivalent to*, Q) iff both $P \boldsymbol{<} Q$ and $P \approx Q$.
A proof is a *rewriting ambiguity*, iff it has one of the forms $\langle x \leftarrow y \rightarrow z\rangle$, $\langle x \leftarrow y \leftrightarrow z\rangle$, or $\langle x \leftrightarrow y \rightarrow z\rangle$.
R' is *locally pseudo-confluent with R in A'* iff $\forall\, a = \langle x\ {}_{R'}{\leftarrow}\ y\ {}_{R}{\rightarrow}\ z\rangle\ \exists\, w \in B(A')\colon w \boldsymbol{<}\!\approx a$.
R' is *locally pseudo-coherent in A'* iff $\forall\, a = \langle x\ {}_{R'}{\leftarrow}\ y\ {}_{E}{\leftrightarrow}\ z\rangle\ \exists\, w \in B(A')\colon w \boldsymbol{<}\!\approx a$.

If w is non-trivial and non-empty, it can always be assumed to be free of trivial (or empty) subproofs; we shall implicitly make this assumption in the sequel. Our definition of a rewriting ambiguity is by an abuse of the notation for the case of empty $\leftrightarrow$. When, for a rewriting ambiguity a, there exists $w \boldsymbol{<}\!\approx a$, we also say that w *subconnects* (the side-elements of) a, or that w is a *subconnecting chain*. We use subconnectedness as the common notion for pseudo-confluence and pseudo-coherence. Local pseudo-confluence and pseudo-coherence are suggested by the method of proof induction. Now proofs in *A'* still contain ${}_{E}{\leftrightarrow}$-steps at arbitrary locations, so that a slight specialization is necessary.

DEF: $Bw_E(R') = \{w \in B(R' \cup E) \mid w = p_1.p_2.\ \dots\ p_{n-1}.p_n,\ p_i \in Bv_E(R')\}$.
R' is *locally pseudo-confluent modulo E with R* iff $\forall\, a = \langle x\ {}_{R'}{\leftarrow}\ y\ {}_{R}{\rightarrow}\ z\rangle\ \exists\, w \in Bw_E(R')\colon w \boldsymbol{<}\!\approx a$.
R' is *locally pseudo-coherent modulo E* iff $\forall\, a = \langle x\ {}_{R'}{\leftarrow}\ y\ {}_{E}{\leftrightarrow}\ z\rangle\ \exists\, w \in Bw_E(R')\colon w \boldsymbol{<}\!\approx a$.
R' is *pseudo-coherent modulo E* iff $\forall\, a = \langle x\ {}_{R'}{\leftarrow}\ y\ {}_{E}{\leftrightarrow}\ z'\ {}_{E}{\leftrightarrow}^{*}\ z\rangle\ \exists\, w \in Bw_E(R')\colon w \boldsymbol{<}\!\approx a$.

We also write *pseudo-E-confluent* for pseudo-confluent modulo *E*. These conditions may at first look very special. However, when we immediately require w to be in V-form (modulo *E*) we receive the *local confluence*, *local coherence*, and *coherence* properties of [Jo&Ki 84], respectively. Furthermore, Lemma 1 below shows that local pseudo-*E*-coherence in *A'* already gives us these special connecting sequences in $Bw_E(R')$ composed of subproofs in $Bv_E(R')$. In this case we know where ${}_{E}{\leftrightarrow}$-steps occur in the subconnecting sequence, so we shall also say that *R'* is *pseudo-E-confluent in R'*.

LEMMA 1: Let *R'* be locally pseudo-*E*-coherent. Then $\forall\, P \in B(A')\ \exists\, Q \in Bw_E(R')$: either $Q = P$, or else $Q \boldsymbol{<}\!\approx P$.

PROOF: Let $P \in B(A')$. If P has already the special form required for Q, we are done. Otherwise, assume for proof induction the hypothesis for all $P' \boldsymbol{<} P$. Now $P = P_1.a.P_2$ must have a subproof $a = \langle x\ {}_{R'}{\leftarrow}\ y\ {}_{E}{\leftrightarrow}\ z\ {}_{E}{\leftrightarrow}^{*}\ z'\rangle$ with $a \notin B(R')$. By local pseudo-*E*-coherence, there exists $w \in Bw_E(R')$, $w \boldsymbol{<}\!\approx \langle x\ {}_{R'}{\leftarrow}\ y\ {}_{E}{\leftrightarrow}\ z\rangle$, and hence $b = w.\langle z\ {}_{E}{\leftrightarrow}^{*}\ z'\rangle \boldsymbol{<} a$. Now $P' = P_1.b.P_2 \boldsymbol{<} P$, $P' \in B(R' \cup E)$, so that, by hypothesis, we are done □

COROLLARY: Let *R'* be locally pseudo-*E*-coherent in *A'*. Then *R'* is pseudo-coherent modulo *E*.

PROOF: Let $a = \langle x\ {}_{R'}{\leftarrow}\ y\ {}_{E}{\leftrightarrow}^{*}\ z\rangle$. By Lemma 1, $\exists\, Q \in Bw_E(R')$, $Q \boldsymbol{<}\!\approx P$ □

LEMMA 2: Let *R* be *E*-terminating and let *R'* be locally pseudo-coherent modulo *E*. Then t is ${}_{R/E}{\rightarrow}$-reducible iff it is ${}_{R'}{\rightarrow}$-reducible.

PROOF: The if-part is trivial. Now if t is ${}_{R/E}{\rightarrow}$-reducible there is some proof $r = \langle t\ {}_{R/E}{\rightarrow}\ t'\rangle$. By the definition of *R/E*, there is a corresponding proof $r' \in B(A')$ for which by Lemma 1 there is a proof b starting with a non-trivial subproof $p \in Bv_E(R')$. Now $p \in B(E)$ or $p = \langle t\ {}_{E}{\leftrightarrow}^{*}\ t''\rangle.\langle t''\ {}_{R'}{\leftarrow}^{*}\ t'\rangle$ would both contradict *E*-termination of *R*, whence t must be *R'*-reducible □

Our proof ordering $\gg$ has by its definition as a multiset ordering the *embedding property* of proposition 1: $p \gg q$ implies $w_1.p.w_2 \gg w_1.q.w_2$. For our applications to term-rewriting systems, we shall have to work with stronger orderings for which embedding does not hold in general. Instead, it is sufficient, but essential, to have embedding for our transformations on proofs, so that they can be applied locally. So we shall require of a proof-ordering that it be *stable under embedding of rewriting ambiguities*, i.e., $p \gg q$ implies $w_1.p.w_2 \gg w_1.q.w_2$ if p is a rewriting ambiguity. This property was first given special consideration in [Ba&De 86], where it is called monotonicity.

We are now ready for the main result of this chapter, which is a generalization of the interesting direction of the Buchberger-Newman Lemma.

THEOREM 1: (Equational Generalized Buchberger-Newman Lemma)

Let $\gg$ be a proof ordering which is stable under embedding of rewriting ambiguities. Then *R* is *R'*-Church-Rosser modulo *E* if *R'* is locally pseudo-*E*-confluent with *R* and locally pseudo-*E*-coherent.

PROOF: Let $P \in B(R \cup E)$; clearly, $P \in B(R' \cup E)$. We assume for proof induction the hypothesis that $\forall W \ll P\ \exists V \in Bv_E(R')$: $V \approx W$. Now if $P \in Bv_E(R')$, we are done. Otherwise P contains at least one rewriting ambiguity a as subproof. So there exists, according to the premises, a proof $a' \ll\approx a$, $a' \in B(R' \cup E)$. So $W = p_1.a'.p_2 \ll P = p_1.a.p_2$ by embedding and hence, by our induction hypothesis, we are done □

Note that we did not require that $\gg$ contain ${}_{R/E}\!\rightarrow$. For example, ${}_{R/E}\!\rightarrow$ may not be Noetherian, so that we get a new confluence test for non-Noetherian rewriting systems.

EXAMPLE 1: Theorem 1 (but not Newman's Lemma) implies each of the following:
a) Let *R* consist of infinitely many rules $1 \rightarrow 2$, $2 \rightarrow 3$, ... *R* is clearly CR, taking $> = \emptyset$.
b) Let *R* be such that $\forall x, y, z$: $x \leftarrow z \rightarrow y$ implies $x \leftrightarrow y$. Then *R* is CR, taking $> = \emptyset$.
c) Let $R = \{A \rightarrow B, A \rightarrow C, C \rightarrow D, D \rightarrow B, B \rightarrow 1, 1 \rightarrow 2, 2 \rightarrow 3, \dots\}$. *R* is CR, taking $> = \{A > D\}$.
Note that the system in c) is not even strongly confluent (but clearly CR) □

Under these weak assumptions, the Church-Rosser property does not imply that there exists a Noetherian ordering according to which the rewriting ambiguities of *A'* are subconnected. However, the implication stated in the theorem is still the one that is most interesting, because our aim is to prove the Church-Rosser property. For our application to term-rewriting systems we shall utilize the special case where $\gg \supseteq {}_{R/E}\!\rightarrow$, so that default confluence implies subconnectedness.

COROLLARY: (Equational Buchberger-Newman Lemma, EBNL)

Let $> \supseteq {}_{R/E}\!\rightarrow$ be an *E*-termination ordering and $\gg$ the associated proof ordering. Then *R* is *R'*-Church-Rosser modulo *E* iff *R'* is locally pseudo-*E*-confluent with *R* and locally pseudo-*E*-coherent.

PROOF: The only-if-part holds by definition and $> \supseteq {}_{R/E}\!\rightarrow$, the if-part is covered by Theorem 1 □

Obviously, Theorem 1 implies EBNL under the condition $\rightarrow \subseteq >$. EBNL generalizes the interesting direction of Newman's Diamond Lemma in that it requires a local property (subconnectedness) that is strictly weaker than local confluence. The corresponding lemma for the case of empty *E* was first stated in [Bu 84] as the Generalized Newman Lemma, and proved in [Wi&Bu 83]. Globally, of course, subconnectedness and local confluence are equivalent properties, so that the name may have been misleading. Incidentally, in [Wi&Bu 83] the lemma also used a definition of "connectedness" that implies $\rightarrow \subseteq >$ if it holds globally (for every rewriting ambiguity).

The following is again the generalization to subconnectedness of a lemma in [Jo&Ki 84].

LEMMA 3: Let R be E-terminating. Let R' be locally pseudo-E-coherent and locally pseudo-E-confluent. Then normal forms of t with respect to ${}_{R/E}{\rightarrow}$ and with respect to ${}_{R'}{\rightarrow}$ are E-equivalent.

PROOF: Let $W = \langle t_1 \;{}_{R/E}{\leftarrow}^{*}\; t \;{}_{R'}{\rightarrow}^{*}\; t_2 \rangle$; let $w' = \langle t_1 \;{}_{A'}{\leftrightarrow}^{*}\; t_2 \rangle$ be the corresponding proof in $B(A')$ which exists according to the definition of ${}_{R/E}{\rightarrow}$. By Theorem 1, R is R'-Church-Rosser modulo E, so $\exists\, V \in Bv_E(R')$: $V = \langle t_1 \;{}_{A'}{\leftrightarrow}^{*}\; t_2 \rangle$. Now t_2 is ${}_{R'}{\rightarrow}$-irreducible, and t_1 is ${}_{R/E}{\rightarrow}$-irreducible, hence also ${}_{R'}{\rightarrow}$-irreducible; so necessarily $V = \langle t_1 \;{}_{E}{\leftrightarrow}^{*}\; t_2 \rangle$ □

3 Subconnectedness in Term Rewriting Systems Modulo Equations

We shall now apply the results of the previous section to equational theories, i.e. congruence relations on free term-algebras, which are particular instances of equivalence relations. To make the presentation self-contained, we also reproduce necessary terminology from [Hu&Op 80], [Hu 81], and [Jo&Ki 84].

3.1 Basic Definitions

DEF: Let V be a denumerable set of variables. Let Σ be a finite or denumerable set of operator symbols disjoint from V, and *arity* a function from Σ to $\mathbb{N}_0$. The set T of *terms* is defined as the free arity-graded Σ-algebra generated by V.

DEF: Let $t \in T$. $O(t)$ denotes the set of subterm occurrences in t, a subset of a tree domain. Occurrences are called *positions* throughout this paper. Positions are represented as strings of natural numbers, with concatenation operator $\cdot$ and identity ε. Two positions u and v are *disjoint*, $u|v$, if neither is a prefix of the other. ε is the *top position* in any term, i. e. $t = t|_{\varepsilon}$ (t *at* ε) $\forall\, t \in T$. Term s *occurs* in t (as subterm), which we write t[s], if $\exists\, u \in O(t)$: $t|_u = s$. $G(t) := \{u \in O(t) \mid t|_u \notin V\}$ is the set of all *non-variable positions* in t.

DEF: An *axiom-system* is a finite set A of pairs of terms ⟨g, d⟩ called *equations* and written g = d. $_A{\leftrightarrow}$ is the smallest symmetric relation that contains A and is closed under substitution and replacement. $_A{=}$, *equality under A*, is the transitive and reflexive closure $_A{\leftrightarrow}^{*}$. It is the finest congruence containing A and closed under substitution.

DEF: Let $V(t)$ be the set of all variables occurring in t. An *A-substitution* σ is a mapping $V \rightarrow T$. In the special case of an injection where all terms of σ are variables, we call σ a *permutation*, or *renaming of variables*. For a set of variables V', $\sigma|_{V'}$ is the restriction of σ on V'. Substitutions σ and τ over the same domain $D \subseteq V$ are *A-equal*, if $x\sigma\ _A{=}\ x\tau\ \forall\, x \in D$. Let S be the set of A-substitutions. $_A{\leq}$ denotes the *subsumption preorder modulo A* on T, i. e. $s\ _A{\leq}\ t$ iff $\exists\, \sigma \in S$: $s\sigma\ _A{=}\ t$. If $s\ _A{\leq}\ t$ we say that s *A-matches* t with A-matching substitution σ; we say that s and t are *A-unifiable*, $s\ _A{\nabla}\ t$, iff $\exists\, \mu \in S$: $s\mu\ _A{=}\ t\mu$. A set of A-unifiers μ^{*} of s and t for which $s\mu^{*}\ _A{\leq}\ s\mu$, for each A-unifier μ, is called a *complete set of most general A-unifiers (CSU*(s, t, *A*)*)*, and for each μ^{*}, $s\mu^{*}$ is a *most general common instance (mgci)*, of s and t. Of course we omit subscripts if no ambiguity arises.

DEF: An *equational term-rewriting system (ETRS)* R_A is an axiom-system whose elements, called *rules* and pictured as oriented equations, all satisfy $V(d) \subseteq V(g)$. Given the equations of any A, we say that rule R = ⟨g, d⟩ is *A-applicable* to term t if $\exists\, u \in O(t)$: $g\ _A{\leq}\ t|_u$. We say that t *A-reduces to* t' in u, and we write $t' = t[u \leftarrow d\sigma]$, and $t\ _{R,A}{\rightarrow}_{[u,\, \sigma,\, g\rightarrow d]}\ t'$, if σ is the A-matching substitution of g on $t|_u$. Again, we shall usually list only the indispensible subscripts. $_{R,A}{\rightarrow}$ is the smallest relation that contains R_A and is closed under A-substitution and replacement. t is in $_{R,A}{\rightarrow}$*-normal form* if no rule in R is A-applicable to t. We also write R,A for R_A, and, since $g\ _{R,A}{\rightarrow}\ d$ if $\langle g, d\rangle \in R_A$, we also denote rules by ⟨g → d⟩.

DEF: A term-rewriting system R is said to be locally confluent (Church-Rosser, Noetherian, etc) iff $_R{\rightarrow}$ is locally confluent (Church-Rosser, Noetherian, etc). It is said to be *subconnected*, iff all rewriting ambiguities in $_R{\rightarrow}$ are subconnected. R is *interreduced*, if for each $\langle l \rightarrow r\rangle \in R$, r is in R-normal form and l is in $R - \{\langle l \rightarrow r\rangle\}$-normal form.

DEF: Let s be a non-variable term and t a term with position u in $G(t)$. Then s *A-superposes* on t at position u in $G(t)$ with a complete set Θ of *A-superposition substitutions* iff there exists a set of unifiers $\Theta \neq \emptyset$, s.th. $\Theta = CSU(t|_u, s, A)$. In this case there also exists a complete set of *A-superpositions* $SP(t|_u, s, A) = \{t\theta \mid \theta \in \Theta\}$. In the case of empty A there is one superposition which is unique up to variable permutation. Following [Jo&Ki 84] we also call the superposition substitutions *overlappings*. Given rules $\langle l \rightarrow r\rangle$ and $\langle g \rightarrow d\rangle$ such that $V(l) \cap V(g) = \emptyset$, and l overlaps g at position u in $G(g)$ with the complete set of *A-overlappings* Θ, then the set $\{\langle\langle p, q\rangle\rangle \mid p = g\theta[\varepsilon \leftarrow d\theta] = d\theta,\ q = g\theta[u \leftarrow r\theta]\}$ is called a *complete set of A-critical pairs* of the rule $\langle l \rightarrow r\rangle$ on the rule $\langle g \rightarrow d\rangle$ at position u. $\{g\theta \mid \theta \in \Theta\}$ is the corresponding set of A-superpositions. Critical pairs are *trivial* if $\langle g \rightarrow d\rangle = \langle l \rightarrow r\rangle$ and the overlap position is ε.

3.2 Subconnectedness and the Church-Rosser Property for Term-Rewriting Systems

We closely follow [Jo&Ki 84], using their terminology, but we generalize their results to the use of pseudo-E-confluence and pseudo-E-coherence. In addition, we employ our notation of proofs. In fact, our generalization is immediately apparent from the proof diagrams given in [Jo&Ki 84], which, due to the method of proof induction, we need not close completely; instead, we are done with each rewriting ambiguity as soon as we have constructed an equivalent, but simpler, proof for it.

We intend to work with the reduction relation $R' = Rl \cup Rnl{,}E$ generated by two rewrite-systems Rl and Rnl, with linear and non-linear rules, respectively, and an axiom-system E; furthermore we have $Rl \cup Rnl = R$, and we set $A = R \cup E$ and $A' = R' \cup E$. We assume that equivalence classes in ${}_E{=}$ are finite, and that we have a finite and complete unification algorithm for the theory E. In addition, we assume that we are given a Noetherian ordering on E-equivalence classes, the reduction ordering $\succ \supseteq {}_{R/E}{\rightarrow}$, which is stable under substitution and replacement; in particular s $\succ$ t implies s' $\succ$ t' if s' ${}_E{=}$ s and t' ${}_E{=}$ t. We shall at first work with the proof ordering $\gg$ given by the multiset extension of $\succ$. Note that $\succ \supseteq {}_{R'}{\rightarrow}$, which immediately gives us

<u>LEMMA 4: (Default subconnectedness)</u>

Any R'-confluent rewriting ambiguity is $\gg$-subconnected modulo E in R'.

