Formalized Confluence of Quasi-Decreasing, Strongly Deterministic Conditional TRSs*

Thomas Sternagel and Christian Sternagel

University of Innsbruck, Austria
{thomas,christian}.sternagel@uibk.ac.at

Abstract

We present an Isabelle/HOL formalization of a characterization of confluence for quasi-reductive strongly deterministic conditional term rewrite systems, due to Avenhaus and Loría-Sáenz.

1 Introduction

Already in 1994 Avenhaus and Loría-Sáenz [1] proved a critical pair criterion for deterministic conditional term rewrite systems with extra variables in right-hand sides, provided their rewrite relation is decidable and terminating. We use this criterion in our conditional confluence checker ConCon [6]. In the following we provide a description of our formalization of the conditional critical pair criterion where we strengthened the original result from quasi-reductivity to quasi-decreasingness. This is a first step towards certifying the confluence criterion that a quasi-decreasing and strongly deterministic CTRS is confluent if all of its critical pairs are joinable. The formalization described in this paper is part of a greater effort to formalize all methods employed by ConCon to be able to certify its output.

Contribution. We have formalized Theorem 4.1 from Avenhaus and Loría-Sáenz [1] in Isabelle/HOL [4] as well as strengthened the original theorem from quasi-reductivity to quasi-decreasingness. It is now part of the formal library IsaFoR [7] (the Isabelle Formalization of Rewriting) and freely available online at:

http://cl2-informatik.uibk.ac.at/rewriting/mercurial.cgi/IsaFoR/file/dbc03280d673/thys/Conditional_Rewriting/ALS94.thy

2 Preliminaries

We assume familiarity with the basic notions of (conditional) term rewriting [2, 5], but shortly recapitulate terminology and notation that we use in the remainder. Given an arbitrary binary relation $\to_\alpha$, we write ${}_\alpha\!\leftarrow$, $\to_\alpha^+$, $\to_\alpha^*$ for the *inverse*, the *transitive closure*, and the *reflexive transitive closure* of $\to_\alpha$, respectively. We use $\mathcal{V}(\cdot)$ to denote the set of variables occurring in a given syntactic object, like a term, a pair of terms, a list of terms, etc. The set of terms $\mathcal{T}(\mathcal{F},\mathcal{V})$ over a given signature of function symbols $\mathcal{F}$ and set of variables $\mathcal{V}$ is defined inductively: $x \in \mathcal{T}(\mathcal{F},\mathcal{V})$ for all variables $x \in \mathcal{V}$, and for every n-ary function symbol $f \in \mathcal{F}$ and terms $t_1,\ldots,t_n \in \mathcal{T}(\mathcal{F},\mathcal{V})$ also $f(t_1,\ldots,t_n) \in \mathcal{T}(\mathcal{F},\mathcal{V})$. We say that terms s and t *unify*, written $s \sim t$, if $s\sigma = t\sigma$ for some substitution σ. A substitution σ is *normalized with respect to* $\mathcal{R}$ if $\sigma(x)$ is a normal form with respect to $\to_\mathcal{R}$ for all $x \in \mathcal{V}$. We call a bijective variable substitution $\pi : \mathcal{V} \to \mathcal{V}$ a *variable renaming* or *(variable) permutation*, and denote its inverse by π^-. A term t is *strongly*

*The research described in this paper is supported by FWF (Austrian Science Fund) project P27502.

