MAX-PLANCK-INSTITUT FÜR INFORMATIK

Non-Symmetric Rewriting

.

Georg Struth

MPI–I–96–2–004 June 1996

INFORMATIK

Im Stadtwald
D 66123 Saarbrücken
Germany

Authors' Addresses

Max-Planck-Institut für Informatik
Im Stadtwald
D-66123 Saarbrücken
Germany
E-Mail: `struth@mpi-sb.mpg.de`
Phone: +49 681 9325 228

Acknowledgements

We wish to thank Leo Bachmair, David Basin, Harald Ganzinger, Krishna Rao, Jürgen Stuber and Uwe Waldmann for helpful discussions on the subject of this paper.

Abstract

Rewriting is traditionally presented as a method to compute normal forms in varieties. Conceptually, however, its essence are commutation properties. We develop rewriting as a general theory of commutation for two possibly non-symmetric transitive relations modulo a congruence and prove a generalization of the standard Church-Rosser theorem. The theorems of equational rewriting, including the existence of normal forms, derive as corollaries to this result. Completion also is purely commutational and we show how to extend it to plain transitive relations. Nevertheless the loss of symmetry introduces some unpleasant consequences: unique normal forms do not exist, rewrite proofs cannot be found by don't-care nondeterministic rewriting and also simplification during completion requires backtracking. On the non-ground level, variable critical pairs have to be considered.

Keywords

Transitive Relations, Rewriting, Commutation, Completion.

1 Introduction

Term rewriting is one of the standard decision procedures for varieties. Any algebra free in a variety is isomorphic to the quotient of the corresponding term algebra and the congruence generated by the equations which hold in the variety. By effectively mapping each congruence class to one of its members—its normal form—term rewriting often yields a method to compute the congruence and thereby a solution to the associated word problem. In this spirit Dershowitz and Jouannaud write in their survey article on rewrite systems [7] that "*the theory of rewriting is in essence a theory of normal forms*".

We present a different view on rewriting. We show that the essential concepts of rewriting are *commutation* and *reduction*, whereas normal forms only arise as a mere side-effect in a special case. According to this more liberal view, rewriting techniques apply beyond equational theories to arbitrary (non-symmetric) transitive relations, quasi-orderings and inequalities, and therefore may also contribute to a better understanding of the algorithmic aspects of deduction in general. The restricted attention paid to this aspect of rewriting is perhaps surprising. First the applicability of rewrite-techniques to transitive relations is quite obvious, since rewrite relations themselves are transitive, but not symmetric. Second already Messequer in his framework of *rewrite logic* [16] advocated a liberal understanding of rewriting. Third, some of the ideas of our approach already appear in the work of Levy and Agustí [15], Levy [14], and Bachmair and Ganzinger [3, 4], but were never generalized far enough to yield a generalization of equational rewriting modulo a congruence. Moreover the main statements in the work of Levy and Agustí [15], Levy [14] are false. We will discuss the relation between our work and theirs in a special section.

We develop our theory of non-symmetric rewriting as a commutation theory for two arbitrary binary relations along the lines of and in full symmetry to equational rewriting, studying these relations both as abstract reductions and as induced by rewrite rules over a term algebra. We also include a third relation, which plays a rôle similar to that of the unorientable equations in equational rewriting modulo a congruence, but which is not assumed to be symmetric. Concretely, we show how to localize a generalized Church-Rosser property—essentially, the Church-Rosser property *is* a commutation property—in presence of a reduction ordering to effective criteria on critical pairs. A generalized critical pair lemma can even be proven by a simple renaming some of the relations used in the equational case, since also the critical pair lemma is purely commutational. The theorems of equational rewriting follow as easy corollaries in a special case and also the emergence of normal forms can be easily understood. Besides the conceptual study, our general formalism provides a basis for completion procedures—essentially, completion is about commutation and reduction—for transitive relations as well as for very general chaining calculi, including subterm-chaining and congruences.

After a brief review of terminology in the first section we informally sketch the basic ideas of our approach in the second section. In the third section, an abstract local commutation theorem is proven and discussed. It can be seen as a generalization of a similar theorem of Bachmair and Ganzinger, a correction and generalization of the central abstract theorem of Levy and Agustí, and as a generalization of the localization theorem of equational abstract reduction modulo an equivalence. We also state a counterexample to the statements of Levy and Agustí and discuss their abstract results. In the fourth section, we adapt our abstract theorem to term rewriting and to the concept of critical pairs. Again our theorem is more general that that of Levy and Agustí. In the fifth section we discuss our results with respect to various restrictions and applications. The sixth section we relate our work with that of Bachmair and Ganzinger, Levy and Agustí and Levy. The seventh and last section contains a conclusion.

2 Preliminaries

We presuppose the notation proposed by Dershowitz and Jouannaud [8] and an elementary knowledge about abstract reduction and term-rewriting, including unification theory, as provided by the surveys of Dershowitz and Jouannaud [7], and Klop [13].

We are concerned with *abstract reduction systems* (ARS) $\langle S, A, B, C\rangle$ of a (non-empty) set S endowed with binary relations A, B, and C. Usually we omit the attribute 'binary'. AB denotes the *relational product* of the respective two relations. An *R-chain* or a *proof* of length n is a sequence $\Pi = \langle s_0, \ldots, s_n\rangle$ whose adjacent elements are related by the relation R. Replacement of a subproof of a proof Π by a proof Ξ is called a *proof transformation* and denoted by $\Pi[\Xi]$. $\Pi \Longrightarrow \Xi$ expresses the transformation of a proof Π to a proof Ξ. For details, see [1]. Abusing notation, we also call strings of relation symbols, like $ABBACA$, proofs.

R^{-1} denotes the *converse*, $R^{\leftrightarrow}$ the *symmetric closure*, R^{+}, the *transitive* *closure* and R^*, the *reflexive transitive closure* of a relation R. R is *well-founded*, if there are no infinite R-chains, a *quasi-ordering*, if it is reflexive and transitive and a *partial ordering*, if it is also antisymmetric. For relations R and S, $R/S = S^*RS^*$. S is not assumed to be symmetric, so R/S is not a quotient relation.

