Equational Theories and Validity for Logically Constrained Term Rewriting

Takahito Aoto
Niigata University, Japan

Naoki Nishida
Nagoya University, Japan

Jonas Schöpf
University of Innsbruck, Austria

Abstract

Logically constrained term rewriting is a relatively new formalism where rules are equipped with constraints over some arbitrary theory. Although there are many recent advances with respect to rewriting induction, completion, complexity analysis and confluence analysis for logically constrained term rewriting, these works solely focus on the syntactic side of the formalism lacking detailed investigations on semantics. In this paper, we investigate a semantic side of logically constrained term rewriting. To this end, we first define constrained equations, constrained equational theories and validity of the former based on the latter. After presenting the relationship of validity and conversion of rewriting, we then construct a sound inference system to prove validity of constrained equations in constrained equational theories. Finally, we give an algebraic semantics, which enables one to establish invalidity of constrained equations in constrained equational theories. This algebraic semantics derives a new notion of consistency for constrained equational theories.

2012 ACM Subject Classification Theory of computation → Equational logic and rewriting

Keywords and phrases constrained equation, constrained equational theory, logically constrained term rewriting, algebraic semantics, consistency

Digital Object Identifier 10.4230/LIPIcs.FSCD.2024.31

Related Version *Full Version*: `https://arxiv.org/abs/2405.01174` [1]

Funding This research was supported by the FWF (Austrian Science Fund) project I 5943-N and JSPS-FWF Grant Number JPJSBP120222001.
Takahito Aoto: JSPS KAKENHI Grant Numbers 21K11750, 24K14817
Naoki Nishida: JSPS KAKENHI Grant Number 24K02900
Jonas Schöpf: FWF (Austrian Science Fund) project I 5943-N

Acknowledgements We thank the anonymous reviewers for their valuable feedback, which improved the paper.

1 Introduction

Logically constrained term rewriting is a relatively new formalism building upon many-sorted term rewriting and built-in theories. The rules of a logically constrained term rewrite system (LCTRS, for short) are equipped with constraints over some arbitrary theory, which have to be fulfilled in order to apply rules in rewrite steps. This formalism intends to live up with data structures which are often difficult to represent in basic rewriting, such as integers and bit-vectors, with the help of external provers and their built-in theories.

Logical syntax and semantics are often conceived as two sides of the same coin. This is not exceptional, especially for equational logic in which term rewriting lies. On the other hand, although there are many recent advances in rewriting induction [9], completion [20], complexity analysis [21], confluence analysis [13, 15, 17] and (all-path) reachability [4, 12, 11] for LCTRSs, these works solely focus on the syntactic side of the formalism, lacking detailed investigations on semantics.

In this paper, we investigate a semantic side of the LCTRS formalism. To this end, we first define *constrained equations* (CEs, for short) and *constrained equational theories* (CE-theories, for short). In (first-order) term rewriting, the equational version of rewrite rules is obtained by removing the orientation of the rules. However, in the case of LCTRSs, if we consider a constrained rule $\ell \to r\ [\varphi]$ and relate this naively to a CE $\ell \approx r\ [\varphi]$, which does not distinguish between left- and right-hand sides, we lose information about the restriction on the possible instantiation of variables. This motivates us to add an explicit set X to each CE $\ell \approx r\ [\varphi]$ as $\Pi X.\, \ell \approx r\ [\varphi]$[1] – we name variables in X as *logical variables* with respect to the equation. A CE-theory is then defined as a set of CEs. Similar to the rewrite steps of LCTRSs, we define validity by convertibility if all logical variables are instantiated by values – we denote this notion of validity as *CE-validity* for clarity.

After establishing fundamental properties of the CE-validity, we present its relation to the conversion of rewriting. However, the conversion of rewriting is useful in general to establish the validity of arbitrary CEs. This motivates us to introduce $\mathbf{CEC}_0$, an inference calculus for deriving valid CEs. After demonstrating the usefulness of $\mathbf{CEC}_0$ via some derivations, we present a soundness theorem for the calculus. We also show a partial completeness result, followed by a discussion why our system seems incomplete. Afterwards we consider the opposite question, namely how to prove that a CE is not valid for a particular CE-theory. To this end, we introduce an algebraic semantics that captures CE-validity. We give a natural notion of models for CE-theory, which we call *CE-algebras*. We establish soundness and completeness with respect to CE-validity for this.

Figure 1 presents the relationships between the introduced notions and results of this paper. The following concrete contributions are covered in this paper:

1. We propose a formulation of CEs and CE-theories.
2. On top of that we devise a notion of validity of a CE for a CE-theory $\mathcal{E}$, which we call CE-validity.
3. We give a proof system $\mathbf{CEC}_0$, and show soundness (Theorem 4.6) and a partial completeness result (Theorem 4.10) with respect to CE-validity.
4. We give a notion of CE-algebras and based on it we define algebraic semantics, which is sound (Theorem 5.6) and complete (Theorem 5.17) with respect to CE-validity for *consistent* CE-theories.

We want to discuss some highlights of the last item for readers who are familiar with algebraic semantics of equational logic. First of all, our definition of CE-algebras admits extended underlying models, contrast to those that precisely contain the same underlying models; we will demonstrate why this generalization is required to obtain the completeness result. To reflect this definition, it was necessary to modify the definition of congruence relation to a non-standard one. Also, the notion of consistency with respect to values arises to guarantee this modified notion of congruence in the term algebras. Moreover, it also turns out that value-consistency is equivalent to a more intuitive notion of consistency.

The remainder of the paper is organized as follows. In the next section, we briefly explain the LCTRS formalism, and present some basic lemmas that are necessary for our proofs. Section 3 introduces the notion of CEs, CE-theories and CE-validity, and presents basic

[1] In the literature, some other approaches exist. The computation of critical pairs is also prone of losing information [17]. They solved it by adding dummy constraints $x = x$ to the critical pair. Another approach was proposed in [20] where $\mathcal{LV}\mathsf{ar}(\ell \approx r\ [\varphi])$ was simply defined as $\mathcal{V}\mathsf{ar}(\varphi)$.

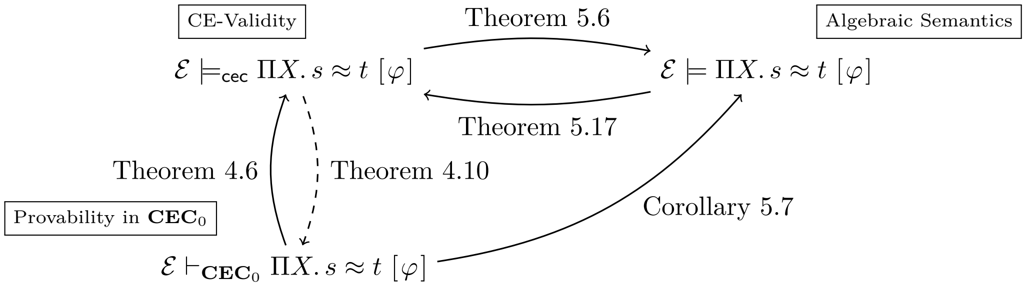

Figure 1 An overview of the main results of this paper.

properties on CE-validity and its relation to the conversion of rewriting. Section 4 is devoted to our inference system $\mathbf{CEC}_0$, including its soundness and partial completeness with respect to CE-validity. In Section 5, we present algebraic semantics, and soundness and completeness results with respect to CE-validity. Before concluding this paper in Section 7, we briefly describe related work in Section 6. We provide only brief proof sketches of selected results in this paper. However, all detailed proofs are given in the full version of this paper [1].

2 Preliminaries

In this section, we briefly recall LCTRSs [13, 9, 17]. Familiarity with the basic notions on mathematical logic [8, 19] and term rewriting [2, 16] is assumed.

The (sorted) signature of an LCTRS is given by the set $\mathcal{S}$ of sorts and the set $\mathcal{F}$ of $\mathcal{S}$-sorted function symbols. Each $f \in \mathcal{F}$ is equipped with a sort declaration $f\colon \tau_1 \times \cdots \times \tau_n \to \tau_0$ with $\tau_0, \ldots, \tau_n \in \mathcal{S}$; $\tau_1 \times \cdots \times \tau_n \to \tau_0$ is said to be the sort of f, and we denote by $\mathcal{F}^{\tau_1 \times \cdots \times \tau_n \to \tau_0}$ the set of function symbols of sort $\tau_1 \times \cdots \times \tau_n \to \tau_0$. For constants of sort $\to \tau$ we drop $\to$ and write τ instead of $\to \tau$. The set of $\mathcal{S}$-sorted variables is denoted by $\mathcal{V}$ and the set of $\mathcal{S}$-sorted terms over $\mathcal{F}, \mathcal{V}$ is $\mathcal{T}(\mathcal{F}, \mathcal{V})$. For each $\tau \in \mathcal{S}$, we denote by $\mathcal{V}^\tau$ the set of variables of sort τ and by $\mathcal{T}(\mathcal{F}, \mathcal{V})^\tau$ the set of terms of sort τ; we also write t^τ for a term t such that $t \in \mathcal{T}(\mathcal{F}, \mathcal{V})^\tau$. The set of variables occurring in a term $t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ is denoted by $\mathcal{V}\mathsf{ar}(t)$ and can be restricted by a set of sorts T with $\mathcal{V}\mathsf{ar}^T(t) = \{x^\tau \in \mathcal{V}\mathsf{ar}(t) \mid \tau \in T\}$. A substitution σ is a mapping $\mathcal{V} \to \mathcal{T}(\mathcal{F}, \mathcal{V})$ such that $\mathcal{D}\mathsf{om}(\sigma) = \{x \in \mathcal{V} \mid x \neq \sigma(x)\}$ is finite and $\sigma(x^\tau) \in \mathcal{T}(\mathcal{F}, \mathcal{V})^\tau$ is satisfied for all $x \in \mathcal{D}\mathsf{om}(\sigma)$.

In the LCTRS formalism, sorts are divided into two categories, that is, each sort $\tau \in \mathcal{S}$ is either a *theory sort* or a *term sort*, where we denote by $\mathcal{S}_{\mathsf{th}}$ the set of theory sorts and by $\mathcal{S}_{\mathsf{te}}$ the set of term sorts, i.e. $\mathcal{S} = \mathcal{S}_{\mathsf{th}} \uplus \mathcal{S}_{\mathsf{te}}$. Accordingly, the set of variables is partitioned as $\mathcal{V} = \mathcal{V}_{\mathsf{th}} \uplus \mathcal{V}_{\mathsf{te}}$ by letting $\mathcal{V}_{\mathsf{th}}$ for the set of variables of sort $\tau \in \mathcal{S}_{\mathsf{th}}$ and $\mathcal{V}_{\mathsf{te}}$ for the set of variables of sort $\tau \in \mathcal{S}_{\mathsf{te}}$. Furthermore, we assume each function symbol $f \in \mathcal{F}$ is either a theory symbol or a term symbol, where all former symbols $f\colon \tau_1 \times \cdots \times \tau_n \to \tau_0$ need to satisfy $\tau_i \in \mathcal{S}_{\mathsf{th}}$ for all $0 \leqslant i \leqslant n$. The sets of theory and term symbols are denoted by $\mathcal{F}_{\mathsf{th}}$ and $\mathcal{F}_{\mathsf{te}}$, respectively: $\mathcal{F} = \mathcal{F}_{\mathsf{th}} \uplus \mathcal{F}_{\mathsf{te}}$. Throughout the paper, we consider signatures consisting of four components $\langle \mathcal{S}_{\mathsf{th}}, \mathcal{S}_{\mathsf{te}}, \mathcal{F}_{\mathsf{th}}, \mathcal{F}_{\mathsf{te}} \rangle$. In some cases term/theory signature stands for the two respective term/theory components of such a signature.

An LCTRS is also equipped with a model over the sorts $\mathcal{S}_{\mathsf{th}}$ and the symbols $\mathcal{F}_{\mathsf{th}}$, which is given by $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$, where $\mathcal{I}$ assigns each $\tau \in \mathcal{S}_{\mathsf{th}}$ a *non-empty* set $\mathcal{I}(\tau)$, specifying its domain, and $\mathcal{J}$ assigns each $f\colon \tau_1 \times \cdots \times \tau_n \to \tau_0 \in \mathcal{F}_{\mathsf{th}}$ an interpretation function $\mathcal{J}(f)\colon \mathcal{I}(\tau_1) \times \cdots \times \mathcal{I}(\tau_n) \to \mathcal{I}(\tau_0)$. In particular, $\mathcal{J}(c) \in \mathcal{I}(\tau)$ for any constant $c \in \mathcal{F}_{\mathsf{th}}^\tau$. We suppose for each $\tau \in \mathcal{S}_{\mathsf{th}}$, there exists a subset $\mathcal{V}\mathsf{al}_\tau \subseteq \mathcal{F}_{\mathsf{th}}^\tau$ of constants of sort τ such that (the restriction of) $\mathcal{J}$ to $\mathcal{V}\mathsf{al}_\tau$ forms a bijection $\mathcal{V}\mathsf{al}_\tau \cong \mathcal{I}(\tau)$. We let $\mathcal{V}\mathsf{al} = \bigcup_{\tau \in \mathcal{S}_{\mathsf{th}}} \mathcal{V}\mathsf{al}_\tau$, whose elements are called *values*. For simplicity, we do not distinguish between $c \in \mathcal{V}\mathsf{al}$ and $\mathcal{J}(c)$. Note that, in [13, 9], an arbitrary overlap between term and theory symbols is allowed provided it is covered by values. For simplicity, we assume $\mathcal{F}_{\mathsf{th}} \cap \mathcal{F}_{\mathsf{te}} = \varnothing$.

A *valuation* over a model $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$ is a family $\rho = (\rho_\tau)_{\tau \in \mathcal{S}_{\mathsf{th}}}$ of mappings $\rho_\tau : \mathcal{V}^\tau \to \mathcal{I}(\tau)$. The *interpretation* $[\![t]\!]_{\mathcal{M},\rho} \in \mathcal{I}(\tau)$ of a term $t^\tau \in \mathcal{T}(\mathcal{F}_{\mathsf{th}}, \mathcal{V})$ in the model $\mathcal{M}$ with respect to the valuation $\rho = (\rho_\tau)_{\tau \in \mathcal{S}_{\mathsf{th}}}$ is inductively defined as follows: $[\![x^\tau]\!]_{\mathcal{M},\rho} = \rho^\tau(x)$ and $[\![f(t_1, \dots, t_n)]\!]_{\mathcal{M},\rho} = \mathcal{J}(f)([\![t_1]\!]_{\mathcal{M},\rho}, \dots, [\![t_n]\!]_{\mathcal{M},\rho})$. We abbreviate $[\![t]\!]_{\mathcal{M},\rho}$ as $[\![t]\!]_\rho$ if $\mathcal{M}$ is known from the context. Furthermore, for any ground term $t \in \mathcal{T}(\mathcal{F}_{\mathsf{th}})$, the valuation ρ has no impact on the interpretation $[\![t]\!]_\rho$ which can be safely ignored and written as $[\![t]\!]$.

