Certified Ordered Completion[*]

Christian Sternagel and Sarah Winkler

Department of Computer Science
University of Innsbruck, Innsbruck, Austria
{christian.sternagel|sarah.winkler}@uibk.ac.at

Abstract

On the one hand, ordered completion is a fundamental technique in equational theorem proving that is employed by automated tools. On the other hand, their complexity makes such tools inherently error prone. As a remedy to this situation we give an Isabelle/HOL formalization of ordered rewriting and completion that comes with a formally verified certifier for ordered completion proofs. By validating generated proof certificates, our certifier increases the reliability of ordered completion tools.

1 Introduction

Completion has evolved as a fundamental technique in automated reasoning since the groundbreaking work by Knuth and Bendix [5]. Its goal is to transform a given set of equations into a terminating and confluent term rewrite system that induces the same equational theory and can thus be used to decide equivalence with respect to the initial set of equations. Since the original procedure can fail if unorientable equations are encountered, ordered completion was developed to remedy this shortcoming [2]. The systems generated by ordered completion tools are in general only ground confluent, but this turns out to be sufficient for practical applications like refutational theorem proving.

Consider for example the following equational system $\mathcal{E}_0$ which the tool MædMax [10]

$$\begin{array}{ccc} x \div y \approx \langle \mathsf{0}, y\rangle & x \div y \approx \langle \mathsf{s}(q), r\rangle & x - \mathsf{0} \approx x \\ \mathsf{0} - y \approx \mathsf{0} & \mathsf{s}(x) - \mathsf{s}(y) \approx x - y & \mathsf{s}(x) > \mathsf{s}(y) \approx x > y \\ \mathsf{s}(x) > \mathsf{0} \approx \mathsf{true} & \mathsf{s}(x) \leq \mathsf{s}(y) \approx x \leq y & \mathsf{0} \leq x \approx \mathsf{true} \end{array}$$

transforms by ordered completion into the following rules $\mathcal{R}$ ($\to$) and equations $\mathcal{E}$ ($\approx$):

$$\begin{array}{cccc} x - \mathsf{0} \to x & \mathsf{0} - x \to \mathsf{0} & \mathsf{s}(x) - \mathsf{s}(y) \to x - y & x \div y \to \langle \mathsf{0}, y\rangle \\ \mathsf{0} \leq x \to \mathsf{true} & \mathsf{s}(x) \leq \mathsf{s}(y) \to x \leq y & \mathsf{s}(x) > \mathsf{0} \to \mathsf{true} & \\ \mathsf{s}(x) > \mathsf{s}(y) \to x > y & \langle \mathsf{s}(x), y\rangle \approx \langle \mathsf{s}(q), r\rangle & \langle \mathsf{s}(q), r\rangle \approx \langle \mathsf{0}, y\rangle & \langle \mathsf{0}, x\rangle \approx \langle \mathsf{0}, y\rangle \end{array}$$

This system can be used to decide a given ground equation by checking whether the terms' unique normal forms (with respect to ordered rewriting) are equal.

Such ground complete systems are useful for other tools, like ConCon [9]—a tool for automatically proving confluence of conditional term rewrite systems—which employs ordered completion for proving infeasibility of conditional critical pairs. In fact, $\mathcal{E}_0$ from our initial example is the equational system that ConCon derives from Cops #361 for that purpose. The latter models division with remainder, though the transformation performed by ConCon creates some equations which do not fit into this semantics but are required to decide confluence.

[*] This work is supported by the Austrian Science Fund (FWF): projects T789 and P27502.

However, automated tools like ConCon and MædMax are complex and highly optimized. The produced proofs often comprise hundreds of equations and thousands of steps. Hence care should be taken to trust the output of such tools.

To improve this situation we follow a two-staged certification approach and first (1) add the relevant concepts and results to a formal library, and then (2) use code generation to obtain a trusted certifier. More specifically, our contributions are as follows:

- Regarding stage (1), we extended the ***Isa**belle **F**ormalization **o**f **R**ewriting*[1] (IsaFoR) by ordered rewriting and a generalization of the ordered completion calculus oKB [2], and proved the latter correct for finite runs using ground-total reduction orders (Section 3). Moreover, we established ground-totality of the lexicographic path order and the Knuth-Bendix order.

