

*Regular Paper***Soundness of Rewriting Induction based on an Abstract Principle**TAKAHITO AOTO[†]

Rewriting induction (Reddy, 1990) is a method to prove inductive theorems of term rewriting systems automatically. Koike and Toyama (2000) extracted an abstract principle of rewriting induction in terms of abstract reduction systems. Based on their principle, the soundness of the original rewriting induction system can be proved. It is not known, however, whether such an approach can be adapted also for more powerful rewriting induction systems. In this paper, we give a new abstract principle that extends Koike and Toyama's abstract principle. Using this principle, we show the soundness of a rewriting induction system extended with an inference rule of simplification by conjectures. Inference rules of simplification by conjectures have been used in many rewriting induction systems. Replacement of the underlying rewriting mechanism with ordered rewriting is an important refinement of rewriting induction—with this refinement, rewriting induction can handle non-orientable equations. It is shown that, based on the introduced abstract principle, a variant of our rewriting induction system based on ordered rewriting is sound, provided that its base order is ground-total. In our system based on ordered rewriting, the simplification rule extends those of the equational fragment of some major systems from the literature.

1. Introduction

Properties of programs are often proved by induction on data structures such as natural numbers or lists. Such properties are called *inductive properties* of programs. Inductive properties are indispensable in formal treatments of programs such as program verification and program transformation. For such applications, automated reasoning on inductive properties is crucial.

Term rewriting systems (TRSs) are a computational model based on equational logic that has been studied extensively^{2),21)}. Inductive properties of TRSs are called *inductive theorems*, and methods that automatically perform inductive reasoning in term rewriting have been investigated for many years^{4)~7),10),12)~18),20),22)}.

Rewriting induction[☆] proposed by Reddy¹⁸⁾ is one of such inductive theorem proving methods. Contrasted to *inductionless induction*^{12),13),15),17),22)}, in which some kind of Church-Rosser property is needed, the basis of rewriting induction is noetherian induction. *Test set induction*^{5)~7)} used for the basis of well-known inductive theorem prover SPIKE can be regarded as a variant of rewriting induction.

An inference system for proving inductive theorems is said to be *sound* if every successfully derived equation is an inductive theorem. Koike and Toyama¹⁶⁾ extracted an abstract principle from rewriting induction in terms of abstract reduction systems. Based on their principle, the soundness of the original rewriting induction system can be proved¹⁾. It is not known, however, whether such an approach can be adapted also for more powerful rewriting induction systems.

Many refinements have been introduced for rewriting induction to increase its power and efficiency of theorem proving. The underlying rewriting mechanism has been replaced by ordered rewriting in 9) so that rewriting induction can also handle non-orientable equations; not only ordered rewriting but also relaxed rewriting is used in the inference systems of SPIKE^{5)~7)} to get more flexible expansion and simplification rules. Another refinement is to use simplification by conjectures (equations to prove)^{5)~9)}. More inference rules are added to get efficient proofs and/or failure detection in some systems. Another direction for extension is to make the framework more general. The induction systems of SPIKE^{5)~7)} can handle not only equational theories but conditional ones; moreover, inductive properties can be given not only in equations but also in clauses. Further generalization is given in 8) whose underlying logical theory is replaced with an abstract first-order deductive relation.

[†] RIEC, Tohoku University

[☆] Originally, it is called “*term rewriting induction*”. The terminology “*rewriting induction*” is introduced in 16).

Stratulat^{4),20)} strengthens such an abstraction further by a general abstract inference system that can be used to prove general inductive properties of any first-order deductive relation.

In this paper, we give a new abstract principle that extends Koike and Toyama's abstract principle. Using this principle, we show the soundness of a rewriting induction system extended with an inference rule of simplification by conjectures (equations to prove).

It is also shown that, based on the same abstract principle, a variant of our rewriting induction system based on ordered rewriting is sound, provided that its base order is ground-total. Contrasted to many previous work, our approach can handle only first-order term rewriting and proof of equations. On the other hand, in our system based on ordered rewriting, our general simplification-by-conjectures rule extends those of the equational fragment of some major systems from the literature. Furthermore, the soundness of our system is not explained by the abstract frameworks of (8) and (20).