We suppose a special sort $\mathsf{Bool} \in \mathcal{S}_{\mathsf{th}}$ such that $\mathcal{I}(\mathsf{Bool}) = \mathbb{B} = \{\mathsf{true}, \mathsf{false}\}$, and usual logical connectives $\neg, \wedge, \vee, \ldots \in \mathcal{F}_{\mathsf{th}}$ with their default sorts. We assume that there exists for each $\tau \in \mathcal{S}_{\mathsf{th}}$ an equality symbol $=_\tau$ of sort $\tau \times \tau \to \mathsf{Bool}$ in $\mathcal{F}_{\mathsf{th}}$. For brevity we will omit $_\tau$ from $=_\tau$. We assume, for all of these theory symbols, that their interpretation functions model their default semantics. The terms in $\mathcal{T}(\mathcal{F}_{\mathsf{th}}, \mathcal{V})^{\mathsf{Bool}}$ are called *logical constraints*.[2] Note that $\mathcal{V}\mathsf{ar}(\varphi) \subseteq \mathcal{V}_{\mathsf{th}}$ for any logical constraint φ, thus in this case $\mathcal{T}(\mathcal{F}_{\mathsf{th}}, \mathcal{V})^{\mathsf{Bool}} = \mathcal{T}(\mathcal{F}_{\mathsf{th}}, \mathcal{V}_{\mathsf{th}})^{\mathsf{Bool}}$. We say that a logical constraint φ is over a set $X \subseteq \mathcal{V}_{\mathsf{th}}$ of theory variables if $\mathcal{V}(\varphi) \subseteq X$. A logical constraint φ is said to be *valid* in a model $\mathcal{M}$, written as $\models_{\mathcal{M}} \varphi$ (or $\models \varphi$ when the model $\mathcal{M}$ is known from the context), if $[\![\varphi]\!]_{\mathcal{M},\rho} = \mathsf{true}$ for any valuation ρ over the model $\mathcal{M}$. Considering the bijection $\mathcal{V}\mathsf{al}_\tau \cong \mathcal{I}(\tau)$, an arbitrary substitution σ is equivalent to a valuation ρ. Suppose that $\mathcal{VD}\mathsf{om}(\sigma) = \{x \in \mathcal{D}\mathsf{om}(\sigma) \mid \sigma(x) \in \mathcal{V}\mathsf{al}\}$ and $\mathcal{V}\mathsf{ar}(\varphi) \subseteq \mathcal{VD}\mathsf{om}(\sigma)$. Then the substitution σ can be seen as a valuation over φ, and $\models_{\mathcal{M}} \varphi\sigma$ coincides with $[\![\varphi]\!]_{\mathcal{M},\sigma} = \mathsf{true}$. More generally, we have the following.

▶ **Lemma 2.1.** *Let $t \in \mathcal{T}(\mathcal{F}_{\mathsf{th}}, \mathcal{V}_{\mathsf{th}})$, ρ a valuation, and σ a substitution.*

1. *Suppose $\sigma(x) \in \mathcal{T}(\mathcal{F}_{\mathsf{th}}, \mathcal{V}_{\mathsf{th}})$ for all $x \in \mathcal{V}_{\mathsf{th}}$. Let $[\![\sigma]\!]_{\mathcal{M},\rho}$ be a valuation defined as $[\![\sigma]\!]_{\mathcal{M},\rho}(x) = [\![\sigma(x)]\!]_{\mathcal{M},\rho}$. Then, $[\![t]\!]_{\mathcal{M},[\![\sigma]\!]_{\mathcal{M},\rho}} = [\![t\sigma]\!]_{\mathcal{M},\rho}$.*
2. *Suppose that $\mathcal{V}\mathsf{ar}(t) \subseteq \mathcal{VD}\mathsf{om}(\sigma)$. Then, $[\![t]\!]_{\mathcal{M},\hat{\sigma}} = [\![t\sigma]\!]_{\mathcal{M}}$, where the valuation $\hat{\sigma}$ is defined by $\hat{\sigma}(x^\tau) = \xi(\sigma(x)) \in \mathcal{I}(\tau)$ for $x \in \mathcal{VD}\mathsf{om}(\sigma)$, where ξ is a bijection $\mathcal{V}\mathsf{al}^\tau \cong \mathcal{I}(\tau)$.*

Proof (Sketch).

1. Use structural induction on $t \in \mathcal{T}(\mathcal{F}_{\mathsf{th}}, \mathcal{V}_{\mathsf{th}})$.
2. Similar to **1**, using the assumption $\mathcal{V}\mathsf{ar}(t) \subseteq \mathcal{VD}\mathsf{om}(\sigma)$. ◀

From Lemma 2.1 the following characterizations, which are used later on, are obtained. Note that $\models \varphi = \mathsf{true}$ ($\models \varphi = \mathsf{false}$) if and only if $\models \varphi$ ($\models \neg\varphi$), for a logical constraint φ.

▶ **Lemma 2.2.** *Let φ be a logical constraint.*

1. *$\models_{\mathcal{M}} \varphi$ if and only if $\models_{\mathcal{M}} \varphi\sigma$ for all substitutions σ such that $\mathcal{V}\mathsf{ar}(\varphi) \subseteq \mathcal{VD}\mathsf{om}(\sigma)$.*
2. *If $\models_{\mathcal{M}} \varphi$, then $\models_{\mathcal{M}} \varphi\sigma$ for all substitutions σ such that $\sigma(x) \in \mathcal{T}(\mathcal{F}_{\mathsf{th}}, \mathcal{V}_{\mathsf{th}})$ for all $x \in \mathcal{V}\mathsf{ar}(\varphi) \cap \mathcal{D}\mathsf{om}(\sigma)$.*
3. *The following statements are equivalent: (1) $\models_{\mathcal{M}} \neg\varphi$, (2) $\not\models_{\mathcal{M}} \varphi\sigma$ for all substitutions σ such that $\mathcal{V}\mathsf{ar}(\varphi) \subseteq \mathcal{VD}\mathsf{om}(\sigma)$, and (3) $\sigma \models_{\mathcal{M}} \varphi$ for no substitution σ.*

Here, $\sigma \models_{\mathcal{M}} \varphi$ denotes that $\mathcal{V}\mathsf{ar}(\varphi) \subseteq \mathcal{VD}\mathsf{om}(\sigma)$ and $\models_{\mathcal{M}} \varphi\sigma$ hold.

---

[2] Logical constraints are quantifier-free, which is not restrictive: Consider, for example, a formula $\forall x.\ \varphi$ with n free variables $x_1, \dots, x_n$ and a quantifier-free formula φ. By introducing an n-ary predicate symbol p defined as $[\![p(x_1, \dots, x_n)]\!]_{\mathcal{M},\rho} = [\![\forall x.\ \varphi]\!]_{\mathcal{M},\rho}$, we can replace the formula by the quantifier-free formula $p(x_1, \dots, x_n)$. Clearly, this applies to arbitrary first-order formulas. Another approach can be seen in [9, Section 2.2].

Proof (Sketch).
1. ($\Rightarrow$) Let σ be a substitution such that $\mathcal{V}\mathsf{ar}(\varphi) \subseteq \mathcal{VD}\mathsf{om}(\sigma)$, and $\hat{\sigma}$ be defined as in Lemma 2.1. Then, $[\![\varphi]\!]_{\mathcal{M},\hat{\sigma}} = \mathsf{true}$, and hence $[\![\varphi\sigma]\!]_{\mathcal{M}} = \mathsf{true}$ by Lemma 2.1. Therefore, $\models_{\mathcal{M}} \varphi\sigma$. ($\Leftarrow$) Let ρ be a valuation over a model $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$. Then, in the view of $\mathcal{V}\mathsf{al}_\tau \cong \mathcal{I}(\tau)$, we can take a substitution $\check{\rho}$ given by $\check{\rho}(x) = \rho(x) \in \mathcal{V}\mathsf{al}$ for all $x \in \mathcal{V}\mathsf{ar}(\varphi)$. Then, use Lemma 2.1 to obtain $[\![\varphi]\!]_{\mathcal{M},\rho} = [\![\varphi]\!]_{\mathcal{M},\hat{\check{\rho}}} = \mathsf{true}$, from which $\models_{\mathcal{M}} \varphi$ follows.
2. Take a substitution σ' such that $\sigma'(x) = \sigma(x)$ for $x \in \mathcal{V}\mathsf{ar}(\varphi)$ and $\sigma'(x) = x$ otherwise. Then, using Lemma 2.1, we have $[\![\varphi]\!]_{[\![\sigma]\!]_\rho} = [\![\varphi]\!]_{[\![\sigma']\!]_\rho} = [\![\varphi\sigma']\!]_\rho = [\![\varphi\sigma]\!]_\rho$. Thus, $[\![\varphi\sigma]\!]_\rho = \mathsf{true}$ for any ρ. Therefore, $\models_{\mathcal{M}} \varphi\sigma$.
3. Use **1**. ◀

LCTRSs admit special rewrite steps over $\mathcal{T}(\mathcal{F}, \mathcal{V})$ specified by the underlying model $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$. Such rewrite steps are called *calculation steps* and denoted by $s \to_{\mathsf{calc}} t$, which is defined as follows: $s \to_{\mathsf{calc}} t$ if $s = C[f(c_1, \ldots, c_n)]$ and $t = C[c_0]$ for $f \in \mathcal{F}_{\mathsf{th}} \setminus \mathcal{V}\mathsf{al}$ and $c_0, \ldots, c_n \in \mathcal{V}\mathsf{al}$ with $c_0 = \mathcal{J}(f)(c_1, \ldots, c_n)$ and a context C. The following lemma connects calculation steps and interpretations over ground theory terms $\mathcal{T}(\mathcal{F}_{\mathsf{th}})$. In the following $s \to^! t$ is used for $s \to^* t$ with t being a normal form with respect to $\to$.

▶ **Lemma 2.3.** *Let $s, t \in \mathcal{T}(\mathcal{F}_{\mathsf{th}})$. Then, all of the following holds:*
1. $[\![t]\!] \in \mathcal{V}\mathsf{al}$,
2. $t \to^!_{\mathsf{calc}} [\![t]\!]$,
3. $s \to^*_{\mathsf{calc}} t$ *implies* $[\![s]\!] = [\![t]\!]$, *and*
4. $s \leftrightarrow^*_{\mathsf{calc}} t$ *if and only if* $[\![s]\!] = [\![t]\!]$.

Proof (Sketch).
1. This claim follows as $[\![t^\tau]\!] \in \mathcal{I}(\tau) \cong \mathcal{V}\mathsf{al}^\tau$.
2. Show $t \to^*_{\mathsf{calc}} [\![t]\!]$ by structural induction on t. Then, the claim follows, since values are normal forms with respect to calculation steps.
3. We use the fact that the set of calculation rules forms a confluent LCTRS [13]. Since $s \to^!_{\mathsf{calc}} [\![s]\!]$ and $t \to^!_{\mathsf{calc}} [\![t]\!]$ from **2**, $s \to^*_{\mathsf{calc}} t$ implies $[\![s]\!] = [\![t]\!]$ by confluence.
4. The *only-if* part follows from **3**, and the *if* part follows from **1**. ◀

The other type of rewrite steps in LCTRSs are rule steps specified by rewrite rules. Let us fix a signature $\langle \mathcal{S}_{\mathsf{th}}, \mathcal{S}_{\mathsf{te}}, \mathcal{F}_{\mathsf{th}}, \mathcal{F}_{\mathsf{te}} \rangle$. A constrained rule of an LCTRS is a triple $\ell \to r$ $[\varphi]$ of terms ℓ, r with the same sort satisfying $root(\ell) \in \mathcal{F}_{\mathsf{te}}$ and a logical constraint φ. We define $\mathcal{LV}\mathsf{ar}(\ell \to r\ [\varphi]) = (\mathcal{V}\mathsf{ar}(r) \setminus \mathcal{V}\mathsf{ar}(\ell)) \cup \mathcal{V}\mathsf{ar}(\varphi)$, whose members are called *logical variables* of the rule. The intention is that the logical variables of rules in LCTRSs are required to be instantiated only by values. Let us also fix a model $\mathcal{M}$. Then, a substitution γ is said to *respect a rewrite rule* $\ell \to r$ $[\varphi]$ if $\mathcal{LV}\mathsf{ar}(\ell \to r\ [\varphi]) \subseteq \mathcal{VD}\mathsf{om}(\gamma)$ and $\models_{\mathcal{M}} \varphi\gamma$. Using this notation, a rule step $s \to_{\mathsf{rule}} t$ over the model $\mathcal{M}$ by the rewrite rule $\ell \to r$ $[\varphi]$ is given as follows: $s \to_{\mathsf{rule}} t$ if and only if $s = C[\ell\gamma]$ and $t = C[r\gamma]$ for some context C and some substitution γ that respects the rewrite rule $\ell \to r$ $[\varphi]$.

Finally, a *logically constrained term rewrite system* (LCTRS, for short) consists of a signature $\Sigma = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{S}_{\mathsf{te}}, \mathcal{F}_{\mathsf{th}}, \mathcal{F}_{\mathsf{te}} \rangle$, a model $\mathcal{M}$ over $\Sigma_{\mathsf{th}} = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{F}_{\mathsf{th}} \rangle$ (which induces the set $\mathcal{V}\mathsf{al} \subseteq \mathcal{F}_{\mathsf{th}}$ of values) and a set $\mathcal{R}$ of constrained rules over the signature Σ. All this together defines rewrite steps consisting of calculation steps and rule steps. In a practical setting, often some predefined (semi-)decidable theories are assumed and used as model $\mathcal{M}$ and theory signature $\langle \mathcal{S}_{\mathsf{th}}, \mathcal{F}_{\mathsf{th}} \rangle$. An example of such a theory is *linear integer arithmetic*, whose model consists of standard boolean functions and the set of integers including standard predefined functions on them. From this point of view, we call the triple $\mathfrak{U} = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{F}_{\mathsf{th}}, \mathcal{M} \rangle$

of the theory signature and its respective model the *underlying model* or *background theory* of the LCTRS. We also denote an LCTRS as $\langle \mathcal{M}, \mathcal{R} \rangle$ with an implicit signature or $\langle \mathcal{M}, \mathcal{R} \rangle$ over the signature $\Sigma = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{S}_{\mathsf{te}}, \mathcal{F}_{\mathsf{th}}, \mathcal{F}_{\mathsf{te}} \rangle$ for an explicit signature.

3 Validity of Constrained Equational Theories

In this section, we introduce validity of constrained equational theories (CE-validity), which is a key concept used throughout the paper. Subsequently, we present fundamental properties of CE-validity, and show their relation to the conversion of rewriting.

3.1 Constrained Equational Theory and Its Validity

In this subsection, after introducing the notion of CEs, we define equational systems, which are sets of CEs, and rewriting with respect to such systems. This gives an equational version of the rewrite step in LCTRSs. Furthermore, based on these notions, we define the validity of CEs.

Recall that logical variables of a constrained rule are those which are only allowed to be instantiated by values. As we have seen in the previous section, rewrite steps of LCTRSs depend on the correct instantiation of the logical variables of the applied rule. However, the sets of logical variables $\mathcal{LV}\mathsf{ar}(\ell \to r\ [\varphi])$ and $\mathcal{LV}\mathsf{ar}(r \to \ell\ [\varphi])$ are not necessarily equivalent, and the CE $\ell \approx r\ [\varphi]$ alone does not suffice to specify the correct logical variables. This motivates us to add an explicit set X to the CE $\ell \approx r\ [\varphi]$ as $\Pi X.\, \ell \approx r\ [\varphi]$ which specifies its logical variables.