- With respect to stage (2), we extended the XML-based *certification problem format* (CPF for short) [8] by certificates comprising the initial equations, the resulting system along with a reduction order, and a stepwise derivation of the latter from the former. We then formalized check functions that verify that the supplied derivation corresponds to a valid oKB run whose final state matches the resulting system (Section 4). As a result CeTA (the certifier accompanying IsaFoR) can now certify ordered completion proofs produced by the tool MædMax [10].

2 Preliminaries

In the sequel we use standard notation from term rewriting [1]. We consider the *set of all terms* $\mathcal{T}(\mathcal{F},\mathcal{V})$ over a signature $\mathcal{F}$ and an infinite set of variables $\mathcal{V}$, while $\mathcal{T}(\mathcal{F})$ denotes the *set of all ground terms*. A *substitution* σ is a mapping from variables to terms. As usual, we write $t\sigma$ for the *application* of σ to a term t. A *variable permutation* (or *renaming*) π is a bijective substitution such that $\pi(x) \in \mathcal{V}$ for all $x \in \mathcal{V}$. For an equational system (ES) $\mathcal{E}$ we write $\mathcal{E}^{\leftrightarrow}$ to denote its symmetric closure $\mathcal{E} \cup \{t \approx s \mid s \approx t \in \mathcal{E}\}$. For a reduction order $>$ and an ES $\mathcal{E}$, the term rewrite system (TRS) $\mathcal{E}^{>}$ consists of all rules $s\sigma \to t\sigma$ such that $s \approx t \in \mathcal{E}$ and $s\sigma > t\sigma$.

Given a reduction order $>$, an *extended overlap* is given by two variable-disjoint variants $\ell_1 \approx r_1$ and $\ell_2 \approx r_2$ of equations in $\mathcal{E}^{\leftrightarrow}$ such that $p \in \mathcal{P}\mathsf{os}_{\mathcal{F}}(\ell_2)$ and ℓ_1 and $\ell_2|_p$ are unifiable with most general unifier μ. An extended overlap which in addition satisfies $r_1\mu \not> \ell_1\mu$ and $r_2\mu \not> \ell_2\mu$ gives rise to the *extended critical pair* $\ell_2[r_1]_p\mu \approx r_2\mu$. The set $\mathrm{CP}_{>}(\mathcal{E})$ consists of all extended critical pairs among equations in $\mathcal{E}$. A TRS $\mathcal{R}$ is *(ground) complete* if it is terminating and confluent (on ground terms). Finally, we say that a TRS $\mathcal{R}$ is a presentation of an ES $\mathcal{E}$, whenever $\leftrightarrow_{\mathcal{E}}^{*} = \leftrightarrow_{\mathcal{R}}^{*}$.

3 Formalizing Ordered Completion

We consider the following definition of ordered completion.

Definition 1 (Ordered Completion)**.** The inference system oKB of ordered completion operates on pairs $(\mathcal{E},\mathcal{R})$ of equations $\mathcal{E}$ and rules $\mathcal{R}$ over a common signature $\mathcal{F}$. It consists of the following inference rules, where $\mathcal{S}$ abbreviates $\mathcal{R} \cup \mathcal{E}^{>}$ and π is a renaming.

