Certification extends Termination Techniques

Christian Sternagel* (`christian.sternagel@uibk.ac.at`), University of Innsbruck, Austria
René Thiemann (`rene.thiemann@uibk.ac.at`), University of Innsbruck, Austria

1   Introduction

Termination provers for term rewrite systems (TRSs) became more and more powerful in the last years. One reason is that a proof of termination no longer is just some reduction order which contains the rewrite relation of the TRS. Currently, most provers combine basic termination techniques in a flexible way using the dependency pair framework (DP framework) or rule removal. Hence, a termination proof is a tree where at each node a specific technique is applied. Therefore, instead of just stating the precedence of some lexicographic path order or giving some polynomial interpretation, current termination provers return proof trees consisting of many different techniques and reaching sizes of several megabytes. Thus, it would be too much work to check by hand whether these trees really form a valid proof. (Also, checking by hand does not provide a very high degree of confidence.)

It is regularly demonstrated that we cannot blindly trust in the output of termination provers. Every now and then, some termination prover delivers a faulty proof. Most often, this is only detected if there is another prover giving a contradicting answer on the same problem. To improve this situation, three systems have been developed over the last few years: CiME/Coccinelle [5, 6], Rainbow/CoLoR [4], and CeTA/IsaFoR [16]. These systems either certify or reject a given termination proof. Here, Coccinelle and CoLoR are libraries on rewriting for Coq (`http://coq.inria.fr`) and IsaFoR is our library on rewriting for Isabelle [15]. (Throughout this paper we just write Isabelle whenever we refer to Isabelle/HOL.) And indeed, using certifiers several bugs have been detected. For example, in the termination competition of the last year (November 2009), at least eight faulty proofs were spotted by certifiers.[1] (Caused by three different bugs, all of which were most likely due to some output error.)

Although many termination techniques have already been formalized—CeTA can certify termination or nontermination proofs for 1522 out of the 2132 TRSs from the TPDB version 7.0.2 which is over 70 % of the whole database—there are still several techniques that have not been formalized. So, clearly there are termination proofs that are produced by some termination tool where the certifiers have to become more powerful.

However, a similar situation also occurs in the other direction. We have formalized termination techniques in a more general setting as they have been introduced. Hence, currently we can certify proofs using techniques that no termination tool supports so far. In this paper we shortly present two of these formalizations.

(a) Polynomial orders with negative constants [12].

(b) Arctic termination [13].

Here, for (a) we were able to lift the result from the naturals as introduced in [12] to an arbitrary carrier, including matrices (Sec. 3). For (b) we have generalized the arctic semiring and the arctic semiring below zero into one semiring which subsumes both existing approaches and extends them to the rationals (Sec. 4).

Note that all the proofs that are presented (or omitted) in the following, have been formalized in our Isabelle library IsaFoR. This library and the executable certifier CeTA are available at CeTA's website:

---

[1]Result IDs `http://termcomp.uibk.ac.at/termcomp/competition/resultDetail.seam?resultId=135160`, 136252, 136278, 136365, 136378, 136499, 137163, and 137465

2 Preliminaries

We assume familiarity with term rewriting [2]. Still, we recall the most important notions that are used later on. A *term t* over a set of *variables* $\mathcal{V}$ and a set of *function symbols* $\mathcal{F}$ is either a variable $x \in \mathcal{V}$ or an *n*-ary function symbol $f \in \mathcal{F}$ applied to *n* argument terms $f(t_1, \ldots, t_n)$.

A *rewrite rule* is a pair of terms $\ell \to r$ and a TRS $\mathcal{R}$ is a set of rewrite rules. The *rewrite relation (induced by $\mathcal{R}$)* $\to_{\mathcal{R}}$ is the closure under substitutions and under contexts of $\mathcal{R}$, i.e., $s \to_{\mathcal{R}} t$ iff there is a context C, a rewrite rule $\ell \to r \in \mathcal{R}$, and a substitution σ such that $s = C[\ell\sigma]$ and $t = C[r\sigma]$. A TRS $\mathcal{R}$ is terminating, written $\mathsf{SN}(\mathcal{R})$, if there is no infinite derivation $t_1 \to_{\mathcal{R}} t_2 \to_{\mathcal{R}} t_3 \to_{\mathcal{R}} \cdots$.

