arXiv:2602.14636v1 [cs.LO] 16 Feb 2026

Rewriting Induction for Existentially Quantified Equations in Logically Constrained Rewriting (Full Version)*,**

Naoki Nishida✉, Kazushi Nishie, and Misaki Kojima✉

Graduate School of Informatics, Nagoya University,
Furo-cho, Chikusa-ku, 4648601 Nagoya, Japan
nishida@i.nagoya-u.ac.jp kojima@i.nagoya-u.ac.jp

Abstract. Rewriting Induction (RI) is a principle to prove that an equation over terms is an inductive theorem of a rewrite system, i.e., that any ground instance of the equation is a theorem of the rewrite system. RI has been adapted to several kinds of rewrite systems, and RI for constrained rewrite systems has been extended to inequalities. In this paper, we extend RI for constrained equations to existentially quantified equations in logically constrained rewriting. To this end, we first extend constrained equations by introducing existential quantification to the equation part of constrained equations. Then, in applying a constrained rewrite rule to such extended constrained equations, we introduce existential quantification to extra variables of the applied rule. Finally, using the extended application of constrained rewrite rules, we extend RI for constrained equations to existentially quantified equations.

Keywords: Constrained rewriting · Equivalence verification · Inductive theorem · Theorem proving

1 Introduction

在项重写领域，关于归纳定理的自动推理已得到充分研究。这里，项重写系统（简称 TRS） $\mathcal{R}$ 的归纳定理是一个方程 $s \approx t$ ，该方程在归纳意义上有效，即其所有基实例 $s\sigma \approx t\sigma$ 都是 $\mathcal{R}$—$s\sigma \leftrightarrow^*_{\mathcal{R}} t\sigma$的定理。作为证明归纳定理的原理，我们列举无归纳归纳 [25, 14] 和重写归纳（简称 RI） [30]„ 二者都称为隐式归纳原理。基于 RI 原理的框架（简称重写归纳框架）由推理规则组成，用于证明给定的方程是归纳定理。

* This work was partially supported by Denso Corporation, NSITEXE, JSPS KAKENHI Grant Number JP24K02900, Grant-in-Aid for JSPS Fellows Grant Number JP24KJ1240, and the Kayamori Foundation of Informational Science Advancement.

** This work was mainly done as the master's study of the second author who graduated in March 2020.

基于 RI 的方法是在重写归纳框架内，按照指定策略或以交互方式应用推理规则的过程。

In the last two decades, various RI-based methods for *constrained rewriting* have been developed [3, 31, 9, 23, 12]. Constrained rewrite systems have built-in semantics for some function and predicate symbols and can be computation models of not only functional but also imperative programs [7, 10, 13, 8, 36, 23, 12, 19, 5]. For this reason, it is worth developing verification techniques by means of constrained rewrite systems [12, 37, 6, 28, 5]. The recent trend of constrained rewrite systems is the formalism of *logically constrained term rewrite systems* (LCTRSs, for short) [22]. LCTRSs are used for several verification methods to ensure, e.g., termination [20, 11], equivalence [23, 12], reachability [6, 16], runtime errors [16, 15, 17], confluence [32, 33], total correctness [4], etc. RI has been extended to LCTRSs [23, 12] and an LCTRS tool for RI-based equivalence verification of constrained equations has been developed [24].

为了重新审视逻辑约束项重写系统的重写归纳框架，我们先来看一个简单的例子。

例*1.1.* 考虑以下整数签名上的逻辑约束项重写系统：

$$\mathcal{R}_1 = \{\ \mathsf{f}(x,y) \to x+z\ [x > y \wedge z \geq x],\quad \mathsf{f}(x,y) \to x\ [x \leq y]\ \ \}$$

约束等式 $\mathsf{f}(x,0) \approx x+x\ [x \geq 1]$ 是 $\mathcal{R}_1$的一个归纳定理，因为对于任意正整数 $n \geq 1$，我们有 $\mathsf{f}(n,0) \to^*_{\mathcal{R}_1} n+n$。

要证明约束等式 $s \approx t\ [\phi]$ 是逻辑约束项重写系统 $\mathcal{R}$的一个归纳定理，我们必须证明：对于任意满足 ϕ的基代换 σ，$s\sigma \leftrightarrow^*_{\mathcal{R}} t\sigma$。更确切地说，对于每个基代换 σ，只需证明存在一个序列 $s\sigma \leftrightarrow_{\mathcal{R}} u_1 \leftrightarrow_{\mathcal{R}} \cdots \leftrightarrow_{\mathcal{R}} u_n \leftrightarrow_{\mathcal{R}} t\sigma$。然而，对于 $s \approx t\ [\phi]$，重写归纳的扩展和分情况推理规则会基于 s 或 t 的某个位置，通过应用 $\mathcal{R}$中的重写规则进行穷尽式分类讨论。扩展通过在 p 处应用所有适用规则来归约该方程，从而进行穷尽式分类讨论，并将 $s \to t\ [\phi]$ ($t \to s\ [\phi]$) 添加到受约束重写规则集合 $\mathcal{H}$ 中，作为<...>，其中 $\mathcal{R} \cup \mathcal{H} \cup \{s \to t\ [\phi]\}$ ($\mathcal{R} \cup \mathcal{H} \cup \{t \to s\ [\phi]\}$)是终止的。分情况的作用方式与扩展类似，但不会向 $\mathcal{H}$中添加任何规则。一般而言，扩展和分情况的应用并不完备。

Example 1.2. Let us consider $\mathcal{R}_1$ and $\mathsf{f}(x,0) \approx x+x\ [x \geq 1]$ in Example 1.1 again. The root position of $\mathsf{f}(x,0)$ in the equation is *reduction-complete* w.r.t. $\mathcal{R}_1$—all ground instances are redexes of $\mathcal{R}_1$—and thus Expansion and Case are applicable to $\mathsf{f}(x,0) \approx x+x\ [x \geq 1]$. Both Expansion and Case can convert the constrained equation to the following one:

$$x+z \approx x+x\ [x \geq 1 \wedge z \geq x]$$

上述方程不是归纳定理，因为例如对于满足 $x \geq 1 \wedge z \geq x$ 的 $\sigma = \{x \mapsto 1, z \mapsto 2\}$，我们有 $(x+z)\sigma \to^*_{\mathcal{R}_1} 3$ 与 $(x+x)\sigma \to^*_{\mathcal{R}_1} 2$。注意，$\mathcal{R}_1$ 隐式包含计算规则 $x_1+x_2 \to x\ [x = x_1+x_2]$。

还要注意，这个问题并非源于受约束重写。[1] 对于每个正整数 $n \geq 1$，项 $\mathsf{f}(n, \mathsf{0})$ 有无穷多个带有 $k \geq n$ 的归约项 $n + k$，但要使该方程成为归纳定理，只需其中一个归约项借助 $\leftrightarrow_{\mathcal{R}_1}$ 到达 $n + n$。另一方面，扩展和分情况会生成子目标 $x + z \approx x + x \ [x \geq 1 \wedge z \geq x]$，而为了证明它是归纳定理，我们必须考虑满足 $x \geq 1 \wedge z \geq x$ 的所有 替换。我们对应用扩展和分情况的期望是，将约束等式转换为如下问题：

> for any ground substitution σ for x with $x\sigma \geq 1$, is there *some* k such that $k \geq x\sigma$ and $(x\sigma + k) \leftrightarrow^*_{\mathcal{R}_1} (x\sigma + x\sigma)$.

To formulate the above problem as a constrained equation, the introduction of *existential quantification* to constrained equations would be reasonable:

$$(\exists z : z \geq x.\ x + z \approx x + x) \ [x \geq 1]$$

Note that Simplification has the similar problem: if we use the *most general constrained rewriting* [35] which is usually implemented in RI-based tools for LCTRSs, then we have the same problem; otherwise, in applying a constrained rewrite rule to a constrained term, we have to choose appropriate values and/or variables for the extra variables (e.g., choose x for z above) of the applied rule.

In this paper, we introduce existential quantification to the equation part of constrained equations, formulating *constrained existentially quantified equations* (constrained ∃-equations, for short) of the form

$$(\exists \vec{x} : \eta.\ s \approx t) \ [\phi]$$

in the LCTRS formalism (Section 4). Then, we extend the RI framework for LCTRSs to constrained ∃-equations (Section 5). To simplify discussions, we restrict ourselves to left-value-free LCTRSs that are left-linear w.r.t. theory variables (Section 3). All omitted proofs of the claims are provided in both the appendix.

In the extended RI framework, when we apply a constrained rewrite rule $\ell \to r \ [\varphi]$ to a constrained ∃-equation $(\exists \vec{x} : \eta.\ s \approx t) \ [\phi]$, we introduce existential quantification to the *extra variables*—variables appear in r but not in ℓ—of the applied rule: Roughly speaking, the constrained ∃-equation is reduced by the rule at a position p of s by means of a substitution γ to

$$(\exists \vec{x}, \vec{z} : \eta \wedge \varphi\gamma.\ s[r\gamma]_p \approx t) \ [\phi]$$

其中 $\vec{z}$ 是所应用规则的额外变量。尽管方程是存在量化的，我们不会扩展逻辑约束项重写系统中的受约束重写规则。将受约束 ∃-方程 $(\exists \vec{x} :\ \eta.\ s \approx t) \ [\phi]$ 从左向右定向时，我们将其转换为 $s \to t \ [\phi \wedge \eta]$。

[1] The equation $\mathsf{f}(x) \approx \mathsf{a}$ is an inductive theorem of the TRS $\mathcal{R}_2 = \{\mathsf{f}(\mathsf{z}) \to \mathsf{a}, \mathsf{f}(\mathsf{z}) \to \mathsf{b}, \mathsf{f}(\mathsf{s}(x)) \to \mathsf{a}\}$, not all equations $\mathsf{a} \approx \mathsf{a}, \mathsf{b} \approx \mathsf{a}$ obtained from $\mathsf{f}(x) \approx \mathsf{a}$ by applying Expansion or Case are inductive theorems of $\mathcal{R}_2$.

将重写归纳扩展到受约束 ∃-方程的关键在于推理规则删除。在逻辑约束项重写系统的重写归纳框架中，如果 $s = t$ 或 ϕ 不可满足，删除会从子目标中移除受约束方程 $s \approx t\ [\phi]$ 。注意，这类方程显然是归纳定理。在扩展重写归纳框架中，如果$s = t$、 ϕ不可满足，或者 s， t是理论项，且（$\phi \Rightarrow$ （$\exists \vec{x}.$（ $\eta \wedge s = t$））有效，则删除会从子目标中移除受约束方程（$\exists \vec{x} :\ \eta.\ s \approx t$） $[\phi]$ 。设 s， t 为理论项， γ 为满足 ϕ的替换，且其定义域不包含 $\vec{x}$。要使用第三个新条件，我们不验证 $s\gamma = t\gamma$的有效性，而是检查其可满足性。这一区别的影响比我们预想的更大。

A constrained object $P(\vec{y})\,[\phi]$ represents the set of instances of $P(\vec{y})$ w.r.t. ϕ: $\{P(\vec{v}) \mid \vec{v} \text{ satisfy } \phi\}$. We consider it the conjunction of $P(\vec{v})$: $\bigwedge_{\vec{v} \text{ satisfy } \phi} P(\vec{v})$. On the other hand, a constrained ∃-object $(\exists \vec{x} : \eta.\ P(\vec{y}, \vec{x}))\ [\phi]$ represents the family of the sets of instances of $P(\vec{y}, \vec{x})$ w.r.t. ϕ: $\{\, \{P(\vec{v}, \vec{w}) \mid \vec{v}, \vec{w} \text{ satisfy } \eta\} \mid \vec{v} \text{ satisfy } \phi \,\}$. The inner set can be considered the disjunction of $P(\vec{v}, \vec{w})$, and the whole as the conjunction of the disjunctions: $\bigwedge_{\vec{v} \text{ satisfy } \phi} \bigvee_{\vec{v}, \vec{w} \text{ satisfy } \eta} P(\vec{v}, \vec{w})$. Viewed in this light, constrained ∃-objects are very similar to CNFs.