[1] http://cl-informatik.uibk.ac.at/isafor

deduce $$\frac{\mathcal{E},\mathcal{R}}{\mathcal{E}\cup\{s\pi\approx t\pi\},\mathcal{R}} \quad \text{if } s \xleftarrow[\mathcal{R}\cup\mathcal{E}]{} \cdot \xrightarrow[\mathcal{R}\cup\mathcal{E}]{} t$$

compose $$\frac{\mathcal{E},\mathcal{R}\uplus\{s\to t\}}{\mathcal{E},\mathcal{R}\cup\{s\pi\to u\pi\}} \quad \text{if } t\to_{\mathcal{S}} u$$

orient $$\frac{\mathcal{E}\uplus\{s\approx t\},\mathcal{R}}{\mathcal{E},\mathcal{R}\cup\{s\pi\to t\pi\}} \quad \text{if } s>t$$ $$\frac{\mathcal{E}\uplus\{s\approx t\},\mathcal{R}}{\mathcal{E},\mathcal{R}\cup\{t\pi\to s\pi\}} \quad \text{if } t>s$$

simplify $$\frac{\mathcal{E}\uplus\{s\approx t\},\mathcal{R}}{\mathcal{E}\cup\{u\pi\approx t\pi\},\mathcal{R}} \quad \text{if } s\to_{\mathcal{S}} u$$ $$\frac{\mathcal{E}\uplus\{s\approx t\},\mathcal{R}}{\mathcal{E}\cup\{s\pi\approx u\pi\},\mathcal{R}} \quad \text{if } t\to_{\mathcal{S}} u$$

delete $$\frac{\mathcal{E}\uplus\{s\approx s\},\mathcal{R}}{\mathcal{E},\mathcal{R}}$$

collapse $$\frac{\mathcal{E},\mathcal{R}\uplus\{t\to s\}}{\mathcal{E}\cup\{u\pi\approx s\pi\},\mathcal{R}} \quad \text{if } t\to_{\mathcal{S}} u$$

We write $(\mathcal{E},\mathcal{R})\vdash(\mathcal{E}',\mathcal{R}')$ if $(\mathcal{E}',\mathcal{R}')$ is obtained from $(\mathcal{E},\mathcal{R})$ by employing one of the above inference rules. A finite sequence of inferences $(\mathcal{E}_0,\varnothing)\vdash(\mathcal{E}_1,\mathcal{R}_1)\vdash\cdots\vdash(\mathcal{E}_n,\mathcal{R}_n)$ is called a *run*. Definition 1 differs from the original formulation of ordered completion [2] in two ways. First, collapse and simplify do not require an encompassment condition. This omission is possible since we only consider *finite* runs. Second, we allow variants of rules and equations to be added. This relaxation tremendously simplifies certificate generation in tools, where facts are renamed upon generation to avoid the maintenance and processing of many renamed versions of one equation.

The following inclusions express straightforward properties of oKB.

Lemma 1. *If $(\mathcal{E},\mathcal{R})\vdash^*(\mathcal{E}',\mathcal{R}')$ then $\mathcal{R}\subseteq{>}$ implies $\mathcal{R}'\subseteq{>}$.* □

Lemma 2. *If $(\mathcal{E},\mathcal{R})\vdash^*(\mathcal{E}',\mathcal{R}')$ then the conversion equivalence $\leftrightarrow^*_{\mathcal{E}\cup\mathcal{R}}=\leftrightarrow^*_{\mathcal{E}'\cup\mathcal{R}'}$ holds.* □

The following abstract result is the key ingredient to our proof of ground completeness.

Lemma 3. *Let $\mathcal{E}$ be an ES and $>$ a reduction order such that $s>t$ or $t\approx s\in\mathcal{E}$ holds for all $s\approx t\in\mathcal{E}$. If for all $s\approx t\in\mathrm{CP}_>(\mathcal{E})$ we have $s\downarrow_{\mathcal{E}^>}t$ or there is some $s'\approx t'\in\mathcal{E}^\leftrightarrow$ such that $s\approx t=(s'\approx t')\sigma$ then $\mathcal{E}^>$ is ground complete.* □

In combination, Lemmas 1, 2, and 3 allow us to obtain our main correctness result: acceptance of a certificate by our check function implies that $\mathcal{R}\cup\mathcal{E}^>$ is a ground complete presentation of $\mathcal{E}_0$. For simplicity's sake, we give only the corresponding high-level result (that is, not mentioning our concrete implementation):

