Relative Termination

by

Alfons Geser

Relative Termination

Dissertation

zur Erlangung des Grades des
Doktors der Naturwissenschaften
an der Fakultät für Mathematik und Informatik
der Universität Passau

von

Alfons Geser

Passau 1990

Abstract

"Relative termination" is a property that generalizes both termination and "termination modulo". In order to prove that a term rewrite system relatively terminates, one may reuse the common termination quasiorderings. Further proof methods become available by the cooperation property. Relative termination sets up new proof techniques for termination and confluence. The usefulness of the notion of relative termination is finally demonstrated by a proof of completeness for "reduced narrowing" and "normal narrowing", two attractive variants of the narrowing procedure.

Zusammenfassung

"Relative Termination" ist eine Eigenschaft, die sowohl Termination als auch "Termination modulo" verallgemeinert. Daß ein Termersetzungs-system relativ terminiert, läßt sich etwa mit den bekannten Terminations-Quasiordnungen beweisen. Weitere Beweismethoden erhält man durch die Eigenschaft der Kooperation. Relative Termination ermöglicht neue Beweismethoden für Termination und Konfluenz. Schließlich wird gezeigt, daß unter der Voraussetzung der relativen Termination zwei naheliegende Varianten der Narrowing-Prozedur vollständig sind, nämlich "reduced narrowing" und "normal narrowing".

Acknowledgements

To all those who supported me in writing this dissertation, I owe a debt of gratitude. First of all, I wish to thank Prof. Wirsing and Prof. Broy, who gave me the opportunity to write this thesis, and who were cooperative supervisors. I gratefully acknowledge a number of conversations with my colleagues at the department and in the ESPRIT project 432, METEOR.

In particular, I am indebted to Heinrich Hußmann and Peter Padawitz, who introduced me to the field of term rewriting. I wish to express my warmest thanks to Alexander Bockmayr, Dieter Hofbauer, and in particular, to Oliver Geupel, for their close cooperation and their repeatedly reading drafts of this thesis. Thanks also to Deepak Kapur, Pierre Lescanne, Ursula Martin, and the other members of the rewriting community, for valuable advice.

For their moral support, I am grateful to Thomas Belzner, Christian Lengauer, Thomas Streicher, and Muffy Thomas. Thanks go to Monica Eckhardt and Victor Pollara for their correcting my English. Finally, special thanks to my wife Eva-Maria for her patience and her continuous encouragement.

Table of Contents

Introduction and motivation 1
1. Basic term rewrite notions 7
1.1. Abstract relations 7
1.2. Terms, substitutions, and occurrences 8
1.3. Term rewrite systems 11
1.4. No restrictions? 12
2. Termination, termination modulo, and relative termination 14
2.1. Relative termination — Definition and basic properties 14
2.2. Necessary syntactic conditions 17
2.3. Some termination quasiorderings 19
2.4. How to prove relative termination 24
2.5. Relative termination in restricted systems 28
2.6. On the descriptive power of relative termination 28
3. How to strengthen termination orderings 30
3.1. Termination inheritance 31
3.2. Lexicographic combination proofs 33
3.3. Commutation and related properties 36
3.4. Cooperation 39
3.5. Local cooperation and strong cooperation 41
3.6. Critical pair criteria 43
3.7. Criteria for local cooperation 47
3.8. Criteria for strong cooperation, and their applications 53
4. Confluence criteria 59
4.1. The role of coherence 60
4.2. Further localization 65
4.3. On a confluence criterion of Klop 69
5. Applications of relative termination 75
5.1. Oriented paramodulation and narrowing 75
5.2. Normal narrowing is not complete 79
5.3. Relative termination and reduced narrowing 82
5.4. A completeness result for normal narrowing 84
Summary 90
Extensions or: What has not been treated 91
References 93
Index 102

One page principle:

A specification that will not fit on one page of 8.5 x 11 inch paper cannot be understood.

Mark Ardis

Introduction and motivation

This thesis deals with a *weakening* of the notion of *termination* of a term rewrite system.

A *term rewrite system* is a (usually finite) set of rewrite rules. A rule $l \rightarrow r$ allows one to replace any instance of the term l by the corresponding instance of the term r, in any context. Term rewriting has its early roots in the work of [Church, Rosser 36] on confluence in the lambda calculus and [Herbrand 30] on unification. The classical work that probably gave term rewriting its main impulse, is [Knuth, Bendix 70], in which a procedure is given that solves the *simple word problem* in some equational theories. The Knuth-Bendix procedure transforms a system of equations, that describes an equational theory, into a confluent and terminating term rewrite system. The termination property ensures that every term has at least one normal form, and that normal forms can safely be computed. Moreover, if confluence holds, then normal forms are unique. In a confluent and terminating term rewrite system semantic equality can be decided by a syntactic comparison of normal forms. Much work has been done to develop the theory of confluence and termination. Besides that, topics like automated theorem proving, equational unification, and narrowing have been studied. The pure theory has been enriched by equational rewriting, graph rewriting, and conditional rewriting. See [Dershowitz, Jouannaud 89] for an overview and a list of references.

An algebraic (or equational) specification is a set of functions which is called the *signature* and a (usually finite) set of equations l ’ r. For simplicity, we will use an impoverished notion of algebraic specifications, where all formulas are unconditional equations, and specifications are homogeneous ("single-sorted", without sort/type information). Algebraic specification was studied starting in 1974 by Liskov and Zilles, and continued by Guttag and the ADJ group. Nowadays there is abundant literature in that area, see [Wirsing 90] for an introduction and a list of references. Briefly summarized, the algebraic specification world negotiates with *model semantics* of specification: A specification is associated with a certain class of models; a model is an algebra where every given equation holds in all contexts and under all instantiations.

Term rewriting, in contrast, is mainly concerned with technical issues of equational specifications. It assigns to an algebraic specification, so to speak, an *operational semantics*. An algebraic specification is turned into a term rewrite system where each equation l ’ r is replaced by a rewrite rule $l \rightarrow r$. In contrast to an equation, a rewrite rule may be used only in an oriented way, from left to right.

It is a classical programming paradigm to develop software in *modules*. [Wirsing et al. 83] introduces the basic notion of *hierarchical specification*, and shows that important properties for a working modular approach are *sufficient completeness* and *hierarchy consistency*. These two notions on the one hand, and confluence and termination on the other hand, are closely connected (see [Nipkow, Weikum 83] and [Kapur et al. 87] for sufficient completeness, and [Padawitz 88] for hierarchy consistency). This stresses the need of a hierarchical treatment of confluence and termination.

Both confluence and termination are however, in general, not modular, i.e. a term rewrite system $R \cup S$ may fail to be confluent or terminating although its components R and S are. In a series of articles, a special case has been studied: The two components R and S have no common function symbols; then $R \cup S$ is also called the *direct sum* of R and S. Surprisingly, confluence of R and S entails confluence of $R \cup S$ in this case ([Toyama 87b]). A number of counterexamples showed that the problem is far more difficult with termination of direct sums ([Toyama 87a], [Ganzinger, Giegerich 87], [Klop 87]). Still, under some restrictions, termination results exist ([Toyama et al. 87], [Rusinowitch 87a], [Middeldorp 89]).

Often $R \cup S$ is not a direct sum. Consider for instance the following algebraic specification of queues:

Example: *(Queues)*
Assume a primitive algebraic specification P of items to be given, and let F_P denote a set of function symbols that contains at least the function symbols occurring in P. P and F_P may be unknown at the beginning; the pair (F_P, P) might be seen as a parameter specification to the (parameterized) queue specification below. Let the set of new function symbols be

$F_Q =_{def}$ {empty, app, bottom, upper, length},

where "empty" (empty queue) is a constant, "bottom" (bottom element of the queue), "upper" (queue when the bottom element has been removed), and "length" are unary, and "app" (append a token at the top of a queue) is a binary function symbol. F_P has to satisfy $F_P \cap F_Q = \emptyset$. The functions in F_Q are specified by

$$
\begin{aligned}
Q =_{def} \{&\text{bottom}(\text{app}(x, \text{empty})) \rightarrow x,\\
&\text{bottom}(\text{app}(x, \text{app}(y, q))) \rightarrow \text{bottom}(\text{app}(y, q)),\\
&\text{upper}(\text{app}(x, \text{empty})) \rightarrow \text{empty},\\
&\text{upper}(\text{app}(x, \text{app}(y, q))) \rightarrow \text{app}(x, \text{upper}(\text{app}(y, q))),\\
&\text{length}(\text{empty}) \rightarrow 0,\\
&\text{length}(\text{app}(x, q)) \rightarrow s(\text{length}(q))\}.
\end{aligned}
$$

Q is terminating, as can easily be shown. Under which circumstances is Q∪P terminating? Q∪P is not a direct sum, because 0 and s (zero and successor, respectively) which occur in Q, may also be function symbols in P. The termination of P is certainly necessary. But even if P is terminating, it is questionable whether Q∪P also is. According to a theorem of [Bachmair, Dershowitz 86], a sufficient condition here is "P terminating and left-linear". This is not too strong a condition since most rewrite systems are indeed left-linear, i.e. the left hand side of each rule contains each variable at most once.

But if we do not know whether P terminates, can we still say something sensible about the termination behaviour of Q in connection with P? Yes, sometimes we can. We could for instance ask whether P-steps can force infinitely many Q-steps to occur.

□

The following small example shall illustrate what this amounts to: Let a and b denote constants. Assume two term rewrite systems R∪S and R∪S´ to be given by

$$R = \{a \rightarrow b\}, \quad S = \{b \rightarrow a\}, \quad S' = \{b \rightarrow b\}\ .$$

Both systems are obviously non-terminating, but in the system R∪S, the progress achieved by R-steps is repeatedly destroyed by S-steps, where in the system R∪S´ finally (here: immediately) S´-steps preserve the R-normal form b. Even better, *no derivation* in the latter system *contains infinitely many R-steps*. This effect has been called "*relative termination*" by Jan Willem Klop in [Klop 87]. Now back to our example:

Example: *(Queues, continued)*

When does Q relatively terminate to P? A necessary condition is "P left-nonerasing", i.e. each variable that occurs on the right also occurs on the left of a rule from P. (This condition is often presupposed anyway.) Again using Bachmair and Dershowitz´ theorem, we find that "P right-linear and left-nonerasing" is sufficient. P is called right-linear if no variable occurs twice on the right hand side of a rewrite rule. If P is right-linear and left-nonerasing then Q-steps occur only finitely often in a Q∪P-derivation.

□

R∪S terminates if and only if R relatively terminates to S and S terminates. This property can be used to glue termination proofs together. Technically, this gluing corresponds to the *lexicographic combination of termination orderings*, a technique which in [Ben-Cherifa, Lescanne 86] has been shown useful for the polynomial interpretation method.

"Relative termination" also generalizes the notion of termination *modulo* an equational theory E. We will regard an equational theory as a symmetry-closed term rewrite system. So we may take termination modulo E to be the same as relative termination to E, for symmetric E. The theory of "termination modulo" is comparatively well-developed ([Lankford, Ballantyne 77], [Huet 80], [Peterson, Stickel 81], [Jouannaud, Muñoz 84]). A crucial question is therefore whether relative termination contributes anything new to the notion of termination modulo. The answer is settled positively in this thesis: There are rewrite systems R, S, such that R terminates relative to S, but not modulo S.

The article [Bachmair, Dershowitz 86] contains the first use and application of relative termination in the literature. Following [Jouannaud, Muñoz 84], it introduces commutation-like properties of rewrite systems in order to derive termination orderings. Independently [Bellegarde, Lescanne 86] coins the related notions of *transformation ordering* and *cooperation*. As many examples have shown, the transformation ordering is both powerful and easy to use. For instance, homomorphic interpretation orderings seem to be basically transformation orderings.

As the first application of relative termination, [Klop 87] uses a criterion called "splitting effect" to prove confluence of rewrite systems $R \cup S$, where R terminates relative to S.

Building on the work reviewed above, this thesis is concerned with the following questions:

1) How do the notions of termination, termination modulo, and relative termination correlate?

The three notions are, in fact, very closely related. Termination of R is a special case of relative termination of R to S, where S = Ø. Moreover termination of R modulo E is a special case, where E = S is symmetric. On this account, one may expect that relative termination satisfies some properties which are known from termination or termination modulo. For instance, relative termination, like termination modulo, may be proven by termination quasiorderings. As a side-effect, rewriting modulo is re-integrated into classic rewriting theory.

2) What can relative termination contribute to termination proof techniques?

The first approach uses the fact that relative termination of R to S is a necessary condition for $R \cup S$ Noetherian. Moreover, if S is Noetherian, relative termination of R to S is even equivalent to termination of $R \cup S$. So in order to prove termination of $R \cup S$, it may be advantageous to proceed in two steps: First prove that R is relatively Noetherian to S, then prove that S is Noetherian. The underlying fundamental property of termination is that R∪S *inherits* termination from the termination of R and S when R∪S is transitive.

The second approach establishes a relative termination result by the *quasi-commutation* property. This thesis investigates the quasi-commutation and *cooperation* methods of Bachmair and Dershowitz, and of Bellegarde and Lescanne. It moreover demonstrates that these two methods are instances of a more general cooperation method that admits *local cooperation* and *strong cooperation* criteria, similar to the local and strong criteria for confluence.

3) How can one prove confluence in the case of relative termination?

Since confluence proof techniques are known for termination and termination modulo, this question is natural. In this thesis, the confluence proof, like in the termination modulo approach, is attacked by a *coherence* property. This leads to a confluence criterion for R∪S which is local with the exception of the confluence proof for S. In other words, confluence proofs can be done *hierarchically*. In the confluence modulo approach, the primitive theory may also be built-in. Then people also speak about the *class approach*. A possibility for a class approach not requiring symmetry is sketched but not finished in this thesis. Finally, if one aims at local diagrams even for S, then a new criterion called *strong coherence*, in the spirit of strong confluence, leads to a confluence result that generalizes Klop´s confluence result.

4) Where else does relative termination apply?

Wherever termination is needed, but not in its full strength, relative termination becomes an attractive candidate. Relative termination still provides an inductive ordering, which is useful for an inductive proof. A demonstration of the power of relative termination on this account is given in this thesis by two proofs. In the case that a dedicated subset S of the given rules R∪S serves for reduction, reduced narrowing and normal narrowing are complete, if R relatively terminates to S.

In summary, we are interested in relative termination for a number of reasons:

(1) Relative termination is a notion well suited to speak about the termination property.

(2) Termination "inherits" by relative termination. This is the basis of stepwise ("modular") termination proofs.

(3) Termination and termination modulo an equational specification are special cases of relative termination.

(4) Termination of R relative to S means that the ordering $(R/S)^+$ is Noetherian. This ordering can be applied in various inductive proofs, for instance proofs of confluence.

(5) Techniques based on commuting diagrams define termination orderings (the transformation orderings) which are closely correlated with relative termination. These orderings are interesting in their own right: They can be used to perform difficult termination proofs.

The thesis is organized as follows:
The first chapter "Basic term rewrite notions" explains the working set of definitions, conventions, and basic results used later in the thesis. A definition of relative termination, and its typical properties and proof methods are the subject of the second chapter "Termination, termination modulo, and relative termination". The third chapter, "How to strengthen termination orderings", touches the inheritance problem area, and redraws the transformation ordering approach.
The remaining two chapters deal with applications of relative termination. Chapter 4, entitled "Confluence criteria", develops critical pair criteria for confluence of rewrite systems where a part of the system is relatively terminating to the rest. The thesis is finished in chapter 5, "Applications of relative termination", with a result about completeness of the normal narrowing procedure.

1. Basic term rewrite notions

This chapter contains some basic definitions which will be used freely throughout this thesis, and which are standard in the rewriting community. With one major exception: *Every* binary relation on terms is called a term rewrite system. We will plead for this decision; it has a basic impact on the whole thesis. For surveys on term rewriting in general, see [Huet, Oppen 80], [Jouannaud, Lescanne 86], [Klop 87], [Dershowitz, Jouannaud 89], [Avenhaus, Madlener 90].

The set of natural numbers will be denoted by $\mathbb{N}$, naturally ordered by $\geq_{\mathbb{N}}$. For convenience, let us reserve the names c, m, n, i, and k for natural numbers. Of course, here and in the sequel, all names may also occur indexed or primed or both indexed and primed.

1.1. Abstract relations

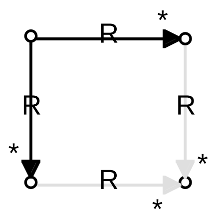
First, let us establish some notation for arbitrary binary relations R (over some implicit universe U). We will sometimes drop the prefix "binary". Relations will preferably be called Q, R, S, and T. *Composition* of relations is denoted by juxtaposition. The inverse relation R^{-1} of R differs from R by the exchange of left and right hand sides:

$$R^{-1} =_{def} \{ (r, l).\ (l, r) \in R \} .$$

The symmetric, reflexive, transitive, and reflexive-transitive closures of R are denoted by $\overline{R}$, R^{ε}, R^{+}, and by R^{*}, respectively.

Many properties of binary relations are of the form $P \subseteq Q$, more conveniently, in logic terms: For all t, t´, if $(t, t') \in P$ holds, then $(t, t') \in Q$ holds. It is customary to represent such a fact by a *diagram*. A diagram is a directed graph, where nodes represent objects (t and t´), and arrows represent their relations (P and Q). Black arrows denote premises ("if $(t, t') \in P$ ..."), and grey (elsewhere, dashed) arrows denote conclusions ("... then $(t, t') \in Q$ ").

For instance, R is called *confluent*, if $(R^{-1})^{*}R^{*} \subseteq R^{*}(R^{-1})^{*}$ holds. In other words, R is confluent if $(t, t') \in (R^{-1})^{*}R^{*}$ implies $(t, t') \in R^{*}(R^{-1})^{*}$ for all t, t´. In a diagram presentation finally, R is confluent if



holds. The three definitions are perfectly equivalent. Remember that confluence is equivalent to the *Church-Rosser property*: $\overline{R^{*}} \subseteq R^{*}(R^{-1})^{*}$.

R is called *cyclic*, if R^+ is reflexive, and *acyclic*, if R^+ is irreflexive. R is called *finitely branching*, if for all t, the set $\{t'.\ (t, t')\in R\}$ of immediate descendants of t is finite. A (finite or infinite) sequence $t_0, t_1, t_2, \ldots$ such that $(t_i, t_{i+1})\in R$ holds for all $i\in \mathbb{N}$, is also called an R-*derivation*. R is called *Noetherian*, if it admits no infinite derivations. In this thesis we will use the predicates "is Noetherian" and "terminates" as synonymous.
An object t is called *(R-)normal*, or *in R-normal form*, if there is no t´ such that $(t, t')\in R$. The set of all R-normal forms is denoted by NF_R. The relation R^{NF} ("*R-normalization*") is defined by $R^{NF} =_{def} \{(t, t')\in R^*.\ t'\in NF_R\}$. The set of normal forms of an object t is the set $NF_R(t) =_{def} \{t'.\ (t, t')\in R^{NF}\}$. If every object has a normal form, i.e. if $NF_R(t) \neq \emptyset$ for all t, then R is called *normalizing*. Remember that Noetherian relations are normalizing, particularly.
A reflexive and transitive relation is also called a *quasiordering*, an irreflexive and transitive relation a *strictordering*. For a quasiordering and its inverse we will preferably use the symbols $\geq$ and $\leq$. The set difference $\geq\setminus\leq$ (a strictordering) will then be denoted by $>$, and the intersection $\geq\cap\leq$ (an equivalence relation) by the symbol $\sim$. By abuse of notation, quasiorderings and strictorderings will also be called *orderings*. A quasiordering $\geq$ will (by abuse of notation) be called Noetherian, if its associated strictordering $>$ is Noetherian.

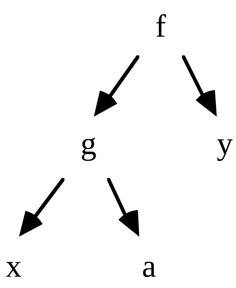
1.2. Terms, substitutions, and occurrences

Let F denote a finite set, and X an infinite, countable set disjoint from F. We call elements of F *function symbols*, and elements of X *variables*. A function arity: $F \to \mathbb{N}$ assigns to function symbols their *arity*. Function symbols of arity 0 are also called *constants*. The set of (finite) *terms* is the ($\subseteq$-)least fixpoint of the equation

$$\text{Term} = X \cup \bigcup_{f\in F} (\{f\} \times \text{Term}^{\text{arity}(f)})$$

i.e. the least set that extends X and contains the tuple $(f, t_1, \ldots, t_n)$ if $\text{arity}(f) = n$ and $t_1, \ldots, t_n$ are in the set. Since function symbols may also be seen as functions which construct terms, $(f, t_1, \ldots, t_n)$ is rather written f, if f is a constant, and $f(t_1, \ldots, t_n)$ otherwise. In this respect, there is an algebra (Term, F) of terms and their functions. (Do not confuse this with the notion of *term algebra* in the literature, which assumes $X = \emptyset$.) For certain function symbols, ad hoc mixfix syntax will be used, like for "+" in x+y, or for "-" in -x. We will prefer the names x, y, and z for variables, a and b for constants, f, g, h, s, -, +, and * for unary and binary function symbols, and l, r, and t for terms.
Terms may be seen as particular trees where nodes are labelled by function symbols or variables. For instance, if f and g are binary, then $t =_{def} f(g(x, a), y)$ is a term. It may be depicted as

t =



For this reason, f is also called the *top symbol* of the term t, and the terms g(x, a) and y are called the first, second son, respectively, of t. Note that the equality sign "=" is not a symbol from the object language (as is f, for instance) but a *meta symbol* which we will use to indicate *syntactic equality* of terms. The other "equalities" on terms which we will cope with, are:

1. equations as part of algebraic specifications (there we will write l ’ r),
2. equations that are to be solved (also called goals; we will write eq(t, t´) where "eq" is a fresh function symbol), and finally,
3. the semantic equality, i.e. the congruence structure on terms which models the application domain (denoted by $=_R$, where R is the underlying term rewrite system).

Needless to say, these equality notions must not be confused. Details will be explained later.

The functions Var: Term $\to \wp(X)$ and Func: Term $\to \wp(F)$ deliver the set of *variables* (functions, respectively) *that occur in* a term; they are defined in a straightforward way:

$\mathrm{Var}(x) = \{x\}$, $\quad \mathrm{Var}(f(t_1, ..., t_n)) = \mathrm{Var}(t_1) \cup ... \cup \mathrm{Var}(t_n)$,

$\mathrm{Func}(x) = \emptyset$, $\quad \mathrm{Func}(f(t_1, ..., t_n)) = \{f\} \cup \mathrm{Func}(t_1) \cup ... \cup \mathrm{Func}(t_n)$.

If Var(t) = Ø, then the term t is called *ground*. In our example, Var(f(g(x, a), y)) = {x, y} and Func(f(g(x, a), y)) = {f, g, a}. The term f(g(x, a), y)) is not ground.

Occurrences are finite sequences of natural numbers. We will prefer the names u, v, and w for occurrences. We will denote concatenation of occurences by the dot notation, e.g. in u.v for occurrences u and v. The empty occurrence or top occurrence is denoted by λ. An occurrence may be seen as a path from the root of t down to a unique node of t. An occurrence i.u, where i is a natural number, means: Go to the i-th son, and continue with u. In our example above, the occurrence 1.2 points to the node labelled by a. The *subterm* of t whose root is identified by u this way, is denoted by t/u. The *replacement* of t/u, within its context in t, by the term t´, is denoted by t [u ← t´]. Subterm and replacement are defined in a straightforward way:

$t / \lambda = t$, $\quad f(t_1, ..., t_n) / i.u = t_i / u$,

$t [\lambda \leftarrow t'] = t'$, $\quad f(t_1, ..., t_n) [i.u \leftarrow t'] = f(t_1, ..., t_i [u \leftarrow t'], ..., t_n)$.

In our example above, $t[1 \leftarrow a] = f(a, y)$. That is to say: In order to replace the subterm in t at occurrence 1 by the term a, one removes the subterm $g(x, a)$ from t and inserts a instead. The function $\mathrm{Occ}: \mathrm{Term} \to \wp(\mathbb{N}^*)$ that assigns to a term *its set of occurrences*, is the set of occurrences u for which t/u is defined. The set of *functional occurrences*, $\mathrm{FOcc}(t)$, is the set of occurrences $u \in \mathrm{Occ}(t)$ such that $t/u \in F$, i.e. the set of occurrences labelled with a function symbol in t. We have in our example $\mathrm{FOcc}(t) = \{\lambda, 1, 1.2\}$. A partial ordering on occurrences is defined by the *prefix ordering*

$$u \leq_{pre} u' \Leftrightarrow_{def} \text{ there is an occurrence } v \text{ such that } u.v = u'.$$

Taken as positions in a term, $u \leq_{pre} u'$ means that u is above u'.

A *substitution* is an endomorphism $\sigma: \mathrm{Term} \to \mathrm{Term}$, in the algebra (Term, F), i.e. it satisfies

$$\sigma(f(t_1, ..., t_n)) = f(\sigma(t_1), ..., \sigma(t_n))$$

for each function symbol f. So a substitution is already determined by its images of variables, a fact that justifies the notation $[t_1/x_1, t_2/x_2, ...]$ for the substitution which maps x_1 to t_1, x_2 to t_2, and so on. Substitutions will be denoted by small greek letters, except λ (empty occurrence), ε (reflexive closure), and ω (least transfinite ordinal number). In order not to confuse term construction with substitution application, we will write $t\sigma$ instead of $\sigma(t)$. The (functional) *composition* of substitutions σ and τ is denoted by $\sigma\tau$. Since composition is associative and extends application, parentheses may be omitted in expressions, as in $t\lambda\sigma\tau$. The *subsumption* quasiordering $\leq_{sub}$ on terms is defined by

$$t \leq_{sub} t' \Leftrightarrow_{def} \text{ there is a substitution } \sigma \text{ such that } t' = t\sigma.$$

A term $t\sigma$ is called an *instance* of t (by σ), or, *more special than* t. Vice versa, we say that t is *more general than* $t\sigma$, or that t *subsumes* $t\sigma$.

By abuse of notation, the *domain* of a substitution σ is the set

$$\mathrm{dom}\,\sigma = \{x \in X.\ x\sigma \neq x\},$$

its *range* is the set

$$\mathrm{ran}\,\sigma = \bigcup_{x \in \mathrm{dom}\,\sigma} \mathrm{Var}(x\sigma).$$

Idempotent substitutions, i.e. substitutions σ where $x\sigma\sigma = x\sigma$ holds for all x, are characterized by the property $\mathrm{dom}\,\sigma \cap \mathrm{ran}\,\sigma = \emptyset$. Bijective renamings are typical non-idempotent substitutions. Substitutions have a very technical nature. It is therefore important to know some techniques for dealing with them. For instance, substitutions are often interesting on a finite subset W of X. Sometimes $W = \mathrm{Var}(t)$ for some term t. It is known that every substitution σ with $\mathrm{dom}\,\sigma \subseteq W$ can be represented on W as a composition of an idempotent substitution μ with a renaming ρ: $\forall x \in W.\ x\sigma = x\mu\rho$. (This is elsewhere written $\sigma = \mu\rho\ [W]$.)

1.3. Term rewrite systems

Let R denote a binary relation on *terms*. R is called *closed under contexts*, if for all terms $t_1, ..., t_n, t'$, and for all $f \in F$ where arity(f) = n,

$(t_i, t') \in R$ implies $(f(t_1, ..., t_n), f(t_1, ..., t_{i-1}, t', t_{i+1}, ..., t_n)) \in R$.

R is called *closed under instantiation*, if for all terms t, t´, and substitutions σ,

$(t, t') \in R$ implies $(t\sigma, t'\sigma) \in R$.

(Closure under contexts is elsewhere also called F-stability or monotonicity, and closure under instantiation is also called stability or closure under substitution.)
For proofs, we can profit from a characterization of context closure:

Fact:
R is closed under contexts if and only if, for all terms t, t´, and occurrences $u \in Occ(t)$,

$(t/u, t') \in R$ implies $(t, t[u \leftarrow t']) \in R$.

□

(Recall from the previous section that t/u denotes the subterm of t at occurrence u, and $t[u \leftarrow t']$ denotes t where the term t´ replaces the subterm at occurrence u.)

In order to represent term reductions, people use *(term) rewrite systems*, i.e. relations on terms that are explicitly given by a (not necessarily finite) set R of term pairs (l, r) which are called *rewrite rules*, and are written $l \to r$. In order to say that R contains a rule $l \to r$, we will write $(l \to r) \in R$. The *rewrite relation* $\underset{R}{\to}$ is the smallest relation containing R and closed under contexts and instantiation. It will be used in infix notation: $t \underset{R}{\to} t'$. A term rewrite system R is called Noetherian, confluent, or finitely branching, if its associated rewrite relation $\underset{R}{\to}$ is. Recall that the symbols $\underset{R}{\to}^{\varepsilon}$, $\underset{R}{\to}^{+}$, $\underset{R}{\to}^{*}$ denote the reflexive, transitive, and reflexive-transitive closures of $\underset{R}{\to}$, respectively. Likewise, $\underset{R}{\to}^{NF}$ denotes the rewriting to ($\underset{R}{\to}$-)normal form. For convenience, we will write ${}^{*}\underset{R}{\leftarrow}$ instead of $\underset{R}{\leftarrow}^{*}$, and so on. The congruence closure of $\underset{R}{\to}$ is denoted by $=_R$.
For technical purposes, we will sometimes use the notation $t \xrightarrow[l \to r]{u} t'$, to denote that "rewriting happens at occurrence u using rule $l \to r$ ", i.e. that there is a substitution σ where $t/u = l\sigma$ and $t' = t[u \leftarrow r\sigma]$. In that case, t/u is called a *redex* for $l \to r$, and u is called the redex occurrence for $l \to r$ in t. It is obvious that whenever $t \underset{R}{\to} t'$ holds, there are suitable u, l, and r, such that $t \xrightarrow[l \to r]{u} t'$ and $(l \to r) \in R$ hold.

A rule $l \to r$ is called *left-linear*, if each variable occurs at most once in l, *left-nonerasing*, if $Var(l) \supseteq Var(r)$, i.e. every variable that occurs in l also occurs in r, and *left-nonisolating*, if $l \notin X$ (the left hand side of the rule is not just a variable). Likewise, a rewrite system R is called left-linear, left-nonerasing, or left-nonisolating, if *all* $(l \to r) \in R$ are so. $l \to r$ is called *left-nonlinear*, if it is not left-linear, *left-erasing* if it is

not left-nonerasing, etc. If $l \to r$ is left-linear, then $r \to l$ is called *right-linear*, etc. (Other authors also call a left-nonerasing rule left-non-annihilating or regular, a right-nonisolating rule non-collapsing or collapse-free.)
For example, the rule $x*x \to x$ is left-nonlinear (since x occurs twice on the left hand side) and right-isolating (x appears isolated on the right hand side). The rule $x \to x+y$ is both left-linear and right-linear (the variables x and y occur at most once on each side), but left-erasing (y appears on the right hand side, but not on the left hand side). $f(x) \to 0$ finally is right-erasing (because x disappears at the right hand side), both left-linear and right-linear, and both left-nonisolating and right-nonisolating (the left hand side begins with a (unary) function symbol f, and the right hand side is a constant 0, so both sides do not consist of a variable only).

If the premise part of a diagram is described by the transitive closure $\to^+$ of a rewrite relation $\to$, as is often the case, then it is advantageous to first prove a diagram which in its premise just uses single $\to$-steps instead of $\to$-derivations of arbitrary length. Such a diagram is called *local*. For localization, i.e. for reducing the proof of a diagram to that of its local counterpart, usually certain restrictions must be satisfied.
Since [Huet 80], it has become common to prove rewrite diagrams in two phases: The purpose of the first phase is to *localize* the diagram. For this phase, one may do without using typical rewrite notions (like substitutions, contexts, or occurrences), and without using rewrite properties (like closure under contexts and instantiation). In other words, the rewrite relation may be treated as an *abstract* binary relation. During this phase, we may therefore safely confuse R with $\underset{R}{\to}$. The rewrite notions and rewrite properties are exploited in the second phase, where decidable, sufficient properties are developed — the so-called critical pair criteria. The notion of "critical pair" will be defined in chapter 3.

1.4. No restrictions?

In the definition of a term rewrite system, we did not mention any such restriction as left-nonerasing or left-nonisolating, although that is quite widespread in the term rewrite literature. A motive for these restrictions may be that a "neat" rewrite system satisfies them: Every Noetherian rewrite system is both left-nonerasing and left-nonisolating. (See section 2.2 in this thesis for details.) On the other hand, if one drops the restrictions (as in [Padawitz 88], [Dershowitz, Jouannaud 89], [Hofbauer, Kutsche 89]), then every binary relation on terms may be considered a rewrite system. If R is not definitely Noetherian, one must be careful whether left-erasing and left-isolating rules behave as intended. After all, what could be a good reason for adopting such a general notion? Among other things it satisfies *general duality*: Every term rewrite system R has an opposite term rewrite system R^{-1}.

Suppose we are given a rewrite system R, and we want to ignore the orientation of the rules, i.e. consider the symmetric closure $\overline{R} =_{def} R \cup R^{-1}$ of R. If we forbid left-isolating or left-erasing rewrite rules, then $\overline{R}$ could not be a rewrite system if R contained right-isolating or right-erasing rules (because R^{-1} then contains forbidden rules). However, many rewrite systems contain such rules. For instance, $x+0 \rightarrow x$ is right-isolating, and $x*0 \rightarrow 0$ is right-erasing.

Systems of term equations may be treated as if they were symmetric rewrite systems. Thus if E is a system of term equations, and $(l, r) \in E$ is an equation (elsewhere also noted as l ’ r or, by abuse of notation, as $l = r$), then E is considered as a symmetry closed set of rules $l \rightarrow r$ (i.e. the rule $r \rightarrow l$ is also in E). So we need no particular notation for equational axioms. We can even represent E as $E =_{def} \overline{R}$ for some suitable rewrite system R.