▶ **Definition 3.1** (constrained equation). *Let $\Sigma_{\mathsf{te}} = \langle \mathcal{S}_{\mathsf{te}}, \mathcal{F}_{\mathsf{te}} \rangle$ be a term signature over the underlying model $\mathfrak{U} = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{F}_{\mathsf{th}}, \mathcal{M} \rangle$. A* constrained equation *(CE, for short) over $\mathfrak{U}$ and Σ_{te} is a quadruple $\Pi X.\, s \approx t\ [\varphi]$ where s, t are terms with the same sort, φ is a logical constraint, and $X \subseteq \mathcal{V}_{\mathsf{th}}$ is a set of theory variables satisfying $\mathcal{V}\mathsf{ar}(\varphi) \subseteq X$. A* logically constrained equational system *(LCES, for short) is a set of CEs. We abbreviate $\Pi X.\, s \approx t\ [\varphi]$ to $s \approx t\ [\varphi]$ if $\mathcal{V}\mathsf{ar}(\varphi) = X$. A CE $\Pi X.\, s \approx t\ [\mathsf{true}]$ is abbreviated to $\Pi X.\, s \approx t$.*

We remark that a constrained rewrite rule $\ell \to r\ [\varphi]$ is naturally encoded as a CE $\Pi X.\, \ell \approx r\ [\varphi]$ by taking $X = \mathcal{LV}\mathsf{ar}(\ell \to r\ [\varphi])$. Furthermore, let us illustrate the aforementioned issues, without an explicit set of logical variables, by an example.

▶ **Example 3.2.** Consider the LCTRS $\mathcal{R}$ over the theory of integer arithmetic and its (labeled) rules

$$\alpha\colon \mathsf{f}(x, y) \to \mathsf{g}(z)\ [x = \mathsf{1}] \qquad\qquad \beta\colon \mathsf{g}(z) \to \mathsf{f}(x, y)\ [x = \mathsf{1}]$$

with their sets of logical variables $\mathcal{LV}\mathsf{ar}(\alpha) = \{x, z\}$ and $\mathcal{LV}\mathsf{ar}(\beta) = \{x, y\}$. Transforming them naively into the CE $\mathsf{f}(x, y) \approx \mathsf{g}(z)\ [x = \mathsf{1}]$ and $\mathsf{g}(z) \approx \mathsf{f}(x, y)\ [x = \mathsf{1}]$ would give the set of logical variables $\{x\}$ for both. We use the notion of logical variables in Winkler and Middeldorp [20], where the set of logical variables of a CE consists of the variables appearing in the constraint. Obviously, we lose concrete information about logical variables of the original rules. Clearly, in our notion this information remains intact: $\Pi\{x, z\}.\, \mathsf{f}(x, y) \approx \mathsf{g}(z)\ [x = \mathsf{1}]$ and $\Pi\{x, y\}.\, \mathsf{g}(z) \approx \mathsf{f}(x, y)\ [x = \mathsf{1}]$. Note that variables appearing solely in the set of logical variables and not in the CE have no effect but are allowed. For example, in the CE $\Pi\{x, z, z'\}.\, \mathsf{f}(x, y) \approx \mathsf{g}(z)\ [x = \mathsf{1}]$ the logical variable z' has no effect and could be dropped.

In the following we extend the notion of rewrite steps by using CEs instead of rewrite rules.

▶ **Definition 3.3** ($\leftrightarrow_{\mathcal{E}}$)**.** *Let $\mathcal{E}$ be an LCES over the underlying model $\mathfrak{U} = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{F}_{\mathsf{th}}, \mathcal{M} \rangle$ and the term signature $\Sigma_{\mathsf{te}} = \langle \mathcal{S}_{\mathsf{te}}, \mathcal{F}_{\mathsf{te}} \rangle$. For terms $s, t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$, we define a* rule step *$s \leftrightarrow_{\mathsf{rule},\mathcal{E}} t$ if $s = C[\ell\sigma]$ and $t = C[r\sigma]$ (or vice versa) for some CE $\Pi X.\, \ell \approx r\ [\varphi] \in \mathcal{E}$ and some X-valued substitution σ such that $\models_{\mathcal{M}} \varphi\sigma$. Here, a substitution is said to be X*-valued *if $X \subseteq \mathcal{VD}\mathsf{om}(\sigma)$. We let $\leftrightarrow_{\mathcal{E}} = \leftrightarrow_{\mathsf{calc}} \cup \leftrightarrow_{\mathsf{rule},\mathcal{E}}$, where $\leftrightarrow_{\mathsf{calc}}$ is the symmetric closure of the calculation steps $\rightarrow_{\mathsf{calc}}$ specified by $\mathcal{M}$.*

We give examples on rewriting with CEs.

▶ **Example 3.4.** Consider integer arithmetic as underlying model $\mathcal{M}$. We consider the term sorts $\mathcal{S}_{\mathsf{te}} = \{\mathsf{Unit}\}$ and the term signature $\mathcal{F}_{\mathsf{te}} = \{\mathsf{cong} \colon \mathsf{Int} \to \mathsf{Unit}\}$ where Int is the respective sort of the integers. The set $\mathcal{E}$ of CEs consists of $\{\mathsf{cong}(x) \approx \mathsf{cong}(y)\ [\mathsf{mod}(x, 12) = \mathsf{mod}(y, 12)]\}$. Arithmetic values in intermediate steps of rewrite sequences wrapped in cong have the property that they are *congruent modulo 12* and thus $\mathcal{E}$ simulates modular arithmetic with modulus 12. Consider the following sequence:

$$\mathsf{cong}(7 + 31) \leftrightarrow_{\mathsf{calc}} \mathsf{cong}(38) \leftrightarrow_{\mathsf{rule},\mathcal{E}} \mathsf{cong}(14)$$

From this we conclude that $7 + 31$, which gives 38, and 14 are congruent modulo 12. Note that the rule step $\leftrightarrow_{\mathsf{rule},\mathcal{E}}$ does not allow to directly convert $\mathsf{cong}(7 + 31)$ and $\mathsf{cong}(14)$.

▶ **Example 3.5.** Consider integer arithmetic as the underlying model $\mathcal{M}$. We take a term signature $\mathcal{S}_{\mathsf{te}} = \{\mathsf{G}\}$ and $\mathcal{F}_{\mathsf{te}} = \{\mathsf{e} \colon \mathsf{G}, \mathsf{inv} \colon \mathsf{G} \to \mathsf{G}, * \colon \mathsf{G} \times \mathsf{G} \to \mathsf{G}, \mathsf{exp} \colon \mathsf{G} \times \mathsf{Int} \to \mathsf{G}\}$. Let the set $\mathcal{E}$ of CEs consist of:

$$\begin{array}{rcl@{\qquad}rcl}
(x * y) * z & \approx & x * (y * z) & \mathsf{e} * x & \approx & x \\
\mathsf{inv}(x) * x & \approx & \mathsf{e} & \mathsf{exp}(x, 0) & \approx & \mathsf{e} \\
\mathsf{exp}(x, 1) & \approx & x & \Pi\{n, m\}.\, \mathsf{exp}(x, n) * \mathsf{exp}(x, m) & \approx & \mathsf{exp}(x, m + n)
\end{array}$$

As in first-order equational reasoning, one can show $x * \mathsf{e} \overset{*}{\leftrightarrow}_{\mathcal{E}} x$. Thus, $\mathsf{exp}(x, -1) \leftrightarrow_{\mathcal{E}} \mathsf{e} * \mathsf{exp}(x, -1) \leftrightarrow_{\mathcal{E}} (\mathsf{inv}(x) * x) * \mathsf{exp}(x, -1) \leftrightarrow_{\mathcal{E}} \mathsf{inv}(x) * (x * \mathsf{exp}(x, -1)) \leftrightarrow_{\mathcal{E}} \mathsf{inv}(x) * (\mathsf{exp}(x, 1) * \mathsf{exp}(x, -1)) \leftrightarrow_{\mathcal{E}} \mathsf{inv}(x) * \mathsf{exp}(x, 1 + (-1)) \leftrightarrow_{\mathcal{E}} \mathsf{inv}(x) * \mathsf{exp}(x, 0) \leftrightarrow_{\mathcal{E}} \mathsf{inv}(x) * \mathsf{e} \overset{*}{\leftrightarrow}_{\mathcal{E}} \mathsf{inv}(x)$ as expected. This encodes a system of groups with an explicit exponentiation operator exp.

▶ **Example 3.6.** Consider integer arithmetic as the underlying model $\mathcal{M}$. We take a term signature $\mathcal{S}_{\mathsf{te}} = \{\mathsf{Elem}, \mathsf{List}, \mathsf{ElemOp}\}$ and $\mathcal{F}_{\mathsf{te}} = \{\mathsf{nil} \colon \mathsf{List}, \mathsf{cons} \colon \mathsf{Elem} \times \mathsf{List} \to \mathsf{List}, \mathsf{none} \colon \mathsf{ElemOp}, \mathsf{some} \colon \mathsf{Elem} \to \mathsf{ElemOp}, \mathsf{length} \colon \mathsf{List} \to \mathsf{Int}, \mathsf{nth} \colon \mathsf{List} \times \mathsf{Int} \to \mathsf{ElemOp}\}$. Let the set $\mathcal{E}$ of CEs consist of

$$\begin{array}{rcl@{\qquad}rcll}
\mathsf{length}(\mathsf{nil}) & \approx & 0 & \mathsf{length}(\mathsf{cons}(x, xs)) & \approx & \mathsf{length}(xs) + 1 & \\
\Pi\{n\}.\, \mathsf{nth}(\mathsf{nil}, n) & \approx & \mathsf{none} & \mathsf{nth}(xs, n) & \approx & \mathsf{none} & [n < 0] \\
\mathsf{nth}(\mathsf{cons}(x, xs), 0) & \approx & \mathsf{some}(x) & \mathsf{nth}(\mathsf{cons}(x, xs), n) & \approx & \mathsf{nth}(xs, n - 1) & [n > 0]
\end{array}$$

This LCES encodes common list functions that use integers. For program verification purposes, one may deal with the validity problem of a formula such as $\mathsf{nth}(xs, n) \not\approx \mathsf{none} \Leftrightarrow 0 \leqslant n \wedge n < \mathsf{length}(xs)$.

We continue by giving some immediate facts which are used later on.

▶ **Lemma 3.7.** *Let $\mathcal{E}$ be an LCES over the underlying model $\mathfrak{U} = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{F}_{\mathsf{th}}, \mathcal{M} \rangle$ and the term signature $\Sigma_{\mathsf{te}} = \langle \mathcal{S}_{\mathsf{te}}, \mathcal{F}_{\mathsf{te}} \rangle$. Then, all of the following hold:*

1. *$\leftrightarrow_{\mathcal{E}}$ is symmetric,*
2. *$\leftrightarrow_{\mathcal{E}}$ is closed under contexts i.e. $s \leftrightarrow_{\mathcal{E}} t$ implies $C[s] \leftrightarrow_{\mathcal{E}} C[t]$ for any context C, and*
3. *$\leftrightarrow_{\mathcal{E}}$ is closed under substitutions, i.e. $s \leftrightarrow_{\mathcal{E}} t$ implies $s\sigma \leftrightarrow_{\mathcal{E}} t\sigma$ for any substitution σ.*

Proof (Sketch). **1** and **2** are trivial. For **3** the case $s \leftrightarrow_{\mathsf{calc}} t$ is clear. Suppose $s \leftrightarrow_{\mathsf{rule},\mathcal{E}} t$. Then $s = C[\ell\rho]$ and $t = C[r\rho]$ (or vice versa) for some CE $\Pi X.\, \ell \approx r\ [\varphi] \in \mathcal{E}$ and an X-valued substitution ρ such that $\models_{\mathcal{M}} \varphi\rho$. Then $\varphi\rho = (\varphi\rho)\sigma = \varphi(\sigma \circ \rho)$ and hence $\models_{\mathcal{M}} \varphi(\sigma \circ \rho)$. Then, the claim follows, as $s\sigma = C[\ell\rho]\sigma = C\sigma[\ell(\sigma \circ \rho)]$ and $t\sigma = C[r\rho]\sigma = C\sigma[r(\sigma \circ \rho)]$. ◀

We proceed by defining constrained equational theories (CE-theories) and validity of CEs (CE-validity) with respect to a CE-theory.

▶ **Definition 3.8** (constrained equational theory)**.** *A* constrained equational theory *is specified by a triple $\mathfrak{T} = \langle \mathfrak{U}, \Sigma_{\mathsf{te}}, \mathcal{E}\rangle$, where $\mathfrak{U} = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{F}_{\mathsf{th}}, \mathcal{M}\rangle$ is an underlying model, Σ_{te} is a term signature over $\mathfrak{U}$ (as given in the LCTRS formalism), and $\mathcal{E}$ is an LCES over $\mathfrak{U}, \Sigma_{\mathsf{te}}$. If no confusion arises, we refer to the CE-theory by $\langle \mathcal{M}, \mathcal{E}\rangle$, without stating its signature explicitly. We also say that a CE-theory $\langle \mathcal{M}, \mathcal{E}\rangle$ is defined over the signature $\Sigma = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{S}_{\mathsf{te}}, \mathcal{F}_{\mathsf{th}}, \mathcal{F}_{\mathsf{te}}\rangle$ in order to make the signature explicit.*

▶ **Definition 3.9** (CE-validity)**.** *Let $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E}\rangle$ be a CE-theory. Then a CE $\Pi X.\, s \approx t\ [\varphi]$ is said to be a* constrained equational consequence *(CE-consequence, for short)* of $\mathfrak{T}$ *or* valid *(CE-valid, for clarity), written as $\mathfrak{T} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$, if $s\sigma \xleftrightarrow{*}_{\mathcal{E}} t\sigma$ for all X-valued substitutions σ such that $\models_{\mathcal{M}} \varphi\sigma$. We write $\mathcal{E} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$ if $\mathcal{M}$ is known from the context.*

We conclude this subsection with an example on CE-validity.

▶ **Example 3.10.** Consider integer arithmetic as the underlying model $\mathcal{M}$. We take the term signature $\mathcal{F}_{\mathsf{te}} = \{\mathsf{abs}\colon \mathsf{Int} \to \mathsf{Int}, \mathsf{max}\colon \mathsf{Int} \times \mathsf{Int} \to \mathsf{Int}\}$ the set of CEs $\mathcal{E}$ consisting of

$$\begin{array}{rcll@{\qquad\qquad}rcll} \mathsf{abs}(x) & \approx & -x & [x < \mathsf{0}] & \mathsf{abs}(x) & \approx & x & [x \geqslant \mathsf{0}] \\ \mathsf{max}(x,y) & \approx & x & [x \geqslant y] & \mathsf{max}(x,y) & \approx & y & [x < y] \end{array}$$

The following are valid CE-consequences:

$$\mathfrak{T} \models_{\mathsf{cec}} \Pi\{x\}.\, \mathsf{abs}(x) \approx \mathsf{abs}(-x) \qquad \mathfrak{T} \models_{\mathsf{cec}} \Pi\{x,y\}.\, \mathsf{max}(x,y) \approx \mathsf{max}(y,x)$$
$$\mathfrak{T} \models_{\mathsf{cec}} \Pi\{x,y\}.\, \mathsf{abs}(\mathsf{max}(x,y)) \approx \mathsf{max}(\mathsf{abs}(x), \mathsf{abs}(y))\ [\mathsf{0} \leqslant x \wedge \mathsf{0} \leqslant y]$$

On the other hand, the CE $\Pi\varnothing.\, \mathsf{abs}(x) \approx \mathsf{abs}(-x)$ is not a valid CE-consequence: For the $\varnothing$-valued identity substitution σ, we have that $\mathsf{abs}(x)\sigma = \mathsf{abs}(x) \not\xleftrightarrow{*}_{\mathcal{E}} \mathsf{abs}(-x) = \mathsf{abs}(-x)\sigma$.