The rest of the paper is organized as follows. After fixing basic notation (Section 2), we review rewriting induction (Section 3). In Section 4, we present our extension of rewriting induction and discuss its soundness. Section 5 introduces a variant of our system based on ordered rewriting. In Section 6, we compare our system with other major systems. Section 7 concludes.

2. Preliminaries

Let us fix some notation for *abstract reduction systems (ARSs)*. Let \rightarrow be a binary relation on a set A . The reflexive transitive closure (symmetric closure, equivalence closure) of \rightarrow is denoted by \rightarrow^* (\leftrightarrow , $\overset{*}{\leftrightarrow}$, respectively). The relation \rightarrow is *well-founded* (denoted by $\text{SN}(\rightarrow)$) if there exists no infinite chain $a_0 \rightarrow a_1 \rightarrow \dots$. An element a is said to be *normal* if there is no b such that $a \rightarrow b$. The set of normal elements is denoted by $\text{NF}(\rightarrow)$. The union $\rightarrow_i \cup \rightarrow_j$ of two binary relations \rightarrow_i and \rightarrow_j is abbreviated as $\rightarrow_{i \cup j}$. We assume \cup associates stronger than the closure operations so that, for example, $\overset{*}{\leftrightarrow}_{1 \cup 2}$ stands for the equivalence closure of $\rightarrow_1 \cup \rightarrow_2$. We use \circ for the composition operator. A binary relation $\overset{*}{\rightarrow}_i \circ \overset{*}{\leftarrow}_i$ is abbreviated as \downarrow_i .

We next introduce notation for term rewriting used in this paper. (For details, see 2).)

The sets of function symbols and variables are denoted by \mathcal{F} and V , respectively. The arity of a function symbol f is denoted by $\text{arity}(f)$. A function symbol of arity 0 is called a *constant*. The set $\text{T}(\mathcal{F}, V)$ of terms over \mathcal{F}, V is defined as usual. We use \equiv to denote the syntactical equality. The set of variables contained in a term t is denoted by $V(t)$.

A *position* is a (possibly empty) sequence of natural numbers. The empty sequence is denoted by ϵ . The set of positions of a term t is denoted by $\text{Pos}(t)$ and the *subterm* of t at the position $p \in \text{Pos}(t)$ by t/p . We write $u \trianglelefteq t$ if u is a subterm of t . The *root symbol* of a term t is denoted by $\text{root}(t)$. Let \square be a constant not occurring in \mathcal{F} . A *context* is an element in $\text{T}(\mathcal{F} \cup \{\square\}, V)$. The special constant \square in contexts is called a *hole*. If a context C has n holes in it, we denote by $C[t_1, \dots, t_n]$ a term obtained by replacing holes with t_1, \dots, t_n from left to right. We write $C[u]_p$ if $C/p \equiv \square$.

A mapping σ from V to $\text{T}(\mathcal{F}, V)$ is called a *substitution*; as usual, we identify σ and its homomorphic extension. The *domain* of a substitution σ is denoted by $\text{dom}(\sigma)$, i.e. $\text{dom}(\sigma) = \{x \in V \mid \sigma(x) \neq x\}$. A term $\sigma(t)$ is called an *instance* of the term t ; $\sigma(t)$ is also written as $t\sigma$. We denote by $\text{mgu}(s, t)$ the *most general unifier* of terms s, t . A pair $\langle l, r \rangle$ of terms l, r satisfying conditions (1) $\text{root}(l) \in \mathcal{F}$ and (2) $V(r) \subseteq V(l)$ is said to be a *rewrite rule*. As usual, a rewrite rule $\langle l, r \rangle$ is denoted by $l \rightarrow r$. A *term rewriting system (TRS)* is a set of rewrite rules. We also specify the set \mathcal{F} of function symbols and write $\langle \mathcal{F}, \mathcal{R} \rangle$ instead of \mathcal{R} if there exists a function symbol that does not occur in the rewrite rules. Let \mathcal{R} be a TRS. If there exist a context C , a substitution σ , and a rewrite rule $l \rightarrow r \in \mathcal{R}$ such that $s \equiv C[l\sigma]_p$ and $t \equiv C[r\sigma]_p$, we write $s \rightarrow_{\mathcal{R}} t$. We call $s \rightarrow_{\mathcal{R}} t$ a *rewrite step*. The rewrite step $s \rightarrow_{\mathcal{R}} t$ is sometimes written as $s \xrightarrow{p, l \rightarrow r}_{\mathcal{R}} t$ to indicate the position p and the rewrite rule $l \rightarrow r$ used in this rewrite step. $\rightarrow_{\mathcal{R}}$ forms a relation on $\text{T}(\mathcal{F}, V)$, called the *rewrite relation* of \mathcal{R} . Closure operations and the notion of normal terms are adapted to rewrite relations as usual. An *equation* $l \doteq r$ is a pair $\langle l, r \rangle$ of terms. When we write $l \doteq r$, however, we do not distinguish $\langle l, r \rangle$ and $\langle r, l \rangle$. The rewrite relation of a set E of equations is defined in a way similar to that of a TRS, i.e. $s \leftrightarrow_E t$ if there exist a context C , a substitution σ and an equation $\langle l, r \rangle \in E$