By taking equational axioms as symmetric rewrite systems, we may consider equational rewriting as a special case (namely, the symmetric case) of rewriting. A comparison between equational rewriting and rewriting is possible, this way.

Another comfortable consequence of general duality is that critical pair criteria (defined in chapter 3) become applicable in a more general setting. For instance, a criterion for (R, S)-critical pairs applies also for (R^{-1}, S)-critical pairs, for (R, S^{-1})-critical pairs, and for (R^{-1}, S^{-1})-critical pairs. Suppose we have a theorem about rewrite systems R and S (which often will be the case later), then we may drop the corresponding theorem concerning R^{-1} and S for example, because it is a *trivial* corollary.

It is all these simplifying effects which makes the *general* notion of term rewrite system so compelling.

2. Termination, termination modulo, and relative termination

In this chapter, we define and investigate the notion of *relative termination*. Given two relations R and S, we call R relatively Noetherian (or relatively terminating) to S, if every R∪S-derivation contains finitely many R-steps. This is a generalization of "termination modulo" where S is required to be symmetric. (Remember that we may consider systems of term equations as symmetric rewrite systems.) On the other hand, relative termination is also a weakening of termination: If R∪S is Noetherian, then particularly R is relatively Noetherian to S. It is also a *strengthening* of termination: If R is relatively Noetherian, then R is Noetherian, particularly. This demonstrates that relative termination is a central notion in the study of termination of rewriting, and that it deserves closer attention.
Because of the relationship between termination and termination modulo on the one hand to relative termination on the other hand, it is interesting to ask how far their properties, techniques and methods carry over to relative termination. In this chapter, we will show that necessary conditions for relative termination (except trivial boundary cases) fit those known for termination and termination modulo, but are in general slightly more liberal. Standard termination quasiorderings can basically be carried over to relative termination. A characterization by means of a termination quasiordering, as it is available for termination modulo, is however far less obvious in the case of relative termination. The last section in this chapter shows that relative termination is a proper extension of both termination and termination modulo.

2.1. Relative termination — Definition and basic properties

Terminating (or Noetherian) rewrite systems are valuable, for a number of reasons. For instance, every rewrite strategy is safe, i.e. finally leads to a normal form. Recent overviews of termination of term rewriting are given in [Dershowitz 85] and [Dershowitz 87]. Many interesting term rewrite systems though, are *not* Noetherian. Some of them at least have a Noetherian subset R of rules which is "robust" against the rest, S, of the rules in the following sense: Application of R-rules with intermediate application of arbitrarily many S-rules is finally blocked. Let us make this more precise:

Definition: *([Klop 87])*
Let R and S denote binary relations. R is called *relatively Noetherian to* S, if every (infinite) derivation $t_1 \xrightarrow[R\cup S]{} t_2 \xrightarrow[R\cup S]{} \dots$ contains only *finitely* many $\xrightarrow[R]{}$-steps. If S is presupposed, then R is just called *relatively Noetherian*. The phenomenon that R is relatively Noetherian, is called *relative termination*.

Example: *(Set)*

Let "a" and "b" denote two distinct constant elements. Now let an algebraic specification of subsets of {a, b} be given that defines constants "true", "false", and Ø, and binary functions "ins" (insertion of elements) and "elem" (the membership relation ∈). Axioms are provided by the two rewrite systems R and S, as follows:

$R =_{def}$ {elem(x, Ø) → false,
elem(x, ins(x, s)) → true,
elem(a, ins(b, s)) → elem(a, s),
elem(b, ins(a, s)) → elem(b, s)},

$S =_{def}$ {ins(x, ins(x, s)) → ins(x, s), *"left-idempotence"*
ins(x, ins(y, s)) → ins(y, ins(x, s))}. *"left-commutativity"*

R is relatively Noetherian to S. For instance, the derivation

elem(a, ins(b, ins(a, ins(a, empty)))) $\xrightarrow[R]{}$
elem(a, ins(a, ins(a, empty))) $\xrightarrow[S]{}$
elem(a, ins(a, ins(a, empty))) $\xrightarrow[S]{}$ ...

is indeed infinite, but contains only one R-step.

□

(This and other examples will be used as running examples.)

Relative termination is closely connected with the following composed relation:

Definition: *([Bachmair, Dershowitz 86])*

The relation $R/S =_{def} S^* R S^*$ is called *R relative to S.*

□

The notation R/E is known as "R modulo E" from the case where E is symmetric. Because the word "modulo" suggests that E is an equivalence relation, we prefer not to use it for potentially unsymmetric S.

The $(R/S)^+$-derivations can be seen as $(R \cup S)^*$-derivations which contain at least one R-step. The equality $(R/S)^+ = S^* R (R \cup S)^*$ will be useful later. Let us adopt the convention that the operator "/" binds stronger than "∪", and weaker than composition. So for example, $RS/Q \cup R$ means $((RS) / Q) \cup R$.

Relative termination can now be characterized in several ways.

Lemma:

Let R and S denote binary relations. Then the following propositions are equivalent:

1. R/S is Noetherian.
2. S^*R is Noetherian.
3. For every rewrite sequence $t_1 \xrightarrow[R \cup S]{} t_2 \xrightarrow[R \cup S]{} \dots$ there is $n \in \mathbb{N}$ such that after t_n no more R-steps occur.
4. R is relatively Noetherian to S.

Proof:

(1⇒2) $S^*R \subseteq R/S$.

(2⇒3)

By contradiction. Let $t_1 \xrightarrow[R\cup S]{} t_2 \xrightarrow[R\cup S]{} \ldots$ be a derivation such that for all $n \in \mathbb{N}$, there is at least one R-step after t_n. Call the position where the next R-step takes place, next(n), in other words, $t_n \xrightarrow[S]{}^* t_{next(n)} \xrightarrow[R]{} t_{next(n)+1}$ holds. Since this construction works for all $n \in \mathbb{N}$, there is an infinite sequence

$$t_1 \xrightarrow[S]{}^* \xrightarrow[R]{} t_{next(1)+1} \xrightarrow[S]{}^* \xrightarrow[R]{} t_{next(next(1)+1)+1} \xrightarrow[S]{}^* \xrightarrow[R]{} \cdots$$

contradicting S^*R Noetherian.

(3⇒4)

Directly. Let $t_1 \xrightarrow[R\cup S]{} t_2 \xrightarrow[R\cup S]{} \ldots$ be a derivation such that there is no more R-step after t_n for some $n \in \mathbb{N}$. Then it contains at most n R-steps, i.e. finitely many.

(4⇒1)

By contradiction. Every infinite derivation $t_1 \xrightarrow[S]{}^* \xrightarrow[R]{} \xrightarrow[S]{}^* t_2 \xrightarrow[S]{}^* \xrightarrow[R]{} \xrightarrow[S]{}^* \ldots$ contains infinitely many R-steps.

□

Characterization number 1 will be used in the sequel as a shorthand and for orderings in inductive proofs. A number of useful properties about relative termination can immediately be derived from these equivalences:

Fact:

1. $R^+ \subseteq (R/S)^+ \subseteq (R\cup S)^+$. So in particular,

   $R\cup S$ Noetherian implies R/S Noetherian, and

   R/S Noetherian implies R Noetherian.

2. If $R' \subseteq R$, and $S' \subseteq S$, then $R'/S' \subseteq R/S$. So relative termination is *closed under subsets*, i.e. if R is relatively Noetherian to S, and $R' \subseteq R$, and $S' \subseteq S$, then R´ is relatively Noetherian to S´.

3. $(R / S)^+ = (R / (S\setminus R))^+ = (R / (R\cup S))^+$, etc. That is to say, only the part of S matters that is disjoint from R.

□

The inclusions and implications in 1 are usually strict, i.e. it happens that the converse is false:

Example:

1. *([Porat, Francez 86], simplified)*

Let $R =_{def} \{s(x)+y \rightarrow x+s(y)\}$ and $S =_{def} \{x+y \rightarrow y+x\}$. As we will prove in the next two sections, R is Noetherian, and S is not. Although R is Noetherian, R is *not relatively Noetherian* to S, as the derivation $s(x)+x \xrightarrow[R]{} x+s(x) \xrightarrow[S]{} s(x)+x \xrightarrow[R]{} \ldots$ contains infinitely many R-steps.

2. *(Set, continued)*
Recall the algebraic specification of subsets of {a, b} at the beginning of this section. $R \cup S$ is not Noetherian because we could provide an infinite $R \cup S$-derivation. On the other hand, R/S is Noetherian, as we will prove in section 2.4.

□

2.2. Necessary syntactic conditions

Recall from the previous chapter that a rewrite system R is Noetherian only if R is both left-nonerasing and left-nonisolating. Now it is interesting to ask what is necessary for a rewrite system R to be *relatively* Noetherian to a rewrite system S. An answer to this question helps us to judge methods for relative termination, because we can distinguish between unavoidable conditions and merely accidental, technically motivated conditions. For example, if $(f(x) \to f(y)) \in S$ and R is nonempty, then R/S cannot be Noetherian. On the other hand, for $S = \{x \to x\}$ and R Noetherian, always R/S is Noetherian. The necessary condition we will obtain, matches the one given in [Jouannaud, Muñoz 84] for termination modulo.
The proof that a condition is necessary, is usually done by contradiction. In order to disprove termination, one may for example use the fact that a relation which contains cycles is non-Noetherian. This can be relaxed to looping relations:

Definition: *([Dershowitz 81])*
A rewrite relation $\to$ is called *looping*, if there are terms t, t', an occurrence u, and a substitution σ, such that both $t \to^{+} t'$ and $t'/u = t\sigma$. In other words, there is a derivation where an instance of the first term appears as a subterm in the last one.

Fact: *([Dershowitz 81])*
A rewrite system R whose rewrite relation $\underset{R}{\to}$ is looping, is non-Noetherian.

□

The rewrite system $R =_{def} \{x+y \to f(y+s(x))\}$ for instance has a looping derivation

$$x+x \underset{R}{\to} f(x+s(x)) \underset{R}{\to} f(f(s(x)+s(x)))$$

where $u = 1.1$ and $\sigma = [s(x) / x]$. For this reason, R is not Noetherian.
Now a *left-erasing* rewrite rule $l \to r$ always admits a looping derivation $l \underset{R}{\to} r[l/x]$ where x denotes a variable that occurs in r but not in l. A *left-isolating* rule $x \to r$ even is already a looping derivation. So we have the following lemma, which is commonly known, but has apparently not yet been written down:

Fact:
If R is Noetherian, then R is left-nonerasing and left-nonisolating.

□

(This does not carry over to *many-sorted* systems. For instance if a: B, (" a has type B ") and f: A $\rightarrow$ B, then the rewrite system a $\rightarrow$ f(x) is Noetherian although left-erasing. The candidate for a loop, a $\rightarrow$ f(a) $\rightarrow$ f(f(a)) $\rightarrow$ ..., is ill-sorted.)

For relative termination we have a similar property. First, we need one more (very uncomfortable) technical notion:

Definition:

A rewrite rule $l \rightarrow r$ is called *right-nonduplicating*, if $l \in X$ and $r/u = r/v = l$ imply $u = v$. In words: $l \rightarrow r$ is right-nonduplicating, if l is not an isolated variable that occurs more than once in r. ("right-nonduplicating" is a weakening of "right-linear" and of "left-nonisolating".)

Theorem: *(necessary condition)*

Let R/S be Noetherian, and let R contain at least one rule $g \rightarrow d$ where $Var(d) \neq Ø$. Then S is left-nonerasing and right-nonduplicating.

Proof:

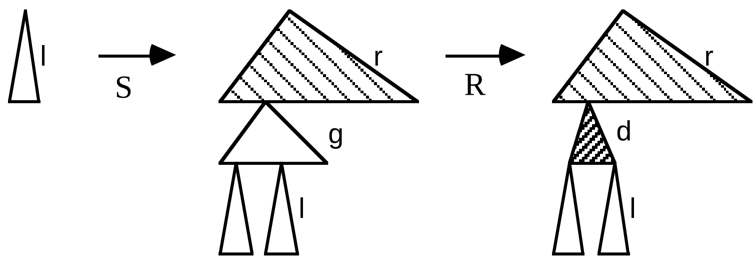
Since R/S is Noetherian, in particular R is Noetherian. So we may already assume that R is both left-nonerasing and left-nonisolating (see previous chapter). We claim that the existence of any left-erasing or right-duplicating rule $(l \rightarrow r) \in S$ causes a looping derivation for S^*R. Without loss of generality, we may assume that

$Var(R) \cap Var(S) = Ø$.

1. *(for symmetric S, see [Jouannaud, Kirchner 86])*

Assume that $l \rightarrow r$ is left-erasing, i.e. that there is some $x \in Var(r) \setminus Var(l)$. Due to the premises, there is at least one rule $(g \rightarrow d) \in R$ where $y \in Var(d)$ for some suitable y. Moreover, $y \in Var(g) \cap Var(d)$ because R is left-nonerasing. Hence we have the looping derivation $l \underset{S}{\rightarrow} r[g/x][l/y] \underset{R}{\rightarrow} r[d/x][l/y]$.

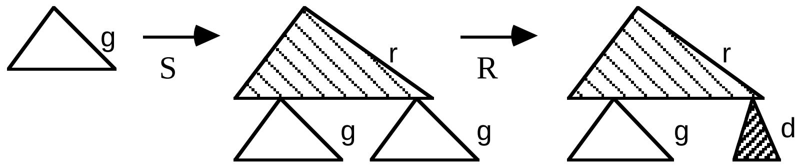
Informally, the new variable in r carries a copy of l, which is preserved by the R-step. This is illustrated in the following diagram:



2.

Now let $(g \rightarrow d) \in R$, and let $l \rightarrow r$ be right-duplicating, i.e. $(x \rightarrow r) \in S$ where $r/u = r/v = x$ and $u \neq v$. Call r' the term $r' =_{def} r[u \leftarrow d]$. Then $x \in Var(r')$ because $r'/v = x$. Thus we can construct the looping derivation $g \underset{S}{\rightarrow} r[g/x] \underset{R}{\rightarrow} r'[g/x]$.

Informally, instantiating the variable x by g, one of the two copies of g can be used for an R-step $g \to d$, and the other one to repeat the game.



□

In the case of symmetric S, the above conditions meet the ones mentioned in [Jouannaud, Muñoz 84] (without the above marginal restriction put on R): S is (both left- and right-) nonerasing, and nonduplicating. The merit of relaxation to an arbitrary S is indicated by the idempotence rule $f(x, x) \to x$: Idempotence is admissible in S straight away, but its inverse $x \to f(x, x)$ is not admissible (otherwise relative termination is lost).

2.3. Some termination quasiorderings

Now that the notion of relative termination is settled, and a necessary syntactic criterion is available, we may start to develop sufficient criteria for relative termination. Termination quasiorderings play a fundamental role in proving termination of rewrite systems. See [Dershowitz 87] or [Dershowitz, Jouannaud 89] for a comprehensive treatment. The class of simplification orderings is a well known class of termination quasiorderings. Among them the lexicographic recursive path ordering, and the polynomial interpretation ordering are worth mentioning. We will briefly describe these two orderings, where the description of the lexicographic path ordering by means of a finite term rewrite system with *one* hidden function is new.

A binary relation R is Noetherian if and only if its transitive closure R^+ is Noetherian. It is therefore sensible to investigate *Noetherian orderings* (elsewhere also called well-founded orderings), i.e. transitive and Noetherian relations. A Noetherian ordering on terms, closed under contexts and instantiation, is called a *termination ordering*. (A Noetherian ordering closed under contexts is elsewhere called a reduction ordering.) For instance, if R is a Noetherian term rewrite system, then the transitive closure $\underset{R}{\to}^+$ of the term rewrite relation is a termination ordering. This motivates the following general proof method:

Fact: *([Manna, Ness 70])*
A rewrite system R is Noetherian if and only if, there is a termination ordering $>$ such that $R \subseteq >$.

□

In other words, a termination proof for a rewrite system R consists of a suitable *termination ordering* $>$ such that $l > r$ holds for all rules $(l \to r) \in R$. Finding a termination ordering however may be difficult. Termination of rewrite systems has been

shown undecidable even for strongly restricted classes of rewrite systems, for the class of single rule systems ([Dauchet 88]) for example, or for the class of rewrite systems where all function symbols have arity 0 or 1 ([Huet, Lankford 78]). These negative results posed the challenge of designing powerful termination orderings.
For technical reasons, a termination ordering is often provided by a quasiordering:

Definition:
1. A *Noetherian quasiordering* is a quasiordering $\geq$ whose associated strictordering $>$ is Noetherian.
2. A *termination quasiordering* is a quasiordering closed under contexts and instantiation whose strictordering is a termination ordering.

□

(The notion of Noetherian quasiordering is strongly related to that of a well-quasiordering, as pointed out in [Dershowitz, Jouannaud 89].) Proofs of termination modulo actually require a Noetherian *quasiordering* because both the associated strictordering and the associated equivalence relation are needed for the proof.
Most of the currently known termination quasiorderings are simplification orderings:

Definition:
The *subterm ordering* $|\geq$ is defined by $t \mathrel{|\geq} t/u$, whenever $u \in Occ(t)$. A quasiordering that extends the subterm ordering and is closed under contexts, is called a *simplification ordering*.

□

It is known that, as an obvious consequence of Kruskal´s tree theorem, every simplification ordering is Noetherian. (Commonly, the subterm condition is replaced by a slightly stronger condition: For all t, and $u \neq \lambda$, the inequality $t > t/u$ must hold, in other words, $|> \subseteq >$ must hold. Note that the above definition, like the one in [Dershowitz, Jouannaud 89], rather admits $t \sim t/o$, too, which may be advantageous in the framework of relative termination.)
Among the simplification orderings, the two most popular subclasses are the path orderings, with the *lexicographic (recursive) path ordering* ([Dershowitz 79], [Kamin, Lévy 80], [Dershowitz 82]) as prominent representative, and the homomorphic interpretation orderings, where the *polynomial interpretation ordering* ([Lankford 75], [Lankford 79], [Ben Cherifa, Lescanne 87]) is known best.
Klop gave an excellent description of recursive path ordering in [Klop 87], Def. 3.3, by means of a term rewrite system with hidden functions. The following is a slightly changed variant of it:

Definition:

The class of *lexicographic (recursive) path orderings* is described by the following scheme: Suppose we have a quasiordering $\geq$ on F, the so-called *precedence*. Next, each $f \in F$ either has some *lexicographic status*, given by a permutation on the set $\{1, ..., arity(f)\}$ of argument positions, or f *has multiset status*, or it has none of them (indifferent status). If f is a binary function symbol, then the two lexicographic statuses are also referred to as left-to-right (i.e. the identical permutation) and right-to-left. We will use the abbreviation $\pi(t_1, ..., t_n) =_{def} (t_{\pi(1)}, ..., t_{\pi(n)})$ for the application of a permutation to a sequence of terms.

Let there be a fresh unary function symbol *, i.e. $* \notin F$, with arity(*) = 1. For simplicity of notation, we drop the pair of parentheses after *. The symbol * is called the *marker symbol*. A marked term *t may be taken as a nondeterministic placeholder for some term smaller than t itself. (Accordingly, the following rewrite system is non-confluent, see [Hußmann 89].) The finite rewrite system RPO on terms in the extended signature $F \cup \{*\}$ is given by the following rules (assume n = arity(f), k = arity(g)):

Introduce marker: $x \to *x$
Make copies below strictly lesser top: $*f(x_1, ..., x_n) \to g(*f(x_1, ..., x_n), ..., *f(x_1, ..., x_n))$ if $f > g$
Push marker down (lex): $*f(\pi(x_1, ..., x_n)) \to g(\rho(x_1, ..., x_{i-1}, *x_i, *f(\pi(x_1, ..., x_n)), ..., *f(\pi(x_1, ..., x_n))))$ if $f \sim g$ have lexicographic status π^{-1}, ρ^{-1}, respectively, and $i \in \{1, ..., \min(n, k+1)\}$
Push marker down (mult): $*f(x_1, ..., x_n) \to g(\pi(x_1, ..., x_{i-1}, *x_i, ..., *x_i, x_{i+1}, ..., x_n))$ if $f \sim g$ have multiset status, $i \in \{1, ..., n\}$, $k \geq n-1$, and π denotes an arbitrary k-permutation
Select argument: $*f(x_1, ..., x_n) \to x_i$ if $i \in \{1, ..., n\}$

Now let $>_{rpo}$ denote $\xrightarrow[RPO]{}^{+}$ restricted to terms that do not contain markers. $>_{rpo}$ is called the *lexicographic path ordering (with precedence > and status).*

□

By definition, $>_{rpo}$ is transitive, closed under contexts and instantiation (for terms and substitutions that do not contain a marker), and contains the strict subterm ordering. Moreover, it can be shown that $>_{rpo}$ is irreflexive. Hence we have:

Fact:
$>_{rpo}$ is a simplification ordering, closed under instantiation.

□

Note that the first rule in RPO is left-isolating — see section 1.4. (We omit the proof that $>_{rpo}$ matches the definition in [Kamin, Lévy 80]. Elsewhere, $>_{rpo}$ is also called the generalized lexicographic path ordering, or the recursive path ordering with status.)

Example:
Let $R =_{def} \{s(x)+y \to x+s(y)\}$. Then R is Noetherian, proven by the lexicographic path ordering with precedence $+ > s$, and $+$ having status left-to-right. The proof amounts to show $R \subseteq >_{rpo}$, i.e. $s(x)+y >_{rpo} x+s(y)$. Redices are underlined:

$$\begin{array}{ll}
\underline{s(x)+y} & \xrightarrow[\text{Introduce marker}]{} \\
\underline{*(s(x)+y)} & \xrightarrow[\text{Push marker down (lex)}]{} \\
\underline{*s(x)}+*(s(x)+y) & \xrightarrow[\text{Select argument}]{} \\
x+\underline{*(s(x)+y)} & \xrightarrow[\text{Make copies below strictly lesser top}]{} \\
x+s(\underline{*(s(x)+y)}) & \xrightarrow[\text{Select argument}]{} \quad x+s(y).
\end{array}$$

□

Klop´s presentation differs in several aspects:
(1) He uses $\{*f.\ f \in F\}$, rather than $\{*\}$ as the set of new function symbols. In other words, the marker is part of the function symbol $*f$. This precludes him from comfortably using the marker at variables like for example in $*x$.
(2) Klop defines an infinite (ground) tree replacement system. His rule "In Context" and his use of replacement schemata indicate that there is an equivalent *finite rewrite system*.
(3) Klop assumes that function symbols have variable arity. This is not necessary; a function symbol with two arities can be split into two different function symbols with fixed arity. This explains the additional function symbol g in the rule "Push marker down (mult)". In order to keep the original power, the set F of function symbols should be sufficiently rich. For $f(t_1, t_2, t_3) >_{rpo} g(t_3)$, for instance, there should be an "interpolating" function symbol $h \sim f$ with $arity(h) = n-1$ whenever $f \sim g$ have multiset status and $k < n-1$ holds. The proof works by

$$f(t_1, t_2, t_3) >_{rpo} h(t_1, t_3) >_{rpo} g(t_3).$$

Note that *finitely many* such additional functions are required.
(4) In [Klop 87], terms are considered up to permutations of arguments — it saves technical trouble for the multiset status. But it forbids one to have both function symbols with lexicographic status and function symbols with multiset status at the same time.

(Klop´s assumption can be taken into account by *equational rewriting*, with permutation equations for each function symbol that has multiset status.)

The lexicographic path strictordering can easily be extended towards a quasiordering $\geq_{rpo}$ where $t \sim_{rpo} t'$ holds if t and t' differ only by function symbols which are equivalent in the precedence, and by permutations of parameters of function symbols which have multiset status. For classifications of path orderings with status and Knuth-Bendix orderings, see [Rusinowitch 87b], [Steinbach 88], [Dershowitz, Okada 88], and [Lescanne 89]. Knuth-Bendix orderings are not treated here (see also the conclusion of this thesis).

A function $[\_]: F \to \mathbb{N}(X)$ that maps n-ary function symbols to polynomials in n variables with coefficients from $\mathbb{N}$, is called a *polynomial interpretation*. In a straightforward way, $[\_]$ is homomorphically extended to terms, yielding a function $[\_]: Term \to \mathbb{N}(X)$. (Recall that $(Term, F)$ forms an algebra. Likewise does $(\mathbb{N}(X), \mathbb{N}(X))$ form an algebra.) It is known that, provided the subterm property holds, the polynomial interpretation ordering » induced by

$$t \gg t' \Leftrightarrow_{def} \text{the polynomial } [t] - [t'] \text{ is positive everywhere,}$$

is a simplification ordering, closed under instantiation.

By abuse of notation, we will drop square brackets around variables. Likewise, we will use ordinary notation for polynomials, and thus overload function symbols like + with addition on $\mathbb{N}$. Now the rewrite system R above is proven Noetherian using the polynomial interpretation

$$[s(x)] = x+1, \ [x+y] = 2x+y.$$

We have the proof

$$[s(x)+y] - [x+s(y)] = 2(x+1)+y - (2x+y+1) = 1 > 0.$$

There are many rewrite systems whose termination is impossible to prove by a simplification ordering. The reason is that they admit a *(homeomorphically) self-embedding* derivation: (t, t') is called self-embedding, if $t \xrightarrow[\lhd|]{}^{+} t'$ holds. (Recall: $\lhd|$ denotes the subterm strictordering.) For such a situation, there is the class of semantic path orderings ([Kamin, Lévy 80], [Dershowitz 87]). Sometimes also a "hand-made" ordering works:

Example: *(FF)*

Let $R =_{def} \{ffx \to fgfx\}$. (The only function symbols f and g are assumed unary, and in the case where all function symbols have arity 0 or 1, parentheses may be omitted without raising confusion. Such rewrite systems enjoy a close relationship to Thue systems.) R is self-embedding, as we now show. If there is a termination ordering $> \supseteq R$, then $ffx > fgfx$ holds. On the other hand, if $>$ is a simplification ordering, then by the subterm property, $gfx \geq fx$ holds, so by closure under contexts, $fgfx \geq ffx$, which contradicts $>$ irreflexive. So every simplification ordering must fail to prove R Noetherian. Though R is Noetherian, proven by the Noetherian ordering $>$ defined by

$$t \geq t' \Leftrightarrow_{def} \forall\sigma.\ \#\, t\sigma \geq_{\mathbb{N}} \#\, t'\sigma \ \wedge\ \#\, ft\sigma \geq_{\mathbb{N}} \#\, ft'\sigma,$$

where $\#t$ denotes the number of pairs of "ff patterns" (i.e. pairs of adjacent f symbols) in t. The complicated definition of the ordering is to ensure that $>$ is closed under contexts and instantiation.

□

2.4. How to prove relative termination

Proving relative termination, like proving termination and termination modulo, is based on Noetherian quasiorderings. Termination modulo can even be *characterized* by means of a Noetherian quasiordering. It is, however, still unclarified whether the corresponding characterization also holds for relative termination. We can answer positively for the case where the acyclic part of S is Noetherian — it is a little more general than termination modulo.

Termination modulo can be characterized by a Noetherian quasiordering, as follows:

Fact:

Let R and S denote binary relations. $R/\overline{S}$ is Noetherian if and only if, there is a Noetherian quasiordering $\geq$ such that $R \subseteq >$ and $S \subseteq \sim$ hold.

□

This characterization suggests an extension towards relative termination. As we will see later, a characterization of relative termination by means of a quasiordering is a nontrivial problem. For the moment, let us state the important fact that the existence of a Noetherian quasiordering is *sufficient*:

Fact: *(quasiordering lemma)*

If there is a Noetherian quasiordering $\geq$ where $R \subseteq >$ and $S \subseteq \geq$, then R/S is Noetherian.

□

Now let us consider some obvious applications of quasiorderings for proving a term rewrite system relatively Noetherian. On the spot, the criterion can be instantiated with termination quasiorderings.

Theorem: *(termination quasiordering criterion)*

Let R and S denote rewrite systems. If $\geq$ is a termination quasiordering, and $R \subseteq >$ and $S \subseteq \geq$ hold, then R/S is Noetherian.

Proof:

By definition, $>$ also is closed under contexts and instantiation. Hence $\xrightarrow[S]{} \subseteq \geq$ and $\xrightarrow[R]{} \subseteq >$. The claim follows by the "quasiordering lemma" above.

□

So termination quasiorderings are applicable for proofs of relative termination. This includes the class of simplification orderings:

Corollary:

Let R and S denote rewrite systems.

1. Let $\geq_{rpo}$ denote any lexicographic path ordering. If $S \subseteq \geq_{rpo}$ and $R \subseteq >_{rpo}$, then R/S is Noetherian.

2. Let [_] denote any polynomial interpretation. If $[l] - [r] \geq 0$ for every $(l \rightarrow r) \in S$ and $[l] - [r] > 0$ for every $(l \rightarrow r) \in R$, then R/S is Noetherian.

Example:

1. *(Nonfin)*

Let $S =_{def} \{cx \rightarrow fcx\}$, $R =_{def} \{csx \rightarrow cx\}$. In order to prove that R/S is Noetherian, choose a polynomial interpretation: Take $[cx] \geq x$, $[sx] > x$ arbitrary, and let $[fx] = x$.

2. *(Set, continued)*

Recall the specification of subsets of {a, b}, with the empty set, an insertion function, and the membership relation:

$R =_{def}$ {elem(x, Ø) → false,
elem(x, ins(x, s)) → true,
elem(a, ins(b, s)) → elem(a, s),
elem(b, ins(a, s)) → elem(b, s)},

$S =_{def}$ {ins(x, ins(x, s)) → ins(x, s), *"left-idempotence"*
ins(x, ins(y, s)) → ins(y, ins(x, s))}. *"left-commutativity"*

We claimed that R is relatively Noetherian to S. This is proven for example by the polynomial interpretation defined by

[true] = [false] = [a] = [b] = [Ø] = 2,

[ins(x, s)] = [elem(x, s)] = x+s.

We have in particular for the left-idempotence rule:

$[ins(x, ins(x, s))] - [ins(x, s)] = x+x+s - (x+s) = x > 0$,

and for left-commutativity:

$[ins(x, ins(y, s))] = x+y+s = [ins(y, ins(x, s))]$,

This suffices to prove R relatively Noetherian to S, but not yet to prove R∪S Noetherian.

□

Let us now stop with the sufficient conditions of relative termination. The rest of this section investigates when the existence of a Noetherian quasiordering is also *necessary* for relative termination. To begin with, relative termination is, in a straightforward way, characterized by a pair composed of a quasiordering and a strictordering ($\geq$ and $»$):

Lemma: *(two orderings)*
Let R and S denote binary relations. R/S is Noetherian if and only if, there are a Noetherian strictordering $» \supseteq R$ and a quasiordering $\geq \supseteq (» \cup S)$, such that $\geq» \subseteq »$ holds.

Proof:
($\Rightarrow$) Set $» =_{def} (R/S)^+$ and $\geq =_{def} (R \cup S)^*$.
($\Leftarrow$) It can easily be shown that $(R \cup S)^+ \subseteq \geq$ and then that $(S^*R)^+ \subseteq »$ holds. Since $»$ is Noetherian, S^*R and thus R/S is Noetherian.

□

Instantiating $» =_{def} >$, we obtain the "quasiordering lemma" again. But otherwise, we must look for both, a quasiordering $\geq$ and a Noetherian subrelation $»$, in order to prove relative termination now. Can we get out of this inconvenience? Here is an example of a quasiordering $\geq$ where $>$ is not Noetherian but has Noetherian subrelations:

Example:
Let $\geq$ denote the natural ordering on $\mathbb{Q}^+$, the set of positive rational numbers. The strictordering $> =_{def} \geq \setminus \leq$ is not Noetherian, as it admits the infinite derivation $1 > 1/2 > 1/3 > ...$ On the other hand, the strictordering $»_1$ defined by

$$p »_1 p' \Leftrightarrow_{def} p > p'+1 ,$$

is actually Noetherian — every derivation starting from p has length bounded by p. Moreover it satisfies both $»_1 \subseteq >$ and $\geq»_1 \subseteq »_1$. Another, less trivial, Noetherian strictordering $»_2$ on $\mathbb{Q}^+$ is defined by

$$p »_2 p' \Leftrightarrow_{def} \exists n, i \in \mathbb{N}.\ p > n + \frac{i}{i+1} \geq p' .$$

Its termination proof relies on the fact that $>$ restricted to the set $\{n + \frac{i}{i+1}.\ n, i \in \mathbb{N}\}$ is Noetherian, as it is order-isomorphic to $\mathbb{N} x \mathbb{N}$ with lexicographic order.

□

As we see, it is by no means obvious whether $\geq$ can always be chosen such that $>$ is Noetherian. We are lucky when the acyclic part $S \setminus (S^{-1})^*$ of S is Noetherian. Then the converse of the "quasiordering lemma" holds, choosing the straightforward ordering $\geq = (R \cup S)^*$.

Lemma: *(quasiordering supplement)*
If both $S \setminus (S^{-1})^*$ and R/S are Noetherian, then there is a Noetherian quasiordering $\geq$ where $R \subseteq >$ and $S \subseteq \geq$.

Proof:
One easily proves by induction on n that $(S \setminus (S^{-1})^*)^n = S^n \setminus (S^{-1})^*$. Hence the transitive closure of $S \setminus (S^{-1})^*$ is $S^+ \setminus (S^{-1})^*$. It is Noetherian by premise.

Because R/S is Noetherian, $(R/S)^+$ is irreflexive, and so

$$(R/S)^+ \cap ((R \cup S)^{-1})^* = \emptyset .$$

This property will be used in the following reasoning.

Let $\geq =_{def} (R \cup S)^*$. It remains to be shown that $\geq \backslash \leq$ is Noetherian.

$$\begin{aligned} > &= (S^+ \cup (R/S)^+) \setminus ((R \cup S)^{-1})^* \\ &= S^+ \setminus ((R/S)^{-1})^+ \setminus (S^{-1})^* \cup (R/S)^+ \\ &= S^+ \setminus (S^{-1})^* \cup (R/S)^+. \end{aligned}$$

Since both $S^+ \setminus (S^{-1})^*$ and $(R/S)^+$ are Noetherian, so is $>$. The reason is that an infinite $R \cup S$-derivation either contains an infinite $S^+ \setminus (S^{-1})^*$-derivation, or contains infinitely many R-steps, in which case there is an infinite R/S-derivation. (See also the "inheritance by transitivity" lemma in section 3.1.)