PROOF: Let $P = \langle p\ {}_{A'}{\leftrightarrow}\ u\ {}_{A'}{\leftrightarrow}\ q\rangle$ be a rewriting ambiguity and $Q = Q'.M.Q'' = \langle p\ {}_{R'}{\rightarrow}^{*}\ p_1\rangle.\langle p_1\ {}_{E}{\leftrightarrow}^{*}\ q_1\rangle.\langle q_1 \leftarrow^{*} q\rangle$ in $Bv_E(R')$. If $P = \langle p \leftarrow u \rightarrow q\rangle$, then clearly $u \rightarrow^{+} t_i$ for all terms $t_i \in Q' \cup Q''$ (Q' and Q" may be trivial, but not empty), and hence $u \succ t_i$ by $\succ \supseteq R/E \supseteq R'$. Furthermore, $\forall\, t_i \in M$ $\exists\, s \in Q'$: $t_i\ {}_{E}{\leftrightarrow}^{*}\ s$, which gives $u \succ t_i$ in this case, too, by a property of $\succ$. If $P = \langle p\ {}_{R'}{\leftarrow}\ u\ {}_{E}{\leftrightarrow}\ q\rangle$, we have again $P \gg Q'$ and $P \gg M$ by the same reasoning as above. Now Q" cannot be trivial, for otherwise $p_1\ {}_E{=}\ q$, which, with $u\ {}_E{=}\ q$ and $u \succ q$, yields the contradiction $q \succ q$. So we have $q \rightarrow^{+} t_i$, and hence $u \succ t_i$, for all remaining terms $q \neq t_i \in Q''$. Altogether we get $u \succ t_i$ for all terms in the connecting sequence $C = Q \setminus \{p, q\}$ of Q, and therefore $P \gg Q$ because $Q = (P - \{u\}) \cup C$ □

Note that in the coherence case the peak term u is not greater than each term in the new proof Q, but it is indeed greater than all new elements that are not already in P. Here we really need something stronger than Buchberger's original definition of connectedness, in the manner of Theorem 1. The additional result that Q" is not trivial in the coherence case will be needed again below.

In complete analogy to the case of empty E accomplished by Knuth, we shall be able to lift the treatment of rewriting ambiguities to the most general level of critical pairs.

LEMMA 5: (E-Critical Pairs Lemma [Jo 83])

Assume $\langle t\ {}_{R}{\rightarrow}[\varepsilon, \sigma, g\rightarrow d]\ t_1\rangle$ or $\langle t\ {}_{E}{\leftrightarrow}[\varepsilon, \sigma, g\rightarrow d]\ t_1\rangle$, and $\langle t\ {}_{R,E}{\rightarrow}[n, \sigma, l\rightarrow r]\ t_2\rangle$, with $n \in G(g)$, and $n \neq \varepsilon$ if $g\rightarrow d \in E$. Then there exists a critical pair $\langle\langle p, q\rangle\rangle = \langle\langle d\Theta, g[n\leftarrow r]\Theta\rangle\rangle$ in a complete set of E-critical pairs of the rule $l\rightarrow r$ on the rule $g\rightarrow d$ at occurrence n, and a substitution τ such that $\Theta \in \mathrm{CSU}(g|_n, l, E)$, and $t_1\ {}_{E}{\leftrightarrow}^{*}\ p\tau$ and $\sigma\ {}_{E}{\leftrightarrow}^{*}\ \Theta\tau|_{(\mathcal{V}(g)\,\cup\,\mathcal{V}(l))}$, therefore $t_2\ {}_{E}{\leftrightarrow}^{*}\ q\tau$.

PROOF: By the definition of a complete set of E-unifiers, see [Jo 83] □

For empty E, the E-critical pairs specialize of course to the usual critical pairs. Following again Jouannaud and Kirchner, let $SCP(R, R)$, $SCP(E, R)$, and $SCP(R, E)$ be the sets of non-trivial critical pairs for respectively: all $\langle l\rightarrow r\rangle$ and $\langle g\rightarrow d\rangle$ both in R, all $\langle l\rightarrow r\rangle$ and $\langle r\rightarrow l\rangle$ for $\langle l = r\rangle$ in E with all $\langle g\rightarrow d\rangle$ in R, and all $\langle l\rightarrow r\rangle$ in R with all $\langle g\rightarrow d\rangle$ and $\langle d\rightarrow g\rangle$ for $\langle g = d\rangle$ in E. Top critical pairs are not considered in $SCP(R, E)$ because they duplicate those in $SCP(E, R)$. Furthermore, let $CSECP(R, R)$ and $CSECP(R, E)$ be the complete sets of non-trivial E-critical pairs for respectively all $\langle l\rightarrow r\rangle$ in R with all $\langle g\rightarrow d\rangle$ in R, and all $\langle l\rightarrow r\rangle$ in R with all $\langle g\rightarrow d\rangle$ and $\langle d\rightarrow g\rangle$ for $\langle g = d\rangle$ in E. Top critical pairs will not be needed in $CSECP(R, E)$.

Again we take some convenient liberties with these notations; so, e.g., $SCP(\langle g\rightarrow d\rangle, u, \langle l\rightarrow r\rangle)$ represents the critical pair of equation $\langle g\rightarrow d\rangle$ on rule $\langle l\rightarrow r\rangle$ at position u in l. If it is unknown whether $\langle g\rightarrow d\rangle$ is a rule or an equation, or whether $\langle l\rightarrow r\rangle$ is in Rl or Rnl, we write $CP(\langle g\rightarrow d\rangle, u, \langle l\rightarrow r\rangle)$ for the set of critical pairs according to the true gender of the superposition partners.

We intend to show that subconnectedness of the critical pairs implies subconnectedness of all rewriting ambiguities. We face the difficulty that the subconnecting sequence (after substitution and replacement) alone is not an equivalent proof to the rewriting ambiguity, but that we also need the equality steps $Q' = \langle t_1\ {}_{E}{\leftrightarrow}^{*}\ p\tau\rangle$ and $Q'' = \langle t_2\ {}_{E}{\leftrightarrow}^{*}\ q\tau\rangle$. For confluence situations this presents no problem, because both $Q' \lessdot P$ and $Q'' \lessdot P$, so that we obtain a proof of $t_1 = t_2$ completely below P. For coherence situations, however, $t\ {}_{E}{\leftrightarrow}^{*}\ t_1$ and the proof Q" is not simpler than P in our proof ordering.

Here it is essential to notice that $d\sigma = t_1\ {}_{E}{\leftrightarrow}^{*}\ p\tau = d\Theta\tau$, and that the substitutions σ and $\Theta\tau$ are E-equal, so that there is a proof $\langle d\sigma\ {}_{E}{\leftrightarrow}^{*}\ d\Theta\tau\rangle$ in which the E-steps take place within the substitution part of d. So, obviously, there must be a stronger proof ordering which takes occurrences of E-applications into account. A new class of orderings of this type has recently been introduced in [Ba&De 86]. Within the class, stronger orderings are obtained through lexicographic extensions by additional Noetherian orderings. While the orderings of Bachmair and Dershowitz are based on complexity comparisons of elementary proofs, we shall extend our term-comparisons to stay compatible with [Kü 86]. Alternatively, we could also give the subsequence Q" separate treatment, leaving the ordering weaker but complicating proofs of our theorems.

DEF: We define the *complexity* of an intermediate result t in an equational proof as a tuple (t, S), where t is a term and S is the multiset of subterms which are replaced by the affixed proof steps. To each subterm we adjoin one of the *modes* r or e, according to whether it is replaced by a rule or an equation, respectively, and we write (r, s) to denote the pair of mode and term. So in a proof with subproof $\langle s\ {}_{R'}{\leftrightarrow}[h, ,]\ t\ {}_{E}{\leftrightarrow}[n, ,]\ u\rangle$, t has complexity $(t, \{(r, t|_h), (e, t|_n)\})$. Occasions where we need the mode information will be rare, and usually we will only write the subterm for simplicity, and think of the mode as additional information available on demand. Of course, S contains a single term if t is in an elementary proof, and S is empty if t is in a trivial proof. ${}_{E}{\succ}$ is an ordering on terms with mode, defined as $s\ {}_{E}{\succ}\ t$ iff either the mode of s is e and the mode of t is r, or else $\exists\, u \neq \varepsilon$: $s|_u\ {}_{E}{=}\ s'[t]$; i.e. there exists a strict subterm of s which is E-equal to a term that contains t (equivalently, there is a term s" in the E-equivalence class of s, s. th. t is a strict subterm of s"). ${}_{E}{\succ}'$

is the multiset extension of ${}_E{\succ}$. The complexity ordering $\succ_c$ is the lexicographic ordering obtained when comparing term complexities by $\succ$ in the first component, and, if first components are E-equal, comparing second components by ${}_E{\succ}'$. Finally, the *extended proof ordering* ${}_E{\boldsymbol{\succ}}$ is defined as the multiset extension of $\succ_c$.

${}_E{\succ}$ is actually a subterm relation on E-equivalence classes. To see this, we note that its definition is representation independent: let $s\ {}_E{\succ}\ t$, and $s_1\ {}_E{=}\ s$, $t_1\ {}_E{=}\ t$. Then by definition $\exists$ s': $s\ {}_E{=}\ s'[t]$, so that $s_1\ {}_E{=}\ s'[t]$. Now $t\ {}_E{=}\ t_1$ implies $s'[t]\ {}_E{=}\ s'[t_1]$ by congruence, so that $s_1\ {}_E{=}\ s'[t_1]$ with a strict subterm occurrence, and hence $s_1\ {}_E{\succ}\ t_1$.

LEMMA 6:

${}_E{\boldsymbol{\succ}}$ is a Noetherian ordering on term-complexities if E-equivalence classes are finite.

PROOF: By assumption, $\succ$ is a Noetherian ordering on E-equivalence classes. We first show that ${}_E{\succ}$ is Noetherian: let $u_1\ {}_E{\succ} \ldots u_i\ {}_E{\succ}\ u_{i+1} \ldots$ be an infinite sequence. There is some index j s. th. the modes of all u_i with $i > j$ are the same. For all $i > j$, we have $u_i\ {}_E{=}\ u_i''[u_{i+1}]$. So, by stability of ${}_E{=}$ under replacement, there is a sequence of terms $u_i\ {}_E{=}\ u_i''[u_{i+1}]\ {}_E{=}\ u_i''[u''_{i+1}[u_{i+2}]]\ {}_E{=} \ldots$ in which subterm occurrences are strict by definition and therefore term sizes cannot be bounded. So the sequence must be infinite, contrary to our assumption that E-equivalence classes are finite. Consequently, both ${}_E{\succ}$ and its multiset extension ${}_E{\succ}'$ are Noetherian. Now $\succ_c$ is Noetherian as a lexicographic extension of Noetherian orderings: Assume to the contrary that there exists an infinite sequence C $\succ_c$ C' $\succ_c \ldots$. We cannot have an infinite subsequence of only ${}_E{\succ}'$ steps. So in the first component we have a sequence of $\succ$ steps interspersed with finite subsequences of E-equivalent terms. The latter can be factored out, however, yielding an infinite sequence of $\succ$ steps on E-equivalence classes, contradicting the first assumption. As a conclusion, ${}_E{\boldsymbol{\succ}}$ is Noetherian as a multiset extension of $\succ_c$ □

Again we identify ${}_E{\boldsymbol{\succ}}$, which is defined on the multisets of term-complexities, and its associated ordering on proofs. Clearly, ${}_E{\boldsymbol{\succ}} = \boldsymbol{\succ}$ if comparison is only in the first component; so ${}_E{\boldsymbol{\succ}} \supseteq \boldsymbol{\succ}$, and the extension preserves well-foundedness. We shall now prove that the extension also preserves stability, a crucial result for lifting the treatment of subconnectedness to the most general level of critical pairs in the same way as for local confluence.

LEMMA 7: (Stability of ${}_E{\boldsymbol{\succ}}$ under substitution and replacement)

Let $P = \langle p_1\ {}_{A'}{\leftrightarrow}\ p_2\ {}_{A'}{\leftrightarrow} \ldots {}_{A'}{\leftrightarrow}\ p_n\rangle$, $Q = \langle q_1\ {}_{A'}{\leftrightarrow}\ q_2\ {}_{A'}{\leftrightarrow} \ldots {}_{A'}{\leftrightarrow}\ q_m\rangle$ be proofs in B(A'); let t be a term and σ an E-substitution. Then $P\sigma = \langle p_1\sigma\ {}_{A'}{\leftrightarrow}\ p_2\sigma\ {}_{A'}{\leftrightarrow} \ldots {}_{A'}{\leftrightarrow}\ p_n\sigma\rangle$ and $t[P] = \langle t[u \leftarrow p_1]\ {}_{A'}{\leftrightarrow}\ t[u \leftarrow p_2]\ {}_{A'}{\leftrightarrow} \ldots {}_{A'}{\leftrightarrow}\ t[u \leftarrow p_n]\rangle$ are also proofs in B(A'). Moreover, if $P\ {}_E{\boldsymbol{\succ}}\ Q$ for Q $\in$ B(A'), then both $P\sigma\ {}_E{\boldsymbol{\succ}}\ Q\sigma$ and $t[P]\ {}_E{\boldsymbol{\succ}}\ t[Q]$. Hence the proof ordering ${}_E{\boldsymbol{\succ}}$ is stable under substitution and replacement.

PROOF: We look at the associated multisets, and we note that subterm modes do not change under substitution and replacement. We have $p_i\sigma\ {}_{A'}{\leftrightarrow}\ p_{i+1}\sigma$ if $p_i\ {}_{A'}{\leftrightarrow}\ p_{i+1}$, and $t[u \leftarrow p_i]\ {}_{A'}{\leftrightarrow}\ t[u \leftarrow p_{i+1}]$ if $p_i\ {}_{A'}{\leftrightarrow}\ p_{i+1}$, because of stablity of ${}_{A'}{\leftrightarrow}$ under substitution and replacement, respectively; so the multisets of terms associated to Pσ and t[P] are indeed proofs. Let $Q = \langle q_1\ {}_{A'}{\leftrightarrow}\ q_2\ {}_{A'}{\leftrightarrow} \ldots {}_{A'}{\leftrightarrow}\ q_m\rangle$. Now $p_i \succ q_j$ implies both $p_i\sigma \succ q_j\sigma$ and $t[u \leftarrow p_i] \succ t[u \leftarrow q_j]$ by stability of $\succ$ under substitution and replacement, so we already have the result for $\boldsymbol{\succ}$, by its definition as the multiset extension of $\succ$. For comparison in the second component, we have $p_i\ {}_E{=}\ q_j$, and positions u, v, s.th. $p_i|_u = r$, $q_j|_v = s$, with $r\ {}_E{\succ}\ s$; so by definition $r|_h\ {}_E{=}\ t[s]$ for some $h \neq \varepsilon$. By stability of ${}_E{=}$, comparison after substitution and replacement is again in the second component. Replacement, i.e. adding context in a proof, does not change the subterms to which the proof steps are affixed, so second components remain unchanged, which trivially preserves the ordering; in the case of substitution we have $r\sigma|_h = (r|_h)\sigma \;_{E}{=}\; t\sigma[s\sigma]$, hence also stability □

As remarked earlier, stability of $_{E}\!\succ$ under embedding is no longer trivial, because term complexities are now sensitive to the context, i.e. to the adjacent proof. In terms of multiset orderings, this means that the middle term of a rewriting ambiguity no longer gets replaced by the subconnecting sequence, but the complexities of all three terms get replaced by the complexities of the new proof. To obtain stability under our proof-transformations, we must now even take into account just how coherence ambiguities will get subconnected.

LEMMA 8: (Stability of $_{E}\!\succ$ under embedding of rewriting ambiguities)

Let A be a rewriting ambiguity, and $A' \;_{E}\!\prec\!\approx A$, where A' is constructed by the completion process. Then $W_1.A'.W_2 \;_{E}\!\prec\!\approx W_1.A.W_2$.

PROOF: [Confluence ambiguity] Let $A = \langle t'' \;_{R'}\!\leftarrow t \;_{R'}\!\rightarrow t'\rangle$, $A' = \langle t'' \;_{A'}\!\leftrightarrow^{*} t'\rangle$ (note that A' must be equivalent to A, so that both side terms must be present in A'). Since $t \succ t''$ and $t \succ t'$, comparison for $\succ_c$ is solely in the first component, which is unchanged by adding context.
[Coherence ambiguity] Let $A = \langle t'' \;_{R'}\!\leftarrow_{[n,\,,\,l\to r]}\, t \;_{E}\!\leftrightarrow_{[h,\,,\,g\to d]}\, t'\rangle$, $A' = \langle t'' \;_{A'}\!\leftrightarrow^{*} t'\rangle$. Again, t" poses no problems.
(i) If $A' = \langle t'' \;_{A'}\!\leftrightarrow^{*} u \;_{R'}\!\leftarrow t'\rangle$, the mode of $t'|_h$ changes from e to r, so complexity decreases in $_{E}\!\succ'$.
(ii) If $A' = P.Q' = \langle t'' \;_{A'}\!\leftrightarrow^{*} u \;_{R'}\!\leftarrow u'\rangle.\langle u' \;_{E}\!\leftrightarrow^{*} t'\rangle$, we must assume that $_{E}\!\leftrightarrow$-applications in Q' are at strict subterms of h, in order to get $t' \;_{E}\!\succ' u_i$ for $u' \neq u_i \in Q'$. This will be guaranteed during completion. Embedding the rewriting ambiguity adds the same context subterm to $\{t'|_h\}$ in both complexities, and so preserves the ordering. The complete analysis for the coherence case is done in the proof of lemma 9, where the form of subconnecting sequences is discussed in detail □

To emphasize that a subconnecting sequence for a coherence ambiguity fulfills the extra condition for case (ii) in the above proof, we shall speak of the *standard subconnectedness* of a coherence ambiguity.

COROLLARY (Default $_{E}\!\prec$-subconnectedness):

Any R'-confluent rewriting ambiguity is $_{E}\!\prec$-subconnected modulo E in R'.

PROOF: We have either a confluence ambiguity or case (i) of a coherence ambiguity □

In the following, we shall keep in mind that the ordering problem is confined to the treatment of coherence. So, e.g., the weak proof-ordering suffices to obtain the complete correctness proof for empty E; this was done in [Kü 86]. Moreover, the weak ordering suffices if we can always assume coherence: subconnecting proofs are then in $Bw_E(R')$, so that we always have case (i) for coherence ambiguities. Working with $\succ$, we do not replace t', and all terms of the subconnecting sequence are less than t because $\succ$ is an ordering on E-equivalence classes. Coherence may be assumed, e.g., if we work with a particular form of Jouannaud and Kirchner's E-completion algorithm which uses automatic Peterson-Stickel extensions instead of coherence pairs. This algorithm is available in Reve 3.4 through a "strategy" option; it still contains the Peterson-Stickel algorithm as a special case. We shall not treat these special cases separately, but we shall indicate in the following proofs where we need the extension of the weak ordering. All our definitions will be assumed for $_{E}\!\prec$ from now on; all previous results, with the exception of proposition 1, hold for $_{E}\!\prec$-subconnectedness, too.