Theorem 1. *Suppose $(\mathcal{E}_0,\varnothing)\vdash^*(\mathcal{E},\mathcal{R})$ was obtained using a ground-total reduction order $>$ with minimal constant c and for all $s\approx t\in\mathrm{CP}_>(\mathcal{E}^\leftrightarrow\cup\mathcal{R})$ either $s\downarrow_{\mathcal{R}\cup\mathcal{E}^>}t$, or $s\approx t=(s'\approx t')\sigma$ for some $s'\approx t'\in\mathcal{E}^\leftrightarrow$. Then $\leftrightarrow^*_{\mathcal{E}_0}=\leftrightarrow^*_{\mathcal{R}\cup\mathcal{E}}$ and $\mathcal{R}\cup\mathcal{E}^>$ is ground complete.* □

This result employs the following sufficient condition for ground completeness: all critical pairs are joinable or instances of equations already present. In fact, this is not a necessary condition. Martin and Nipkow [6] gave examples of ground confluent systems that do not satisfy this condition, and presented a stronger criterion. However, ground confluence is known to be undecidable even for terminating TRSs [4], hence no complete criterion can be implemented.

Ground-total reduction orders. Ground confluence crucially relies on ground-total reduction orders. Our IsaFoR proofs of the following results follow the standard textbook approach [1].

Lemma 4. *If $>$ is a total precedence on $\mathcal{F}$ then $>_{\mathsf{lpo}}$ is total on $\mathcal{T}(\mathcal{F})$.* □

Lemma 5. *If $>$ is a total precedence on $\mathcal{F}$ then $>_{\mathsf{kbo}}$ is total on $\mathcal{T}(\mathcal{F})$.* □

In addition, we proved that for any given KBO $>_{\mathsf{kbo}}$ (LPO $>_{\mathsf{lpo}}$) defined over a total precedence $>$ there exists a minimal constant c such that $t\geqslant_{\mathsf{kbo}}c$ ($t\geqslant_{\mathsf{lpo}}c$) holds for all $t\in\mathcal{T}(\mathcal{F})$.

4 Checking Ordered Completion Proofs

While CeTA has supported certification of standard completion for quite some time [7], certification of ordered completion proofs is considerably more intricate. For standard completion, the certificate contains the initial set of equations $\mathcal{E}_0$, the resulting TRS $\mathcal{R}$ together with a termination proof, and stepwise $\mathcal{E}_0$-conversions from ℓ to r for each rule $\ell \to r \in \mathcal{R}$. The certifier first checks the termination proof to guarantee termination of $\mathcal{R}$. This allows us to establish confluence of $\mathcal{R}$ by ensuring that all critical peaks are joinable. At this point it is easy to verify $\leftrightarrow^*_{\mathcal{E}_0} \subseteq \leftrightarrow^*_{\mathcal{R}}$: for each equation $s \approx t \in \mathcal{E}_0$ compute the $\mathcal{R}$-normal forms of s and t and check for syntactic equality. The converse inclusion $\leftrightarrow^*_{\mathcal{R}} \subseteq \leftrightarrow^*_{\mathcal{E}_0}$ is taken care of by the provided $\mathcal{E}_0$-conversions. Overall, we obtain that $\mathcal{R}$ is a complete presentation of $\mathcal{E}_0$ without mentioning a specific inference system for completion.

Unfortunately, the same approach does not work for ordered completion: The inclusion $\leftrightarrow^*_{\mathcal{E}_0} \subseteq \leftrightarrow^*_{\mathcal{R}\cup\mathcal{E}}$ cannot be established by rewriting equations in $\mathcal{E}_0$ to normal form, since they may contain variables but $\mathcal{R} \cup \mathcal{E}^{>}$ is only ground confluent. Therefore, we instead ask for certificates that contain the input equalities $\mathcal{E}_0$, the resulting equations and rules $(\mathcal{E}, \mathcal{R})$, the reduction order $>$, and a sequence of inference steps according to Definition 1. A valid certificate ensures (by Lemma 2) that the relations $\leftrightarrow^*_{\mathcal{E}_0}$ and $\leftrightarrow^*_{\mathcal{R}\cup\mathcal{E}}$ coincide.