□

On account of the "quasiordering supplement" lemma, it is useful to know whether $S \setminus (S^{-1})^*$ is Noetherian. This is the case, especially, when $S \setminus (S^{-1})^* = \emptyset$, i.e. when S is cyclic. Therefore the characterization is no problem in the termination modulo approach, where S is always cyclic. The following criterion is a little more general:

Lemma: *([Guttag et al. 83])*

If $S^+ \setminus (S^{-1})^*$ is finitely branching, then $S \setminus (S^{-1})^*$ is Noetherian.

Proof:

$S^+ \setminus (S^{-1})^*$ is transitive, and irreflexive. Then it is in particular acyclic. According to [Huet 80], a finitely branching and acyclic relation is Noetherian.

□

The question remains open whether the condition "$S \setminus (S^{-1})^*$ Noetherian" may still be relaxed, in the following sense: For all R, S, where R/S is Noetherian, does there exist some $S' \supseteq S$ such that both R/S' and $S' \setminus (S'^{-1})^*$ are Noetherian? In the following example, there is still such an S´:

Example: *(FF, continued)*

Let the term rewrite systems $R =_{def} \{ffx \to fgfx\}$ and $S =_{def} \{fa \to gfa\}$ be given. R/S is Noetherian but $S \setminus (S^{-1})^* = S$ is not. $S' \supseteq S$ must be chosen such that S´ satisfies $S' \setminus (S'^{-1})^*$ Noetherian. That can only be achieved if for suitable $m > n$, S´ contains a cycle of the form $g^m fa \to^+ g^n fa$. The value $n = 0$ is badly chosen since it would cause a cycle in R/S´, implying that R/S´ is not Noetherian. But for instance the choice $S' = S \cup \{ggfa \to gfa\}$ works.

□

2.5. Relative termination in restricted systems

Now let us consider a special case which has been studied in the literature: If all infinite R-derivations contain a cycle, then R is called quasi-terminating. In order to prove that a quasi-terminating R is Noetherian, it is sufficient to show that R admits no cycles. This is the underlying idea of the two-step termination proof technique in [Guttag et al. 83]. A natural question is, whether the same technique is applicable for relative termination of R to S.

The property "R^+ finitely branching" is called "R globally finite" in [Huet 80] and [Guttag et al. 83], and "R quasi-terminating" in [Dershowitz 87]. The termination proof method in [Guttag et al. 83] says: In order to prove R terminating, first prove that R is quasi-terminating, then prove that R satisfies some strictordering. The idea works for proofs of relative termination, too.

Lemma: *(for S = Ø, see [Guttag et al. 83])*
Let $R \cup S$ be quasi-terminating. R/S is Noetherian if and only if, there is a quasiordering $\geq$ such that both $R \subseteq >$ and $S \subseteq \geq$.

Example: *(Set, continued)*
Call a rule $l \to r$ *length-reducing,* if $|Occ(l)| > |Occ(r)|$ and every variable occurs in l at least as often as in r ([Guttag et al. 83]). The latter condition is called left-dominance in [Drosten 89]; here it ensures closure under contexts and instantiation.

$R =_{def}$ {elem(x, Ø) $\to$ false,
elem(x, ins(x, s)) $\to$ true,
elem(a, ins(b, s)) $\to$ elem(a, s),
elem(b, ins(a, s)) $\to$ elem(b, s)},

$S =_{def}$ {ins(x, ins(x, s)) $\to$ ins(x, s), *"left-idempotence"*
ins(x, ins(y, s)) $\to$ ins(y, ins(x, s))}. *"left-commutativity"*

R/S is Noetherian, because

(1) $R \cup S$ is quasi-terminating, as length-reducing.

(2) All rules from R are even *strictly* length-reducing.

□

2.6. On the descriptive power of relative termination

Relative termination generalizes both termination and termination modulo, in the sense that R/S Noetherian is implied by the Noetherian property of $R \cup S$ or $R/\overline{S}$. In this section we will show that the converse is not true, i.e. that there are indeed R and S such that R/S is Noetherian, but neither $R \cup S$ nor $R/\overline{S}$ is.

The Set example may again serve as a motivation. Following [Huet 80], it is quite natural to have a rewrite system S that describes the data structures, and another rewrite system R that describes the algorithms. Regarding this, left-commutativity and left-idempotence certainly both belong to S. Now R/S is Noetherian, but R∪S is not Noetherian, because left-commutativity is cyclic. Neither is $R/\overline{S}$ Noetherian:

Example: *(Set, continued)*
Forming the symmetric closure of S turns out harmful to relative termination:
R is not relatively Noetherian to $\overline{S}$, i.e. R is not Noetherian modulo $\overline{S}$, because there is a cycle

$$\text{elem}(a, \text{ins}(b, s)) \underset{S}{\leftarrow} \text{elem}(a, \text{ins}(b, \text{ins}(b, s))) \underset{R}{\rightarrow} \text{elem}(a, \text{ins}(b, s))$$

□

Nevertheless $R/\overline{S}$ Noetherian could be maintained, if left-idempotence was removed from S and put into R instead. Such a move would not work in the following examples:

Example:
1. *(FF, continued)*
Let $R =_{def} \{ffx \rightarrow fgfx\}$ and $S =_{def} \{fa \rightarrow gfa\}$. We already proved that R/S is Noetherian. S and R∪S are obviously not Noetherian. Neither is R/S^{-1} Noetherian (nor $R/\overline{S}$), since there is a cycle

$$ffa \underset{R}{\rightarrow} fgfa \underset{S}{\leftarrow} ffa.$$

2. Consider the rewrite systems

$$R =_{def} \{(x+y)*z \rightarrow x*z+y*z\} \quad \text{and}$$
$$S =_{def} \{x*x+y*y \rightarrow x*y+x*y\}.$$

R is the right-distributive law, S is a rule like $x^2+y^2 \rightarrow 2xy$. Neither S nor S^{-1} is Noetherian, because the left and the right hand side have a common instance x*x+x*x. So, particularly, neither R∪S nor $R \cup S^{-1}$ are Noetherian. Nor is R/S^{-1} Noetherian, nor $R/\overline{S}$, because of the looping derivation

$$x*(x+x) + x*(x+x) \underset{S}{\leftarrow} x*x + (x+x)*(x+x) \underset{R}{\rightarrow} x*x + (x*(x+x) + x*(x+x)).$$

R/S in turn *is* Noetherian, as can be proven by the polynomial interpretation

$$[x+y] = x+y+c, \quad [x*y] = x*y,$$

for arbitrary $c > 0$. One gets

$$[(x+y)*z] - [x*z+y*z] = (x+y+c)z - (xz+yz+c) = (z-1)c > 0 \quad \text{and}$$
$$[x*x+y*y] - [x*y+x*y] = x^2+y^2+c - (2xy+c) = (x-y)^2 \geq 0.$$

Of course one can find instantiations for x and y such that $x-y = 0$, and likewise there are instantiations such that $x-y \neq 0$. But none of the two cases holds uniformly.

□

The mentioned examples demonstrate that relative termination has strictly greater expressive power than termination modulo.

3. How to strengthen termination orderings

The previous chapter introduced relative termination and compared it to the related notions of termination and termination modulo. The main question of this chapter will be, how to obtain from a (relative) termination result a *stronger* one. Two basic concepts are investigated:

(1) Termination inheritance: Infer $R \cup S$ Noetherian from R/S Noetherian, and

(2) Commutation and Cooperation: Infer R/S Noetherian from R Noetherian.

In the first case, the knowledge of relative termination is applied, whereas in the second case, it is derived. We have seen in the previous chapter already that the implications are not generally valid. So what we are after, is a set of sufficient conditions.

Inheritance of termination means the transferance of termination from the components R and S to the termination of the composed system $R \cup S$. Termination inheritance has been studied successfully for the direct sum of term rewrite systems. Briefly speaking, transitivity turns out to be another sufficient condition for inheritance: If $R \cup S$ is transitive, then the termination of $R \cup S$ follows from the termination of both R and S. This property gives rise to a couple of lemmas concerning the inheritance of relative termination. One of these lemmas admits an interpretation as a termination proof method by the lexicographic combination of termination orderings. A current major weakness of this method leads us to the second problem area of this chapter:

Many currently available termination quasiorderings, for example path orderings, enjoy a considerable expressive power, but on the other hand, have a small associated equivalence relation. They can rarely be directly used for relative termination. Having a means to strengthen a result "R is Noetherian" to "R is relatively Noetherian to S" is therefore very important.

If R commutes over S, then all R-steps in an $R \cup S$-derivation can be shifted towards the beginning. Thus a derivation that contains infinitely many R-steps can be transformed into an infinite R-derivation. This reasoning led to criteria for termination modulo ([Jouannaud, Muñoz 84]) and relative termination ([Bachmair, Dershowitz 86], [Bellegarde, Lescanne 86], [Bellegarde, Lescanne 87]). The essential commutation-like property is called *cooperation*. We will generalize the cooperation idea, so as to infer "$R/(S \cup Q)$ Noetherian" from "R/S Noetherian" in a fairly general setting. Two local conditions for cooperation are investigated here: The first one redraws the local cooperation approach, which becomes the special case $Q = S^{-1}$. The second one is a new property, *strong cooperation*. It is similar to Huet´s strong confluence. This approach covers the quasi-commutation approach, setting $S = Ø$. All currently known termination criteria based on commutation-like properties are thus instances of one scheme.

In order to get effectively verifiable criteria, the term rewrite structure must finally be taken into account, leading to *critical pair criteria*. This is a most typical step in term rewriting. First the notion of critical pair criterion is explained in full generality. Then we state some critical pair criteria for cooperation, and using some of the inheritance results, critical pair criteria for termination of term rewrite systems. A couple of examples taken from the field of algebraic specification conclude this chapter.

3.1. Termination inheritance

It is obvious that $R \cup S$ Noetherian implies both R Noetherian and S Noetherian. The converse is usually not the case. If $R \cup S$ Noetherian is equivalent to R Noetherian and S Noetherian, then one may say that $R \cup S$ *inherits termination* from R (and S). On this account, the adjective "relative" in "relative termination" is justified, because on the one hand, R is Noetherian if and only if, R is relatively Noetherian to Ø, and on the other hand, $R \cup S$ inherits termination from S by the relative termination of R to S.

A number of termination inheritance criteria exist for a rather special case: R and S use no common function symbols. Then, $R \cup S$ is also called the *direct sum* of R and S ([Toyama et al. 87], [Rusinowitch 87a], [Middeldorp 89]). In this section a quite different termination inheritance result is presented which relies on a *transitivity* requirement. A few applications of the inheritance result are shown.

Theorem: *(termination inheritance by transitivity)*
Let R and S denote binary relations such that $R \cup S$ is transitive. Then $R \cup S$ is Noetherian if and only if, both R and S are Noetherian.

Proof:
(I sent the claim as a question to the "rewriting" mailbox at CRIN (Centre de Recherche en Informatique, Nancy), and got several beautiful proofs, from Jean-Pierre Jouannaud, Dieter Hofbauer, Thomas Streicher, Werner Nutt, Franz Baader, and George McNulty. There were three kinds of proofs:
1. by the infinite version of Ramsey´s theorem,
2. by minimal counterexample, similar to the Nash-Williams proof of Kruskal´s tree theorem,
3. by a case analysis on R-normal forms.
The following proof (scheme 3) has been communicated by Dieter Hofbauer.)

For ease of notation, let $\rightarrow$ denote the relation $R \cup S$. The proof is done by contradiction. For this purpose let $t_1 \rightarrow t_2 \rightarrow ...$ denote an infinite $\rightarrow$-derivation, i.e. $t_i \rightarrow t_j$ holds for all $i < j$, due to transitivity of $\rightarrow$. Next let $C =_{def} \{t_1, t_2, ...\}$, and let M denote the set of all elements of C which are R-normal. We show by case analysis on the cardinality of M that either an infinite R-derivation or an infinite S-derivation can be constructed, each one yielding a contradiction.

Case 1: M is infinite.

Then $M = \{t_{i_1}, t_{i_2}, ...\}$ where $i_1 < i_2 < ...$ are ascending indices. Then $t_{i_1} \rightarrow t_{i_2}$ but t_{i_2} is in R-normal form, so $t_{i_1}\ S\ t_{i_2}$ must hold. Likewise $t_{i_1}\ S\ t_{i_2}$ and so forth. Summarized, $t_{i_1}\ S\ t_{i_2}\ S\ ...$ is an infinite S-derivation.

Case 2: M is finite.

Let $n =_{def} \max \{i.\ t_i \in M\}$. Then for all $k > n$ there is $k' > k$ such that $t_k\ R\ t_{k'}$ holds. This way, one gets an infinite R-derivation.

□

Immediately a few applications of this criterion can be seen. For instance, $(RS^*)^+ = R^+ \cup (R^+S^+)^+$, so: R/S is Noetherian if and only if, both R and R^+S^+ are. Some particularly interesting applications for relative termination are listed in the following corollary. We will use them at the end of this chapter.

Corollary: *(inheritance of relative termination)*

Let R, S, and Q denote arbitrary binary relations.

1. $(R\cup S)/Q$ is Noetherian if and only if, both $R/(S\cup Q)$ and S/Q are.
2. Let $R, S \subseteq Q$. Then $(R\cup S)/Q$ is Noetherian if and only if, both R/Q and S/Q are Noetherian.
3. Let $S \subseteq Q$. Then $R/Q\cup S$ is Noetherian if and only if, both R/Q and S are Noetherian.

Proof:

1:

$((R\cup S)/Q)^+ = (R/Q\cup S/Q)^+ = ((R/Q)/(S/Q))^+ \cup (S/Q)^+ = (R/(S\cup Q))^+ \cup (S/Q)^+$.

Note that $R/(S\cup Q)$ may not be replaced by the weaker $(R/S)/Q$, nor by $R/(S/Q)$.

2:

Actually, this is just a reformulation of 1, by closure under subsets. It will be used in the next chapter, last section.

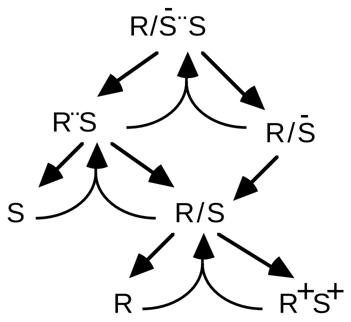
3:

$S^* (R/Q) S^* = R/Q$. So $(R/Q\cup S)^+ = S^* ((R/Q) S^*)^+ \cup S^+ = (R/Q)^+ \cup S^+$.

□

Lemma 1 in [Bachmair, Dershowitz 86] is a special case of our "inheritance of relative termination" corollary, part 1, for $Q = Ø$: $R\cup S$ is Noetherian if and only if, both R/S and S are.

The interdependence of termination between some binary relations that can be built using R and S, is illustrated in the following figure:



Read a (single or double) arrow as "termination of ... and ... entails termination of ..." or read it as "the transitive closure of ... together with the transitive closure of ... is a superset of the transitive closure of ...". The diagram illustrates the central role of R/S among R, R∪S, and R/$\overline{S}$. It shows that the knowledge R/S Noetherian is important, no matter whether S later turns out Noetherian (then R∪S is Noetherian) or cyclic (then we have equational rewriting, and R/$\overline{S}$ is Noetherian) or none of them (particularly important, as we saw in section 2.6). On the one hand, such additional properties of S are not really needed sometimes. For instance rewriting using R with interspersed S-steps is already safe when R/S is Noetherian. Equational rewriting may be generalized on that account. Anyway, it is advisable to leave the decision open whether to switch to R/$\overline{S}$ ("equational rewriting") or to R∪S ("classical rewriting") later.

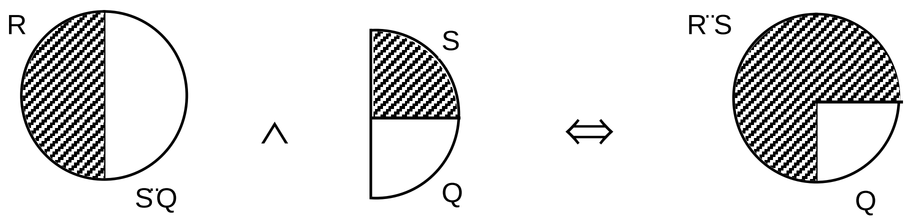
3.2. Lexicographic combination proofs

Recall from the previous section the "inheritance of relative termination" corollary (part 1):

(R∪S)/Q is Noetherian if and only if, both R/(S∪Q) and S/Q are.

This fact is linked to a certain termination proof method — the lexicographic combination of Noetherian orderings. Indeed, the Noetherian ordering for (R∪S)/Q is simply the lexicographic combination of the orderings that prove R/(S∪Q) and S/Q Noetherian. So we have a method to prove termination of rewriting stepwise, by relative termination. In order to demonstrate the strength of the method, we will present two known examples that can be proved Noetherian this way, but cannot be proven by the pure orderings.

The "inheritance of relative termination" corollary (part 1) can be visualized by "cake diagrams":



Shaded areas "relatively terminate to" the white ones. As a mnemonic, one may say that the cake diagram on the right is the cake diagram on the left where the white area is replaced by the cake diagram in the middle. Thus, more and more from the white area becomes shaded.

Provided that $\geq_1$ proves R/(S∪Q) Noetherian, i.e. that $R \subseteq >_1$ and $S \subseteq \geq_1$, and provided that $\geq_2$ likewise proves S/Q Noetherian, we can even state an ordering which proves (R∪S)/Q Noetherian. It is the ordering $(\geq_1, \geq_2)$, the *lexicographic combination* of $\geq_1$ and $\geq_2$. Recall from the "two orderings" lemma, section 2.4, that relative termination is characterized by a pair of quasiordering and strictordering. The reasoning works also in this more general case: Assume that $\geq_1$ and $»_1$ together prove R/(S∪Q) Noetherian, i.e. that $S \cup Q \subseteq \geq_1$ and $R \subseteq »_1$ hold, and moreover assume that $\geq_2$ and $»_2$ together prove S/Q Noetherian, i.e. that $Q \subseteq \geq_2$ and $S \subseteq »_2$ hold. Then the pair $\geq_1 \cup \geq_2$, $»_1 \cup (\geq_1 \cap »_2)$ proves (R∪S)/Q Noetherian, by the reasoning $Q \subseteq \geq_1$, $R \subseteq »_1$, $S \subseteq \geq_1 \cap »_2$. The notion of lexicographic combination may be extended in this respect, towards a combination of pairs of quasiordering and strictordering.

The lexicographic combination of termination orderings for R/(S∪Q) and S/Q provides a termination ordering for (R∪S)/Q. This fact suggests that we prove termination of rewrite systems by lexicographic combination of termination orderings. Interestingly, this proof method is already known, without the background of relative termination. It has been introduced for combinations of polynomial interpretations in [Ben-Cherifa, Lescanne 87], and for combinations of the lexicographic path ordering in [Dershowitz 87]. The combination method sometimes even succeeds when the pure methods fail, as is witnessed by the following two examples:

Example:

1. *([Dershowitz 87], Ex. 18)*

Let f be a unary, g and h be binary function symbols, and let x, y be variables. R and S are defined by

$R =_{def} \{h(f(x), y) \rightarrow f(g(x, y))\}$ and

$S =_{def} \{g(x,y) \rightarrow h(x, y)\}$.

R∪S cannot be proven Noetherian by any recursive path ordering $\geq_{rpo}$. It is easy to see by checking the definition of $\geq_{rpo}$ that the precedence quasiordering ≥ must satisfy $h > f$ and $h \geq g$ in order to prove R Noetherian. The precedence $h \geq g$ however, prevents proving S Noetherian. But $h \sim g$ suffices to prove $S \subseteq \geq_{rpo}$ which altogether yields R/S Noetherian. S may be proven Noetherian separately for example by $\geq_{rpo}$ with precedence $h < g$.

2. *([Lankford 79], Ex. 3, simplified)*

Assume given the following piece of Peano arithmetic:

$R =_{def} \{x*(y+z) \to (x*y)+(x*z)\}$,

$S =_{def} \{0+x \to x, \quad s(x)+y \to s(x+y)\}$,

$E =_{def} \{x+y \to y+x, \quad x+(y+z) \to (x+y)+z\}$.

E is actually cyclic (!), and therefore $[x+y] = [y+x]$ as well as $[x+(y+z)] = [(x+y)+z]$ is to hold. By [Ben-Cherifa, Lescanne 87], Prop. 4, the interpretation of + must be either $[x+y] = x+y+b$, or $[x+y] = a(x+b)(y+b) - b$, for some fixed $a, b \in \mathbb{N}$, $a > 0$. The latter interpretation fails, by $[x*(y+z)] - [x*y+x*z] < 0$. The former interpretation yields $[s(x)+y] - [s(x+y)] = 0$ which suffices for the proof of $R/(S \cup E)$ Noetherian, but not yet of $(R \cup S)/E$ Noetherian. This finally may be established by separately proving S/E Noetherian, for example by the polynomial interpretation $[s(x)] = x+1$, $[x+y] = xy$.

□

With the notion of relative termination, there is another view of the combination method: If $R \subseteq >_1$ and $S \subseteq \geq_1$, then we already proved R/S Noetherian, even if we knew nothing about $\geq_2$. This is important information, as the previous section stressed.

Iteration of the combination method leads to an *incremental* termination proof technique: Suppose the considered rewrite system R is split into slices $R_1, ..., R_n$. Try to prove that $R_1 / (R_2 \cup ... \cup R_n)$ is Noetherian. If this succeeds, R_1 may be completely discarded for the rest of the termination proof. (If it fails, a rearrangement of the slices may help.) It remains to be shown that $R_2 \cup ... \cup R_n$ is Noetherian. Next try to prove that $R_2 / (R_3 \cup ... \cup R_n)$ is Noetherian, and so forth. In that sense, the termination proof may be called incremental. (Compare this with the incremental proof method of [Detlefs, Forgaard 85], which is incremental with respect to the precedence > of $>_{rpo}$.) The main problem is that proofs for $R_1 / (R_2 \cup ... \cup R_n)$ are hard to obtain, since the existing termination quasiorderings $\geq$ are designed for a powerful strictordering $>$, disregarding their equivalence relation $\sim$. All path orderings have a weak equivalence relation $\sim_{rpo}$ (see [Steinbach 88]), hence path orderings are particularly poorly suited for our purposes, the example above being a rare exception. As experience with small examples has shown, polynomial interpretations work a little better than path orderings.

Example: *(INT2-ADD, cf. [Padawitz 88], p. 19)*

Let $R =_{def} \{x+0 \to 0, \quad x+s(y) \to s(x+y)\}$ and

$S =_{def} \{x+(-y) \to -(-x+y)\}$

together define addition on the integer numbers. The polynomial interpretation

$[0] = 2$, $[s(x)] = x+1$, $[x+y] = xy$, $[-x] = x$

proves

$[x+0] - [0] > 0$, $[x+s(y)] - [s(x+y)] > 0$, but only

$[x+(-y)] - [-(-x+y)] = 0$.

So it proves R/S Noetherian, but does not yet prove R∪S Noetherian. Note that the interpretation [-x] = x is perfectly admissible. In order to prove that R∪S is Noetherian, we still have to prove that S is Noetherian. That can be done by another polynomial interpretation, for instance $[x+y] = (x-1)y^2$, $[-x] = x+1$. It yields

$$[x+(-y)] - [-(-x+y)] = (x-1)(y+1)^2 - (1+xy^2) = 2y(x-1)+x-2 > 0.$$

□

The lexicographic combination method can be used, for instance, to show termination in some associative theories, i.e. theories that contain an associativity axiom $A =_{def} \{(x+y)+z \to x+(y+z)\}$. Obviously, A forms a Noetherian rewrite system. Given R∪A, termination of R/A remains to be shown. The method is: Show that $R/\overline{A}$ terminates (remember that $\overline{A} =_{def} A \cup A^{-1}$). It profits from the fact that for the termination of $R/\overline{A}$, special powerful proof tools are available, for example the associative path orderings ([Bachmair, Plaisted 85], [Gnaedig 87]).

Example: *(Associativity and Endomorphism, cf. [Bellegarde 86])*

Let $A =_{def} \{(x+y)+z \to x+(y+z)\}$,

$E =_{def} \{f(x)+f(y) \to f(x+y)\}$,

$E' =_{def} \{f(x)+(f(y)+z) \to f(x+y)+z\}$.

The rewrite rule E specifies that f is an endomorphism for +. E´ appears in order to have a locally confluent rewrite system; E´ might be generated from A and E during the run of a Knuth-Bendix completion procedure. The lexicographic path ordering $>_{rpo}$ can just prove that A∪E is Noetherian, by precedence + > f, and status + lexicographic left-to-right. But the proof extension to E´ fails. $>_{rpo}$ actually cannot prove that A∪E∪E´ is Noetherian.

A∪E∪E´ is Noetherian, because according to our method $(E \cup E')/\overline{A}$ can be proven Noetherian, for example by the polynomial interpretation $[f(x)] = x+1$, $[x+y] = x+y$. Another polynomial interpretation proves A∪E∪E´ Noetherian at once: $[f(x)] = 2x$, $[x+y] = xy+x$ ([Lankford 79]).

□

The method fails when $R/\overline{A}$ cannot be proven Noetherian, as in the following case, due to Franz Baader (personal communication): Let $R =_{def} \{y+(x+y) \to x+x\}$. Then $R/\overline{A}$ is not Noetherian, witnessed by the cycle

$$a+(a+(a+a)) \underset{A}{\leftarrow} a+((a+a)+a) \underset{R}{\rightarrow} (a+a)+(a+a) \underset{A}{\rightarrow} a+(a+(a+a)).$$

Recently, it has been shown by Frank Drewes (personal communication) that nevertheless R/A is Noetherian, via the polynomial interpretation $[f(x,y)] = x^2+xy$.

3.3. Commutation and related properties

The commutation property and its local counterparts play an important role in the interplay of binary relations R and S. Commutation goes back to Hindley ([Hindley 64]).

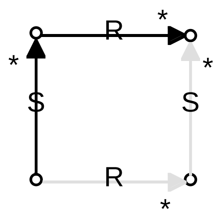
Commutation and some of its variants are used in [Rosen 73] and [Staples 75] for confluence proofs (see [Klop 87] for a collection of examples). Commutation is also an essential ingredient in Peterson and Stickel´s "congruence class approach" ([Peterson, Stickel 81]). In [Raoult, Vuillemin 80] commutation is used for deriving the equivalence of operational and denotational semantics of programing languages. [Dershowitz 81] and [Guttag et al. 83] use commutation for proofs of termination by forward and overlap closures. In [Toyama 88], commutation without termination assumptions is used for confluence proofs.

In this section, we summarize some basic facts about commutation-like properties of binary relations. These facts explain what makes commutation interesting in the framework of relative termination.

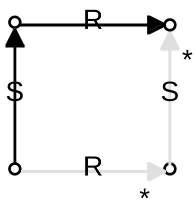
Let us for the moment switch to arbitrary binary relations R and S.

Definition:

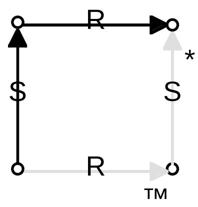
The following diagrams represent some properties which are related to commutation:



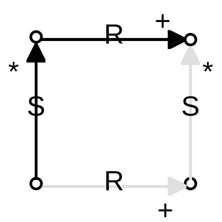
R commutes over S



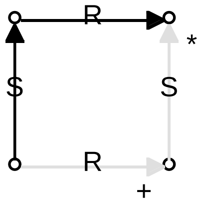
R locally commutes over S



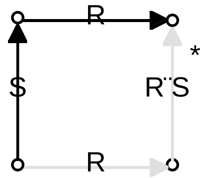
R strongly commutes over S



R strictly commutes over S



R strictly locally commutes over S



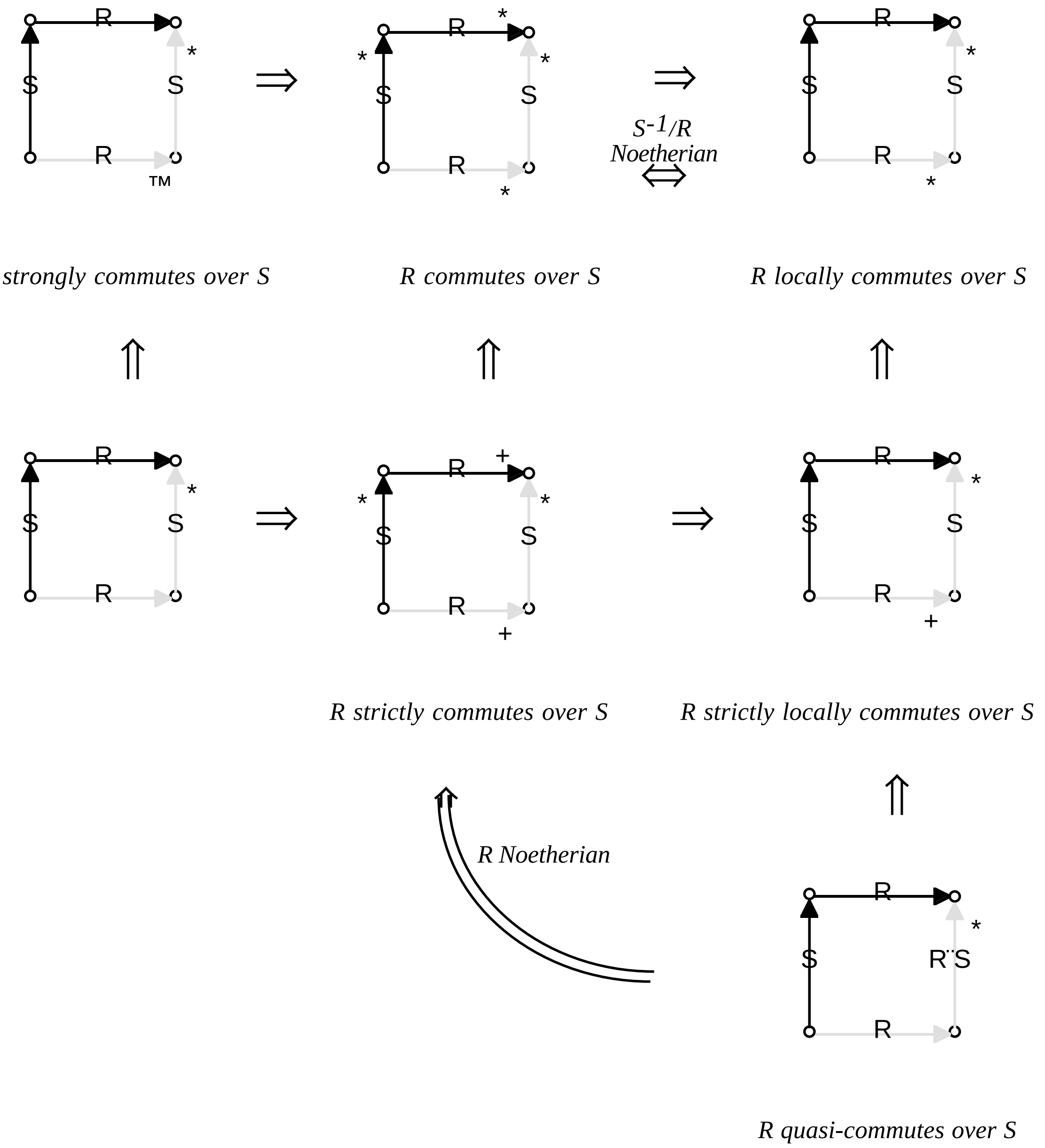
R quasi-commutes over S

□

Bachmair and Derhowitz use the phrase "... *with* S " so as to say "... over S^{-1} ". So for instance "R locally commutes with S" means "R locally commutes over S^{-1}". They also coined the notion of quasi-commutation. (Elsewhere, strict commutation is also called local commutation, and strict local commutation is also called local commutation.)

Lemma:

In the following diagram, some logical dependencies between the various commutation-like properties are drawn. A label at an implication sign is to indicate a sufficient condition for that implication.



Proof:

Most of the implications are standard or even trivial. The equivalence in the topmost line will be proven in the "local cooperation" lemma, in the next section. The curved arrow is proven by straightforward induction along R^+ ([Bachmair, Dershowitz 86]).

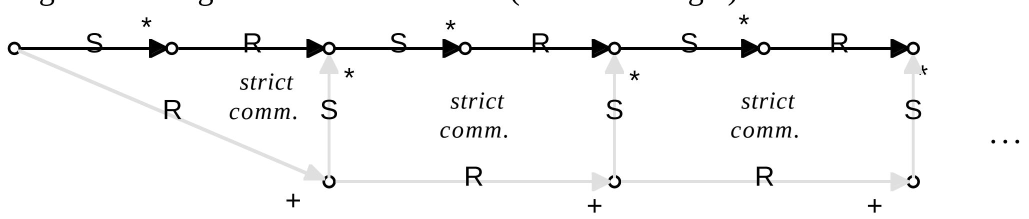
□

If R is Noetherian, it is more convenient to check for strict local commutation than for quasi-commutation: They are equivalent, and checking for strict local commutation is less complex because $R^+S^* \subseteq R(R \cup S)^*$.

Commutation properties contain confluence properties as a special case. For instance, R is confluent if and only if, R commutes over R^{-1}. R is locally confluent if and only if, R commutes locally over R^{-1}. The arrows in the topmost row in the overview above then collapse to the strong confluence lemma of Huet (left arrow), and Newman´s lemma, respectively (right arrows; note that $R/R = R^+$ holds.)
Quasi-commutation is useful in the framework of relative termination, for the following central fact:

Lemma: *(quasi-commutation; [Bachmair, Dershowitz 86], lemma 2)*
If R quasi-commutes over S, then R/S is Noetherian if and only if, R is Noetherian.