We also study *term rewrite systems* (TRS) of the form $\langle T_\Sigma(X), A, B, C\rangle$, where $T_\Sigma(X)$ denotes the free algebra with generators X over a signature Σ and A, B, and C are sets of rules inducing rewrite relations. We will also use the letter C for context variables of the meta-language. We denote with $\longrightarrow_{R/S}$ the rewrite relation $\longrightarrow_S^*\longrightarrow_R\longrightarrow_S^*$. A *linear* term has no multiple occurrences of a variable. A rule $\langle l, r\rangle \in R$ is *left-linear*, if l is linear, *right-linear*, if r is linear and *linear* if it is left- and right-linear. It *preserves left variables*, if all variables from r also occur in l, *preserves right variables* in the converse case and *preserves variables*, if it preserves left and right variables. A TRS is left-linear, right-linear, linear, preserves left variables, preserves right variables or preserves variables, if all rules have this property.

3 General Ideas

In this section we informally develop the basic ideas of our approach. Ordering a theory presented by non-symmetric relations leads to two rewrite relations, say A and B.

Consider a presentation of lattice theory with AC-operators $\vee$ and $\wedge$ and assume a lexicographic path ordering corresponding to a precedence $\succ$ with $\vee \succ \wedge$. We have the laws

$$x \vee x \leq_A x, \qquad x \leq_B x \wedge x, \qquad x \wedge y \leq_A x, \qquad x \leq_B x \vee y,$$

where $\leq$ is a partial ordering, $\leq_A = \leq \cap \succ$, and $\leq_B = \leq \cup \prec$. Moreover we have the *isotony rules*

$$\frac{x \leq y}{z \vee x \leq z \vee y}, \qquad \frac{x \leq y}{z \wedge x \leq z \wedge y},$$

expressing monotonicity of $\vee$ and $\wedge$. A proof of the distributive inequality $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$, for instance, can be visualized as

$$\begin{tikzcd}
 & & (x \wedge (y \vee z)) \vee (x \wedge (y \vee z)) \arrow[dr, "A"] & \\
 & (x \wedge (y \vee z)) \vee (x \wedge z) \arrow[ur, "B"] & & x \wedge (y \vee z) \\
(x \wedge y) \vee (x \wedge z) \arrow[ur, "B"] & & &
\end{tikzcd}$$

This proof has a peak structure. The arrows indicate the direction of the relation $\leq$. When terms increase with respect to the lpo, arrows point upwards, and they point downwards, when terms decrease. Here, B-steps increase terms, whereas A-steps decrease them.

At a more abstract level, peaks and valleys alternate in proofs. In equational rewriting, $B = A^{-1}$, and the Church-Rosser property states that for an arbitrary proof consisting of A-steps and A^{-1}-steps, there exists a so called *rewrite proof* of the form $A^*(A^{-1})^*$. This property is equivalent to the property of *confluence* which states that all proofs of the form $(A^{-1})^*A^*$ can be replaced by rewrite proofs and thus amounts to say that A^*-steps *commute* over $(A^{-1})^*$-steps. Confluence makes the existence of more than one normal form impossible. In this sense, the existence of normal forms in equational rewriting can be seen as a side effect of commutation and of the existence of unique rewrite proofs. Nevertheless different proofs leading to that normal form may exist.

In the setting of two relations A and B, the property that arbitrary proofs consisting of A-steps and B-steps can be replaced by a rewrite proof of the form A^*B^* generalizes the Church-Rosser property. Evidently our above example does not have this property. The peak cannot be eliminated. In the context of transitive relations, where A and B are obtained by intersection with $\succ$ and $\prec$, respectively, rewrite proofs of the form $A^+B^* \cup B^+$ are even more convenient. Confluence is generalized to the *commutation* property that all peaks of the form B^*A^* can be replaced by rewrite proofs. Rewrite proofs again contain minimal elements (where A-steps switch to B-steps, or else at the beginning or at the end of the rewrite proof), but these minimal elements are no longer unique. Imagine that two different minimal elements exist. Then two divergences must exist along the proof, but the only criterion to force uniqueness is to require that A or B^{-1} is confluent, which makes no sense in our non-symmetric context. So normal forms do not exist for non-symmetric rewriting.

In equational rewriting, confluence is equivalent to *local confluence*, i.e., the property that all $A^{-1}A$-proofs can be replaced by rewrite proofs, in case A^+ is well-founded. Under this well-foundedness assumption, normal forms become effective functions, and rewrite proofs can be calculated don't-care nondeterministically. In our more general setting, local confluence is an instance of the commutation property that any proof of the form BA can be replaced by a rewrite proof. To prove equivalence to the commutation property of B^*A^*, Levy and Agustí proposed well-foundedness of both A^+ and $(B^{-1})^+$. The counterexample in the next section shows, however, that well-foundedness of $(A \cup B^{-1})^+$ must be required. Nevertheless, if both A^+ and $(B^{-1})^+$ are well-founded, then rewrite proofs can be effectively constructed, if they exist. In terms of graphs, a rewrite proof between two objects s and t is constructed by generating the directed acyclic A-graph from A from s and the directed acyclic B^{-1}-graph from t and checking for a common vertex of both graphs. Under the above assumptions, both graphs have only finite paths and if moreover all vertices have finite out-degree, then the construction is effective. Nevertheless, it is a search procedure requiring backtracking and it depends on the implementation, which among the rewrite proofs is found.

The above lattice example indicates that it is desirable to include for some operators of the signature monotonicity properties as well as non-orientable rules or equations, as for example the permutative congruence AC. This means that critical pairs and a property similar to *coherence* also have to be investigated.

Let us conclude this section with a summary and an outlook. We motivated that in the context of rewriting in theories presented by non-symmetric relations, commutation properties play a key rôle; they generalize confluence and local confluence from the equational case. Moreover, normal forms no longer exist, because the commutation properties of the non-symmetric case are weaker than those of the equational case. Solving inequalities instead of equalities, backtracking therefore replaces don't-care nondeterminism. It is obvious that coherence also is a commutation property. Thus even extended completion of equational theories is basically a procedure to calculate certain commutations and it should be possible, to specify such a procedure for the non-symmetric case. The following sections will show that this is indeed the case.

4 Abstract Commutation

In this section we prove for an ARS $\langle S, A, B, C\rangle$ that commutativity of peaks and cliffs together with a well-foundedness assumption allow us to replace any proof of the form $(A \cup B \cup C)^+$ by an appropriate rewrite proof. This statement implies its analog from equational rewriting by setting $B = A^{-1}$ and requiring that C is symmetric. Our statement also implies the one used by Bachmair and Ganzinger [1] by setting $C = \emptyset$.