3.2 Properties of CE-Validity

This subsection covers important properties related to CE-validity, for example, we show that validity forms an equivalence and a congruence relation. Furthermore, we cover in which way it is closed under substitutions and contexts, and how equality can be induced from constraints.

Our first two lemmas follow immediately from the definition of the CE-validity.

▶ **Lemma 3.11.** *Let $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E}\rangle$ be a CE-theory. Then for any $\Pi X.\, s \approx t\ [\varphi] \in \mathcal{E}$, we have $\mathfrak{T} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$.*

▶ **Lemma 3.12** (congruence)**.** *Let $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E}\rangle$ be a CE-theory. For any set $X \subseteq \mathcal{V}_{\mathsf{th}}$ and logical constraint φ such that $\mathcal{V}\mathsf{ar}(\varphi) \subseteq X$, the binary relation $\mathfrak{T} \models_{\mathsf{cec}} \Pi X.\, \cdot \approx \cdot\ [\varphi]$ over terms is a congruence relation over Σ.*

For stability under substitutions, we differentiate two kinds; for each CE $\Pi X.\, s \approx t\ [\varphi]$, the first one considers substitutions instantiating variables in X; the second one considers substitutions instantiating variables not in X.

▶ **Lemma 3.13** (stability of theory terms). *Let $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E} \rangle$ be a CE-theory. Let $X, Y \subseteq \mathcal{V}_{\mathsf{th}}$ be sets of theory variables and σ a substitution such that $\sigma(y) \in \mathcal{T}(\mathcal{F}_{\mathsf{th}}, X)$ for any $y \in Y$. If $\mathfrak{T} \models_{\mathsf{cec}} \Pi Y.\, s \approx t\ [\varphi]$, then $\mathfrak{T} \models_{\mathsf{cec}} \Pi X.\, s\sigma \approx t\sigma\ [\varphi\sigma]$.*

Proof (Sketch). Take any X-valued substitution θ with $\models_{\mathcal{M}} (\varphi\sigma)\theta$. This gives a Y-valued substitution ξ by defining $\xi(y) = [\![(\theta \circ \sigma)(y)]\!]$ for each $y \in Y$. From Lemma 2.3, we know $(\theta \circ \sigma)(y) \overset{*}{\leftrightarrow}_{\mathcal{E}} \xi(y)$ for any $y \in Y$. We also have $\models_{\mathcal{M}} \varphi\xi$ by Lemma 2.1, and hence $s\xi \overset{*}{\leftrightarrow}_{\mathcal{E}} t\xi$ by assumption. Thus, using Lemma 3.7, we obtain $(s\sigma)\theta = s(\theta \circ \sigma) \overset{*}{\leftrightarrow}_{\mathcal{E}} s\xi \overset{*}{\leftrightarrow}_{\mathcal{E}} t\xi \overset{*}{\leftrightarrow}_{\mathcal{E}} t(\theta \circ \sigma) = (t\sigma)\theta$. ◀

▶ **Lemma 3.14** (general stability). *Let $\langle \mathcal{M}, \mathcal{E} \rangle$ be a CE-theory and σ a substitution such that $\mathcal{D}\mathsf{om}(\sigma) \cap X = \varnothing$. Then, if $\mathcal{E} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$ then $\mathcal{E} \models_{\mathsf{cec}} \Pi X.\, s\sigma \approx t\sigma\ [\varphi]$.*

Proof (Sketch). Take any X-valued substitution δ such that $\models_{\mathcal{M}} \varphi\delta$. Take $\gamma = \delta \circ \sigma$. From $\mathcal{D}\mathsf{om}(\sigma) \cap X = \varnothing$, we have $\varphi\gamma = \varphi\delta$, and therefore, $s\sigma\delta \overset{*}{\leftrightarrow}_{\mathcal{E}} t\sigma\delta$ holds. ◀

One may expect that $\mathcal{E} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$ holds for equivalent terms s, t such that $\varphi \Rightarrow s = t$ is valid. In fact, a more general result can be obtained.

▶ **Lemma 3.15** (model consequence). *Let $\langle \mathcal{M}, \mathcal{E} \rangle$ be a CE-theory, $X \subseteq \mathcal{V}_{\mathsf{th}}$ a set of theory variables, $s, t \in \mathcal{T}(\mathcal{F}_{\mathsf{th}}, X)$, and φ a logical constraint over X. If $\models_{\mathcal{M}} (\varphi\sigma \Rightarrow s\sigma = t\sigma)$ holds for all X-valued substitutions σ, then $\mathcal{E} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$.*

Proof (Sketch). For any X-valued substitution σ with $\models_{\mathcal{M}} \varphi\sigma$, we have $[\![s\sigma]\!]_{\mathcal{M}} = [\![t\sigma]\!]_{\mathcal{M}}$. Then, use Lemma 2.3 to obtain $s\sigma \overset{*}{\leftrightarrow}_{\mathcal{E}} t\sigma$. ◀

▶ **Corollary 3.16.** *Let $\langle \mathcal{M}, \mathcal{E} \rangle$ be a CE-theory, $X \subseteq \mathcal{V}_{\mathsf{th}}$ a set of theory variables, and $\varphi \Rightarrow s = t$ a logical constraint over X such that $\models_{\mathcal{M}} (\varphi \Rightarrow s = t)$. Then, $\mathcal{E} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$.*

3.3 Relations to Conversion of Rewrite Steps

In this subsection, we present characterizations of CE-validity from the perspective of logically constrained rewriting with respect to equations.

▶ **Theorem 3.17.** *For a CE-theory $\langle \mathcal{M}, \mathcal{E} \rangle$, $s \overset{*}{\leftrightarrow}_{\mathcal{E}} t$ if and only if $\mathcal{E} \models_{\mathsf{cec}} \Pi\varnothing.\, s \approx t\ [\mathsf{true}]$.*

Proof (Sketch). We have $\mathcal{E} \models_{\mathsf{cec}} \Pi\varnothing.\, s \approx t\ [\mathsf{true}]$ if and only if $s\sigma \overset{*}{\leftrightarrow}_{\mathcal{E}} t\sigma$ for any $\varnothing$-valued substitution σ such that $\sigma \models \mathsf{true}$ if and only if $s\sigma \overset{*}{\leftrightarrow}_{\mathcal{E}} t\sigma$ for any substitution σ. Thus, the claim follows by Lemma 3.7. ◀

We consider now the general case with a possibly non-empty set X of theory variables and a non-trivial constraint $\varphi \neq \mathsf{true}$ (also $\neg\varphi$) for the CE $\Pi X.\, s \approx t\ [\varphi]$. In this case, the following partial characterization can be made by using the notion of trivial CEs [17]. We can naturally extend the notion of trivial CEs in [17] to our setting as follows: a CE $\Pi X.\, s \approx t\ [\varphi]$ is said to be *trivial* if $s\sigma = t\sigma$ for any X-valued substitution σ such that $\models_{\mathcal{M}} \varphi\sigma$.

▶ **Theorem 3.18.** *Let $\langle \mathcal{M}, \mathcal{E} \rangle$ be a CE-theory, and $\Pi X.\, s \approx t\ [\varphi]$ a CE. Suppose $s \overset{*}{\leftrightarrow}_{\mathcal{E}} s'$ and $t \overset{*}{\leftrightarrow}_{\mathcal{E}} t'$ for some s', t' such that $\Pi X.\, s' \approx t'\ [\varphi]$ is trivial. Then, $\mathcal{E} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$.*

Proof (Sketch). Take an arbitrary X-valued substitution σ such that $\models_{\mathcal{M}} \varphi\sigma$. Then, it follows from our assumptions that $s\sigma \overset{*}{\leftrightarrow}_{\mathcal{E}} s'\sigma = t'\sigma \overset{*}{\leftrightarrow}_{\mathcal{E}} t\sigma$. ◀

Unfortunately, none of the CE-consequences in Example 3.10 can be handled by Theorems 3.17 and 3.18.

4 Proving CE-Validity

As mentioned in the previous section, CE-validity of a CE $\Pi X.\, s \approx t\ [\varphi]$ with respect to a CE-theory $\langle \mathcal{M}, \mathcal{E} \rangle$ is very tedious to be shown by the convertibility of s and t in $\mathcal{E}$. This motivates us to introduce another approach to reason about CE-validity. In this section, we introduce an inference system for proving CE-validity of CEs together with a discussion on its applicability and generality.

4.1 Inference System CEC_0 and Its Soundness

In this subsection, we introduce an inference system $\mathbf{CEC}_0$ (*Constrained Equational Calculus for elementary steps*) for proving CE-validity of CEs. We prove soundness of it, by which it is guaranteed that all CEs $\Pi X.\, s \approx t\ [\varphi]$ derivable from $\mathcal{E}$ in the system $\mathbf{CEC}_0$ are valid, i.e. $\mathcal{E} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$.

▶ **Definition 4.1** (derivation of $\mathbf{CEC}_0$)**.** *Let $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E} \rangle$ be a CE-theory. The inference system $\mathbf{CEC}_0$ consists of the inference rules given in Figure 2. We assume in the rules that X, Y range over a (possibly infinite) set of theory variables, φ ranges over logical constraints. Let $\Pi X.\, s \approx t\ [\varphi]$ be a CE. We say that $\Pi X.\, s \approx t\ [\varphi]$ is derivable in $\mathbf{CEC}_0$ from $\mathcal{E}$ (or $\Pi X.\, s \approx t\ [\varphi]$ is a consequence of $\mathcal{E}$), written by $\mathcal{E} \vdash_{\mathbf{CEC}_0} \Pi X.\, s \approx t\ [\varphi]$, if there exists a derivation of $\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]$ in the system $\mathbf{CEC}_0$. When no confusion arises, $\mathcal{E} \vdash_{\mathbf{CEC}_0} \Pi X.\, s \approx t\ [\varphi]$ is abbreviated as $\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]$.*

We proceed with intuitive explanations of each rule. The rules *Refl*, *Trans*, *Sym*, *Cong*, and *Rule* are counterparts of the inference rules used in equational logic.

In order to handle instantiations, we consider two cases, namely *Theory Instance* and *General Instance*. The former rule covers instantiations affecting the logical constraint whereas the latter covers the case not affecting it.

The *Weakening* and *Split* rules handle logical reasoning in constraints. The *Weakening* rule logically weakens the constraint equation by strengthening its constraint. Note here the direction of the entailment $\varphi \Rightarrow \psi$ in the side condition: the rule is sound because the constrained equation is valid under the stronger constraint φ if the equation is valid under the weaker constraint ψ. Since some rules, like *Cong* and *Trans*, have premises with equality constraints, it may be required to first apply the *Weakening* rule to synchronize the constraints before using these rules. On the other hand, in the *Split* rule, the constraint of the conclusion $\varphi \vee \psi$ is logically weaker than the independent ones, φ and ψ, in each premise. The inference is still sound as it only joins two premises. Using the *Split* rule, one can perform reasoning based on case analysis.

The *Axiom* rule makes it possible to use equational consequences entailed in the constraint part of equational reasoning. The *Abst* rule incorporates consequences entailed in the constraint part in a different way, that is, to infer a possible abstraction of the equation.

The rules *Enlarge* and *Restrict* are used to adjust the set of instantiated variables (the "ΠX" part of CEs), with the proviso that it does not affect the validity. Note that, in *Enlarge*, $Y \subseteq X$ implies the side condition $\mathcal{V}\mathsf{ar}(s,t) \cap (Y \setminus X) = \varnothing$. We also want to remark that despite its name, the restriction $X \subseteq Y$ can be added to *Enlarge*, provided that removed variables are not used in s, t (the side condition $\mathcal{V}\mathsf{ar}(s,t) \cap (Y \setminus X) = \varnothing$ has to be satisfied).

▶ **Lemma 4.2.** *Let $\langle \mathcal{M}, \mathcal{E} \rangle$ be a CE-theory. If $\mathcal{E} \vdash_{\mathbf{CEC}_0} \Pi X.\, s \approx t\ [\varphi]$, then $\Pi X.\, s \approx t\ [\varphi]$ is a CE.*

Refl
$$\frac{}{\mathcal{E} \vdash \Pi X.\, s \approx s\ [\varphi]}\ \mathcal{V}\mathsf{ar}(\varphi) \subseteq X$$

Trans
$$\frac{\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi] \quad \mathcal{E} \vdash \Pi X.\, t \approx u\ [\varphi]}{\mathcal{E} \vdash \Pi X.\, s \approx u\ [\varphi]}$$

Sym
$$\frac{\mathcal{E} \vdash \Pi X.\, t \approx s\ [\varphi]}{\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]}$$

Cong
$$\frac{\mathcal{E} \vdash \Pi X.\, s_1 \approx t_1\ [\varphi] \quad \dots \quad \mathcal{E} \vdash \Pi X.\, s_n \approx t_n\ [\varphi]}{\mathcal{E} \vdash \Pi X.\, f(s_1, \dots, s_n) \approx f(t_1, \dots, t_n)\ [\varphi]}$$

Rule
$$\frac{}{\mathcal{E} \vdash \Pi X.\, \ell \approx r\ [\varphi]}\ (\Pi X.\, \ell \approx r\ [\varphi]) \in \mathcal{E}$$

Theory Instance
$$\frac{\mathcal{E} \vdash \Pi Y.\, s \approx t\ [\varphi]}{\mathcal{E} \vdash \Pi X.\, s\sigma \approx t\sigma\ [\varphi\sigma]}\ \forall x \in Y.\ x\sigma \in \mathcal{T}(\mathcal{F}_{\mathsf{th}}, X)$$

General Instance
$$\frac{\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]}{\mathcal{E} \vdash \Pi X.\, s\sigma \approx t\sigma\ [\varphi]}\ \mathcal{D}\mathsf{om}(\sigma) \cap X = \varnothing$$

Weakening
$$\frac{\mathcal{E} \vdash \Pi X.\, s \approx t\ [\psi]}{\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]}\ \models_{\mathcal{M}} (\varphi \Rightarrow \psi), \mathcal{V}\mathsf{ar}(\varphi) \subseteq X$$

Split
$$\frac{\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi] \quad \mathcal{E} \vdash \Pi X.\, s \approx t\ [\psi]}{\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi \vee \psi]}$$

Axiom
$$\frac{}{\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]}\ \begin{array}{l}\models_{\mathcal{M}} (\varphi\sigma \Rightarrow s\sigma = t\sigma) \text{ for all } \sigma \text{ s.t. } X \subseteq \mathcal{VD}\mathsf{om}(\sigma),\\ \mathcal{V}\mathsf{ar}(\varphi) \subseteq X\end{array}$$

Abst
$$\frac{\mathcal{E} \vdash \Pi X.\, s\sigma \approx t\sigma\ [\varphi\sigma]}{\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]}\ \begin{array}{l}\models_{\mathcal{M}} (\varphi \Rightarrow \bigwedge_{x \in X} x = \sigma(x)),\\ \mathcal{V}\mathsf{ar}(\varphi) \subseteq X, (\bigcup_{x \in X} \mathcal{V}\mathsf{ar}(\sigma(x))) \subseteq X\end{array}$$

Enlarge
$$\frac{\mathcal{E} \vdash \Pi Y.\, s \approx t\ [\varphi]}{\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]}\ \mathcal{V}\mathsf{ar}(s,t) \cap (Y \setminus X) = \varnothing,\ \mathcal{V}\mathsf{ar}(\varphi) \subseteq X$$

Figure 2 Inference rules of $\mathbf{CEC}_0$.