We are now ready for the generalization of the main result of [Jo&Ki 84] to subconnectedness, which we do in the following three steps, closely following the case analysis of [Jo&Ki 84].

LEMMA 9:

Let $R = Rl \cup Rnl$ be an E-terminating set of rules such that Rl is left-linear, a complete and finite unification algorithm exists for the theory E, and E-congruence classes are finite.
Then $R' = Rl \cup Rnl{,}E$ is locally pseudo-E-coherent in A' iff all *coherence pairs* $\langle\langle p, q\rangle\rangle$ in $SCP(Rl, E) \cup SCP(E, Rl) \cup CSECP(Rnl, E)$ are subconnected in A'.

PROOF: By definition, R' is locally pseudo-E-coherent in A' iff $\forall$ A = $\langle t'' \;{}_{R'}{\leftarrow}_{[n,\, \sigma,\, l\rightarrow r]}\; t \;{}_{E}{\leftrightarrow}_{[h,\, \sigma,\, g\rightarrow d]}\; t'\rangle$ $\exists$ W $\in$ B(A'): W ${}_{E}{\lessdot}{\approx}$ A. The only-if part is now trivial, because coherence pairs have the form of A.
For the if-part, we show ${}_{E}\lessdot$-subconnectedness.

1) h and n are disjoint; we then have default subconnectedness.

2) For the remaining cases, one occurrence is prefix of the other. If neither occurrence is ε, we strip the context of the smaller occurrence from all terms in the rewriting ambiguity A. This gives us a rewriting ambiguity A', for which we shall construct a proof W' ${}_{E}{\lessdot}{\approx}$ A' below. Adding the stripped context to W' then gives a proof W ${}_{E}{\lessdot}{\approx}$A by stability of ${}_{E}\lessdot$. Note that this argument also holds if we get $\lessdot$-subconnectedness from below.

3) n is a prefix of h (therefore n $= \varepsilon$), and $l\rightarrow r \in Rnl$.
So t ${}_{E}{\leftrightarrow}$ t', hence t' ${}_{Rnl,E}{\rightarrow}_{[n, , l\rightarrow r]}$ t", giving default subconnectedness.

4) n is a prefix of h (therefore n $= \varepsilon$), and $l\rightarrow r \in Rl$, and h $\notin$ G(l).
We have again default subconnectedness, through reduction with a variable prefix.

5) n is a prefix of h (therefore n $= \varepsilon$), and $l\rightarrow r \in Rl$, and h $\in$ G(l).
Here we have a (classical) critical pair by Lemma 5, whose $\lessdot$- or ${}_{E}\lessdot$-subconnectedness immediately implies the $\lessdot$- or ${}_{E}\lessdot$-subconnectedness of our rewriting ambiguity by stability of ${}_{E}\gtrdot$, because there are no extra E-steps.

6) h is a prefix of n (therefore h $= \varepsilon$), and n $\notin$ G(l), thus n $\neq \varepsilon$.
We have default $\lessdot$-subconnectedness through reduction with a variable prefix.

7) h is a strict prefix of n (therefore h $= \varepsilon$), and n $\neq \varepsilon$, and n $\in$ G(g) with $l\rightarrow r \in RL$
The result follows from $\lessdot$- or ${}_{E}\lessdot$-subconnectedness of a classical critical pair of $SCP(Rl, E)$; there are no extra E-steps in this case. A top critical pair is not needed since this is computed in (5).

8) h is a strict prefix of n (therefore h $= \varepsilon$), and n $\neq \varepsilon$, and n $\in$ G(g) with $l\rightarrow r \in Rnl$. So G(g) $\neq \emptyset$.
Note that the case n $= \varepsilon$ is covered in (3). By the E-critical pairs lemma, there is a pair $\langle\langle p, q\rangle\rangle$ $= \langle\langle d\Theta, g[n\leftarrow r]\Theta\rangle\rangle$ in $CSECP(Rnl, E)$ and a substitution τ such that $\sigma \;{}_{E}{=}\; \Theta\tau|_{(\mathcal{V}(g) \cup \mathcal{V}(l))}$; therefore there exists a proof Q' $= \langle p\tau \;{}_{E}{\leftrightarrow}^{*}\; t'\rangle = \langle d\Theta\tau \;{}_{E}{\leftrightarrow}^{*}\; t'\rangle$ with E-applications at occurrences outside of G(d), and a proof Q" $= \langle t'' \;{}_{E}{\leftrightarrow}^{*}\; q\tau\rangle$ (these are indeed finite sequences, i.e. proofs, because E-equivalence classes are finite). Now $\langle\langle p, q\rangle\rangle$ is ${}_{E}\lessdot$-subconnected in A', hence, by stability of ${}_{E}\lessdot$, $\langle\langle p\tau, q\tau\rangle\rangle$ is also ${}_{E}\lessdot$-subconnected in A', say with proof W. Again Q" poses no problems, with Q" $\lessdot$ ⟨t⟩. Now t' $=$ dσ in A has complexity (dσ, $\{d\sigma|_{\varepsilon}\}$), while for t' in Q' we have complexity (dσ, $\{d\sigma|_{h0}\}$), $h_0 \notin$ G(d). As equality steps occur entirely inside the substitution part of d, we can write every other intermediate result u_i in Q" as a substitution instance of d, for some substitution $\sigma_i \;{}_{E}{=}\; \sigma$, i.e. $u_i = d\sigma_i$. This gives $(d\sigma_i, \{d\sigma_i|_{hi}, d\sigma_i|_{ni}\})$ with h_i, $n_i \notin$ G(d), as complexity of an intermediate result u_i. Then $d\sigma \;{}_{E}{=}\; d\sigma_i[d\sigma_i|_{hi}]$, where the

subterm occurrence is strict. Therefore, $d\sigma \;{}_{E}\!\succ\; d\sigma_i|_{hi}$, and, by the same reasoning, $d\sigma|_{\varepsilon} \;{}_{E}\!\succ\; d\sigma_i|_{ni}$, which gives $Q' \;{}_{E}\!\prec\; A$. Then, finally, we get $Q''.W.Q' \;{}_{E}\!\prec\!\approx\; A$, whence A is subconnected in this case, too. Note that if W is a standard subconnecting sequence, then trailing E-applications on the right of W are all at strict subterms of $d\Theta$, so that W.Q' is also a standard sequence □

All subconnecting sequences indeed satisfy the conditions of lemma 8: We never introduce ${}_{E}\!\leftrightarrow$-steps in proofs other than those covered by *Rnl,E*-rewriting, which do not appear in *A'*-proofs, or those which only apply at special positions as dicussed in case 8 above. A formal proof will not be possible until we have presented the completion algorithm itself, but the reasoning can already be outlined: enforcing subconnectedness by making a coherence pair to a rewrite rule gives a standard sequence, because no ${}_{E}\!\leftrightarrow$-steps are introduced into the *A'* subconnecting sequence; and predicting subconnectedness implied by some critical pair will yield a standard sequence as in case (8) above.

LEMMA 10:

Let $R = Rl \cup Rnl$ be an E-terminating set of rules such that Rl is left-linear, a complete and finite unification algorithm exists for the theory E, and E-congruence classes are finite. Furthermore, let $R' = Rl \cup Rnl,E$ be pseudo-E-coherent.
Then $R' = Rl \cup Rnl,E$ is locally pseudo-E-confluent with R in A' iff all *confluence pairs* <<p, q>> in $SCP(Rl, Rl) \cup SCP(Rl, Rnl) \cup CSECP(Rnl, Rnl) \cup CSECP(Rnl, Rl)$ are subconnected in A'.

PROOF: By definition, R' is locally pseudo-E-confluent in A' iff $\forall$ A = $\langle t'' \;{}_{R}\!\leftarrow[n, \sigma, l\rightarrow r]\; t_n \;{}_{R'}\!\rightarrow[h, \sigma, g\rightarrow d]\; t'\rangle$ $\exists$ W $\in$ B(R/E): W $\prec\!\approx$ A. The only-if part is now trivial, because confluence pairs have the form of A.
For the if-part, we show $\prec$-subconnectedness.

1) h and n are disjoint; we then have default $\prec$-subconnectedness.

2) For the remaining cases, one occurrence is prefix of the other. If neither occurrence is ε, we strip the context of the smaller occurrence from all terms in the rewriting ambiguity A. This gives us a rewriting ambiguity A', for which we shall construct a proof W' $\prec\!\approx$ A' below. Adding the stripped context to W' then gives a proof W $\prec\!\approx$A by stability of $\prec$.

3) n = ε. If we have reduction with a variable as prefix we get default $\prec$-subconnectedness as usual. The remaining case is proved through the $\prec$-subconnectedness of a classical critical pair (in $SCP(Rl, Rl)$ or $SCP(Rl, Rnl)$) if ${}_{R'}\!\rightarrow$ is ${}_{Rl}\!\rightarrow$, and through the $\prec$-subconnectedness of an E-critical pair (in $CSECP(Rnl, Rnl)$ or $CSECP(Rnl, Rl)$) if ${}_{R'}\!\rightarrow$ is ${}_{Rnl,E}\!\rightarrow$. In this case, top critical pairs are indeed necessary.

4) h = ε and n $\neq$ ε. If we have reduction with a variable as prefix we get default $\prec$-subconnectedness as usual. If ${}_{R'}\!\rightarrow$ is ${}_{Rl}\!\rightarrow$, the proof is again by the $\prec$-subconnectedness of a classical critical pair (in $SCP(Rl, Rl)$ or $SCP(Rnl, Rl) \subseteq CSECP(Rnl, Rl)$). If ${}_{R'}\!\rightarrow$ is ${}_{Rnl,E}\!\rightarrow$, the E-critical pair lemma does not apply, and we use the pseudo-E-coherence property. We have A = P.M.Q = $\langle t'' \;{}_{R}\!\leftarrow[n, \sigma, l\rightarrow r]\; t_n\rangle.\langle t_n \;{}_{E}\!\leftrightarrow^{*}\; t\rangle.\langle t \;{}_{R}\!\rightarrow[h, \sigma, g\rightarrow d]\; t'\rangle$. If M = $\langle\rangle$, we must have $t_n = t$, and we get $\prec$-subconnectedness as in case (3). Otherwise pseudo-E-coherence yields a proof p' $\prec\!\approx$ P.M, whence p'.Q $\prec\!\approx$ A □

THEOREM 2:

Let $R = Rl \cup Rnl$ be an E-terminating set of rules such that Rl is left-linear, a complete and finite unification algorithm exists for the theory E, and E-congruence classes are finite. Then R is

Church-Rosser modulo E (in $Rl \cup Rnl, E$) iff
All *confluence pairs* <<p, q>> in *SCP(Rl, Rl)* ∪ *SCP(Rl, Rnl)* ∪ *CSECP(Rnl, Rnl)* ∪ *CSECP(Rnl, Rl)* are R'-pseudo-confluent modulo E (pseudo-E-confluent in R').
All *coherence pairs* <<p, q>> in SCP(Rl, E) ∪ SCP(E, Rl) ∪ CSECP(Rnl, E) are R'-pseudo-confluent modulo E (pseudo-E-confluent in R').

PROOF: For the only-if part, we first remark that ${}_{R/E}\!\rightarrow \subseteq \succ$. Now let A = $\langle x\ {}_{R'}\!\leftarrow y\ {}_{E}\!\leftrightarrow z\rangle$ where <<x, z>> is a coherence pair. Then there exists a proof V ∈ $Bv_E(R')$, V ≈ A. So V = $\langle x\ {}_{R'}\!\rightarrow^* t_1\rangle.\langle t_1\ {}_{E}\!\leftrightarrow^* t_2\rangle.\langle t_2\ {}_{R'}\!\leftarrow^* z\rangle$, where the subproof $\langle t_2\ {}_{R'}\!\leftarrow^* z\rangle$ cannot be empty or trivial lest ${}_{R/E}\!\rightarrow$ were not Noetherian. So V ⋖ A, because y ≻ t_i for all t_i ∈ V - {x, z}. The case of confluence pairs is completely analogous.

For the if-part, we have local pseudo-E-coherence in R' by lemma 9, and hence pseudo-E-coherence by lemma 1 and its corollary. From lemma 10 we then get local pseudo-E-confluence, whence Theorem 1 (EGBNL) concludes the proof □

COROLLARY: [Jo&Ki 84]

Let $R = Rl \cup Rnl$ be an E-terminating set of rules such that Rl is left-linear, a complete and finite unification algorithm exists for the theory E, and E-congruence classes are finite. Then the R''-Church-Rosser property is decidable for every R'' with $R \subseteq R' \subseteq R'' \subseteq R/E$.

PROOF: According to Theorem 2, finite tests on finitely many critical pairs imply the Church-Rosser property in R' modulo E, which implies the Church-Rosser property in R'' modulo E by $R' \subseteq R''$. Now assume A is Church-Rosser modulo E in R''. Then all critical pairs are confluent modulo E in R'', i.e., for every <<p, q>> there are unique R''-normal forms t_1, t_2 s. th. $t_1\ {}_{E}\!= t_2$. Now the critical pairs of R' are contained in those of R'' by $R' \subseteq R''$, and R'-normal forms are the same as R''-normal forms, whence the pairs of R' are all confluent □

4 Completion Modulo Equations with Subconnectedness Criteria

4.1 Subconnectedness Criteria

For Theorem 2 to be of any practical use, we must now demonstrate that we can efficiently test for subconnectedness of critical pairs. Our method is based on two abstract tests, which yield practical criteria by restricting their application to situations where it is guaranteed that the preconditions will eventually be fulfilled. In practice we shall not even exhaust the theoretical possibilities, but resort to applying more restricted criteria which capture the vast majority of all cases at reasonable cost.

To give some intuition, we first we recall from [Kü 86] the pseudo-confluence criterion for empty E.

LEMMA : (Basic Subconnectedness Criterion)

Let A = $\langle x \; {}_{R}{\leftarrow}[\varepsilon, \mu, L \to R] \; z \; {}_{R}{\to}[h, \mu, g \to d] \; y\rangle \in B(R)$ be a rewriting ambiguity with an mgu μ such that $\langle\langle x, y\rangle\rangle$ is the critical pair, and let $\langle z \; {}_{R}{\to}[m, \tau, l \to r] \; t\rangle$. Then $\langle\langle x, y\rangle\rangle$ is subconnected (in R) if all critical pairs that exist between $\langle L \to R\rangle$ and $\langle l \to r\rangle$ (and $\langle l \to r\rangle$ and $\langle L \to R\rangle$), and between $\langle l \to r\rangle$ and $\langle g \to d\rangle$ (and $\langle g \to d\rangle$ and $\langle l \to r\rangle$), are subconnected.

PROOF: A subconnecting sequence for A is obtained from the concatenation of two proofs m'_1 and m'_2 which subconnect the proofs $m_1 = \langle x \; {}_{R}{\leftarrow}[\varepsilon, \mu, L \to R] \; z \; {}_{R}{\to}[m, \tau, l \to r] \; t\rangle$ and $m_2 = \langle t \; {}_{R}{\leftarrow}[m, \tau, l \to r] \; z \; {}_{R}{\to}[h, \mu, g \to d] \; y\rangle$, respectively. By the case analysis of the relative reduction positions in m_1 and m_2, which is familiar from lemma 10, we have the usual $\lessdot$-subconnectedness due to default cases without critical overlaps, or else due to subconnectedness of classical critical pairs □

For the equational case, we have to consider three types of coherence pairs and four types of confluence pairs. In addition, reduction by the "middle rule" $\langle l \to r\rangle$ can alternatively be in ${}_{Rl}{\to}$ or ${}_{Rnl,E}{\to}$. This gives us 14 different situations which demand due consideration of the usual relative overlap positions. Fortunately, our stronger ordering ${}_{E}{\lessdot}$ enables us to reduce drastically the number of cases to be considered in the criteria. Therefore we shall not go into the details of showing where we can have $\lessdot$-subconnectedness, and where we necessarily depend on ${}_{E}{\lessdot}$-subconnectedness. In general, $\lessdot$-subconnectedness follows from default subconnectedness, from classical critical pairs, and from confluence pairs. The following lemma accomplishes the reduction.

LEMMA 11: (Semi ${}_{E}{\lessdot}$-subconnectedness)

Let A = $\langle x \; {}_{A'}{\leftrightarrow}[n.h, , L \to R] \; z \; {}_{A'}{\leftrightarrow}[n, , g \to d] \; y\rangle \in B(R' \cup E)$, and let $\langle z \; {}_{R'}{\to}[n.m, , l \to r] \; t\rangle$ with $m \neq \varepsilon$. Then there exists A' $\in B(R' \cup E)$, A' ${}_{E}{\lessdot}{\approx}$ A, if there exists a' ${}_{E}{\lessdot}{\approx}$ a = $\langle t \; {}_{R'}{\leftarrow}[n.m, , l \to r] \; z \; {}_{A'}{\leftrightarrow}[n, , g \to d] \; y\rangle$.

PROOF: Let A' = $\langle x \; {}_{A'}{\leftrightarrow}[n.h, , L \to R] \; z \; {}_{R'}{\to}[n.m, , l \to r] \; t\rangle$.a'. Clearly A' $\approx$ A. The complexity of A is CA = $\{(x, \{x|_{n.h}\}), (z, \{z|_{n.h}, z|_{n}\}), (y, \{y|_{n}\})\}$; the complexity of A' is CA' = $\{(x, \{x|_{n.h}\}), (z, \{z|_{n.h}, z|_{n.m}\}), (t, \{t|_{n.m}, t|_{u}\}), \ldots \}$. We have $z|_{n} \; {}_{E}{>} \; z|_{n.m}$, and therefore $(z, \{z|_{n.h}, z|_{n}\}) >_c (z, \{z|_{n.h}, z|_{n.m}\})$. We also have $z > t$ and therefore $(z, \{z|_{n.h}, z|_{n}\}) >_c (t, \{t|_{n.m}, t|_{u}\})$. For the remaining complexities of type $(t_i, \{t_i|_{ni}, t_i|_{ui}\})$ from a' there could only be a problem if $(t, \{t|_{n.m}\}) >_c (t_i, \{t_i|_{ni}, t_i|_{ui}\})$, because the complexities of z and y from a are unchanged in A; however, $t > t_i$

implies $z \succ t_i$, and $\{t|_{n.m}\}\ {}_{E}{\succ}'\ \{t_i|_{ni}, t_i|_{ui}\}$ implies $\{t|_{n.m}, t|_{u}\}\ {}_{E}{\succ}'\ \{t_i|_{ni}, t_i|_{ui}\}$, whence $(z, \{z|_{n.h}, z|_{n}\}) \succ_c (t, \{t|_{n.m}, t|_{u}\}) \succ_c (t_i, \{t_i|_{ni}, t_i|_{ui}\})$. Note that standard subconnectedness of a implies standard subconnectedness of A, because the complexity of x is unchanged □

Elaborating on this proof exhibits a recurring situation in which we always get ${}_{E}{\prec}$-subconnectedness without further preconditions. This observation forms the basis for the composite superposition test in [K&M&N 86], which consequently can be applied without restrictions, and in addition to the test which we shall derive. Its compatibility with existing subconnectedness criteria was first proved in [Ba&De 86]; in the subjoined lemma, we generalize it to rewriting modulo equations.