The certificate corresponding to our initial example contains the equations $\mathcal{E}_0$, the resulting system $(\mathcal{E}, \mathcal{R})$, and the reduction order $>_{\mathsf{kbo}}$ with precedence $> \; > \mathsf{s} > \leq \; > \mathsf{true} > - > \div > \langle\cdot,\cdot\rangle > \mathsf{0}$, $w_0 = 1$, and $w(\mathsf{0}) = 2$, $w(\div) = w(\mathsf{true}) = w(\mathsf{s}) = 1$, and all other symbols having weight 0. In addition, a sequence of inference steps explains how $(\mathcal{E}, \mathcal{R})$ is obtained from $\mathcal{E}_0$:

$\mathsf{simplify}_{\mathsf{left}}$	$x \div y \approx \langle \mathsf{s}(q), r\rangle$ to $\langle \mathsf{0}, y\rangle \approx \langle \mathsf{s}(q), r\rangle$
deduce	$\langle \mathsf{0}, x\rangle \leftarrow \langle \mathsf{s}(u), v\rangle \to \langle \mathsf{0}, y\rangle$
deduce	$\langle \mathsf{s}(x), y\rangle \leftarrow \langle \mathsf{0}, u\rangle \to \langle \mathsf{s}(q), r\rangle$
deduce	$x > y \leftarrow \mathsf{s}(x) > \mathsf{s}(y) \to \mathsf{s}(\mathsf{s}(x)) > \mathsf{s}(\mathsf{s}(y))$
deduce	$\mathsf{s}(\mathsf{s}(x)) > \mathsf{s}(\mathsf{0}) \leftarrow \mathsf{s}(x) > \mathsf{0} \to \mathsf{true}$
$\mathsf{orient}_{\mathsf{rl}}$	$\mathsf{0} \leq x \to \mathsf{true}$
$\mathsf{orient}_{\mathsf{lr}}$	$\mathsf{s}(\mathsf{s}(x)) > \mathsf{s}(\mathsf{0}) \to \mathsf{true}$
$\mathsf{orient}_{\mathsf{rl}}$	$\mathsf{s}(x) > \mathsf{s}(y) \to x > y$
$\mathsf{orient}_{\mathsf{lr}}$	$\mathsf{s}(x) > \mathsf{0} \to \mathsf{true}$
$\mathsf{orient}_{\mathsf{rl}}$	$\mathsf{s}(\mathsf{s}(x)) > \mathsf{s}(\mathsf{s}(y)) \to x > y$
$\mathsf{orient}_{\mathsf{rl}}$	$x - \mathsf{0} \to x$
$\mathsf{orient}_{\mathsf{lr}}$	$x \div y \to \langle \mathsf{0}, y\rangle$
$\mathsf{orient}_{\mathsf{rl}}$	$\mathsf{s}(x) - \mathsf{s}(y) \to x - y$
$\mathsf{orient}_{\mathsf{rl}}$	$\mathsf{0} - x \to \mathsf{0}$
$\mathsf{orient}_{\mathsf{rl}}$	$\mathsf{s}(x) \leq \mathsf{s}(y) \to x \leq y$
$\mathsf{collapse}$	$\mathsf{s}(\mathsf{s}(x)) > \mathsf{s}(\mathsf{s}(y)) \to x > y$ to $\mathsf{s}(x) > \mathsf{s}(y) \approx x > y$
$\mathsf{simplify}_{\mathsf{left}}$	$\mathsf{s}(x) > \mathsf{s}(y) \approx x > y$ to $x > y \approx x > y$
$\mathsf{collapse}$	$\mathsf{s}(\mathsf{s}(x)) > \mathsf{s}(\mathsf{0}) \to \mathsf{true}$ to $\mathsf{s}(x) > \mathsf{0} \approx \mathsf{true}$
$\mathsf{simplify}_{\mathsf{left}}$	$\mathsf{s}(x) > \mathsf{0} \approx \mathsf{true}$ to $\mathsf{true} \approx \mathsf{true}$
delete	$x > y \approx x > y$
delete	$\mathsf{true} \approx \mathsf{true}$