Definition 4.1 *For an ARS $\langle S, A, B, C\rangle$ and arbitrary relations A_C and B_C satisfying $A \subseteq A_C \subseteq A/C$ and $B \subseteq B_C \subseteq B/C$, the set of* rewrite proofs *is defined as $P\downarrow = A_C^+ C^* B_C^* \cup A_C^* C^* B_C^+$. Rewrite proofs, i.e., elements of $P\downarrow$ are denoted by $\Pi\downarrow$. A is said to* commute *over B, if BA is contained in $P\downarrow$.*

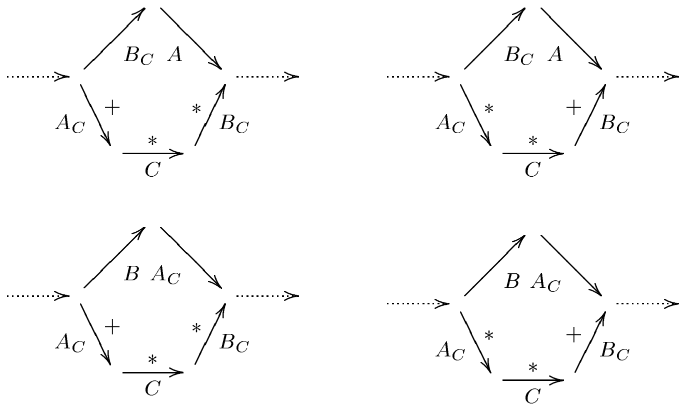
These definitions are quite similar to, and chosen for the same reasons as in the equational case; so we do not discuss them. Our rewrite proofs $\Pi\downarrow$, however, are only a subset of the proofs of the form $A_C^* C^* B_C^*$, which one would expect from the equational case. This has two reasons. First, our abstract commutation theorem does not hold for the latter rewrite proofs, as our counterexample from the end of this section shows—not even for proofs from $P\downarrow \cup C^+$. Second, our rewrite proofs are conceived for the case, where the relations A, B and C stem from the intersection with a syntactic ordering. The case of a transitive relation with reflexive part or a quasi-ordering is then an easy consequence of our result. We now introduce some terminology for the following proof.

Definition 4.2 *We call proofs of the form $s_i B A_C s_j$ and $s_i B_C A s_j$* peaks *and proofs of the form $s_i C A_C s_j$ and $s_i B_C C s_j$* cliffs*. We call s_i the* initial vertex *of the peak or cliff and s_j the* final vertex*. We call* initial steps with respect to a cliff *CA_C the steps of the cliff and the initial C-proof and first A-step of the corresponding rewrite proof. We call* final steps with respect to a cliff *$B_C C$ the steps of the cliff and the final B-step and C-steps of the corresponding rewrite proof.*

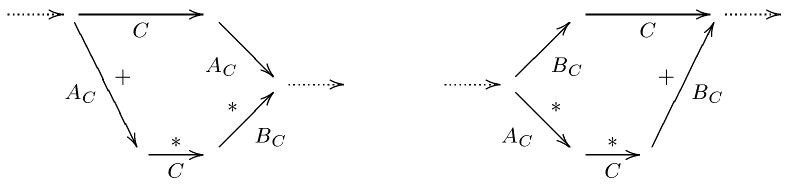
In the following theorem, we will assume that the relation $\succ = (A/C \cup (B/C)^{-1})^+$ is well-founded. Under this assumption, rewrite proofs corresponding to cliffs have a special form: Those corresponding to a cliff CA_C must contain at least one A-step; those corresponding to a cliff $B_C C$ must

[1] c.f. Lemma 1 of [4]

contain at least one B-step. All other rewrite proofs would lead to circles with respect to $\succ$. Transformation of peaks can therefore be visualized as



and transformation of cliffs as



We are now in the position to prove the following abstract commutation theorem:

Theorem 4.1 *Let $\langle S, A, B, C\rangle$ be an ARS and let $\succ = (A/C \cup (B/C)^{-1})^+$ be a well-founded relation. Then $(A \cup B \cup C)^+$ is contained in $P\downarrow \cup C^+$, if BA_C, B_CA, CA_C and B_CC are contained in $P\downarrow$.*

Proof The general scenario is to show that the proof transformation defined by the above commutation relations terminates. An induction measure $M(\Pi)$ together with a well-founded ordering $\gg$ over the domain of M, satisfying the replacement property, is associating with each proof Π. It then remains to show that $\Theta \Longrightarrow \Xi$ implies $M(\Theta) \gg M(\Xi)$ for all generators $\langle\Theta, \Xi\rangle$. This is a necessary and sufficient condition to ensure the above statement of termination [6]. Our induction measure, however, will be non-local in a sense specified below and therefore the replacement property does not hold a priori, but must be verified during the induction.

It is obvious that $(A \cup B \cup C)$-proofs containing only C-steps are not in $P\downarrow$, but they trivially fulfill the condition of the premise of the theorem. We can therefore restrict to the case, where the $(A \cup B \cup C)$-proofs contain at least one A-step or B-step.

In equational rewriting an induction ordering on equivalence classes can be defined, but here C is not assumed symmetric. But similarly to equational rewriting, one must distinguish C-steps within A_C-steps or B_C-steps from 'non-covered' ones. Transforming for instance a cliff to a rewrite proof by $CA \Longrightarrow A_C C = (CCCA)C$, C-steps originating from an A_C-step must lead to a measure smaller than that of the C-step of the cliff, which is not 'covered' by an A_C-step.

In general, call the left C-steps of an A_C-step *left-covered* and the right C-steps of a B_C-step *right-covered*. Clearly this definition is non-local and can destroy the replacement property of the induction measure.

Associate with the i-th step of a proof $\Pi = \langle s_0, \ldots, s_n \rangle$ an ordered pair $\mu_i^\Pi = \langle s_{\rho(i)}, \beta_i^\Pi \rangle$. For the initial (final) steps of a cliff, set $\rho(i) = k_i$, where k_i is the index of the initial (final) vertex of the cliff. Otherwise, for non-initial and non-final steps, set $\rho(i) = i - 1$ for A-steps and C-steps and and $\rho(i) = i$ for B-steps.