We have used a simple example (Example 1.1) to clearly illustrate the key problem. On the other hand, we have a practical motivation of introducing existential quantification to constrained equations, which is the reduction of constrained inequalities to constrained equations.

The RI framework for constrained TRSs in [31] has been extended for constrained *inequalities* [26]. In the following, we describe the extended RI framework that are informally and naively adapted to LCTRSs.

Let us consider the following convergent (i.e., terminating and confluent) LCTRS over the integer signature (cf. Example 2.1 in Section 2 for details):

$$\mathcal{R}_3 = \{\ \ \mathsf{pow}(x, y) \to 1\ [y < 1], \quad \mathsf{pow}(x, y) \to x \times \mathsf{pow}(x, y - 1)\ [y \geq 1]\ \ \}$$

The function symbol pow is defined by $\mathcal{R}_3$ as the power function over the integers: for integers m, n, $\mathsf{pow}(m, n) \to^*_{\mathcal{R}_3} m^n$. Let us try to prove that the following inequality is an inductive theorem of $\mathcal{R}_3$:

$$\mathsf{pow}(2, n) \geq n\ [n \geq 0] \tag{1}$$

In proving validity of constrained inequalities by means of the RI framework in [26], the application of Simplification w.r.t. oriented inequalities is in general *not* complete (see [26, Example 6.1] for details). If we found a subgoal is not an inductive theorem, then we backtrack and try to another application of inference rules. Note that the method in [26] succeeds in proving the inequality (1) an inductive theorem of $\mathcal{R}_3$.

对于方程的重写归纳框架，由于规则和归纳假设都是定向方程，化简总是完备的。在 [26, Section 1], 中，讨论了如何将不等式化为方程，以及如何引入一个用于 $\geq$ 的二元符号。例如，(1) 被化为约束等式 $\mathsf{geq}(\mathsf{pow}(2, n)\ n) \approx$真 $[n \geq 0]$, 并引入了规则 $\mathsf{geq}(x, y) \to$真 $[x \geq y]$ 和 $\mathsf{geq}(x, y) \to$假 $[x \not\geq y]$。这

由于 geq 会阻止我们以预期的方式化简左部中的真子项，因此 [26] 中没有采用这种方法。

A naive way in first-order logic to reduce inequalities to equations is the use of *existential quantification*. For example, inequality (1) is reduced to the following formula:

$$(\exists m : m \geq 0.\ \mathsf{pow}(2, n) \approx n + m)\ [n \geq 0] \tag{2}$$

Unfortunately, RI frameworks cannot deal with such an equation. Our goal is to extend the RI framework for LCTRSs to constrained ∃-equations so as to prove that the constrained ∃-equation (2) above is an inductive theorem of $\mathcal{R}_3$.

The contribution of this paper is to combine the RI framework for inequalities with that for equations by reducing inequalities to equations. Inequalities are useful to verify some properties of functions; for example, the returned values are always greater than or equal to an expression over input arguments, and the returned number of computation steps is always less than or equal to an estimated upper bound. The RI framework for inequalities needs some special treatments of (oriented) inequalities, and Simplification is in general not complete. The simple combination of the two frameworks such that both inequalities and equations can be handled is more complicated than the framework for equations, and still has incompleteness of Simplification. On the other hand, the RI framework for constrained ∃-equations is a conservative extension of that for constrained equations, Simplification is complete, and we can focus on only constrained (∃-)equations.

2 Preliminaries

In this section, we briefly recall LCTRSs [22, 12]. Familiarity with basic notions and notations on term rewriting [1, 29] is assumed.

为了定义一个 LCTRS [22, 12]，其签名 Σ按 $\mathcal{S}$排序，我们考虑以下排序、签名、映射和常量：$\mathcal{S}_{theory}$ 中的理论排序和 $\mathcal{S}_{term}$中的项排序，满足 $\mathcal{S} = \mathcal{S}_{theory} \uplus \mathcal{S}_{term}$；理论签名 Σ_{theory}和项签名 Σ_{terms}，满足 $\Sigma = \Sigma_{theory} \cup \Sigma_{terms}$和 $\iota_1, \ldots\ldots, \iota_n$，对于任意符号 f：$\iota_1 \times \cdots \times \iota_n \to \iota \in \Sigma_{theory}$；映射 $\mathcal{I}$为每个理论排序 ι 指定一个（非空）集合 $\mathcal{U}_\iota$，称为 ι 的全域（即 $\mathcal{I}(\iota) = \mathcal{U}_\iota$）；映射 $\mathcal{J}$称为 Σ_{theory}的解释，它为每个函数符号 f：$\iota_1 \times \cdots \times \iota_n \to \iota \in \Sigma_{theory}$指定一个函数 $f^{\mathcal{J}}$，其属于 $\mathcal{I}(\iota_1) \times \cdots \times \mathcal{I}(\iota_n) \to \mathcal{I}(\iota)$（即 $\mathcal{J}(f) = f^{\mathcal{J}}$）；值常量 a的集合 $\mathcal{V}al_\iota \subseteq \Sigma_{theory}$：每个理论排序 ι 对应一组值常量，使得 $\mathcal{J}$给出从 $\mathcal{V}al_\iota$ 到 $\mathcal{I}(\iota)$的双射。我们用 $\mathcal{V}al$表示 $\bigcup_{\iota \in \mathcal{S}_{theory}} \mathcal{V}al_\iota$。注意，$\mathcal{V}al \subseteq \Sigma_{theory}$。为便于阅读，我们可以不区分 $\mathcal{V}al_\iota$和 $\mathcal{I}(\iota)$，即对于每个 $v \in \mathcal{V}al_\iota$，$v$ 和 $\mathcal{J}(v)$可以视为相同，并称它们为值。我们要求 $\Sigma_{terms} \cap \Sigma_{theory} \subseteq \mathcal{V}al$。[2] $\Sigma_{theory} \setminus \mathcal{V}al$ 中的符号是计算符号，我们可以对其使用中缀记法。$T(\Sigma_{theory}, \mathcal{V})$中的项

[2] In this paper, we may assume that $\Sigma_{terms} \cap \Sigma_{theory} = \emptyset$.

称为理论项。我们将基理论项的解释 $[\![\cdot]\!]_{\mathcal{J}}$定义为 $[\![f(s_1,\ldots,s_n)]\!]_{\mathcal{J}} = \mathcal{J}(f)([\![s_1]\!]_{\mathcal{J}},\ldots,[\![s_n]\!]_{\mathcal{J}})$。

我们通常选择一个理论签名 $\mathcal{S}_{theory}$，使得 $\mathcal{S}_{theory} \supseteq \mathcal{S}_{core}$ =｛布尔型｝、$\mathcal{V}al_{bool} = \{$真、假: 布尔型$\}$、$\Sigma_{theory} \supseteq \Sigma_{core} = \mathcal{V}al_{bool} \cup \{\wedge,\vee,\Rightarrow,\Leftrightarrow$: 布尔型×布尔型 $\to$布尔型 $\neg$: 布尔型 $\to$布尔型$\}\cup\{=_\iota,\neq_\iota$: $\iota\times\iota \to$布尔型 $\mid \iota \in \mathcal{S}_{theory}\}$，并按预期解释这些符号。当上下文明确时，我们省略 ι 中的排序下标 $=_\iota$ 和$\neq_\iota$。排序为 $bool$ 的理论项称为约束。如果对于所有 $x \in \mathcal{V}ar(\phi)$ 和 $[\![\phi\gamma]\!]_{\mathcal{J}} =$ 真，替换 γ 都满足约束 ϕ，则称该替换尊重约束。若对于任意（某个）满足 $\mathcal{D}om(\gamma) \supseteq \mathcal{V}ar(\phi)$ 以及$\mathcal{R}an(\gamma|_{\mathcal{V}ar(\phi)}) \subseteq \mathcal{V}al$的替换 γ，约束 ϕ 均（有一个）为 $[\![\phi\gamma]\!]_{\mathcal{J}} =$ 真，则称该约束有效（可满足）。我们经常考察形如 $\phi \Rightarrow (\exists\vec{x}.\ \psi)$ 的一阶公式的有效性；在我们的设定中，该公式不是约束，其中 ϕ 和 ψ 是约束（即理论项）。我们定义有效性如下：当且仅当对于任意满足 $\mathcal{D}om(\gamma) = \mathcal{V}ar(\phi) \cup (\mathcal{V}ar(\psi) \setminus \{\vec{x}\})$ 的替换 γ，存在一个替换 γ'，使得 $\mathcal{D}om(\gamma') = \{\vec{x}\}$、$\mathcal{R}an(\gamma') \subseteq \mathcal{V}al$，并且 $[\![\phi\gamma \Rightarrow \psi\gamma'\gamma]\!]_{\mathcal{J}} =$ 真时，$\phi \Rightarrow (\exists\vec{x}.\ \psi)$ 才是有效的。注意，$(\exists\vec{x}.\ \phi) \Leftrightarrow (\exists\vec{y}.\ \psi)$ 的有效性由 $\phi \Rightarrow (\exists\vec{y}.\ \psi)$ 和 $\psi \Rightarrow (\exists\vec{x}.\ \phi)$ 的有效性定义，其中 ϕ 和 ψ 是约束。

A *constrained rewrite rule* is a triple $\ell \to r\ [\varphi]$ such that ℓ and r are terms of the same sort, φ is a constraint, and ℓ is neither a theory term nor a variable. If $\varphi = \mathsf{true}$, then we may write $\ell \to r$. We define $\mathcal{LV}ar(\ell \to r\ [\varphi])$ as $\mathcal{V}ar(\varphi) \cup (\mathcal{V}ar(r) \setminus \mathcal{V}ar(\ell))$, the set of *logical variables in* $\ell \to r\ [\varphi]$ which are variables instantiated with values in rewriting terms. We say that a substitution γ *respects* $\ell \to r\ [\varphi]$ if $\gamma(x) \in \mathcal{V}al$ for all logical variables $x \in \mathcal{LV}ar(\ell \to r\ [\varphi])$ and $[\![\varphi\gamma]\!]_{\mathcal{J}} = \mathsf{true}$.[3] We denote the set $\{f(x_1,\ldots,x_n) \to y\ [y = f(x_1,\ldots,x_n)] \mid f \in \Sigma_{theory} \setminus \mathcal{V}al,\ x_1,\ldots,x_n,y$ are pairwise distinct variables$\}$ by $\mathcal{R}_{calc}$.[4] The elements of $\mathcal{R}_{calc}$ are also called constrained rewrite rules (or *calculation rules*) even though their left-hand sides are theory terms.

A constrained rewrite rule $\ell \to r\ [\varphi]$ is said to be *left-value-free* if ℓ includes no value, i.e., $\ell \in T(\Sigma\setminus\mathcal{V}al, \mathcal{V})$ [21, 34, 35]. The constrained rewrite rule $\ell \to r\ [\varphi]$ is said to be *left-linear w.r.t. logical variables* (left-LV-linear, for short) if every logical variable appears in ℓ at most once [34, 35]. The constrained rewrite rule $\ell \to r\ [\varphi]$ is said to be *left-linear w.r.t. theory variables* (left-TV-linear, for short) if every variable with a theory sort appears in ℓ at most once. Note that any left-TV-linear constrained rule is left-LV-linear.

一组受约束重写规则的重写关系 $\to_{\mathcal{R}}$ 是定义在项上的二元关系，定义如下：对于项 s, t, $s \to_{\mathcal{R}} t$ 当且仅当存在一条受约束重写规则 $\ell \to r\ [\varphi] \in \mathcal{R} \cup \mathcal{R}_{calc}$、$s$的一个位置以及一个替换 $s|_p = \ell\gamma$，使得 $t = s[r\gamma]_p$，且 γ 满足 $\ell \to r\ [\varphi]$。我们可以说该归约发生在位置 p，并可用 $\to_{p,\mathcal{R}}$ 或 $\to_{p,\ell\to r\ [\varphi]}$代替 $\to_{\mathcal{R}}$。使用 $\mathcal{R}_{calc}$ 的归约步称为计算。逻辑受约束项重写系统（简称 LCTRS）定义为一个抽象归约系统（$T(\Sigma,\mathcal{V}) \to_{\mathcal{R}}$），简记为 $\mathcal{R}$。LCTRS 通常

[3] Not all substitutions γ respecting φ respect $\ell \to r\ [\varphi]$: Such γ ensures that $\gamma(x) \in \mathcal{V}al$ for all variables $x \in \mathcal{V}ar(\varphi)$ but not that $\gamma(x) \in \mathcal{V}al$ for all $x \in \mathcal{V}ar(r) \setminus \mathcal{V}ar(\varphi)$.