Proof:
"Only if" is trivial. For "if", assume R Noetherian and quasi-commuting over S. Then, as we can gather from the overview above, R strictly commutes over S. Now suppose there is a sequence $t_1 \xrightarrow[R \cup S]{} t_2 \xrightarrow[R \cup S]{} \ldots$ that contains infinitely many R steps. Then, the following infinite diagram can be constructed (from left to right):



Thus there is an infinite R^+-derivation which contradicts R Noetherian.

□

Since R/S strictly locally commutes over S, there is even the characterization:

Corollary:
R/S is Noetherian if and only if, there is $R' \supseteq R$, such that both R' is Noetherian and strictly locally commutes over S.

□

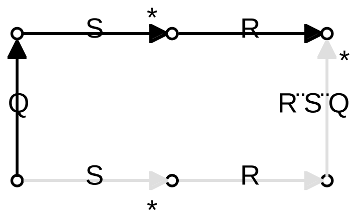
3.4. Cooperation

Commutation-like criteria that are even more interesting and powerful, can also be developed for relatively Noetherian systems. Suppose R, S and Q are binary relations. We seek a criterion for the proposition

"R/S Noetherian implies $R/(S \cup Q)$ Noetherian",

in the spirit of the "quasi-commutation" lemma. In this section we will arrive at such a sufficient condition which we will call *cooperation.*
First observe that $(R / (S \cup Q))^+ = ((R/S) / (S \cup Q))^+$ holds. So it is to be shown that R/S quasi-commutes over $S \cup Q$. (Let us plead for this decision: The other choice "R/S quasi-commutes over Q/S" is equivalent by $(R/S)\,(R/S \cup Q/S)^* = (R/S)\,(R \cup S \cup Q)^*$.

"R/S quasi-commutes over Q" is also sufficient, but more restrictive. It forbids for instance the situation where the diagram only joins by RQS .) Since R/S trivially quasi-commutes over S, it still has to be shown that $Q\, S^{*}RS^{*} \subseteq S^{*}R\,(R\cup S\cup Q)^{*}$. This is achieved by showing that the diagram

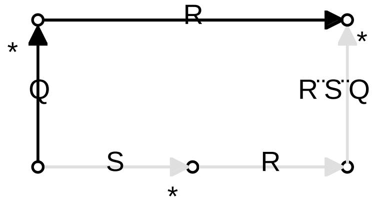


holds.

The first step to local properties now is a separation of the S^{*} and R parts into two diagrams. A naive candidate for the first diagram is commutation of S over Q. For the second diagram, we define:

Definition:

R S-*cooperates over* Q, if



□

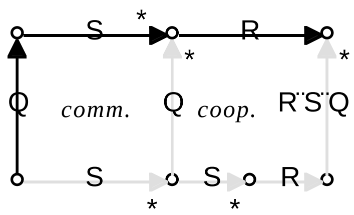
So as to obtain the lemma:

Lemma: *(cooperation)*

Suppose that S commutes over Q, and that R S-cooperates over Q. Then R/(S∪Q) is Noetherian if and only if, R/S is Noetherian.

Proof:

R/S quasi-commutes over S∪Q:



Application of the "quasi-commutation" lemma completes the proof.

□

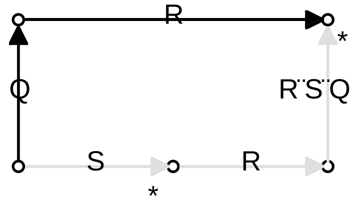
This lemma demonstrates the prominent role of cooperation in proofs of relative termination. Basically the same decomposition idea is briefly sketched in [Bachmair, Dershowitz 86], proposition 1, however for *symmetric* S. The quasi-commutation lemma is a special case, by S = Ø. Likewise, the criterion in [Jouannaud, Muñoz 84] is a special case, with S = Ø and Q symmetric. Another particularly useful special case is

$Q \subseteq S^{-1}$. The notion of cooperation, coined in [Bellegarde, Lescanne 86] ("R S-cooperates over S^{-1} " is called "R cooperates *with* S" there), and investigated also in [Bachmair, Dershowitz 86], theorem 4, describes the case $Q = S^{-1}$. There, the commutation of S over Q becomes the confluence property for S. So we find out that the scenario just sketched covers quite a number of special cases. The next sections will be devoted to further localization, and to executable criteria for cooperation.

3.5. Local cooperation and strong cooperation

The cooperation diagram can be localized. Two localizations will be undertaken below. The first one follows closely the local cooperation approach ([Bachmair, Dershowitz 86]), which it contains for the setting $Q = S^{-1}$. The second approach is new; it uses a local property ("strong cooperation") in the spirit of Huet´s strong confluence, and may therefore be applied without additional termination requirements. It contains the quasi-commutation approach as a special case (for $S = \emptyset$).
Local cooperation is defined thus:

Definition: *(cf. [Bellegarde, Lescanne 86], where $Q = S^{-1}$)*
R *locally* S-*cooperates over* Q, if



□

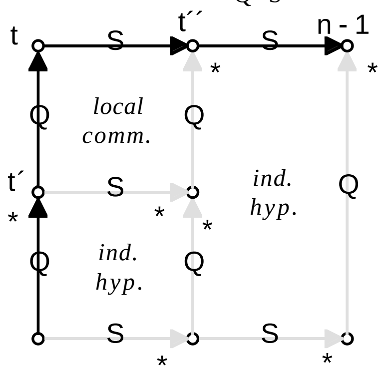
Lemma: *(local cooperation)*
If Q^{-1}/S is Noetherian, S locally commutes over Q, and R locally S-cooperates over Q, then R S-cooperates over Q.

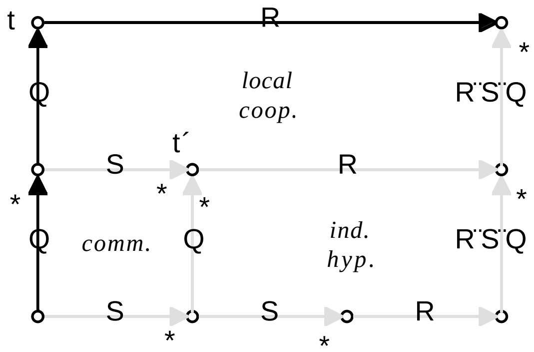
Proof:
We first prove that S commutes over Q, by induction using the ordering » on pairs (t, n), defined by

$$(t, n) \; » \; (t´, n´) \;\; \Leftrightarrow_{def}$$
$$t \; (\underset{Q}{\leftarrow} / \underset{S}{\rightarrow})^{+} \; t´ \;\; \vee$$
$$t \; (\underset{Q}{\leftarrow} \cup \underset{S}{\rightarrow})^{*} \; t´ \;\; \wedge \;\; n >_{\mathbb{N}} n´.$$

Observe that » is indeed Noetherian. Suppose $\underset{Q}{\rightarrow}^{m} \; t \; \underset{S}{\rightarrow}^{n}$. The case where $m = 0$ or $n = 0$ is trivial. The remaining case is shown by the first diagram below. The inductive hypothesis in the small box is justified through $t \underset{Q}{\leftarrow} t´$, the other one through $t \underset{S}{\rightarrow} t´´$, $n >_{\mathbb{N}} n\text{-}1$.

Next we prove that R S-cooperates over Q whenever $\underset{Q}{\rightarrow}^{*}\ t \underset{R}{\rightarrow}$, by induction using $(Q^{-1}/S)^{+}$ on t. This is done by the second diagram below. The inductive hypothesis is justified through $t \underset{Q}{\leftarrow} \underset{S}{\rightarrow}^{*} t'$.





□

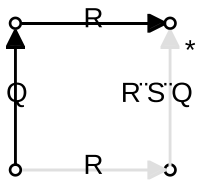
Choosing $Q = S^{-1}$, one gets a technically simpler result:

Corollary: *([Bachmair, Dershowitz 86], lemma 5)*
If S is Noetherian and locally confluent, and R locally S-cooperates over S^{-1}, then R S-cooperates over S^{-1}.

□

Sometimes cooperation can still be proven if Q^{-1}/S is not Noetherian, but like for strong confluence, one needs a more restrictive local diagram.

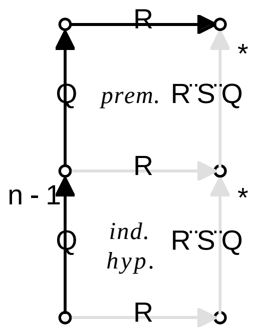
Definition:
R *strongly* S-*cooperates over* Q, if



holds.

Lemma: *(strong cooperation)*
If S commutes over Q and R strongly S-cooperates over Q, then R S-cooperates over Q.

Proof:
By induction on the length n of the Q-derivation. The case n = 0 is trivial. The case n > 0 is treated by the diagram



□

Certainly, commutation of S over Q is, in such a situation, proven by strong commutation. Note, finally, the special case where S = Ø. There strong cooperation becomes quasi-commutation (of R over Q), and the lemma coincides with the "quasi-commutation" lemma again.

3.6. Critical pair criteria

Now we come to the second phase in the development of a criterion. The first phase provided us with a local property, $\underset{S}{\leftarrow}\underset{R}{\rightarrow} \subseteq \underset{T}{\rightarrow}$ say. Even if R is a *finite* rewrite system, its rewrite relation $\underset{R}{\rightarrow}$ is usually still an *infinite* relation, by context and instantiation closure. In other words, the claim is to be shown for infinitely many cases $t \underset{S}{\leftarrow}\underset{R}{\rightarrow} t'$. In order to obtain an effective test for the local property, the pairs (t, t´) are grouped into two sets. The first set contains those (t, t´) where the redices do not overlap, which therefore can be solved by a standard construction. Sometimes suitable syntactic restrictions must be obeyed in order to succeed there. The second set assembles those (t, t´) where the redices in $t \underset{S}{\leftarrow}\underset{R}{\rightarrow} t'$ do overlap — the *critical pairs*. If R and S are finite, then there are only finitely many critical pairs. The check for a local property needs to be done for the critical pairs only. This way it becomes *effective*.
Let us begin with the notion of critical pair:

Definition: *(overlap, critical pair; [Knuth, Bendix 70])*
Let $l \rightarrow r$ and $g \rightarrow d$ be rewrite rules. Without loss of generality, assume that $Var(l \rightarrow r) \cap Var(g \rightarrow d) = Ø$, via appropriate renaming.
1. g *overlaps* l in u, if g is Ø-unifiable with $l/u \notin X$.
2. The pair $(r\sigma, (l[u \leftarrow d])\sigma)$ of terms is called a *critical pair* of $l \rightarrow r$ *above* $g \rightarrow d$, if g overlaps l in u, and σ is the most general (Ø-)unifier of g and l/u, i.e. $g\sigma = (l/u)\sigma$ and for all τ where $g\tau = (l/u)\tau$, then $\tau \geq_{sub} \sigma$.
3. Let R and S denote rewrite systems. The set of all critical pairs of rules from R above or below rules from S is denoted by CP(R, S).

□

Note that according to this definition, l/u may not be a variable. In contrast, g may well be a variable (i.e. $g \to d$ may be a *left-isolating* rule). In the latter situation the critical pair is also called a *variable critical pair*. The quasi-commutation criterion of [Dershowitz 81] erroneously assumed that these critical pairs might be neglected. They used a critical pair lemma for restricted rules, but by rule inversion left-isolating rules came up. [Ganzinger, Giegerich 87] gave a correction. Again it turns out to be more elegant to admit left-isolating rewrite rules anyway.

If R and S are finite, then CP(R, S) is finite as well. (In the literature, usually the set of critical pairs of R *above* S is distinguished, and called SCP(R, S). We have CP(R, S) = SCP(R, S) $\cup$ SCP(S, R)$^{-1}$.)

Critical pair criteria are developed following a well known procedure. Because of its technical nature and its standard form, it is worthwhile to put the essence of critical pair criteria into a *scheme* and to have all special aspects as a parameter to the scheme. The scheme is, so to speak, a proof skeleton, which has to be augmented by a number of syntactic assumptions on the rewrite systems involved. The instantiated scheme together with a few trivial considerations will provide a proof "from the stock".

Known instances of the critical pair scheme are:

(1) the Knuth-Bendix critical pair criterion ([Knuth, Bendix 70]). For finite and Noetherian rewrite systems R, to check whether all critical pairs join is a decision algorithm for confluence.

(2) the strong confluence criterion ([Huet 80]),

(3) the "confluence modulo" approach ([Huet 80]). (The congruence class approach relies on *equational critical pairs*; this requires much more sophistication, and is not treated here.)

(4) construction of forward closures ([Dershowitz 81]) and overlap closures ([Guttag et al. 83]). Finally,

(5) commutation and cooperation properties ([Bellegarde, Lescanne 86]; proper critical pairs are excluded in [Bachmair, Dershowitz 86]). These criteria play a prominent role in the framework of relative termination. We have already arrived at local conditions for cooperation; their critical pair criteria will be the subject of the next section.

Next the general scheme of critical pair criteria is described. We will do the proof informally, although a rigorous formal proof can be done (see for example [Huet 80]). The properties required for $\underset{T}{\to}$ are usually trivially satisfied.

Theorem: *(general critical pair scheme)*

Let R, S, and T denote (not necessarily finite) term rewrite systems. Let

1. $\underset{R}{\rightarrow}\underset{S}{\leftarrow} \subseteq \underset{T}{\rightarrow}$,
2. for all m, n$\in\mathbb{N}$, where

   m > 0, if R is right-nonerasing,

   m ≤ 1, if R is right-linear, and

   n = 0, if R is left-linear,

then $\underset{S}{\rightarrow}^n \underset{R}{\rightarrow} {}^m\underset{S}{\leftarrow} \subseteq \underset{T}{\rightarrow}$ holds,

3. for all m, n$\in\mathbb{N}$, where

   m > 0, if S is right-nonerasing,

   m ≤ 1, if S is right-linear, and

   n = 0, if S is left-linear,

then $\underset{R}{\rightarrow}^n \underset{S}{\rightarrow} {}^m\underset{R}{\leftarrow} \subseteq \underset{T}{\leftarrow}$ holds,

4. CP(R, S) $\subseteq \underset{T}{\rightarrow}$.

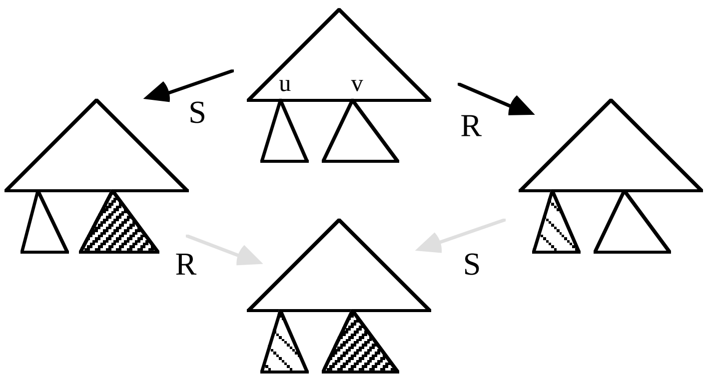
Then $\underset{S}{\leftarrow}\underset{R}{\rightarrow} \subseteq \underset{T}{\rightarrow}$ holds.

Proof: *([Knuth, Bendix 70], [Huet 80])*

Let $t \overset{v}{\underset{S}{\leftarrow}} \overset{u}{\underset{R}{\rightarrow}} t'$ be given. Now $t \underset{T}{\rightarrow} t'$ is to be proven. We perform a case analysis on the positions of u and v relative to each other:

<u>Case 1:</u> u and v are incomparable, i.e. neither $u \leq_{pre} v$ nor $v \leq_{pre} u$ holds.

Then we have the following situation:



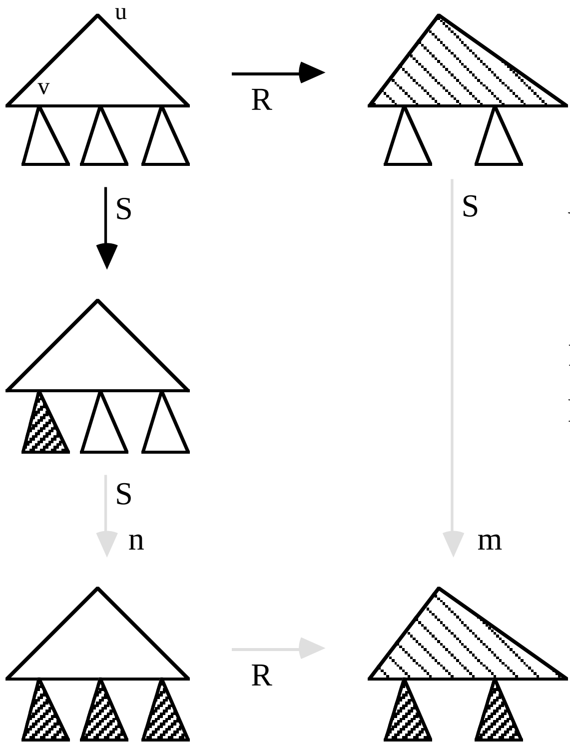
The R-step and the S-step commute. Premise 1 cares that $\underset{R}{\rightarrow}\underset{S}{\leftarrow} \subseteq \underset{T}{\rightarrow}$ holds.

<u>Case 2:</u> $u \leq_{pre} v$.

Without loss of generality, $u = \lambda$, other cases follow immediately by context closure. Let l denote the left hand side of the applied rule from R. Now it has to be distinguished whether there is an overlap with l.

<u>Case 2.1:</u> $v \notin FOcc(l)$, i.e. the rules from R and S do not overlap.

Then the situation is like sketched in the following diagram:

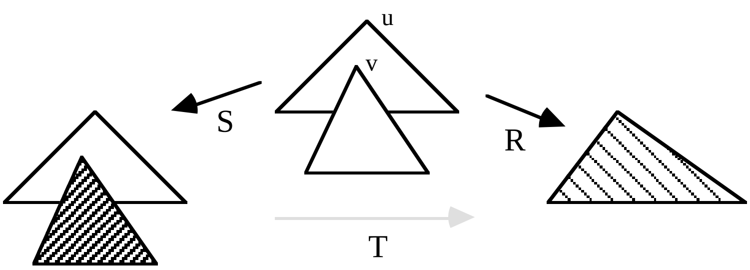


where $m > 0$, if R is right-nonerasing,
$m \leq 1$, if R is right-linear,
$n = 0$, if R is left-linear.

Premise 2 cares that $\underset{S}{\rightarrow}^{n} \underset{R}{\rightarrow} {}^{m}\underset{S}{\leftarrow} \subseteq \underset{T}{\rightarrow}$ holds.

<u>Case 2.2:</u> $v \in FOcc(l)$, i.e. the rules from R and S overlap.

Then, by Huet´s critical pair lemma, the pair (t, t') is an instance of a critical pair from CP(S, R). The well-behaviour of the critical pair is ensured by premise 4, the critical pair criterion $CP(S, R) \subseteq \underset{T}{\rightarrow}$. Closure under instantiation cares that the pair (t, t') works accordingly.



<u>Case 3:</u> $u \geq_{pre} v$.

like in case 2, with the following changes:

(1) u and v are exchanged,

(2) R and S are exchanged,

(3) $\underset{T}{\rightarrow}$ is replaced by $\underset{T}{\leftarrow}$,

(4) "Premise 2" is replaced by "premise 3",

(5) CP(R, S) is replaced by $CP(R, S)^{-1}$.

□

Every time critical pairs are encountered in the literature, the proof is done more or less according to the above scheme. Thanks to the "general critical pair scheme", we can now successfully dodge all technical details, and need not write down any more critical pair proofs. The "critical" pairs where $g \in X$ and $u = \lambda$ can actually be dropped since they are already covered. Trivial critical pairs $(r, r) \in CP(\{l \to r\}, \{l \to r\})$ can often be excluded explicitly, but they impose no problem.

The premises 1, 2, and 3 in the critical pair scheme are responsible for the syntactic restrictions put onto the rewrite systems R and S. For instance, in a local confluence proof, we have the settings R = S and $\underset{T}{\rightarrow} = \underset{R}{\rightarrow}^{*}\,{}^{*}\underset{R}{\leftarrow}$. Here premise 1 means $\underset{R}{\rightarrow}\underset{R}{\leftarrow} \subseteq \underset{R}{\rightarrow}^{*}\,{}^{*}\underset{R}{\leftarrow}$.

For a proof that S strictly locally commutes over R^{-1}, however, for instance premise 2 means $\underset{S}{\rightarrow}^{n}\,\underset{R}{\rightarrow}\,{}^{m}\underset{S}{\leftarrow} \subseteq \underset{R}{\rightarrow}^{*}\,{}^{+}\underset{S}{\leftarrow}$. Its proof does not work in general; it needs $m > 0$, i.e. it works only under the assumption that R is right-nonerasing.

3.7. Criteria for local cooperation

In the previous sections, we developed a notion called cooperation, which allows to strengthen termination of R/S to termination of $R/(S \cup Q)$, and we approached two local conditions for cooperation — local cooperation and strong cooperation. This section presents critical pair criteria for local cooperation, and illustrates them by examples. In particular, the criterion of Bellegarde and Lescanne is generalized, and a new criterion for local cooperation is added.

By the critical pair scheme, which was the subject of the previous section, we obtain a new straightforward criterion for local cooperation of term rewrite systems.

Theorem: *(first local cooperation criterion)*

Let R and S be left-linear rewrite systems and let Q be a right-linear and left-nonerasing term rewrite system. If Q^{-1}/S is Noetherian, and every (Q^{-1}, S)-critical pair locally commutes, and every (Q^{-1}, R)-critical pair locally S-cooperates, then $R/(Q \cup S)$ is Noetherian if and only if R/S is Noetherian.

Proof:

"Only if" is trivial. "If" is assembled by critical pair properties and the previously proven lemmas on cooperation. Since S is left-linear and Q is right-linear, the local commutation of (Q^{-1}, S)-critical pairs implies the local commutation of S over Q. Likewise, R locally S-cooperates over Q, because all (Q^{-1}, R)-critical pairs do, and R is left-linear and Q is right-linear and left-nonerasing. According to the "local cooperation" lemma, R S-cooperates over Q. Together with the termination of R/S, the cooperation lemma yields the wanted result.

□

If in addition S is Noetherian, the result can be strengthened:

Corollary:

Let R and S be left-linear rewrite systems and let Q be a right-linear and left-nonerasing term rewrite system. If $Q^{-1} \cup S$ is Noetherian, and every (Q^{-1}, S)-critical pair locally commutes, and every (Q^{-1}, R)-critical pair locally S-cooperates, then $R/(Q \cup S) \cup S$ is Noetherian if and only if R/S is Noetherian.

□

The following is a typical application of it:

Example: *(cf. Ex. 27 in [Dershowitz 87])*

Let $E =_{def} \{x*(y+1) \to x*(y+1*0)+x,$

$x+0 \to x, \quad x*1 \to x, \quad x*0 \to 0\}$.

E is Noetherian, but no simplification ordering can prove it, since the first rule contains an embedding 1 into 1*0. A proof could be given by means of the semantic path ordering ([Kamin, Lévy 80], [Dershowitz 87]), setting precedence * > +, and using the natural interpretation for summands.

A proof can also be given alike the transformation ordering method (which will be explained below): We intend to provide rewrite systems R, S and Q such that both $R \cup Q^{-1} \cup S$ is Noetherian and $E \subseteq (\underset{R}{\to}/\underset{S \cup Q}{\longrightarrow} \cup \underset{S}{\to})^+$ holds. A first attempt with

$R =_{def} \{x*(y+1) \to x*y+x, \quad x*1 \to x\},$

$S =_{def} \{x+0 \to x, \quad x*0 \to 0\},$ and

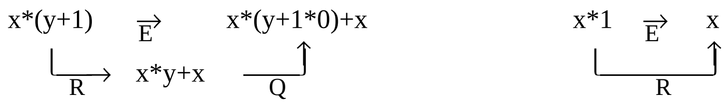
$Q =_{def} S^{-1} = \{x \to x+0, \quad 0 \to x*0\}$

fails, "just" because the second rule in Q is *left-erasing* — x disappears at the left hand side of the second rule. Hence for example the (non-critical pair) branching diagram

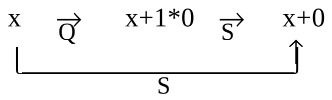
$$0 \underset{Q}{\to} (x*(y+1))*0 \underset{R}{\to} (x*y+x)*0$$

does not join appropriately. So it is advisable to design $Q \neq S^{-1}$. We are now going to demonstrate that the corollary to the "first cooperation criterion" works. Let us choose

$R =_{def} \{x*(y+1) \rightarrow x*y+x, \quad x*1 \rightarrow x\}$,
$S =_{def} \{x*0 \rightarrow 0\}$, and
$Q =_{def} \{x \rightarrow x+1*0, \quad x \rightarrow x+0\}$,
with the intention that $E \subseteq (\underset{R}{\rightarrow}/\underset{S\cup Q}{\longrightarrow} \cup \underset{S}{\rightarrow})^+$ holds:



The remaining two rules from E are already in S. Both R and S are left-linear, and Q is right-linear and left-nonerasing. $R \cup Q^{-1} \cup S$ is Noetherian, proven for example by some lexicographic path ordering. The (Q^{-1}, S)-critical pairs locally commute:



The (Q^{-1}, R)-critical pairs locally S-cooperate since there are no such critical pairs. So the corollary to the "first local cooperation criterion" applies yielding $R/(S \cup Q) \cup S$ Noetherian. In particular, E is Noetherian.

□

The restriction "R and S left-linear" in the critical pair conditions to local cooperation is rather uncomfortable. Exchanging one restriction for another one, it may be disposed of when $Q \subseteq \overset{*}{\underset{S}{\leftarrow}}$. Then, R/S and Q^{-1}/S are Noetherian if and only if $(R \cup Q^{-1})/S$ is, by the "inheritance of relative termination" corollary, part 1, of section 3.1. Thus we arrive at another criterion:

Theorem: *(second local cooperation criterion)*
Let R and S be arbitrary rewrite systems, and $Q \subseteq \overset{*}{\underset{S}{\leftarrow}}$ a right-linear and left-nonerasing rewrite system. If $(R \cup Q^{-1})/S$ is Noetherian, and every (Q^{-1}, S)-critical pair locally commutes, and every (Q^{-1}, R)-critical pair locally S-cooperates, then even $R/(S \cup Q) \cup Q^{-1}/S$ is Noetherian.

□

Again, it can be shown frequently that S is Noetherian. This allows one to tighten the result:

Corollary: *(for $Q = S^{-1}$, see [Bellegarde, Lescanne 87])*
Let R and S be any term rewrite system, and $Q \subseteq \overset{*}{\underset{S}{\leftarrow}}$ a right-linear and left-nonerasing term rewrite system. If $R \cup S$ is Noetherian, and every (Q^{-1}, S)-critical pair locally commutes, and every (Q^{-1}, R)-critical pair locally S-cooperates, then even $R/(S \cup Q) \cup S$ is Noetherian.

Proof:

$R \cup S$ is Noetherian, which by $Q \subseteq {}^{*}\!\underset{S}{\leftarrow}$ is equivalent to $R \cup S \cup Q^{-1}$ Noetherian, which by the "inheritance" lemma implies $(R \cup Q^{-1})/S$ Noetherian and S Noetherian. The "second local cooperation criterion" then supplies that $R/(S \cup Q) \cup Q^{-1}/S$ is Noetherian. From $R/(S \cup Q)$ and S Noetherian we may infer that $R/(S \cup Q) \cup S$ is Noetherian, by "inheritance of relative termination", number 3.

□

This corollary is the basis of a method to prove termination of a term rewrite system P, by showing that $P \subseteq (\underset{R}{\rightarrow}/\underset{S \cup Q}{\longrightarrow} \cup \underset{S}{\rightarrow})^{+}$ holds, and by proving that the corollary applies. The method has (for $Q = S^{-1}$) been investigated by Bellegarde and Lescanne, who called it *transformation ordering*, and it has been implemented at CRIN by Bruno Galabertier. The implemented procedure works in a way similar to the Knuth-Bendix completion procedure: Given the rewrite systems P and S, the system R is constructed computing critical pairs step by step. There is a rich set of examples of transformation orderings in [Bellegarde, Lescanne 86] and [Bellegarde, Lescanne 87], among them a couple of termination proofs even for self-embedding term rewrite systems. Let us just recall their favourite example.

Example: *(Associativity and Endomorphism, continued)*

Let $A =_{def} \{(x+y)+z \rightarrow x+(y+z)\}$,

$E =_{def} \{f(x)+f(y) \rightarrow f(x+y)\}$, and

$E' =_{def} \{f(x)+(f(y)+z) \rightarrow f(x+y)+z\}$.

The rewrite rule E specifies that f is an endomorphism for +. $A \cup E \cup E'$ cannot be proven Noetherian by $>_{rpo}$. It can be proven Noetherian, using a suitable transformation system ([Bellegarde, Lescanne 86]):

$$S =_{def} \{f(x)+y \rightarrow f(x+y),\ \ x+f(y) \rightarrow f(x+y),\ \ (x+y)+z \rightarrow x+(y+z)\}.$$

Informally speaking, S is a transformer who cares that f is moved outside, and parentheses are moved to the right. Choosing $Q =_{def} S^{-1}$, we get Q right-linear and left-nonerasing as required. It is certainly a matter of intuition to find good Q and S. Next it is easy to prove that S terminates, so we may hope to apply the corollary to the "second local cooperation criterion".

S is locally confluent. Now we have to design R, in a way that

$$A \cup E \cup E' \subseteq (\underset{R}{\rightarrow}/\underset{S \cup Q}{\longrightarrow} \cup \underset{S}{\rightarrow})^{+}$$

holds. A is already covered by $A \subseteq S$. Since S is Noetherian and confluent, S-normal forms exist and are unique. We may so choose the unique S-normal forms of E-rules and E´-rules for R-candidates.

$$\begin{array}{ccc} f(x)+f(y) & \xrightarrow[E]{} & f(x+y) \\ \downarrow S & & \uparrow R \\ f(x+f(y)) & \xrightarrow[S]{} & f(f(x+y)) \end{array}$$

$$\begin{array}{ccc} f(x)+(f(y)+z) & \xrightarrow[E']{} & f(x+y)+z \\ \downarrow S & & \downarrow S \\ f(x)+f(y+z) & & (f(x)+y)+z \\ \downarrow S & & \downarrow S \\ f(f(x)+(y+z)) & & f(x)+(y+z) \\ \downarrow S & & \downarrow S \\ f(f(x+(y+z))) & \xrightarrow[R]{} & f(x+(y+z)) \end{array}$$

We see that R should be extended by a rule $f(f(x+y)) \to f(x+y)$, in order to solve the two diagrams. (Also possible: $f(f(x)) \to f(x)$.) $>_{rpo}$ proves $R \cup S$ Noetherian. Now it remains to be shown that (S, R)-critical pairs locally S-cooperate:

$$\begin{array}{ccccc} f(f(x))+y & & \xrightarrow[R]{} & & f(x)+y \\ \downarrow S & & & & \downarrow S \\ f(f(x)+y) & & & & f(x+y) \\ & \xrightarrow[S]{} & f(f(x+y)) & \xrightarrow[R]{} & \uparrow \end{array}$$

□

Another example of a self-embedding rewrite system, which I communicated to Pierre Lescanne, has recently been solved by Lescanne, Bellegarde, and Galabertier (private communication) with support of their tool:

Example: *(conversion into binary numbers)*
Assume we want to specify a conversion of $\mathbb{N}$ into the set of binary numbers. Binary numbers are sequences of bits. The rewrite system uses two constants "O" and "I" (the bits zero and one), the unary function symbols "half" (integer division by two) and "lastBit" (to yield "O" for even numbers, and "I" for odd numbers), the constant "empty" (the empty bitstring), and finally the binary function symbol "&" (append a bit at the right to a bitstring; in infix notation). Note the difference between the natural number 0 and the bit O. The rewrite system looks as follows:

$C =_{def}$ {half(0) → 0,
half(s(0)) → 0,
half(s(s(x))) → s(half(x)),
lastBit(0) → O,
lastBit(s(0)) → I,
lastBit(s(s(x))) → lastBit(x),
conv(0) → empty & O,
conv(s(x)) → conv(half(s(x))) & lastBit(s(x)) }.

The rewrite system C is Noetherian, as we will demonstrate. All rewrite rules, but the last one, can be easily shown Noetherian by $>_{rpo}$ provided with a suitable precedence $>$. Let us fix a particular choice which will be useful in the following, too:

s > half, s > conv > &, conv > lastBit > O,
lastBit > I, 0 > O, 0 > empty, 0 > &.

The last rewrite rule causes a problem for all simplification orderings, because it contains an embedding s(x) into half(s(x)). Now the essential idea is to invent a unary auxiliary function symbol q with precedence conv > q > &, and to have a transformer system

$S =_{def}$ {conv(0) $\rightarrow$ empty & O,
conv(half(x)) $\rightarrow$ q(x)}.

The rest is routine. (Actually Galabertier´s system computes the following proof.) $S \subseteq >_{rpo}$, and therefore S is Noetherian. S is confluent since it has no nontrivial critical pairs. Also, S is left-linear and right-nonerasing. Next we have to choose R such that $C \subseteq (\underset{R}{\Rightarrow}/{=_S} \cup \underset{S}{\Rightarrow})^+$. The rules for "half" and "lastBit" are already in S-normal form, therefore it is advisable to put them into R. Now consider the last two rules from C:

conv(0) $\underset{C}{\Rightarrow}$ empty & O, with conv(0) $\underset{S}{\rightarrow}$ empty & O

conv(s(x)) $\underset{C}{\Rightarrow}$ conv(half(s(x))) & lastBit(s(x))
↓R ↓S
q(s(x)) & lastBit(s(x))

We find that R needs the rule conv(s(x)) $\rightarrow$ q(s(x)) & lastBit(s(x)) to handle the diagram to the right. Finally, R has to be extended in a way that R locally S-cooperates over S^{-1}. The (R, S)-critical pairs are

conv(half(0)) $\underset{R}{\Rightarrow}$ conv(0)
↓S ↓S
q(0) $\underset{R}{\Rightarrow}$ empty & O

conv(half(s(0))) $\underset{R}{\Rightarrow}$ conv(0)
↓S ↓S
q(s(0)) $\underset{R}{\Rightarrow}$ empty & O

conv(half(0)) $\underset{R}{\Rightarrow}$ conv(s(half(x)))
$\underset{S}{\rightarrow}$ q(s(s(x))) $\underset{R}{\rightarrow}$ conv(s(half(x)))

New R-rules are:

q(0) $\rightarrow$ empty & O,
q(s(0)) $\rightarrow$ empty & O, and
q(s(s(x))) $\rightarrow$ conv(s(half(x))).