irreducible with respect to $\mathcal{R}$ if $t\sigma$ is a normal form with respect to $\to_{\mathcal{R}}$ for all normalized substitutions σ. A *strongly deterministic oriented 3-CTRS (SDTRS)* $\mathcal{R}$ is a set of conditional rewrite rules of the shape $\ell \to r \Leftarrow c$ where ℓ and r are terms and c is a possibly empty sequence of pairs of terms $s_1 \approx t_1, \ldots, s_n \approx t_n$. For all rules in $\mathcal{R}$ we have that $\ell \notin \mathcal{V}$, $\mathcal{V}(r) \subseteq \mathcal{V}(\ell, c)$, $\mathcal{V}(s_i) \subseteq \mathcal{V}(\ell, t_1, \ldots, t_{i-1})$ for all $1 \leqslant i \leqslant n$, and t_i is strongly irreducible with respect to $\mathcal{R}$ for all $1 \leqslant i \leqslant n$. We sometimes label rules like $\rho : \ell \to r \Leftarrow c$. For a rule $\rho : \ell \to r \Leftarrow c$ of an SDTRS $\mathcal{R}$ the set of *extra variables* is defined as $\mathcal{EV}(\rho) = \mathcal{V}(c) - \mathcal{V}(\ell)$. The rewrite relation $\to_{\mathcal{R}}$ is the smallest relation $\to$ satisfying $t[\ell\sigma]_p \to t[r\sigma]_p$ whenever $\ell \to r \Leftarrow c$ is a rule in $\mathcal{R}$ and $s\sigma \to_{\mathcal{R}}^* t\sigma$ for all $s \approx t \in c$. Two variable-disjoint variants of rules $\ell_1 \to r_1 \Leftarrow c_1$ and $\ell_2 \to r_2 \Leftarrow c_2$ in $\mathcal{R}$ such that $\ell_1|_p \notin \mathcal{V}$ and $\ell_1|_p\mu = \ell_2\mu$ with most general unifier (mgu) μ, constitute a *conditional overlap*. A conditional overlap that does not result from overlapping two variants of the same rule at the root, gives rise to a *conditional critical pair* (CCP) $r_1\mu \approx r_1[r_2]_p\mu \Leftarrow c_1\mu, c_2\mu$. A CCP $u \approx v \Leftarrow c$ is *joinable* if $u\sigma \downarrow_{\mathcal{R}} v\sigma$ for all substitutions σ such that $s\sigma \to_{\mathcal{R}}^* t\sigma$ for all $s \approx t \in c$. We denote the proper subterm relation by $\rhd$ and define $\succ_{\mathsf{st}} = (\succ \cup \rhd)^+$ for some reduction order $\succ$. Let $\succ$ be a reduction order on $\mathcal{T}(\mathcal{F}, \mathcal{V})$ then an SDTRS $\mathcal{R}$ is *quasi-reductive with respect to* $\succ$ if for every substitution σ and every rule $\ell \to r \Leftarrow s_1 \approx t_1, \ldots, s_n \approx t_n$ in $\mathcal{R}$ we have $s_j\sigma \succeq t_j\sigma$ for $1 \leqslant j \leqslant i$ implies $\ell\sigma \succ_{\mathsf{st}} s_{i+1}\sigma$, and $s_j\sigma \succeq t_j\sigma$ for $1 \leqslant j \leqslant n$ implies $\ell\sigma \succ r\sigma$.[1] On the other hand, an SDTRS $\mathcal{R}$ over signature $\mathcal{F}$ is *quasi-decreasing* if there is a well-founded order $\succ$ on $\mathcal{T}(\mathcal{F}, \mathcal{V})$ such that $\succ = \succ_{\mathsf{st}}$, $\to_{\mathcal{R}} \subseteq \succ$, and for all rules $\ell \to r \Leftarrow s_1 \approx t_1, \ldots, s_n \approx t_n$ in $\mathcal{R}$, all substitutions $\sigma\colon \mathcal{V} \to \mathcal{T}(\mathcal{F}, \mathcal{V})$, and $0 \leqslant i < n$, if $s_j\sigma \to_{\mathcal{R}}^* t_j\sigma$ for all $1 \leqslant j \leqslant i$ then $\ell\sigma \succ s_{\mathrm{i}+1}\sigma$. Quasi-reductivity implies quasi-decreasingness (cf. [5, proof of Lemma 7.2.40]).

3 Confluence of Quasi-Decreasing SDTRSs

The main result from Avenhaus and Loría-Sáenz is the following theorem:

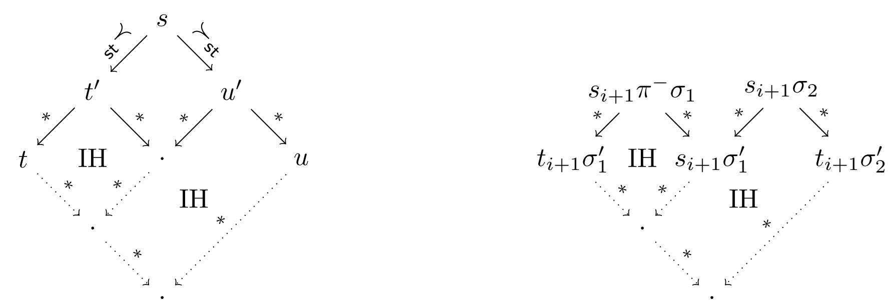
Theorem 1 (Avenhaus and Loría-Sáenz [1, Theorem 4.1])**.** *Let $\mathcal{R}$ be an SDTRS that is quasi-reductive with respect to $\succ$. $\mathcal{R}$ is confluent if and only if all conditional critical pairs are joinable.*

That all critical pairs of any CTRS $\mathcal{R}$ (no need for strong determinism or quasi-reductivity) are joinable if $\mathcal{R}$ is confluent is straight-forward so we will concentrate on the other direction. Our formalization is quite close to the original proof. The good news is: we could not find any errors (besides typos) in the original proof but as is often the case with formalizations there are places where the paper proof is too vague or does not spell out the technical details in favor of readability. A luxury we cannot afford. For example we heavily rely on an earlier formalization of permutations [3] in order to formalize variants of rules up to renaming. Even the change from quasi-reductivity to quasi-decreasingness did not pose a problem.

In the following we will give a description of the main theorem of our formalization and its proof.

Theorem 2. *Let $\mathcal{R}$ be an SDTRS that is quasi-decreasing with respect to $\succ$ and where all conditional critical pairs are joinable, then $\mathcal{R}$ is confluent.*

[1] This is the definition from [1] which differs from the one in [5, Definition 7.2.36] in two respects. First $\succ$ is a reduction order (hence also closed under substitutions; this is needed in the proof of [1, Theorem 4.2]) whereas in Ohlebusch $\succ$ is a well-founded partial order that is closed under contexts. Moreover Ohlebusch allows a signature extension for the substitutions σ which is not part of this definition.



(a) (b)

Figure 1

Proof. Assume that all critical pairs are joinable. We will look at an arbitrary peak $t \;{}_{\mathcal{R}}^{*}\!\leftarrow s \to_{\mathcal{R}}^{*} u$ and prove that $t \downarrow_{\mathcal{R}} u$ by well-founded induction on the relation $\succ_{\mathsf{st}}$. If $s = t$ or $s = u$ then t and u are trivially joinable and we are done. So we may assume that the peak contains at least one step in each direction: $t \;{}_{\mathcal{R}}^{*}\!\leftarrow t' \;{}_{\mathcal{R}}\!\leftarrow s \to_{\mathcal{R}} u' \to_{\mathcal{R}}^{*} u$.

We will proceed to prove that $t' \downarrow_{\mathcal{R}} u'$ then $t \downarrow_{\mathcal{R}} u$ follows by two applications of the induction hypothesis as shown in Figure 1a. Assume that $s = C[\ell_1\sigma_1]_p \to_{\mathcal{R}} C[r_1\sigma_1]_p = t'$ and $s = D[\ell_2\sigma_2]_q \to_{\mathcal{R}} D[r_2\sigma_2]_q = u'$ for rules $\rho_1 : \ell_1 \to r_1 \Leftarrow c_1$ and $\rho_2 : \ell_2 \to r_2 \Leftarrow c_2$ in $\mathcal{R}$, contexts C and D, positions p and q, and substitutions σ_1 and σ_2 such that $u\sigma_1 \to_{\mathcal{R}}^{*} v\sigma_1$ for all $u \approx v \in c_1$ and $u\sigma_2 \to_{\mathcal{R}}^{*} v\sigma_2$ for all $u \approx v \in c_2$. There are three possibilities: $p \parallel q$, $p \leqslant q$, or $q \leqslant p$. In the first case $t' \downarrow_{\mathcal{R}} u'$ holds because the two redexes do not interfere. The other two cases are symmetric and we only consider $p \leqslant q$ here. If $s \rhd s|_p = \ell_1\sigma_1$ then $s \succ_{\mathsf{st}} \ell_1\sigma_1$ (by definition of $\succ_{\mathsf{st}}$) and there is a position r such that $q = pr$ and so we have the peak $r_1\sigma_1 \;{}_{\mathcal{R}}^{*}\!\leftarrow \ell_1\sigma_1 \to_{\mathcal{R}}^{*} \ell_1\sigma_1[r_2\sigma_2]_r$ which is joinable by induction hypothesis. But then the peak $t' = s[r_1\sigma_1]_p \;{}_{\mathcal{R}}^{*}\!\leftarrow s[\ell_1\sigma_1]_p \to_{\mathcal{R}}^{*} s[\ell_1\sigma_1[r_2\sigma_2]_r]_q = u'$ is also joinable (by closure under contexts) and we are done. So we may assume that $p = \epsilon$ and thus $s = \ell_1\sigma_1$. Now, either q is a function position in ℓ_1 or there is a variable position q' in ℓ_1 such that $q' \leqslant q$. In the first case we either have a CCP which is joinable by assumption or we have a root-overlap of variants of the same rule. Then $\rho_1\pi = \rho_2$ for some permutation π. Moreover, $s = \ell_1\sigma_1 = \ell_2\sigma_2$ and we have