[4] Note that $\mathcal{R}_{calc}$ is not determined by $\mathcal{R}$ but by Σ_{theory}.

通过提供 Σ_{theory}、 Σ_{terms}、 $\mathcal{R}$，以及对 $\mathcal{I}$和 $\mathcal{J}$的非正式描述来给出；如果根据上下文无法清楚确定这些内容，则需提供该描述。 $\mathcal{R}$ 的范式集合记作$NF_{\mathcal{R}}$。 $\mathcal{R}$的基范式集合记作$GNF_{\mathcal{R}}$。如果重写关系 $\to_{\mathcal{R}}$ 是终止的，则称 LCTRS$\mathcal{R}$ 终止。

标准整数签名 Σ_{int}是 $\Sigma_{core} \cup \{+, -, \times$,幂函数，除法，取模 : 整数 $\times$整数 $\to$整数 $\} \cup \{\geq, >$: 整数 $\times$ 整数 $\to$布尔型$\} \cup \mathcal{V}al_{int}$，其中 $\mathcal{S}_{theory} \supseteq$ {整数，布尔型},$\mathcal{V}al_{int} = \mathbb{Z}$, $\mathcal{I}$(整数) $= \mathbb{Z}$，以及 $\mathcal{J}(n) = n$，适用于任意 $n \in \mathbb{Z}$。我们以自然的方式定义 $\mathcal{J}$。具有 $\Sigma_{theory} = \Sigma_{int}$ 的 LCTRS 称为整数 LCTRS。

例*2.1.* 设 $\mathcal{S} =$ {整数，布尔型}，以及 $\Sigma = \Sigma_{terms} \cup \Sigma_{theory}$，其中 Σ_{terms} ={ 幂函数 : 整数 $\times$整数 $\to$ 整数 }。那么，整数 和 布尔型 都是理论排序。理论项的例子有 $0 = 0+-1$ 和 $x+3 \geq y+-42$，它们是约束。 5+9也是一个（基）理论项，但不是约束。 pow(2，y) 不是理论项。我们用计算规则 $x_1 - x_2 \to x\ [x = x_1 - x_2]$经过一步将 $3-1$ 化简为 2，并用三步将 $3 \times (2 \times (1 \times 1))$ 化简为 6。为了实现一个在 $\mathbb{Z}$ 上计算幂函数的 LCTRS，我们使用上述签名 Σ 以及第 1 节中的 LCTRS $\mathcal{R}_3$。使用 $\mathcal{R}_3$中的受约束重写规则，pow(2，3) 经过十步化简为 8：pow(2，3) $\to_{\mathcal{R}_3} 2 \times$ pow(2，$3-1$) $\to_{\mathcal{R}_3} 2 \times$ pow(2，2) $\to_{\mathcal{R}_3} \cdots \to_{\mathcal{R}_3} 8$。

A function symbol f is called a *defined symbol* of an LCTRS $\mathcal{R}$ if there exists a rule $f(\ell_1, \ldots, \ell_n) \to r\ [\varphi] \in \mathcal{R} \cup \mathcal{R}_{calc}$; non-defined elements of Σ are called *constructors* of $\mathcal{R}$. Note that all values are constructors of $\mathcal{R}$. Note also that not all constructors are constants. We denote the sets of defined symbols and constructors of $\mathcal{R}$ by $\mathcal{D}_{\mathcal{R}}$ and $\mathcal{C}_{\mathcal{R}}$, respectively: $\mathcal{D}_{\mathcal{R}} = \{f \mid f(\ldots) \to r\ [\varphi] \in \mathcal{R} \cup \mathcal{R}_{calc}\}$ and $\mathcal{C}_{\mathcal{R}} = \Sigma \setminus \mathcal{D}_{\mathcal{R}}$. A term in $T(\mathcal{C}_{\mathcal{R}}, \mathcal{V})$ is called a *constructor term* of $\mathcal{R}$. A term of the form $f(t_1, \ldots, t_n)$ with $f \in \mathcal{D}_{\mathcal{R}}$ and constructor terms $t_1, \ldots, t_n$ is called *basic*. The LCTRS $\mathcal{R}$ is called *quasi-reducible* if every ground basic term is a redex of $\mathcal{R}$. A method to prove quasi-reducibility of left-linear LCTRSs can be found in [27]. When considering quasi-reducibility, we usually assume that for each sort ι, there exists a constant with sort ι. The LCTRS $\mathcal{R}$ is called *sufficiently complete* if every ground term can be reduced to a ground constructor term. Note that a terminating and quasi-reducible LCTRS is sufficiently complete.

A *constrained term* is a pair $s\,[\phi]$ of a term s and a constraint ϕ with possibly $\mathcal{V}ar(\phi) \not\subseteq \mathcal{V}ar(s)$. The constrained term $s\,[\phi]$ is considered the set of all instances of s w.r.t. ϕ. The set of ground instances of s w.r.t. substitutions that respect ϕ is denoted by $\mathcal{G}(s\,[\phi])$: $\mathcal{G}(s\,[\phi]) = \{s\gamma \in T(\Sigma) \mid \gamma$ is a substitution respecting $\phi\}$.[5] Two constrained terms $s\,[\phi]$ and $t\,[\psi]$ are called *unifiable* if s and t are unifiable with an mgu σ such that $\mathcal{R}an(\sigma|_{\mathcal{V}ar(\phi,\psi)}) \subseteq T(\Sigma_{theory}, \mathcal{V})$ and $(\phi \wedge \psi)\sigma$ is satisfiable [27, Definition 4.4] (cf. [32, Definition 2]).

我们称受约束项 $s\,[\phi]$ 与 $t\,[\psi]$ 等价，记作 $s\,[\phi] \sim t\,[\psi]$，如果对任意满足 ϕ 的替换 γ，都存在满足 ψ 的替换 δ，使得 $s\gamma = t\delta$，反之亦然。注意，$s\,[\phi] \sim t\,[\psi]$ 当且仅当 $\mathcal{G}(s\,[\phi]) = \mathcal{G}(t\,[\psi])$。受约束项上的重写关系 $\rightsquigarrow_{\mathcal{R}}$ 定义如下： $s\,[\phi] \rightsquigarrow_{\mathcal{R}} t\,[\psi]$ 当且仅当 $s\,[\phi] \sim \cdot \to_{\mathsf{base},\mathcal{R}} \cdot \sim t\,[\psi]$,

[5] Since this paper deals with inductive theorems, we consider ground instances of constrained terms.

其中 $\to_{\mathsf{base},\mathcal{R}} = \{(s'[\ell\gamma]_p\,[\phi'], s'[r\gamma]_p\,[\phi']) \mid \ell \to r\ [\varphi] \in \mathcal{R} \cup \mathcal{R}_{calc},\ \mathcal{D}om(\gamma) \supseteq \mathcal{LV}ar(\ell \to r\ [\varphi])\ \forall x \in \mathcal{LV}ar(\ell \to r\ [\varphi]).\, x\gamma \in \mathcal{V}al \cup \mathcal{V}ar(\phi'), (\phi \Rightarrow \varphi\gamma)$ 有效$\}$。对于受约束项上的 $\tilde{\to}_{\mathcal{R}}$，我们可以说该归约发生在位置 p，并可以写 $\tilde{\to}_{p,\mathcal{R}}$ 或 $\tilde{\to}_{p,\ell\to r\ [\varphi]}$ 来代替 $\tilde{\to}_{\mathcal{R}}$。

Example 2.2. Consider the LCTRS $\mathcal{R}_3$ in Example 2.1 again. The constrained term $\mathsf{pow}(2,y)\,[y > 2]$ represents the set $\{\mathsf{pow}(2,3), \mathsf{pow}(2,4)\ \ldots\}$, and is reduced by $\mathcal{R}_3$ as follows: $\mathsf{pow}(2,y)\,[y > 2] \tilde{\to}_{\mathcal{R}_3} 2 \times \mathsf{pow}(2, y-1)\,[y > 2] \tilde{\to}_{\mathcal{R}_3} 2 \times (2 \times \mathsf{pow}(2,y'))\,[y > 2 \wedge y' = y-1] \tilde{\to}_{\mathcal{R}_3} 2 \times (2 \times (2 \times \mathsf{pow}(2,y')))\,[y > 2 \wedge y'' = y' - 2]$.

3 Restriction to LCTRSs

Constrained rewriting is defined with equivalence $\sim$ over constrained terms, which makes definitions, proofs, discussions, etc, very complicated. To avoid the use of $\sim$, we restrict ourselves to some class of LCTRSs. To be more precise, LCTRSs in this paper are assumed to satisfy all of the following:

- **A1**. for any constrained rewrite rule $\ell \to r\ [\varphi]$, all the extra variables—variables in $\mathcal{V}ar(r) \setminus \mathcal{V}ar(\ell)$—appear in φ: $\mathcal{V}ar(r) \subseteq \mathcal{V}ar(\ell, \varphi)$,
- **A2**. every constrained rewrite rule is left-value-free, and
- **A3**. every constrained rewrite rule is left-linear w.r.t. theory variables (left-TV-linear).

The logical variables of $\ell \to r\ [\varphi]$ are instantiated with values in applying $\ell \to r\ [\varphi]$ to terms and are instantiated with values or logical variables in applying $\ell \to r\ [\varphi]$ to constrained terms. Thus, to simplify discussions, we assume **A1**: For $\ell \to r\ [\varphi]$, if there is a variable x in $\mathcal{V}ar(r) \setminus \mathcal{V}ar(\ell, \varphi)$, then we convert $\ell \to r\ [\varphi]$ to $\ell \to r\ [\varphi \wedge \bigwedge_{x \in \mathcal{V}ar(r) \setminus \mathcal{V}ar(\ell,\varphi)} (x = x)]$.

The assumption **A2** is not an actual limitation because for any LCTRS $\mathcal{R}$, there exists a left-value-free and left-LV-linear LCTRS $\mathcal{R}'$ such that $\to_{\mathcal{R}} = \to_{\mathcal{R}'}$ on ground terms.

Theorem 3.1. *Let $\ell \to r\ [\phi]$ be a constrained rewrite rule, $p_1, \ldots, p_n$ the positions with $\{p_1, \ldots, p_n\} = \{p \in \mathcal{P}os(\ell) \mid \ell|_p \in \mathcal{V}al \cup \mathcal{V}ar(\phi)\}$, and $x_1, \ldots, x_n$ pairwise distinct variables such that $\{x_1, \ldots, x_n\} \cap \mathcal{V}ar(\ell, r, \phi) = \emptyset$. Let $\ell' \to r\ [\phi']$ be a constrained rule such that $\ell' = \ell[x_1, \ldots, x_n]_{p_1,\ldots,p_n}$ and $\phi' = (\phi \wedge (\bigwedge_{i=1}^{n}(x_i = \ell|_{p_i})) \wedge (\bigwedge_{y \in \mathcal{V}ar(r) \setminus \mathcal{V}ar(\ell,\varphi)}(y = y))$. Then, $\to_{\ell\to r\ [\phi]} = \to_{\ell'\to r\ [\phi']}$.*

Proof. Trivial by the definition of $\to_{\mathcal{R}}$ and the construction of ℓ', ϕ'. □

在此之前使用受约束项上的等价性 $\sim \to_{\mathsf{base},\ \mathcal{R}}$ 以便对受约束项 $s\,[\phi]$，重命名 s 和 ϕ中的变量，将一个值移至约束部分，将约束 ϕ' 与 ϕ合取，以便在 $\to_{\mathsf{base}}$处应用受约束重写规则 $\ell \to r\ [\varphi]$，等等。$\sim$ 对于 $\tilde{\to}_{\mathcal{R}}$ 的主要作用是使规则 $\ell \to r\ [\varphi]$ 能够应用于$\to_{\mathsf{base},\ \mathcal{R}}$-步。对于左值自由且左 TV 线性的逻辑约束项重写系统，我们有如下性质。

定理 3.2。设 $\ell \to r\ [\varphi]$ 是 $\mathcal{R}$中的一个左值自由且左 *TV* 自由的受约束重写规则，$s\,[\phi]$, $t\,[\psi]$ 是受约束项，p 是 s 的一个位置，且$\mathcal{V}ar(\ell, r, \varphi) \cap \mathcal{V}ar(s, \phi, t, \psi) = \emptyset$。若 $s\,[\phi] \sim \cdot \to_{\mathsf{base},\ p,\ \ell\to r\ [\phi]} t\,[\psi]$，则存在一个替换 γ，使得 $s\,[\phi] \sim s\,[\phi \wedge \varphi\gamma] \to_{\mathsf{base},\ p,\ \ell\to r\ [\varphi]} s[r\gamma]_p\,[\phi \wedge \varphi\gamma] \sim t\,[\psi]$。

Thanks to Theorem 3.2, removing $\sim$ from $\tilde{\to}$, we reformulate constrained rewriting of LCTRSs satisfying **A1**–**A3** as follows.