Set the *cover-number* β to $\beta_i^\Pi = 0$ for A-steps and B-steps, $\beta_i^\Pi = 1$ for left-covered and right-covered, $\beta_i^\Pi = 2$ for left-covered but not right-covered, $\beta_i^\Pi = 3$ for right-covered but not left-covered, and $\beta_i^\Pi = 4$ for non-covered C-steps. Let $M(\Pi) = \{\mu_1^\Pi, \ldots, \mu_n^\Pi\}$ be the induction measure for Π.

Define the induction ordering as $\gg = ((\succ, >)_{lex})_{mul}$, where $>$ denotes the (strict) ordering on natural numbers. Thus the μ are compared lexicographically with $\succ$ for the first and $>$ for the second component. This ordering is extended to multisets to compare proofs.

Now consider the transformation of a peak or a cliff to a rewrite proof and compare the induction measures involved according to $\gg$. For peaks, which are either of the form $B_C A$ or BA_C, the first component of the μ associated with the B-step of the peak majorizes those of the rewrite proof by $\succ$ and therefore $M(\Pi[B_C A]) \gg M(\Pi[(B_C A)\downarrow])$ and $M(\Pi[BA_C]) \gg M(\Pi[(BA_C)\downarrow])$.

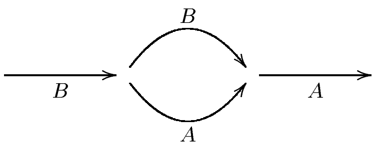
For cliffs, which are of the form CA_C or $B_C C$, the arguments are more involved. First consider a cliff of the form CA_C. It is transformed to a rewrite proof of the form $A_C^+ C^* B_C^*$. The first step of the rewrite proof can be an A-step or a C-step, but then the first component of $\mu_1^{CA_C}$ and the first component of $\mu_1^{(CA_C)\downarrow}$ are the same. So for our argument we can entirely concentrate on β, the second component of μ.

If the first step from the first A_C-step of the rewrite proof $(CA_C)\downarrow$ is an A-step, then $\beta_1^{(CA_C)\downarrow} = 0$ and $\beta_1^{CA_C} > 0$. If the first such step is a C-step, then $\beta_1^{(CA_C)\downarrow} \leq 2$. Now the C-step from the cliff could be either not covered, or right-covered, or left-covered and right-covered. But in the last case we have to consider a peak instead of a cliff. In both of the other cases, $\beta_1^{CA_C} \geq 3$. These cases are exhaustive and we can conclude that always $\beta_1^{(CA_C)\downarrow} < \beta_1^{CA_C}$. Hence $\mu_1^{(CA_C)\downarrow}$ is smaller than $\mu_1^{CA_C}$ on the lexicographical combination of $\succ$ and $>$, because the first components are the same for all these μ. Therefore $\mu_1^{CA_C}$ majorizes all the $\mu_i^{(CA_C)\downarrow}$, $M(CA_C) \gg M((CA_C)\downarrow$ $)$ and $M(\Pi[CA_C]) \gg M(\Pi[(CA_C)\downarrow])$.

The case analysis for cliffs of the form $B_C C$ exploits the symmetry to CA_C-cliffs, which is established by reading proofs backwards. Only the case, where the C-step in the cliff is left-covered and the corresponding rewrite proof starts with a C-step too, is critical, because the β of this step would majorize those of the cliff. Fortunately we can analyze this case as a CA_C-cliff.

This finishes the case analysis of peaks and cliffs. The transformation process terminates and the minimal proofs are the rewrite proofs. $\square$

The necessity of well-foundedness of unions of relations, not only of both the particular relations, is illustrated by the following simple example:



A commutes over B, but globally there is no rewrite proof. A^+ and $(B^{-1})^+$ are well-founded, but of course $(A \cup B^{-1})^+$ cycles. This counterexample also justifies the shape of our rewrite proofs. Replacement of B by C in the left diagram leads to a counterexample for candidates of the form $P\downarrow \cup A_C^* C^+ B_C^*$ and thus also for $A_C^* C^* B_C^*$. In our proof, these C-steps would not be covered and a rewrite proof could have a bigger measure than a cliff.

Another important feature is that our well-foundedness assumption did not assume C to be symmetric. This weaker assumption is not trivial because well-foundedness of a relation R/C is not generally preserved under symmetric closure of C. Our result clearly expresses the commutative content of equational rewriting. We will later see that if C is symmetric, the rewrite proofs can be chosen similar to the equational case and also the induction measure can now incorporate equivalence classes.

5 Term Commutation

Theorem 4.1 suffices as a basis for ordering transitive relations. Here we consider the refinement to a TRS with monotonic operators, like for example the lattice operators satisfying the isotony laws. Along the lines of equational rewriting modulo a congruence, we reduce theorem 4.1 to a statement on critical pairs. Nevertheless our rewrite proofs contain three relations instead of two. Therefore we have to consider also variable critical pairs and the concept of overlap has to be generalized to cover variable positions. Let us first consider how two rewrite steps $\longrightarrow_R$ and $\longrightarrow_S$ commute in a term with respect to the positions where they apply. This purely commutational lemma has a direct counterpart in standard rewriting.

Lemma 5.1 *Let $\langle T_\Sigma(X), R, S\rangle$ be a TRS with rewrite relations $\longrightarrow_R$ and $\longrightarrow_S$.*

(i) For disjoint positions p and q

$$\underset{R}{\longrightarrow}^{p}\underset{S}{\longrightarrow}^{q}\subseteq\underset{S}{\longrightarrow}^{q}\underset{R}{\longrightarrow}^{p},$$

(ii) if p is a prefix of $q = pq'q''$ and S applies below a variable-position q' of a variable from R, then

$$\begin{aligned}\underset{R}{\longrightarrow}^{p}\underset{S}{\longrightarrow}^{q} &\subseteq \underset{S}{\longrightarrow}^{\mathbf{q}_l\cup q}\underset{R}{\longrightarrow}^{p}\underset{S}{\longleftarrow}^{\mathbf{q}_r},\\ \underset{S}{\longrightarrow}^{q}\underset{R}{\longrightarrow}^{p} &\subseteq \underset{S}{\longleftarrow}^{\mathbf{q}_l}\underset{R}{\longrightarrow}^{p}\underset{S}{\longrightarrow}^{\mathbf{q}_r\cup q},\end{aligned}$$

where $\longrightarrow_S^{\mathbf{q}_l}$ ($\longrightarrow_S^{\mathbf{q}_r}$) denotes parallel rewriting at all left-hand (right-hand) positions q_i such that $q_i = pq_i'q''$ and $q_i \neq q$ is a variable-position associated with the same variable as q'.