They cause no more critical pairs, so we are finished. Luckily, $R \subseteq >_{rpo}$ still holds now, so R∪S is Noetherian. The corollary to the "second local cooperation criterion" applies — C is proven Noetherian.

□

Finally, here is an example where $Q \subseteq S^{-1}$ but $Q \neq S^{-1}$ holds.

Example: *(Ex. 27 in [Dershowitz 87], continued)*

Let $E =_{def} \{x*(y+1) \to x*(y+1*0)+x,$
$x*1 \to x, \quad x+0 \to x, \quad x*0 \to 0\}.$

E is Noetherian, but self-embedding. Cooperation failed when $Q = S^{-1}$. The "first local cooperation criterion" was successful. Now let us apply the "second local cooperation criterion". Choose

$R =_{def} \{x*(y+1) \to x*y+x, \quad x*1 \to x\},$

$S =_{def} \{x+0 \to x, \quad x*0 \to 0\},$ and

$Q =_{def} \{x \to x+1*0\},$

with the intention that $E \subseteq (\xrightarrow[R]{} / \xrightarrow[S \cup Q]{} \cup \xrightarrow[S]{})^+$ holds. R can actually be constructed like in the examples above. (Likewise, one might choose $Q =_{def} \{x*y \to x*(y+1*0)\}$, or $Q =_{def} \{0 \to 1*0\}$.)

Both R and S are left-linear, and Q is right-linear and left-nonerasing. We are now going to prove that $R/(Q \cup S) \cup S$ is indeed Noetherian. The requirement $Q \subseteq \overset{*}{\xleftarrow[S]{}}$ is satisfied because

$$x \xleftarrow[S]{} x+0 \xleftarrow[S]{} x+1*0$$

holds. (Note that the inclusion is strict here.) The (Q^{-1}, S)-critical pairs locally commute:

$$x \xrightarrow[Q]{} x+1*0 \xrightarrow[S]{} x+0, \qquad x \xrightarrow[S]{} x+0$$

Since there are no (Q^{-1}, R)-critical pairs, the local properties are satisfied. There is no problem proving $R \cup S$ Noetherian by a suitable simplification ordering. We may apply the corollary, and we get the stronger $R/(S \cup Q) \cup S$ Noetherian. So E terminates, which was the claim.

□

3.8. Criteria for strong cooperation, and their applications

So far about the *local cooperation* criteria. In contrast, strong cooperation does not need the termination of Q^{-1}/S. This section finishes the cooperation approach; a critical pair criterion for strong cooperation is given. We have as interesting special cases, a new criterion for termination modulo from relative termination ($Q^{-1} = S$), and the quasi-commutation criterion ($S = \emptyset$). It turns out that quasi-commutation is hardly suited for termination proofs.

Critical pair criteria for the "strong cooperation" lemma raise the following theorem. Unlike the "second local cooperation criterion", it cannot dispense with the syntactic condition "R left-linear".

Theorem: *(strong cooperation criterion)*
Let R and S be left-linear rewrite systems, and Q be a right-linear and left-nonerasing term rewrite system. Suppose that S commutes over Q, and that every (Q^{-1}, R)-critical pair strongly S-cooperates. Then R/(S∪Q) is Noetherian if and only if, R/S is Noetherian.

Example: *(Nonfin, continued)*
Let f, c, s denote unary function symbols, x a variable, and let

$S =_{def} \{fcx \to cx\}$,

$Q =_{def} \{cx \to fcx\}$, and

$R =_{def} \{csx \to cx\}$.

Remember that parentheses may be dropped in the case of constant and unary function symbols exclusively. R∪S terminates. To prove that $R/\overline{S}$ is Noetherian, also a strong cooperation argument works. S commutes over Q, i.e. S is confluent. The rewrite systems R, S, and Q are linear and nonerasing, and there is just one (Q^{-1}, R)-critical pair to consider:

$$\begin{array}{ccccc} csn & \xrightarrow[Q]{} & fcsn & \xrightarrow[R]{} & fcn \\ \llcorner & \xrightarrow[R]{} & cn & \xrightarrow[Q]{} & \uparrow \end{array}$$

Therefore R strongly S-cooperates over Q, and, since R/S is Noetherian, R/(S∪Q) = $R/\overline{S}$ is Noetherian.

□

Consider the setting $Q = S^{-1}$, and assume that there are no (R, S)-critical pairs and R and S are left-linear. In this frequent case, thanks to the "strong cooperation criterion", we do not need the termination of S so as to prove termination of $R/\overline{S}$:

Corollary:
Let R be a left-linear, S be a confluent, left-linear, and right-nonerasing term rewrite system, and suppose there are no (R, S)-critical pairs. Then $R/\overline{S}$ is Noetherian if and only if, R/S is Noetherian.

□

Example: *(cf. Ex. in [Bockmayr 88])*
Let the addition on $\mathbb{N}$ be specified by

$S =_{def} \{0+x \to x,\quad s(x)+y \to s(x+y)\}$,

and square numbers by

$R =_{def} \{sq(0) \to 0,\quad sq(s(x)) \to s(x+(x+sq(x)))\}$.

The last rule is suggested by the binomial equation $(x+1)^2 = 1 + 2x + x^2$. R/S (even R∪S) terminates, shown for instance by $\geq_{rpo}$ with precedence sq > + > s. Both R and S are confluent, because they are left-linear, and there are no (R, R)- nor (S, S)-critical pairs. As there are no (R, S)-critical pairs, R is left-linear, and S is right-nonerasing, we may employ the above corollary to the "strong cooperation criterion" so as to infer $R/\overline{S}$ Noetherian. Note that termination of S has indeed not been used in this reasoning. An alternative termination proof of $R/\overline{S}$ may be obtained using the polynomial interpretation

$$[s(x)] = x+1, \ [x+y] = x+y, \ [sq(x)] = 2x^2+3.$$

□

As mentioned earlier, strong cooperation becomes quasi-commutation in the case S = Ø. Likewise, critical pair criteria for strong cooperation become criteria for quasi-commutation. Dershowitz´ quasi-commutation is so another special case (where $CP(Q^{-1}, R) = \emptyset$) of the "strong cooperation criterion":

Corollary: *(quasi-commutation criterion; without critical pairs, see [Dershowitz 81])*
Let R be a left-linear, Q a right-linear and left-nonerasing rewrite system, such that all (Q^{-1}, R)-critical pairs quasi-commute. Then R/Q is Noetherian if and only if R is Noetherian.

Example:

1. *(Integer numbers; cf. INT2 in [Padawitz 88])*
Let $Q =_{def} \{-0 \rightarrow 0, \ --x \rightarrow x, \ s(-s(x)) \rightarrow -x\}$
be a piece of a specification of ℤ, the integer numbers, and let

$$R =_{def} \{x+0 \rightarrow x, \ x+s(y) \rightarrow s(x+y), \ x+(-y) \rightarrow -(-x+y)\}$$

specify integer addition. R quasi-commutes over Q, since R is left-linear, Q is right-linear and left-nonerasing, and the (Q^{-1}, R)-critical pairs strictly locally commute:

$x+(-0) \overleftarrow{\rightarrow}_Q x+0 \overleftarrow{\rightarrow}_R x$
$\downarrow_R$ $\uparrow_Q$
$-(-x+0) \xrightarrow[R]{} --x$

$x+(--0) \overleftarrow{\rightarrow}_Q x+0 \overleftarrow{\rightarrow}_R x$
$\downarrow_R$ $\uparrow_Q$
$-(-x+(-0))$ $--x$
$\downarrow_R$ $\uparrow_Q$
$--(--x+0) \xrightarrow[R]{} ----x$

$x+(--s(y)) \overleftarrow{\rightarrow}_Q x+s(y) \overleftarrow{\rightarrow}_R s(x+y)$
$\downarrow_R$ $\uparrow_Q$
$-(-x+(-s(y))$ $--s(x+y)$
$\downarrow_R$ $\uparrow_Q$
$--(--x+s(y)) \xrightarrow[R]{} --s(--x+y)$

$x+(---y) \overleftarrow{\rightarrow}_Q x+(-y) \overleftarrow{\rightarrow}_R -(-x+y)$
$\xrightarrow[R]{} -(-x+(--y)) \xrightarrow[Q]{} \uparrow$

$x+s(-s(y)) \overleftarrow{\rightarrow}_Q x+(-y) \overleftarrow{\rightarrow}_R -(-x+y)$
$\downarrow_R$ $\uparrow_Q$
$s(x+(-s(y))) \overleftarrow{\rightarrow}_R s(-x+s(y)) \overleftarrow{\rightarrow}_R s(-s(-x+y))$

R is Noetherian, as has been demonstrated in the previous chapter. By the fact that R quasi-commutes over Q, R/Q is Noetherian. Q is Noetherian by the polynomial interpretation

$[-x] = x+1 = [s(x)]$.

Together with R/Q Noetherian, we have R∪Q Noetherian.

2. *(FF, continued)*

Let R $=_{def}$ {ffx → fgfx}, Q $=_{def}$ {a → ga}. R is Noetherian. There are no overlaps betwen ffx and ga. So there are no (Q^{-1}, R)-critical pairs. R is left-linear, and Q is right-linear and left-nonerasing. Therefore R/Q is Noetherian. All termination criteria based on direct sums (for instance the one in [Toyama et al. 89]) fail simply because g is a common function symbol in R and Q.

□

Next, we show a small example from the algebraic specification domain.

Example: *(Maps)*

Assume primitive specifications BOOL (for truth values), DATA (some data domain together with a conditional "if"), and INDEX (a set of tokens provided with a total equality function "eq"). The new functions "empty" (constant), "put" (binary), and "get" (unary) are specified by the rewrite system

MAP $=_{def}$ { get(put(m, i, d), j) → if(eq(i, j), d, get(m, j)) }.

Informally, expressions built with "empty" and "put" represent tables or finite mappings from indices to data; "put" is an update operator, and "get" a retrieval operator on maps. Since MAP is left-linear and Noetherian, the following statement may be made: Provided that BOOL ∪ DATA ∪ INDEX is right-linear, MAP / (BOOL ∪ DATA ∪ INDEX) is Noetherian, because there are no overlaps between left hand sides from MAP and right hand sides of the primitive specifications.

□

The quasi-commutation technique suffers from hard syntactic restrictions. Critical pairs may cause additional problems.

Example: *(Stack of $\mathbb{N}$)*

Let Peano arithmetic be specified by a rewrite system NAT as usual:

NAT $=_{def}$ ADD ∪ MULT,

ADD $=_{def}$ {0+y → y, s(x)+y → s(x+y)},

MULT $=_{def}$ {0*y → 0, s(x)*y → (x*y)+y}.

NAT is Noetherian, a fact which we can prove for example by the lexicographic path ordering using precedence * > + > s. In order to specify stacks, we use further function symbols "empty" (constant), "first", "rest", "length" (unary), and "app" (binary). Stacks are constructed hierarchically on the natural numbers. Let x and w denote variables. Consider the rewrite system

$$\text{STACK} =_{\text{def}} \{\text{first}(\text{app}(x, w)) \rightarrow x, \ \text{rest}(\text{app}(x, w)) \rightarrow w,$$
$$\text{length}(\text{empty}) \rightarrow 0, \ \text{length}(\text{app}(x, w)) \rightarrow s(\text{length}(w))\}$$

STACK is obviously Noetherian (proven by $\geq_{rpo}$ using precedence length > s, length > 0). Is STACK $\cup$ NAT Noetherian as well?

Let us first try to prove that STACK quasi-commutes over NAT. Except for critical pairs like

$$\text{first}(0+\text{app}(x, w)) \xrightarrow[\text{NAT}]{} \text{first}(\text{app}(x, w)) \xrightarrow[\text{STACK}]{} x,$$

which may be ruled out for reasons of well-sortedness, there are no overlappings between left hand sides of STACK and right hand sides of NAT, although there are common function symbols 0, s in STACK and NAT ([Ganzinger, Giegerich 87]). By the quasi-commutation criterion, we may infer that STACK quasi-commutes over ADD, and therefore that STACK $\cup$ ADD is Noetherian. But the same reasoning does not apply to STACK and MULT, as the first multiplication rule is left-erasing in y, and the second rule is not right-linear in y.

Now, in a second attempt, let us try to prove that NAT quasi-commutes over STACK. NAT is left-linear, and STACK is right-linear, but left-erasing. Moreover, there are the following (STACK^{-1}, NAT)-critical pairs:

$$\text{first}(\text{app}(0, w))+y \xrightarrow[\text{STACK}]{} 0+y \xrightarrow[\text{NAT}]{} y$$

$$\text{first}(\text{app}(s(x), w))+y \xrightarrow[\text{STACK}]{} s(x)+y \xrightarrow[\text{NAT}]{} s(x+y)$$

$$\text{first}(\text{app}(0, w))*y \xrightarrow[\text{STACK}]{} 0*y \xrightarrow[\text{NAT}]{} 0$$

$$\text{first}(\text{app}(s(x), w))*y \xrightarrow[\text{STACK}]{} s(x)*y \xrightarrow[\text{NAT}]{} (x*y)+y$$

$$\text{rest}(\text{app}(w, 0))+y \xrightarrow[\text{STACK}]{} 0+y \xrightarrow[\text{NAT}]{} y$$

$$\text{rest}(\text{app}(w, s(x)))+y \xrightarrow[\text{STACK}]{} s(x)+y \xrightarrow[\text{NAT}]{} s(x+y)$$

$$\text{rest}(\text{app}(w, 0))*y \xrightarrow[\text{STACK}]{} 0*y \xrightarrow[\text{NAT}]{} 0$$

$$\text{rest}(\text{app}(w, s(x)))*y \xrightarrow[\text{STACK}]{} s(x)*y \xrightarrow[\text{NAT}]{} (x*y)+y$$

$$\text{length}(\text{empty})+y \xrightarrow[\text{STACK}]{} 0+y \xrightarrow[\text{NAT}]{} y$$

$$\text{length}(\text{app}(x, w))+y \xrightarrow[\text{STACK}]{} s(\text{length}(w))+y \xrightarrow[\text{NAT}]{} s(\text{length}(w)+y)$$

$$\text{length}(\text{empty})*y \xrightarrow[\text{STACK}]{} 0*y \xrightarrow[\text{NAT}]{} 0$$

$$\text{length(app(x, w))*y} \xrightarrow[\text{STACK}]{} \text{s(length(w))*y} \xrightarrow[\text{NAT}]{} \text{(length(w)*y)+y}$$

Again the critical pairs that contain "rest" symbols might be ruled out, using well-sortedness information. None of the mentioned critical pairs quasi-commutes. Adopting a Knuth-Bendix-like technique, one may add these critical pairs to NAT, and may even succeed to prove that NAT remains Noetherian. But then further critical pairs emerge. Summarizing, the use of quasi-commutation heavily depends on which rewrite relation quasi-commutes over which one. (Indeed STACK ∪ NAT is Noetherian, which can simply be proven by a standard termination ordering at once.)

□

Although quasi-commutation is far from being a powerful criterion, its obvious advantage is an easy check by syntactic criteria. For syntactically restricted rewrite systems, it is an interesting termination proof method.

4. Confluence criteria

Confluence, also called the Church-Rosser property, is probably the most important, and the most typical notion of term rewriting. Informally speaking, the order of the rewrite steps is irrelevant for a confluent relation. It is known that confluence of rewriting is undecidable ([Huet 80]), even for the class of systems where the function symbols have arity 0 or 1 ([Book et al. 81]). Confluence is decidable for the class of ground rewrite systems ([Dauchet et al. 87], [Oyamaguchi 87]). According to [Knuth, Bendix 70], confluence is also decidable for the class of Noetherian systems: A Noetherian rewrite system R is confluent if and only if for each (R, R)-critical pair (t, t´), the normal forms of t and t´ are (syntactically) equal. Knuth and Bendix designed a procedure that attempts (and sometimes succeeds) to convert a system of equations into a confluent and Noetherian term rewrite system. For non-Noetherian rewrite systems, confluence can be attacked by strong confluence criteria ([Rosen 73], [Huet 80]). The strong confluence approach originates from the confluence proof of lambda calculus; it disposes completely with the termination property, but compensates it with a considerably harder local condition.

It has been a major goal since the beginnings of confluence theorems to *decompose* the confluence proof of a reduction $R \cup S$ into those of R and S, or at least, to profit from the confluence of S, say. This goal has brought up a variety of sufficient conditions, see [Klop 87] for examples. The surprisingly powerful criterion "if rewrite systems R and S have no function symbols in common, then R and S confluent implies $R \cup S$ confluent" is given in [Toyama 87b]. If R and S have no common function symbols, then $R \cup S$ is also called the direct sum of R and S. We allow that R and S have common function symbols, but impose the restriction that R/S is Noetherian instead.

Confluence criteria for composed systems $R \cup S$, where R/S is Noetherian, may be developed along the proof methods of "confluence modulo". Since confluence of $R \cup E$ (E symmetric) is the same as the E-Church-Rosser property of R, Jouannaud´s approach for "confluence modulo" can be compared to the confluence approach here.

The objective of this chapter is

(1) to show how to localize $R \cup S$-confluence diagrams step by step,

(2) to point out the limits of localization,

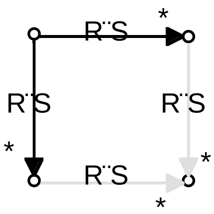
(3) and finally to come down to critical pair criteria.

A confluence proof for S may be delayed, or strong confluence may be used for it. Klop´s confluence criterion ([Klop 87]) is of the latter kind. Such a criterion may be seen as a common generalization of the Newman criterion and strong confluence criterion.

4.1. The role of coherence

Let R and S denote relations, and let R/S be Noetherian. How can we prove confluence of $R \cup S$? As we will see, in a way very similar to confluence modulo. There for symmetric E, essentially confluence of $R \cup E$ is sought. Noetherian relations are proven confluent by the Newman lemma. In this spirit, we start to localize the ${}^{*}\xleftarrow[R\cup S]{} \xrightarrow[R\cup S]{}{}^{*}$ -diagrams. Localization gets stuck in a diagram that has a counterpart in the "confluence modulo" approach. The key notion that helps to continue localizing then, has been called *coherence*. Coherence means, roughly speaking, that R-steps may always be put before E-steps. We will set up a suitable notion of coherence for R and S where S is an arbitrary rewrite system, rather than symmetry closed.

In order to simplify talking about confluence diagrams, let us agree to say that a relation Q *joins*, if $Q \subseteq (R\cup S)^* \, ((R\cup S)^{-1})^*$ holds. Confluence of $R \cup S$ in this respect means that $((R\cup S)^{-1})^* \, (R\cup S)^*$ joins:



In the case where S is some symmetric relation E, the property of E-confluence in [Jouannaud 83] precisely means joinability. The property which corresponds to the Church-Rosser property in the case of equational rewriting, the E-Church-Rosser property, precisely means confluence of $R \cup S$. The liberal notion of rewrite system makes this possible.

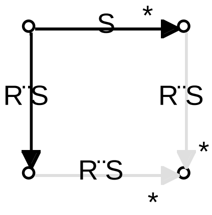
For the inductive proofs of this chapter, we will use the Noetherian ordering » on pairs (t, n), defined by

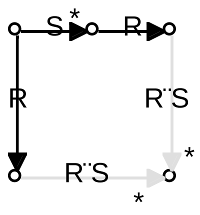
$$(t, n) \gg (t', n') \;\Leftrightarrow_{def}$$
$$t \, (\xrightarrow[R]{} / \xrightarrow[S]{})^{+} \, t' \;\vee$$
$$t \xrightarrow[R\cup S]{}^{*} t' \;\wedge\; n >_{\mathbb{N}} n'.$$

In the naive attempt to localize as much as possible from the confluence diagram for $R \cup S$, one arrives at the following lemma. It characterizes confluence in the case of relative termination:

Lemma: *(first localization)*

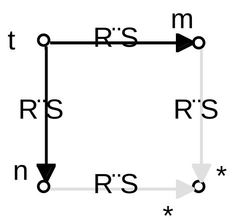
Let R/S be Noetherian. Then R∪S is confluent if and only if the following diagrams hold:



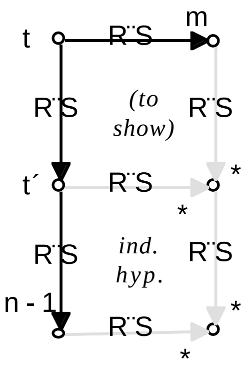


Proof:

In order to show that

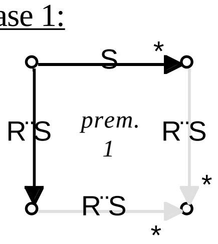


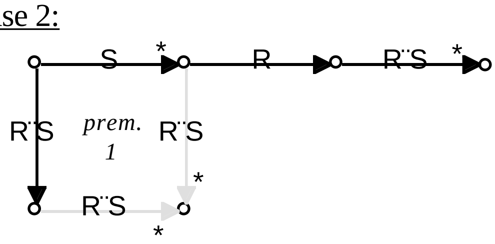
holds for all t, and all m ≥ n, we use induction » on the pair (t, n). The case m = 0 is trivial. Now assume that n ≥ 1. Since we may use the inductive hypothesis in the case $t \xrightarrow[R\cup S]{} t'$, n > n-1, the proof is done if we arrive to show that in the proof attempt



the upper part holds. There are two cases to consider, according to the equality
$(R\cup S)^* = S^* \cup S^* R (R\cup S)^*$.

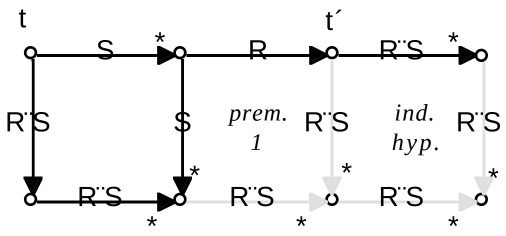
<u>case 1:</u> <u>case 2:</u>





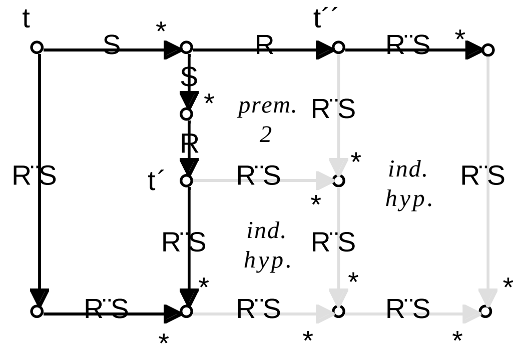
Case 2 needs again a case analysis: Whether the downgoing grey arrow contains an R-step or not. The achieved part of the proof diagram becomes black, because it may now be taken as a premise.

<u>case 2.1:</u> (no R-step)



The inductive hypothesis is justified by $t \xrightarrow[S]{}{}^{*} \xrightarrow[R]{} t'$.

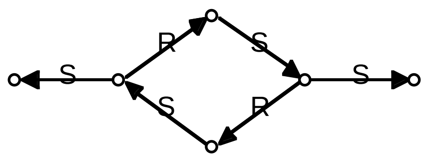
<u>case 2.2:</u> (at least one R-step)

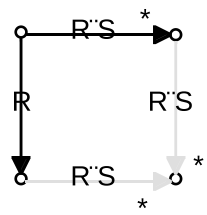


The inductive hypothesis is justified by $t \xrightarrow[S]{}{}^{*} \xrightarrow[S]{}{}^{*} \xrightarrow[R]{} t'$, and by $t \xrightarrow[S]{}{}^{*} \xrightarrow[R]{} t''$.

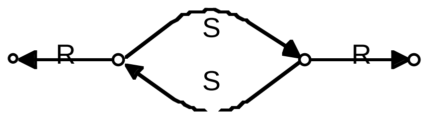
□

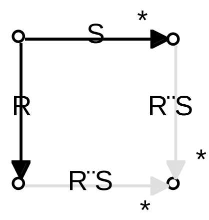
The strength of this lemma is shown by the counterexample (R/S is not Noetherian) at the left hand side below, where R∪S is not confluent, although both R and S are confluent and Noetherian, and the diagram at the right hand side below holds:





Notice that the diagram for $\xleftarrow[R]{} \xrightarrow[S]{}{}^{*} \xrightarrow[R]{}$ fits to the "confluence modulo" diagram for $\xleftarrow[R]{} =_E \xrightarrow[R]{}$ in [Huet 80]. Next we want to get rid of the composed reduction $\xrightarrow[S]{}{}^{*} \xrightarrow[R]{}$ in that diagram. But the conditions for confluence of R∪S can be continued localizing only under further restrictions. This is demonstrated by another counterexample ($\xleftarrow[R]{} \xrightarrow[S]{}{}^{*} \xrightarrow[R]{}$ -diagrams do not join) at the left hand side below, where R∪S is not confluent, although R/S is Noetherian, R and S are confluent, and the following diagram holds:





In order to break $\xleftarrow[R]{} \xrightarrow[S]{}{}^{*} \xrightarrow[R]{}$ -diagrams apart, we have to take care that there is no infinite S-derivation which connects R-redices. The basic idea is to use a Noetherian ordering » that guards such S-derivations. For simplicity reasons, we will not develop this concept in general, but instantiate » by $(R/S)^+$. (It is useless to choose » $=_{def}$ S if S is

Noetherian. In this case, fully local conditions are achieved, applying Newman´s lemma for R∪S.)

For "confluence modulo", Jouannaud ([Jouannaud 83]) coined the notion of coherence, which we widen for the purpose to prove confluence of R∪S where R is relatively Noetherian to S:

Definition:

Assume that R, R´, and S are given, and $R \subseteq R' \subseteq S^*R$ holds. A triple (t_0, t_1, t_2) of terms is called *coherent*, if one of the following cases holds:

(1) $t_1 \xrightarrow[S]{}^{*}\ {}^{*}\!\xleftarrow[R\cup S]{} t_2$ or

(2) $t_1 \xrightarrow[R']{} \xrightarrow[R\cup S]{}^{*}\ {}^{*}\!\xleftarrow[R\cup S]{} t_2$ or

(3) $\exists t_3.\ t_0 \xrightarrow[R/S]{}^{+} t_3 \ \wedge\ t_1 \xrightarrow[S]{}^{*} t_3 \xrightarrow[R\cup S]{}^{*}\ {}^{*}\!\xleftarrow[R\cup S]{} t_2$.

□

Note that if S is cyclic (as in the "confluence modulo" approach), cases 1 and 3 cannot occur since they would immediately cause a cycle in the R/S relation, and thus contradict R/S Noetherian. The remaining case 2 in our case enumeration then coincides with Jouannaud´s notion of coherence. Jouannaud calls R E-coherent, if ${}^{*}\!\xleftarrow[E]{} \xrightarrow[R]{} \xrightarrow[E^*R]{}^{*}$ is coherent. The coherence of ${}^{*}\!\xleftarrow[E]{} \xrightarrow[R]{}$ does already the same job. This motivates the following definition:

Definition:

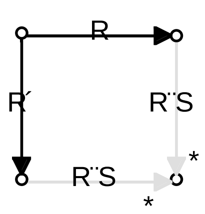
R is called *S-coherent*, if $t_1\ {}^{*}\!\xleftarrow[S]{} t_0 \xrightarrow[R]{} t_2$ implies that t_0, t_1, t_2 are coherent.

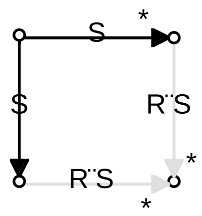
□

Using S-coherence, we can continue to localize confluence of R∪S:

Lemma: *(second localization)*

Let R and S denote binary relations and let R/S be Noetherian. R∪S is confluent if and only if, there is R´ such that $R \subseteq R' \subseteq R/S$ holds, the diagrams



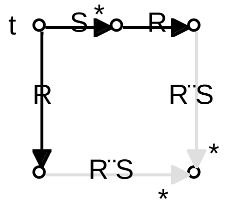


hold, and R is S-coherent.

Proof:

Let us call the two mentioned diagrams premise 1, premise 2, respectively. By induction on the (Noetherian) lexicographic ordering $((R/S)^+, >)$ on $(t, \min(m, n))$, we prove simultaneously

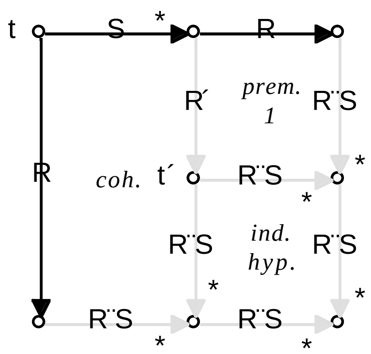
1. that $^m\xleftarrow[R\cup S]{} t \xrightarrow[R\cup S]{}{}^n$ joins, and
2. the diagram



(As here the expression min(m,n) is not defined, we rather use the first transfinite ordinal number ω.) .

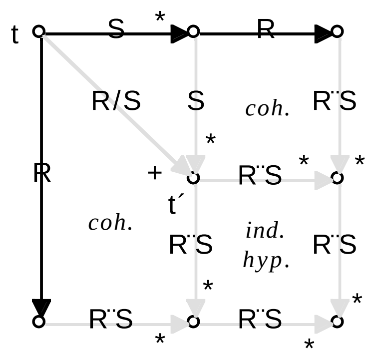
Claim 2 is needed precisely as premise 2 for the "first localization" proof. For the proof of claim 1, we may so take a copy of the proof of the "first localization" lemma, where we replace "premise 2" by "inductive hypothesis 2". This already finishes the proof of claim 1. We have, so to speak, "reused" the proof of the "first localization" lemma.
Claim 2 remains to be proved. A $^*\underset{S}{\leftarrow}\ \underset{R'}{\rightarrow}$ -diagram may join in 3 different ways, where the first case is covered the third one. We employ case analysis along the remaining two alternatives:

<u>case 1:</u>



The inductive hypothesis is justified by $t \underset{S}{\rightarrow}{}^* \underset{R'}{\rightarrow} t'$.

<u>case 2:</u>



Justification: $t \xrightarrow[R/S]{}{}^+ t'$.

□

(Jouannaud uses for his proofs essentially the same Noetherian ordering as we do here.) Following [Jouannaud 83], we introduced an auxiliary relation R´ where $R \subseteq R' \subseteq S^*R$ holds. This has a number of technical advantages:

1. If we instantiate R´ by S^*R, we get a copy of the "first localization" lemma. Thus, we can keep the "if and only if" for the next lemmas.
2. The instantiation R´ = R leads us to a result in the spirit of Huet´s "confluence modulo" approach. At the end of this chapter, we will present two critical pair criteria for this case.
3. In the case where R and S denote rewrite systems, finally, the rewrite relation $\underset{R'}{\rightarrow}$ may be instantiated by a class rewrite relation $\xrightarrow[R\rfloor S]{}$, extending Jouannaud´s "congruence class approach". Here

$$t \xrightarrow[R\rfloor S]{v} t' \text{ holds if } t \xrightarrow[S]{u_1} \dots \xrightarrow[S]{u_n} \xrightarrow[R']{v} t' \text{ for some } u_1 \geq_{pre} v, \dots, u_n \geq_{pre} v .$$

The class approach is however not continued within this thesis. See also the discussion in the conclusion.

4.2. Further localization

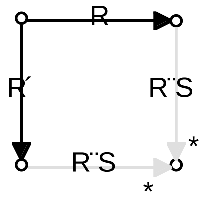
Suppose that S might be a primitive rewrite system, and R might be defined hierarchically on top of S. In such a situation, it is reasonable to assume a priori that $\xleftarrow[S]{} \xrightarrow[S]{}^*$ joins. The only non-local condition for confluence of $R \cup S$ on this account, is the S-coherence diagram. A very natural choice is to adopt the restriction that S is "almost" confluent, not too hard a restriction after all. Then we get a confluence result for local $\xleftarrow[S]{} \xrightarrow[R]{}$ diagrams. The section is concluded with critical pair criteria for this case.

Definition:
R´ is called *locally S-coherent*, if $t_1 \xleftarrow[S]{} t_0 \xrightarrow[R']{} t_2$ implies that t_0, t_1, t_2 are coherent.

□

Local S-coherence is a local version of S-coherence. In the same vein, S^* may be called locally S-coherent if $t_1 \xleftarrow[S]{} t_0 \xrightarrow[S]{}^* t_2$ implies that t_0, t_1, t_2 are coherent. This property contains confluence of S as a special case. Using these new notions, the next localization step takes place:

Lemma: *(third localization)*
Let R/S be Noetherian. Then $R \cup S$ is confluent if and only if, there is some R´ such that $R \subseteq R' \subseteq R/S$, the diagram



holds, and both R´ and S^* are locally S-coherent.

Proof:
"Only if" is easy by $R' =_{def} R/S$. Cases 1 and 2 in the coherence definition cover all $t_1 \xrightarrow[R \cup S]{}^* {}^*\xleftarrow[R \cup S]{} t_2$ in question.

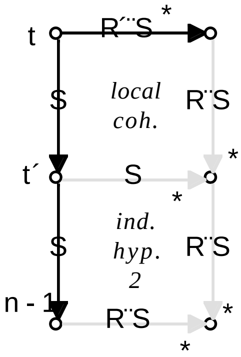
For "if", we perform induction using $((R/S)^+, >)$ upon (t, n) to show simultaneously that for all t, t_1, and t_2,

1. ${}^*\xleftarrow[R \cup S]{} t \xrightarrow[R \cup S]{}^*$ joins (there we set $n = \omega$), and
2. $t_1 \,{}^n\xleftarrow[S]{} t \xrightarrow[R' \cup S^*]{} t_2$ implies that t, t_1, t_2 are coherent.