Definition 3.3 ($\rightharpoonup_{\mathcal{R}}$). *The constrained rewriting $\rightharpoonup_{\mathcal{R}}$ of a left-value-free and left-TV-linear LCTRS $\mathcal{R}$ satisfying* **A1** *is defined as follows: $s\,[\phi] \rightharpoonup_{\mathcal{R}} t\,[\psi]$ if and only if there exist a constrained rewrite rule $\ell \to r\ [\varphi] \in \mathcal{R} \cup \mathcal{R}_{calc}$, a position p of s, and a substitution γ such that*

- $s|_p = \ell\gamma$, $t = s[r\gamma]_p$, $\psi = (\phi \wedge \varphi\gamma)$,
- $x\gamma \in \mathcal{V}al \cup \mathcal{V}ar(\phi)$ *for any variable* $x \in \mathcal{V}ar(\varphi) \cap \mathcal{V}ar(\ell)$,
- $x\gamma \in \mathcal{V}al \cup \mathcal{V}ar(\phi) \cup (\mathcal{V} \setminus \mathcal{V}ar(s))$ *for any variable* $x \in \mathcal{V}ar(\varphi) \setminus \mathcal{V}ar(\ell)$,[6] *and*
- $(\phi \Rightarrow (\exists \vec{z}.\ \varphi\gamma))$ *is valid, where* $\{\vec{z}\} = \{z \in \mathcal{V} \setminus \mathcal{V}ar(\phi) \mid \exists x \in \mathcal{V}ar(\varphi) \setminus \mathcal{V}ar(\ell).\ x\gamma = z\}$.[7]

By definition, it is clear that $\rightharpoonup_{\mathcal{R}} \subseteq \tilde{\to}_{\mathcal{R}}$. Therefore, by Theorem 3.2, we have that $(\rightharpoonup_{\mathcal{R}} \cdot \sim) = \tilde{\to}_{\mathcal{R}}$, and thus $(\rightharpoonup^n_{\mathcal{R}} \cdot \sim) = \tilde{\to}^n_{\mathcal{R}}$ for all $n \geq 1$.

4 Constrained ∃-Equations

In this section, we first introduce existential quantification to the equation part of constrained equations, formulating *constrained ∃-equations*. Then, we extend constrained rewriting to constrained ∃-equations.

4.1 Introduction of Existential Quantification to Equations

First, we introduce *existentially quantified equations*.

定义*4.1*（∃-方程）。存在量化方程（简称∃-方程）是一个四元组 $\exists\vec{x}:\ \eta.\ s \approx t$，由有限变量序列 $\vec{x}$、可满足约束 η以及两个具有相同排序的项 s、t 组成，且满足 $\{\vec{x}\} \subseteq \mathcal{V}ar(\eta) \cap \mathcal{V}ar(s, t)$。请注意，若 $\vec{x}$ 是 ϵ，则 η 是封闭有效公式，例如真。若 $\vec{x} = \epsilon$，我们可以用$s \approx t$ 代替 $\exists\vec{x}:\ \eta.\ s \approx t$ 。如果 $\mathcal{V}ar(s, t, \eta) = \{\vec{x}\}$，则称 $\exists\vec{x}:\ \eta.\ s \approx t$ 是封闭的。我们用 $\mathcal{G}(\exists\vec{x}:\ \eta.\ s \approx t)$表示 $\exists\vec{x}:\ \eta.\ s \approx t$ 的基实例集合：$\mathcal{G}(\exists\vec{x}:\ \eta.\ s \approx t) = \{s\gamma \approx t\gamma \mid s\gamma, t\gamma \in \mathcal{T}(\Sigma)\ \ \gamma$ 是一个遵循 $\eta\}$的替换。

[6] In the definition of $\to_{\mathsf{base},\mathcal{R}}$, for a variable $x \in \mathcal{V}ar(\varphi) \setminus \mathcal{V}ar(\ell)$, we can choose a value or a variable used in the constraint part. In the latter case, we can choose a fresh variable y by adding a redundant constraint $y = y$. Note that $\mathcal{V}ar(r) \subseteq \mathcal{V}ar(\varphi, \ell)$ by **A1**.

[7] Since we can choose fresh variables for variables in $\mathcal{V}ar(\varphi) \setminus \mathcal{V}ar(\ell)$, we existentially quantify such fresh variables $\vec{z}$ introduced by γ.

我们假设 η 可满足，从而 $\exists\vec{x}:\ \eta.\ s \approx t$ 表示至少一个方程。当存在量化变量$\vec{x}$没有约束时，我们写作冗余约束，例如 η中的 $x = x$ 。

例*4.2*。 考虑例2.1中的签名。我们有 ∃-方程 $\exists x{:}x \geq 0.\,\mathsf{pow}(2,\ y) \approx x$, $\exists x:$ $x = x.\,\mathsf{pow}(2,\ x) \approx 2$, 等等。

接下来，我们引入受约束的 ∃-方程。

定义*4.3*（受约束的 ∃-方程）。受约束的 ∃-方程是一个对 $(\exists\vec{x}:\ \eta.\ s \approx t)\ [\phi]$，由一个 ∃-方程 $\exists\vec{x}:\ \eta.\ s \approx t$ 和一个约束 ϕ 组成，满足 $\mathcal{V}ar(\eta) \setminus \{\vec{x}\} \subseteq \mathcal{V}ar(\phi)$，且 $(\phi \Rightarrow (\exists\vec{x}.\ \eta))$ 有效。[8] 当 $\phi = \top$ 为真时，我们简单记作$\exists\vec{x}:\ \eta.\ s \approx t$ 。我们将满足约束 ϕ 的替换下，$(\exists\vec{x}:\ \eta.\ s \approx t)\ [\phi]$ 的闭合 ∃-方程实例集合记作 $\mathcal{G}((\exists\vec{x}:\eta.\ s \approx t)\ [\phi])$: $\mathcal{G}((\exists\vec{x}:\ \eta.\ s \approx t)\ [\phi]) = \{\exists\vec{x}:\ \eta\gamma|_{\mathcal{V}ar(\phi)\setminus\{\vec{x}\}}.\ s\gamma \approx t\gamma \mid s\gamma, t\gamma \in T(\Sigma)\ \ \gamma$ 是满足约束 $\phi\}$的替换。

Example 4.4. Consider the signature in Example 2.1. We have constrained ∃-equations $(\exists x : x \geq 2.\ \mathsf{pow}(2, y) \approx x)\ [y > 0]$, $(\exists x : x > 0.\ \mathsf{pow}(y, x) \approx x)\ [y > 0]$, etc. We also have that $\mathcal{G}((\exists x : x \geq 2.\ \mathsf{pow}(2, y) \approx x)\ [y > 0]) = \{\exists x : x \geq 2.\ \mathsf{pow}(2, n) \approx x \mid n \in \mathbb{Z}, n > 0\}$ and $\mathcal{G}((\exists x : x > 0.\ \mathsf{pow}(y, x) \approx x)\ [y > 0]) = \{\exists x : x > 0.\ \mathsf{pow}(n, x) \approx x \mid n \in \mathbb{Z}, n > 0\}$.

4.2 Constrained Rewriting of ∃-Terms

In the RI framework, by considering $\approx$ a binary function symbol, constrained equations are reduced by constrained rewrite rules. In this section, considering equations as terms, we extend constrained rewriting to constrained ∃-equations.

To simplify discussions, we introduce (constrained) ∃-*terms* as well as (constrained) ∃-equations. An *existentially quantified term* (∃-term, for short) is a triple $\exists\vec{x} : \eta.\ s$ of a finite variable sequence $\vec{x}$, a satisfiable constraint η, and a term s such that $\{\vec{x}\} \subseteq \mathcal{V}ar(\eta) \cap \mathcal{V}ar(s)$. We say that $\exists\vec{x} : \eta.\ s$ is *closed* if $\mathcal{V}ar(s) = \{\vec{x}\}$. A *constrained* ∃-*term* is a pair $(\exists\vec{x} : \eta.\ s)\ [\phi]$ of an ∃-term $\exists\vec{x} : \eta.\ s$ and a constraint ϕ such that $\mathcal{V}ar(\eta) \setminus \{\vec{x}\} \subseteq \mathcal{V}ar(\phi)$. As for (constrained) ∃-equations, we use $\mathcal{G}$ for (constrained) ∃-terms.

As for constrained rewriting over usual constrained terms, we do not consider the equivalence between constrained ∃-terms. Without using $\sim$, we define constrained rewriting of constrained ∃-terms as follows.

Definition 4.5 (constrained rewriting $\rightharpoonup_{\mathcal{R}}$ of constrained ∃-terms). *The reduction $\rightharpoonup_{\mathcal{R}}$ of an LCTRS $\mathcal{R}$ over constrained ∃-terms is defined as follows:* $(\exists\vec{x} : \eta.\ s)\ [\phi] \rightharpoonup_{\mathcal{R}} (\exists\vec{y} : \delta.\ t)\ [\psi]$ *if and only if there exist a constrained rewrite rule $\ell \to r\ [\varphi] \in \mathcal{R} \cup \mathcal{R}_{calc}$, a position p of s, and a substitution γ such that*

- $s|_p = \ell\gamma$, $t = s[r\gamma]_p$, $\psi = (\phi \wedge \varphi\gamma)$,

[8] 这确保对于每个满足 ϕ 的替换 γ，至少存在一个方程 $s\gamma \approx t\gamma$，即 $\mathcal{G}(\exists\vec{x}:$ $\eta\gamma|_{\mathcal{V}ar(\eta)\setminus\{\vec{x}\}}.\ s\gamma \approx t\gamma) \neq \emptyset$。

– 对任意变量 $x \in \mathcal{V}ar(\varphi)$, $x\gamma \in \mathcal{V}al \cup \mathcal{V}ar(\phi) \cap \mathcal{V}ar(\ell)$; – 对任意变量 $x \in \mathcal{V}ar(\varphi)$, $x\gamma \in \mathcal{V} \setminus (\mathcal{V}ar(s) \cup \{\vec{x}\}) \setminus \mathcal{V}ar(\ell)$; [9]– $(\phi \Rightarrow (\exists \vec{z}.\ \varphi\gamma))$ 有效; 以及 – $(\exists \vec{y}.\ \delta) = (\exists \vec{x}, \vec{z}.\ (\eta \wedge \varphi\gamma))$, 其中 $\{\vec{z}\} = \{x\gamma \mid \exists x \in \mathcal{V}ar(\varphi) \setminus \mathcal{V}ar(\ell)\}$。

In the above definition, we assume w.l.o.g. that $\{\vec{x}\} \cap \mathcal{V}ar(s, \phi) = \emptyset$*: if* $\{\vec{x}\} \cap \mathcal{V}ar(s, \phi) \neq \emptyset$*, then we may rename* $\vec{x}$ *fresh variables.*

For readability, we often simplify ψ and δ in Definition 4.5 to *equivalent* ones,[10] respectively, without notice. The differences of $\rightharpoonup_{\mathcal{R}}$ in Definition 4.5 from $\rightharpoonup_{\mathcal{R}}$ in Definition 3.3 are the following:

- variables in $\mathcal{V}ar(\phi) \setminus \mathcal{V}ar(\ell)$ are instantiated by γ with fresh variables so as to be existentially quantified, and
- $\varphi\gamma$ is conjuncted with η as $\exists \vec{x}, \vec{z}.\ (\eta \wedge \varphi\gamma)$.