Proof (Sketch). The proof proceeds by induction on the derivation of $\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]$ that (1) $s, t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ have the same sort, (2) φ is a logical constraint, (3) $X \subseteq \mathcal{V}_{\mathsf{th}}$, and (4) $\mathcal{V}\mathsf{ar}(\varphi) \subseteq X$. ◀

Below we present some examples of derivations which cover all of our inference rules at least once. In the following example we denote *Theory Instance* by *TInst* and *General Instance* by *GInst* accordingly.

▶ **Example 4.3.** Let $\langle \mathcal{M}, \mathcal{E} \rangle$ be the CE-theory given in Example 3.5. Below, we present a derivation of $\mathcal{E} \vdash \Pi\{n\}.\, \mathsf{exp}(x, n) * \mathsf{exp}(x, -n) \approx \mathsf{e}$.

$$\dfrac{\dfrac{\dfrac{}{\mathcal{E} \vdash \Pi\{n, m\}.\, \mathsf{exp}(x, n) * \mathsf{exp}(x, m) \approx \mathsf{exp}(x, n + m)}\,\mathit{Rule}}{\mathcal{E} \vdash \Pi\{n\}.\, \mathsf{exp}(x, n) * \mathsf{exp}(x, -n) \approx \mathsf{exp}(x, n + (-n))}\,\mathit{TInst} \qquad \begin{array}{c}(1)\\ \mathcal{E} \vdash \Pi\{n\}.\, \mathsf{exp}(x, n + (-n)) \approx \mathsf{e}\end{array}}{\mathcal{E} \vdash \Pi\{n\}.\, \mathsf{exp}(x, n) * \mathsf{exp}(x, -n) \approx \mathsf{e}}\,\mathit{Trans}$$

where (1) is

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\mathcal{E}\vdash x\approx x}\,\textit{Refl}}{\mathcal{E}\vdash \Pi\{n\}.\,x\approx x}\,\textit{Enlarge} \quad \dfrac{}{\mathcal{E}\vdash\Pi\{n\}.\,n+(-n)\approx 0}\,\textit{Axiom}}{\mathcal{E}\vdash \Pi\{n\}.\,\mathsf{exp}(x,n+(-n))\approx \mathsf{exp}(x,0)}\,\textit{Cong} \quad \dfrac{\dfrac{}{\mathcal{E}\vdash \mathsf{exp}(x,0)\approx\mathsf{e}}\,\textit{Rule}}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{exp}(x,0)\approx\mathsf{e}}\,\textit{Enlarge}}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{exp}(x,n+(-n))\approx\mathsf{e}}\,\textit{Trans}$$

Here, $\mathcal{E}\vdash\Pi\{n\}.\,n+(-n)\approx 0$ is derived by the *Axiom* rule, because of $\models_{\mathcal{M}} \sigma(n+(-n)) = 0$ holds for all $\{n\}$-valued substitutions σ.

▶ **Example 4.4.** Let $\langle\mathcal{M},\mathcal{E}\rangle$ be the CE-theory given in Example 3.6. Below, we present a derivation of $\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(x{::}y{::}zs, n+2)\approx\mathsf{nth}(zs,n)\ [n>0]$.

$$\dfrac{(2) \quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(x{::}xs,n)\approx\mathsf{nth}(xs,n-1)\ [n>0]}\,\textit{Rule}}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(x{::}xs,n+1)\approx\mathsf{nth}(xs,(n+1)-1)\ [n+1>0]}\,\textit{TInst} \quad (1)}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(x{::}xs,n+1)\approx\mathsf{nth}(xs,n)\ [n+1>0]}\,\textit{Trans}}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(x{::}xs,n+1)\approx\mathsf{nth}(xs,n)\ [n>0]}\,\textit{Weaken}}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(y{::}zs,n+1)\approx\mathsf{nth}(zs,n)\ [n>0]}\,\textit{GInst}}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(x{::}y{::}zs,n+2)\approx\mathsf{nth}(zs,n)\ [n>0]}\,\textit{Trans}$$

where (1) is

$$\dfrac{\dfrac{\dfrac{}{\mathcal{E}\vdash\Pi\{n\}.\,xs\approx xs}\,\textit{Refl} \quad \dfrac{}{\mathcal{E}\vdash\Pi\{n\}.\,(n+1)-1\approx n}\,\textit{Axiom}}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(xs,((n+1)-1)\approx\mathsf{nth}(xs,n)}\,\textit{Cong}}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(xs,((n+1)-1)\approx\mathsf{nth}(xs,n)\ [n+1>0]}\,\textit{Weaken}$$

and (2) is

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(x::xs,n)\approx\mathsf{nth}(xs,n-1)\ [n>0]}\,\textit{Rule}}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(x::xs,n+2)\approx\mathsf{nth}(xs,(n+2)-1)\ [n+2>0]}\,\textit{TInst} \quad (3)}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(x::xs,n+2)\approx\mathsf{nth}(xs,n+1)\ [n+2>0]}\,\textit{Trans}}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(x::ys,n+2)\approx\mathsf{nth}(ys,n+1)\ [n>0]}\,\textit{Weaken}}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(x::y::zs,n+2)\approx\mathsf{nth}(y::zs,n+1)\ [n>0]}\,\textit{GInst}$$

where (3) is

$$\dfrac{\dfrac{\dfrac{}{\mathcal{E}\vdash\Pi\{n\}.\,xs\approx xs}\,\textit{Refl} \quad \dfrac{}{\mathcal{E}\vdash\Pi\{n\}.\,(n+2)-1\approx n+1}\,\textit{Axiom}}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(xs,((n+2)-1)\approx\mathsf{nth}(xs,n+1)}\,\textit{Cong}}{\mathcal{E}\vdash\Pi\{n\}.\,\mathsf{nth}(xs,(n+2)-1)\approx\mathsf{nth}(xs,n+1)\ [n+2>0]}\,\textit{Weaken}$$

In the next example, we illustrate usages of the *Split* rule and the *Abst* rule.

▶ **Example 4.5.** Let $\mathsf{f}\colon \mathsf{Bool}\to\mathsf{Int}\in\mathcal{F}_{\mathsf{te}}$. Let $\mathcal{E}=\{\Pi\varnothing.\,\mathsf{f}(\mathsf{true})\approx 0\ [\mathsf{true}], \Pi\varnothing.\,\mathsf{f}(\mathsf{false})\approx 0\ [\mathsf{true}]\}$. Then we have $\mathsf{f}(\mathsf{true})\leftrightarrow_{\mathcal{E}} 0$ and $\mathsf{f}(\mathsf{false})\leftrightarrow_{\mathcal{E}} 0$. Thus, for all $\{x\}$-valued substitutions σ, we have $\mathsf{f}(x)\sigma \overset{*}{\leftrightarrow}_{\mathcal{E}} 0\sigma$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\mathcal{E}\vdash\Pi\varnothing.\,\mathsf{f}(\mathsf{true})\approx 0}\,\textit{Rule}}{\mathcal{E}\vdash\Pi\varnothing.\,\mathsf{f}(\mathsf{true})\approx 0\ [\mathsf{true}=\mathsf{true}]}\,\textit{Weaken}}{\mathcal{E}\vdash\Pi\{x\}.\,\mathsf{f}(x)\approx 0\ [x=\mathsf{true}]}\,\textit{Abst} \quad \dfrac{\dfrac{\dfrac{}{\mathcal{E}\vdash\Pi\varnothing.\,\mathsf{f}(\mathsf{false})\approx 0}\,\textit{Rule}}{\mathcal{E}\vdash\Pi\varnothing.\,\mathsf{f}(\mathsf{false})\approx 0\ [\mathsf{false}=\mathsf{false}]}\,\textit{Weaken}}{\mathcal{E}\vdash\Pi\{x\}.\,\mathsf{f}(x)\approx 0\ [x=\mathsf{false}]}\,\textit{Abst}}{\mathcal{E}\vdash\Pi\{x\}.\,\mathsf{f}(x)\approx 0\ [x=\mathsf{true}\vee x=\mathsf{false}]}\,\textit{Split}}{\mathcal{E}\vdash\Pi\{x\}.\,\mathsf{f}(x)\approx 0\ [\mathsf{true}]}\,\textit{Weaken}$$

We now present soundness of the system $\mathbf{CEC}_0$ with respect to CE-validity.

▶ **Theorem 4.6** (soundness of the system $\mathbf{CEC}_0$)**.** *Let $\langle \mathcal{M}, \mathcal{E} \rangle$ be a CE-theory and $\Pi X.\, s \approx t\ [\varphi]$ a CE. If $\mathcal{E} \vdash_{\mathbf{CEC}_0} \Pi X.\, s \approx t\ [\varphi]$, then $\mathcal{E} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$.*

Proof (Sketch). The proof proceeds by induction on the derivation. The cases for all rules except for *Abst* and *Enlarge* follow by Lemmas 3.11–3.15 and well-known properties in logic. For the case *Abst*, suppose that $\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]$ is derived from $\mathcal{E} \vdash \Pi X.\, s\sigma \approx t\sigma\ [\varphi\sigma]$ as given in Figure 2. Let ρ be an X-valued substitution such that $\models_{\mathcal{M}} \varphi\rho$. Then by the side conditions we have $[\![\rho(x)]\!] = [\![\rho(\sigma(x))]\!]$ for any $x \in X$. Hence, $\models_{\mathcal{M}} \varphi\sigma\rho$, and $s\sigma\rho \xleftrightarrow{*}_{\mathcal{E}} t\sigma\rho$ by the induction hypothesis. Then by $\mathcal{V}\mathsf{ar}(s,t) \subseteq X$, we have $s\rho \xleftrightarrow{*}_{\mathcal{E}} s\sigma\rho \xleftrightarrow{*}_{\mathcal{E}} t\sigma\rho \xleftrightarrow{*}_{\mathcal{E}} t\rho$. For the case *Enlarge*, suppose that $\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]$ is derived from $\mathcal{E} \vdash \Pi Y.\, s \approx t\ [\varphi]$ as given in Figure 2. Let δ be an X-valued substitution such that $\models_{\mathcal{M}} \varphi\delta$. Define a substitution δ' as follows: $\delta'(z^\tau) = c^\tau$ if $x \in Y \setminus X$, and $\delta'(x) = \delta(x)$ otherwise, where c^τ is (arbitrarily) taken from $\mathcal{V}\mathsf{al}^\tau$. Clearly, δ' is Y-valued. We also have $s\delta' = s\delta$, $t\delta' = t\delta$, and $\varphi\delta' = \varphi\delta$ by the side conditions. Thus, $s\delta = s\delta' \xleftrightarrow{*}_{\mathcal{E}} t\delta' = t\delta$ using the induction hypothesis. ◀

▶ Remark 4.7. We remark that some of our inference rules utilize validity in the model. Thus, $\mathbf{CEC}_0$ does not have convenient properties like recursive enumerability of its theorems like we are used to from other formal systems.

4.2 Partial Completeness of CEC_0

In this subsection, we present some results regarding the completeness property of $\mathbf{CEC}_0$.

▶ **Lemma 4.8.** *Let $\langle \mathcal{M}, \mathcal{E} \rangle$ be a CE-theory and $\Pi X.\, s \approx t\ [\varphi]$ a CE such that φ is satisfiable. Suppose $s\sigma = t\sigma$ for all X-valued substitutions σ such that $\models_{\mathcal{M}} \varphi\sigma$. Then $\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]$.*

Proof (Sketch). The case $s, t \in \mathcal{T}(\mathcal{F}_{\mathsf{th}}, X)$ follows by the assumption using the *Axiom* rule. Next, we consider the case $s = x \in \mathcal{V}$ with $x \notin X$. In this case, we can derive $t = x$ using the assumption, and the case follows using the *Refl* rule. For the general case, from the assumption, one can let $s = C[s_1, \ldots, s_n]$ and $t = C[t_1, \ldots, t_n]$ for a multi-hole context C and terms s_i, t_i $(1 \leqslant i \leqslant n)$ such that either one of s_i or t_i is a variable. Thus, by the previous cases, we know that $\mathcal{E} \vdash \Pi X.\, s_i \approx t_i\ [\varphi]$ for each $1 \leqslant i \leqslant n$, possibly using the *Sym* rule. Thus, the claim is obtained using *Refl*, *Trans* and *Cong* rules. ◀

▶ **Lemma 4.9.** *Let $\langle \mathcal{M}, \mathcal{E} \rangle$ be a CE-theory and $\Pi X.\, s \approx t\ [\varphi]$ a CE such that φ is satisfiable. Suppose $s\sigma \leftrightarrow^{=}_{\mathsf{calc}} t\sigma$ for all X-valued substitutions σ such that $\mathcal{D}\mathsf{om}(\sigma) = X$ and $\models_{\mathcal{M}} \varphi\sigma$. Then $\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]$.*

Proof (Sketch). First of all, the claim for the case $s, t \in \mathcal{T}(\mathcal{F}_{\mathsf{th}}, X)$ follows using the *Axiom* rule. If $s\sigma = t\sigma$ for all X-valued substitutions σ, the claim follows from Lemma 4.8. Thus, it remains to consider the case that there exists an X-valued substitution σ such that $s\sigma \leftrightarrow_{\mathsf{calc}} t\sigma$, $\models_{\mathcal{M}} \varphi\sigma$ and $X = \mathcal{D}\mathsf{om}(\sigma)$. Suppose that $s\sigma = C[f(v_1, \ldots, v_n)]_q$ and $t\sigma = C[v_0]_q$ with $f \in \mathcal{F}_{\mathsf{th}}$ and $v_0, \ldots, v_n \in \mathcal{V}\mathsf{al}$ such that $\mathcal{I}(f)(v_1, \ldots, v_n) = v_0$. As $\mathcal{D}\mathsf{om}(\sigma) = X$ and σ is X-valued, we have $s|_q = f(s_1, \ldots, s_n)$ with $s_1, \ldots, s_n \in \mathcal{V}\mathsf{al} \cup X$ and $t|_q \in \mathcal{V}\mathsf{al} \cup X$; hence $s|_q, t|_q \in \mathcal{T}(\mathcal{F}_{\mathsf{th}}, X)$, and thus, $\mathcal{E} \vdash \Pi X.\, s|_q \approx t|_q\ [\varphi]$ holds as we mentioned above. Let $s = C_1[f(s_1, \ldots, s_n)]_q$ and $t = C_2[t_0]_q$ with $C_1\sigma = C_2\sigma$ for any X-valued substitution σ such that $\mathcal{D}\mathsf{om}(\sigma) = X$ and $\models_{\mathcal{M}} \varphi\sigma$. Then, $\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]$ follows using $\mathcal{E} \vdash \Pi X.\, s|_q \approx t|_q\ [\varphi]$, Lemma 4.8, and the *Cong* and *Trans* rules. ◀

From Lemma 4.9, the partial completeness for at most one calculation step follows.