Claim 2 implies that t, t_1, t_2 are coherent for $t_1 \,{}^*\xleftarrow[S]{} t \xrightarrow[R]{} t_2$, which is needed in order to reuse the proof of the "second localization" lemma for claim 1.

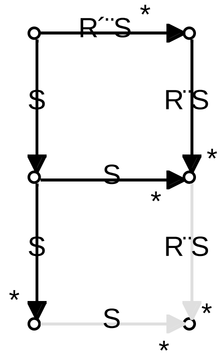
We enter now the proof of the second claim. The proof is by a case analysis along the 3 cases in the last premise. In each case, we need in addition a case analysis depending on which case, the inductive hypothesis yields.

<u>case 1:</u>

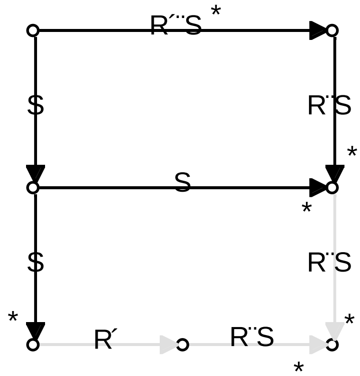


Justification: $t \xrightarrow[S]{} t'$, $n > n-1$.

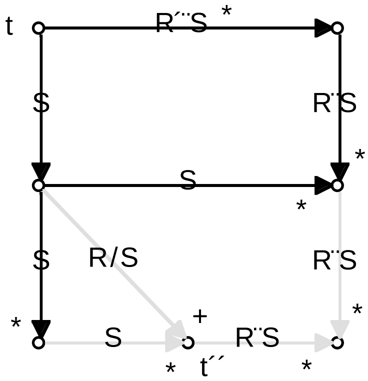
<u>case 1.1:</u>



<u>case 1.2:</u>

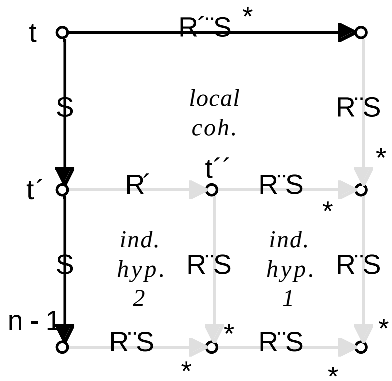


<u>case 1.3:</u>



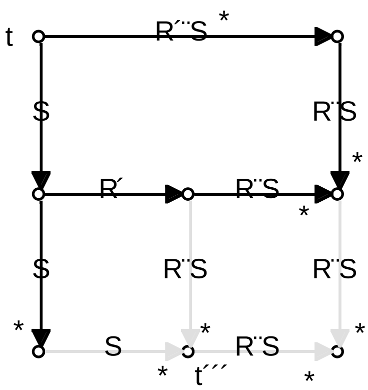
As required, $t \xrightarrow[R/S]{}^{+} t''$ holds, via $t \xrightarrow[S]{} t' \xrightarrow[R/S]{}^{+} t''$.

<u>case 2:</u>



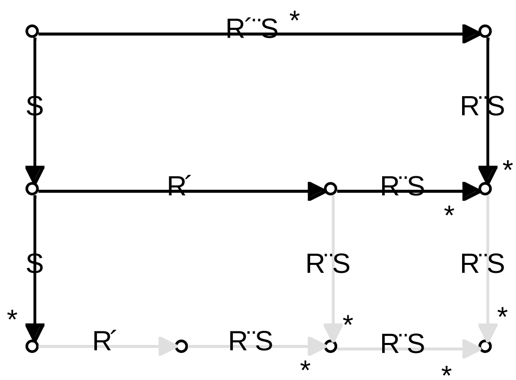
Ind. hyp. 2 justified by $t \xrightarrow[S]{} t'$, $n > n-1$,
ind. hyp. 1 justified by $t \xrightarrow[S]{} t' \xrightarrow[R']{} t''$.

<u>case 2.1:</u>

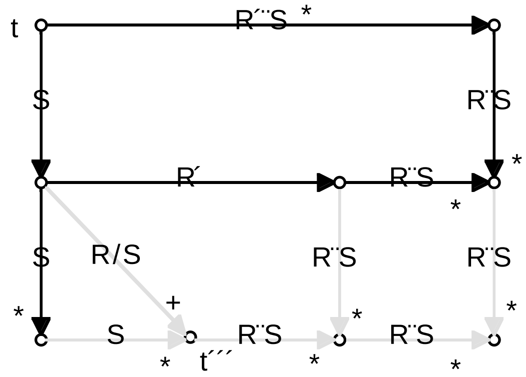


As required, $t \xrightarrow[R/S]{}^{+} t'''$ holds, via $t \xrightarrow[S]{} \xrightarrow[R']{} \xrightarrow[R \cup S]{}^{*} t'''$.

<u>case 2.2:</u>

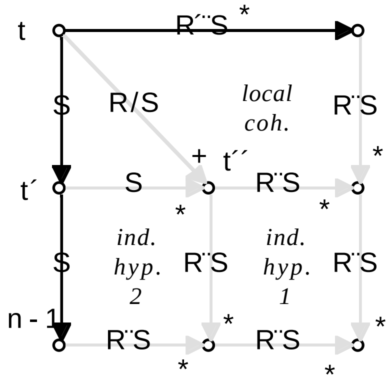


case 2.3:



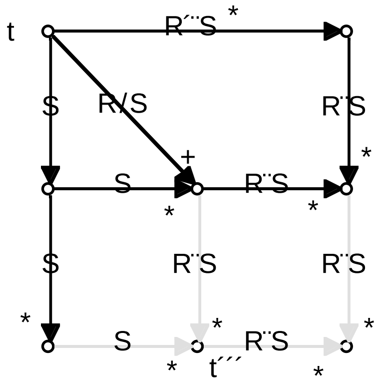
As required, $t \xrightarrow[R/S]{}^{+} t'''$ holds, via $t \underset{S}{\Rightarrow} \xrightarrow[R/S]{}^{+} t'''$.

case 3:



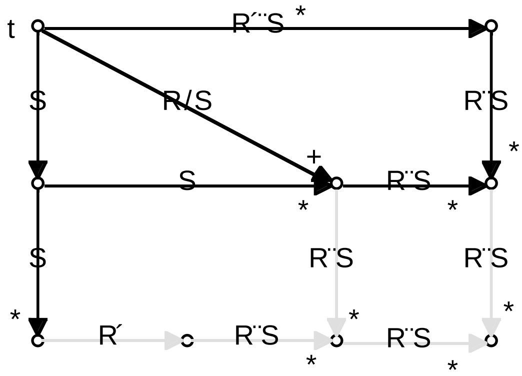
Ind. hyp. 2 justified by $t \underset{S}{\Rightarrow} t'$, $n > n\text{-}1$.
ind. hyp. 1 justified by $t \xrightarrow[R/S]{}^{+} t''$.

case 3.1:

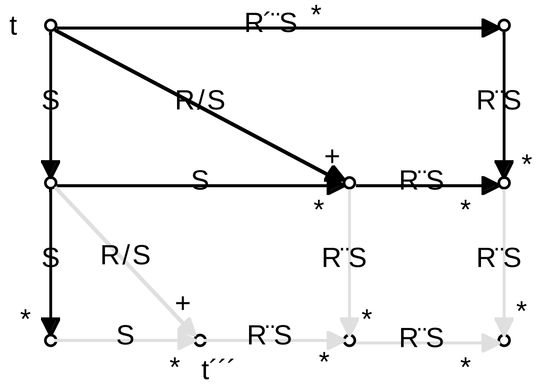


As required, $t \xrightarrow[R/S]{}^{+} t'''$ holds, via $t \xrightarrow[R/S]{}^{+} \xrightarrow[R\cup S]{}^{*} t'''$.

case 3.2:



case 3.3:



As required, $t \xrightarrow[R/S]{}^{+} t'''$ holds, via $t \underset{S}{\Rightarrow} \xrightarrow[R/S]{}^{+} t'''$.

□

Note that case 3 in the coherence notion is indispensable for the proof, case 2.1, even if we skipped case 3 in local S-coherence. This points to the fact that the coherence notion is well-chosen.

For rewrite systems R and S, coherence of $\underset{S}{\leftarrow}\underset{R}{\rightarrow}$ is supported by a critical pair criterion. One arrives at the theorem:

Theorem: *(first confluence criterion)*
Let R be a left-linear rewrite system, S a confluent rewrite system, and R/S Noetherian. If for every (S, R)-critical pair (t, t´), either $t \underset{S}{\rightarrow}^{*} {}^{*}\!\underset{R\cup S}{\longleftarrow} t'$ or $t \underset{R}{\rightarrow} \underset{R\cup S}{\longrightarrow}^{*} {}^{*}\!\underset{R\cup S}{\longleftarrow} t'$ holds, and all (R, R)-critical pairs (t, t´) satisfy $t \underset{R\cup S}{\longrightarrow}^{*} {}^{*}\!\underset{R\cup S}{\longleftarrow} t'$, then $R\cup S$ is confluent.

Example: *(Nonfin, continued)*
Let f, c, s denote unary function symbols, x a variable, and let

$S =_{def} \{cx \rightarrow fcx\}$, and

$R =_{def} \{csx \rightarrow cx\}$.

S is left-linear and there are no (S, S)-critical pairs. So S is confluent. By the same argument, R is confluent. For confluence of $R\cup S$, the following critical pair is to consider:

$$\begin{array}{ccc} csx & \underset{R}{\rightarrow} & cx \\ \downarrow S & & \downarrow S \\ fcsx & \underset{R}{\rightarrow} & fcx \end{array}$$

This diagram satisfies case 2 of the "first confluence criterion", therefore $R\cup S$ is confluent.
In comparison to the commutativity criterion in [Toyama 88], corollary 3.1, S needs not be left-linear. So for example, our criterion treats the systems

$R =_{def} \{c(s(x), s(y)) \rightarrow c(x, y)\}$,

$S =_{def} \{c(x, x) \rightarrow f(c(x, x))\}$

(where c stands for a binary function symbol now) in the same way as above, whereas Toyama´s criterion would fail.

□

The "first confluence criterion" can also be compared to [Huet 80], theorem 3.3. In contrast to Huet, we may not replace $t \underset{R\cup S}{\longrightarrow}^{*} {}^{*}\!\underset{R\cup S}{\longleftarrow} t'$ by $t \underset{R}{\rightarrow}^{*} \underset{S}{\rightarrow}^{*} {}^{*}\!\underset{S}{\leftarrow} {}^{*}\!\underset{R}{\leftarrow} t'$, since we cannot move an R-step before an S-step. In order to justify such moves, we would in addition need coherence of $\underset{S}{\rightarrow}\underset{R}{\rightarrow}$. Without going into details, Huet´s theorem can easily be instantiated ($E = \overline{S}$) in this spirit:

Theorem: *([Huet 80], theorem 3.3)*
Let R be a left-linear rewrite system, S a confluent rewrite system, and R/S Noetherian. If every ($\overline{S}\cup R$, R)-critical pair (t, t´) satisfies $t \underset{R}{\rightarrow}^{*} \underset{S}{\rightarrow}^{*} {}^{*}\!\underset{S}{\leftarrow} {}^{*}\!\underset{R}{\leftarrow} t'$, then $R\cup S$ is confluent, and moreover $=_{R\cup S} \; = \; \underset{R}{\rightarrow}^{*} \underset{S}{\rightarrow}^{*} {}^{*}\!\underset{S}{\leftarrow} {}^{*}\!\underset{R}{\leftarrow}$ holds.

□

Confluence of S may still be weakened to ${}^{*}\underset{S}{\leftarrow}\ \underset{S}{\rightarrow}{}^{*} \subseteq \underset{R}{\rightarrow}{}^{*}\ \underset{S}{\rightarrow}{}^{*}\ {}^{*}\underset{S}{\leftarrow}\ {}^{*}\underset{R}{\leftarrow}$ here (proof omitted).

4.3. On a confluence criterion of Klop

If we want to localize even the (S^*, S)-diagrams, then we must enforce still stronger conditions, very much like Huet´s strong confluence. This is an idea due to [Klop 87]. In this section, we will first recall Klop´s confluence criterion, which is the first mentioned confluence criterion for relative termination in the literature. Then, we will show in two steps how Klop´s criterion can be generalized further. The first step aims at a reformulation of Klop´s result in simpler terms. Starting from the lemma in the previous section, the second step develops a "strongly localized" descendant which obviously generalizes that reformulation. This descendant is particularly interesting even for another reason: It is a common generalization of Newman´s lemma and Huet´s strong confluence lemma. The result is based on the new notion of "strong coherence", which has no counterpart in the equational approach.

Definition: *([Klop 87], Ex. 1.7.11)*
A relation S that commutes over R^{-1} is said to *have splitting effect* (to R), if there are $t \underset{S}{\leftarrow}\ \underset{R\cup S}{\longrightarrow} t'$, such that all n which satisfy $t \underset{R\cup S}{\longrightarrow}{}^{n}\ {}^{*}\underset{R\cup S}{\longleftarrow} t'$ are greater than 1.

□

Klop arrives at the theorem:

Theorem: *([Klop 87], Ex. 1.7.11)*
Let Q_i, $i \in \{1, ..., n\}$, denote a crowd of binary relations, and let $Q = Q_1 \cup ... \cup Q_n$. Suppose that for all i, the following two conditions hold:

(1) Q_i commutes over Q^{-1}, and,

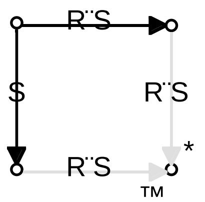
(2) if Q_i has splitting effect to Q, then Q_i is relatively Noetherian to Q.

Then Q is confluent.

□

Now we are going to show that this is a special case of an even further localized variant of the "third localization" lemma of the previous section. First, the condition to have splitting effect becomes much easier to understand when turned into its contrary:

Definition:
Call a relation S *non-splitting* (to R), if the following diagram holds:



□

Note that "non-splitting" is a property similar to "strongly commuting" (cf. the overview in the previous chapter, third section).

Fact:
Let S commute over R^{-1}. Then S is non-splitting to R if and only if, S has no splitting effect to R.

□

Now let all Q_i which have splitting effect, be assembled into a binary relation R, and let S denote Q\R. The property "all Q_i which have splitting effect, are relatively Noetherian to Q" can be replaced by "R is relatively Noetherian to Q", thanks to the "inheritance of relative termination" corollary, part 3, in section 3.1. Thus we get:

Lemma:
If R/S is Noetherian, R locally confluent, and S non-splitting, then R∪S is confluent.

□

Already this lemma is a slight generalization of Klop´s lemma, since it does not require that R commutes with S. But it still admits an interesting relaxation, which can be derived from the "third localization" lemma in the previous section. Namely, if $\xrightarrow[R\cup S]{}^{\varepsilon}$ is an R-step, or an S-step that is guarded by a proper R/S-derivation, then further R∪S-steps may follow:

Definition:
R´ is called *strongly S-coherent*, if $t_1 \xleftarrow[S]{} t_0 \xrightarrow[R']{} t_2$ implies that

(1) $t_1 \xrightarrow[S]{}^{\varepsilon}\ {}^{*}\!\xleftarrow[R\cup S]{} t_2$ or

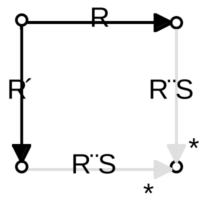
(2) $t_1 \xrightarrow[R']{} \xrightarrow[R\cup S]{}^{*}\ {}^{*}\!\xleftarrow[R\cup S]{} t_2$ or

(3) $\exists t_3.\ t_0 \xrightarrow[R/S]{}^{+} t_3 \wedge t_1 \xrightarrow[S]{}^{\varepsilon} t_3 \xrightarrow[R\cup S]{}^{*}\ {}^{*}\!\xleftarrow[R\cup S]{} t_2$.

□

Notice the ε symbols in cases 1 and 3. There is also a notion of strong E-coherence in [Jouannaud 83], with a different meaning, however. Strong S-coherence actually has no counterpart in the equational approach. (S-coherence and strong S-coherence coincide if S is cyclic and R/S is Noetherian.) Strong S-coherence of S essentially means strong confluence of S. Strong coherence satisfies the following result:

Lemma: *(full localization)*
Let R´ be such that $R \subseteq R' \subseteq R/S$ holds. If R/S is Noetherian, the diagram



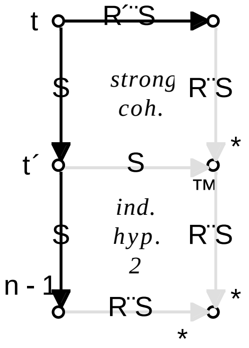
holds, and $R' \cup S$ is strongly S-coherent, then $R \cup S$ is confluent.

Proof:
Using the inductive ordering $((R/S)^+, >)$ on (t, n), we show simultaneously

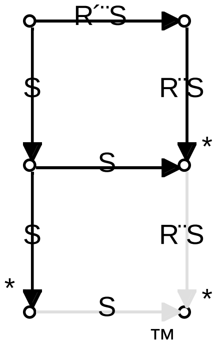
1. the joining of the diagram ${}^*\!\xleftarrow[R\cup S]{} t \xrightarrow[R\cup S]{}\!{}^*$ (let $n =_{def} \omega$ here), and
2. all t, t_1, t_2 with $t_1 \;{}^n\!\xleftarrow[S]{} t \xrightarrow[R'\cup S]{} t_2$ are strongly coherent.

For claim 1 we reuse the proof of the "second localization" lemma. So claim 2 remains to be proven. If n = 0, then everything is trivial (case 1 of the claim holds). Let now n > 0. Then we can apply the premise, which leads to a case analysis very similar to that in the "third localization" lemma.

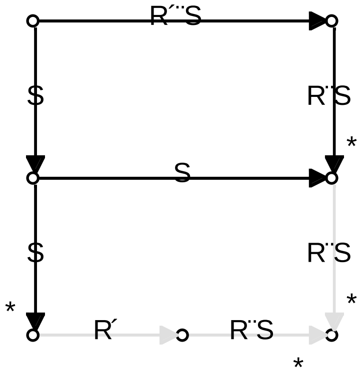
case 1:



case 1.1:

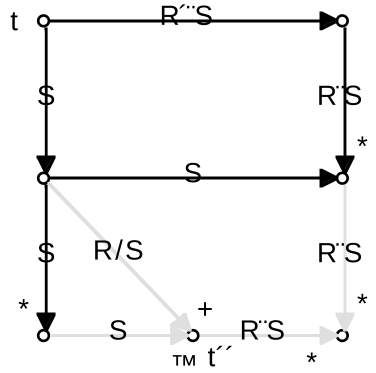


case 1.2:



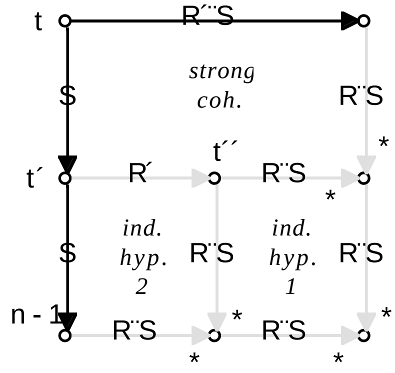
Justification: $t \xrightarrow[S]{} t'$, $n > n-1$.

case 1.3:



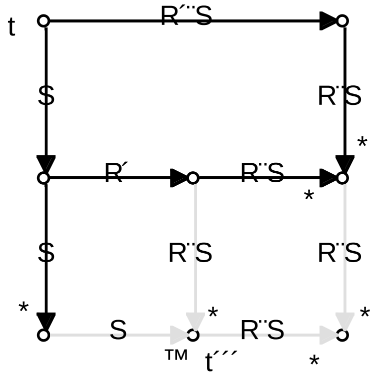
As required, $t \xrightarrow[R/S]{}^{+} t´´$ holds, via $t \xrightarrow[S]{} \xrightarrow[R/S]{}^{+} t´´$.

case 2:



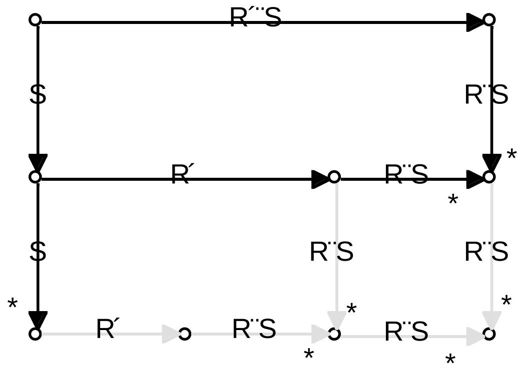
Ind. hyp. 2 justified by $t \xrightarrow[S]{} t´$, n > n-1, ind. hyp. 1 justified by $t \xrightarrow[S]{} \xrightarrow[R´]{} t´´$.

case 2.1:

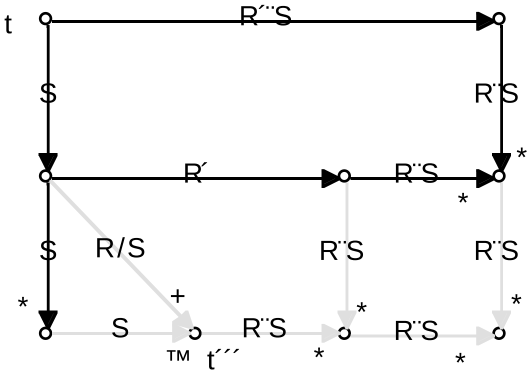


As required, $t \xrightarrow[R/S]{}^{+} t´´´$ holds, via $t \xrightarrow[S]{} \xrightarrow[R´]{} \xrightarrow[R \cup S]{}^{*} t´´´$.

case 2.2:

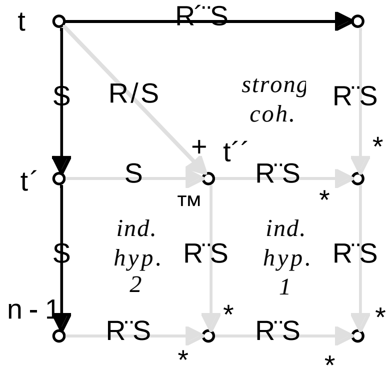


case 2.3:

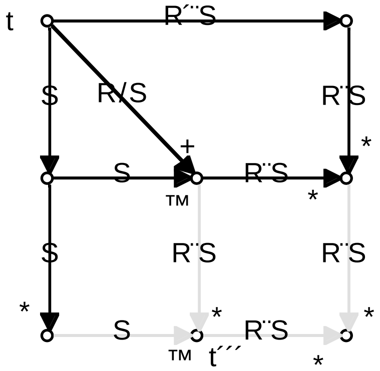


As required, $t \xrightarrow[R/S]{}^{+} t´´´$ holds, via $t \xrightarrow[S]{} \xrightarrow[R/S]{}^{+} t´´´$.

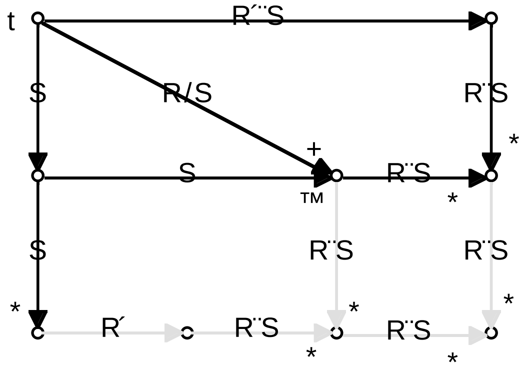
case 3:



<u>case 3.1:</u>

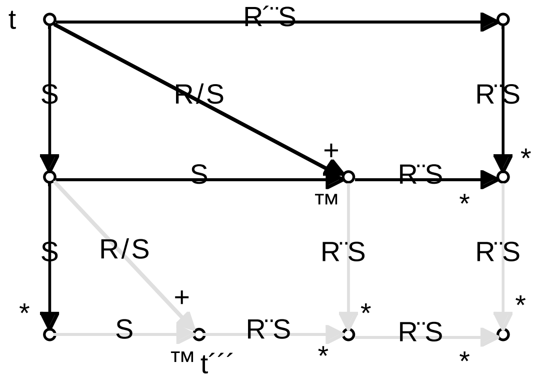


<u>case 3.2:</u>



As required, $t \xrightarrow[R/S]{}{}^{+} t'''$ holds,
via $t \xrightarrow[R/S]{}{}^{+} \xrightarrow[R\cup S]{}{}^{*} t'''$.

<u>case 3.3:</u>



As required, $t \xrightarrow[R/S]{}{}^{+} t'''$ holds, via $t \xrightarrow[S]{} \xrightarrow[R/S]{}{}^{+} t'''$.

□

Note that case 2.1 in the proof relies on case 3 in the definition of strong coherence (cf. the note after the "first localization" lemma in the previous section).
Let now R and S denote rewrite systems, and let $R' = R$. By the critical pair theorem, we get:

Theorem: *(second confluence criterion)*
Let R be a left-linear rewrite system, S a left- and right-linear rewrite system, and R/S Noetherian. If for every $(S, R\cup S)$-critical pair (t, t'), either $t \xrightarrow[S]{}{}^{\varepsilon}\ {}^{*}\xleftarrow[R\cup S]{} t'$ or $t \xrightarrow[R]{} \xrightarrow[R\cup S]{}{}^{*}\ {}^{*}\xleftarrow[R\cup S]{} t'$ holds,   and all (R, R)-critical pairs (t, t') satisfy $t \xrightarrow[R\cup S]{}{}^{*}\ {}^{*}\xleftarrow[R\cup S]{} t'$, then $R\cup S$ is confluent.

□

This result can be seen as a common generalization of the Knuth-Bendix criterion on the one hand (except for the left-linearity requirement on R, which may be dropped when S = Ø), and Huet´s first strong confluence criterion on the other hand (for R = Ø).

Example: *(FF, continued)*

Consider R $=_{def}$ {ffx $\to$ fgfx}, S $=_{def}$ {fa $\to$ gfa}. We learnt in the previous chapter that R/S is Noetherian and S is not. R is left-linear, S is left- and right-linear and has no critical pairs. The only (R, R)-critical pair joins:

$$\begin{array}{ccc} \text{fffx} & \underset{R}{\rightarrow} & \text{fgffx} \\ \downarrow_R & & \downarrow_R \\ \text{ffgx} & \underset{R}{\rightarrow} & \text{fgfgfx} \end{array}$$

The only (R, S)-critical pair is trivial. So it meets case 1 in the definition of strong coherence. Therefore R$\cup$S is confluent, according to the "second confluence criterion". Toyama´s confluence criterion ([Toyama 87b]) for direct sums fails because R and S share the function symbol g.

□

5. Applications of relative termination

This chapter presents two results about narrowing where relative termination plays a key role. It is shown that narrowing with intermediate rewriting (not necessarily to normal form; "reduced narrowing") is complete if the rules used for this rewriting are relatively Noetherian to the whole rule set. Moreover it is shown that *normal narrowing* where normalization is done with a normalizing subset of the rule set, is complete, if the normal forms are finally preserved. (Recall that normalizing means that normal forms always exist.) These two results generalize the classical theorem of [Fay 79] that normal narrowing is complete for Noetherian rewrite systems. By a counterexample, a previous claim of the completeness of normal narrowing in [Hußmann 85] is shown wrong, and the mistake in the proof is analyzed and repaired.

5.1. Oriented paramodulation and narrowing

Equational unification is the task to solve an arbitrary equation in a given equational theory. Universal unification is accordingly a procedure that assigns to an equational theory E and an equation (t, t´), the set of E-unifiers of t and t´. Paramodulation steps and narrowing steps are basic steps of a complete universal unification procedure, where completeness means that every solution is covered by a computed unifier. This section is to introduce the notions of paramodulation and narrowing, their connection to each other, and their role in rewriting and equational reasoning. The notion of paramodulation is presented in a new style.

Paramodulation ([Robinson, Wos 69]) was invented in order to handle equality in resolution in an adequate and fairly efficient way. See [Padawitz 88], [Furbach et al. 89], and [Hölldobler 89] for a comprehensive treatment of paramodulation. Commonly paramodulation is defined for conditional, symmetric rewrite systems. Employing our liberal understanding of term rewrite system, it appears technically more convenient to drop the symmetry condition. (In other words: The orientation of rules is taken into account. Elsewhere the notion of *oriented paramodulation* is used to stress this. Here usual paramodulation is modelled by oriented paramodulation using a symmetry closed rewrite system.) In this thesis, we will need paramodulation and narrowing only for the unconditional case, and we will always mean the oriented variant.

Solving an equation (t, t´) in an equational theory E means to find an E-*unifier* σ of the left hand side t and the right hand side t´ of the equation, i.e. a substitution σ such that $t\sigma =_E t'\sigma$ holds. (Recall that $=_E$ denotes the congruence closure of $\underset{E}{\rightarrow}$.) Since we adopt a liberal view of term rewrite system, we may assume that $E = \overline{R}$ for some rewrite system R. Let us in the following assume that R is confluent. It is well known that R then satisfies the Church-Rosser property:

$t\sigma =_R t'\sigma$ if and only if for some t'', both $t\sigma \xrightarrow[R]{}^* t''$ and $t'\sigma \xrightarrow[R]{}^* t''$.

For convenience, we encode the two derivations $t\sigma \xrightarrow[R]{}^* t''$ and $t'\sigma \xrightarrow[R]{}^* t''$ into one. For this purpose, we fix the following convention (the idea to this encoding goes back to [Hullot 80] who used the name "h" instead of "eq".):

Encoding convention:

Let there be a binary function symbol eq$\in$ F to express equality, with the reflexive axiom $(eq(x, x) \rightarrow true) \in R$, and "true" and "eq" do not appear as a top symbol on any other left hand side in R.

□

Now we may treat equations (t, t') as if they were terms $eq(t, t')$:

Lemma: *(encoding)*

Let R denote a confluent rewrite system where the encoding convention holds. Then a substitution σ is a $\overline{R}$-unifier of the equation (t, t') if and only if, $eq(t, t')\sigma \xrightarrow[R]{}^* true$ holds.

Proof:

($\Leftarrow$)

Because reflexivity is the only rule where "eq" occurs on the left hand side, the topmost symbol "eq" cannot be removed from the goal, unless by application of reflexivity. Reflexivity leads to the term "true", which is in normal form, and which can therefore only be the last term in the rewrite derivation. So the derivation has for some suitable t'' the form $eq(t, t')\sigma \xrightarrow[R]{}^* eq(t'', t'') \xrightarrow[R]{} true$, and all rewrite steps, except the last one, happen strictly below the top. Therefore we have both $t\sigma \xrightarrow[R]{}^* t''$ and $t'\sigma \xrightarrow[R]{}^* t''$, i.e. σ is indeed an $\overline{R}$-unifier of (t, t').

($\Rightarrow$)

Let σ denote an $\overline{R}$-unifier of (t, t'), i.e. σ satisfies both $t\sigma \xrightarrow[R]{}^* t''$ and $t'\sigma \xrightarrow[R]{}^* t''$ for some t''. So in particular $eq(t, t')\tau \xrightarrow[R]{}^* eq(t'', t'') \xrightarrow[R]{} true$ holds, where the last applied rule is reflexivity.

□

Systems of equations might be treated likewise, by means of an additional binary function symbol and$\in$ F, with the rewrite rule $(and(true, x) \rightarrow x) \in R$, and "and" does not appear as top symbol on any other left hand side in R. The system of equations

$(t_1, t_1'), ..., (t_n, t_n')$

could be encoded into

$and(eq(t_1, t_1'), ..., and(eq(t_n, t_n'), true) ...)$.

We will however stick to the single equation case in the following.

So far, we have reduced the unification problem to the problem of finding all those substitutions σ which enable a certain derivation. Now it appears quite natural to consider the single-step problem, and this is the key idea to paramodulation, as we will see in a minute. Fix an occurrence u and a rewrite rule $(l \to r) \in R$, which has been renamed such that $Var(l \to r) \cap Var(t) = Ø$, without loss of generality. We have to enumerate the set

$$P = \{ \sigma.\ t\sigma \xrightarrow[l\to r]{u} (t\sigma)[u \leftarrow r\sigma] \}$$

of all substitutions σ such that the instance $t\sigma$ admits a rewrite step using the rule $l \to r$ at u. Obviously P contains all the information needed to compute E-unifiers step by step. In the definition of P, we use already the fact that the right hand side of the rewrite step is uniquely determined by u, $l \to r$, and σ, even when $l \to r$ should be right-erasing. (Here one must be careful because of the liberal notion of rewrite rule.) On this account, P is characterized by

$$P = \{ \sigma.\ (t\sigma)/u = l\sigma \}.$$

P is often infinite, though a finite description is desirable. For instance, it can easily be verified that for each $\sigma \in P$, also $\sigma\tau \in P$. On this account, it makes sense to define a paramodulation step as a step that computes a set of most general (i.e. minimal with respect to the subsumption ordering $\leq_{sub}$) elements of P.

Definition:

Let t, t´ be terms, u an occurrence, $l \to r$ a rewrite rule, and σ a substitution. Then t *admits a paramodulation step at* u *with* σ *(to* t´ *)*, (in symbols $t \xrightarrow[l\to r]{P\ u}_{\sigma} t'$) if

(1) $t\sigma \xrightarrow[l\to r]{u} t'$, and

(2) $t\sigma' \xrightarrow[l\to r]{u} t''$ implies that there is a substitution η such that both $t\sigma\eta = t\sigma'$ and $t'\eta = t''$.

□

(Elsewhere this definition is called the *lifting lemma*, since it appears as a consequence of a different definition.) In short, one may say that, given a term t, an occurrence u, and a rule $l \to r$, paramodulation describes *the most general instance* $t\sigma$ of t *that admits a rewrite step* at u using rule $l \to r$. For this reason, rewrite steps may be considered as a special case of paramodulation steps.

Above we suggested that there is a finite presentation of P. The set of paramodulation steps for fixed u and $l \to r$ is actually finite, provided F is finite. So we can *effectively compute* paramodulation steps, where we have to distinguish two cases:

<u>Case 1:</u> $u \in FOcc(t)$.