Example 4.6. The constrained $\exists$-term $(\exists m : m \geq 0.\ (2 \times \mathsf{pow}(2, n-1)) + m)\ [n > 1]$ is reduced by $\mathcal{R}_3$ as follows:

$$(\exists m :\ m \geq 0.\ (2 \times \mathsf{pow}(2,\ n-1))\ +\ m)\ \ [n > 1] \rightharpoonup_{\mathcal{R}_3} (\exists m,\ \ n' :\ m \geq 0 \wedge n' = n-1.\ (2 \times \mathsf{pow}(2,\ n'))\ +\ m)\ \ [n > 1 \wedge n'' = n-1] \rightharpoonup_{\mathcal{R}_3} (\exists m,\ \ n' :\ m \geq 0 \wedge n' = n-1.\ (2 \times (2 \times \mathsf{pow}(2,\ n'-1)))\ +\ m) [n > 1 \wedge n'' = n-1]$$

注意，变量 n'' 是将 n' 重命名后的变量，以避免存在量化变量的约束部分与约束之间共享变量。

粗略地说，要在 s 的位置 p 处用规则 $\ell \to r\ [\varphi]$ 归约受约束项 $s\,[\phi]$，$\mathcal{G}(s\,[\phi])$ 中的所有基项都必须能在 p 处被 $\ell \to r\ [\varphi]$ 归约。另一方面，要在位置 p 处用 $\ell \to r\ [\varphi]$ 归约 $\exists$-项 $\exists \vec{x}\colon\ \phi.\ s$，$\mathcal{G}(\exists \vec{x} :\ \phi.\ s)$ 中并非所有基项都必须能在 p 处被 $\ell \to r\ [\varphi]$ 归约。注意，根据定义，$\mathcal{G}(s\,[\phi]) = \mathcal{G}(\exists \vec{x} :\ \phi.\ s)$。受约束的 $\exists$-项也同样如此。

Example 4.7. Let us consider $\mathcal{R}_1$ in Example 1.1 again. The constrained term $\mathsf{f}(x, y)\,[x \geq y \wedge y \geq 0]$ cannot be reduced by the first rule of $\mathcal{R}_1$ because $\mathsf{f}(0, 0) \in \mathcal{G}(\mathsf{f}(x, 0)\,[x \geq 0])$ is not reducible by the first rule. On the other hand, the constrained $\exists$-term $(\exists x : x \geq y.\ \mathsf{f}(x, y))\ [y \geq 0]$ is reduced by the first rule of $\mathcal{R}_1$ to $(\exists x, z : x \geq y \wedge x > y \wedge z \geq x.\ x + z)\ [y \geq 0]$, while $\mathsf{f}(0, 0) \in \mathcal{G}((\exists x : x \geq y.\ \mathsf{f}(x, y))\ [y \geq 0])$.

受约束 $\exists$-项的受约束重写 $\rightharpoonup_{\mathcal{R}}$ 对于项的重写是健全的，同时也适用于通常的受约束重写 [12, 定理 2.19 和 2.20]。

[9] For a variable $x \in \mathcal{V}ar(\varphi) \setminus \mathcal{V}ar(\ell)$, we choose a fresh variable which is existentially quantified in the resulting constrained $\exists$-term.

[10] Constraints ϕ and ϕ' are *equivalent* if $\mathcal{V}ar(\phi) = \mathcal{V}ar(\phi')$ and $(\phi \Leftrightarrow \phi')$ is valid.

定理 4.8。对于受约束 $\exists$-项 $(\exists\vec{x}:\ \eta.\ s)\ [\phi]$ 和 $(\exists\vec{y}:\ \delta.\ t)\ [\psi]$，其中$\{\vec{x}\} \cap \mathcal{V}ar(\phi) = \emptyset$ 且 $\{\vec{y}\} \cap \mathcal{V}ar(\psi) = \emptyset$，若$(\exists\vec{x}:\ \eta.\ s)\ [\phi] \rightharpoonup_{\mathcal{R}} (\exists\vec{y}:\ \delta.\ t)\ [\psi]$，则以下两个陈述均成立：

1. *for every substitution θ respecting $\phi \wedge \eta$, there exists a substitution σ such that σ respects $\psi \wedge \delta$ and $s\theta \to_{\mathcal{R}} t\sigma$, and*
2. *for every substitution σ respecting $\psi \wedge \delta$, there exists a substitution θ such that θ respects $\phi \wedge \eta$ and $s\theta \to_{\mathcal{R}} t\sigma$.*

By definition, it is clear that all of the following are equivalent: $s \to_{\mathcal{R}} t$, $s\,[\mathsf{true}] \rightharpoonup_{\mathcal{R}} t\,[\mathsf{true}]$, and $(\exists\epsilon : \mathsf{true}.\ s)\ [\mathsf{true}] \rightharpoonup_{\mathcal{R}} (\exists\epsilon : \mathsf{true}.\ t)\ [\mathsf{true}]$. Thus, Theorem 4.8 implies the following corollary.

Corollary 4.9. *A left-value-free and left-TV-linear LCTRS $\mathcal{R}$ satisfying* **A1** *is terminating if and only if $\rightharpoonup_{\mathcal{R}}$ over constrained $\exists$-terms is terminating.*

5 Rewriting Induction for Constrained $\exists$-Equations

In this section, we adapt the notion of *inductive theorems* to constrained $\exists$-equations and then extend three main inference rules of the RI framework in [12] to constrained $\exists$-equations.

When using RI frameworks, we often assume that a given system $\mathcal{R}$ is terminating, confluent, and quasi-reducible (i.e., sufficiently complete). Termination is necessary to use RI principles, and confluence is necessary to disprove equations inductive theorems. For page limitation, we do not deal with inference rules for disproving. The reason why $\mathcal{R}$ is assumed to be quasi-reducible is to use a decidable sufficient condition—being a *basic* term—for *reduction completeness* which ensures that, given a position of terms, we can make an exhaustive case analysis based on the application of rules in $\mathcal{R}$. In summary, we assume only termination of LCTRSs.

5.1 Adapting Inductive Theorems to Constrained $\exists$-Equations

We naturally adapt the notion of inductive theorems to constrained $\exists$-equations.

Definition 5.1 (inductive theorem). *A constrained $\exists$-equation $(\exists\vec{x} : \eta.\ s \approx t)\ [\phi]$ is said to be an* inductive theorem *of $\mathcal{R}$ if for every ground normalized substitution γ respecting ϕ such that $\mathcal{D}om(\gamma) = \mathcal{V}ar(s,t,\phi) \setminus \{\vec{x}\}$ and $\mathcal{R}an(\gamma) \subseteq GNF_{\mathcal{R}}$, there exists a substitution θ such that $\mathcal{D}om(\theta) = \{\vec{x}\}$, θ respects $\eta\gamma$, and $s\gamma\theta \leftrightarrow^*_{\mathcal{R}} t\gamma\theta$.*

Example 5.2. The following constrained $\exists$-equation which corresponds to the inequality (1) in Section 1 is an inductive theorem of $\mathcal{R}_3$:

$$(\exists m : m \geq 0.\ \mathsf{pow}(x,n) \approx n + m)\ [x = 2 \wedge n \geq 0] \tag{3}$$

其中，为了对其定向，预先将幂函数 pow(2，n) 中的 2 替换为变量 x，并将其与 $x = 2$ 合取。

5.2 RI Inference Rules for Constrained ∃-Equations

如第 1 节所述，重写归纳框架通常由一些推理规则组成。给定方程的有限集 $\mathcal{E}$，我们将推理规则应用于初始对 $(\mathcal{E},\ \emptyset)$，并尝试得到某个重写规则集 $\mathcal{H}$ 对应的 $(\emptyset,\ \mathcal{H})$:

$$(\mathcal{E},\emptyset) = (\mathcal{E}_0,\mathcal{H}_0) \vdash_{\mathrm{RI}} (\mathcal{E}_1,\mathcal{H}_1) \vdash_{\mathrm{RI}} \cdots \vdash_{\mathrm{RI}} (\mathcal{E}_n,\mathcal{H}_n) = (\emptyset,\mathcal{H})$$

where $\vdash_{\mathrm{RI}}$ denotes the application of inference rules in one step. A pair $(\mathcal{E}_i,\mathcal{H}_i)$ is called an *RI state*. $\mathcal{E}_i$ is a set of equations and $\mathcal{H}_i$ is a set of rewrite rules obtained by orienting equations. Equations in $\mathcal{E}_{i+1} \setminus \mathcal{E}_i$ are so-called *subgoals* for equations in $\mathcal{E}_i \setminus \mathcal{E}_{i+1}$. Rewrite rules in $\mathcal{H}_i$ perform as *induction hypotheses* that can be used for $(\mathcal{E}_j,\mathcal{H}_j)$ with $i < j$. The main inference rules are

- Expansion—a rule-based case analysis with setting an induction hypothesis,
- Simplification—the application of rules in $\mathcal{R} \cup \mathcal{H}_i$ to an equation in $\mathcal{E}_i$, and
- Deletion—the removal of *trivial* inductive theorems, e.g., $s \approx s$.

In this section, we adapt these three main inference rules for LCTRSs in [12] to constrained ∃-equations. In the following, $s \simeq t$ denotes either $s \approx t$ or $t \approx s$.

Before adapting the inference rules to constrained ∃-equations, we introduce the notion of *reduction completeness* for positions of terms.

Definition 5.3 (reduction-completeness). *A position p of a term t (and also $t|_p$) is said to be* reduction-complete w.r.t. a constraint ϕ *if $t|_p\gamma$ is a redex of $\mathcal{R}$ for every substitution γ such that $\mathcal{D}om(\gamma) = \mathcal{V}ar(t|_p)$, $\mathcal{R}an(\gamma) \subseteq NF_{\mathcal{R}}(\Sigma)$, and γ respects ϕ.*

Roughly speaking, for a reduction-complete position p of a term t, every ground instance of $t|_p$ can be reduced by $\mathcal{R}$, and thus we can make an exhaustive rule-based case analysis at position p. A naive sufficient condition for $f(t_1,\ldots,t_n)$ being reduction-complete w.r.t. a constraint ϕ is that $t_1,\ldots,t_n \in \mathcal{V}ar(\phi) \cup \mathcal{V}al$ and $\bigvee_{f(y_1,\ldots,y_n)\to r\ [\varphi]\in\mathcal{R}\cup\mathcal{R}_{calc}} (\varphi\{y_i \mapsto t_i \mid 1 \le i \le n\})$ is valid (cf. [31, Theorem 5.1]).

The three main inference rules are adapted to constrained ∃-equations as shown in Figure 1. The application of inference rules to $(\mathcal{E},\mathcal{H})$ with the resulting RI state $(\mathcal{E}',\mathcal{H}')$ is denoted by $(\mathcal{E},\mathcal{H}) \vdash_{\mathrm{RI}} (\mathcal{E}',\mathcal{H}')$.

The application of the inference rules in Figure 1 is sound, that is, if we obtain $(\emptyset,\mathcal{H})$ by applying the inference rules to the initial RI state $(\mathcal{E},\emptyset)$, then all constrained ∃-equations in $\mathcal{E}$ are inductive theorems of $\mathcal{R}$.