3 Polynomial Orders with Negative Constants

Polynomial orders [14] are a well-known technique to prove termination. They are an instance of the termination technique of well-founded monotone algebras. Such algebras can be used for all termination techniques that rely on *reduction pairs* [1]. Here, a reduction pair consists of two partial orders $(\succsim, \succ)$ where $\succsim$ and $\succ$ are stable, $\succsim$ is reflexive and monotone, $\succ$ is well-founded, and $\succsim$ is compatible to $\succ$, i.e., $\succsim \circ \succ \subseteq \succ$. If additionally $\succ$ is monotone, then we call $(\succsim, \succ)$ a *monotone* reduction pair.

It is well-known that reduction pairs can be used for proving termination of TRSs within the DP framework [1, 10, 11]. Moreover, monotone reduction pairs can be used for direct termination proofs or rule removal [3, 9, 14].

To formalize polynomial orders, we first assume some semiring over which the polynomials are built.

Definition 1. *A structure* $(\mathcal{U}, \oplus, \odot, \underline{0}, \underline{1})$ *with universe* $\mathcal{U}$*, two binary operation* $\oplus$ *and* $\odot$ *on* $\mathcal{U}$*, and with* $\underline{0}, \underline{1} \in \mathcal{U}$ *is a* semiring with one-element *iff*

- $\oplus$ *and* $\odot$ *are associative and* $\oplus$ *is commutative*

- $\underline{0} \neq \underline{1}$*,* $\underline{0}$ *and* $\underline{1}$ *are neutral elements w.r.t.* $\oplus$ *and* $\odot$*, respectively, and* $\underline{0} \odot x = x \odot \underline{0} = \underline{0}$

- $\odot$ *distributes over* $\oplus$*:* $x \odot (y \oplus z) = x \odot y \oplus x \odot z$ *and* $(x \oplus y) \odot z = x \odot z \oplus y \odot z$

To obtain polynomial orders, we assume a strict and a non-strict order. Moreover, we demand the existence of a unary predicate mono where $\mathsf{mono}(x)$ indicates that multiplication with x is monotone w.r.t. the strict order.

Definition 2. *A structure* $(\mathcal{U}, \oplus, \odot, \underline{0}, \underline{1}, \geq, >, \mathsf{mono})$ *is an* ordered semiring *iff* $(\mathcal{U}, \oplus, \odot, \underline{0}, \underline{1})$ *is a semiring with one-element and additionally:*

- $\geq$ *is reflexive and transitive;* $>$ *and* $\geq$ *are compatible:* $> \circ \geq\, \subseteq\, >$ *and* $\geq \circ >\, \subseteq\, >$

- $\underline{1} \geq \underline{0}$ *and* $\mathsf{mono}(\underline{1})$

- $\oplus$ *is left-monotone w.r.t.* $\geq$*: if* $x \geq y$ *then* $x \oplus z \geq y \oplus z$

- $\oplus$ *is left-monotone w.r.t.* $>$*: if* $x > y$ *then* $x \oplus z > y \oplus z$

- $\odot$ *is left-monotone w.r.t.* $\geq$*: if* $x \geq y$ *and* $z \geq \underline{0}$ *then* $x \odot z \geq y \odot z$*;* $\odot$ *is right-monotone w.r.t.* $\geq$

- $\odot$ *is right-monotone w.r.t.* $>$*: if* $\mathsf{mono}(x)$*,* $x \geq \underline{0}$*, and* $y > z$ *then* $x \odot y > x \odot z$

- $\{(x, y) \mid x > y \wedge y \geq \underline{0}\}$ *is well-founded*

Note that using the approach of well-founded monotone algebras, every interpretation of the function

symbols over some ordered semiring gives rise to a strict ($\succ$) and a non-strict ($\succsim$) order on terms. For example, for a polynomial interpretation $\mathcal{P}ol$ we define $s \succ_{\mathcal{P}ol} t$ iff $[s] > [t]$, and $s \succsim_{\mathcal{P}ol} t$ iff $[s] \geq [t]$ where $[s]$ is the homeomorphic extension of $\mathcal{P}ol$ to terms.