(iii) Under the same assumptions as in (ii), if moreover R preserves right variables, then $\mathbf{q}_l$ in the first equation of (ii) is non-void and if R preserves left variables, then $\mathbf{q}_r$ in the second equation of (ii) is non-empty. □

The proof of lemma 5.1 is a straightforward adaption from equational rewriting. We can think of the right-hand sides of the above equations as rewrite proofs induced by the commutation properties of terms. These rewrite proofs now have to be compared with those defined in the last section, to be compatible with our abstract results. But first we fix the rewrite relations induced by A_C and B_C and adapt some notions from standard rewriting. Due to the fact that C is non-symmetric, we cannot simply C-unify terms in the sense of semantic unification. So we first define a corresponding non-symmetric concept.

Definition 5.1 *For a TRS $\langle T_\Sigma(X), R\rangle$ and two terms s and t, we say that a substitution σ is a* solution to the R-reduction problem *for s and t, if $s\sigma \longrightarrow_R^* t\sigma$. The concept of a* complete minimal set *of such solutions is defined as usual.*

This definition can be seen as a kind of one-way semantic unification; it is also closely related to narrowing. This reduction problem again requires backtracking and unique solutions do not in general exist. We do not want to discuss this definition further, because in practical cases, C will most probably be a permutative congruence, and therefore symmetric.

Definition 5.2 *Let $\langle T_\Sigma(X), A, B, C\rangle$ be a TRS. Then*

$$\underset{A_C}{\longrightarrow}^p = \overset{*}{\underset{C}{\longrightarrow}}{}^{\leq p} \underset{A}{\longrightarrow}^p, \qquad \underset{B_C}{\longrightarrow}^p = \underset{B}{\longrightarrow}^p \overset{*}{\underset{C}{\longrightarrow}}{}^{\leq p},$$

where '$\leq p$' denotes that all positions of the C-reductions apply below p [2].

Two rules overlap, *if the left-hand side of the one and a subterm of the right-hand side of the other have a solvable C-reduction problem, or vice versa* [3]. *If the overlap occurs at a variable position, it is called a* variable overlap *and else a* proper overlap. *The critical pairs generated by such overlaps are called* proper *or* variable critical pairs. *So for rules $\langle l_1, r_1\rangle$ and $\langle l_2, r_2\rangle$ and a solution σ for the C-reduction problem of $r_1|_p$ and l_2, $\langle r_1\sigma[l_1\sigma]_p, r_2\sigma\rangle$ is a proper critical pair, if $r_1|_p \notin X$ and $\langle r_1[C[l_1]]_p, r_2\rangle$ is a variable critical pair, if $r_1|_p \in X$ and C is a context variable. The set of variable critical pairs is denoted by P_C^X, the set of proper critical pairs by P_C^P; $P_C = P_C^X \cup P_C^P$ is the set of critical pairs.*

[2]The definition is compatible with the requirements of the previous section, namely $\longrightarrow_A \subseteq \longrightarrow_{A_C} \subseteq \longrightarrow_{A/C}$ and $\longrightarrow_B \subseteq \longrightarrow_{B_C} \subseteq \longrightarrow_{B/C}$.

[3]The definition deviates from standard rewriting, where left-hand sides unify with left-hand sides. If C is symmetric, we define the overlap with respect to a complete minimal set of C-unfiers

Lemma 5.2 *Let $\langle T_\Sigma(X), A, B, C\rangle$ be a TRS with complete minimal sets of solutions of the C-reduction problem. Let p be a prefix of q, if a rule from A is applied at p and a strict prefix, if a rule from B or C is applied at p* [4].

(i) For disjoint p and q in general and variable-overlaps with A left-linear, B right-linear and C linear in the respective variable, and moreover variable preserving

$$(\xrightarrow[B\cup C]{}{}^{p}\xrightarrow[A_C]{}{}^{q} \cup \xrightarrow[B_C]{}{}^{q}\xrightarrow[A\cup C]{}{}^{p}) \subseteq P\downarrow .$$

(ii) For proper overlaps and non-linear variable overlaps

$$(\xrightarrow[B\cup C]{}{}^{p}\xrightarrow[A_C]{}{}^{q} \cup \xrightarrow[B_C]{}{}^{q}\xrightarrow[A\cup C]{}{}^{p}) \subseteq \xrightarrow[C]{*}\xrightarrow[P_C]{}\xrightarrow[C]{*},$$

where all C-steps at the left-hand side go to and all C-steps at the right-hand side come from-hand below variable positions of the rule. $\square$

Lemma 5.2 compares the rewrite proofs induced by lemma 5.1 with the ones from the abstract commutation theorem. The lemma documents the necessity of considering variable critical pairs. Unfortunately there can be infinitely many of them even in the case when C is empty and therefore, in presence of monotonicity, the completion process is faced with a severe obstacle. We will discuss this issue further in the next section. The lemma is a straightforward generalization of the critical pair lemma of equational rewriting. Its proof is a simple renaming of relations from the equational case. Thus the critical pair lemma of equational rewriting is purely commutational.

In lemma 5.2 we assumed that C preserves variables. This assumption rules out that a cliff is transformed to a single $\xrightarrow[C]{+}$-step. In general, every well-founded rewrite relation is induced by rules which preserve right variables and consequently the relation is finitely branching. Moreover if R and S induce a well-founded rewrite relation $\longrightarrow_{R/S}$ and R contains at least one rule with a variable in a right-hand side, then S preserves right variables. It is easy to construct a self-embedding chain by reductio ad absurdum. So in our case, if A is well-founded, then it preserves right variables, if B^{-1} is well-founded, then it preserves left variables. In the following we assume that at least one rule from A contains a variable in its right-hand side and some rule from B contains a variable in its left-hand side. If this was not

[4] The variable restrictions are tailored for the case analysis in theorem 5.3.

the case we could also assume that C preserves left and right variables, to prove the following theorem.