LEMMA 12: (Composite ${}_{E}{\prec}$-subconnectedness modulo Equations)

Let $A = \langle x\ {}_{A'}{\leftrightarrow}[n, , L\rightarrow R]\ z\ {}_{A'}{\leftrightarrow}[n.h, , g\rightarrow d]\ y\rangle \in B(R'\cup E)$, and let $\langle z\ {}_{A'}{\leftrightarrow}[n.h.m, , l\rightarrow r]\ t\rangle$ with $m \neq \varepsilon$. Then there exists $A' \in B(R'\cup E)$, $A'\ {}_{E}{\prec}{\approx}\ A$.

PROOF: Let $A' = \langle x\ {}_{A'}{\leftrightarrow}[n, , L\rightarrow R]\ z\ {}_{R'}{\rightarrow}[n.h.m, , l\rightarrow r]\ t\ {}_{R'}{\leftarrow}[n.h.m, , l\rightarrow r]\ z\ {}_{A'}{\leftrightarrow}[n.h, , g\rightarrow d]\ y\rangle$. Clearly $A' \approx A$. The complexity of A is $CA = \{(x, \{x|_{n}\}), (z, \{z|_{n}, z|_{n.h}\}), (y, \{y|_{n.h}\})\}$; the complexity of A' is $CA' = \{(x, \{x|_{n}\}), (z, \{z|_{n}, z|_{n.h.m}\}), (t, \{t|_{n.h.m}, t|_{n.h.m}\}), (z, \{z|_{n.h.m}, z|_{n.h}\}), (y, \{y|_{n.h}\})\}$. If $\langle l\rightarrow r\rangle \in R'$, we have $z \succ t$ and $CA'\ {}_{E}{\prec}\ CA$; if $\langle l\rightarrow r\rangle \in E$, we have $z\ {}_{E}{=}\ t$, $z|_{n.h.m}\ {}_{E}{=}\ t|_{n.h.m}$, hence $z|_{n.h}\ {}_{E}{\succ}\ t|_{n.h.m}$, and therefore also $CA'\ {}_{E}{\prec}\ CA$. Again we have standard subconnectedness, because the complexity of x and y is unchanged □

COROLLARY: (Equational KMN Subconnectedness Criterion)

Let $A = \langle x\ {}_{A'}{\leftrightarrow}[n, \mu, L\rightarrow R]\ z\ {}_{A'}{\leftrightarrow}[n.h, \mu, g\rightarrow d]\ y\rangle \in B(A')$ with an mgu μ such that $\langle\langle x, y\rangle\rangle$ is the critical pair, and let $\langle z\ {}_{R'}{\rightarrow}[n.h.m, \tau, l\rightarrow r]\ t\rangle$ with $m \neq \varepsilon$. Then $\langle\langle x, y\rangle\rangle$ is (standard) subconnected in A' □

We are now ready for the equational subconnectedness tests. We state the tests in much more detail than is required for an implementation, in order to have a theoretical basis for more refinements. The basic idea behind the equational tests is the same as for the case of empty equations: we show that the subconnectedness of a critical pair follows from the subconnectedness of other critical pairs. For the test, we find an additional reduction on the superposition of a critical pair, so that we obtain a new proof of the critical pair, like in lemmas 11 and 12, whose left part already forms part of a subconnecting sequence. Conditions on critical pairs of the middle rule with the other rules then assure subconnectedness also of the right part. The task is even simpler for the case of coherence pairs, where the middle rule splits a coherence ambiguity into both a coherence and a rewriting ambiguity. By construction of ${}_{E}{\succ}$, the confluence ambiguity itself is always simpler than the original coherence ambiguity, whence we only have to look at coherence pairs.

LEMMA 13: (Weak Abstract Pseudo-E-Coherence Test)

a) [For $SCP(E, RI)$] Let $A = \langle x\ {}_{E}{\leftrightarrow}[h, \mu, g\rightarrow d]\ z\ {}_{RI}{\rightarrow}[\varepsilon, \mu, L\rightarrow R]\ y\rangle \in B(R'\cup E)$ with an mgu μ such that $\langle\langle x, y\rangle\rangle$ is the critical pair, and let $\langle z\ {}_{R'}{\rightarrow}[m, \tau, l\rightarrow r]\ t\rangle$. Furthermore, let the following critical pair be subconnected (in $R'\cup E$) below the superpositions: if $m = \varepsilon$, any coherence pair between $\langle g\rightarrow d\rangle$ and $\langle l\rightarrow r\rangle$ at position h. Then $\langle\langle x, y\rangle\rangle$ is subconnected (in $R'\cup E$).

b) [For $SCP(Rl, E)$] Let $A = \langle x \;_{Rl}{\leftarrow}[h, \mu, g\rightarrow d]\; z \;_{E}{\leftrightarrow}[\varepsilon, \mu, L\rightarrow R]\; y\rangle \in B(R'\cup E)$ with an mgu μ such that $\langle\langle x, y\rangle\rangle$ is the critical pair, and let $\langle z \;_{R}{\rightarrowtail}[m, \tau, l\rightarrow r]\; t\rangle$. Furthermore, let the following critical pairs be subconnected (in $R'\cup E$) below their superpositions: if $\langle l\rightarrow r\rangle \in Rl$, then any coherence pair that exists between $\langle l\rightarrow r\rangle$ and $\langle L\rightarrow R\rangle$ at position; if $\langle l\rightarrow r\rangle \in Rnl$, then any coherence pairs that exist between $\langle l\rightarrow r\rangle$ and $\langle L\rightarrow R\rangle$ at position m. Then $\langle\langle x, y\rangle\rangle$ is subconnected (in $R'\cup E$).

c) [For $CSECP(Rnl, E)$] Let $A = \langle x \;_{Rnl,E}{\leftarrow}[h, \mu, g\rightarrow d]\; z \;_{E}{\leftrightarrow}[\varepsilon, \mu, L\rightarrow R]\; y\rangle \in B(R'\cup E)$ with an mgu μ such that $\langle\langle x, y\rangle\rangle$ is the critical pair, and let $\langle z \;_{R}{\rightarrowtail}[m, \tau, l\rightarrow r]\; t\rangle$ (we always have $h \neq \varepsilon$). Furthermore, let the following critical pairs be subconnected (in $R'\cup E$) below their superpositions: if $\langle l\rightarrow r\rangle \in Rl$, then any coherence pair that exists between $\langle l\rightarrow r\rangle$ and $\langle L\rightarrow R\rangle$ at position m; if $\langle l\rightarrow r\rangle \in Rnl$ and $m \neq \varepsilon$, then any coherence pairs in $CSECP(\langle l\rightarrow r\rangle, m, \langle L\rightarrow R\rangle)$. Then $\langle\langle x, y\rangle\rangle$ is subconnected (in $R'\cup E$).

PROOF: By the "middle rule" $l\rightarrow r$, a coherence pair is split into both a coherence ambiguity and a confluence ambiguity. Standard subconnectedness of the parts is by default if there are non-critical overlaps; it also follows, by lemma 11 and the case analysis of lemmas 9 and 10, from the required standard subconnectedness of the coherence pairs, if these exist. The concatenation is again a standard subconnecting sequence if both parts are standard. We now show that we need not consider confluence pairs.

In case a), we have $\{(z, \{(e, z|_h), (r, z)\})\} \;_{E}{\gg}\; \{(t, \{(-, -), (-, -)\}), (z, \{(r, z|_m), (r, z)\}), (y, \{(-, -)\})\}$, no matter what the reduction subterms of t and y are, because $z \succ t$, $z \succ y$, and because $(e, z|_h) \;_{E}{\succ}\; (r, z|_m)$ since the mode changes from e to r. If $m \neq \varepsilon$, we have also $\{(z, \{(e, z|_h), (r, z)\})\} \;_{E}{\gg}\; \{(z, \{(e, z|_h), (r, z|_m)\})\}$, so that $\langle x \;_{E}{\leftrightarrow}\; z \;_{Rl}{\mapsto}\; y\rangle \;_{E}{\gg}\; \langle x \;_{E}{\leftrightarrow}\; z \rightarrow t\rangle.\langle t \leftarrow z \;_{Rl}{\mapsto}\; y\rangle$; If $m = \varepsilon$, we need to assume subconnectedness of the corresponding coherence pair.

The remaining cases are justified analogously □

LEMMA 14: (Weak Abstract Pseudo-E-Confluence Test)

a) [For $SCP(Rl, Rl)$] Let $A = \langle x \;_{Rl}{\leftarrow}[h, \mu, g\rightarrow d]\; z \;_{Rl}{\mapsto}[\varepsilon, \mu, L\rightarrow R]\; y\rangle \in B(R'\cup E)$ with an mgu μ such that $\langle\langle x, y\rangle\rangle$ is the critical pair, and let $\langle z \;_{R}{\rightarrowtail}[m, \tau, l\rightarrow r]\; t\rangle$. Furthermore, let the following critical pairs be subconnected (in $R'\cup E$) below their superpositions: if $\langle l\rightarrow r\rangle \in Rl$, then any confluence pair that exists between $\langle l\rightarrow r\rangle$ and $\langle L\rightarrow R\rangle$ at position m, and, if $m = \varepsilon$, any confluence pair between $\langle g\rightarrow d\rangle$ and $\langle l\rightarrow r\rangle$ at position h. If $\langle l\rightarrow r\rangle \in Rnl$, then any confluence pairs in $CSECP(\langle l\rightarrow r\rangle, m, \langle L\rightarrow R\rangle)$; if in addition $m = \varepsilon$ and $h = \varepsilon$ then any confluence pairs in $CSECP(\langle l\rightarrow r\rangle, \varepsilon, \langle g\rightarrow d\rangle)$, else if $m = \varepsilon$ and $h \neq \varepsilon$ then let $\langle g\rightarrow d\rangle$ be coherent, and let all confluence pairs of its coherence rules with $\langle l\rightarrow r\rangle$ be subconnected (we do not know which one applies directly at l), as well as any confluence pair in $SCP(\langle g\rightarrow d\rangle, h, \langle l\rightarrow r\rangle)$. Then $\langle\langle x, y\rangle\rangle$ is subconnected (in $R'\cup E$).

b) [For $SCP(Rl, Rnl)$] Let $A = \langle x \;_{Rl}{\leftarrow}[h, \mu, g\rightarrow d]\; z \;_{Rnl}{\mapsto}[\varepsilon, \mu, L\rightarrow R]\; y\rangle \in B(R'\cup E)$ with an mgu μ such that $\langle\langle x, y\rangle\rangle$ is the critical pair, and let $\langle z \;_{R}{\rightarrowtail}[m, \tau, l\rightarrow r]\; t\rangle$. Furthermore, let the following critical pairs be subconnected (in $R'\cup E$) below their superpositions: if $\langle l\rightarrow r\rangle \in Rl$, then any confluence pair that exists in $SCP(\langle l\rightarrow r\rangle, m, \langle L\rightarrow R\rangle)$, and, if $m = \varepsilon$, any confluence pair between $\langle g\rightarrow d\rangle$ and $\langle l\rightarrow r\rangle$ at position h. If $\langle l\rightarrow r\rangle \in Rnl$, then any confluence pairs in $CSECP(\langle l\rightarrow r\rangle, m, \langle L\rightarrow R\rangle)$; if in addition $m = \varepsilon$ and $h = \varepsilon$, then any confluence pairs in

$\mathit{CSECP}(\langle l\to r\rangle, \varepsilon, \langle g\to d\rangle)$, else if $m = \varepsilon$ and $h \neq \varepsilon$ then let $\langle g\to d\rangle$ be coherent, and let all confluence pairs of its coherence rules and $\langle l\to r\rangle$ be subconnected as well as all confluence pairs in $\mathit{SCP}(\langle g\to d\rangle, h, \langle l\to r\rangle)$. Then $\langle\langle x, y\rangle\rangle$ is subconnected (in $R'\cup E$).

c) [For $\mathit{CSECP}(Rnl, Rnl)$] Let $A = \langle x \;_{Rnl,E}{\leftarrow}_{[h,\, \mu,\, g\to d]}\; z \;_{Rnl,E}{\to}_{[\varepsilon,\, \mu,\, L\to R]}\; y\rangle \in B(R'\cup E)$ with an mgu μ such that $\langle\langle x, y\rangle\rangle$ is the critical pair, and let $\langle z \;_{R'}{\to}_{[m,\, \tau,\, l\to r]}\; t\rangle$. Furthermore, let the following critical pairs be subconnected (in $R'\cup E$) below their superpositions: if $\langle l\to r\rangle \in Rl$, and $m \neq \varepsilon$, then let $\langle l\to r\rangle$ be coherent, and let all confluence pairs of its coherence rules and $\langle L\to R\rangle$ be subconnected as well as any confluence pair that exists in $\mathit{SCP}(\langle l\to r\rangle, m, \langle L\to R\rangle)$, else, if $m = \varepsilon$, let any confluence pairs in $\mathit{CSECP}(\langle L\to R\rangle, \varepsilon, \langle l\to r\rangle)$ and $\mathit{CSECP}(\langle g\to d\rangle, h, \langle l\to r\rangle)$ be subconnected. If $\langle l\to r\rangle \in Rnl$, then let all confluence pairs in $\mathit{CSECP}(\langle l\to r\rangle, m, \langle L\to R\rangle)$ be subconnected, and, if in addition $m = \varepsilon$ and $h = \varepsilon$, all confluence pairs in $\mathit{CSECP}(\langle g\to d\rangle, h, \langle l\to r\rangle)$, else, if $m = \varepsilon$ and $h \neq \varepsilon$, then let $\langle g\to d\rangle$ be coherent, and let all confluence pairs of its coherence rules and $\langle l\to r\rangle$ be subconnected as well as any pairs in $\mathit{CSECP}(\langle g\to d\rangle, h, \langle l\to r\rangle)$. Then $\langle\langle x, y\rangle\rangle$ is subconnected (in $R'\cup E$).

d) [For $\mathit{CSECP}(Rnl, Rl)$] Let $A = \langle x \;_{Rnl,E}{\leftarrow}_{[h,\, \mu,\, g\to d]}\; z \;_{Rl}{\to}_{[\varepsilon,\, \mu,\, L\to R]}\; y\rangle \in B(R'\cup E)$ with an mgu μ such that $\langle\langle x, y\rangle\rangle$ is the critical pair, and let $\langle z \;_{R'}{\to}_{[m,\, \tau,\, l\to r]}\; t\rangle$. Furthermore, let the following critical pairs be subconnected (in $R'\cup E$) below their superpositions: if $\langle l\to r\rangle \in Rl$, then any confluence pair that exists in $\mathit{SCP}(\langle l\to r\rangle, m, \langle L\to R\rangle)$, and, if $m = \varepsilon$, then all confluence pairs in $\mathit{CSECP}(\langle g\to d\rangle, h, \langle l\to r\rangle)$. If $\langle l\to r\rangle \in Rnl$, then let all confluence pairs in $\mathit{CSECP}(\langle l\to r\rangle, m, \langle L\to R\rangle)$ be subconnected, and, if in addition $m = \varepsilon$ and $h = \varepsilon$, all confluence pairs in $\mathit{CSECP}(\langle g\to d\rangle, h, \langle l\to r\rangle)$, else, if $m = \varepsilon$ and $h \neq \varepsilon$, then let $\langle g\to d\rangle$ be coherent, and let all confluence pairs of its coherence rules and $\langle l\to r\rangle$ be subconnected as well as any pairs in $\mathit{CSECP}(\langle g\to d\rangle, h, \langle l\to r\rangle)$. Then $\langle\langle x, y\rangle\rangle$ is subconnected (in $R'\cup E$).

PROOF: By Lemma 11 we need never consider overlaps between the left and the middle rule except when the middle rule applies on the top, and by Lemma 12 we need never consider cases where h is a strict prefix of m. By the case analysis of lemmas 9 and 10, subconnectedness then follows from the required subconnectedness of the critical pairs if it is not already by default. If $E = \emptyset$, cases a and b specialize to the classical critical pair criterion. For all cases where we have to assume coherence, note that for equational overlaps there exists a whole set of superpositions, which are all E-equal. If the middle rule matches the superposition to which the side rules apply without E-steps, we do not need to assume coherence, but instead subconnectedness of the respective critical pair, if any. This will be essential for Lemma 15. For case (c) and $_{Rnl,E}{\to}$ rewriting by the middle rule at ε, observe that critical pairs in $\mathit{CSECP}(\langle g\to d\rangle, h, \langle l\to r\rangle)$ do not cover the cases where there are E-steps above the overlap position, so that again we have to assume coherence, and subconnectedness of the critical pairs of the coherence rule which applies directly at $\langle l\to r\rangle$.

As an example, we prove case (a) with $_{Rnl,E}{\to}$ rewriting by the middle rule at ε and $h \neq \varepsilon$:
From $A = \langle x \;_{Rl}{\leftarrow}_{[h,\, \mu,\, g\to d]}\; z \;_{Rl}{\to}_{[\varepsilon,\, \mu,\, L\to R]}\; y\rangle$ and $\langle z \;_{Rnl,E}{\to}_{[\varepsilon,\, \tau,\, l\to r]}\; t\rangle$ we get $B = p.q = \langle x \;_{Rl}{\leftarrow}_{[h,\, \mu,\, g\to d]}\; z \;_{Rnl,E}{\to}_{[\varepsilon,\, \tau,\, l\to r]}\; t\rangle.\langle t \;_{Rnl,E}{\leftarrow}_{[\varepsilon,\, \tau,\, l\to r]}\; z \;_{Rl}{\to}_{[\varepsilon,\, \mu,\, L\to R]}\; y\rangle$, $B \approx A$. We can immediately subconnect q by default or a critical pair in $\mathit{CSECP}(\langle l\to r\rangle, \varepsilon, \langle L\to R\rangle) \subseteq \mathit{CSECP}(Rnl, Rnl)$; so let $q' \lessdot q$. If the middle rule applies without E-steps, we get similarly $p' \lessdot p$, and hence $p'.q' \lessdot B$. Otherwise we make the E-steps explicit in $B' = r.s.q' = \langle x \;_{Rl}{\leftarrow}_{[h,\, \mu,\, g\to d]}\; z \;_{E}{\leftrightarrow}^{*}\; z'\rangle.\langle z' \;_{Rnl}{\to}_{[\varepsilon,\, \tau,\, l\to r]}\; t\rangle.q'$, where $B' \approx B$. We subconnect r by the coherence assumption, obtaining $r' = \langle x \;_{A'}{\leftrightarrow}^{*}\; x' \;_{R'}{\leftarrow}_{[,\, ,\, g'\to d']}\; z'\rangle$, where $\langle g'\to d'\rangle$ is a coherence rule of $\langle g\to d\rangle$. Now $r'.s.q' = r''$.