satisfying either $s \equiv C[l\sigma]$ and $t \equiv C[r\sigma]$ or $t \equiv C[l\sigma]$ and $s \equiv C[r\sigma]$ (or equivalently, an equation $l \doteq r \in E$ such that $s \equiv C[l\sigma]$ and $t \equiv C[r\sigma]$).

The set of *defined function symbols* is given by $\mathcal{D}_{\mathcal{R}} = \{\text{root}(l) \mid l \rightarrow r \in \mathcal{R}\}$ and the set of *constructor symbols* by $\mathcal{C}_{\mathcal{R}} = \mathcal{F} \setminus \mathcal{D}_{\mathcal{R}}$. The set of defined symbols appearing in a term t is denoted by $\mathcal{D}_{\mathcal{R}}(t)$. When \mathcal{R} is obvious from its context, we omit the subscript \mathcal{R} from $\mathcal{D}_{\mathcal{R}}$, $\mathcal{C}_{\mathcal{R}}$. Terms in $\mathbb{T}(\mathcal{C}, V)$ are said to be *constructor terms*; a substitution σ such that $\sigma(x) \in \mathbb{T}(\mathcal{C}, V)$ for any $x \in \text{dom}(\sigma)$ is called a *constructor substitution*. A term of the form $f(c_1, \dots, c_n)$ for some $f \in \mathcal{D}$ and $c_1, \dots, c_n \in \mathbb{T}(\mathcal{C}, V)$ is said to be *basic*. The set $\{u \trianglelefteq s \mid \exists f \in \mathcal{D}. \exists c_1, \dots, c_n \in \mathbb{T}(\mathcal{C}, V). u \equiv f(c_1, \dots, c_n)\}$ of basic subterms of s is written as $\mathcal{B}(s)$.

A term t is said to be *ground* if $V(t) = \emptyset$. The set of ground terms is denoted by $\mathbb{T}(\mathcal{F})$. If $t\sigma \in \mathbb{T}(\mathcal{F})$, $t\sigma$ is called a *ground instance* of t . The ground instance of a rewrite rule, an equation, etc. is defined similarly. A *ground substitution* is a substitution σ_g such that $\sigma_g(x) \in \mathbb{T}(\mathcal{F})$ for any $x \in \text{dom}(\sigma_g)$. A TRS \mathcal{R} is said to be *quasi-reducible* if no ground basic term is normal. Without loss of generality, we can assume that $t\sigma_g$ is ground (i.e. $V(t) \subseteq \text{dom}(\sigma_g)$) when we speak of an instance $t\sigma_g$ of t by a ground substitution σ_g ; and so for ground instances of rewrite rules, equations, etc. An *inductive theorem* of a TRS \mathcal{R} is an equation that is valid on $\mathbb{T}(\mathcal{F})$, i.e. $s \doteq t$ is an inductive theorem if $s\sigma_g \xrightarrow{*}_{\mathcal{R}} t\sigma_g$ holds for any ground instance $s\sigma_g \doteq t\sigma_g$. In other words, a set E of equations is a set of inductive theorems of \mathcal{R} iff $\xrightarrow{*}_{\mathcal{R}} = \xrightarrow{*}_{\mathcal{R} \cup E}$ holds on $\mathbb{T}(\mathcal{F})$.