Theorem 3. *Let $\mathcal{P}ol$ be a polynomial interpretation over an ordered semiring $(\mathcal{U}, \oplus, \odot, \underline{0}, \underline{1}, \geq, >, \mathsf{mono})$ where $[f](x_1, \ldots, x_n) = f_0 \oplus f_1 \odot x_1 \oplus \cdots \oplus f_n \odot x_n$ and $f_i \geq \underline{0}$ for all $0 \leq i \leq n$ and every n-ary symbol f. Then $(\succsim_{\mathcal{P}ol}, \succ_{\mathcal{P}ol})$ is a reduction pair. If moreover, $\mathsf{mono}(f_i)$ for all $1 \leq i \leq n$ then $(\succsim_{\mathcal{P}ol}, \succ_{\mathcal{P}ol})$ is a monotone reduction pair.*

Example 4 (Ordered Semirings). *$(\mathbb{N}, +, \cdot, 0, 1, \geq, >, \geq 1)$, $(\mathbb{Z}, +, \cdot, 0, 1, \geq, >, \geq 1)$, and $(\mathbb{Q}, +, \cdot, 0, 1, \geq, >_\delta, \geq 1)$ are ordered semirings. In the last case, we assume a fixed rational number δ with $0 < \delta$, and where $>_\delta$ is defined by $x >_\delta y$ iff $x - y \geq \delta$.*

To formalize matrix-interpretations [8], we followed the approach of [7] and used a domain with an additional strict-dimension and where the elements are matrices—instead of vectors as in [8]. In detail, we have proven that if $0 < sd \leq n$ and $(\mathcal{U}, \oplus, \odot, \underline{0}, \underline{1}, \geq, >, \mathsf{mono})$ is an ordered semiring, then $(\mathcal{U}^{n \times n}, \oplus^{n \times n}, \odot^{n \times n}, \underline{0}^{n \times n}, \underline{1}^{n \times n}, \geq^{n \times n}, >_{sd}^{n \times n}, \mathsf{mono}_{sd}^{n \times n})$ is also an ordered semiring where all operations and constants are lifted to work on n-dimensional matrices, with the strict-dimension sd. Here, $\geq^{n \times n}$ compares the arguments component-wise, and $M >_{sd}^{n \times n} M'$ iff $M \geq^{n \times n} M'$ and at least one entry in the upper-left $sd \times sd$-submatrix is strictly decreasing w.r.t. $>$. Moreover, $\mathsf{mono}_{sd}^{n \times n}$ demands that for every column in the upper-left $sd \times sd$-submatrix there is at least one monotone entry.

As observed in [7], choosing $sd = 1$, is comparable to the classic definition of matrix-interpretations. Choosing $sd = n$, is always best if one does not require monotonic reduction pairs. However, to ensure monotonicity also a small value of sd might be attractive.

To lift the requirement in Thm. 3 that all f_i have to be at least $\underline{0}$, in [12], polynomial orders with negative constants have been introduced. There, the constant part can be arbitrary but the interpretation of a function is always wrapped into a $\max(\underline{0}, \cdot)$ operation to ensure well-foundedness. This complicates the comparison of terms, as the resulting interpretations are not pure polynomials anymore, but also contain the $\max$-operator. To this end, approximations $[\cdot]_{left}$ and $[\cdot]_{right}$ have been introduced which interpret terms by polynomials without $\max$, such that $[s]_{left} \leq [s] \leq [s]_{right}$.