Theorem 5.4. *Given a set $\mathcal{E}$ of constrained ∃-equations, if an LCTRS $\mathcal{R}$ is terminating and $(\mathcal{E},\emptyset) \vdash_{\mathrm{RI}}^{*} (\emptyset,\mathcal{H})$, then all constrained ∃-equations in $\mathcal{E}$ are inductive theorems of $\mathcal{R}$.*

例 *5.5.* 现在我们证明，例 5.2 中的受约束 ∃-方程 (3) 是逻辑约束项重写系统 $\mathcal{R}_3$ 的一个归纳定理。我们从以下重写归纳状态开始:

$$(\{\ (3)\ (\exists m : m \ge 0.\ \mathsf{pow}(x,n) \approx n + m)\ [x = 2 \wedge n \ge 0]\ \},\emptyset)$$

SIMPLIFICATION

$$\frac{(\mathcal{E} \uplus \{\ (\exists \vec{x} : \eta.\ s \approx t)\ [\phi]\ \}, \mathcal{H})}{(\mathcal{E} \cup \{\ (\exists \vec{y} : \eta'.\ s' \approx t')\ [\phi']\ \}, \mathcal{H})}$$

如果 $(\exists \vec{x} \colon\ \eta.\ s \approx t)\ \ [\phi] \rightharpoonup_{\mathcal{R} \cup \mathcal{H}} (\exists \vec{y} \colon\ \eta'.\ s' \approx t')\ \ [\phi']$。

EXPANSION

$$\frac{(\mathcal{E} \uplus \{\ (\exists \vec{x} : \eta.\ s \simeq t)\ [\phi]\ \}, \mathcal{H})}{(\mathcal{E} \cup \mathit{Expd}_{\mathcal{R}}(s \to t\ [\phi \wedge \eta],\ p), \mathcal{H} \cup \{s \to t\ [\phi \wedge \eta]\})}$$

if all of the following hold:

- p is a reduction-complete position of s w.r.t. ϕ,
- $s \to t\ [\phi \wedge \eta]$ is a constrained rewrite rule, and
- $\mathcal{R} \cup \mathcal{H} \cup \{\ s \to t\ [\phi \wedge \eta]\ \}$ is terminating,

where $\mathit{Expd}_{\mathcal{R}}(s \to t\ [\phi \wedge \eta],\ p)$ denotes the following set that is finite up to variable renaming:

$$\{\ (\exists \vec{y} : \eta'.\ s' \approx t')\ [\phi'] \mid \ell \to r\ [\varphi] \in \mathcal{R},\ \theta \text{ is an idempotent mgu of } s|_p \text{ and } \ell,\ (\exists \vec{x} : \eta\theta|_{\mathcal{V}ar(\phi) \setminus \{\vec{x}\}}.\ s\theta \approx t\theta)\ [\phi\theta] \rightharpoonup_{1.p, \ell \to r\ [\varphi]} (\exists \vec{y} : \eta'.\ s' \approx t')\ [\phi']\ \}$$

Note that $\ell \to r\ [\varphi]$ in the above description is freshly renamed: $\mathcal{V}ar(\ell, r, \varphi) \cap \mathcal{V}ar(s, t, \phi, \eta) = \emptyset$.

DELETION

$$\frac{(\mathcal{E} \uplus \{\ (\exists \vec{x} : \eta.\ s \approx t)\ [\phi]\ \}, \mathcal{H})}{(\mathcal{E}, \mathcal{H})}$$

if one of the following holds:

- $s = t$,
- ϕ is unsatisfiable, or
- $s, t \in T(\Sigma_{theory}, \mathcal{V}ar(\phi) \cup \{\vec{x}\})$ and $(\phi \Rightarrow \exists \vec{x}.\ (\eta \wedge s = t))$ is valid.

Fig. 1. Inference rules of RI for constrained ∃-equations.

The left-hand side is reduction-complete w.r.t. $x = 2 \wedge n \geq 0$, and $\mathcal{R}_3 \cup \{\, \mathsf{pow}(x, n) \to n + m\ [x = 2 \wedge n \geq 0 \wedge m \geq 0] \,\}$ is terminating. Thus, we can apply EXPANSION to the above RI state, obtaining the following one:

$$(\left\{\begin{array}{ll} \text{(c)} & (\exists m : m \geq 0.\ 1 \approx n + m)\ [x = 2 \wedge n \geq 0 \wedge n < 1], \\ \text{(d)} & (\exists m : m \geq 0.\ 2 \times \mathsf{pow}(2, n-1) \approx n + m)\ [x = 2 \wedge n \geq 0 \wedge n \geq 1] \end{array}\right\},$$
$$\{\ (3')\ \mathsf{pow}(x, n) \to n + m\ \ [x = 2 \wedge n \geq 0 \wedge m \geq 0]\ \})$$

Since $(x = 2 \wedge n \geq 0 \wedge n < 1 \Rightarrow (\exists m.\ m \geq 0 \wedge 1 = n + m))$ is valid, the constrained ∃-equation (c) is dropped from the set by DELETION, obtaining the following RI state:

$$(\{\ (\mathrm{d})\ \}, \{\ (3')\ \})$$

将化简应用于上述状态后，我们化简 $n - 1$:

$$(\{\ (\mathrm{d}')\ (\exists m, n' : m \geq 0 \wedge n' = n - 1.\ 2 \times \mathsf{pow}(2, n') \approx n + m)\ [x = 2 \wedge n \geq 1]\ \}, \{(3')\})$$

将化简应用于上述状态后，我们用 (3′) 化简幂函数$(2, n')$，得到如下结果：

$$(\left\{\begin{array}{r}(\mathrm{d}'')\ (\exists m, n', m' : m \geq 0 \ \wedge\ n' = n-1 \ \wedge\ m' \geq 0.\ 2 \times (n'+m') \approx n+m) \\ [x = 2 \ \wedge\ n \geq 1]\end{array}\right\},\ \{\,(3')\,\})$$

我们可以通过删除删除 (d′′)，得到重写归纳状态 $(\emptyset, \{(3')\ \})$。因此，受约束的 ∃-方程 (3) 是 $\mathcal{R}_3$ 的归纳定理。

如第 1 节所述，不等式的重写归纳框架可以证明不等式 (1) 是 $\mathcal{R}_3$ 的归纳定理。受约束∃-方程的重写归纳框架可以追踪证明，而无需不完整地应用重写归纳推理规则。

6 相关工作

本文的主要成果是将存在量化引入约束等式，并将逻辑约束项重写系统的重写归纳框架扩展到受约束的 ∃-方程。据我们所知，目前尚无工作将存在量化引入受约束重写中的方程。 [34] 中引入的形式为 $\Pi X.\ s\,[\exists \vec{x}.\ \phi]$ 的存在约束项，对 $\mathcal{V}ar(\phi) \setminus \mathcal{V}ar(s)$ 中的变量使用存在量化，其中 X 用于显式表示逻辑变量。存在量化的作用是显式表示 $\mathcal{V}ar(\phi)\backslash\mathcal{V}ar(s)$ 中的变量，并使 $\mathcal{V}ar(\phi)\backslash\{\vec{x}\} \subseteq \mathcal{V}ar(s)$。因此，存在量化的用法与我们的方法大不相同。守卫项 [2] 是受约束项的一种推广，但不包括 ∃-项。守卫项表示其所有实例构成的集合，而 ∃-项表示其一个 实例。

As described in Example 5.5, the RI framework for constrained ∃-equations would cover the RI framework for inequalities [26] because every inequality can be transformed into a semantically equivalent ∃-equation.

7 Conclusion

In this paper, we introduced existential quantification to the equation part of constrained equations, formulating constrained ∃-equations. We defined the reduction over constrained ∃-equations (∃-terms) and then extended the RI framework for LCTRSs to constrained ∃-equations.

我们已经实现了一个用于受约束 ∃ 方程的重写归纳框架原型，但尚未公开该原型。该原型没有用于证明逻辑约束项重写系统终止性的强大方法，并且只能通过扩展重写归纳框架，以交互模式证明归纳定理。我们确认，原型无需证明终止性即可完成例 5.5 中的推理，而 $\mathcal{R}_3 \cup \{(3')\ \}$ 的终止性

可以通过用于验证逻辑约束项重写系统的工具 Ctrl [24], a 证明。我们将自动应用推理规则，并发布该原型。

In the extend RI framework, we consider only the main three inference rules, while there are other useful inference rules for LCTRSs. The extension of such excluded inference rules to constrained ∃-equations is left as future work.

References

1. Baader, F., Nipkow, T.：《项重写及其他》。剑桥大学出版社（1998 505888 2 10 1145 505863）。https://doi.org/。/。。Bae, K., Rocha, C.：用于模 SMT 重写的守卫项。载于：Proença, J., Lumpe, M.（编）《第14届组件软件形式化方面国际会议论文集》。《计算机科学讲义》，第10487卷，第 78 97 2017 10 1007 978 3 319 68034 7_5 –页。施
3
普林格（）。https://doi.org/。/----。Bouhoula, A., Jacquemard, F.：利用受约束树自动机进行自动归纳。载于：Armando, A., Baumgartner, P., Dowek, G.（编）《第4届自动推理国际联合会议论文集》。《计算机科学讲义》，第5195卷，第539–554页。施普林格（2008年）。https://doi.org/
10 1007 978 3 540 71070 7_44 。/----。Buruiană, A.S.,
4
Ciobâcă, Ş.：通过转换语言语义将完全正确性归约为部分正确性。载于：Niehren, J., Sabel, D.（编）《第5届程序转换与求值重写技术国际研讨会论文集》。《理论计算机科学电子论文集》，第289卷，第1–16页。开放出版协会（2018年）。
https://doi.org/10 1 5 4204 289 。/EPTCS. . . Ciobâcă, Ş., Lucanu, D., Buruiană, A.：使用逻辑约束项重写系统进行基于操作语义的程序等价性证明。《程序设计中的逻辑与代数方法杂志》**135**，1 100894 6 22 2023 10 1016 2023 –（）。https://doi.org/。/j.jlamp. . . Ciobâcă, Ş., Lucanu, D.：一种用于证明逻辑约束项重写系统中可达性性质的余归纳方法。载于：Galmiche, D., Schulz, S., Sebastiani, R.（编）《第9届自动推理国际联合会议论文集》。《计算机科学讲义》，第10900卷，第295–311页。施普林格（ 2018 10 1007 978 3 319 94205 6_20 ）。
7
https://doi.org/。/----。Falke, S., Kapur, D.：针对含内置数值和语义数据结构的重写的依赖对。载于：Voronkov, A.（编）《第19届重写技术与应用国际会议论文集》。《计算机科学讲义》，第5117卷，第94–109页。施普林格（2008年）。
https://doi.org/10.1007/978-3-540- 70590-1 78 。Falke, S., Kapur, D.：一种用于命令式程序自动终止性分析的项重写方法。载于：Schmidt, R.A.（编）《第22届自动演绎国际会议论文集》。《计算机科学讲义》，第5663卷，第277–293页。施普林格（2009年）。https://doi.org/10.1007/978-3- 642-02959-2 229 。
Falke, S., Kapur, D.：线性算术决策过程的重写归纳 + 。载于：Gramlich, B., Miller, D., Sattler, U.（编）《第6届自动推理国际联合会议论文集》。《计算机科学讲义》，第7364卷，第241–255页。施普林格（2012年）。
https://doi.org/10.1007/978-3-642-31365- 3 20_