Another fact from lemma 5.2 is crucial, namely the fact that the outer C-steps arising with proper and variable critical pairs lie below variables. This phenomenon is well-known from equational rewriting. A critical pair corresponding to a cliff is (with respect to unification) the most general way in which such an overlap may occur. Thus a most general solution of the corresponding reduction problem (or the unification problem) of the critical pair must be further instantiated to yield a substitution for the cliff. This instantiation generally leads to C-steps connecting the cliff with the rewrite proof, coming from the substitution. In equational rewriting the fact that under additional assumptions these outer C-steps lie 'deep' in the terms is used to make the proof transformation work. We will transfer this method to the non-symmetric case.

Theorem 5.3 *Let $\langle T_\Sigma(X), A, B, C\rangle$ be a TRS with a complete minimal set of solutions of the C-reduction problem* [5]*, let $\rhd$ denote the (strict) subterm relation. Let $(\longrightarrow_{A/C} \cup \longleftarrow_{B/C})^+$ and $\longrightarrow^+_{\rhd/C^\leftrightarrow}$ be well-founded. Then $(\longrightarrow_A \cup \longrightarrow_B \cup \longrightarrow_C)^+$ is contained in $\longrightarrow_{P\downarrow} \cup \longrightarrow^+_C$, if $\longrightarrow_{P_C}$, the rewrite relation induced by the set of proper and variable critical pairs, is contained in $\longrightarrow_{P\downarrow}$.*

Proof As we have seen, well-foundedness of A/C and of $(B/C)^{-1}$ imply that C preserves variables. Thus cliffs cannot simply be closed by C-steps. Part of the theorem is already proven by theorem 4.1. However, the induction measure has to be strengthened, as transformations of critical pairs may introduce non-covered C-steps via substitution in the converted proof which could let terms increase. A cliff $\longrightarrow_C\longrightarrow_{A_C}$, for instance, could be transformed to $\longrightarrow_C\longrightarrow_C\longrightarrow_{P\downarrow}\longrightarrow_C$, and the measure of the reduct could be bigger than that of the cliff. Fortunately, by lemma 5.2, the outer $\longrightarrow_C$-steps of the converted proof lie 'deeper' in the terms than those of the cliff and this fact can be included in the μ of the induction measure M, as long as the encompassment ordering is well-founded.

So for the induction measure M, define $\mu_i^\Pi = \langle s_{\rho(i)}, \delta_i^\Pi, \beta_i^\Pi\rangle$, where $\delta_i^\Pi = [s_{i-1}|_{p_i}]$, the brackets denote equivalence classes with respect to $C^\leftrightarrow$, and p_i is the position at which the reduction occurs for C-steps, and $\delta_i^\Pi = \perp$ otherwise. The rest of the measure is defined as in theorem 4.1. The δ are com-

[5] If C is symmetric, assume a complete minimal set of C-unifiers.

pared with respect to the ordering $\blacktriangleright/C^{\leftrightarrow}$, defined on the encompassment-ordering $\blacktriangleright$ [6]. $\blacktriangleright/C^{\leftrightarrow}$ is well-founded if and only if $\rhd/C^{\leftrightarrow}$ is [1]. This is the case if all $C^{\leftrightarrow}$-congruence classes are finite. $\perp$ is supposed to be minimal in the subterm ordering.

The disjoint case and the prefix case can be considered separately. The disjoint case is obvious. The analysis of the prefix case is suggested by lemma 5.2. Consider a cliff of the form $\longrightarrow^{o}_{B}\xrightarrow[C]{*}{}^{\leq p}\longrightarrow^{q}_{A}$, where $\leq p$ denotes that all C-rewrites occur below p. If $q \geq o \geq p$ we analyze this as a $\longrightarrow_{B}\longrightarrow_{A_C}$ chain. Thus o must be strictly greater than q and greater than p to analyze the case as a $\longrightarrow_{B_C}\longrightarrow_{A}$ chain. Also A-steps and B-steps absorb adjacent C-steps as long as the latter are not strictly bigger. This covers all cases, and therefore lemma 5.2 provides all information necessary for cliffs. Moreover the consideration of cliffs is sufficient, as the rest is implied by theorem 4.1 and by symmetry we can even restrict our attention to cliffs of the form $\longrightarrow^{q}_{C}\longrightarrow^{p}_{A_C}$, where p is a (non-strict) prefix of q. Assume it is transformed to a chain

$$\xrightarrow[C]{*}{}^{\leq p'}\xrightarrow[A_C]{+}{}^{p''}\xrightarrow[C]{*}{}^{p'''}\xrightarrow[B_C]{*}{}^{q''}\xrightarrow[C]{*}{}^{\leq q'}$$

Then by lemma 5.2, $p' \leq p$. By assumption, $\rhd/C$ is well-founded and thus the leftmost term of the cliff may not be a variable. Thus $p' < p$ and therefore the measure of the C-step of the cliff majorizes those of the C-steps from the reduct by comparing the δ. To the A-step and the further steps we can apply our arguments from theorem 4.1. Thus the measure of the whole reduct is smaller than that of the cliff and the proof is finished. $\Box$

Obviously our assumption of well-foundedness of the subterm relation modulo $C^{\leftrightarrow}$ holds whenever the $C^{\leftrightarrow}$-equivalence classes are finite [12]. As a counterexample for the converse direction let $C^{\leftrightarrow} = \{\langle f(g(a)), f(g(g(a)))\rangle\}$. Obviously equivalence classes are infinite, but it is easy to see that the subterm-ordering modulo $C^{\leftrightarrow}$ is well-founded. As in the case of equational rewriting, this assumption excludes rules like identity or idempotence from C.

[6] $s \blacktriangleright t$ iff $s|_p = t\sigma$ where p is not the root-position, and $s \blacktriangleright/C^{\leftrightarrow} t$ iff either $s \blacktriangleright t$ or $s \longrightarrow_{C^{\leftrightarrow}} s[t\sigma]$, where the rewrites occur strictly below the root. Note that the syntactic restriction in the definition plays a rôle in the proof only in so far as well-foundedness of the relation must be assured.

6 Discussion

In this section we briefly discuss some syntactic restrictions, sketch a completion procedure and describe some consequences for theorem proving.