However, the existing approximations are unsound if generalized naively. For example, in the case where the constant part is negative, it is removed. This works fine for the integers and the rationals, but not for matrices, as here some parts of the matrix may be negative, but other parts can also be positive and thus, cannot be removed. Thus, we formalized the following approximations which are equivalent to those of [12], but also work for matrices:

Definition 5. *Let $\mathsf{cp}(\cdot)$ be the constant part and $\mathsf{ncp}(\cdot)$ be the non-constant part of a polynomial.*

$$[x]_{left} = [x]_{right} = x$$

$$[f(t_1, \ldots, t_n)]_{left} = \begin{cases} \max(\underline{0}, \mathsf{cp}(p_{left})) & \text{if } \mathsf{ncp}(p_{left}) = \underline{0} \\ p_{left} & \text{otherwise} \end{cases}$$

$$[f(t_1, \ldots, t_n)]_{right} = \mathsf{ncp}(p_{right}) \oplus \max(\underline{0}, \mathsf{cp}(p_{right}))$$

$$\text{where } p_{left} = [f]([t_1]_{left}, \ldots, [t_n]_{left}) \quad \text{and} \quad p_{right} = [f]([t_1]_{right}, \ldots, [t_n]_{right})$$

Note that for Def. 5 we have to extend ordered semirings by the additional unary operation: $\max(\underline{0}, \cdot)$.

Definition 6. *A structure $(\mathcal{U}, \oplus, \odot, \underline{0}, \underline{1}, \geq, >, \mathsf{mono}, \mathsf{max}\underline{0})$ is an ordered semiring with max iff $(\mathcal{U}, \oplus, \odot, \underline{0}, \underline{1}, \geq, >, \mathsf{mono})$ is an ordered semiring and additionally:*

- $\mathsf{max}\underline{0}(x) \geq \underline{0}$ *and* $\mathsf{max}\underline{0}(x) \geq x$

- $y \geq x \geq \underline{0}$ *implies* $\mathsf{max}\underline{0}(y) \geq \mathsf{max}\underline{0}(x) = x$

Theorem 7. *Let* $(\mathcal{U}, \oplus, \odot, \underline{0}, \underline{1}, \geq, >, \mathsf{mono}, \mathsf{max}\underline{0})$ *be an ordered semiring with max and* $\mathcal{P}ol$ *be a polynomial interpretation where* $[f](x_1, \ldots, x_n) = f_0 \oplus f_1 \odot x_1 \oplus \cdots \oplus f_n \odot x_n$ *and* $f_i \geq \underline{0}$ *for all* $1 \leq i \leq n$ *and every n-ary symbol f. Then* $(\succsim_{\mathcal{P}ol}, \succ_{\mathcal{P}ol})$ *is a reduction pair where* $s \succ / \succsim t$ *can be approximated by* $[s]_{left} > / \geq [t]_{right}$.

Example 8. *All ordered semirings of Ex. 4 are also ordered semirings with max, where* $\mathsf{max}\underline{0}$ *is the standard operation on* $\mathbb{N}$, $\mathbb{Z}$, *and* $\mathbb{Q}$, *and* $\mathsf{max}\underline{0}$ *is performed component-wise for matrices.*

For example, for $\mathbb{Q}$ *it is now possible to use interpretations like*

$$[\mathsf{half}](x) = \frac{1}{2} \cdot x + \frac{1}{2} \qquad\qquad [\mathsf{p}](x) = x - 1 \qquad\qquad [\mathsf{s}](x) = x + 1$$

where

$$[\mathsf{s}(x)]_{left} = x + 1 > \frac{1}{2} \cdot x + \frac{1}{2} = [\mathsf{p}(\mathsf{half}(\mathsf{s}(\mathsf{s}(x))))]_{right}$$

Since we are not aware of any termination tool that supports these interpretation, we would like to encourage their integration, perhaps an interpretation like

$$[\mathsf{f}](x,y) = \begin{pmatrix} \frac{1}{2} & 8 \\ \frac{7}{5} & 0 \end{pmatrix} \cdot x + y + \begin{pmatrix} -\frac{1}{3} & 3 \\ -5 & \frac{2}{9} \end{pmatrix}$$

increases the power in the next competition.

4   Arctic Semirings

In [13], the *arctic semiring* as well as the *arctic semiring below zero*, where used the first time in the well-founded monotone algebra setting.