Then $(t\sigma)/u = (t/u)\sigma$, so $P = \{ \sigma.\ (t/u)\sigma = l\sigma \}$. In other words, P is the set of Ø-unifiers of t/u and l. As it is well known, Ø-unifiers are decidable, and the most general Ø-unifier, if it exists, is unique up to renaming. Such a step is also called a *narrowing step* (in symbols $t \xrightarrow[l\to r]{N\ u}_{\sigma} t'$).

Case 2: $u \notin FOcc(t)$.

Then there are occurrences v, w, and a variable x such that $t/v = x$, $(x\sigma) / w = l\sigma$, and $u = v.w$ hold. Moreover v, w, and x are unique. Without going much into details, let us state that here the finite set

$$\{ [l'[w \leftarrow l] \ / \ x]. \quad \forall w' \in FOcc(l').\ w' <_{pre} w \}$$

is equal (modulo renaming) to the set of most general elements from P. The term l' is called *the prefix to* l *in* $l'[w \leftarrow l]$ which is substituted for x. [Padawitz 88] shows that prefixed rules $l'[w \leftarrow l] \ \rightarrow \ l'[w \leftarrow r]$ allow to simulate proper paramodulation steps by narrowing steps.

Even if both R and F are finite, paramodulation is usually infinitely branching, i.e. from a term t infinitely many paramodulation steps may start, due to infinitely many occurrences $u \notin FOcc(t)$ below a variable x. This drawback is not shared by narrowing, provided R is finite. Narrowing is a restricted form of paramodulation; it coincides with paramodulation when σ is normal. (A substitution σ is called *normal*, if $x\sigma$ is normal for all $x \in X$.) This fact makes narrowing more attractive than paramodulation. I found it instructive to perform all proofs for the paramodulation case first, and to add a corollary for narrowing.

Example:

1. Let $R =_{def} \{0+x \rightarrow x,\ s(x)+y \rightarrow s(x+y)\}$ and $t =_{def} z+z$. Narrowing steps for t can take place at occurrence λ only. Up to renaming, they are

$$t \xrightarrow[R]{P\ \lambda}_{\sigma} 0, \qquad \text{and}$$

$$t \xrightarrow[R]{P\ \lambda}_{\sigma'} s(z'+s(z')),$$

where $\sigma =_{def} [0/x, 0/z]$, and $\sigma' =_{def} [z'/x, s(z')/y, s(z')/z]$. An infinite crowd of further paramodulation steps (which are no narrowing steps) is for instance

$$t \xrightarrow[R]{P\ u}_{\sigma} s^i(0) + s^i(0+0), \qquad i \in \mathbb{N},$$

where $u = 1. \ldots .1$ (i times), and $\sigma'' =_{def} [0/x,\ s^i(0+0) / z]$.

2. Let $R =_{def} \{eq(x, x) \rightarrow true\}$ and $g =_{def} eq(f(y), z)$. The only R-paramodulation step (actually a narrowing step) for the goal g is

$$g \xrightarrow[R]{P\ \lambda}_{\sigma} true,$$

where $\sigma =_{def} [f(y)/x, f(y)/z]$.

□

A paramodulation step is the basic step of a *complete universal unification procedure*: A set U of E-unifiers of (t, t') is called *complete*, if every E-unifier τ of t and t' is *covered* by some computed unifier $\sigma \in U$, i.e. $eq(t, t')\tau \geq_{sub} eq(t, t')\sigma$ holds. (There is a different notion of completeness in the literature, see [Fages, Huet 83], which uses subsumption *modulo E* . Our procedures may produce some superfluous substitutions on that account.) Given an equational specification E and two terms t and t´, the paramodulation procedure indeed delivers a complete set of E-unifiers of t and t´.

Theorem: *(completeness of paramodulation)*
Assume that R is a confluent rewrite system satisfying the "encoding convention". Let U denote the set of substitutions $\sigma = \sigma_1 ... \sigma_n$ where eq(t, t´) $\xrightarrow{P}_{R}{}_{\sigma_1} \ldots \xrightarrow{P}_{R}{}_{\sigma_n}$ true is a paramodulation derivation. Then U is a complete set of $\overline{R}$-unifiers of (t, t´).

Proof:
After the explanations above, the proof is not hard.
Correctness: I.e. U only contains $\overline{R}$-unifiers of (t, t´). Assume given a paramodulation derivation eq(t, t´) $\xrightarrow{P}_{R}{}_{\sigma_1} \ldots \xrightarrow{P}_{R}{}_{\sigma_n}$ true, and let $\sigma = \sigma_1 ... \sigma_n$. Paramodulation by definition describes most general rewrite steps, so here there is a rewrite derivation eq(t, t´)$\sigma \xrightarrow[R]{}{}^{*}$ true. Employing the "encoding" lemma, this means that σ is an $\overline{R}$-unifier of (t, t´).
Completeness: I.e. every $\overline{R}$-unifier of (t, t´) is covered. Let τ denote an $\overline{R}$-unifier of (t, t´). Due to the "encoding" lemma, τ satisfies eq(t, t´)$\tau \xrightarrow[R]{}{}^{*}$ true. According to the definition of paramodulation, there exists a paramodulation derivation eq(t, t´) $\xrightarrow{P}_{R}{}_{\sigma_1} \ldots \xrightarrow{P}_{R}{}_{\sigma_n}$ true and some η where $\tau = \sigma_1 ... \sigma_n \eta$. Hence τ is covered by the computed unifier $\sigma =_{def} \sigma_1 ... \sigma_n$.

□

If the substitution τ is normal, every paramodulation step is actually a narrowing step.

Corollary: *(completeness of narrowing; for R Noetherian, see [Hullot 80]; [Hußmann 85])*
Assume that R is a confluent rewrite system which satisfies the encoding convention. Let U denote the set of substitutions $\sigma = \sigma_1 ... \sigma_n$ where eq(t, t´) $\xrightarrow{N}_{R}{}_{\sigma_1} \ldots \xrightarrow{N}_{R}{}_{\sigma_n}$ true is a narrowing derivation. Then U is a set of $\overline{R}$-unifiers of (t, t´) which is complete for normal $\overline{R}$-unifiers of (t, t´).

□

5.2. Normal narrowing is not complete

The pure narrowing procedure is very inefficient as theoretical considerations ([Bockmayr 86]) and practical use ([Geser, Hußmann 85], [Hammes 86]) have shown. Various improvements have therefore been investigated: Basic narrowing ([Hullot 80]), redex selection strategies ([Fribourg 84], [Padawitz 87], [Echahed 88]), and *normal narrowing*, i.e. narrowing with intermediate normalization of terms ([Fay 79]). Overviews of narrowing optimizations are given in [Rety 87], [Nutt et al. 87] and [Padawitz 88].

Normal narrowing has up to now only been considered when the whole set of rewrite rules was terminating (except in [Hußmann 85]). However it is also an interesting question whether narrowing with normalization by a *normalizing subset* R of the rules remains complete, although the whole set $R \cup S$ of rules is potentially nonterminating. This question is connected with relative termination, as we will see. In this section we will show by a counterexample that, against all expectations, *R-normal R∪S-narrowing is not complete* for normal solutions, even when R terminates. This counterexample falsifies a conjecture of [Hußmann 85] and shows that Hußmann´s (correct) proof attempt was insufficient.

A normal paramodulation step (and accordingly a normal narrowing step) for t consists in reducing t to an R-normal form — for this reason let us assume that R is normalizing — followed by a paramodulation step. Formally, normal paramodulation is defined thus:

Definition:

Let R be normalizing. An *R-normal R∪S-paramodulation step* from t to t´ is defined by:

$$t \xrightarrow[R,R\cup S]{NP}_{\sigma} t´, \text{ if } t \xrightarrow[R]{}^{NF} \xrightarrow[R\cup S]{P}_{\sigma} t´.$$

□

The optimizing effect is obvious as a normal paramodulation derivation is a special case of a paramodulation derivation (by taking rewrite steps as paramodulation steps), and some paramodulation derivations are cut off. For the same reason, normal paramodulation is correct against the paramodulation procedure. The same reasoning applies to normal *narrowing*. It is commonly known that if $S = \emptyset$, completeness can be easily proven by induction on R ([Fay 79]). The completeness proof in the case $S \neq \emptyset$ nonterminating is, however, much more intricate. Hußmann attempted to give such a proof for the conditional case with [Hußmann 85], lemma 5.6. We will reexamine the reasoning for the unconditional case only. An unconditional version of the lemma which Hußmann proved looks as follows:

Fact:

If R is confluent, then $t \xrightarrow[R]{}^{*} true$ and $t \xrightarrow[R]{} t´$ imply $t´ \xrightarrow[R]{}^{*} true$.

□

Using this lemma, arbitrarily many R-normalization steps may be interleaved with the narrowing steps without loosing completeness. But let us be precise:

Theorem:

Let R be a confluent rewrite system, and $n \in \mathbb{N}$ arbitrary. Let U denote the set of substitutions $\sigma = \sigma_1 ... \sigma_k$ where either

(1) $k \leq n$ and $eq(t, t´) \xrightarrow[R,R\cup S]{NP}_{\sigma_1} ... \xrightarrow[R,R\cup S]{NP}_{\sigma_k} true$, or

(2) $k > n$ and $eq(t, t´) \xrightarrow[R,R\cup S]{NP}_{\sigma_1} ... \xrightarrow[R,R\cup S]{NP}_{\sigma_n} \xrightarrow[R]{P}_{\sigma_{n+1}} ... \xrightarrow[R]{P}_{\sigma_k} true$

hold. (Informally: As soon as the length of the normal paramodulation derivation exceeds n, normalization is switched off.) Then U is a complete set of $\overline{R}$-unifiers of (t, t´).

□

The difference to normal paramodulation is very small: An arbitrary upper bound for the number of normalizations exists. But this theorem does not say that normal paramodulation is complete.

Lemma:
R-normal R∪S-narrowing may be *incomplete* although R is Noetherian, and R, S, and R∪S are confluent.

Proof:
By counterexample. Let a, b, c be constants, and let

$R =_{def} \{a \to b, \quad eq(x, x) \to true\}$ and

$S =_{def} \{b \to a, \quad a \to c\}$.

The goal $g =_{def} eq(b, c)$ has the trivial solution *id*, the identity substitution (there is no unknown to be solved). This solution is obtained by means of the following narrowing derivation:

$eq(b, c) \quad \xrightarrow{N}_{S} id \quad eq(a, c) \quad \xrightarrow{N}_{S} id \quad eq(c, c) \quad \xrightarrow{N}_{R} id \quad true.$

On the other hand, the only narrowing derivation with R-normalization is

$eq(b, c) \quad \to_{R}^{NF} \quad eq(b, c) \quad \xrightarrow{N}_{S} id$

$eq(a, c) \quad \to_{R}^{NF} \quad eq(b, c) \quad \xrightarrow{N}_{S} id$

$eq(a, c)$ ...

which becomes cyclic and therefore yields no solution.
(S contains a left hand side "a" which is not in R-normal form. It may seem that this was the reason for incompleteness. However a slightly changed example points out the contrary: Let f be a unary function symbol, and a, b, and c be constants. The setting

$R =_{def} \{f(a) \to b, \; eq(x, x) \to true\}$,

$S =_{def} \{b \to f(a), \; a \to c\}$,

$g =_{def} eq(b, f(c))$

works the same way.)

□

What went wrong? The missing link is a *fairness* argument. In the counterexample, the application of a narrowing step after R-normalization destroyed R-normal forms again and again. In other words, S did not finally preserve R-normal forms (this notion will be defined below). Although every intermediate goal has the potential to reach the solution, it is not certain whether sufficiently many steps decrease the distance to (i.e. the length of the shortest derivation to) the solution. If S does finally preserve R-normal forms, then the distance to the solution finally decreases, and completeness holds indeed, as we will prove in the last section.

5.3. Relative termination and reduced narrowing

Before we prove a completeness result for normal narrowing based on the premise that S finally preserves R-normal forms, let us first consider the special case R relatively Noetherian to S. The issue becomes comparatively simple here since we need not care about normal forms. We actually need not perform R-*normalization*, but may perform arbitrarily less R-rewrite steps. Padawitz ([Padawitz 88], section 8.7) calls this technique "R-reduced R∪S-paramodulation". We will arrive at a surprisingly simple proof of completeness of R-reduced R∪S-paramodulation and narrowing.

Definition:

An *R-reduced R∪S-paramodulation step* from t to t´ is defined by:

$$t \xrightarrow[R,R\cup S]{RP}_{\sigma} t´, \text{ if } t \underset{R}{\rightarrow}^{*} \xrightarrow[R\cup S]{P}_{\sigma} t´.$$

□

This definition does not yet cover the following fact: A procedure for reduced paramodulation performs the R-reduction in a "trap door" way, i.e. it disregards alternative R-reduction steps. But at a point where a paramodulation step is due, *all* possible paramodulation steps are considered. We may take this into account by the following definition:

Definition:

A set D of reduced paramodulation derivations starting from t is called a *computed set*, if it satisfies the following constraints:

(1) If some reduced paramodulation derivation in D has the prefix

$$t \xrightarrow[R,R\cup S]{RP}_{\sigma_1} \ldots \xrightarrow[R,R\cup S]{RP}_{\sigma_{n-1}} \underset{R}{\rightarrow}^{*} t´ \xrightarrow[R\cup S]{P}_{\sigma_n} t´´,$$

then for every paramodulation step $t´ \xrightarrow[R\cup S]{P}_{\sigma_n´} t´´´$, D contains a reduced paramodulation derivation which has the prefix

$$t \xrightarrow[R,R\cup S]{RP}_{\sigma_1} \ldots \xrightarrow[R,R\cup S]{RP}_{\sigma_{n-1}} \underset{R}{\rightarrow}^{*} t´ \xrightarrow[R\cup S]{P}_{\sigma_n´} t´´´.$$

(2) Every reduced paramodulation derivation in D which has the prefix

$$t \xrightarrow[R,R\cup S]{RP}_{\sigma_1} \ldots \xrightarrow[R,R\cup S]{RP}_{\sigma_{n-1}} \underset{R}{\rightarrow}^{*} t´,$$

continues with a rewrite step or a paramodulation step, provided that t´ admits a paramodulation step.

□

This definition will in the following only be used informally, however. The proof of the following completeness theorem relies on the fact that, as long as R-steps are performed, the goal decreases with respect to the ordering $(\underset{R}{\rightarrow} / \underset{S}{\rightarrow})^{+}$, otherwise this ordering is preserved and the length of the remaining derivation decreases.

Theorem: *(completeness of R-reduced R∪S-paramodulation)*
If R∪S is confluent and R/S is Noetherian, then R-reduced R∪S-paramodulation is complete, i.e. every computed set of R-reduced R∪S-paramodulation derivations computes a complete set of $\overline{R\cup S}$-unifiers.

Proof:
We prove

$$\text{If } g\tau \xrightarrow[R\cup S]{}^{n} \text{true, then } g \xrightarrow[R, R\cup S]{RP}{}_{\sigma}^{*} \text{ true where } g\sigma \leq_{sub} g\tau$$

by induction along the ordering » on pairs $(g\tau, n)$, defined by

$$(t, n) \gg (t', n') \Leftrightarrow_{def}$$
$$t \ (\xrightarrow[R]{} / \xrightarrow[S]{})^{+} \ t' \ \vee$$
$$t \xrightarrow[R\cup S]{}^{*} t' \ \wedge \ n >_{\mathbb{N}} n'.$$

Case 1: $g\tau$ = true.

Obvious.

Case 2: $g\tau \xrightarrow[R\cup S]{} \xrightarrow[R\cup S]{}^{n-1}$ true.

According to the definitions of reduced paramodulation and computed set, now either an R-rewrite step or an R∪S-paramodulation step is done. It must be shown that no matter which one is chosen, an approximant of τ is safely computed.

Case 2.1: An R-rewrite step is chosen.

Then $g \xrightarrow[R]{} g'$ and, since R∪S is confluent, $g'\tau \xrightarrow[R\cup S]{}^{*}$ true. Because $g\tau \xrightarrow[R]{} g'\tau$, the induction hypothesis applies and yields the claim.

Case 2.2: An "ordinary" paramodulation step is chosen.

By definition of a paramodulation step: $g \xrightarrow[R]{P}{}_{\mu} g'$, $\mu\tau' = \tau$, $g'\tau' \xrightarrow[R\cup S]{}^{n-1}$ true. The inductive hypothesis applies, because $g\tau \xrightarrow[R\cup S]{} g'\tau'$ and $n > n-1$. It yields a substitution σ' where $g'\sigma' \leq_{sub} g'\tau'$. One can choose σ' such that $g\mu\sigma' \leq_{sub} g\mu\tau'$ holds. So $g\sigma \leq_{sub} g\tau$, where $\sigma =_{def} \mu\sigma'$.

□

Corollary: *(completeness of R-reduced R∪S-narrowing)*
If R∪S is confluent, and R/S is Noetherian, then R-reduced R∪S-narrowing is complete for normal substitutions.

Proof:
Like above. Notice that in case 2.2, the substitution τ' is R∪S-normal since τ is. So the paramodulation step actually is a narrowing step.

□

5.4. A completeness result for normal narrowing

As promised above, even the comparatively weak condition "S finally preserves R-normal forms, and R normalizing" suffices for a completeness proof of R-normal $R \cup S$-paramodulation. The section begins with a definition of final normal form preservation together with a number of basic facts about it. The main problem which we come across is then: Instantiation along a paramodulation derivation does not preserve normal forms at all. How can we take use of final normal form preservation anyway? The essential trick is to prove that finally there is no more strict instantiation. The proof is rather technical in nature; any reader who is not familiar with substitution handling is suggested to skip it. The remainder of the section is devoted to a detailed proof of the completeness claim.

Definition:

1. S *preserves* R-*normal forms*, if for all t, t' such that $t \underset{S}{\rightarrow}^* t'$ and $t \in NF_R$, also $t' \in NF_R$ holds.
2. The relation $\underset{R}{\rightarrow}^{+NF}$ (*"proper R-normalization"*) is defined by

   $$t \underset{R}{\rightarrow}^{+NF} t' \;\Leftrightarrow_{def}\; t \underset{R}{\rightarrow}^{+} t' \wedge t' \in NF_R.$$

Note that as a consequence, $t \notin NF_R$. Accordingly $\underset{R}{\rightarrow}^{+NF}$ is Noetherian.

3. S *finally preserves* R-*normal forms*, if every derivation

   $$t_0 \underset{R}{\rightarrow}^{NF} \underset{S}{\rightarrow}^* t_1 \underset{R}{\rightarrow}^{NF} \underset{S}{\rightarrow}^* t_2 \underset{R}{\rightarrow}^{NF} \underset{S}{\rightarrow}^* \ldots$$

contains only finitely many $t_i \notin NF_R$.

□

These three notions are closely correlated:

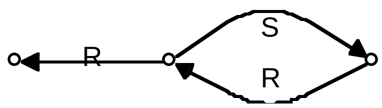
Facts:

1. If S preserves R-normal forms, then S finally preserves R-normal forms.
2. S finally preserves R-normal forms if and only if, $\underset{R}{\rightarrow}^{+NF} / \underset{S}{\rightarrow}$ is Noetherian.
3. If R/S is Noetherian, then S finally preserves R-normal forms.

(Proof: $(\underset{R}{\rightarrow}^{+NF} / \underset{S}{\rightarrow})^+ \subseteq (\underset{R}{\rightarrow}^{+} / \underset{S}{\rightarrow})^+ = (\underset{R}{\rightarrow} / \underset{S}{\rightarrow})^+$.)

□

The converse of the third lemma does not hold: S may preserve R-normal forms although R/S is not Noetherian, as the following counterexample demonstrates:



Now the main result of this chapter can be formulated:

Theorem:*(completeness of R-normal (oriented) R∪S-paramodulation)*
If R∪S is confluent, R is normalizing, and S finally preserves R-normal forms, then R-normal (oriented) R∪S-paramodulation is complete.

□

Let us first attack the completeness proof informally. Suppose that goal g has a solution τ, i.e. there exists a derivation $g\tau \xrightarrow[R\cup S]{}^{n}$ true for some $n\in\mathbb{N}$. In order to compute a unifier that covers τ, we must step by step construct a normal paramodulation derivation that approximates τ. The first normal paramodulation step $g \xrightarrow[R,R\cup S]{NP}_{\mu} g'$ brings up the following goal g'. The substitution μ must satisfy $g\tau \geq_{sub} g\mu$, otherwise τ could no longer be covered. (Such a normal paramodulation step really exists, as will be shown below.) In other words, there is a substitution τ' that satisfies $g\tau = g\mu\tau'$. By confluence of R∪S, a derivation $g'\tau' \xrightarrow[R\cup S]{}^{n'}$ true exists. Now the proof would be finished if the inductive hypothesis could be applied to that derivation. This means, we need a suitable Noetherian ordering > that compares the two derivations:

$$(g\tau \xrightarrow[R\cup S]{}^{n} \text{true}) \;>\; (g'\tau' \xrightarrow[R\cup S]{}^{n'} \text{true}) .$$

Final normal form preservation means that $(\xrightarrow[R]{}^{+NF} / \xrightarrow[S]{})^{+}$ is a Noetherian ordering. As soon as normal forms are preserved, the normal paramodulation steps come down to "ordinary" paramodulation steps. So far, so good. But paramodulation steps may *instantiate* goals — instantiation may at any time destroy normal forms. This means a severe problem to the proof since the normal form preservation property cannot work as long as it is interfered by instantiation. Renamings are by the way harmless; they cannot turn a normal form into a rewrite redex. The crucial fact that solves the problem is: Strict instantiation cannot happen infinitely often. A Noetherian ordering > will be defined that compares τ with τ' such that either $\tau > \tau'$ or τ' is essentially a renaming of τ. Renaming can easily be factored away. So sooner or later $t\tau = t\tau'$ must be reached, and then normal form preservation ticks. The Noetherian ordering which we need will be defined as a lexicographic combination on triples (τ, g, n).

Let σ be an approximant of τ, i.e. $g\tau = g\mu\tau'$ holds for some suitable substitution τ'. One may then say that for g the substitution τ is "missing" to the final instance $g\tau$, and likewise τ' for $g\mu$. The "missing" substitutions are ordered by a Noetherian ordering.

Definition:

1. *Multisets* are collections of elements where in contrast to sets also the multiplicity of elements counts. Given an ordering $>$ on elements, its *multiset extension* $>_{mult}$, an ordering on multisets, is defined as the closure under $+$ (the multiset sum) and under transitivity of the relation:

$$\{ ([y], m).\quad y > x \text{ for all } x \in m \}.$$

It is known that the multiset extension of a Noetherian ordering is Noetherian on finite multisets ([Dershowitz, Manna 79]).

2. Recall from chapter "Termination, termination modulo, and relative termination", section "Termination orderings for rewrite systems" the subterm ordering $|>$ on terms: $t |> t'$ means that t is a strict superterm of t'.

Define the relation » on triples (σ, t, n) by

$$(\sigma, t, n) \gg (\sigma', t', n') \Leftrightarrow_{def}$$
$$[x\sigma.\ x \in Var(t)] \ |>_{mult} \ [x\sigma'.\ x \in Var(t')] \ \vee$$
$$t\sigma = t\sigma' \ \wedge \ (t\ (\underset{R}{\rightarrow}^{NF+} / \underset{S}{\rightarrow})^+\ t' \ \vee$$
$$t\ (\underset{R}{\rightarrow}^{NF} \cup \underset{S}{\rightarrow})^*\ t' \ \wedge \ n >_{\mathbb{N}} n'),$$

where square brackets denote multiset comprehension, for example if $y, z \in Var(t)$ are distinct variables, and $y\sigma = z\sigma$, then $y\sigma$ occurs twice in the multiset $[x\sigma.\ x \in Var(t)]$.

□

For the proof of completeness, we need some facts about »:

Lemma:

1. If S finally preserves R-normal forms, then » is a Noetherian ordering.
2. Let the term t be given, and let $t\mu\tau' = t\tau$. Then
   (1) $[x\tau.\ x \in Var(t)] \ |>_{mult} \ [x\tau'.\ x \in Var(t\mu)]$ or
   (2) $t\mu$ is a renaming of t.

Proof:

<u>1:</u>

The subterm ordering $|>$ is Noetherian, so the relation $|>_{mult}$ is Noetherian on finite multisets. If $t\sigma = t\sigma'$, then in particular $[x\sigma.\ x \in Var(t)] = [x\sigma'.\ x \in Var(t')]$. The relation $(\underset{R}{\rightarrow}^{+NF} / \underset{S}{\rightarrow})^+$ is Noetherian by the premise that S finally preserves R-normal forms. The relation $(\underset{R}{\rightarrow}^{+NF} / \underset{S}{\rightarrow})^+$ absorbs $(\underset{R}{\rightarrow}^{NF} \cup \underset{S}{\rightarrow})^*$. So the lexicographic combination » is Noetherian as well.

<u>2:</u>

Assume a term t' such that $y \in Var(t')$ holds. Then $t'\tau' |\geq y\tau'$ by definition of $|\geq$. Accordingly by definition of multiset extension, $[t'\tau'] \ |\geq_{mult} \ [y\tau'.\ y \in Var(t')]$ holds.

With $t' =_{def} x\mu$, $x\in Var(t)$, we get:

$[x\mu\tau'.\ x\in Var(t)]\ \ |\geq_{mult}\ \ [y\tau'.\ y\in Var(x\mu)\ \wedge\ x\in Var(t)]$,

which is equivalent to

$[x\tau.\ x\in Var(t)]\ \ |\geq_{mult}\ [y\tau'.\ y\in Var(t\mu)]$.

Finally we show that whenever $[x\tau.\ x\in Var(t)] = [y\tau'.\ y\in Var(t\mu)]$, then the term $t\mu$ is just a renaming of t. So assume that $[x\tau.\ x\in Var(t)] = [y\tau'.\ y\in Var(t\mu)]$, or equivalently, that $|\{x\in Var(t).\ x\tau = t_0\}| = |\{y\in Var(t\mu).\ x\tau' = t_0\}|$ holds for every term t_0. Observe that the set of nontrivial such t_0 is finite due to the finiteness of $Var(t)$. Choose a maximal nontrivial such t_0, i.e. if $t_0' \,|\!> t_0$ then $\{x\in Var(t).\ x\tau = t_0'\} = \emptyset$. By definition, there is a bijection from $\{y\in Var(t\mu).\ x\tau' = t_0\}$ to $\{x\in Var(t).\ x\tau = t_0\}$. This way the set can be exhausted, and the wanted bijection is the disjoint union of the assembled pieces.

□

Due to confluence of R∪S, we may continue with a normal form of g, and may be sure that from this normal form still a successful rewrite derivation exists. But that derivation may turn out longer than n. Now because of final normal form preservation, finally g must be a R-normal form itself. In that case, we can take the next step from the rewrite derivation for $g\tau \xrightarrow[R\cup S]{}^{n}$ true, so we decrease the length of the derivation by 1. This is the essential step. Let us now finish the proof:

Theorem:*(completeness of R-normal R∪S-paramodulation)*

If R∪S is confluent, R is normalizing, and S finally preserves R-normal forms, then R-normal R∪S-paramodulation is complete.

Proof:

Fix some arbitrary (need not be most general) solution τ of the goal g, that is, $g\tau \xrightarrow[R\cup S]{}^{n}$ true holds for some $n\in\mathbb{N}$. By induction on the triples (τ, g, n), using » as Noetherian relation, we are now able to prove that there is a normal paramodulation derivation $g \xrightarrow[R,R\cup S]{NP}{}_{\sigma}^{*}$ true where $\sigma \leq_{sub} \tau$.

Let $g_0 \in NF_R(g) \neq \emptyset$ be some arbitrary normal form of g. Note that in general, g_0 needs not be unique, for R is not necessarily confluent. Because R∪S is confluent, there is a derivation $g_0\tau \xrightarrow[R\cup S]{}^{m}$ true. If already $g\in NF_R(g)$, i.e. $g = g'$, then we may obviously take the given derivation of length n. (We will still need this fact below in case 2.2.1.) There are the cases:

<u>Case 1:</u> $g_0\tau$ = true.

Obvious.

Case 2: $g_0\tau \xrightarrow[R\cup S]{} \xrightarrow[R\cup S]{}^{m-1}$ true, $m > 0$.

By def. of paramodulation there are μ, τ', g', such that $g_0 \xrightarrow{P}_{R} {}_\mu\, g'$, $\mu\tau' = \tau$, and $g'\tau' \xrightarrow[R\cup S]{}^{*}$ true. A case analysis shows that in either of the following subcases, the inequation $(\tau, g, n) \gg (\tau', g', m)$ holds.

Case 2.1: $[x\tau.\ x\in Var(g)]\ |\!>_{mult}\ [x\tau'.\ x\in Var(g')]$.

τ and τ' differ by a strict instantiation.

Case 2.2: $[x\tau.\ x\in Var(g)] = [x\tau'.\ x\in Var(g')]$.

I.e. τ and τ' differ only by a bijective renaming. So the paramodulation step actually was a rewrite step: $g_0 \xrightarrow[R\cup S]{} g'$, $g'\tau \xrightarrow[R\cup S]{}^{*}$ true. Since g_0 was R-normal, even $g_0 \xrightarrow[S]{} g'$ holds.

Case 2.2.1: $g = g_0$.

Then using the paramodulation/rewrite step taken from the derivation of length n, $g \xrightarrow[S]{} g'$ and $n > n-1 = m-1$ hold.

Case 2.2.2: $g \neq g_0$.

Then $g\ (\xrightarrow[R]{}^{+NF} / \xrightarrow[S]{})^{+}\ g'$ holds.

In all subcases (2.1, 2.2.1, and 2.2.2) the inequation $(\tau, g, n) \gg (\tau', g', m)$ holds, which justifies the inductive hypothesis for $g'\tau' \xrightarrow[R\cup S]{}^{m}$ true. We may so continue with case 2 in general. The inductive hypothesis supplies a normal paramodulation derivation $g' \xrightarrow{NP}_{R,R\cup S} {}_{\sigma'}^{*}$ true, where $g'\sigma' \leq_{sub} g'\tau'$ holds. The substitution σ' can be chosen such that $g\mu\sigma' \leq_{sub} g\mu\tau'$ holds. Thus there is a substitution $\sigma =_{def} \mu\sigma'$ together with the step $g \xrightarrow[R]{}^{NF} g_0 \xrightarrow{NP}_{R,R\cup S} {}_{\mu}\, g'$ which completes the desired normal paramodulation derivation $g \xrightarrow{NP}_{R,R\cup S} {}_{\sigma}^{*}$ true.

□

For normal narrowing, there is a corresponding result. Normal solutions are approximated by normal substitutions only, and for normal substitutions, narrowing and paramodulation steps coincide (this concerns case 2 in the above proof). So we have:

Corollary: *(completeness of R-normal R∪S-narrowing)*

If R∪S is confluent, R is normalizing, and S finally preserves R-normal forms, then R-normal R∪S-narrowing is complete for normal solutions.

□

The following example demonstrates the strength of the theorem:

Example:

Let $R =_{def} \{a(x) \to b(x),\ b(x) \to c(x),\ eq(x, x) \to true\}$,

$S =_{def} \{b(x) \to a(x),\ c(s(x)) \to a(x)\}$, and

$g =_{def} eq(c(n), c(0))$.

R/S is not Noetherian because of the cycle $a(x) \xrightarrow[R]{} b(x) \xrightarrow[S]{} a(x)$. But R´/S is Noetherian, where $R' =_{def} \{a(x) \to c(x),\ b(x) \to c(x)\}$. Therefore, particularly, $\xrightarrow[R]{}^{+NF} / \xrightarrow[S]{}$ is

Noetherian, and by $\underset{R}{\rightarrow}^{+NF} = \underset{R}{\rightarrow}^{+NF}$, also $\underset{R}{\rightarrow}^{+NF} / \underset{S}{\rightarrow}$ is Noetherian . So R-normal R∪S-narrowing is complete.

Normal narrowing derivations are of the form

$$\begin{array}{llllll}
eq(c(n), c(0)) & \underset{R}{\rightarrow}^{NF} & eq(c(n), c(0)) & \underset{S}{\overset{N}{\longrightarrow}}_{[s(n_1) / n]} & & \\
eq(a(n_1), c(0)) & \underset{R}{\rightarrow}^{NF} & eq(c(n_1), c(0)) & \underset{S}{\overset{N}{\longrightarrow}}_{[s(n_2) / n_1]} & & \\
\ldots & & & & & \\
eq(a(n_k), c(0)) & \underset{R}{\rightarrow}^{NF} & eq(c(n_k), c(0)) & \underset{R}{\overset{N}{\longrightarrow}}_{[0 / n_k]} & true, &
\end{array}$$

which deliver the full set of solutions $\{[s^k(0) / n].\ k \in \mathbb{N}\}$. Note that the R-normal forms $c(s^k(0))$ are destroyed k times during the rewrite process; this indicates that normal forms are not preserved at once, but finally.

□

Summary

The property of *relative termination*, invented by [Bachmair, Dershowitz 86] and independently by [Klop 87], is the topic of this thesis. Relative termination to a rewrite system is a straightforward generalization of *termination* as well as of *termination modulo* an equational theory. The generalization is *strict*, as is proven by an example (section 2.6) that is relatively Noetherian, but neither Noetherian nor Noetherian modulo. Necessary syntactic conditions for relative termination are stated (section 2.2). It is shown that existing techniques and methods to prove termination and termination modulo basically can be reused to prove relative termination (section 2.3). This holds in particular for the lexicographic recursive path ordering and for polynomial interpretations. The question, whether there is a general characterization of relative termination by means of a *termination quasiordering*, is still open. But it is shown that, provided that the acyclic part of the binary relation S is Noetherian (as is the case with termination modulo), then relative termination to S is characterized by means of a termination quasiordering.

Relative termination is investigated in connection with finitely branching relations (section 2.4), among other things with the *quasi-termination* property. Quasi-termination and relative termination are similar notions. Another notion which is similar to relative termination, is *final preservation of normal forms* (treated in section 5.4). These notions arise quite naturally with considerations on relative termination.