▶ **Theorem 4.10.** *Let $\langle \mathcal{M}, \mathcal{E} \rangle$ be a CE-theory and $\Pi X.\, s \approx t\ [\varphi]$ a CE such that φ is satisfiable. Suppose $s\sigma \leftrightarrow^{=}_{\mathsf{calc}} t\sigma$ for all X-valued substitutions σ such that $\models_{\mathcal{M}} \varphi\sigma$. Then $\mathcal{E} \vdash_{\mathbf{CEC}_0} \Pi X.\, s \approx t\ [\varphi]$.*

One may expect that Theorem 4.10 can be extended to the general completeness theorem for arbitrary $\mathcal{E}$ in such a way that $\mathcal{E} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$ implies $\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]$ (full completeness). Rephrasing this, we have: if $s\sigma \stackrel{*}{\leftrightarrow}_{\mathcal{E}} t\sigma$ for all X-valued substitutions σ such that $\models_{\mathcal{M}} \varphi\sigma$, then $\mathcal{E} \vdash \Pi X.\, s \approx t\ [\varphi]$. The partial completeness result above is far from this formulation of full completeness in that the assumption does not assume arbitrary conversions $s\sigma \stackrel{*}{\leftrightarrow}_{\mathcal{E}} t\sigma$ but only $s\sigma \leftrightarrow^{=}_{\mathsf{calc}} t\sigma$ (i.e. at most one calculation step). However, full completeness does not seem to hold for the system $\mathbf{CEC}_0$, as witnessed by the following example.

▶ **Example 4.11.** Consider the following LCES:

$$\mathcal{E} = \left\{ \begin{array}{ll} \Pi\{x\}.\, \mathsf{nneg}(x) \approx \mathsf{true}\ [x = 0] & (1) \\ \Pi\{x, y\}.\, \mathsf{nneg}(x) \approx \mathsf{nneg}(y)\ [x + 1 = y] & (2) \end{array} \right.$$

For each $n \geqslant 0$, we have $\mathsf{nneg}(n) \stackrel{*}{\leftrightarrow}_{\mathcal{E}} \mathsf{true}$:

$$\mathsf{nneg}(n) \leftrightarrow_{\mathcal{E}} \mathsf{nneg}(n-1) \leftrightarrow_{\mathcal{E}} \cdots \leftrightarrow_{\mathcal{E}} \mathsf{nneg}(0) \leftrightarrow_{\mathcal{E}} \mathsf{true}$$

Thus, for the CE $\Pi\{x\}.\, \mathsf{nneg}(x) \approx \mathsf{true}\ [x \geqslant 0]$, we have for all σ such that $\models_{\mathcal{M}} \sigma(x) \geqslant 0$, $\mathsf{nneg}(x)\sigma \stackrel{*}{\leftrightarrow}_{\mathcal{E}} \mathsf{true}\sigma = \mathsf{true}$. On the other hand, for each $n \geqslant 0$, one can give a derivation of $\Pi\varnothing.\, \mathsf{nneg}(n) \approx \mathsf{true}$ – for example, for $n = 2$,

$$\dfrac{\dfrac{\dfrac{}{(2)}\,\mathit{Rule}}{\Pi\varnothing.\, \mathsf{nneg}(2) \approx \mathsf{nneg}(1)}\,\mathit{TInst} \quad \dfrac{\dfrac{\dfrac{}{(2)}\,\mathit{Rule}}{\Pi\varnothing.\, \mathsf{nneg}(1) \approx \mathsf{nneg}(0)}\,\mathit{I} \quad \dfrac{\dfrac{}{(1)}\,\mathit{Rule}}{\Pi\varnothing.\, \mathsf{nneg}(0) \approx \mathsf{true}}\,\mathit{TInst}}{\Pi\varnothing.\, \mathsf{nneg}(1) \approx \mathsf{true}}\,\mathit{Trans}}{\Pi\varnothing.\, \mathsf{nneg}(2) \approx \mathsf{true}}\,\mathit{Trans}$$

However, these derivations differ for each $n \geqslant 0$, and and are hardly merged. As a conclusion, it seems that the CE $\Pi\{x\}.\, \mathsf{nneg}(x) \approx \mathsf{true}\ [x \geqslant 0]$ is beyond the derivability of $\mathbf{CEC}_0$.

▶ Remark 4.12. After looking at Example 4.11, it might seem reasonable that adding some kind of induction reasoning is required for our proof system. However, rules for the induction on positive integers, etc. are only possible when working with a specific model. Such rules have clearly a different nature than rules in our calculus that work with any underlying model. Our calculus $\mathbf{CEC}_0$ intends to be a general calculus that is free from specific underlying models and does not include model-specific rules.

▶ Remark 4.13. We remark a difficulty to extend Theorem 4.10 to multiple (calculation) steps, i.e. to have a statement like $\mathcal{E} \vdash_{\mathbf{CEC}_0} \Pi X.\, s \approx t\ [\varphi]$ whenever $s\sigma \leftrightarrow^{*}_{\mathsf{calc}} t\sigma$ for all X-valued substitutions σ such that $\models_{\mathcal{M}} \varphi\sigma$. Or even to obtain a slightly weaker statement like $\mathcal{E} \vdash_{\mathbf{CEC}_0} \Pi X.\, s \approx t\ [\varphi]$ whenever there exists a natural number n such that $s\sigma \leftrightarrow^{n}_{\mathsf{calc}} t\sigma$ for all X-valued substitutions σ such that $\models_{\mathcal{M}} \varphi\sigma$. It might look that induction on the length of $s\sigma \leftrightarrow^{*}_{\mathsf{calc}} t\sigma$ (or the one on n in the case of the latter) can be applied. However, to apply Theorem 4.10 to each step, we need the form $s_0\sigma \leftrightarrow_{\mathsf{calc}} s_1\sigma \leftrightarrow_{\mathsf{calc}} \cdots \leftrightarrow_{\mathsf{calc}} s_n\sigma$ for each σ which is not generally implied by $s\sigma \leftrightarrow^{*}_{\mathsf{calc}} t\sigma$ or $s\sigma \leftrightarrow^{n}_{\mathsf{calc}} t\sigma$, as intermediate terms may vary depending on the substitution σ. Extending Theorem 4.10 to multiple steps remains as our future work.

▶ Remark 4.14. Our final remark deals with the difficulty to extend Theorem 4.10 to a single rule step, i.e. to have a statement like $\mathcal{E} \vdash_{\mathbf{CEC}_0} \Pi X.\, s \approx t\ [\varphi]$ whenever $s\sigma \leftrightarrow_{\mathsf{rule},\mathcal{E}} t\sigma$ for all X-valued substitutions σ such that $\models_{\mathcal{M}} \varphi\sigma$. For the rule step, there may be multiple choices of positions and multiple choices of CEs to be applied for the step $s\sigma \leftrightarrow_{\mathsf{rule},\mathcal{E}} t\sigma$. Thus, we have to divide X-valued substitutions satisfying φ depending on each position p that a CE is applied and each applied CE $\Pi X_i.\, \ell_i \approx r_i\ [\varphi_i] \in \mathcal{E}$, and combine the obtained consequences. However, it is in general not guaranteed that such a division of substitutions can be characterized by a constraint. Note that the set of sets of substitutions is in general not countable but the set of constraints is countable. Thus, it may be necessary to assume some assumption on the expressiveness of constraints to obtain the extension for the single rule step. On the other hand, we conjecture that the (full) completeness would hold for CE-theories with a finite underlying model.

5 Algebraic Semantics for CE-Validity

In this section, we explore algebraic semantics for CE-validity. In this approach, CE-validity is characterized by validity in models in a class of algebras, which we call *CE-algebras*. We show that this characterization is sound and complete, in the sense that CE-validity can be fully characterized.

5.1 CE-Algebras

In this subsection, we introduce a notion of CE-algebras and validity in them. After presenting basic properties of our semantics, we prove its soundness with respect to the CE-validity.

▶ **Definition 5.1** (CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra)**.** *Let $\Sigma = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{S}_{\mathsf{te}}, \mathcal{F}_{\mathsf{th}}, \mathcal{F}_{\mathsf{te}} \rangle$ be a signature and $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$ be a model over $\mathcal{S}_{\mathsf{th}}$ and $\mathcal{F}_{\mathsf{th}}$. A* constrained equational $\langle \Sigma, \mathcal{M} \rangle$-algebra *(CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra, for short) is a pair $\mathfrak{M} = \langle \mathfrak{I}, \mathfrak{J} \rangle$ where $\mathfrak{I}$ assigns each $\tau \in \mathcal{S}$ a non-empty set $\mathfrak{I}(\tau)$, specifying its domain, and $\mathfrak{J}$ assigns each $f : \tau_1 \times \cdots \times \tau_n \to \tau_0 \in \mathcal{F}$ an interpretation function $\mathfrak{J}(f) : \mathfrak{I}(\tau_1) \times \cdots \times \mathfrak{I}(\tau_n) \to \mathfrak{I}(\tau_0)$ that extends the model $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$, that is, $\mathfrak{I}(\tau) \supseteq \mathcal{I}(\tau)$ for all $\tau \in \mathcal{S}_{\mathsf{th}}$ and $\mathfrak{J}(f) \restriction_{\mathcal{I}(\tau_1) \times \cdots \times \mathcal{I}(\tau_n)} = \mathcal{J}(f)$ for all $f \in \mathcal{F}_{\mathsf{th}}$ (or more generally there exists an injective homomorphism $\iota : \mathcal{M} \to \mathfrak{M}$).*

Let $\mathfrak{M} = \langle \mathfrak{I}, \mathfrak{J} \rangle$ be a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra. A valuation ρ over $\mathfrak{M}$ is defined similarly to $\mathcal{M}$, but $\mathcal{S}$ instead of $\mathcal{S}_{\mathsf{th}}$, $\mathcal{F}$ instead of $\mathcal{F}_{\mathsf{th}}$, etc. Similarly, a valuation ρ over $\mathfrak{M}$ satisfies a logical constraint φ, denoted by $\models_{\mathfrak{M}} \varphi$, if $[\![\varphi]\!]_{\rho,\mathfrak{M}} = \mathsf{true}$.

Careful readers may wonder why the interpretation functions for the theory part are not the same but an extension of the underlying model $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$. Indeed, in the definition of CE-$\langle \Sigma, \mathcal{M} \rangle$-algebras $\mathfrak{M} = \langle \mathfrak{I}, \mathfrak{J} \rangle$ above, we only demand that $\mathfrak{I}(\tau) \supseteq \mathcal{I}(\tau)$ for all $\tau \in \mathcal{S}_{\mathsf{th}}$ and not $\mathfrak{I}(\tau) = \mathcal{I}(\tau)$ for all $\tau \in \mathcal{S}_{\mathsf{th}}$. In fact, this is required to obtain the completeness result; however, this explanation is postponed until Example 5.18. We continue to present some basic properties of our semantics which are proven in a straightforward manner.

▶ **Lemma 5.2.** *Let $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E} \rangle$ be a CE-theory over a signature Σ, and $\mathfrak{M} = \langle \mathfrak{I}, \mathfrak{J} \rangle$ a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra. Then, the binary relation over terms given by $[\![\cdot]\!]_{\mathfrak{M},\rho} = [\![\cdot]\!]_{\mathfrak{M},\rho}$ for any valuation ρ on $\mathfrak{M}$, is closed under substitutions and contexts.*

▶ **Lemma 5.3.** *Let $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E} \rangle$ be a CE- theory over a signature Σ such that $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$, $\mathfrak{M}$ a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra, and $X \subseteq \mathcal{V}_{\mathsf{th}}$ a set of theory variables and suppose $t \in \mathcal{T}(\mathcal{F}_{\mathsf{th}}, X)$. Then, for any valuation ρ on $\mathfrak{M}$ such that $\rho(x) \in \mathcal{I}(\tau)$ for all $x^\tau \in X$, we have $[\![t]\!]_{\mathfrak{M},\rho} = [\![t]\!]_{\mathcal{M},\rho}$.*

Next, we extend the definition of validity on CE-algebras to CEs, by which we can give a notion of models of CE-theories, and the semantic consequence relation.

▶ **Definition 5.4** (model of constrained equational theory)**.** *Let $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E} \rangle$ be a CE-theory over a signature Σ such that $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$, and $\mathfrak{M} = \langle \mathfrak{I}, \mathfrak{J} \rangle$ a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra.*

1. *A CE $\Pi X.\, \ell \approx r\ [\varphi]$ is said to be* valid *in $\mathfrak{M}$, denoted by $\models_{\mathfrak{M}} \Pi X.\, \ell \approx r\ [\varphi]$, if for all valuations ρ over $\mathfrak{M}$ satisfying the constraint φ (i.e. $[\![\varphi]\!]_{\mathfrak{M},\rho} = \mathsf{true}$ holds) and $\rho(x) \in \mathcal{I}(\tau)$ holds for all $x^\tau \in X$, we have $[\![\ell]\!]_{\mathfrak{M},\rho} = [\![r]\!]_{\mathfrak{M},\rho}$.*
2. *A CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra $\mathfrak{M} = \langle \mathfrak{I}, \mathfrak{J} \rangle$ is said to be a* model *of the CE-theory $\mathfrak{T}$ if $\models_{\mathfrak{M}} \mathcal{E}$. Here, $\models_{\mathfrak{M}} \mathcal{E}$ denotes that $\models_{\mathfrak{M}} \Pi X.\, \ell \approx r\ [\varphi]$ for all $\Pi X.\, \ell \approx r\ [\varphi] \in \mathcal{E}$.*
3. *Let $\Pi X.\, \ell \approx r\ [\varphi]$ be a CE. We write $\mathfrak{T} \models \Pi X.\, \ell \approx r\ [\varphi]$ (or $\mathcal{E} \models \Pi X.\, \ell \approx r\ [\varphi]$ if no confusion arises) if $\models_{\mathfrak{M}} \Pi X.\, \ell \approx r\ [\varphi]$ holds for all CE-$\langle \Sigma, \mathcal{M} \rangle$-algebras $\mathfrak{M}$ that are models of $\mathfrak{T}$.*

We remark that, in item **1**, as $\varphi \in \mathcal{T}(\mathcal{F}_{\mathsf{th}}, \mathcal{V}_{\mathsf{th}})$, we have $[\![\varphi]\!]_{\mathfrak{M},\rho} = \mathsf{true}$ if and only if $[\![\varphi]\!]_{\mathcal{M},\rho} = \mathsf{true}$ by Lemma 5.3. Based on the preceding lemmas, soundness of our semantics with respect to conversion is not difficult to obtain.