$s'.q' = \langle x \; {}_{A'}\!\overset{*}{\leftrightarrow} \; x'\rangle.\langle x' \; {}_{R'}\!\leftarrow_{[\;,\;,\;g'\to d']} \; z' \; {}_{Rnl}\!\to_{[\varepsilon,\;\tau,\;l\to r]} \; t\rangle.q'$, and the remaining confluence ambiguity s' is subconnected by default or by a critical pair between $\langle g'\to d'\rangle$ and $\langle l\to r\rangle$; so we have $s'' \lessdot s'$. Finally, $r'' \lessdot \langle z\rangle$, $s'' \lessdot \langle z'\rangle$ implies $s'' \lessdot \langle z\rangle$, and $q' \lessdot \langle z\rangle$, so that $r''.s''.q' \lessdot A$ □

For implementations it is common practice to create all complete sets of critical pairs between two rules together, so that we do not need to have specific knowledge about certain overlap positions at which critical pairs are subconnected. At present there is no definite answer as to the trade-off between the cost of elaborate testing for preconditions and the additional gains of more specific criteria, which, after all, is a question of good software engineering.

4.2 Completion with Subconnectedness

As we have already seen, Theorem 2 yields a decision procedure for the Church-Rosser property of term-rewriting systems. Certainly, we shall find this property only very rarely in a rewrite system, and it would be most desirable to have some automated means of modifying a given rewrite system R until it is Church-Rosser. Now we know from Theorem 2 a finite number of critical pairs at which the desired property fails, i.e., which R fails to subconnect. So it is natural to amend R by additional rules which are valid consequences of the equational theory R, and which mend those initial defects. Having more rules, however, there may be more critical pairs, i.e. secondary defects which force our process into one more iteration. This is the principle of the completion algorithm devised by D. E. Knuth around 1966 [Kn&Be 70].

One of the simplest ways to close a rewriting ambiguity $\langle x \leftarrow z \rightarrow y\rangle$ is to enforce its local confluence by adding one of the rules $\langle x \rightarrow y\rangle$ or $\langle x \leftarrow y\rangle$. The pair $\langle\langle x, y\rangle\rangle$ may also be normalized first, because $\langle x \rightarrow^{*} x'\rangle.\langle x' \leftrightarrow y'\rangle.\langle y' \leftarrow y\rangle$ also makes it confluent. Now we have seen that it suffices to enforce subconnectedness which locally is more general than confluence. Obviously we cannot expect any gain during a successful Church-Rosser test, because globally the properties are equivalent. Locally, however, subconnectedness is strictly weaker than confluence, and a critical pair of a rewrite system which is not Church-Rosser may well be subconnected when it is not confluent. Therefore, completion with subconnectedness may disregard many critical pairs whose confluence would otherwise be enforced. In practice, these savings are aggravated further: critical pairs are often (inherently) unorderable until they are further reduced at later stages of the completion process; making a wrong ordering decision may lead the completion process into a dead alley requiring backtracking; making an unnecessary ordering decision may require a stronger ordering.

Let us come back to some abstract scheme of completion: we adopt the view of completion as a *proof transformation process* τ: $B \rightarrow B$ on sets of proofs. τ transforms a set of proofs by adding to it subconnecting sequences for all its critical pairs, i.e., $\tau(P) = P \cup S$ s. th. $\forall A \in CP(P) \; \exists p \in S$: $p \; {}_{E}\!\lessdot\!\approx A$. Starting from some initial set P^0, $P^0 = B(A')$ for some axiom system A, we successively compute the sets $\tau(P^i) = P^{i+1}$ until we reach a fixedpoint of the transformation, i.e. until we have $\tau(P^j) = P^j$ for some j.

THEOREM 3: (Fixedpoint Semantics of Abstract Completion)

Let $A = R \cup E$ be a set of axioms. Then $\tau(B(R' \cup E)) = B(R' \cup E)$ iff A is Church-Rosser modulo E in R'.

PROOF: Immediate by Theorem 2 and the definition of τ □

Clearly, S need not contain any subconnecting sequences already in P, so that it is obvious even at the abstract level that we gain efficiency by moving from local confluence to local subconnectedness. Of course, many more improvements are possible on abstract completion. First of all, the overall abstract organization is by no means practicable, because it amounts to a level saturation procedure. In practice, we convert pairs to rules one by one, working with carefully tailored selection strategies, which guarantee that eventually each level will be exhausted.

The fixedpoint approach to completion semantics also brings about a natural ordering on fixedpoints: $P_1 \leq P_2$ iff $P_1 \subseteq P_2$. Now there may be two cases when a fixedpoint P_1 is less than a fixedpoint P_2: P_2 may contain more reductions, but still present the same theory (then the rewrite system generating P_2 cannot be interreduced); or P_2 may contain additional proofs which are no valid consequences of proofs in P_1 (then P_2 represents an extended theory, e.g. a group as opposed to a semi-group).

DEF: We shall write $P \models S$ if all models for the equalities which have proofs in P are also models for the equalities with proofs in S. We call P a *small* fixedpoint of R if $R \models P$ and $\tau(P) = P$. (In [De&Ma 84], a rewrite system R is called Church-Rosser *for* a theory A, if $B(R)$ is a small fixedpoint of A.)

It is now immediate that τ computes small fixedpoints if the basic completion process is *sound*, i.e. it generates only valid proofs. In order to generate a unique least fixedpoint, we have to keep superfluous proof sequences out of the approximations P^i, which means that the respective generating rewrite systems R_i must be interreduced. Moreover, practical experience makes it mandatory to keep rewrite systems interreduced and therefore small in size. This, however, amounts to introducing deletions of reducible rules in the derivation process, which precludes easy monotonicity, so that in turn it becomes harder to prove that the process indeed generates *least* fixedpoints. So we shall conduct a more specific completeness proof in the next section, where we shall also come back to the question of uniqueness of fixedpoints in Theorem 6.

The subconnectedness tests of Lemmas 13 and 14 show essentially that reducible rules are not needed during completion. This is an important means for our understanding of the completion procedure, because after reducing a rewrite rule we immediately face the question whether all future derivations possible with the help of the unreduced object are still possible after its reduction. While this is comparatively easy to see for our positive reduction moves, it is not at all obvious with respect to the negative moves of pair generation, especially since these pairs are in general not reducible themselves.

Why, then, can a reducible rule not generate any essential critical pairs? For the first time, this question was implicitly solved in Huet's correctness proof for the KB-algorithm [Hu 81]. A concise and easy proof is now possible through subconnectedness criteria: assuming coherence, the reducing rule also reduces all superpositions of the reducible rule, so that it can always serve as a middle rule and subconnectedness of its critical pairs implies subconnectedness of all rewriting ambiguities in which the reducible rule takes part. This proof was first given in [Kü 85] for the case of empty E. In [Ba&De 86], an equivalent proof is obtained via a stronger ordering than $\lessdot$.

LEMMA 15: (Justification of intermediate reductions)

Let $\langle L\to R\rangle$ and $\langle l\to r\rangle$ be rules in R such that L or R is R'-reducible by $\langle l\to r\rangle$, and let $\langle g\to d\rangle \in RUE$ be either a rule or an equation. Let all critical pairs between $\langle l\to r\rangle$ and $\langle L\to R\rangle$, and between $\langle l\to r\rangle$ and $\langle g\to d\rangle$ (and $\langle g\to d\rangle$ and $\langle l\to r\rangle$) be subconnected. In addition, let $\langle l\to r\rangle$ be coherent, and let all critical pairs between its coherence rules and $\langle g\to d\rangle$ be subconnected; if $\langle g\to d\rangle \in R$, then let also $\langle g\to d\rangle$ be coherent, and let all critical pairs between its coherence rules and $\langle l\to r\rangle$ be subconnected. Then all critical pairs between $\langle L\to R\rangle$ and $\langle g\to d\rangle$ (and $\langle g\to d\rangle$ and $\langle L\to R\rangle$) are also subconnected.

PROOF: If $\langle l\to r\rangle$ reduces the right-hand side R, then all critical pairs of the unreduced rule reduce to the corresponding critical pairs of the reduced rule, whence the lemma follows from $\succ \supseteq \rightarrow$. Now let $\langle L \;{}_{R'}{\rightarrow}_{[m,\,,\,l\to r]}\; L'\rangle$. We first observe that $\langle\langle L', R\rangle\rangle$ is (E-equal to) a critical pair of $\langle l\to r\rangle$ and $\langle L\to R\rangle$. Let $A = \langle x \;{}_{R'}{\leftarrow}_{[h,\,,\,g\to d]}\; z \;{}_{R'}{\rightarrow}_{[n,\,,\,L\to R]}\; y\rangle \in B(A')$ be associated to the confluence pair

$\langle\langle x, y\rangle\rangle$. Observing that $\langle l\to r\rangle$ applies directly at $\langle L\to R\rangle$, we make the ${}_E\!\leftrightarrow$-steps involved in the application of $\langle L\to R\rangle$ explicit, and we get an equivalent proof A' = p.q = $\langle x \; {}_{R'}\!\leftarrow [h, , g\to d] \; z \; {}_E\!\leftrightarrow^{*} \; z' \; {}_{R'}\!\to [m, , l\to r] \; t\rangle.\langle t \; {}_{R'}\!\leftarrow [m, , l\to r] \; z' \; {}_R\!\to [\varepsilon, , L\to R] \; y\rangle$ which involves $\langle l\to r\rangle$. Now the right part q is subconnected by subconnectedness of the critical pair $\langle\langle L', R\rangle\rangle$, while subconnectedness of the left part p follows from coherence and the subconnectedness of the critical pairs of the coherence rule, as in the proof of Lemma 14. In case A is a coherence ambiguity, subconnectedness of p is immediate by the coherence assumption □

In essence, Lemma 15 tells us that it suffices to create the reduced rule, which is the critical pair between the reducing and the reducible rule, and then continue to work as usual with the reducing rule. Note that this lemma also justifies intermediate reductions on critical pairs: we did not need to assume coherence of the reducible rule, nor the existence of any critical pairs other than that represented by the reduced rule, which we could not establish or create in case we reduce a critical pair prior to its conversion into a rewrite rule.

Of course, we must assure during completion that the coherence rules and their confluence pairs will eventually be created. This is not a trivial endeavour, because we may conceive of a situation where a rule *Rnl,E*-reduces one of its own coherence rules at a subterm. Therefore we follow [Jo&Ki 84] and *protect* coherence pairs against all reductions, thus guaranteeing that they are converted to rules and that their confluence pairs will be created. Note that it makes sense to speak of the left-hand side of a coherence pair, because E-application must result in a $\succ$-larger term than R'-application.

In addition, we adopt the general policy never to remove a reducible rule from a rewrite system in our completion algorithm, because this greatly simplifies the completeness proof. Instead, we merely set a *reducibility flag* on unprotected reducible rules; *flagged* rules then cease to partake in the critical pair generation process, according to the above lemma. In the end, the set of unflagged rules will be shown to comprise the E-unique R/E-rewriting system for the given presentation A and ordering $\succ$; a slightly larger system, essentially including some flagged rules from *Rnl*, will then be even R'-Church-Rosser for A and ordering $\succ$. In practice, one may of course immediately delete those rules that are not needed in the end. On the other hand, they may well aid in the normalization process, especially as long as global coherence is not guaranteed, and they do not burden critical pair generation.

In addition, our generalized equational completion algorithm has a different organization than that in [Jo&Ki 84]. Our tenet is to create as many pairs as possible at any one time, so that a completion strategy have as wide a selection as possible for converting a pair to a rule. At the same time we do not enforce that all pairs be converted to (unmarked) rules, because orientation of pairs may be impossible, especially if a pair is unnecessary for completion.

We take the general view of completion as a producer-consumer process, with pair generation serving as the producer, and pair reduction and orientation as the consumer. The exchange buffer between the two processes is the queue of critical pairs awaiting orientation. We attempt to strengthen the consumer, by reducing stored pairs as much as possible, and to weaken the producer by a suitable selection strategy for prospective new rules and by our critical pair criteria.

$R :=$ GEKB$(A, E, \succ)$

[Generalized Equational Knuth-Bendix Completion Procedure.
$A = A^{*} \cup E$ is a finite set of equations, $\succ$ is a Noetherian E-reduction ordering. A^{*} is $\succ$-orderable, and there exists an E-unification algorithm. If the procedure terminates without failure, R is a Noetherian E-confluent and E-coherent set of rewrite rules for the variety defined by A.]

(1) [Initialize: Q is the queue of critical pairs awaiting conversion to rules, R is the set of rules.]
$Q_0 := A^{*}$; $R_0 := ()$; $\mathrm{i} := 0$; $\mathrm{p} := 0$;

(2) [Find new rule.]

(2.1) [Trivial case.] if $Q_\mathrm{i} = ()$ then $\{R := R_\mathrm{i};$ return$\}$.

(2.2) [Reduce equation.] Select an equation $\mathrm{M} = \mathrm{N}$ in Q_i according to a fair completion strategy. Let $\mathrm{M}\downarrow$ and $\mathrm{N}\downarrow$ be $(Rl_\mathrm{i} \cup Rnl_\mathrm{i}, E)$-normal forms of M and N, respectively, where no reduction takes place on the left-hand side of a protected pair.
if $\mathrm{M}\downarrow {}_{E}{=} \mathrm{N}\downarrow$ then $\{ Q_{\mathrm{i}+1} := Q_\mathrm{i} - \{\mathrm{M} = \mathrm{N}\};\ R_{\mathrm{i}+1} := R_\mathrm{i};\ \mathrm{i} := \mathrm{i}+1;$ goto 2 $\}$
else if $\mathrm{M}\downarrow \succ \mathrm{N}\downarrow$ then $\{ \lambda := \mathrm{M}\downarrow;\ \rho := \mathrm{N}\downarrow \}$
else if $\mathrm{M}\downarrow \prec \mathrm{N}\downarrow$ then $\{ \lambda := \mathrm{N}\downarrow;\ \rho := \mathrm{M}\downarrow \}$ else {return with failure}.

(2.3) [Add new rule.] $\mathrm{p} := \mathrm{p}+1$; Let K be the set of labels k of unprotected rules of R_i whose left-hand side λ_k is reducible by $\lambda \rightarrow \rho$, say to λ'_k. All rules with label $\mathrm{k} \in \mathrm{K}$ are flagged for deletion.
$Q_{\mathrm{i}+1} := Q_\mathrm{i} - \{\mathrm{M} = \mathrm{N}\} \cup \{\lambda_\mathrm{k} = \rho_\mathrm{k} \mid \langle \mathrm{k}{:}\lambda_\mathrm{k} \rightarrow \rho_\mathrm{k} \rangle \in R_\mathrm{i}$ with $\mathrm{k} \in \mathrm{K}\}$;
Let L be the set of labels l of rules of R_i whose right-hand side ρ_l is reducible by $\lambda \rightarrow \rho$, say to ρ'_l. All rules with label $\mathrm{l} \in \mathrm{L}$ are flagged for deletion.
$R_{\mathrm{i}+1} := R_\mathrm{i} \cup \{\langle \mathrm{j}{:}\lambda_\mathrm{j} \rightarrow \rho'_\mathrm{j} \rangle \mid \langle \mathrm{j}{:}\lambda_\mathrm{j} \rightarrow \rho_\mathrm{j} \rangle \in R_\mathrm{i}$ with $\mathrm{l} \in \mathrm{L}\} \cup \{\langle \mathrm{p}{:}\lambda \rightarrow \rho \rangle\}$, where ρ'_j is a normal form of ρ_j using (flagged or unflagged) rules from $R_\mathrm{i} \cup \{\lambda \rightarrow \rho\}$.

(3) [Compute critical pairs]

(3.1) [Compute superpositions.] Let $S = ()$. For each unflagged rule in R_i with label $\mathrm{j} \leq \mathrm{p}$ let $S = S \cup \{$all superpositions between rule p and j (and j and p)$\}$.

(3.2) [Subconnectedness test.] For each superposition $\mathrm{s} = SP(\mathrm{r}_{\mathrm{k'}}, \mathrm{q}, \mathrm{r}_{\mathrm{k''}})$ in S do
{if any rule in R_i with label j matches s at position u then
{if, for each critical pair with origination information (n, v, m) that must be subconnected (according to Lemmas 9 and 10) in order for $CP(\mathrm{r}_{\mathrm{k'}}, \mathrm{q}, \mathrm{r}_{\mathrm{k''}})$ to be subconnected, $(\mathrm{n}, \mathrm{v}, \mathrm{m}) \ll (\mathrm{k'}, \mathrm{q}, \mathrm{k''})$ according to a well founded partial ordering $\ll$, then $S := S - \mathrm{s}$ } }.

(3.3) [Create critical pairs.] Let $Q_{\mathrm{i}+1}$ be Q_i, augmented by the set of critical pairs, with origination information attached, computed from the superpositions still in S; all coherence pairs are protected against reductions on the left-hand side. $\mathrm{i} := \mathrm{i}+1$; goto 2 □

The AC-completion algorithm of [Jo&Ki 84] is more elaborate than our GEKB, e.g. in its protection scheme. Our algorithm is more general than Jouannaud and Kirchner's algorithm EKB only in that it converts fewer critical pairs to rules, and hence may succeed where the other one failed due to orientation problems. Also, it tests pseudo-E-confluence which locally is strictly more general than confluence modulo E. Let us make the relationship more precise. We may picture GEKB as doing the same as EKB, except for marking some critical pairs as disposable. Then it becomes obvious that for each completion with GEKB there is a completion with EKB that converts exactly the same pairs to rules, but in addition has to reduce to tautologies all the marked pairs. In practice, EKB will often convert some marked pair which may be unnecessary, and may result in an unnecessary abort (the pair may also be necessary, when it is around a second time in unmarked form). Of course, we may also have GEKB fail and EKB succeed, because of different completion sequences, see e.g. [De&Ma 84].

In the following chapter we are going to prove completeness of GEKB. In Chapter 6 we discuss refinements of this agorithm motivated by our findings for the case of empty E. We shall see that for this case it can be specialized to a very efficient procedure by a suitable choice of strategies, which is substantiated by empirical results. The AC-subconnectedness test has been implemented in the REVE system [Ki&Ki 83] (on top of version 3.4), but there the overall organization of completion is different, and empirical results are still inconclusive.