A particularly simple consequence of theorem 4.1 in the case $C = \emptyset$ is the following: If $(A \cup B^{-1})^+$ is well-founded and BA is contained in the set of rewrite proofs $A^+B^* \cup B^+$, then all $(A \cup B)$-proofs are contained in that set. This can easily be proven with the first component of our induction measure alone. Note that by assumption, A^+ and B^+ are irreflexive. If the relation R, which is intersected by a strict ordering to obtain A and B, has a reflexive part, then one can put it into C. If C contains nothing else, then the commutation relations for cliffs are very simple, namely $CA_C \subseteq A_C \supseteq A_C C$ and similar for B_C. In particular, we can handle quasi-orderings by assuming that $x \approx x$ is in C. An alternative approach to quasi-orderings would be to prove that if $(A \cup B^{-1})^+$ is well-founded and $BA \subseteq A^*B^*$, then $(A \cup B)^* \subseteq A^*B^*$. This is also straightforward. The result just stated easily carries over to a TRS $\langle T_\Sigma(X), A, B\rangle$.

For a TRS $\langle T_\Sigma(X), A, B, E\rangle$ with E symmetric, critical pairs can be defined, and theorem 5.3 can be stated in terms of E-unification. Also theorem 5.3 can be proven more like the equational case, because the induction measure can now use equivalence classes of terms in the first component. We can even allow pure E-chains as rewrite proofs. The crucial point in the analysis of peaks and cliffs is that closing a cliff with only E-steps is excluded by the well-foundedness assumption. This could not be done in the abstract non-symmetric case, as our counterexample showed; here it contains a cycle with an $\longleftrightarrow_E$-step, contradicting the well-foundedness assumption.

In a TRS $\langle T_\Sigma(X), A, B, C\rangle$, variable critical pairs can be avoided in case A is left-linear, B is right-linear, and C linear. In equational rewriting, the case of a left-linear rewrite system modulo a congruence has a Church-Rosser theorem with particularly simple rewrite proofs [10]. In the non-symmetric case, as a corollary of theorem 5.3, one can show for rewrite proofs of the form $P_L \downarrow = \longrightarrow_A^+ \longrightarrow_C^* \longrightarrow_B^* \cup \longrightarrow_A^* \longrightarrow_C^* \longrightarrow_B^+$ that any proof $(\longrightarrow_A \cup \longrightarrow_B \cup \longrightarrow_C)^+$ is contained in $\longrightarrow_{P_L\downarrow} \cup \longrightarrow_C^+$, if $(\longrightarrow_{A/C} \cup \longleftarrow_{B/C})^+$ is well-founded, $\longrightarrow_A$ commutes over $\longrightarrow_B$ and $\longrightarrow_C$, and $\longrightarrow_B$ commutes over $\longrightarrow_C$ with respect to $P_L \downarrow$. Moreover only proper critical pairs between the above relations have to be considered. This suggests splitting a completion procedure into a linear and a non-linear part, like in equational rewriting. A similar case is to require C linear and containing all monotonic operators. For example, AC is a linear theory.

As one can develop the theorems of non-symmetric rewriting along the lines of standard rewriting, one can also develop a completion procedure along these lines—with two exceptions. First, one must somehow handle the context variables induced by variable critical pairs. Levy [14] proposes to use a restricted second-order unification procedure to this purpose. We propose using a pre-completion procedure which stops, when all critical pairs except those needing superposition into a context variable, are computed. Then the completion can be continued by hand. Second, there is no simplification or collapse mechanism like in rewriting. For example, if $\langle a, b\rangle$ and $\langle a, c\rangle$ are in a relation and this relation is an equivalence, then $\langle b, c\rangle$ is in that relation. If the relation is non-symmetric, this is no longer the case; and we cannot simply generate new (undirected) rules by a simplification mechanism. Nevertheless one can implement simplification as a search procedure and delete rules where they can be replaced by a rewrite proof. The specification of the remainder of a completion procedure working with the extended-rule method is straightforward and so should be the proof of its completeness by combining our methods with those of equational completion proofs with extended rules. As already stated, equational completion is a commutational procedure.

In the domain of theorem proving, our ordering constraints considerably restrict variable chainings, in the sense that one of two terms to be unified is a variable. First, from lemma 5.2, these chainings are only necessary, if the variable is non-linear. Second, for theories allowing for elimination of quantifiers, like for example discrete orderings or dense linear orderings without endpoints, variable chainings can even be completely avoided [3]. Another restriction in ordered chaining calculi is that variable chaining is not needed for negative literals and if the variable is *shielded*, i.e., has an occurance below an operator in the same clause. It might be useful to consider theories, where elimination of at least some variables is possible, in particular.

7 Related Work

Our work is inspired first of all by the work of Levy and Agustí [15], Levy [14], and Bachmair and Ganzinger [3, 4].

Levy and Agustí seem to have been the first to partition an quasi-ordering into two sets of rewrite rules, intersecting it with a (total) syntactic simplification order and its inverse. Consequently, they have called their approach *bi-rewriting*.

Levy and Agustí have also realized that in presence of a Church-Rosser-like property quasi-orderings can be computed by searching for rewrite proofs from both ends and that non-linear rules lead to variable critical pairs. Their attempt to compute with the Church-Rosser property, however, is far from satisfactory. In the equational case of rewriting without congruence classes, it is easy to make the Church-Rosser property effective by showing that it is equivalent to local confluence in presence of some well-foundedness assumption. Levy and Agustí, trying to generalize this lemma to bi-rewriting, used well-foundedness of both A^+ and $(B^{-1})^+$, but not of $(A \cup B^{-1})^+$ which—as our counterexample at the end of section 4 shows—is too weak and makes all the main statements of their work false [7]. This error also has consequences for completion: Levy [14] proposes a canonical system for lattice theory, but the system contains a loop and thus cannot be obtained by completion. The correctness proof for this system therefore remains an open problem. Levy and Agustí also do not localize coherence in case of congruence classes [8]. They must eliminate cliffs in one step and therefore their approach does not yield an effective procedure. Moreover they use a very restrictive concept of rewrite proof [9] and have to restrict to congruence classes generated by rules with linear terms.