▶ **Lemma 5.5** (soundness w.r.t. conversion)**.** *Let $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E} \rangle$ be a CE-theory over a signature Σ, and $\mathfrak{M} = \langle \mathfrak{I}, \mathfrak{J} \rangle$ a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra such that $\models_{\mathfrak{M}} \mathcal{E}$. If $s \overset{*}{\leftrightarrow}_{\mathcal{E}} t$ then $[\![s]\!]_{\mathfrak{M},\rho} = [\![t]\!]_{\mathfrak{M},\rho}$ for any valuation ρ on $\mathfrak{M}$.*

Proof (Sketch). It suffices to consider the case $s \leftrightarrow_{\mathcal{E}} t$ with a root step; the claim easily follows from Lemma 5.2. Let $\Sigma = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{S}_{\mathsf{te}}, \mathcal{F}_{\mathsf{th}}, \mathcal{F}_{\mathsf{te}} \rangle$ and $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$. Let $s \leftrightarrow_{\mathsf{calc}} t$. Then, $s, t \in \mathcal{T}(\mathcal{F}_{\mathsf{th}})$, and hence $[\![s]\!]_{\mathcal{M}} = [\![t]\!]_{\mathcal{M}}$. Thus, $[\![s]\!]_{\mathfrak{M}} = [\![t]\!]_{\mathfrak{M}}$ by Lemma 5.3. Otherwise, let $s \leftrightarrow_{\mathsf{rule},\mathcal{E}} t$. Then, $s = \ell\sigma$ and $t = r\sigma$ for some $\Pi X.\, \ell \approx r\ [\varphi] \in \mathcal{E}$ and an X-valued substitution σ such that $\models_{\mathcal{M}} \varphi\sigma$. We have a valuation $[\![\sigma]\!]_{\mathfrak{M},\rho}$ on $\mathfrak{M}$ by $[\![\sigma]\!]_{\mathfrak{M},\rho}(y) = [\![\sigma(y)]\!]_{\mathfrak{M},\rho}$ for any $y \in \mathcal{V}$. Then, similarly to Lemma 2.1, we have $[\![u\sigma]\!]_{\mathfrak{M},\rho} = [\![u]\!]_{\mathfrak{M},[\![\sigma]\!]_{\mathfrak{M},\rho}}$ for any term $u \in \mathcal{T}(\Sigma, \mathcal{V})$. Furthermore, for $x \in X$, $[\![\sigma]\!]_{\mathfrak{M},\rho}(x) = [\![\sigma(x)]\!]_{\mathfrak{M},\rho} = \sigma(x)$ holds. Hence, by Lemma 5.3, $[\![\varphi]\!]_{\mathfrak{M},[\![\sigma]\!]_{\mathfrak{M},\rho}} = \mathsf{true}$. Thus, $[\![s]\!]_{\mathfrak{M},\rho} = [\![\ell]\!]_{\mathfrak{M},[\![\sigma]\!]_{\mathfrak{M},\rho}} = [\![r]\!]_{\mathfrak{M},[\![\sigma]\!]_{\mathfrak{M},\rho}} = [\![t]\!]_{\mathfrak{M},\rho}$. ◀

Now we present the soundness of our semantics with respect to the CE-validity.

▶ **Theorem 5.6** (soundness w.r.t. CE-validity)**.** *Let $\mathfrak{T}$ be a CE-theory. If $\mathfrak{T} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$, then $\mathfrak{T} \models \Pi X.\, s \approx t\ [\varphi]$.*

Proof (Sketch). Let $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E} \rangle$ and $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$. Suppose $\mathfrak{M} = \langle \mathfrak{I}, \mathfrak{J} \rangle$ is a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra such that $\models_{\mathfrak{M}} \mathcal{E}$. Let ρ be a valuation over $\mathfrak{M}$ satisfying the constraints φ and $\rho(x) \in \mathcal{I}(\tau)$ holds for all $x^\tau \in X$. Now, let $\hat{\rho}$ be a valuation that is obtained from ρ by restricting its domain to X. Then, $\models_{\mathcal{M}} \varphi\hat{\rho}$ by Lemma 5.3, and thus $s\hat{\rho} \overset{*}{\leftrightarrow}_{\mathcal{E}} t\hat{\rho}$ holds. Hence, by Lemma 5.5, $[\![s\hat{\rho}]\!]_{\mathfrak{M},\tau} = [\![t\hat{\rho}]\!]_{\mathfrak{M},\tau}$ holds for any valuation τ. This means that $[\![s]\!]_{\mathfrak{M},\tau'} = [\![t]\!]_{\mathfrak{M},\tau'}$ for any extension τ' of $\hat{\rho}$. In particular, one obtains $[\![s]\!]_{\mathfrak{M},\rho} = [\![t]\!]_{\mathfrak{M},\rho}$. ◀

The combination of Theorem 4.6 and Theorem 5.6 implies the following corollary.

▶ **Corollary 5.7** (soundness of $\mathbf{CEC}_0$ w.r.t. algebraic semantics)**.** *Let $\mathfrak{T}$ be a CE-theory. If $\mathfrak{T} \vdash_{\mathbf{CEC}_0} \Pi X.\, s \approx t\ [\varphi]$, then $\mathfrak{T} \models \Pi X.\, s \approx t\ [\varphi]$.*

▶ **Example 5.8.** Consider integer arithmetic for the underlying model $\mathcal{M}$. Take a term signature $\mathcal{F}_{\mathsf{te}} = \{\mathsf{a} \colon \mathsf{Int}\}$. Consider the LCES $\mathcal{E} = \{\mathsf{a} \approx \mathsf{0}, \mathsf{a} \approx \mathsf{1}\}$ with $\mathsf{0}, \mathsf{1} \in \mathcal{V}\mathsf{al}$ and $0, 1 \in \mathbb{Z}$, hence $\mathcal{J}(\mathsf{0}) = 0$ and $\mathcal{J}(\mathsf{1}) = 1$. Then, for any valuation ρ on a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra $\mathfrak{M} = \langle \mathfrak{I}, \mathfrak{J} \rangle$ we have $\rho(\mathsf{0}) = 0$ and $\rho(\mathsf{1}) = 1$. Thus, if $\mathfrak{M}$ is a model of $\mathcal{E}$ then it follows that $0 = [\![\mathsf{0}]\!] = [\![\mathsf{a}]\!] = [\![\mathsf{1}]\!] = 1$, which is a contradiction. Therefore, there is no CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra $\mathfrak{M}$ which validates $\mathcal{E}$.

This example motivates us to introduce the following definition of consistency for CE-theories.

▶ **Definition 5.9** (consistency). *A CE-theory is said to be* consistent *if it has a model.*

Our definition of consistent CE-theories does not exclude any theory that has only an almost trivial model such that $\mathcal{I}(\tau) = \{\bullet\}$ for all $\tau \in \mathcal{S}_{\mathsf{te}}$.

5.2 Completeness w.r.t. CE-Validity

In this subsection, we prove the completeness of algebraic semantics with respect to the CE-validity. That is, if a CE is valid in all models of a CE-theory then it is a CE-consequence of the CE-theory. We start by defining congruence relations, quotient algebras and term algebras that suit our formalism, incorporating standard notions for example the first-order equational logic, and then present basic results on them.

Let $\Sigma = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{S}_{\mathsf{te}}, \mathcal{F}_{\mathsf{th}}, \mathcal{F}_{\mathsf{te}} \rangle$ be a signature, $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$ a model over $\mathcal{S}_{\mathsf{th}}$ and $\mathcal{F}_{\mathsf{th}}$, and $\mathfrak{M} = \langle \mathfrak{I}, \mathfrak{J} \rangle$ a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra. A *congruence relation* on $\mathfrak{M}$ is an $\mathcal{S}$-indexed family of relations $\sim = (\sim^\tau)_{\tau \in \mathcal{S}}$ that satisfies all of the following:

1. $\sim^\tau$ is an equivalence relation on $\mathfrak{I}(\tau)$,
2. $\sim^\tau \cap\, \mathcal{I}(\tau)^2$ is the identity relation for $\tau \in \mathcal{S}_{\mathsf{th}}$, and
3. for each $f \colon \tau_1 \times \cdots \times \tau_n \to \tau_0 \in \mathcal{F}$, if $a_i \sim^{\tau_i} b_i$ for all $1 \leqslant i \leqslant n$ then $\mathfrak{J}(f)(a_1, \ldots, a_n) \sim^{\tau_0} \mathfrak{J}(f)(b_1, \ldots, b_n)$.

We note here that the difference from the standard notion of congruence relation on algebras is located in item **2**. Given a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra $\mathfrak{M} = \langle \mathfrak{I}, \mathfrak{J} \rangle$ and a congruence relation $\sim$ on it, the quotient CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra $\mathfrak{M}/{\sim} = \langle \mathfrak{I}', \mathfrak{J}' \rangle$ is defined as follows: $\mathfrak{I}'(\tau) = \mathfrak{I}(\tau)/{\sim^\tau} = \{\, [a]_{\sim^\tau} \mid a \in \mathfrak{I}(\tau) \,\}$ where $[a]_{\sim^\tau}$ is the equivalence class of $a \in \mathfrak{I}(\tau)$, i.e. $[a]_{\sim^\tau} = \{ b \in \mathfrak{I}(\tau) \mid a \sim^\tau b \}$, and $\mathfrak{J}'(f)([a_1]_{\sim^{\tau_1}}, \ldots, [a_n]_{\sim^{\tau_n}}) = [\mathfrak{J}(f)(a_1, \ldots, a_n)]_{\sim^{\tau_0}}$. It is easy to see that $\mathfrak{J}'$ is well-defined provided that $\sim$ is a congruence. When no confusion occurs, we omit the superscript τ from $\sim^\tau$.

▶ **Lemma 5.10** (quotient algebra). *Let $\mathfrak{M}$ be a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra, and $\sim$ a congruence on it. Then $\mathfrak{M}/{\sim}$ is a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra.*

Next, we define the term algebra. In contrast to the usual construction, for term CE-algebras we need to take care of identification induced by underlying models.

▶ **Definition 5.11** (term algebra). *Let $\Sigma = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{S}_{\mathsf{te}}, \mathcal{F}_{\mathsf{th}}, \mathcal{F}_{\mathsf{te}} \rangle$ be a signature, $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$ a model over $\mathcal{S}_{\mathsf{th}}$ and $\mathcal{F}_{\mathsf{th}}$, and U a set of variables. The* term algebra generated from U with $\mathcal{M}$ *(denoted by $T[\mathcal{M}](\Sigma, U)$) is a pair $\mathfrak{M} = \langle \mathfrak{I}, \mathfrak{J} \rangle$ where*

- $\mathfrak{I}(\tau) = \mathcal{T}(\mathcal{F}, U)^\tau/{\sim_{\mathsf{c}}}$, *and*
- $\mathfrak{J}(f)([t_1]_{\mathsf{c}}, \ldots, [t_n]_{\mathsf{c}}) = [f(t_1, \ldots, t_n)]_{\mathsf{c}}$ *for any $f \in \mathcal{F}$.*

Here, $\mathcal{F} = \mathcal{F}_{\mathsf{th}} \cup \mathcal{F}_{\mathsf{te}}$, $\sim_{\mathsf{c}} = \leftrightarrow^*_{\mathsf{calc}}$, and $[t]_{\mathsf{c}}$ denotes the $\sim_{\mathsf{c}}$-equivalence class containing a term t. Since $\leftrightarrow^*_{\mathsf{calc}}$ is sort preserving, we regard $\sim_{\mathsf{c}}$ as the sum of the τ-indexed family of relations $\sim^\tau_{\mathsf{c}}$ with $\tau \in \mathcal{S}$. Clearly, $\mathfrak{J}(f)$ is well-defined, since $\leftrightarrow^*_{\mathsf{calc}}$ is closed under contexts.

▶ **Lemma 5.12.** *Let $\Sigma = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{S}_{\mathsf{te}}, \mathcal{F}_{\mathsf{th}}, \mathcal{F}_{\mathsf{te}} \rangle$ be a signature, $\mathcal{M}$ a model over $\mathcal{S}_{\mathsf{th}}$ and $\mathcal{F}_{\mathsf{th}}$, and U a set of variables. Then, the term algebra $T[\mathcal{M}](\Sigma, U)$ is a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra.*

We introduce a syntactic counter part of the notion of consistency of CE-theories for which equivalence of the two notions will be proved only briefly.

▶ **Definition 5.13** (consistency w.r.t. values)**.** *A CE-theory* $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E} \rangle$ *is said to be* consistent with respect to values *(value-consistent, for short) if for any* $u, v \in \mathcal{V}\mathsf{al}^\tau$*,* $u \overset{*}{\leftrightarrow}_\mathcal{E} v$ *implies* $u = v$*.*

Based on the preparations so far, we now proceed to construct canonical models of CE-theories. The first step is to show that $\overset{*}{\leftrightarrow}_\mathcal{E}$ is a congruence relation on the term algebra for each CE-theory $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E} \rangle$; special attention on $\sim_\mathrm{c}$ is required.

▶ **Lemma 5.14.** *Let* $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E} \rangle$ *be a value-consistent CE-theory over a signature* Σ*, and* U *a set of variables. For any* $[s]_\mathrm{c}, [t]_\mathrm{c} \in T[\mathcal{M}](\Sigma, U)$*, let* $\sim_\mathcal{E} = \{ \langle [s]_\mathrm{c}, [t]_\mathrm{c} \rangle \mid s \overset{*}{\leftrightarrow}_\mathcal{E} t \}$*. Then,* $\sim_\mathcal{E}$ *is a congruence relation on the term algebra* $T[\mathcal{M}](\Sigma, U)$*.*

Proof (Sketch). Note first that $\sim_\mathcal{E}$ is well-defined because one has always $\leftrightarrow^*_{\mathsf{calc}} \subseteq \overset{*}{\leftrightarrow}_\mathcal{E}$. Let $\Sigma = \langle \mathcal{S}_{\mathsf{th}}, \mathcal{S}_{\mathsf{te}}, \mathcal{F}_{\mathsf{th}}, \mathcal{F}_{\mathsf{te}} \rangle$, $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$, and $T[\mathcal{M}](\Sigma, U) = \langle \mathfrak{I}, \mathfrak{J} \rangle$. We only present a proof that $\sim^\tau_\mathcal{E} \cap \mathcal{I}(\tau)^2$ equals the identity relation for $\tau \in \mathcal{S}_{\mathsf{th}}$ here. Let $\tau \in \mathcal{S}_{\mathsf{th}}$ and suppose $[u]_\mathrm{c} \sim^\tau_\mathcal{E} [v]_\mathrm{c}$ with $u, v \in \mathcal{I}(\tau) \cong \mathcal{V}\mathsf{al}^\tau$. Then, we have $u \overset{*}{\leftrightarrow}_\mathcal{E} v$ by the definition of $\sim_\mathcal{E}$, and by consistency w.r.t. values of the theory $\mathfrak{T}$, we obtain $u = v$ as $u, v \in \mathcal{V}\mathsf{al}$. Therefore, $[u]_\mathrm{c} = [v]_\mathrm{c}$. ◀

We give a construction of canonical models for each CE-theory $\mathcal{T}$.

▶ **Lemma 5.15.** *Let* $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E} \rangle$ *be a value-consistent CE-theory over a signature* Σ*. Then, the quotient* $\mathcal{T}_\mathcal{E} = T[\mathcal{M}](\Sigma, \mathcal{V})/\sim_\mathcal{E}$ *of the term algebra is a CE-*$\langle \Sigma, \mathcal{M} \rangle$*-algebra. Furthermore, both of the following hold:*

1. $\models_{\mathcal{T}_\mathcal{E}} \Pi X.\, s \approx t\ [\varphi]$ *if and only if* $\mathcal{E} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$*, and*
2. $\models_{\mathcal{T}_\mathcal{E}} \mathcal{E}$*.*

Proof (Sketch). That $\mathcal{T}_\mathcal{E}$ is a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra follows from Lemmas 5.10 and 5.14. Let us abbreviate $[[t]_\mathrm{c}]_{\sim_\mathcal{E}}$ as $[t]_\mathcal{E}$. First we claim that $[u\sigma]_\mathcal{E} = [\![u]\!]_{\mathcal{T}_\mathcal{E}, \rho}$ holds for any term u, for any substitution σ and valuation ρ on $\mathcal{T}_\mathcal{E}$ such that $\rho(x) = [\sigma(x)]_\mathcal{E}$, using induction on u.