5 Complete Correctness of GEKB

First we show that by equational reasoning with the limit rewriting system constructed by GEKB, plus the equations in E, we can prove exactly the same facts as by equational reasoning with A. Then we shall see that the limit rewriting system is even R'-Church-Rosser, so that purely reductional reasoning (modulo E in R') suffices to prove all equalities valid in A. This also implies completeness of the procedure, i.e. every equality valid under A can be proved by purely reductional reasoning after a finite number of iterations of GEKB. Finally, we shall see that the set of all unflagged rules in the limit rewriting system comprises the unique R/E-Church-Rosser term rewriting system for the theory A with equational part E and ordering $\succ$.

DEF: We denote by R_∞ the limit rewriting system constructed by GEKB; we have $R_\infty = \bigcup_i R_i$ because there are no deletions.

DEF: Let A_1 and A_2 be two sets of equations. We write $B(A_1) \subseteq\approx B(A_2)$ iff $\forall$ P $\in B(A_1)$ $\exists$ Q $\in$ $B(A_2)$: P$\approx$Q; and we write $B(A_1) \approx B(A_2)$ iff $B(A_1) \subseteq\approx B(A_2)$ and $B(A_2) \subseteq\approx B(A_1)$.

Note that $B(A) \approx B(A')$, so that we can work with A' as usual.

LEMMA 16: For a finite set of equations $A = R \cup E$, and $\succ$ an E-reduction ordering, there is an iteration i in GEKB(A, E, $\succ$) such that $B(A') \approx B(R_i' \cup E)$, if GEKB does not abort with failure before.
PROOF: $R = Q_0$. By fairness of the completion strategy, for each equation (l = r) in Q_0 there is an iteration i at which it is converted to a rule or reduced to a tautology. If (l = r) is reduced at all before becoming a rule, say to (l' = r') by the respective proofs p = $\langle l \ {}_{A'}\!\!\leftrightarrow^* l'\rangle$ and q = $\langle r \ {}_{A'}\!\!\leftrightarrow^* r'\rangle$, then $\langle l \ {}_{A'}\!\!\leftrightarrow^* l'\rangle.\langle l' \leftrightarrow r'\rangle.\langle r' \ {}_{A'}\!\!\leftrightarrow^* r\rangle \in B(R_i' \cup E)$. Taking the finite maximum iteration m, we get $B(A') \subseteq\approx B(R_m' \cup E)$. Now of course GEKB is sound, i.e. $B(R_i' \cup E) \subseteq\approx B(A)$, because the new equations generated as critical pairs are valid consequences of their parents by equational reasoning. So $B(R_m' \cup E) \subseteq\approx B(A')$ □

COROLLARY: $B(R'_\infty \cup E) \approx B(A')$ □

In the next theorem, we encounter one more fundamental restriction for Jouannaud and Kirchner's method of completion modulo equations to be complete: the strict subset of the E-subsumption preorder must be well-founded. This is not the case for arbitrary equations, but it holds for all equational theories of practical interest [Jo&Ki 84]. In the following, we shall often write λ_r and ρ_r for respectively the left-hand side and right-hand side of a rule r.

DEF: We write R $\blacktriangleright$ r if r *strictly subsumes* R; it is equivalent to say that r reduces (the left-hand side of) R at the top, but R does not reduce r. We define the reducibility ordering $\angle$ on rewrite rules as r $\angle$ R iff r is applicable at the left-hand side of R, while R is not applicable at the left-hand side of r.

If r $\angle$ R and reducibility is at ε, then R $\blacktriangleright$ r, which we have to assume well-founded. $\angle$ is Noetherian on sets of rewrite rules in which no two left-hand sides are E-equal (modulo a permutation of variables): let $r_0, r_1, \ldots, r_i, r_{i+1}, \ldots$ be an infinite sequence where $\forall$ i $\in$ IN: $r_i \angle r_{i-1}$. Clearly, we cannot have an infinite sequence of $\blacktriangleright$-steps, so we must have an infinite sequence of (inverse) $\angle$-steps interspersed with finite $\blacktriangleright$-sequences. Associated is the sequence of instantiated left-hand sides, i.e. $\lambda_{r0}, \lambda_{r1}\sigma_1, \ldots, \lambda_{ri}\sigma_i, \lambda_{ri+1}\sigma_{i+1}, \ldots$ where $\forall$ i $\in$ IN $\exists$ $u_{i-1} \in O(\lambda_{r(i-1)})$: $\lambda_{r(i-1)}|_{u(i-1)} \ {}_E\!= \lambda_{ri}\sigma_i$, so $\lambda_{r(i-1)} \ {}_E\!\succ \lambda_{ri}\sigma_i$ if u_{i-1} is strict, and $\lambda_{r(i-1)} \ {}_E\!= \lambda_{ri}\sigma_i$ otherwise. Collecting substitutions we get λ_{r0}, $\lambda_{r1}\sigma_1, \lambda_{r2}(\sigma_2\sigma_1), \ldots, \lambda_{ri}(\sigma_i\sigma_{i-1} \ldots \sigma_1), \ldots$. We write τ_i for $(\sigma_i\sigma_{i-1} \ldots \sigma_1)$. By observing that t ${}_E\!\succ$ s implies t' ${}_E\!\succ$ s if t' = t, we factor out E-equivalence classes corresponding to $\blacktriangleright$-runs, e.g. by collapsing them to their first term. So we get an infinite sequence $\lambda_{rk(1)}\tau_{k(1)} \ {}_E\!\succ \lambda_{rk(2)}\tau_{k(2)} \ {}_E\!\succ \ldots$, contradicting well-foundedness of ${}_{E}\rangle$.

THEOREM 4: Let E be such that the strict subset of the E-subsumption preorder is well-founded. Then R_∞ is locally pseudo-E-confluent and locally pseudo-E-coherent iff all critical pairs of only unflagged parent rules are subconnected.

PROOF: The only-if part is trivial. For the if-part we order rules by the reducibility ordering $\angle$. Now let $\langle\langle t_1, t_2\rangle\rangle = CP(r_n, h, r_m) \in CP(R_\infty)$. We proceed by Noetherian induction on $\angle$, assuming that all critical pairs of parent rules $\angle\ r_n$ or $\angle\ r_m$ are already subconnected. If both r_n and r_m are unflagged, $CP(r_n, h, r_m)$ is subconnected by assumption. Now assume only r_n is flagged. Then, by construction of the R_i, there must be a reducing rule r' with r' $\angle\ r_n$, and all confluence pairs of r' and r_m, and r' and r_n, are subconnected by induction hypothesis. Furthermore, all coherence rules of r' and r_m, and r' and r_n, exist in R_∞ by fairness of the completion strategy and because they are protected. Confluence pairs of the unflagged coherence rules and the unflagged r_m are subconnected by assumption. So $CP(r_n, h, r_m)$ is subconnected by Lemma 15. If we have a confluence pair and in addition r_m is flagged, there must be a rule r" $\angle\ r_m$ and we have the following situation (with z = $SP(r_n, h, r_m)$): $\langle t'' \; {}_{R}{\leftarrow}[\,,\,,m]\; x \; {}_{R'}{\rightarrow}[\,,\,,r']\; x' \; {}_{R'}{\leftarrow}[\,,\,,r']\; x \; {}_{E}{\leftrightarrow}^{*}\; z \; {}_{E}{\leftrightarrow}^{*}\; y \; {}_{R'}{\rightarrow}[\,,\,,r'']\; y' \; {}_{R'}{\leftarrow}[\,,\,,r'']\; y \; {}_{R}{\rightarrow}[\,,\,,m]\; t'\rangle$. Here, t" and x' are connected below x by a confluence pair of r', x' and some z" $\prec$ z are connected below z and x by coherence of r', z" and y' are connected below z and y by coherence of r", and y' and t' are connected below y by a confluence pair of r" □

LEMMA 17: (Stability of subconnectedness) Let $\langle x \leftrightarrow^{*} y\rangle$ be subconnected in R_i'. Then $\langle x \leftrightarrow^{*} y\rangle$ is subconnected in each R_j' with $j \geq i$.

PROOF: Immediate, since there are no deletions and $\succ$ does not change in the course of GEKB □

LEMMA 18: For each critical pair of R_∞ there is an iteration i of GEKB at which it is subconnected in B(A_i').

PROOF: If the pair $\langle\langle t_1, t_2\rangle\rangle = CP(r_n, h, r_m)$ is ever created and added to Q, then by fairness we eventually get proofs $\langle t_1 \; {}_{R_i'}{\rightarrow}^{*}\; t'_1\rangle$ and $\langle t_2 \; {}_{R_i'}{\rightarrow}^{*}\; t'_2\rangle$, and in addition either $\langle t'_1 \; {}_{E}{\leftrightarrow}^{*}\; t'_2\rangle$, or $\langle t'_1 \leftrightarrow t'_2\rangle \in$ B(R_i') in the form of a rule which implies default subconnectedness. If the pair is not created because a parent rule is flagged, we have subconnectedness by Theorem 4; if a parent rule is reducible on the right, we have subconnectedness by Lemma 15. Otherwise, the subconnectedness test must have applied. We proceed by Noetherian induction on $\ll$, assuming the hypothesis for each critical pair with origination $\ll$ (n, h, m). Observing that $\ll$ is finitely branching, we immediately get a subconnecting sequence in B(A_j') where j is the maximum of the iterations at which the dependent pairs are subconnected □

COROLLARY: R_∞ is Church-Rosser modulo E in R'_∞ □

THEOREM 5: (Completeness for Validity)

Let $A = R \cup E$ be a finite set of term equations and $\succ$ a Noetherian reduction ordering on R/E. Then $A \models x = y$ iff $\exists\, i \in \mathbb{N}, P \in \mathrm{Bv}_E(R'_i) : P = \langle x \leftrightarrow^{*} y\rangle$ (if GEKB(A, E, $\succ$) does not abort with failure before). Hence the generalized Knuth-Bendix Algorithm modulo equations is a semi-decision procedure for validity in equational varieties.

PROOF: By Birkhoff's completeness theorem we have $A \models x = y$ iff $\exists\, W \in B(A) : W = \langle x \leftrightarrow^{*} y\rangle$. By $A \subseteq A'$, $W \in B(A')$, Lemma 16, and the observation that $R_i \subseteq R_{i+1}$, we get $A \models x = y$ iff $\exists\, W = \langle x$

$\leftrightarrow^*$ y> $\in$ B($R'_\infty \cup E$). By the corollary to Lemma 18, R_∞ is CR, so W $\in$ B($R'_\infty \cup E$) only if $\exists$ V $\in$ Bv$_E$(R'_∞): V$\approx$W. Now each proof in Bv$_E$(R'_∞) is finite, so that there is a finite iteration at which Bv$_E$(R_i') contains V □

Recall that $R \cup E$ is a small fixedpoint of an equational theory A iff $A \models R \cup E$ and R is Church-Rosser modulo E in R'. We may also say that R is R'-CR for A.

LEMMA 19: Let $R \cup E$ be a small fixedpoint of A, and let $\succ$ be a Noetherian reduction ordering on R/E. Let S be a $\succ$-ordered ETRS such that S is coherent, $A \models S$, and $\forall$ <l → r> $\in R$ $\exists$ <g → d> $\in S$, t $\in T$: l $_{S'}\!\!\rightarrow_{[\,,\,,\,g \rightarrow d]}$ t. Then $S \cup E$ is a small fixedpoint of A.

PROOF: Let $A \models$ (t_1 = t_2). Since R is R'-CR for A, there exists W = <t_1 $\leftrightarrow^*$ t_2> $\in$ Bv$_E$(R'). We show that there exists V$\approx$W, V $\in$ Bv$_E$(S'). G = $R \cup S$ is Noetherian modulo E because R and S are commonly $\succ$-ordered, so that we can use induction on proofs in B($G' \cup E$). (Note that we can actually use induction on $\lessdot$ because we have coherence). We therefore assume that $\forall$ P $\in$ B($G' \cup E$), P $\lessdot$ W $\exists$ V $\in$ Bv$_E$(S'): V$\approx$P. W.l.o.g. W = p.Q, p = <t_1 → x>, p $\in$ Bv$_E$(R'), and so, by our premises, $\exists$ <g → d> $\in S$, y $\in T$: t_1 $_{S'}\!\!\rightarrow_{[\,,\,,\,g \rightarrow d]}$ y; but q = <y ← t_1 → x> must be subconnected in $R' \cup E$, say by q' $\lessdot\!\approx$ q, because $A \models S$ and $R \cup E$ is a fixedpoint of A. Clearly, q' $\lessdot$ p and by embedding q'.Q $\lessdot$ p.Q = W, whence by hypothesis $\exists$ V $\in$ Bv$_E$(S'), q'.Q $\approx$ V. Now finally <t_1 → y>.V $\in$ Bv$_E$(S') is equivalent to W and in V-form □

Motivated by the following uniqueness result, which is apparently due to Lankford and Ballantyne [La&Ba 83] (see also [De&Ma 84]), we call a Church-Rosser rewrite system *canonical* if it is also interreduced. More precisely, R is a canonical rewrite system modulo E for an equational theory A, if $A \models R \cup E$, and A is Church-Rosser in R/E.

THEOREM 6: (Uniqueness of canonical term-rewriting systems modulo E)

Let R_1 and R_2 be canonical term-rewriting systems modulo E for an equational theory A, and let them be ordered by the same E-reduction ordering $\succ$. Then $R_1 \;_E\!= R_2$.

PROOF: [Jo&Ki 84] □

COROLLARY: Let $\succ$ be a Noetherian E-reduction ordering. Let R be a canonical $\succ$-ordered ETRS for an equational theory A, and S a finite, interreduced, $\succ$-ordered ETRS s.th. $A \models S$, S' is coherent, and all rules in R are S'-reducible on the left-hand side. Then $S \;_E\!= R$ □

The corollary is of limited interest, because usually S is not interreduced if S' is coherent. However, S' is always coherent if E is empty.

LEMMA 20: Any R'-Church-Rosser set of rewrite rules contains a unique set S of rewrite rules which is Church-Rosser in S/E.

PROOF: [Jo&Ki 84] □

THEOREM 7: (Completeness for Canonicity)

Let A = $R \cup E$ be a finite set of term equations s. th. E-equivalence classes are finite and E-subsumption is well founded, $\succ$ a Noetherian reduction ordering on R/E, and S a finite $\succ$-ordered canonical ETRS for A. Then (if GEKB does not fail before) GEKB terminates on (A, E, $\succ$) with result $R_\infty \supseteq S$, where R_∞ is Church-Rosser in R'_∞. Furthermore, S is E-equal to a subset of the set of unflagged rules in R.

PROOF: By the finiteness of S and completeness of GEKB for validity, there exists i ∈ IN s.th. $\mathrm{Bv}_E(R_i')$ contains proofs for all rules in S. Now R_i' must reduce the left-hand side of each rule in S, because otherwise $\succ$ cannot be Noetherian; then, by Lemma 19, any $R \supseteq R_i$ is CR if R' is coherent. Now R_i' will in general not be coherent, but, as E-equivalence classes are finite, there are only finitely many coherence pairs whose subconnectedness would mend the deficiency. Hence, by protection of coherence pairs and fairness of completion, there must be an iteration j $\geq$ i such that all coherence pairs of R_i are subconnected in R_j, and hence $R_j \supseteq R_i$ is CR in R_j', whence $R_j = R_\infty$. By construction, the set F of unflagged rules in R_∞ must reduce the left-hand side of each rule in R_∞, so again by Lemma 19, F is CR if it is coherent. Taking an interreduced subset F^* of F, we get $F^* {}_E{=}\ S$ from the corollary to Lemma 19 and Theorem 6, since by construction F is ordered by $\succ$, and by definition F^*/E is coherent □

Note that for empty E there are no coherence pairs and therefore no protected rules. Therefore, F itself is interreduced so that the unflagged rules in the limit rewrite system computed by GEKB(A, $\emptyset$, $\succ$) comprise the unique canonical rewrite system for (A, $\emptyset$, $\succ$).

COROLLARY: GEKB remains complete when rules are deleted instead of being flagged, and in the following cases protected rules are deleted while their reducing rules are in turn protected: any rule in Rl whose left-hand side is R'-reducible, and any rule in Rnl which is Rnl,E-reducible on top, where the reducing rules must not be flagged.

PROOF: We note that under the above conditions deletions of protected rules do not impair coherence, which is still guaranteed by unflagged rules. We have already seen that reducible rules are not needed for critical pair creation, and we note that normal forms of rewrite systems are preserved under deletion of reducible rules, if coherence is invariant □

This is a reformulation of the completeness result in [Jo&Ki 84] for their algorithm, which uses rule-deletions and an even more elaborate protection scheme.

6 Refinements of Abstract Completion

Algorithm GEKB of chapter 4 is still not fully specified, because it does not tell us how to implement the ordering $\ll$ on critical pairs, and because checking the coherence precondition in some of the subconnectedness criteria is not trivial. By presenting GEKB in abstract form, we wanted to facilitate the development of a variety of specializations of the abstract subconnectedness test. We shall discuss below possible realizations that are known so far, some of which have already worked quite well in practice. At present, this discussion cannot possibly be exhaustive, because of limited computational experience, the more so as there are still significantly different opinions about the best overall organization of the completion procedure apart from subconnectedness criteria.

The majority of our empirical results [Kū 85] have been obtained with the ALDES/SAC-2 TC-system, an implementation of the Knuth-Bendix Algorithm for empty E [Kū 82a]. For the case of completion modulo associativity and commutativity (AC), we have modified the Rève system [Ki&Ki 83] by an instance of our abstract test. However, our basis of empirical results is too limited so far to allow definite conclusions as to optimum realizations of the abstract test. All that we claim to have accomplished so far is demonstrating that there are indeed practical ways to implement (subsets of) the test, both for the basic algorithm and for completion modulo AC. (This was still an open question after [Wi 83]). To date, the only other empirical results put to paper are those in [K&M&N 86], which report a deterioration in run-time behaviour after their criterion was added to the basic algorithm, and a rather dramatic speed-up by up to an order of magnitude for the AC-version. While the authors attribute at least part of the latter improvements to the fact that a subconnectedness test may help to weed out superfluous critical pairs generated from AC-unifiers which are (erroneously) not most general, we shall attempt below an explanation for the other more disappointing findings.

We shall take the basic case of empty E as a foundation for our discussion, entering E-specific considerations afterwards. When exploring the potential of the abstract subconnectedness test, we are faced with the decision of how to assure well-foundedness of the dependency ordering $\ll$ on critical pairs. One of the most general features in this respect would be to dynamically grow with each criterion application a directed graph of dependencies, and to restrict applications so that the graph remains acyclic. This has not been tried so far in practice, because it seems comparatively difficult to implement and costly to perfom; instead, we focussed first on ways to build the ordering into the test itself, i.e. to work with a uniformly restricted test with built-in well-foundedness.