$$x\pi^{-}\sigma_1 = x\sigma_2 \text{ for all variables } x \text{ in } \mathcal{V}(\ell_2). \tag{1}$$

We will prove $x\pi^{-}\sigma_1 \downarrow_{\mathcal{R}} x\sigma_2$ for all x in $\mathcal{V}(\rho_2)$. Since $t' = r_1\sigma_1 = r_2\pi^{-}\sigma_1$ and $u' = r_2\sigma_2$ this shows $t' \downarrow_{\mathcal{R}} u'$. Because $\mathcal{R}$ is terminating (by quasi-decreasingness) we may define two normalized substitutions σ'_i such that

$$x\pi^{-}\sigma_1 \xrightarrow[\mathcal{R}]{*} x\sigma'_1 \text{ and } x\sigma_2 \xrightarrow[\mathcal{R}]{*} x\sigma'_2 \text{ for all variables } x. \tag{2}$$

We prove $x\sigma'_1 = x\sigma'_2$ for $x \in \mathcal{EV}(\rho_2)$ by an inner induction on the length of $c_2 = s_1 \approx t_1, \ldots, s_n \approx t_n$. If ρ_2 has no conditions this holds vacuously because there are no extra variables. In the step case the inner induction hypothesis is that $x\sigma'_1 = x\sigma'_2$ for $x \in \mathcal{V}(s_1, t_1, \ldots, s_i, t_i) - \mathcal{V}(\ell_2)$ and we have to show that $x\sigma'_1 = x\sigma'_2$ for $x \in \mathcal{V}(s_1, t_1, \ldots, s_{i+1}, t_{i+1}) - \mathcal{V}(\ell_2)$. If $x \in \mathcal{V}(s_1, t_1, \ldots, s_i, t_i, s_{i+1})$ we are done by the inner induction hypothesis and strong determinism of $\mathcal{R}$. So assume $x \in \mathcal{V}(t_{i+1})$. From strong determinism of $\mathcal{R}$, (1), (2), and the induction hypothesis we have that $y\sigma'_1 = y\sigma'_2$ for all $y \in \mathcal{V}(s_{i+1})$ and thus $s_{i+1}\sigma'_1 = s_{i+1}\sigma'_2$. With this we can find a join between $t_{i+1}\sigma'_1$ and $t_{i+1}\sigma'_2$ by applying the induction hypothesis twice as shown in Figure 1b. Since t_{i+1} is strongly irreducible and σ_1' and σ_2' are normalized, this yields $t_{i+1}\sigma_1' = t_{i+1}\sigma_2'$ and thus $x\sigma_1' = x\sigma_2'$.

We are left with the case that there is a variable position q' in ℓ_1 such that $q = q'r'$ for some position r'. Let x be the variable $\ell_1|_{q'}$. Then $x\sigma_1|_{r'} = \ell_2\sigma_2$, which implies $x\sigma_1 \to_{\mathcal{R}}^* x\sigma_1[r_2\sigma_2]_{r'}$. Now let τ be the substitution such that $\tau(x) = x\sigma_1[r_2\sigma_2]_{r'}$ and $\tau(y) = \sigma_1(y)$ for all $y \neq x$, and τ' some normalization, i.e., $y\tau \to_{\mathcal{R}}^* y\tau'$ for all y. Moreover, note that