Given such a certificate, CeTA checks that the provided sequence of inferences forms a run $(\mathcal{E}_0\pi, \varnothing) \vdash^* (\mathcal{E}, \mathcal{R})$ for some renaming π. Verifying the validity of individual inferences involves checking side conditions such as orientability of a term pair in an orient step with respect to the given reduction order. Then it is checked that $\mathcal{R} \cup \mathcal{E}^{>}$ is ground confluent according to the criterion of Theorem 1. Finally, it is ensured that the given reduction order $>$ has a total precedence (and is admissible, in the case of KBO). As usual in CeTA, error messages are printed if one of these checks fails, pointing out the reason for the proof being rejected.

5 Conclusion

We presented our formalization of ordered completion in IsaFoR, which enables CeTA (starting with version 2.33) to certify ordered completion proofs. To the best of our knowledge, CeTA thus constitutes the first formally verified certifier for ordered completion.

Together with Hirokawa and Middeldorp we reported on another Isabelle/HOL formalization of ordered completion [3]. The main difference to our current work is that this other formalization is based on a more restrictive inference system of ordered completion that also covers infinite runs, while we restrict to finite runs in the interest of certification. Indeed every finite run akin to [3, Definition 18] is also a run according to Definition 1, while the inference sequence in our running example is not possible in the former setting.

As future work, we plan to add more powerful criteria for ground confluence to IsaFoR, and support equational disproofs based on ground complete systems in CeTA. To that end, it would be useful to also support narrowing in CeTA. Certified equational disproofs could in turn be used to certify confluence proofs by ConCon which rely on infeasibility of conditional critical pairs.

References

[1] F. Baader and T. Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998. doi:10.1017/CBO9781139172752.

[2] L. Bachmair, N. Dershowitz, and D. A. Plaisted. Completion without failure. In H. A. Kaci and M. Nivat, editors, *Resolution of Equations in Algebraic Structures*, volume 2 of *Rewriting Techniques*, pages 1–30. Academic Press, 1989. doi:10.1016/B978-0-12-046371-8.50007-9.

[3] N. Hirokawa, A. Middeldorp, C. Sternagel, and S. Winkler. Infinite runs in abstract completion. In *Proc. 2nd FSCD*, volume 84 of *LIPIcs*, pages 19:1–19:16, 2017. doi:10.4230/LIPIcs.FSCD.2017.19.

[4] D. Kapur, P. Narendran, and F. Otto. On ground-confluence of term rewriting systems. *Inf. Comput*, 86(1):14–31, 1990. doi:10.1016/0890-5401(90)90023-B.

[5] D. Knuth and P. Bendix. Simple word problems in universal algebras. In J. Leech, editor, *Computational Problems in Abstract Algebra*, pages 263–297. Pergamon Press, 1970. doi:10.1016/B978-0-08-012975-4.

[6] U. Martin and T. Nipkow. Ordered Rewriting and Confluence. In *Proc. 10th CADE*, volume 449 of *LNCS*, pages 366–380, 1990. doi:10.1007/3-540-52885-7_100.

[7] C. Sternagel and R. Thiemann. Formalizing Knuth-Bendix orders and Knuth-Bendix completion. In *Proc. 24th RTA*, volume 21 of *LIPIcs*, pages 287–302, 2013. doi:10.4230/LIPIcs.RTA.2013.287.

[8] C. Sternagel and R. Thiemann. The certification problem format. In *Proc. 11th UITP*, volume 167 of *EPTCS*, pages 61–72, 2014. doi:10.4204/EPTCS.167.8.

[9] T. Sternagel and A. Middeldorp. Conditional confluence (system description). In *Proc. RTA/TLCA 2014*, volume 8560 of *LNCS*, pages 456–465, 2014. doi:10.1007/978-3-319-08918-8_31.

[10] S. Winkler and G. Moser. Maedmax: A maximal ordered completion tool. In *Proc. 9th IJCAR*, 2018. To appear.