Example 1 Let \mathcal{R} be a TRS for the addition of natural numbers:

$$\mathcal{R} \begin{cases} 0 + y & \rightarrow y \\ s(x) + y & \rightarrow s(x + y) \end{cases}$$

Consider the equation $(x + y) + z \doteq x + (y + z)$ that expresses the associativity of addition. This equation is an inductive theorem of \mathcal{R} , that is, $((x + y) + z)\sigma_g \xrightarrow{*}_{\mathcal{R}} (x + (y + z))\sigma_g$ for any ground substitution σ_g . (We assume $x, y, z \in \text{dom}(\sigma_g)$, as mentioned above.)

A (strict) partial order $>$ is an irreflexive transitive relation. $a \geq b$ iff $a > b$ or $a = b$; or, if $>$ is a partial order on syntactical objects, $s \geq t$ iff $s > t$ or $s \equiv t$. A partial order $>$ is *well-founded* if there is no infinite descending chain $a_0 > a_1 > \dots$. A relation R on $\mathbb{T}(\mathcal{F}, V)$

is said to be *closed under substitutions* if $s R t$ implies $s\sigma R t\sigma$ for any substitution σ ; *closed under contexts* if $s R t$ implies $C[s] R C[t]$ for any context C . A *reduction order* is a well-founded partial order on $\mathbb{T}(\mathcal{F}, V)$ that is closed under substitutions and contexts. A partial order $>$ on $\mathbb{T}(\mathcal{F}, V)$ is said to be *ground-total* if $s_g \equiv t_g$, $s_g < t_g$ or $t_g > s_g$ hold for any $s_g, t_g \in \mathbb{T}(\mathcal{F})$.

3. Rewriting induction

Rewriting induction (RI for short) proposed by Reddy¹⁸⁾ is a method to prove inductive theorems automatically. This section reviews rewriting induction and proves basic properties of an operation involved in our formulation of rewriting induction.

Let \mathcal{R} be a TRS and $>$ a reduction order. We list the inference rules of rewriting induction in downward fashion in **Fig.1**. In the figure, the relation \uplus expresses the disjoint union and the ternary operation Expd is defined as:

$$\text{Expd}_u(s, t) = \{C[r]\sigma \doteq t\sigma \mid s \equiv C[u], \\ \sigma = \text{mgu}(u, l), l \rightarrow r \in \mathcal{R}, l:\text{basic}\}$$

A rewriting induction procedure starts from a pair $\langle E_0, \emptyset \rangle$ where E_0 is the set of conjectures to prove. It successively applies those inference rules to a pair $\langle E, H \rangle$. Intuitively, E is a set of equations to be proved and H is a set of induction hypotheses and theorems already proved.

Definition 2 If $\langle E', H' \rangle$ is obtained from $\langle E, H \rangle$ by applying one of the inference rules from **Fig.1**, we write $\langle E, H \rangle \rightsquigarrow_{\text{RI}} \langle E', H' \rangle$. The reflexive transitive closure of $\rightsquigarrow_{\text{RI}}$ is denoted by $\rightsquigarrow^*_{\text{RI}}$. We sometimes write $\rightsquigarrow^s_{\text{RI}}$, $\rightsquigarrow^d_{\text{RI}}$, or $\rightsquigarrow^e_{\text{RI}}$ to indicate which inference rule is used.

If a derivation by $\rightsquigarrow_{\text{RI}}$ eventually reaches the form $\langle \emptyset, H' \rangle$ then the procedure returns “success”—this means that the conjectures are inductive theorems of \mathcal{R} . On the other hand, when none of the rules are applicable for $\langle E, H \rangle$ with $E \neq \emptyset$, the procedure reports “failure” and the procedure may also run forever (“divergence”)—in these cases, rewriting induction fails to prove that the conjectures are inductive theorems. A proof of the next proposition will be given afterwards in a more general setting.