The question, when termination of both R and S allows to infer the termination of $R \cup S$, in other words, when $R \cup S$ *inherits termination*, is of basic importance for composed rewrite systems. In the case of *direct sums*, i.e. disjoint sets of function symbols occurring in R and S, there exist strong results for inheritance of confluence ([Toyama 87b]) and termination ([Toyama et al. 89]). As a consequence of the infinite version of Ramsey´s theorem, another sufficient condition for inheritance is given by *transitivity* of $R \cup S$ (section 3.1). An application of this result is the *inheritance of relative termination*. The method to prove termination by the *lexicographic combination* of Noetherian orderings is discovered to mimic precisely inheritance of relative termination (section 3.2).

Path orderings show their weakness when applied to prove termination modulo, and so do they for relative termination. On this account, commutation criteria along [Bachmair, Dershowitz 86] are valuable, since they allow to infer relative termination from termination. The commutation approach is attacked in a fairly general form, such that both the approaches of *quasi-commutation* and *cooperation* can be described as special cases (sections 3.3, 3.4, and 3.5). The value of the general form is demonstrated by an example proof that would not work in the present special cases (section 3.4). Proofs of relative termination are also suitable to prove termination of certain rewrite systems. This

is the basis of the *transformation ordering* proof method. As is known, some self-embedding rewrite systems can be shown terminating by transformation.

In the second part of this thesis, applications of relative termination are investigated, other than termination proofs again. In chapter 4, new *confluence criteria* based on relative termination are worked out. Section 4.1 introduces and motivates a property that matches *coherence* in the confluence modulo approach. For symmetric S, indeed a substantial part of the "confluence modulo" approach ([Jouannaud, Kirchner 86]) is covered. The last one of these confluence criteria (section 4.4) reformulates and generalizes a confluence result of [Klop 87], and generalizes moreover the two classical approaches of [Knuth, Bendix 70] (local confluence of critical pairs) and [Huet 80] (strong confluence for linear rewrite systems).

Chapter 5 finally presents two new results about narrowing with intermediate rewriting ("*reduced narrowing*") and narrowing with intermediate normalization ("*normal narrowing*"), where besides the rewrite system R, used for reduction, normalization, respectively, there may still be other rules S. Reduced narrowing is shown complete when R is relatively Noetherian to S (section 5.2), and normal narrowing is shown complete when R is normalizing and S finally preserves R-normal forms (section 5.3). Both results generalize the classical result about normal narrowing of [Fay 79]. A previous conjecture of [Hußmann 85] which dispenses with final normal form preservation, is shown wrong by a counterexample. The mistake is located and carefully analyzed.

Apart from these main results, the thesis contains a number of small novelties. The well known lexicographic path ordering is defined by means of a rewrite system with *one* hidden function (section 2.3). A dependency graph of commutation-like properties is drawn (section 3.3). A *general critical pair criterion* is stated which assembles all syntactic premises once and for all (section 3.6).

Altogether, it may be stated that the *equational rewriting approach* can be extended to what might be called a "*reductional rewriting approach*", by simply dropping a symmetry condition, and by dropping syntactic restrictions usually put on rewrite systems.

Extensions or: What has not been treated

Relative termination is just one of a number of possible generalizations of termination, and many rewrite systems are *not* relatively Noetherian, for example rewrite systems for while loops. Some terms can be normalized, though, applying a certain rewrite strategy. Rewrite strategies, however, have not been considered in this thesis.

Some known termination orderings, like the *Knuth-Bendix ordering* ([Knuth, Bendix 70]) or the *semantic path ordering* ([Kamin, Lévy 80]), as well as recent improvements in path and *decomposition orderings* ([Rusinowitch 87b]), had to be neglected for space reasons. (Interestingly though, transformation techniques can still handle some crucial examples of improved path orderings.)

Many of the criteria presented in this thesis may be seen as correctness proofs of *methods* to prove termination, confluence, etc., which still may be prepared to software tools. Since concrete software was not an aim of this thesis, this work is left for the interested reader and software developer.

A very promising method for "automated" inductive proving, the "*proof by consistency*" method ([Musser 80], [Huet, Hullot 82], [Jouannaud, Kounalis 86], [Kapur, Musser 87]), may also be extended towards relative termination, the guideline being that strictorderings of the form $(R/S)^+$ serve as inductive orderings. Many of the proofs (of commutation and confluence properties) in this thesis are not far from being formalized on that account. The details, of course, still have to be worked out. It may be expected that the equational approach ([Bachmair 88]) again becomes a special case.

The confluence criteria in chapter 4 are far from being exhaustive. The "*congruence class approach*" of [Peterson, Stickel 81] and [Jouannaud 83] shows a way to scrap the left-linearity restriction. It can be carried over also to "descendants classes" of arbitrary rewrite systems S. Applying Jouannaud´s technique, a rewrite system R´ satisfying $R \subseteq R' \subseteq R/S$ is introduced. Such a starting point can still be found in the lemmas in chapter 4. But the further development towards critical pair criteria would burst this dissertation. In order to deal with them, one needs a couple of notions such as "class rewrite relation", "S-unifier" and "S-critical pair", generalized to arbitrary rewrite systems S, rather than symmetric ones. Furthermore an unsymmetric unification algorithm, and software support in computing examples, must still be made available:

> *The theory of equational term rewriting systems presented here lacks many examples. We apologize for this drawback and explain the reason: interesting examples are simply intractable by hand. Only computer experiments can provide such examples.*
> (conclusion in [Jouannaud, Kirchner 86])

References

The following abbreviations are used:

Proc. Proceedings, Intl. International, Conf. Conference, J. Journal, Vol. Volume, No. Number, pp. pages, LNCS Springer Lecture Notes in Computer Science

[Avenhaus, Madlener 90]

J. Avenhaus, K. Madlener: Term rewriting and equational reasoning. To appear in: R. B. Banerji (ed.): *Formal Techniques in Artificial Intelligence: A source-book*. Elsevier Science publishers B. V., Amsterdam, 1990.

[Bachmair 88]

L. Bachmair: Proof by consistency in equational theories. In: *Proc. Logic in Computer Science*, 1988, pp. 228-233.

[Bachmair, Dershowitz 86]

L. Bachmair, N. Dershowitz: Commutation, transformation, and termination. In: *Proc. 8th Conf. on Automated Deduction*, Oxford 1986, LNCS 230, pp. 5-20.

[Bachmair, Plaisted 85]

L. Bachmair, D. A. Plaisted: Termination orderings for associative-commutative rewriting systems. In: *J. of Symbolic Computation* (1985) 1, pp. 329-349.

[Bellegarde 86]

Rewriting systems on FP-expressions to reduce the number of sequences yielded. In: *Science of Computer Programming* 6 (1986), pp. 11-34.

[Bellegarde, Lescanne 86]

F. Bellegarde, P. Lescanne: Termination Proofs based on Transformation Techniques. Manuscript CRIN 86-R-034, 1986, to be published.

[Bellegarde, Lescanne 87]

F. Bellegarde, P. Lescanne: Transformation ordering. In: *Proc. 12th Colloquium on Trees in Algebra and Programming*, Pisa 1987, LNCS 249, pp. 69-80.

[Ben-Cherifa, Lescanne 86]

Termination of rewriting Systems by polynomial interpretation and its implementation. In: *Proc. 8th Conference on Automated Deduction*, 1986, LNCS 230, pp. 42-51. Also in: Science of Computer Programming 9 (1987), pp. 137-159.

[Bockmayr 86]

A. Bockmayr: *Narrowing with inductively defined functions*. SEKI memo 25/86, Universität Kaiserslautern, 1986.

[Bockmayr 88]

A. Bockmayr: Narrowing with built-in theories. In: *Proc. Intl. Workshop on Algebraic and Logic Programming*, Dresden, Mathematical Research 49, Akademie Verlag, Leipzig, 1988, pp. 83-92. Also in LNCS 343.

[Book et al. 81]

R.V. Book, M. Jantzen, C. Wrathan: Monadic Thue systems. In: *Theoretical Computer Science*, Vol. 19, No. 3, 1981, pp. 231-251.

[Church, Rosser 36]

A. Church, J. B. Rosser: Some properties of conversion. In: *Transactions of the American Mathematical Society* 39, pp. 472-482, 1936.

[Dauchet 88]

M. Dauchet: Termination of rewriting is undecidable in the one-rule case. In: *Proc. Mathematical Foundations of Computer Science* 88, Karlsbad, LNCS 324.

[Dauchet et al. 87]

M. Dauchet, T. Heuillard, P. Lescanne, S. Tyson: Decidability of confluence of ground term rewriting systems. In: *Proc. of the 2nd Symposium on Logic in Computer Science*. Ithaca, New York, June 1987.

[Davis 73]

M. Davis: Hilbert´s 10th Problem is unsolvable. In: *American Mathematic Monthly* 80, 3 (March 1973), pp. 233-269.

[Dershowitz 79]

N. Dershowitz: A note on simplification orderings. In: *Information Processing Letters* Vol. 9, No. 5, 1979, pp. 212-215.

[Dershowitz 81]

N. Dershowitz: Termination of linear term rewriting systems. In: *Proc. 8th Intl. Conf. on Automata, Languages, and Programming*, LNCS 115, pp. 448-458.

[Dershowitz 82]

N. Dershowitz: Orderings for term rewriting systems. In: *Theoretical Computer Science* Vol. 17, No. 3, March 1982, pp. 448-458.

[Dershowitz 85]

N. Dershowitz: Termination. In: *Proc. 1st Intl. Conf. on Rewriting Techniques and Applications*, Dijon, May 1985, LNCS 202, pp. 180-224.

[Dershowitz 87]

N. Dershowitz: Termination of rewriting. In: *J. of Symbolic Computation* (1987) 3, pp. 69-116.

[Dershowitz et al. 83]

N. Dershowitz, J. Hsiang, N. A. Josephson, D. A. Plaisted: Associative-commutative rewriting. In: *Proc. 8th Intl. Joint Conf. on Artificial Intelligence*, Karlsruhe, Aug. 1983, pp. 940-944.

[Dershowitz, Manna 79]

N. Dershowitz, Z. Manna: Proving termination with multiset orderings. *Communications of the ACM* 22, pp. 465-476. Also in: Proc. Intl. Conf. on Automata, Languages, and Programming, Graz, July 1979, pp. 188-202.

[Dershowitz, Jouannaud 89]

N. Dershowitz, J.-P. Jouannaud: Rewriting systems. In: *Handbook of Theoretical Computer Science*, North-Holland, 1989.

[Detlefs, Forgaard 85]

D. Detlefs, R. Forgaard: A procedure for automatically proving the termination of a set of rewrite rules. In: *Proc. 1st Intl. Conf. on Rewriting Techniques and Applications*, Dijon, May 1985, LNCS 202, pp. 255-270.

[Drosten 89]

K. Drosten: *Termersetzungssysteme, Grundlagen der Prototyp-Generierung algebraischer Spezifikationen*. Informatik-Fachberichte 210, Springer, Feb. 1989.

[Echahed 88]

R. Echahed: On completeness of narrowing strategies. In: *Proc. Intl. Colloquium on Trees in Algebra and Programming*, 1988, LNCS 299, pp. 89-101.

[Fages, Huet 83]

F. Fages, G. Huet: Complete sets of unifiers and matchers in equational theories. In: *Proc. Colloquium on Trees in Algebra and Programming*, 1983, LNCS 159, pp. 205-220.

[Fay 79]

M. Fay: First order unification in an equational theory. In: W. H. Joyner (ed.), *Proc. 4th Workshop on Automated Deduction*, Academic Press 1979.

[Fribourg 84]

L. Fribourg: A Narrowing Procedure for Theories with Constructors. In: *Proc. 7th Conf. on Automated Deduction*, May 1984, LNCS 170, pp. 259-281.

[Furbach et al. 89]

U. Furbach, S. Hölldobler, J. Schreiber: Horn equality theories and paramodulation. In: *J. of Automated Reasoning*, Vol. 5, No. 3, Sept. 1989, pp. 309-338.

[Ganzinger, Giegerich 87]

H. Ganzinger, R. Giegerich: A note on termination in combinations of heterogeneous term rewriting systems. In: *Bulletin EATCS* No. 31, Feb. 1987, pp. 22-28.

[Geser, Hußmann 86]

A. Geser, H. Hußmann: Experiences with the RAP system — a specification interpreter combining term rewriting and resolution. In: *Proc. 1st European Symposium on Programming*, March 1986, LNCS 213, pp. 339-350.

[Gnaedig 87]

I. Gnaedig: *Investigations on termination of equational rewriting*. Report INRIA, Le Chesnay, 1987.

[Gnaedig, Lescanne 86]

I. Gnaedig, P. Lescanne: Proving termination of associative rewriting system by rewriting. In: *Proc. 8th Conf. on Automated Deduction*, Oxford, LNCS 230, 1986, pp. 52-61.

[Guttag et al. 83]

J. V. Guttag, D. Kapur, D. R. Musser: On proving uniform termination and restricted termination of rewriting systems. In: *SIAM J. on Computing*, Vol. 12, No. 1, Feb. 1983, pp. 189-214.

[Hammes 86]

D. Hammes: *Gleichheit in PROLOG: Ein Fallbeispiel*. Arbeitspapiere der GMD, Vol. 228, St. Augustin, Oct. 1986.

[Herbrand 30]

J. Herbrand: *Recherches sur la théorie de la démonstration*. Thèse, Université de Paris, 1930. In: Ecrits logiques de Jacques Herbrand, PUF Paris 1968.

[Hindley 64]

R. Hindley: An abstract Church-Rosser theorem. Part 1 in *J. of Symbolic Logic* 34 (1969), pp. 545-560; part 2 in *J. of Symbolic Logic* 39 (1974), pp. 1-21.

[Hofbauer, Kutsche 89]

D. Hofbauer, R.-D. Kutsche: *Grundlagen des maschinellen Beweisens*. Vieweg Verlag, 1989.

[Hölldobler 89]

S. Hölldobler: *Foundations of equational logic programming*. LNCS subseries Lecture Notes in Artificial Intelligence 353, 1989.

[Huet 80]

G. Huet: Confluent reductions: Abstract properties and applications to term rewriting systems. In: *J. of the ACM* Vol. 27, No. 4, Oct. 1980, pp. 797-821.

[Huet, Hullot 82]

Proofs by induction in equational theories with constructors. In: *J. of Computer and System Sciences* 25, 1982, pp. 239-266.

[Huet, Lankford 78]

G. Huet, D. S. Lankford: *On the uniform halting problem for term rewrite systems*. Report 283, INRIA, Le Chesnay, 1978.

[Huet, Oppen 80]

G. Huet, D. C. Oppen: Equations and rewrite rules — A survey. In: R. Book (ed.): *Formal Language Theory - Perspective and Open Problems*, Academic Press (1980).

[Hußmann 85]

H. Hußmann: *Unification in conditional-equational theories*. Report MIP-8502, Universität Passau, 1985. Short version also in: *Proc. European Conference in Computer Algebra* 85, Vol. 2, LNCS 204 (1985), pp. 543-553.

[Hußmann 85/87]

H. Hußmann: *Rapid prototyping for algebraic specifications — RAP system user´s manual*. Report MIP-8504, Universität Passau, 1985. Revised version 1987.

[Hußmann 89]

H. Hußmann: *Nichtdeterministische algebraische Spezifikationen*. Dissertation, Universität Passau, 1989.

[Jouannaud 83]

J.-P. Jouannaud: Confluent and coherent equational term rewrite systems. Applications to proofs in data types. In: *Proc. Colloquium on Trees in Algebra and Programming* 83, LNCS 159, pp. 269-283.

[Jouannaud, Kirchner 86]

J.-P. Jouannaud, H. Kirchner: Completion of a set of rules modulo a set of equations. In: *SIAM J. on Computing* 15, 1986, pp. 1155-1194.

[Jouannaud, Kounalis 86]

J.-P. Jouannaud, E. Kounalis: Automatic proofs by induction in theories without constructors. In: *Proc. 1st Logic in Computer Science*, June 1986, pp. 358-366. Also in: Information and Copmputation, Vol. 8, No. 4, July 1989.

[Jouannaud, Lescanne 86]

J.-P. Jouannaud, P. Lescanne: La Réécriture — Term rewriting. In: *Technique et Sciences Informatiques*, 5(6), 1986, pp. 433-452.

[Jouannaud, Muñoz 84]

J.-P. Jouannaud, M. Muñoz: Termination of a set of rules modulo a set of equations. In: *Proc. 7th Conf. on Automated Deduction*, LNCS 170, 1984, pp. 175-193.

[Kamin, Lévy 80]

S. Kamin, J.-J. Lévy: *Attempts to generalize the recursive path ordering*. Unpublished note, Dept. of computer science, University of Illinois, Urbana, 1980.

[Kapur et al. 85]

D. Kapur, P. Narendran, G. Sivakumar: A path ordering for proving termination of term rewriting systems. In: *Proc. 10th Colloquium on Trees in Algebra and Programming*, LNCS 185, pp. 73-185.

[Kapur et al. 87]

D. Kapur, P. Narendran, H. Zhang: On sufficient completeness and related properties of term rewriting systems. In: *Acta Informatica* 24 (4), Aug. 1987, pp. 395-415.

[Klop 87]

J. W. Klop: Term rewriting systems: A tutorial. In: *Bulletin of the EATCS*, Vol. 32, June 1987, pp. 143-183.

[Knuth, Bendix 70]

D. E. Knuth, P. B. Bendix: Simple word problems in universal algebras. In: J. Leech (ed.): *Computational Problems in Abstract Algebras*, Pergamon Press, 1970, pp. 263-297.

[Lankford 75]

D. Lankford: *Canonical inference*. Report Atp-25, Automated Theorem Proving Project, University of Texas at Austin, May 1975.

[Lankford 79]

D. Lankford: *On proving term rewrite systems are Noetherian*. Report Mtp-3, Mathematics Dept., Louisiana Technical University, 1979.

[Lankford, Ballantyne 77]

D. S. Lankford, A. M. Ballantyne: *Decision procedures for simple equational theories with permutative axioms: Complete sets of permutative reductions*. Report Atp-37, Mathematics Dept., Univ. of Texas at Austin, April 1977.

[Manna, Ness 70]

Z. Manna, S. Ness: On the termination of Markov algorithms. In: *Proc. of the 3rd Hawaii Intl. Conf. on System Science*, Honolulu, Hawaii, 1970, pp. 789-792.

[Middeldorp 89]

A. Middeldorp: A suffiecient condition for the termination of the direct sum of term rewriting systems. In: *Proc. 4th IEEE symposium on Logic in Computer Science*, Asilomar, 1989.

[Newman 42]

M. H. A. Newman: On theories with a combinatorial definition of "equivalence". In: *Annals of Mathematics* 43, 1942, pp. 223-243.

[Nipkow, Weikum 83]

T. Nipkow, G. Weikum: A decidability result about sufficient completeness of axiomatically specified abstract data types. In: *6th GI Conf. on Theoretical Computer Science*, Jan. 1983, LNCS 145.

[Nutt et al. 87]

W. Nutt, P. Réty, G. Smolka: *Basic narrowing revisited*. SEKI-Report SR87-07, Univ. Kaiserslautern, 1987.

[O´Donnell 77]

M. O´Donnell: *Computing in systems described by equations*. LNCS 58, 1977.

[Oyamaguchi 87]

M. Oyamaguchi: The Church-Rosser property for ground term rewriting systems is decidable. In: *Theoretical Computer Science*, Vol. 49, No.1, 1987.

[Padawitz 87]

P. Padawitz: Strategy controlled reduction and narrowing. In: *Proc. 2nd Conf. on Rewriting Techniques and Applications* 87, LNCS 256, pp. 242-255.

[Padawitz 88]

P. Padawitz: *Computing in Horn clause theories*. EATCS Monographs on Theoretical Computer Science, Vol. 16, Aug. 1988.

[Peterson, Stickel 81]

G. E. Peterson, M. E. Stickel: Complete sets of reductions for some equational theories. In: *J. of the ACM*, Vol. 28, No. 2, April 1981, pp. 233-264.

[Plaisted 83]

D. Plaisted: *An associative path ordering*. Report University of Illinois, Computer science dept., 1983.

[Porat, Francez 86]

S. Porat, N. Francez: Full-commutation and fair-termination in equational (and combined) term-rewriting systems. In: *Proc. 8th Conf. on Automated Deduction*, July 1986, LNCS 230, pp. 21-41.

[Raoult, Vuillemin 80]

J. C. Raoult, J. Vuillemin: Operational and semantic equivalence between recursive programs. In: *J. of the ACM* 27, 1980, pp. 772-796.

[Réty 87]

P. Réty: Improved basic narrowing. In: *Proc. 2nd Conf. on Rewriting Techniques and Applications*, Bordeaux, LNCS 256, May 1987.

[Robinson, Wos 69]

G. A. Robinson, L. Wos: Paramodulation and theorem proving in first order theories with equality. In: *Machine Intelligence* 4, 1969.

[Rosen 73]

B. K. Rosen: Tree manipulation systems and Church-Rosser theorems. In: *J. of the ACM*, Vol. 20, No. 1, 1973, pp. 160-187.

[Rusinowitch 87a]

M. Rusinowitch: On termination of the direct sum of term-rewriting systems. In: *Information Processing Letters* 26, 1987/88, pp. 65-70.

[Rusinowitch 87b]

M. Rusinowitch: Path of subterm ordering and recursive decomposition ordering revisited. In: *J. of Symbolic Computation*, No. 3, Vol. 1&2, Oct. 1987, pp. 117-132.

[Staples 75]

J. Staples: Church-Rosser theorems for replacement systems. In: J. Crosley (ed.), *Algebra and Logic*, Lecture Notes in Mathematics 450, 1975, pp. 291-307.

[Steinbach 88]

J. Steinbach: Extensions and comparisons of simplification orderings. In: *Proc. 3rd Intl. Conf. on Rewriting Techniques and Applications*, 1989, LNCS 355, pp. 434-448.

[Toyama 87a]

Counterexamples to termination for the direct sum of term rewriting systems. In: *Information Processing Letters* 25, 1987, pp. 141-143.

[Toyama 87b]

Y. Toyama: On the Church-Rosser property for the direct sum of term rewriting systems. In: *J. of the ACM*, Vol. 34, No. 1, 1987, pp. 128-143.

[Toyama 88]

Commutativity of term rewriting systems. In: *Programming of future generation computers II*, Amsterdam, North Holland, 1988, pp. 393-407.

[Toyama et al. 89]

Y. Toyama, J. W. Klop, H. P. Barendregt: Termination for the direct sum of left-linear term rewriting systems (Preliminary version). In: *Proc. 3rd Intl. Conf. on Rewriting Techniques and Applications*, 1989, LNCS 355, pp. 477-491.

[Wirsing et al. 83]

M. Wirsing, P. Pepper, H. Partsch, W. Dosch, M. Broy: On hierarchies of abstract data types. In: *Acta Informatica* 20, 1983, pp. 1-33.

[Wirsing 90]

M. Wirsing: Algebraic specification: Semantics, parameterization, and refinement. In: *Handbook of Theoretical Computer Science*, North-Holland, 1990.

Index

acyclic 8
approximation 85
arity 8
arrow 7
associative 36
associative path ordering 36
auxiliary function symbol 52
binary numbers 51
binary relation
    abstract binary relation 12
cake diagrams 33
cardinality 32
Church-Rosser property 59; 76
class approach 65
class rewrite relation 64
closed
    under contexts 11
    under instantiation 11
    under subsets 16
closure
    reflexive 7
    reflexive-transitive 7
    symmetric 7
    transitive 7
    under substitution 11
coherence 63
coherent 63
collapse-free 12
commutation 36; 37
complete 78
completeness 85
    of narrowing 79
    of paramodulation 79
    of R-normal R∪S-paramodulation 87
    of R-normal R∪S-narrowing 88
    of R-reduced R∪S-narrowing 83

of R-reduced R∪S-paramodulation 83
composition
of relations 7
of substitutions 10
confluence 39
confluent 7; 59; 76
congruence class approach 64
congruence closure 11
constants 8
conversion 51
cooperation 40
counterexample 62
covered 78
critical pair 43
critical pair criterion 46
critical pair lemma 46
critical pair scheme 44
cyclic 8
decidable 59
diagram 7
local 12
direct sum 31; 59; 74
domain
of a substitution 10
E-Church-Rosser property 60
E-confluence 60
encoding 76
encoding convention 76
endomorphism 10
equality 9
equational rewriting 13
example
Associativity and Endomorphism 36; 50
conversion into binary numbers 51
Ex. 54
Ex. 18 34
Ex. 27 48; 53
Ex. 3 35

FF 23; 27; 29; 56; 74
INT2 35; 55
Maps 56
Nonfin 25; 54; 68
Queues 2; 3
Set 15; 17; 25; 28; 29
Stack of N 56
F-stability 11
fairness 81
finally preserves R-normal forms 84
finitely branching 8
first confluence criterion 68
first local cooperation criterion 47
first localization 61
full localization 71
function symbol 8
general critical pair scheme 45
general duality 13
generalized lexicographic path ordering 22
ground 9
hidden function 20
hierarchical 57
homeomorphic self-embedding 23
homomorphic interpretation ordering 20
idempotent 10
incremental 35
inheritance of relative termination 32
instance 10
join 60
Knuth-Bendix ordering 23
Kruskal´s tree theorem 20
left-commutativity 15
left-dominance 28
left-erasing 12
left-idempotence 15
left-linear 11
left-non-annihilating 12
left-nonerasing 11
left-nonisolating 11

left-nonlinear 12
left-to-right 21
lexicographic combination 34
    of termination orderings 34
lexicographic path ordering 20
lexicographic status 21
lifting lemma 77
local 12
local commutation 37
local cooperation 41
localization 12
localize 12
locally S-coherent 65
looping 17
marker symbol 21
monotonicity 11
more general than 10
more special than 10
multiset 86
multiset extension 86
multiset status 21
narrowing optimizations 79
narrowing step 77
Nash-Williams proof 31
necessary condition 18
Noetherian 8
Noetherian ordering 19
Noetherian quasiordering 20
non-collapsing 12
non-splitting 70
nondeterministic 21
normal
    object 8
    substitution 78
normal form 8
normal form preservation 85
normal paramodulation step 80
normalization 8
normalizing 8

occurrence 9
functional 10
opposite term rewrite system 13
ordering 8
oriented paramodulation 75
overlap 43
paramodulation 75
paramodulation step 77
path ordering 20
permutation 21
polynomial interpretation 23
polynomial interpretation ordering 20
precedence 21
prefix ordering 10
prefixed rule 78
preserves R-normal forms 84
primitive rewrite system 65
primitive specification 56
quasi-commutation 37; 43
quasi-commutation criterion 55
quasi-commutation lemma 39
quasiordering 8
quasiordering lemma 24
quasiordering supplement 26
R-derivation 8
Ramsey´s theorem 31
range
of a substitution 10
recursive path ordering 20
with status 22
redex 11
redex occurrence 11
reduced paramodulation 82
reduction ordering 19
regular 12
relation 7
relative termination 14; 90
relative to 15
relatively Noetherian 14

relatively Noetherian to 14
renaming 10; 85
replacement 9
reuse of a proof 64
rewrite redex 85
rewrite relation 11
rewrite rule 11
rewrite system 11
right-distributive law 29
right-linear 12
right-nonduplicating 18
right-to-left 21
rule 11
S-coherent 63
second confluence criterion 73
second local cooperation criterion 49
second localization 63
self-embedding 23; 50
semantic path ordering 23
simplification ordering 20
splitting effect 69
stability 11
strict commutation 37
strict local commutation 37
strict superterm 86
strictordering 8
strong commutation 37
strong confluence 59
strong cooperation 42
strong cooperation criterion 54
strongly S-coherent 70
substitution 10
subsumption 10
subterm 9
subterm ordering 20; 86
symmetric rewrite system 13
syntactic restrictions 47
term algebra 8
term rewrite system 11

termination inheritance 31
  by transitivity 31
termination ordering 19
termination quasiordering 20
termination quasiordering criterion 24
terms 8
third localization 65
Thue system 23
top symbol 9
transformation ordering 50
transformer system 52
two orderings 26
undecidable 20; 59
unification procedure 78
unifier 43; 75
  computed 78
variable 8
well-founded ordering 19
well-quasiordering 20

Glossary

(Symbols and formulas are explained in the order, they appear in the text for the first time.)

l ’ r equation specification

$l \rightarrow r$ rewrite rule

F_P set of function symbols in the rewrite system P

R/S R relative to S

$\mathbb{N}$ set of natural numbers

$\geq_{\mathbb{N}}$ natural ordering ... $\geq_{\mathbb{N}} 3 \geq_{\mathbb{N}} 2 \geq_{\mathbb{N}} 1 \geq_{\mathbb{N}} 0$

RS composition of binary relations R and S

R^{-1} inverse of R

$\overline{R}$ symmetric closure of R

R^{ε} reflexive closure of R

R^{+} transitive closure of R

R^{*} reflexive-transitive closure of R

$\{t'.\ (t, t') \in R\}$

set comprehension: The set of all those t' which satisfy that t and t' are related by R

NF_R set of all R-normal forms

$NF_R(t)$ set of all R-normal forms of t

R^{NF} R-normalization relation

$\leq$ and $\geq$ quasiorderings

$<$ and $>$ strictorderings, associated to the quasiordering $\leq, \geq$, respectively

« and **»** other strictorderings

~ the equivalence relation associated to the quasiordering $\geq$

$$\bigcup_{f \in F} (\{f\} \times Term^{arity(f)})$$

(disjoint) union of all cartesian products between the singleton set $\{f\}$ and the n-th power of the set Term, where $n = arity(f)$

$(f, t_1, ..., t_n)$ (n+1)-tuple, consisting of the symbol f and the terms $t_1, ..., t_n$.

x+y may also denote the term +(x, y)

-x may also denote the term -(x)

$t =_{def} f(g(x, a), y)$ t will be used to denote the term ...

eq(t,t´) a goal that asks for solutions of " t equals t´ "

$=_R$ semantic equality defined by the rewrite system R

$\wp(X)$ powerset of X

Var(t) set of (free) variables in t

Func(t) set of function symbols in t

Ø empty set

λ empty occurrence

i.u composed occurrence

t/u subterm of t at occurrence u

t [u ← t´] replacement of the subterm of t at occurrence u by the new subterm t´

$\mathbb{N}^*$ set of sequences of natural numbers

Occ(t) set of occurrencves of t

FOcc(t) set of functional occurrences of t

$\leq_{pre}$ prefix ordering on occurrences

σ and τ substitutions

$[t_1/x_1,\ t_2/x_2,\ \dots\ ]$ the substitution that maps x_1 to t_1, etc.

ω least transfinite ordinal number

$t\sigma$ the instance of the term t under substitution σ

$\sigma\tau$ (diagrammatical) composition of substitutions σ and τ

$\geq_{sub}$ subsumption quasiordering on substitutions

dom σ domain of substitution σ

ran σ range of substitution σ

$\xrightarrow[R]{}$ rewrite relation generated by the rewrite system R

$t \xrightarrow[l \to r]{u} t'$

a rewrite step takes place in t at occurrence u, using the rewrite rule $l \to r$, yielding the term t´

$t_1 \xrightarrow[R \cup S]{} t_2 \xrightarrow[R \cup S]{} \dots$ an infinite $\xrightarrow[R \cup S]{}$-derivation

$(f(x) \to f(y)) \in S$ the rewrite system S contains a rule $f(x) \to f(y)$

$S = \{x \to x\}$ S denotes a rewrite system that consists of the single rule $x \to x$

$|\!\geq$ subterm quasiordering

$|\!>$ subterm strictordering

$\pi(t_1,\ \dots,\ t_n)$ application of a permutation π to a sequence of terms

***** also used as the marker symbol

$>_{rpo}$ lexicographic path (strict)ordering

$\geq_{rpo}$ lexicographic path (quasi)ordering

[_] a function in mixfix notation; "_" indicates the parameter position

$\mathbb{N}(X)$ set of polynomials in variables from X with coefficients from $\mathbb{N}$

[t] the polynomial interpretation of the term t

#t number of "ff patterns" in the term t

≥» the relational composition of ≥ and »

$\mathbb{Q}^+$ the set of positive rational numbers

$S \setminus (S^{-1})^*$ the S relation without those pairs that are part of a cycle

S^n the n-th power of S, i.e. S...S n times

$\xrightarrow[Q]{}^{m}\ t\ \xrightarrow[S]{}^{n}$

a diagram instance where the number of $\xrightarrow[Q]{}$-steps may be assumed m, and likewise the number of $\xrightarrow[S]{}$-steps may be taken as n. The term between the two derivations is called t later on.

CP(R, S) the set of all critical pairs of rules from R with rules from S

$t \xleftarrow[S]{v} \xrightarrow[R]{u} t'$

from a term that is not named, there is both a rewrite step at occurrence v using a rule from S, yielding the term t, and another rewrite step at occurrence u using a rule from R, yielding the term t´

$Q \subseteq {}^{*}\!\xleftarrow[S]{}$ every rule in Q can be bridged by a sequence of S-rewrite steps in reversed order

$\mathbb{Z}$ the set of integer numbers 0, 1, -1, ...

$t \xrightarrow[l \to r]{P\ u}_{\sigma} t'$

the term t admits a paramodulation step at occurrence u using the rule $l \to r$. This paramodulation step uniquely defines the substitution σ and the term t´.

$t \xrightarrow[l \to r]{N\ u}_{\sigma} t'$ narrowing step, i.e. a paramodulation step where $u \in FOcc(t)$ holds

$s^{i}(0)$ s(s(...(0)...) i-times

$t \xrightarrow[R, R \cup S]{NP}_{\sigma} t'$ R-normal R∪S-paramodulation

$t \xrightarrow[R, R \cup S]{RP}_{\sigma} t'$ R-reduced R∪S-paramodulation

$t \xrightarrow[R]{}^{+NF} t'$ proper R-normalization

$>_{mult}$ the multiset extension of the ordering > on elements towards multisets of elements

m+n for multisets m and n: their sum

$[x\sigma.\ x \in Var(t)]$

multiset comprehension; the multiset of all $x\sigma$ where $x \in Var(t)$ holds.