Aware of our counterexample, Levy and Agustí revised their work [10], but they merely changed well-foundedness of A_C^+ and $(B_C^{-1})^+$ to well-foundedness of $(A_C \cup B_C^{-1})^+$—all the other restrictions remain. At first sight this assumption looks weaker than ours (well-foundedness of $(A/C \cup (B/C)^{-1})^+$), but we believe that in practice the two assumptions make no difference for a TRS. It is not obvious that there are interesting cases of orderings which are well-founded under the first assumption, but not under the second one. It is first of all this well-foundedness assumption which lead Levy and Agustí to their severe restrictions, and this seems to be too high a prize to be paid: Levy and Agustí cannot draw the analogy to equational rewriting, they cannot localize cliffs, which is an obstacle for effectivity, their simplification mechanisms are much weaker than ours and they have to impose strong syntactic

[7] c.f. lemma 4.8, lemma 4.10, lemma 4.14, lemma 4.15, theorem 4.19 and theorem 5.13 of Levy's thesis [14]

[8] c.f. Lemma 4.14 and Lemma 4.15 of Levy's thesis [14].

[9] Consider their property "*extensionally closed*", which allows to replace any cliff CA_C by a rewrite proof of the form $A_C C^*$.

[10] This revised compilation of results of [15] and [14] has been submitted to the Journal of Symbolic Computation.

restrictions both on the form of rewrite proofs and of terms.

Bachmair and Ganzinger [3, 4], in the context of ordered chaining calculi for transitive relations, have restated the Church-Rosser-like property in the more general setting of two arbitrary binary relations and have noticed its equivalence to a (local) commutation property between these relations [11]. They have stated Levy's and Agustí's simplest localization lemma [12] with the right well-foundedness assumption, but have developed their commutation concept only as far as needed for ordered chaining without subterm-chaining or chaining on equivalence classes. Hence they have considered commutation only abstractly, not for term rewriting.

8 Conclusion

We have presented a general framework for non-symmetric rewriting with arbitrary transitive relations. We think that it provides a new perspective on rewriting. Moreover it allows to specify a completion procedure and can be used as a basis for general chaining systems in automated theorem proving. Compared to the work of Bachmair and Ganzinger, we introduce subterm chaining and congruences; compared to the work of Levy and Agustí, we not only improve and correct their results, we also present them in a more general framework. Our main results can be summarized as follows: (i) We proved commutation theorems both abstractly and over a term algebra, which generalize the Church-Rosser theorem of equational theorem proving modulo an equivalence. (ii) The form of rewrite proofs leads to variable critical pairs. (iii) Completion is based on search and simplification techniques are quite weak. (iv) If C is non-symmetric, a kind of 'directed unification' must eventually be considered. Its applicability is not obvious. We think that the case where C is symmetric is more relevant. (v) If C is symmetric, we can easily reproduce the equational theorems. (vi) and as a conclusion we showed that term rewriting is a theory of reduction and commutation which is not restricted to equations and where normal forms only arise as a side effect for a special case.

Our results can be applied in automated theorem proving to theories, which can be presented by orderings or quasi-orderings in a natural way. A

[11] Commutation properties have been studied earlier by Bachmair and Dershowitz [2], Bellegarde and Lescanne [5], and Geser [9], among others, mostly in the context of termination.

[12] c.f lemma 4.8 of Levy's thesis [14]. Interestingly enough, Bachmair and Ganzinger did not consider this lemma worth proving...

completeness proof of the system for lattice theory proposed by Levy would show its relevance for solving word problems, where equational rewriting fails. We can also imagine applicability to boolean algebras with operators (modal logics), to sort-checking or type-checking, to reasoning in set theory, to Messeguer's rewrite logic, to non-deterministic algebraic specifications [11], and to concurrency in the context of process algebra. In the wide context of deduction we think that non-symmetric rewriting helps to understand the algorithmic properties of tableaux or the sequent calculus, since it can express the property of permutation invariance of deduction steps. But all these possible applications require further investigations.

References

[1] L. Bachmair. *Canonical Equational Proofs.* Birkhäuser, 1991.

[2] L. Bachmair and N. Dershowitz. Commutation, transformation, and termination. In Jörg H. Siekmann, editor, *8th CADE*, LNCS 230, pages 5–20. Springer-Verlag, 1986.

[3] L. Bachmair and H. Ganzinger. Ordered chaining for total orderings. Technical Report MPI-I-93-250, Max-Planck-Institut für Informatik, 1993.

[4] L. Bachmair and H. Ganzinger. Rewrite techniques for transitive relations. Proc. of the 9th Annual IEEE Symposium on Logic in Computer Science, pages 384–393, 1994.

[5] F. Bellegarde and P. Lescanne. Transformation ordering. In H. Ehrig, R. Kowalski, G. Levi, and U. Montanari, editors, *TAPSOFT'87*, volume 249, pages 69–80, 1987.

[6] N. Dershowitz. Termination of rewriting. *J. Symbolic Computation*, 3:69–116, 1987.

[7] N. Dershowitz and J.-P. Jouannaud. Rewrite systems. In J. van Leeuwen et al., editors, *Handbook of Theoretical Computer Science*, volume B, pages 244–320. Elsevier Science Publishers, 1990.

[8] N. Dershowitz and J.-P. Jouannaud. Notations for rewriting. *Bulletin of the European Association of Theoretical Computer Science*, 43:162–172, 1991.

[9] A. Geser. Relative termination. Technical Report Ulmer Informatik-Berichte Nr.91-03, Universität Ulm, Fakultät für Informatik, 1991.

[10] G. Huet. Confluent reductions: Abstract properties and applications to term rewrite systems. *J. ACM*, 27:797–821, 1980.

[11] H. Hußmann. *Nondeterministism in Algebraic Specifications and Algebraic Programs.* Progress in Theoretical Computer Science. Birkhäuser, 1993.

[12] J.-P. Jouannaud and H. Kirchner. Completion of a set of rules modulo a set of equations. *SIAM J. Comput.*, 15:1155–1194, 1986.

[13] J.W. Klop. Term rewriting systems. In S. Abramsky et al., editors, *Handbook of Logic in Computer Science*, volume 2, pages 1–116. Clarendon Press, 1992.

[14] J. Levy. *The Calculus of Refinements: A Formal Specification Model Based on Inclusions.* PhD thesis, Universitat Polytècnica de Catalunya, Departament de Llenguatges i Sistemes Informàtics, 1994.

[15] J. Levy and J. Agustí. Bi-rewriting, a term rewriting technique for monotonic order relations. In C. Kirchner, editor, *Rewriting Techniques and Applications*, number 690 in LNCS, pages 17–31. Springer-Verlag, 1993.

[16] J. Meseguer. Conditional rewriting logic as a unified model of concurrency. *TCS*, 96:73–155, 1992.