1. ($\Rightarrow$) Let σ be an X-valued substitution such that $\models_\mathcal{M} \varphi\sigma$. Take a valuation ρ on $\mathcal{T}_\mathcal{E}$ as $\rho(x) = [\sigma(x)]_\mathcal{E}$. Then, $\rho(x) \in \mathcal{I}(\tau)$ for all $x^\tau \in X$ and $\models_\mathcal{M} \varphi\rho$. Thus, $[\![s]\!]_{\mathcal{T}_\mathcal{E}, \rho} = [\![t]\!]_{\mathcal{T}_\mathcal{E}, \rho}$. Hence, $[s\sigma]_\mathcal{E} = [t\sigma]_\mathcal{E}$ by the claim, and therefore, $s\sigma \overset{*}{\leftrightarrow}_\mathcal{E} t\sigma$. ($\Leftarrow$) Let ρ be a valuation over $\mathcal{T}_\mathcal{E}$ satisfying the constraints φ and $\rho(x) \in \mathcal{I}(\tau)$ for all $x \in X$. Take a substitution σ in such a way that $\sigma(x) = v_x$ for each $x \in X$, where $v_x \in \mathcal{V}\mathsf{al}^\tau$ such that $[v_x]_\mathcal{E} = \rho(x)$. By Lemma 5.3, $[\![\varphi]\!]_{\mathcal{M}, \rho} = \mathsf{true}$, and thus, $\models_\mathcal{M} \varphi\sigma$ by Lemma 2.1. Hence $s\sigma \overset{*}{\leftrightarrow}_\mathcal{E} t\sigma$, and thus $[s\sigma]_\mathcal{E} = [t\sigma]_\mathcal{E}$. Therefore $[\![s]\!]_{\mathcal{T}_\mathcal{E}, \rho} = [\![t]\!]_{\mathcal{T}_\mathcal{E}, \rho}$ by the claim.

Item **2** follows from item **1**. ◀

Before proceeding to the completeness theorem, we connect the two notions related to consistency (Definitions 5.9 and 5.13).

▶ **Lemma 5.16.** *A CE-theory* $\mathfrak{T}$ *is consistent if and only if it is consistent with respect to values.*

Proof (Sketch). ($\Rightarrow$) Suppose that $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E} \rangle$ is a CE-theory over a signature Σ and let $\mathcal{M} = \langle \mathcal{I}, \mathcal{J} \rangle$. Let $\mathfrak{M} = \langle \mathfrak{I}, \mathfrak{J} \rangle$ be a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra such that $\models_\mathfrak{M} \mathcal{E}$. Suppose $u, v \in \mathcal{V}\mathsf{al}^\tau$ with $u \overset{*}{\leftrightarrow}_\mathcal{E} v$. Then $[\![u]\!]_\mathfrak{M} = [\![v]\!]_\mathfrak{M}$ by Lemma 5.5. Therefore, by $u, v \in \mathcal{V}\mathsf{al}^\tau \cong \mathcal{I}(\tau) \subseteq \mathfrak{I}(\tau)$, we have $u = [\![u]\!]_\mathcal{M} = [\![u]\!]_\mathfrak{M} = [\![v]\!]_\mathfrak{M} = [\![v]\!]_\mathcal{M} = v$. ($\Leftarrow$) By Lemma 5.15, $\mathcal{T}_\mathcal{E}$ is a model of $\mathfrak{T}$. This witnesses that $\mathfrak{T}$ is consistent. ◀

We now arrive at the main theorem of this section.

▶ **Theorem 5.17** (completeness)**.** *Let $\mathfrak{T} = \langle \mathcal{M}, \mathcal{E} \rangle$ be a consistent CE-theory. Then, we have $\mathcal{E} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$ if and only if $\mathcal{E} \models \Pi X.\, s \approx t\ [\varphi]$.*

Proof. The *only if* part follows from Theorem 5.6. Thus, it remains to show the *if* part. Suppose contrapositively that $\mathcal{E} \models_{\mathsf{cec}} \Pi X.\, s \approx t\ [\varphi]$ does not hold. Then, by Lemma 5.15 **1**, $\not\models_{\mathcal{T}_\mathcal{E}} \Pi X.\, s \approx t\ [\varphi]$. Since $\models_{\mathcal{T}_\mathcal{E}} \mathcal{E}$, by Lemma 5.15 **2**, this witnesses that there exists a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra $\mathfrak{M}$ such that $\models_\mathfrak{M} \mathcal{E}$ but not $\models_\mathfrak{M} \Pi X.\, s \approx t\ [\varphi]$. This means $\mathcal{E} \not\models \Pi X.\, s \approx t\ [\varphi]$. This completes the proof of the *if* part. ◀

To conclude this section, we explain the postponed question from the beginning of the section on the definition of CE-algebras. The question was on why it is required to include those equipped with underlying extended models – if such models would not be allowed, one does not obtain the completeness result as witnessed by the following example.

▶ **Example 5.18.** Consider integer arithmetic for the underlying model $\mathcal{M}$. Take a term signature $\mathcal{F}_{\mathsf{te}} = \{\mathsf{f} \colon \mathsf{Ints} \to \mathsf{Bool}, \mathsf{g} \colon \mathsf{Ints} \to \mathsf{Bool}\}$. Consider the LCES $\mathcal{E} = \{\mathsf{f}(x) \approx \mathsf{true}\ [x \geqslant \mathsf{0}], \mathsf{f}(x) \approx \mathsf{true}\ [x < \mathsf{0}], \mathsf{g}(x) \approx \mathsf{true}\}$. By orienting the equations in an obvious way, we obtain a complete LCTRS (e.g. [13, 20]). Then as $\mathsf{g}(x){\downarrow} = \mathsf{true} \neq \mathsf{f}(x) = \mathsf{f}(x){\downarrow}$, it turns out that no conversions hold between $\mathsf{g}(x)$ and $\mathsf{f}(x)$. It follows from the Theorem 3.17 that $\mathcal{E} \not\models_{\mathsf{cec}} \Pi\varnothing.\, \mathsf{g}(x) \approx \mathsf{f}(x)$. Now, from Theorem 5.17, we have $\mathcal{E} \not\models \Pi\varnothing.\, \mathsf{g}(x) \approx \mathsf{f}(x)$, i.e. one should find a model that witnesses this invalidity. Indeed, one can take a CE-$\langle \Sigma, \mathcal{M} \rangle$-algebra $\mathfrak{M} = \langle \mathfrak{I}, \mathfrak{J} \rangle$ with $\mathfrak{I}(\mathsf{Ints}) = \mathbb{Z} \cup \{\bullet\}$, where $\bullet \notin \mathbb{Z}$, with the interpretations: $\mathfrak{J}(\mathsf{f})(\bullet) = \mathsf{false}$, $\mathfrak{J}(\mathsf{f})(a) = \mathsf{true}$ for all $a \in \mathbb{Z}$, and $\mathfrak{J}(\mathsf{g})(x) = \mathsf{true}$ for all $x \in \mathbb{Z} \cup \{\bullet\}$. On the other hand, if we would require to take $\mathfrak{I}(\mathsf{Ints}) = \mathbb{Z}$, then we do not get any model that invalidates this CE.

6 Related Work

Constrained rewriting began to be popular around 1990, which has been initiated by the motivation to achieve a tractable solution for completion modulo equations (such as AC, ACI, etc.), by separating off the (intractable) equational solving part as constraints. These constraints mainly consist of (dis)equality of built-in equational theories such as $x{*}y \approx_{AC} y{*}x$. A constrained completion procedure in such a framework is given in [10]; it is well-known that the specification language Maude also deals with such built-in theories [14]. This line of research was extended to a framework of rewriting with constraints of an arbitrary first-order formula in [10], where various completion methods have been developed for this. However, they, similar to us, mainly considered term algebras as the underlying models, because the main motivation was to deal with a wide range of completion problems by separating off some parts of the equational theory as constraints.

Another well-known type of constraints studied in the context of constrained rewriting is membership constraints of regular tree languages. This type of constraints is motivated by dealing with terms over an (order-)sorted signature and representing an infinite number of terms that obeys regular patterns obtained from divergence of theorem proving procedures. In this line of research, [5, 6] give a dedicated completion method for constrained rewrite systems with membership constraints of regular tree languages. Further a method for inductive theorem proving for conditional and constrained systems, which is based on tree grammars with constraints, has been proposed in [3]. We also want to mention [18] as a formalism with more abstract constraints – confluence of term rewrite systems with membership constraints over an arbitrary term set has been considered there.

The work in this era which is in our opinion closest to the LCTRSs formalism is the one given in [7]. This is also motivated by giving a link between (symbolic) equational deduction and constraint solving. Thus, they considered constraints of an arbitrary theory such as linear integer arithmetic, similarly to LCTRSs. Based on the initial model of this framework, they gave an operational semantics of constraint equational logic programming.

The introduction of the LCTRS framework is more recent, and was initiated by the motivation to deal with built-in data structures such as integers, bit-vectors etc. in order to verify programs written by real-world programming languages with the help of SMT-solvers. A detailed comparison to the works in this line of research has been given in [13].

All in all, to the best of our knowledge, there does not exist anything in the literature on algebraic semantics of constrained rewriting and Birkhoff style completeness, as considered in this paper.

7 Conclusion

With the goal to establish a semantic formalism of logically constrained rewriting, we have introduced the notions of constrained equations and CE-theories. For this, we have extended the form of these constrained equations by specifying explicitly the variables, which need to be instantiated by values, in order to treat equational properties in a uniform way. Then we have introduced a notion of CE-validity to give a uniform foundation from a semantic point of view for the LCTRS formalism. After establishing basic properties of the introduced validity, we have shown the relation to the conversion of rewriting. Then we presented a sound inference system $\mathbf{CEC}_0$ to prove validity of constrained equations in CE-theories. We have demonstrated its ability to establish validity via some examples. A partial completeness result and a discussion on why only partial completeness is obtained followed. Finally, we devised sound and complete algebraic semantics, which enables one to show invalidity of constrained equations in CE-theories. Furthermore, we have derived an important characterization of CE-theories, namely, consistency of CE-theories, for which the completeness theorem holds. Thus, we have established a basis for CE-theories and their validity by showing its fundamental properties and giving methods for proving and disproving the validity of constrained equations in CE-theories.

The question whether there exists a sound and complete proof system that captures CE-validity remains open. Part of our future work is the automation of proving validity of constrained equations.

This paper uses the initial formalism of LCTRSs given in [13]. However, there exists a variant which incorporates the interpretation of user-defined function symbols by the term algebra [4]. This variant is incomparable to the initial one. Nevertheless, to investigate the semantic side of LCTRSs, the initial formalism was a reasonable starting point. The adaptation of the current work to the extended formalism is also a part of our future work.

References

1. Takahito Aoto, Naoki Nishida, and Jonas Schöpf. Equational theories and validity for logically constrained term rewriting (full version). *CoRR*, abs/2405.01174, 2024. `doi:10.48550/arXiv.2405.01174`.
2. Franz Baader and Tobias Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998. `doi:10.1145/505863.505888`.

3 Adel Bouhoula and Florent Jacquemard. Sufficient completeness verification for conditional and constrained TRS. *Journal of Applied Logic*, 10(1):127–143, 2012. doi:10.1016/J.JAL.2011.09.001.

4 Ştefan Ciobâcă and Dorel Lucanu. A coinductive approach to proving reachability properties in logically constrained term rewriting systems. In *Proceedings of the 9th IJCAR*, volume 10900 of *Lecture Notes in Computer Science*, pages 295–311. Springer, 2018. doi:10.1007/978-3-319-94205-6_20.

5 Hubert Comon. Completion of rewrite systems with membership constraints. part I: deduction rules. *Journal of Symbolic Computation*, 25(4):397–419, 1998. doi:10.1006/JSCO.1997.0185.

6 Hubert Comon. Completion of rewrite systems with membership constraints. part II: constraint solving. *Journal of Symbolic Computation*, 25(4):421–453, 1998. doi:10.1006/JSCO.1997.0186.

7 John Darlington and Yike Guo. Constrained equational deduction. In *Proceedings of the 2nd CTRS*, volume 516 of *Lecture Notes in Computer Science*, pages 424–435. Springer, 1991. doi:10.1007/3-540-54317-1_111.

8 Heinz-Dieter Ebbinghaus, Jörg Flum, Wolfgang Thomas, and Ann S Ferebee. *Mathematical logic*, volume 1910. Springer, 1994.

9 Carsten Fuhs, Cynthia Kop, and Naoki Nishida. Verifying procedural programs via constrained rewriting induction. *ACM Transactions on Computational Logic*, 18(2):14:1–14:50, 2017. doi:10.1145/3060143.

10 Claude Kirchner and Hélène. Kirchner. Constrained equational reasoning. In *Proceedings of the 14th ISSAC*, pages 3824–389. ACM, 1989. doi:10.1145/74540.74585.

11 Misaki Kojima and Naoki Nishida. From starvation freedom to all-path reachability problems in constrained rewriting. In *Proceedings of the 25th PADL*, volume 13880 of *Lecture Notes in Computer Science*, pages 161–179. Springer Nature Switzerland, 2023. doi:10.1007/978-3-031-24841-2_11.

12 Misaki Kojima and Naoki Nishida. Reducing non-occurrence of specified runtime errors to all-path reachability problems of constrained rewriting. *Journal of Logical and Algebraic Methods in Programming*, 135:1–19, 2023. doi:10.1016/j.jlamp.2023.100903.

13 Cynthia Kop and Naoki Nishida. Term rewriting with logical constraints. In *Proceedings of the 9th FroCoS*, volume 8152 of *Lecture Notes in Computer Science*, pages 343–358, 2013. doi:10.1007/978-3-642-40885-4_24.

14 José Meseguer. Twenty years of rewriting logic. *Journal of Logic and Algebraic Programming*, 81(7-8):721–781, 2012. doi:10.1016/J.JLAP.2012.06.003.

15 Naoki Nishida and Sarah Winkler. Loop detection by logically constrained term rewriting. In *Proceedings of the 10th VSTTE*, volume 11294 of *Lecture Notes in Computer Science*, pages 309–321. Springer, 2018. doi:10.1007/978-3-030-03592-1_18.

16 Enno Ohlebusch. *Advanced Topics in Term Rewriting*. Springer, 2002. doi:10.1007/978-1-4757-3661-8.

17 Jonas Schöpf and Aart Middeldorp. Confluence criteria for logically constrained rewrite systems. In *Proceedings of the 29th CADE*, volume 14132 of *Lecture Notes in Artificial Intelligence*, pages 474–490, 2023. doi:10.1007/978-3-031-38499-8_27.

18 Yoshihito Toyama. Membership conditional term rewriting systems. *IEICE Transactions*, E72(11):1224–1229, 1989.

19 Dirk van Dalen. *Logic and Structure*. Springer-Verlag, Berlin, third edition, 1994.

20 Sarah Winkler and Aart Middeldorp. Completion for logically constrained rewriting. In *Proceedings of the 3rd FSCD*, volume 108 of *LIPIcs*, pages 30:1–30:18. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2018. doi:10.4230/LIPIcs.FSCD.2018.30.

21 Sarah Winkler and Georg Moser. Runtime complexity analysis of logically constrained rewriting. In *Proceedings of the 30th LOPSTR*, volume 12561 of *Lecture Notes in Computer Science*, pages 37–55, 2021. doi:10.1007/978-3-030-68446-4_2.