From this point of view, the tests of Kapur, Musser, and Narendran on the one hand, and Winkler on the other hand, are both *subconnectedness tests with position restriction*, i.e. they limit the positions in a superposition at which a rewrite by a third-party rule, the *middle rule*, may be attempted. We have already shown that the KMN restriction to strict subterms of the innermost overlap preserves well-foundedness of $\ll$ (because it can then be embedded in ${}_{E}{<}$). As mentioned in [K&M&N 86], this restriction contains the *blocked critical pair test* of Lankford, who conjectured that it would be unnecessary to consider critical pairs whose overlap substitution contains reducible terms. The original proposal of Winkler in [Wi 83] amounted to a subconnectedness test where the middle rule is allowed to match at non-top strict prefixes of the overlap position if two dependent pairs exist. The last restriction is easily lifted, and we can observe that the middle rule partitions the overlap position into two strictly smaller substrings. Now we define $\ll_w$ by (r, p, s) $\ll_w$ (R, q, S) if p is a strict substring of q. Clearly, $\ll_w$ is well-founded, which proves completeness of Winkler's original criterion, and it is apparent that $\ll_w$ could be extended to allow p to be lexicographically smaller than q.

The extended $\ll_w$ coincides with the intuition, that, when starting pair generation by a depth-first scan of overlap positions, we will already have created all the pairs lower in the ordering which we may use to show connectedness of later pairs. This intuition formed the basis of the developments in [Kü 85]. It can be made explicit by an appeal to our knowledge of the exact sequence of pair generation engraved in the algorithm. Pairs are stored in the central queue of the consumer-producer process, and we only apply the connectedness test if all immediately dependent pairs are already in the queue (or have already become rules). By fairness and a simple induction, all transitively dependent pairs will then eventually be confluent.

This *age* restriction on critical pairs is appealing both in theory and in practice: it preserves the full power of Lemma 15 (justification of intermediate reductions), because there are no position restrictions; it is easy to code (some additional 30 lines of code both for Reve and for TC), and it is compatible with one of the most powerful completion strategies known, viz. selection of smallest pairs. The latter point is especially important because of the fundamental impact of completion strategies on the overall behaviour of completion, which is second only to variations in the ordering, and much more important than improvements by subconnectedness. To make the restriction more precise, we represent rules by their labels, i.e. the numbers they get upon creation, and we define the *natural dependency ordering* $<<_n$ by (n, q, m) $<<_n$ (n', p, m') if max(n, m) $\leq$ min(n', m') and max(n, m) < max(n', m'). The *natural completion strategy* selects the least complex critical pair for conversion into a rule.

The natural dependency ordering corresponds to a *rule restriction* on the set of possible matching rules in the subconnectedness tests: we use only those rules for the additional reducibility test, for which we know that all their critical pairs have already been created, provided the order of pair creation is the (natural) one of ascending labels, where pairs are first created between new rule n and rule 1 (and 1 and n) through to n and n-1 (and n-1 and n), and n and itself. The natural completion strategy follows the heuristic to always keep things simple; it has been recommended in [Kü 82] for the Knuth-Bendix Algorithm, in [Bu 70] for the Buchberger-Algorithm, and is known as the unit preference strategy in resolution theorem proving.

Clearly, the size of a superposition s between rules r and R grows in proportion to the sizes of the rules' left-hand sides λ_r and λ_R. On the other hand, the likelihood of a rule r' to match (a subterm of) s grows with the inverse of the size of $\lambda_{r'}$, because $\lambda_{r'}$ must not have more symbols than s in order to match s at all. (Here, intuitively, the size of a term is to be a monotonic function on the number of its symbols; e.g. it may or may not include a count of the variable symbols).

Taking the natural dependency ordering $<<_n$, critical pairs with parent rule 1 are always $<<_n$-least because there are no legal rules to match the superposition, while the larger the minimum label of its parents is, the more rules do we have to test reducibility of a superposition s. So it appears to be advisable to give small labels to those rules with small left-hand sides, because those are less likely to produce reducible superpositions and thus do not suffer from a lack of rules to try reductions with; while those rules with large left-hand sides should be given large labels, so that for their large superpositions (which probably produce unwanted new large rules) we have a great number of small rules with which we can reduce them.

Now, given the natural completion strategy, rules are already likely to be ordered by increasing size, so that our confluence criterion is likely to be applicable quite often. This may explain the relative success of our algorithm even on small examples as compared to the results of [K&M&N 86]. With the KMN criterion, there are no explicit restrictions as to the middle rules, but by the requirement that they match within the overlap subterm, rules with larger left-hand side are in effect excluded, because they cannot match these small subterms. In order to tune the rule restriction so that it effectively excludes large rules that are unlikely to match, pair creation should strictly proceed by ascending size of rules rather than following the somewhat haphazard ordering produced by the natural completion strategy.

So a further refinement of GKB consists in sorting the rules at the end of pair creation in ascending order according to the size of left-hand sides. A new rule is provisionally added after the largest rule, whence pair creation proceeds beginning with the new rule and the smallest old rule, proceeding to larger old rules and ending with the new rule and itself; finally the new rule is inserted at its proper place according to its size.

These considerations lead to yet another completion strategy and, moreover, a quality measure for strategies, which were both first proposed for Buchberger's algorithm in [Bu 79], but went largely unnoticed for Knuth-Bendix implementations: We want to have a maximal Noetherian subset of the "true" dependency relation, in which the rules of R_∞ are the $\ll$-least elements, and of course we want the completion process to follow the $\ll$-graph from the bottom, i.e. to convert to rules only the $\ll$-least critical pairs. The essential question when judging the quality of a completion strategy is thus how accurately it can predict whether a pair is a $\ll$-least element in $CP(R_\infty)$. Enforcing the confluence of any other pairs without need will entail superfluous work, later to be undone through deletions and garbage collections. So an appropriate strategy would be to select for conversion to a rule the pair with associated smallest superposition, which is unlikely ever to be found subconnected by the test.

So far we have applied our subconnectedness test only prior to pair creation. Lemma 15 indicates, however, that we may also remove pairs from the critical pair queue if one of their parents is found reducible. Owing to this result, we may call pairs with a reducible parent rule *flagged pairs*. In terms of the age restriction on pairs, removal of flagged pairs is justified by the observation that by the time the pair representing the reduced rule is fed back into R, all the corresponding unflagged critical pairs are computed.

Thus if we refine any completion strategy to the extent that it converts only unflagged pairs into rules it remains complete (if it was so before). For reductions at left-hand sides this is easily incorporated into GKB when, for each newly flagged rule, we remove all its critical pairs from the critical pair queue. It is powerful in practice because it collects a lot of garbage at negligible cost: no matches are needed whatsoever, and the necessary book-keeping information should be present in an implementation anyway, to allow derivation traces of all lemmas generated during completion.

Lemma 15 also justifies the peculiar way in which we treat rules that are reducible on the right-hand side: we preserve the critical pairs of the unreduced rule, yet continue to produce pairs only with the reduced parent. Now since in this case pairs of the unreduced rule reduce to corresponding pairs of the reduced rule, we create the corresponding new ones very efficiently by simply reducing the existing pairs, and subconnecting the flagged pairs will also implicitly subconnect the unflagged ones (and vice versa). So nothing is lost even for those pairs that were not even created owing to the connectedness test, or those that have already been converted to rules. We can now take every liberty in reducing existing pairs: empirical results with our implementation of GKB support the heuristic to keep intermediate results (i.e. the critical pair queue) maximally reduced, obviating the need for the reduction in step 2.2 before conversion to rules. Apart from minimizing storage requirements, the crucial parameter in theorem proving, this also aids completion strategies that judge pairs by their size, as reported in [Kü 82].

Of course we would also want to remove (or flag for deletion) those pairs that have become rules in the meantime. However, this refinement does not preserve completeness in all those cases where the rule had also been derived in a different way. Since all the equivalent forms would have been reduced before, they must now be recomputed, and in practice this means that all critical pairs of the system must be recomputed. Still, a backtrack of this kind might be promising in tight situations with very many rules.

The last observation is important in practice, because it has repercussions on the overall organization of completion with subconnectedness. In the tradition of Huet's completeness proof [Hu 81], which needed a convenient loop-invariant, some implementations (essentially including Reve) empty the pair queue at each iteration and store critical pairs as (unmarked) rules in the rule-system. There they may immediately partake in reductions and help to normalize the system, but they cannot be removed any more by critical pair criteria. If rule-deletions are frequent in an application, this is quite likely a disadvantage.

Our last refinement is only a special case of the more general principle to apply critical pair criteria also to stored pairs. In practice, this can easily be done if superpositions are stored along with the pairs. Now if we tamper with the pair queue, we are in danger of loosing well-foundedness of the age restriction. This is however not the case for other restrictions. As we have already seen, both $\ll_w$ and ${}_E\lessdot$ are Noetherian, so that the criteria of Winkler and Kapur, Musser, and Narendran can also be applied to stored pairs.

Yet another class of criteria suitable for application to stored pairs is associated with *substitution restrictions* based on the strict part ${}_E\!<$ of the E-subsumption ordering, whose well-foundedness is needed anyway in GEKB, and which is also assured if E is empty. In this class, removal of flagged pairs may be justified by the ordering (r, p, s) $\ll_f$ (R, q, S) if $\{\lambda_r, \lambda_s\} \lessdot_s \{\lambda_R, \lambda_S\}$, where $\lessdot_s$ is the multiset extension of ${}_E\!<$. In the same spirit, we may define the ordering $\ll_s$, where (r, p, s) $\ll_s$ (R, q, S) if $\exists$ u $\in$ $O(SP(\mathrm{R}, \mathrm{q}, \mathrm{S}))$: $SP(\mathrm{r}, \mathrm{p}, \mathrm{s})$ ${}_E\!<$ $SP(\mathrm{R}, \mathrm{q}, \mathrm{S})|_u$, i.e., the superposition SP(r, p, s) is smaller than a subterm of the superposition SP(R, q, S) in ${}_E\!<$. Clearly, $\ll_s$ is Noetherian if the equational theory E is such that ${}_E\!<$ is well-founded. This ordering is close to Winkler's original criterion; it has the same serious disadvantage that it is very expensive to test for, because smaller superpositions must be explicitly created and compared separately. In special completion settings, however, where there is domain dependent knowledge, these objections may not hold; the restriction seems to work very well in the Gröbner basis algorithm [Bu 79].

Let us now look at some empirical data for basic completion with subconnectedness. Based on the system documented in [Kü 82a] (written in the ALDES language for the SAC-2 Computer Algebra system), an experimental implementation was made for the case of empty E, and the effect of several of the refinements were measured with some examples from [Kn&Be 70]. The reduction strategy was *innermost labelled* [Kü82b], the reduction ordering was the Knuth-Bendix ordering, and the natural strategies were used, where the size of a critical pair was taken to be the maximum number of non-variable symbols in its terms. Rules are of course deleted instead of flagged, and their reduced forms are recycled into the system with preference; Q is kept in maximally reduced form.

The first version incorporated what was believed to be the core of the method: the weak test, and, because rule-deletions are frequent on these examples, removal of flagged pairs. Additional code is about 30 lines, practically all for the removal algorithm. The second version in addition strictly ordered rules for pair creation according to the extent, i.e. the number of symbols, of their left-hand sides, again at the cost of some 30 lines of code. The third version, finally, stored superpositions together with the pairs and extended the test to the pair queue. The additional reducibility tests were inserted into an already existing algorithm that looks for pairs reducible by the new rule; of course the new test took precedence as its success allows immediate deletion of the pair. The old removal algorithm of the first version was kept in place because it saves matches, and its applications were not counted.

Note that the dependency ordering of the third version is not well-founded, contrary to the premature statement in [Kü 86], but completion succeeded on our examples. (One counterexample is the system {(1) f(x, x) = = A; (2) f(a, x) = = B; (3) f(x, a) = = C} from [K&M&N 86]). Therefore, the figures give only an approximation on the number of additional deletions that might be expected from an extension of the test to stored pairs.

The subjoined table gives figures for version 1 vs. the original form of KB. (A matching attempt was counted for the *matches* column only if at least the top symbols were equal.)

Example	completion steps	pairs generated	Q maximum	matches	rewrites
left group	14/14	72/ 91	9/12	1894/ 2591	111/204
right group	16/17	89/122	18/21	2798/ 4214	143/290
LR-system	13/15	85/134	15/23	3283/ 6048	164/381
RL-system	21/21	197/282	25/27	14300/21009	443/897

The following table is for version 3 / version 2. The *test* column gives the number of successful applications of the weak test, not counting removal of flagged pairs.

Example	steps	pairs	test	Q max	matches	rewrites
LG	14/14	75/ 72	33/31	8/ 9	2006/ 1949	105/113
RG	16/16	85/ 85	47/42	18/18	2953/ 2799	122/134
LR	13/13	83/ 83	39/36	13/14	3203/ 3232	150/160
RL	21/21	203/203	108/98	18/18	14795/15043	446/465

Total completion times of version 3 / the original KB on a (UNIX) VAX/785 are (in milliseconds):

LG	RG	LR	RL
6640/ 6900	8440/ 8850	8250/ 10070	19250/ 21500

These results are of course very much dependent on the examples. Detecting unnecessary critical pairs is a pruning process on some derivation tree, so that long completion runs will benefit most, while short runs will suffer an additional overhead. The actual savings in run-time will be more substantial in applications where rewriting is more costly, as e.g. in the Gröbner basis algorithm of Buchberger, or in special theories where the test can be built into completion, in that whole classes of critical pairs need not be generated at all.

When working with some non-empty set E of equations, additional problems are caused by the coherence property. It becomes more difficult to check the conditions of the pseudo-E-confluence test which require the existence of a set of coherence rules, which may not be readily accessible from a rewrite rule. Most notably, however, these conditions must also be checked at intermediate rule applications, which now introduce more complex dependencies. Therefore, we must explicitly view interreduction on rules and pairs as applications of subconnectedness criteria, and suitably restrict them in order to preserve well-foundedness of $<<$. In this framework the protection scheme of Jouannaud and Kirchner is already an instance of a restriction scheme, guaranteeing for each rule that its coherence rules are present, and, in the absence of connectedness criteria, that critical pairs of its coherence rules will indeed be generated.

To ensure completeness we might restrict application of subconnectedness criteria to such positions that the coherence preconditions are never needed. We could also further exploit the protection scheme by disallowing application of the subconnectedness test to critical pairs with a protected parent. While protection guarantees that all coherence rules exist, the latter provision then assures even in the presence of a connectedness test that all critical pairs of coherence rules are formed.

If eventual coherence is ensured, much the same arguments apply to completion modulo equations as for basic completion. The tentative experiments with Reve are so far inconclusive; changes in run-time behaviour range from a slight deterioration to a two-fold speed-up on very limited examples. In particular, it requires a major and non-trivial reorganization of the system to incorporate removal of flagged pairs, whose effect could therefore not be tested so far. On the other hand, incorporating the subconnectedness criteria with the natural dependency restriction is fairly easy, and the built-in protection guarantees the coherence conditions.

7 Applications of Subconnectedness

We present two applications of the principle of subconnectedness. First, we show that it gives us a unique opportunity to enforce the Church-Rosser property of ground rewriting systems without requiring confluence on a general level, which has immediate applications on inductive theorem proving. Second, we derive a subsumption criterion for resolution theorem proving which predicts situations where a resolvent of two clauses is eventually going to be subsumed by some other clause derived by later stages of the resolution process.

7.1 A Criterion for Pseudo-Confluence of Ground Critical Pairs

We present a criterion to test for the pseudo-confluence of all ground instances of a critical pair, without enforcing general pseudo-confluence of the pair. We thereby obtain a generalization of the Jouannaud-Kounalis algorithm for theorem proving in initial algebras.

We are interested in proving the confluence of a Noetherian term-rewriting system R on ground terms, henceforth called *ground confluence*. Of course R is ground-confluent if it is confluent, but the converse does not hold, as exemplified by $R = \{+(0, x) == x;\ +(S(x), y) == S(+(x, y));\ +(x, +(y, z)) == +(+(x, y), z)\}$.

DEF: For any two rules, the set of *ground critical pairs* is the set of all critical pairs of all ground instances of the rules. Note that for any two non-ground rules, the set of ground instances of critical pairs is a strict subset of the set of ground critical pairs. A critical pair is *ground pseudo-confluent* if all its ground instances are pseudo-confluent. For convenience we sometimes say that the pair is *ground subconnected* (in R) *below* s.

A trivial adaptation of the Buchberger-Newman Lemma for the ground case shows that a Noetherian rewrite system R is ground confluent iff its ground critical pairs are pseudo-confluent. However there are in general infinitely many ground instances for any two non-ground rules, and therefore it is essential that the condition can be restricted to the ground instances of critical pairs of R itself.

LEMMA:

A term-rewriting system R is ground-confluent if all critical pairs of R are ground pseudo-confluent.

PROOF: Clearly, R is ground-confluent if all ground critical pairs, i.e. critical pairs of ground instances of rules of R, are pseudo-confluent. Now, by the usual lifting argument (see e.g. the semi-lifting lemma for critical pairs in [Kü 85]), a ground critical pair is either by default confluent in R (and hence pseudo-confluent), or it is a ground instance of a critical pair of R □

If a critical pair is not pseudo-confluent, it is obviously still difficult to test for pseudo-confluence of at least all ground instances, because there are in general infinitely many. In a completion environment, the traditional remedy would be to add the critical pair to R as a new rule; but this is unnecessary if the pair really is ground pseudo-confluent. Now our confluence criterion can easily be modified to predict specifically ground pseudo-confluence instead of general pseudo-confluence, and may therefore offer at least a partial solution to the problem.

DEF: A term t is called quasi-reducible by R if all ground-instances of t are reducible by R.

Quasi-reducibility was introduced in [Jo&Ko 85] for a new approach to proving inductive theorems with the Knuth-Bendix Algorithm; this is our main area of application for the following criterion.

THEOREM : (Ground Pseudo-Confluence Criterion)

Let $\langle t_1, t_2\rangle$ be a critical pair between rule r and R of R and let s be the corresponding superposition; let $S \subseteq R$. Then $\langle t_1, t_2\rangle$ is ground pseudo-confluent if s is quasi-reducible by S and all critical pairs between r and R on the one hand and rules in S on the other hand are ground pseudo-confluent.