Example 9 (Arctic Semirings)**.** *The arctic semiring* $(\mathbb{A}_{\mathbb{N}}, \mathsf{max}, +, -\infty, 0)$, *the arctic semiring below zero* $(\mathbb{A}_{\mathbb{Z}}, \mathsf{max}, +, -\infty, 0)$, *and the arctic rational semiring* $(\mathbb{A}_{\mathbb{Q}}, \mathsf{max}, +, -\infty, 0)$, *are semirings with one-element as in Def. 1. The carriers are given by* $\mathbb{A}_S = S \cup \{-\infty\}$. *Furthermore, the standard operations* max *and* $+$ *are extended such that* $\mathsf{max}\{x, -\infty\} = x$ *and* $x + -\infty = -\infty + y = -\infty$, *for all x and y.*

Definition 10. *A structure* $(\mathcal{U}, \oplus, \odot, \underline{0}, \underline{1}, \geq, >, \mathsf{pos})$ *is an ordered arctic semiring iff* $(\mathcal{U}, \oplus, \odot, \underline{0}, \underline{1})$ *is a semiring with one-element and additionally:*

- $\geq$ *is reflexive and transitive;* $>$ *and* $\geq$ *are compatible:* $> \circ \geq \,\subseteq\, >$ *and* $\geq \circ > \,\subseteq\, >$

- $\underline{1} \geq \underline{0}$; $\mathsf{pos}(\underline{1})$; $x > \underline{0}$; $x \geq \underline{0}$; *and if* $\underline{0} > x$ *then* $x = \underline{0}$

- $\oplus$ *is left-monotone w.r.t.* $\geq$

- $\oplus$ *is monotone w.r.t.* $>$: *if* $x > y$ *and* $x' > y'$ *then* $x \oplus x' > y \oplus y'$

- $\odot$ *is left- and right-monotone w.r.t.* $\geq$ *and left-monotone w.r.t.* $>$

- *staying positive: if* $\mathsf{pos}(x)$ *and* $\mathsf{pos}(y)$ *then* $\mathsf{pos}(x \oplus z)$ *and* $\mathsf{pos}(x \odot y)$

- $\{(x,y) \mid x > y \wedge \mathsf{pos}(y)\}$ *is well-founded*

Theorem 11. *Let* $\mathcal{P}ol$ *be a polynomial interpretation over an ordered arctic semiring* $(\mathcal{U}, \oplus, \odot, \underline{0}, \underline{1}, \geq, >, \mathsf{pos})$ *where* $[f](x_1, \ldots, x_n) = f_0 \oplus f_1 \odot x_1 \oplus \cdots \oplus f_n \odot x_n$ *and* $\mathsf{pos}(f_i)$ *for some* $0 \leq i \leq n$ *and every n-ary symbol f. Then* $(\succsim_{\mathcal{P}ol}, \succ_{\mathcal{P}ol})$ *is a reduction pair where* $s \succsim / \succ t$ *is approximated by comparing* $[s]$ *and* $[t]$ *component-wise using* $> / \geq$. *(For example to compare* $a \odot x \oplus b \odot y \oplus c > d \odot x \oplus e \odot y \oplus f$ *one demands* $a > d$, $b > e$, *and* $c > f$.)

4

Moreover, if $n > 0$ and $(\mathcal{U}, \oplus, \odot, \underline{0}, \underline{1}, \geq, >, \mathsf{pos})$ is an ordered arctic semiring, then $(\mathcal{U}^{n \times n}, \oplus^{n \times n}, \odot^{n \times n}, \underline{0}^{n \times n}, \underline{1}^{n \times n}, \geq^{n \times n}, >^{n \times n}, \mathsf{pos}^{n \times n})$ is also an ordered arctic semiring where all operations and constants are lifted to work on n-dimensional matrices. Here $\geq^{n \times n}$ and $>^{n \times n}$, compare arguments componentwise and $\mathsf{pos}^{n \times n}$ checks, whether the leftmost topmost element is pos.