10. Fuhs, C., Giesl, J., Plücker, M., Schneider-Kamp, P., Falke, S.：证明整数项重写的终止性。载于：Treinen, R.（编）《第20届重写技术与应用国际会议论文集》。《计算机科学讲义》，第5595卷，第32–47页。施普林格（2009年）。https://doi.org/10.1007/978-3-642- 02348-4 3 11 。Fuhs, C., Guo, L., Kop, C.：用于受约束高阶重写的最内层依赖对框架。载于：Fernández, M.（编）《第10届计算与演绎形式结构国际会议论文集》。LIPIcs，第337卷，第20:1–20:24页。达格斯图尔城堡—莱布尼茨信息学中心（2025年）。https://doi.org/10 20 12 4230 2025 。/LIPIcs.FSCD. . . Fuhs, C., Kop, C., Nishida, N.：通过受约束重写归纳验证过程式程序。《ACM计算逻辑汇刊》**18**(2)，14:1–14:50（2017 3060143 13 10 1145）。https://doi.org/。/。Furuichi, Y., Nishida, N., Sakai, M., Kusakari, K., Sakabe, T.：基于受约束项重写系统的隐式归纳，对过程式程序进行验证的方法。《IPSJ 编程汇刊》**1**(2)，100–121（2008年），日语（可从 http://www.trs.css.i.nagoya-u.ac.jp/crisys/ 获取译文摘要）。14. Huet, G., Hullot, J.M.：具有构造子的等式理论中的归纳证明。《计算机与系统科学杂志》**25**(2)，239–266（1982年）。https://doi.org/10.1016/0022-0000(82)90006-X 15. Kojima, M., Nishida, N.：从无饥饿性到受约束重写中的全路径可达性问题。载于：Hanus, M., Inclezan, D.（编）《第25届声明式语言实践问题国际研讨会论文集》。《计算机科学讲义》，第13880卷，第161–179页。施普林格·自然瑞士（ 2023 10 1007 978 3 031 24841 2 _ 11 ）。https://doi.org/。/ - - - - 。16 Kojima, M., Nishida, N.：将指定运行时错误的不发生性归约为受约束重写中的全路径可达性问题。《程序设计中的逻辑与代数方法杂志》**135**，1–19（2023年）。https://doi.org/10 100903 17 1016 2023 。/j.jlamp. . . Kojima, M., Nishida, N.：在进程公平性下，求解并发重写系统无饥饿性相关的全路径可达性问题。载于：Kovács, L., Sokolova, A.（编）《第18届可达性问题国际会议论文集》。《计算机科学讲义》，第15050卷，第54–70页。施普林格（ 2024 10 1007 978 3 031 72621 7 _ 5 ）。https://doi.org/。/ - - - - 。18 Kojima, M., Nishida, N.：逻辑约束项重写系统满足带常量目标的全路径可达性问题可判定性的一项充分条件。《信息处理杂志》**32**，417–435（2024年）。https://doi.org/10 417 19 2197 32 。/IPSJJIP. . . Kojima, M., Nishida, N., Matsubara, Y.：将带信号量的并发程序转换为逻辑约束项重写系统。《程序设计中的逻辑与代数方法杂志》**143**，1–23（2025年）。https://doi.org/10 101033 20 1016 2024 。/j.jlamp. . . Kop, C.：LCTRS的终止性。载于：《第13届终止性研讨会论文集》。第59–63页（2013年）21. Kop, C.：逻辑约束项重写系统的准可约性。CoRR**abs/1702**02397 22**02397** 2017 1702.（），http://arxiv.org/abs/。。Kop, C., Nishida, N.：带逻辑约束的项重写。载于：Fontaine, P., Ringeissen, C., Schmidt, R.A.（编）《第9届组合系统前沿国际研讨会论文集》。《计算机科学讲义》，

第8152卷，第343–358页。施普林格（2013年）。
https://doi.org/10.1007/978-3-642-40885- 4 24_23. Kop, C., Nishida, N.：面向过程式程序验证的自动约束重写归纳。载于：Garrigue, J.（编）《第12届亚洲编程语言与系统研讨会论文集》。《计算机科学讲义》，第8858卷，第334–353页。施普林格（2014年）。
https://doi.org/10.1007/978-3- 319-12736-1 18_24. Kop, C., Nishida, N.：受约束项重写工具。载于：Davis, M., Fehnker, A., McIver, A., Voronkov, A.（编）《第20届编程、人工智能与推理逻辑国际会议论文集》。《计算机科学讲义》，第9450卷，第549–557页。施普林格（2015年）。https://doi.org/10.1007/978-3-662-48899-7_3825. Musser, D.R.：论抽象数据类型归纳性质的证明。载于：Abrahams, P.W., Lipton, R.J., Bourne, S.R.（编）《第7届ACM 编程语言原理研讨会论文集》。第154–162页（1980年）。
https://doi.org/10.1145/567446.567461 26. Nagao, T., Nishida, N.：受约束不等式的重写归纳。《计算机编程科学》**155**，76–102（2018年）。
https://doi.org/10.1016/j.scico.2017.10.012 27. Nishida, N., Kojima, M., Nakamura, Y.：逻辑约束项重写系统中受约束模式的差异。载于：Thiemann, R., Weidenbach, C.（编）《第15届组合系统前沿国际研讨会论文集》。《计算机科学讲义》，第15979卷，第247–266页。施普林格（2025年）。https://doi.org/10.1007/978-3-032-04167-8_1428. Nishida, N., Winkler, S.：基于逻辑约束项重写的循环检测。载于：Piskac, R., Rümmer, P.（编）《第10届经验证软件：理论、工具与实验工作会议论文集》。《计算机科学讲义》，第11294卷，第309–321页。施普林格（2018年）。
https://doi.org/10.1007/978-3- 030-03592-1 18_29. Ohlebusch, E.：项重写高级专题。施普林格（2002年）。https://doi.org/10.1007/978-1-4757-3661-8 30. Reddy, U.S.：项重写归纳。载于：Stickel, M.E.（编）《第10届自动演绎国际会议论文集》。《计算机科学讲义》，第449卷，第162–177页。施普林格（1990年）。https://doi.org/10.1007/3-540-52885-7 86_31. Sakata, T., Nishida, N., Sakabe, T., Sakai, M., Kusakari, K.：受约束项重写系统的重写归纳。《IPSJ 编程汇刊》**2**(2)，80–96（2009年），日语（译文摘要可从 https://www. trs.css.i.nagoya-u.ac.jp/crisys/ 获取）32. Schöpf, J., Middeldorp, A.：逻辑约束重写系统的合流判据。载于：Pientka, B., Tinelli, C.（编）《第29届自动演绎国际会议论文集》。《人工智能讲义》，第14132卷，第474–490页。施普林格（2023年）。https://doi.org/10.1007/978-3-031-38499- 8 27_33. Schöpf, J., Mitterwallner, F., Middeldorp, A.：再论逻辑约束重写系统的合流性。载于：Benzmüller, C., Heule, M.J.H., Schmidt, R.A.（编）《第12届自动推理国际联合会议论文集》。《计算机科学讲义》，第14740卷，第298–316页。施普林格（2024年）。
https://doi.org/10.1007/978-3-031-63501-4_16

34. Takahata, K., Schöpf, J., Nishida, N., Aoto, T.：通过存在约束项刻画逻辑约束项的等价性。载于：Escobar, S., Titolo, L.（编）《第35届基于逻辑的程序综合与变换国际研讨会论文集》。《计算机科学讲义》，第16117卷，第180–195页。施普林格（2025年）。https://doi.org/10.1007/978-3-032-04848 6 _12 - \ . Takahata, K., Schöpf, J., Nishida, N., Aoto, T.：恢复逻辑约束重写与等价变换的交换性。载于：Małgorzata Biernacka, C.O.（编）《第27届声明式编程原理与实践国际研讨会论文集》。第9:1–9:13页。计算机协会（2025 3756916 36 10 1145 3756907 ）。https://doi.org/ . / . . Vidal, G.：用于验证程序终止的封闭符号执行。载于：《第12届IEEE源代码分析与操作国际工作会议论文集》。第34–43页。IEEE计算机学会（2012年）。https://doi.org/10 13 37 1109 2012 . /SCAM. . . Winkler, S., Middeldorp, A.：逻辑约束重写的完备化。载于：Kirchner, H.（编）《第3届计算与演绎形式结构国际会议论文集》。莱布尼茨国际信息学会议录，第108卷，第30:1–30:18页。Schloss Dagstuhl–莱布尼茨信息学中心（2018年）。https://doi.org/10.4230/LIPIcs.FSCD.2018.30
35

A 省略的证明

A.1 定理 3.2 的证明

定理 3.2. 设 $\ell \to r\ [\varphi]$ 是 $\mathcal{R}$、 $s\,[\phi]$、$t\,[\psi]$ 中一个左值自由且左 *TV* 自由的受约束重写规则， p 是 s 的一个位置，使得$\mathcal{V}ar(\ell$、 r、 $\varphi)\cap\mathcal{V}ar(s$、 ϕ、 t、 $\psi) = \emptyset$。若 $s\,[\phi] \sim \cdot \to_{\mathsf{base},p,\ell\to r\ [\phi]} t\,[\psi]$，则存在一个替换 γ，使得 $s\,[\phi] \sim s\,[\phi \wedge \varphi\gamma] \to_{\mathsf{base},p,\ell\to r\ [\varphi]} s[r\gamma]_p\,[\phi \wedge \varphi\gamma] \sim t\,[\psi]$。

证明。根据定义，我们有 $\phi' = \psi$。由于 $s'\,[\phi'] \to_{\mathsf{base}、\ p、\ \ell\to r\ [\phi]} t\,[\psi]$，存在一个替换 σ，使得 $s'|_p = \ell\sigma$、 $t = s'[r\sigma]_p$，并且 $(\phi' \Rightarrow \varphi\sigma)$ 有效。对于每个受约束项，都存在一个与之等价的值自由且 LV 线性的受约束项 [18, 34]。设 $s_0\,[\phi_0]$ 是 $s\,[\phi]$ 的一个等价的值自由且 LV 线性的受约束项： $s_0\,[\phi_0] \sim s\,[\phi]$。于是，对于任意变量 $x \in \mathcal{V}ar(s_0)\cap\mathcal{V}ar(\phi_0)$，存在一个替换 θ，使得 $x\theta \in \mathcal{V}al\cup\mathcal{V}ar(\phi)$、 $s = s_0\theta$、 $\mathcal{V}ar(\phi) = \mathcal{V}ar(\phi_0\theta)$，并且 $(\phi \Leftrightarrow \phi_0\theta)$ 有效。此外，由于 $s\,[\phi] \sim s'\,[\phi']$，存在一个替换 θ'，使得 $\mathcal{D}om(\theta') = \mathcal{V}ar(s_0)\cap\mathcal{V}ar(\phi)$、 $x\theta' \in \mathcal{V}al\cup\mathcal{V}ar(\phi')$；对于任意变量 $x \in \mathcal{V}ar(s_0)\cap\mathcal{V}ar(\phi_0)$， $s' = s_0\theta'$、 $\mathcal{V}ar(\phi') = \mathcal{V}ar(\phi_0\theta')$，并且 $(\phi' \Leftrightarrow \phi_0\theta')$ 有效。由于 ℓ 值自由且 TV 线性，并与 $s'|_p$ 匹配，因此存在一个替换 σ_0，使得 $s_0|_p = \ell\sigma_0$。于是，我们有 $s|_p = (s_0|_p)\theta = \ell\sigma_0\theta$，$(\phi \wedge \varphi\sigma_0\theta \Rightarrow \varphi\sigma_0\theta)$ 有效，从而 $s\,[\phi \wedge \varphi\gamma] = s\,[\phi \wedge \varphi\sigma_0\theta] \to_{\mathsf{base}、\ p、\ \ell\to r\ [\varphi]} s[r\sigma_0\theta]_p\,[\phi \wedge \varphi\sigma_0\theta] = s[r\gamma]_p\,[\phi \wedge \varphi\gamma] \sim t\,[\psi]$。 □

A.2 Proof of Theorem 4.8

Theorem 4.8. *For constrained ∃-terms* $(\exists\vec{x} : \eta.\ s)\ [\phi]$ *and* $(\exists\vec{y} : \delta.\ t)\ [\psi]$ *with* $\{\vec{x}\} \cap \mathcal{V}ar(\phi) = \emptyset$ *and* $\{\vec{y}\} \cap \mathcal{V}ar(\psi) = \emptyset$*, if* $(\exists\vec{x} : \eta.\ s)\ [\phi] \rightharpoonup_{\mathcal{R}} (\exists\vec{y} : \delta.\ t)\ [\psi]$*, then both of the following statements hold:*

1. *for every substitution* θ *respecting* $\phi \wedge \eta$*, there exists a substitution* σ *such that* σ *respects* $\psi \wedge \delta$ *and* $s\theta \to_{\mathcal{R}} t\sigma$*, and*
2. *for every substitution* σ *respecting* $\psi \wedge \delta$*, there exists a substitution* θ *such that* θ *respects* $\phi \wedge \eta$ *and* $s\theta \to_{\mathcal{R}} t\sigma$*.*