PROOF: Let $\langle a, b\rangle$ be any ground instance of $\langle t_1, t_2\rangle$; we note that $\langle a, b\rangle$ is the critical pair of two corresponding ground instances r' and R' of r and R, respectively, with superposition s', a ground term. Since s is quasi-reducible, there is a ground instance p' of a rule $p \subseteq S$ which reduces s', say to m. Now $\langle a, m\rangle$ and $\langle m, b\rangle$ are critical pairs of r' and p', and R' and p', respectively; hence they are ground critical pairs of the respective uninstantiated rules; hence, by the semi-lifting argument, they are pseudo-confluent if all ground instances of critical pairs between r and R on the one hand and p on the other hand are ground pseudo-confluent. Now since s' reduces to m, and $<$ is compatible with substitution, the concatenation of the subconnecting chains between a and m, and m and b, also subconnects a and b below s. Repeating the argument for all other ground instances of $\langle t_1, t_2\rangle$ we finish the proof □

Note that a term may well be quasi-reducible while not reducible in general, whence the ground pseudo-confluence criterion may apply where our general pseudo-confluence criterion does not.

Suppose we want to prove equalities in the initial algebra I_A of a set A of equational axioms. The set of valid equalities in I_A contains of course all equalities which are universally valid under A (i.e. in all models of A); in addition, it may contain equalities which are valid only in the initial (standard) model (i.e. if only ground substitutions are allowed). The latter are commonly proved by some kind of induction, and hence alternative proof methods came to be known as *inductionless induction*.

Improving earlier work initiated by Musser, it was shown in [Jo&Ko 85] that a comparatively minor modification of the Knuth-Bendix completion procedure constitutes an inductionless induction method. The key observation there is the usefulness of the concept of quasi-reducibility: rewrite rules which are quasi-reducible on the left-hand side do not change normal forms of ground terms.

THEOREM: (Inductive Validity Criterion, Jouannaud, Kounalis 1985)

Let R be a confluent set of rules, and $l \to r$ a rule where l is quasi-reducible by R. If $R \cup \{l \to r\}$ is also confluent, then $l = r$ is valid in the initial model of R.

PROOF: The ground rewrite system corresponding to $R \cup \{l \to r\}$ is confluent, so all ground instances of l and r have a respective common unique normal form, which must be the same as their respective normal forms under R alone □

This proof reveals that asking for general confluence is really more than we need.

THEOREM (Refined Inductive Validity Criterion):

Let R be a set of rules whose critical pairs are ground pseudo-confluent, and $l \to r$ a rule where l is quasi-reducible by R. If all critical pairs of $\{l \to r\}$ and rules in R are also ground pseudo-confluent, then $l = r$ is valid in the initial model of R.

PROOF: Since all ground instances of critical pairs of R are pseudo-confluent, all ground critical pairs of R are pseudo-confluent by the lemma. Hence R is ground confluent, i.e. each ground term has a unique normal form. By our premises the same holds for $R \cup \{l \to r\}$, where obviously all ground instances of l and r have a respective common normal form. Now these normal forms must be the same as those under R alone, because l is quasi reducible under R. So in the initial model of R, i.e. when there are only ground substitutions, $l = r$ is valid □

Of course, the weaker precondition for the above theorem only makes a difference in practice now that we have a method to test for it. It is easy to see how the corresponding completion algorithm would look like: we take our Generalized Knuth-Bendix Algorithm, add a quasi-reducibility test for left-hand sides of rules, and replace the pseudo-confluence test by the ground pseudo-confluence test.

To give an example of the potential of this method, consider the system $R = \{1)\ +(0, x) == x;\ 2)\ +(S(x), y) == S(+(x, y));\ 3)\ +(x, +(y, z)) == +(+(x, y), z)\}$ from [Fr 86]. We prove its ground confluence by considering overlaps of (1) and (3) and (2) and (3) at positions ε and 2, and overlaps of (3) and (3), at position 2 in $+(x, +(y, z))$. We observe that at position ε the term (and hence every instance) is quasi-reducible. Therefore we can quasi-reduce all overlaps with rule (3) by the "middle rules" (1) and (2) at ε. This eliminates all critical pairs except the ones between (1) and (3), and (2) and (3), at position ε, which turn out to be confluent, so that R is ground-confluent by the criterion. Note that producing the pairs corresponding to overlap position 2 results in an infinite completion sequence.

This example is due to Fribourg, who also presents an improvement of the Jouannaud-Kounalis algorithm that will handle this case. The relative strength of the two approaches is currently under investigation, but we conjecture that the Jouannaud-Kounalis algorithm with ground-pseudo confluence test sketched above will be as powerful as with Fribourg's improvements.

7.2 A Subsumption Criterion for Resolution Theorem Proving

In [Pa 85], it was shown that the resolution method of Robinson and the completion method of Knuth and Bendix are intimately connected. We now present the resolution analogue to our subconnectedness test, a criterion to detect whether the resolvent of any two clauses in a set S is eventually going to be subsumed by some other resolvent in S. In particular, we show that subsumed clauses produce only subsumed resolvents, which yields a syntactic justification of their deletion apart from the usual semantic proof that unsatisfiability is invariant.

We assume the usual environment of resolution theorem proving in first-order predicate calculus and of term-rewriting as in [Pa 85]. In particular, S is a set of clauses in Skolem normal form, hence quantifier free. We do not specifically consider factoring steps, so that our notion of a resolvent of clauses C and D includes resolvents of factors of C and of D. Let $E = \{X \vee (Y \vee Z) = (X \vee Y) \vee Z,\ X \vee Y = Y \vee X\}$; by $=_E$ we denote equality modulo E. $R = \{X \vee X \rightarrow X\}$ is a one-rule term-rewrite system; the R/E-normal form of a clause C is denoted by $C \downarrow_R$.

DEF: The clause C_1 *subsumes* the clause C_2 if there is a substitution σ such that either $(C_1\sigma) \downarrow_R =_E C_2$ or $(X \vee C_1)\sigma \downarrow_R =_E C_2$, where X is a variable not otherwise occurring in C_1 or C_2.

So what we have to compute is an AC-match of C_1 (or its extension) onto C_2 followed by removal of duplicate literals. We note that the extension is needed so that we can also detect a subterm of C_2 as an E-instance of C_1; we call this subterm the *focus* of the match. For simplicity, we shall write $(C_1\sigma) \downarrow_R \subseteq C_2$ to denote that C_1 subsumes C_2.

THEOREM: (Subsumption Criterion)

Let $C = C_1 \vee L_C$, $D = D_1 \vee \neg L_D$ be two clauses resolvable on the literals L_C and $\neg L_D$ with m.g.u. μ, and let $SP \downarrow_R = (C_1\mu \vee L_C\mu \vee \neg L_D\mu \vee D_1\mu) \downarrow_R$. Furthermore, let M be a clause (with variables different from those of C and D), which subsumes $SP \downarrow_R$. Then the binary resolvent $R_{CD} = (C_1\mu \vee D_1\mu) \downarrow_R$ is subsumed either by M itself, cr by one of M's descendants under factoring and resolution.

PROOF: By definition of subsumption, there exists a substitution σ such that $(M\sigma)\downarrow_R \subseteq SP\downarrow_R$. We distinguish four cases according to whether $L_C\mu$ or $\neg L_D\mu$ are in the focus of the match. i) If neither $L_C\mu$ nor $\neg L_D\mu$ are in the focus, then it is plain that $(M\sigma)\downarrow_R \subseteq R_{CD}$. ii) Assume now that both $L_C\mu$ and $\neg L_D\mu$ are in the focus of M. Then $M = M_1 \vee L_1 \vee \neg L_2$ and $(L_1\sigma)\downarrow_R = (L_2\sigma)\downarrow_R = L_C\mu = L_D\mu$, where for L_1 and $\neg L_2$ we take the subsets (disjunctions) of literals in M which are unified by σ and matched onto $L_C\mu$ and $\neg L_D\mu$, respectively. Here σ and μ can be merged into a common substitution μ' because the variables are disjoint. Clearly, L_1 and L_D unify, say with m.g.u. δ, and $\mu' = \delta\tau$. Similarly, L_2 and L_C unify, say with γ, and $\mu' = \gamma\tau'$. So both M and C, and M and D, have resolvents $R_{MC} = (C_1\gamma \vee M_1\gamma \vee L_1\gamma)\downarrow_R$ and $R_{MD} = (D_1\delta \vee M_1\delta \vee \neg L_2\delta)\downarrow_R$, respectively. (Note that this may include factoring steps if L_1 or $\neg L_2$ represent more than one literal). Now $L_1\gamma\tau' = L_1\mu' = L_1\sigma = L_2\sigma = L_2\mu' = L_2\delta\tau$; hence $L_1\gamma$ and $L_2\delta$ unify, and $R'_{MCMD} = (D_1\delta\tau \vee M_1\delta\tau \vee C_1\gamma\tau' \vee M_1\gamma\tau')\downarrow_R$ is an instance of the resolvent R_{MCMD} of R_{MC} and R_{MD}. But $(R'_{MCMD})\downarrow_R = (D_1\mu' \vee M_1\mu' \vee C_1\mu' \vee M_1\mu')\downarrow_R = (D_1\mu' \vee C_1\mu' \vee M_1\mu')\downarrow_R = (D_1\mu \vee C_1\mu \vee M_1\sigma)\downarrow_R = (D_1\mu \vee C_1\mu)\downarrow_R$, the latter because $(M_1\sigma)\downarrow_R \subseteq D_1\mu \vee C_1\mu$. Therefore, there exists a substitution Θ s.th. $(R_{MCMD}\Theta)\downarrow_R \subseteq R_{CD}$, whence R_{CD} is subsumed by R_{MCMD}. iii) Assume that $L_C\mu$, but not $\neg L_D\mu$, is in the focus of M's match on $SP\downarrow_R$. This implies that $M = M_1 \vee L_1$, and that $(L_1\sigma)\downarrow_R = L_C\mu = L_D\mu$, where for L_1 we take the subset of literals in M which are unified by σ and matched onto $L_C\mu$. Again, σ and μ can be merged into μ', and L_1 and L_D unify with some δ, with $\mu' = \delta\tau$, whence M and D have a resolvent $R_{MD} = (D_1\delta \vee M_1\delta)\downarrow_R$. In this case, R_{MD} already subsumes R_{CD} because $R_{MD}\tau = (D_1\delta\tau \vee M_1\delta\tau)\downarrow_R = (D_1\mu' \vee M_1\mu')\downarrow_R = (D_1\mu \vee M_1\sigma)\downarrow_R \subseteq (C_1\mu \vee D_1\mu \vee M_1\sigma)\downarrow_R = (D_1\mu \vee C_1\mu)\downarrow_R$, the latter because $(M_1\sigma)\downarrow_R \subseteq (C_1\mu \vee D_1\mu)\downarrow_R$. Finally, the remaining case iv) is purely symmetric to the one just discussed □

Note that, most importantly, the subsumption criterion does *not* require that the resolvents of M and either C or D have already been created. It is quite sufficient to assure that *eventually* they will either be created or else that they themselves will be shown to be subsumed by some other clause. In particular, we can now concisely justify the deletion of subsumed clauses in the absence of other deletion strategies.

COROLLARY: Subsumed clauses can produce only subsumed resolvents □

In complete analogy to the pseudo-confluence criterion for the Knuth-Bendix Algorithm, the above theorem only constitutes the abstract framework for a practicable *subsumption rule*, i.e. a deletion rule based on the subsumption test. Application of the criterion induces a dependency relation << on clauses, i.e. R_{CD} is subsumed only if the necessary resolvents are eventually created. However, the dependency relation induced by the abstract test is clearly reflexive and cyclic, which precludes completeness. Hence in practice we must somehow restrict actual application of the test to keep the corresponding << acyclic, and for the sake of finiteness assure that each resolvent is given fair consideration. Basically we face the same problem with classic subsumption rules: Clearly, any clause subsumes itself, but the actual subsumption rules disallow deletion on this ground.

References

[Ba&Bu 80] Bachmair, L., and Buchberger, B. A Simplified Proof of the Characterization Theorem for Gröbner-Bases. *ACM SIGSAM Bull. 14,* 4 (1980) 29-34.

[Ba&De 86] Bachmair, L., and Dershowitz, N. Critical Pair Criteria for the Knuth-Bendix Completion Procedure. Dept. Comp. Sci, U. Illinois at Urbana-Champaign, 1986.

[Bu 70] Buchberger, B. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes math. 4,* 3 (1970).

[Bu 79] Buchberger, B. "A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner-Bases." In *Symbolic and Algebraic Computation* (Proceedings of EUROSAM'79), E. Ng ed., Lecture Notes in Computer Science, vol. 72. Springer-Verlag 1979.

[Bu 84] Buchberger, B. "A critical pair/ completion algorithm for finitely generated ideals in rings." In *Logic and Machines: Decision Problems and Complexity* (Proceedings of the Symposium "Rekursive Kombinatorik", Münster, May 23-28, 1983), E. Börger ed., Lecture Notes in Computer Science, vol. 171, Springer-Verlag 1984.

[Co&Ka 85] Cosmadakis, S., Kannelakis, P. "Two Applications of Equational Theories to Database Theory." In *Rewriting Techniques and Applications* (Proc. RTA'85, Dijon, May 1985), J.-P. Jouannaud ed., Lecture Notes in Computer Science, vol. 202. Springer-Verlag 1985.

[De&Jo 84] Dershowitz, N., and Josephson, A. "Logic Programming by Completion." In Proc. 2nd Logic Programming Conference (Uppsala, July 2-6, 1984), S.-A. Tärnlund ed., pp 313-320.

[De&Ma 79] Dershowitz, N., and Manna, Z. Proving Termination with Multiset Orderings. *Commun. ACM 22,* 8 (Aug 1979) 465-476.

[De&Ma 84] Dershowitz, N., and Marcus, L. Existence and Construction of Rewrite Systems. Draft of Sept. 1984. Earlier as Technical Report ATR-82(8478)-3, The Aerospace Corporation, Dec 1982.

[Fr 86] Fribourg, L. "A strong restriction of the inductive completion procedure." Proc. ICALP 1986 (to appear).

[G&H&M 78] Guttag, J.V., Horowitz, E., and Musser, D. R., Abstract Data Types and Software Validation. *Commun. ACM 21* (1978), 1048-1064.

[Hs&De 83] Hsiang, J., and Dershowitz, N. "Rewrite Methods for Clausal and Non-clausal Theorem Proving." In *Automata, Languages and Programming* (Proc 10th ICALP, Barcelona, July 1983), J Diaz ed., Lecture Notes in Computer Science, vol. 154, pp 331-346.

[Hu 80] Huet, G. Confluent reductions: abstract properties and their applications to term rewriting systems. *Journ. ACM 27,* 4 (Oct 1980).

[Hu 81] Huet, G. A complete proof of correctness of the Knuth-Bendix Completion Algorithm. *Journ. Comp. Syst. Sci. 23* (1981) 11-21.

[Hu&Op 80] Huet, G., and Oppen, D. "Equations and rewrite rules: A survey." In *Formal Languages: Perspectives and Open Problems* (R. Book ed.). Academic Press 1980.

[Jo&Ki 84] Jouannaud, J.-P., and Kirchner, H. Completion of a Set of Rules Modulo a Set of Equations: Full Paper. Report 84-R-046, CRIN, Nancy, France, 1984.

[Jo&Ko 85] Jouannaud, J.-P., and Kounalis, E. Proofs by Induction in Equational Theories Without Constructors. *Bull. EATCS 27* (Oct. 1985), pp 49-55.

[Ki&Ki 83] Kirchner, C., and Kirchner, H. Current Implementation of the General E-Completion Algorithm. Tech. Report, CRIN, Nancy, France, 1983.

[Kn&Be 70] Knuth, D. E., and Bendix, P. B. "Simple word problems in universal algebra." In *Computational Problems in Abstract Algebra* (Proceedings of a conference held in Oxford 1967), J. Leech ed., Pergamon 1970.

[Kü 82] Küchlin, W. "A Theorem-Proving appproach to the Knuth-Bendix Completion Algorithm." In *Computer Algebra* (Proceedings of EUROCAM'82), J. Calmet ed., Lecture Notes in Computer Science, vol. 144. Springer-Verlag 1982.

[Kü 82a] Küchlin, W. An Implementation and Investigation of the Knuth-Bendix Completion Procedure. Diplomarbeit, Fakultät für Informatik, Universität Karlsruhe, West Germany,1982; also as Internal Report 17/82.

[Kü 82b] Küchlin, W. Some Reduction Strategies for Algebraic Term Rewriting. *ACM SIGSAM Bull. 16*, 4 (Nov 82) pp. 13-23.

[Kü 85] Küchlin, W. "A Confluence Criterion Based on the Generalized Newman Lemma." In *Eurocal '85* (Linz, Austria, April 1985), vol. 2, B. Caviness ed., Lecture Notes in Computer Science, vol. 204. Springer-Verlag 1985, pp 390-399. (Pages 397 and 398 are to be interchanged).

[Kü 86] Küchlin, W. "A Generalized Knuth-Bendix Algorithm". Report 86-01, Mathematics, Swiss Federal Institute of Technology, Zürich, Switzerland, 1986.

[K&M&N 86] Kapur, D., Musser, D., and Narendran, P. Only Prime Superpositions Need Be Considered in the Knuth-Bendix Procedure. Corporate R&D, General Electric Company, Schenectady NY. (Update of an earlier draft of 1985).

[La&Ba 83] Lankford, D., and Ballantyne, A. On the Uniqueness of Term-Rewriting Systems. December 1983.

[La&Ba 77] Lankford, D., and Ballantyne, A. Decision Procedures for Simple Equational Theories with Commutative-Associative Axioms: Complete Sets of Commutative-Associative Reductions. Report ATP-39, Department of Mathematics and Computer Sciences, University of Texas at Austin, August 1977.

[Pa 85] Paul, E. Equational Methods in First Order Predicate Calculus. *J. Symbolic Computation 1*, 1 (1985) pp 7-29.

[Pe&St 81] Peterson, G., and Stickel, M. Complete Sets of Reductions for Some Equational Theories. *Journ. ACM 28* (1981), pp 233-264.

[Wi 83] Winkler, F. A criterion for eliminating unnecessary reductions in the Knuth-Bendix Algorithm. Tech. Report 83-14.0, CAMP, Universität Linz, Austria, May 1983.

[Wi&Bu 83] Winkler, F., and Buchberger, B. "A criterion for eliminating unnecessary reductions in the Knuth-Bendix Algorithm." Colloquium on Algebra, Combinatorics and Logic in Computer Science (Györ, Hungary, Sept 12-16, 1983).

[Wi 84] Winkler, F. The Church-Rosser property in computer algebra and special theorem proving: an investigation of critical pair, completion algorithms. Dissertation der J. Kepler-Universität Linz, VWGÖ, Wien 1984.

[Wi 85] Winkler, F. "Reducing the Complexity of the Knuth-Bendix Completion Algorithm: A "Unification" of Different Approaches." In *Eurocal '85* (Linz, Austria, April 1985), vol. 2, B. Caviness ed., Lecture Notes in Computer Science, vol. 204. Springer-Verlag 1985, pp 378-389.