Example 12 (Ordered Arctic Semirings)**.** *All arctic semirings of Ex. 9 are also ordered arctic semirings. In all three cases, we use the non-strict ordering $x \geq y \equiv y = -\infty \vee (x \neq -\infty \wedge x \geq_{\mathbb{N}/\mathbb{Z}/\mathbb{Q}} y)$. For $\mathbb{A}_{\mathbb{N}}$ and $\mathbb{A}_{\mathbb{Z}}$, we use the strict ordering $x > y \equiv y = -\infty \vee (x \neq -\infty \wedge x >_{\mathbb{N}/\mathbb{Z}} y)$, and for $\mathbb{A}_{\mathbb{Q}}$, we use the strict ordering $x >_{\delta} y \equiv y = -\infty \vee (x \neq -\infty \wedge x - y \geq_{\mathbb{Q}} \delta)$ for some $\delta > 0$. Furthermore, the check for positiveness is defined by $\mathsf{pos}(x) \equiv x \neq -\infty \wedge x \geq_{\mathbb{N}/\mathbb{Z}/\mathbb{Q}} 0$.*

Note that the ordered arctic semiring over $\mathbb{A}_{\mathbb{Q}}$, together with Thm. 11, unifies and extends Theorems 12 and 14 of [13]. Here, the main advantage of our approach is that we only restrict interpretations $[f](x_1, \ldots, x_n) = f_0 \oplus f_1 \odot x_1 \oplus \cdots \oplus f_n \odot x_n$ by demanding that at least one f_i is positive. This is in contrast to the theorem about the arctic semiring below zero in [13] where always the constant part f_0 has to be positive. However, Waldmann observed that for finite TRSs one can transform every polynomial order over the arctic rationals into an order over the arctic naturals by multiplication and shifting.

References

[1] T. Arts and J. Giesl. Termination of term rewriting using dependency pairs. *Theoretical Computer Science*, 236:133–178, 2000.

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

[3] A. Ben Cherifa and P. Lescanne. Termination of Rewriting Systems by Polynomial Interpretations and Its Implementation. *Science of Computer Programming*, 9(2):137–159, 1987.

[4] F. Blanqui, W. Delobel, S. Coupet-Grimal, S. Hinderer, and A. Koprowski. CoLoR, a Coq library on rewriting and termination. In *Proc. WST'06*, pages 69–73, 2006.

[5] É. Contejean, P. Courtieu, J. Forest, A. Paskevich, O. Pons, and X. Urbain. A3PAT, an approach for certified automated termination proofs. In *Proc. PEPM'10*. To appear.

[6] É. Contejean, P. Courtieu, J. Forest, O. Pons, and X. Urbain. Certification of automated termination proofs. In *Proc. FroCoS'07*, LNAI 4720, pages 148–162, 2007.

[7] P. Courtieu, G. Gbedo, and O. Pons. Improved matrix interpretation. In *Proc. SOFSEM'10*, LNCS 5901, pages 283–295, 2010.

[8] J. Endrullis, J. Waldmann, and H. Zantema. Matrix Interpretations for Proving Termination of Term Rewriting. *Journal of Automated Reasoning*, 40(2-3):195–220, 2008.

[9] A. Geser. *Relative Termination*. PhD thesis, University of Passau, Germany, 1990.

[10] J. Giesl, R. Thiemann, P. Schneider-Kamp, and S. Falke. Mechanizing and improving dependency pairs. *Journal of Automated Reasoning*, 37(3):155–203, 2006.

[11] N. Hirokawa and A. Middeldorp. Automating the dependency pair method. *Information and Computation*, 199(1-2):172–199, 2005.

[12] N. Hirokawa and A. Middeldorp. Tyrolean Termination Tool: Techniques and features. *Information and Computation*, 205(4):474–511, 2007.

[13] A. Koprowski and J. Waldmann. Arctic termination . . . below zero. In *Proc. RTA'08*, LNCS 5117, pages 202–216, 2008.

[14] D. Lankford. On proving term rewriting systems are Noetherian. Technical Report MTP-3, Louisiana Technical University, Ruston, LA, USA, 1979.

[15] T. Nipkow, L.C. Paulson, and M. Wenzel. *Isabelle/HOL: A Proof Assistant for Higher-Order Logic*. LNCS 2283. Springer, 2002.

[16] R. Thiemann and C. Sternagel. Certification of termination proofs using CeTA. In *Proc. TPHOLs '09*, LNCS 5674, pages 452–468, 2009.