Proof. Suppose that $(\exists\vec{x} : \eta.\ s)\ [\phi] \rightharpoonup_{\mathcal{R}} (\exists\vec{y} : \delta.\ t)\ [\psi]$. We assume w.l.o.g. that $\{\vec{x}\} \cap \mathcal{V}ar(s, \phi) = \emptyset$. Then, there exist a constrained rewrite rule $\ell \to r\ [\varphi] \in \mathcal{R} \cup \mathcal{R}_{calc}$, a position p of s, and a substitution γ such that

– $s|_p = \ell\gamma$, $t = s[r\gamma]_p$, $\psi = (\phi \wedge (\varphi\gamma))$,– $x\gamma \in \mathcal{V}al \cup \mathcal{V}ar(\phi)$ 对任意变量 $x \in \mathcal{V}ar(\varphi) \cap \mathcal{V}ar(\ell)$,– $x\gamma \in \mathcal{V} \setminus (\mathcal{V}ar(s) \cup \{\vec{x}\})$ 对任意变量 $x \in \mathcal{V}ar(\varphi) \setminus \mathcal{V}ar(\ell)$,– $(\phi \Rightarrow (\exists\vec{z}.\ \varphi\gamma))$ 有效，并且 – $(\exists\vec{y}.\ \delta) = (\exists\vec{x}, \vec{z}.\ (\eta \wedge \varphi\gamma))$，其中 $\{\vec{z}\} = \{x\gamma \mid \exists x \in \mathcal{V}ar(\varphi) \setminus \mathcal{V}ar(\ell)\}$。

我们先证明第一个结论。设 θ 是一个尊重 $\phi \wedge \eta$ 的替换。由于 $(\phi \Rightarrow (\exists\vec{z}.\ \varphi\gamma))$ 有效，因此存在一个替换 θ'，使得 $\mathcal{D}om(\theta') \setminus \{\vec{z}\}, \mathcal{R}an(\theta') \subseteq \mathcal{V}al$，且 $[\![(\varphi\gamma)(\theta \cup \theta')]\!]_{\mathcal{J}} =$ 为真。令 $\sigma = (\theta \cup \theta')$。那么， σ 是一个尊重 $\psi \wedge \delta = (\phi \wedge (\varphi\gamma) \wedge \eta)$ 的替换，因此我们有 $s\theta = (s[\ell\gamma]_p)\theta \to_{\mathcal{R}} (s[r\gamma]_p)(\theta \cup \theta') = t\sigma$。

The second claim can be proved similarly to the first one. □

A.3 Proof of Theorem 5.4

The proof of Theorem 5.4 follows [12, Section 4.4]. For a set $\mathcal{E}$ of constrained $\exists$-equations, we denote the set $\{s \to t\ [\phi \wedge \eta] \mid (\exists \vec{x} : \eta.\ s \approx t)\ [\phi] \in \mathcal{E}\}$ by $\tilde{\mathcal{E}}$. The oriented equation $s \to t\ [\phi \wedge \eta]$ may not be a constrained rewrite rule, but we deal with it as a constrained rewrite rule below.

Definition A.1 ($\leftrightarrow_{\mathcal{E}}$ over ground terms). *Let $\mathcal{E}$ be a set of constrained $\exists$-equations. The relation $\leftrightarrow_{\mathcal{E}}$ over ground terms is defined as follows: for ground terms s, t, $s \leftrightarrow_{\mathcal{E}} t$ if and only if $s \leftrightarrow_{\tilde{\mathcal{E}}} t$.*

Lemma A.2. *If $(\mathcal{E}, \mathcal{H}) \vdash_{\mathrm{RI}} \cdots \vdash_{\mathrm{RI}} (\mathcal{E}', \mathcal{H}')$, then all of the following hold:*

1. *$\leftrightarrow_{\mathcal{E}} \subseteq (\to^*_{\mathcal{R}\cup\mathcal{H}'} \cdot \overline{\leftrightarrow}_{\mathcal{E}'} \cdot \leftarrow^*_{\mathcal{R}\cup\mathcal{H}'})$ over ground terms,*
2. *if $\to_{\mathcal{R}\cup\mathcal{H}} \subseteq (\to_{\mathcal{R}} \cdot \to^*_{\mathcal{R}\cup\mathcal{H}} \cdot \overline{\leftrightarrow}_{\mathcal{E}} \cdot \leftarrow^*_{\mathcal{R}\cup\mathcal{H}})$ over ground terms, then $\to_{\mathcal{R}\cup\mathcal{H}'} \subseteq (\to_{\mathcal{R}} \cdot \to^*_{\mathcal{R}\cup\mathcal{H}'} \cdot \overline{\leftrightarrow}_{\mathcal{E}'} \cdot \leftarrow^*_{\mathcal{R}\cup\mathcal{H}'})$ over ground terms, and*
3. *if $\mathcal{R} \cup \mathcal{H}$ is terminating, then $\mathcal{R} \cup \mathcal{H}'$ is so.*

Proof. It suffices to show the case where $(\mathcal{E}, \mathcal{H}) \vdash_{\mathrm{RI}} (\mathcal{E}', \mathcal{H}')$.

1. Since the case where the applied equation is in $\mathcal{E}'$ is trivial, we consider the remaining case where the applied equation is in $\mathcal{E} \setminus \mathcal{E}'$. We make a case analysis depending on which inference rule is applied.
   - Case where Simplification is applied. Assume that the applied equation is $(\exists \vec{x} : \eta.\ s \simeq t)\ [\phi] \in \mathcal{E} \setminus \mathcal{E}'$, where
     - $(\exists \vec{x} : \eta.\ s \approx t)\ [\phi] \rightharpoonup_{\mathcal{R}\cup\mathcal{H}} (\exists \vec{y} : \eta'.\ s' \approx t')\ [\phi']$, and
     - $(\exists \vec{y} : \eta'.\ s' \approx t')\ [\phi'] \in \mathcal{E}'$.

     It follows from Theorem 4.8 that $\leftrightarrow_{\mathcal{E}} \subseteq \to_{\mathcal{R}\cup\mathcal{H}} \cdot \leftrightarrow_{\mathcal{E}'}$. Therefore, the claim holds.
   - Case where Expansion is applied. Assume that the applied equation is $(\exists \vec{x} : \eta.\ s \simeq t)\ [\phi] \in \mathcal{E} \setminus \mathcal{E}'$, where
     - $s \to t\ [\phi \wedge \eta]$ is a constrained rewrite rule,
     - $\mathcal{E}' \setminus \mathcal{E} = \mathit{Expd}_{\mathcal{R}}(s \to t\ [\phi \wedge \eta],\ p)$,
     - $\mathcal{H}' = \mathcal{H} \cup \{s \to t\ [\phi \wedge \eta]\}$,
     - p is a reduction-complete position of s under ϕ, and
     - $\mathcal{R} \cup \mathcal{H}'$ is terminating.

     Since p is a reduction-complete position of s, there exist a constrained rewrite rule $\ell \to r\ [\varphi] \in \mathcal{R}$ and a substitution θ such that
     - θ is more general than γ,
     - θ is an idempotent mgu of $s|_p$ and ℓ, and
     - $(\exists \vec{x} : \eta\theta.\ s\theta \approx t\theta)\ [\phi\theta] \rightharpoonup_{p,\ell\to r\ [\varphi]} (\exists \vec{y} : \eta'.\ s' \approx t')\ [\phi'] \in \mathit{Expd}_{\mathcal{R}}(s \to t\ [\phi \wedge \eta],\ p)$

     Thus, we have that $\leftrightarrow_{\{(\exists \vec{x}:\eta.\ s\approx t)\ [\phi]\}} \subseteq \to_{\mathcal{R}} \cdot \leftrightarrow_{\mathcal{E}'}$. Therefore, this claim holds.
   - Case where Deletion is applied. Assume that the applied equation is $(\exists \vec{x} : \eta.\ s \approx t)\ [\phi] \in \mathcal{E} \setminus \mathcal{E}'$, where if one of the following holds:
     - $s = t$,
     - ϕ is unsatisfiable, or

- $s, t \in T(\Sigma_{theory}, \mathcal{V}ar(\phi) \cup \{\vec{x}\})$ and $(\phi \Rightarrow \exists \vec{x}.\ (\eta \wedge s = t))$ is valid.

In the first case above, the claim trivially holds. In the second case, the equation is not instantiated. We now consider the third case. Let γ be a ground substitution respecting ϕ. Since $[\![\phi\gamma]\!]_{\mathcal{J}} = \mathsf{true}$, there exists a substitution θ respecting $(\eta \wedge (s = t))\gamma|_{\mathcal{V}ar(\phi)\setminus\{\vec{x}\}}$. Thus, we have that $[\![s\gamma|_{\mathcal{V}ar(\phi)\setminus\{\vec{x}\}}\theta]\!]_{\mathcal{J}} = [\![t\gamma|_{\mathcal{V}ar(\phi)\setminus\{\vec{x}\}}\theta]\!]_{\mathcal{J}}$, and thus $s\gamma|_{\mathcal{V}ar(\phi)\setminus\{\vec{x}\}}\theta \leftrightarrow^*_{\mathcal{R}} t\gamma|_{\mathcal{V}ar(\phi)\setminus\{\vec{x}\}}\theta$. Therefore, the claim holds.

2. Thanks to the assumption, it suffices to consider the case where $\mathcal{H} \subset \mathcal{H}'$, i.e., Expansion is applied. This claim can be proved similarly to the case of applying Expansion in the first claim.
3. Trivial by definition. □

Lemma A.3 (a variant of RI principle [31, Theorem A.1.2]). *Let ARSs $(A, \to_1)$ and $(A, \to_2)$. Assume that*

- $\to_1 \subseteq \to_2$,
- $\to_2$ *is terminating, and*
- $\to_2 \subseteq (\to_1 \circ \to_2^* \circ \leftrightarrow_1^* \circ \leftarrow_2^*)$.

Then, $\leftrightarrow_1^* = \leftrightarrow_2^*$.

Theorem 5.4. *Given a set $\mathcal{E}$ of constrained $\exists$-equations, if an LCTRS $\mathcal{R}$ is terminating and $(\mathcal{E}, \emptyset) \vdash^*_{\mathrm{RI}} (\emptyset, \mathcal{H})$, then all constrained $\exists$-equations in $\mathcal{E}$ are inductive theorems of $\mathcal{R}$.*

Proof. Let $(\exists \vec{x} : \eta.\ s \approx t)\ [\phi] \in \mathcal{E}$, γ a ground substitution respecting ϕ, and θ a ground substitution respecting $\eta\gamma|_{\mathcal{V}ar(\phi)\setminus\{\vec{x}\}}$. We show that $s\eta\gamma|_{\mathcal{V}ar(\phi)\setminus\{\vec{x}\}} \leftrightarrow^*_{\mathcal{R}} t\eta\gamma|_{\mathcal{V}ar(\phi)\setminus\{\vec{x}\}}$. It follows from Lemma A.2 that

$$s\eta\gamma|_{\mathcal{V}ar(\phi)\setminus\{\vec{x}\}}\ (\to^*_{\mathcal{R}\cup\mathcal{H}} \cdot \leftarrow^*_{\mathcal{R}\cup\mathcal{H}})\ t\eta\gamma|_{\mathcal{V}ar(\phi)\setminus\{\vec{x}\}}$$

It follows from Lemma A.3 that $\leftrightarrow^*_{\mathcal{R}} = \leftrightarrow^*_{\mathcal{R}\cup\mathcal{H}}$ over ground terms, and hence

$$s\eta\gamma|_{\mathcal{V}ar(\phi)\setminus\{\vec{x}\}} \leftrightarrow^*_{\mathcal{R}} t\eta\gamma|_{\mathcal{V}ar(\phi)\setminus\{\vec{x}\}}$$

Therefore, $(\exists \vec{x} : \eta.\ s \approx t)\ [\phi] \in \mathcal{E}$ is an inductive theorem of $\mathcal{R}$. □