$$y\sigma_1 \xrightarrow[\mathcal{R}]{*} y\tau \text{ for all } y. \tag{3}$$

We have $u' = \ell_1\sigma_1[r_2\sigma_2]_q = \ell_1\sigma_1[x\tau]_{q'} \to_{\mathcal{R}}^* \ell_1\tau$, and thus $u' \to_{\mathcal{R}}^* \ell_1\tau'$. From (3) we have $r_1\sigma_1 \to_{\mathcal{R}}^* r_1\tau$ and thus $t' = r_1\sigma_1 \to_{\mathcal{R}}^* r_1\tau'$. Finally, we will show that $\ell_1\tau' \to_{\mathcal{R}} r_1\tau'$, concluding the proof of $t' \downarrow_{\mathcal{R}} u'$. To this end, let $s_i \approx t_i \in c_1$. By (3) and the definition of τ' we obtain $s_i\sigma_1 \to_{\mathcal{R}}^* t_i\sigma_1 \to_{\mathcal{R}}^* t_i\tau'$ and $s_i\sigma_1 \to_{\mathcal{R}}^* s_i\tau'$. But then, by induction hypothesis, $s_i\tau' \downarrow_{\mathcal{R}} t_i\tau'$, and furthermore, since t_i is strongly irreducible, $s_i\tau' \to_{\mathcal{R}}^* t_i\tau'$. ◻

4 Conclusion

Our formalization amounts to approximately 1800 lines of Isabelle. At some points we actually had to use variants of rules where the original proof assumes two rules to be identical. Apart from that the formalization was rather straight-forward. Also the modification from quasi-reductivity to quasi-decreasingness did not pose a problem.

Future Work. Formalizing the conditional critical pair criterion was only the first step. There are two challenges for automation: Checking if a term is strongly irreducible, and checking if a conditional critical pair is joinable. Both of these are undecidable in general. Avenhaus and Loría-Sáenz employ *absolute determinism* [1, Definition 4.2] to tackle strong irreducibility as well as *contextual rewriting* to handle joinability of conditional critical pairs. Then we have a computable overapproximation. We already started to extend our formalization to facilitate absolute determinism as well as contextual rewriting. It remains to provide check functions for CeTA [7] and also the proper certifiable output for ConCon.

Acknowledgments. We thank the Austrian Science Fund (FWF project P27502) for supporting our work. Moreover we would like to thank the anonymous reviewers for useful suggestions.

References

[1] Jürgen Avenhaus and Carlos Loría-Sáenz. On conditional rewrite systems with extra variables and deterministic logic programs. In *Proceedings of the 5th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning*, volume 822 of *Lecture Notes in Computer Science*, pages 215–229. Springer, 1994. doi:10.1007/3-540-58216-9_40.

[2] Franz Baader and Tobias Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.

[3] Nao Hirokawa, Aart Middeldorp, and Christian Sternagel. A new and formalized proof of abstract completion. In *Proceedings of the 5th International Conference on Interactive Theorem Proving*, volume 8558 of *Lecture Notes in Computer Science*, pages 292–307. Springer, 2014. doi:10.1007/978-3-319-08970-6_19.

[4] Tobias Nipkow, Lawrence Charles Paulson, and Makarius Wenzel. *Isabelle/HOL - A Proof Assistant for Higher-Order Logic*, volume 2283 of *Lecture Notes in Computer Science*. Springer, 2002. doi:10.1007/3-540-45949-9.

[5] Enno Ohlebusch. *Advanced Topics in Term Rewriting*. Springer, 2002.

[6] Thomas Sternagel and Aart Middeldorp. Conditional confluence (system description). In *Proceedings of the Joint 25th International Conference on Rewriting Techniques and Applications and 12th International Conference on Typed Lambda Calculi and Applications*, volume 8560 of *Lecture Notes in Computer Science*, pages 456–465. Springer, 2014. doi:10.1007/978-3-319-08918-8_31.

[7] René Thiemann and Christian Sternagel. Certification of termination proofs using CeTA. In *Proceedings of the 22nd International Conference on Theorem Proving in Higher Order Logics*, volume 5674 of *Lecture Notes in Computer Science*, pages 452–468. Springer, 2009. doi:10.1007/978-3-642-03359-9_31.