Proposition 3 (Reddy¹⁸⁾) Let \mathcal{R} be a quasi-reducible TRS, E a set of equations, and $>$ a reduction order satisfying $\mathcal{R} \subseteq >$. If $\langle E, \emptyset \rangle \rightsquigarrow^*_{\text{RI}} \langle \emptyset, H \rangle$ for some set H of rewrite rules, then the equations of E are inductive theorems of \mathcal{R} .

$$\begin{array}{l}
\text{Expand} \\
\frac{\langle E \uplus \{s \doteq t\}, H \rangle}{\langle E \cup \text{Expd}_u(s, t), H \cup \{s \rightarrow t\} \rangle} \quad u \in \mathcal{B}(s), s > t \\
\text{Simplify} \\
\frac{\langle E \uplus \{s \doteq t\}, H \rangle}{\langle E \cup \{s' \doteq t\}, H \rangle} \quad s \rightarrow_{\mathcal{R} \cup H} s' \\
\text{Delete} \\
\frac{\langle E \uplus \{s \doteq s\}, H \rangle}{\langle E, H \rangle}
\end{array}$$

Fig. 1 Inference rules of RI

$$\begin{array}{l}
\sim_{\text{RI}}^e \left\langle \left\{ \left\{ (x+y) + z \doteq x + (y+z) \right\}, \{\} \right\} \right\rangle \\
\sim_{\text{RI}}^s \left\langle \left\{ \left\{ \begin{array}{l} y_0 + z \doteq 0 + (y_0 + z) \\ s(x_1 + y_1) + z \doteq s(x_1) + (y_1 + z) \end{array} \right\}, \left\{ (x+y) + z \rightarrow x + (y+z) \right\} \right\} \right\rangle \\
\sim_{\text{RI}}^d \left\langle \left\{ \left\{ \begin{array}{l} y_0 + z \doteq y_0 + z \\ s(x_1 + (y_1 + z)) \doteq s(x_1 + (y_1 + z)) \end{array} \right\}, \left\{ (x+y) + z \rightarrow x + (y+z) \right\} \right\} \right\rangle \\
\sim_{\text{RI}}^d \left\langle \{\}, \left\{ (x+y) + z \rightarrow x + (y+z) \right\} \right\rangle
\end{array}$$

Fig. 2 A process of rewriting induction

Example 4 Let \mathcal{R} be the TRS given in **Example 1** and let $E = \{(x+y) + z \doteq x + (y+z)\}$. Let $>$ be the lexicographic path order²⁾ based on a precedence $+ > s > 0$. In **Fig. 2**, we present a successful derivation by rewriting induction starting from $\langle E, \emptyset \rangle$.

Before we end the section, we introduce two properties of Expd that will be used later.

Lemma 5 Let \mathcal{R} be a quasi-reducible TRS and $u \in \mathcal{B}(s)$. Then (1) $s\sigma_g \rightarrow_{\mathcal{R}} \circ \leftrightarrow_{\text{Expd}_u(s,t)} t\sigma_g$ for any ground constructor substitution σ_g and (2) $v_g \leftrightarrow_{\text{Expd}_u(s,t)} w_g$ implies $v_g \overset{*}{\leftrightarrow}_{\mathcal{R} \cup \{s \doteq t\}} w_g$ for any ground terms v_g, w_g .

Proof (1) Since u is basic and σ_g is a ground constructor substitution, $u\sigma_g$ is a basic ground term. Thus, by the quasi-reducibility of \mathcal{R} , there exists $l \rightarrow r \in \mathcal{R}$ such that $u\sigma_g$ is an instance of l . Then l is basic because $u\sigma_g$ is basic. W.l.o.g. we may assume $V(l) \cap V(s) = \emptyset$ and thus by extending σ_g one can let $u\sigma_g \equiv l\sigma_g$ so that σ_g is a unifier of u and l . Let $\sigma = \text{mgu}(u, l)$. Then we have $\sigma_g = \theta_g \circ \sigma$ for some substitution θ_g . By letting $s \equiv C[u]$, we have $s\sigma_g \equiv C[u]\sigma_g \equiv C\sigma_g[u\theta_g] \equiv C\sigma_g[l\theta_g] \rightarrow_{\mathcal{R}} C\sigma_g[r\theta_g] \equiv C[r]\theta_g \leftrightarrow_{\text{Expd}_u(s,t)} t\theta_g \equiv t\sigma_g$.

(2) Let $v_g \leftrightarrow_{\text{Expd}_u(s,t)} w_g$. By the definition of Expd , for some $C_g, C, \sigma_g, \sigma, u, l \rightarrow r \in \mathcal{R}$, we have $v_g \equiv C_g[C[r]\sigma_g]$, $w_g \equiv C_g[t\sigma_g]$ (or $w_g \equiv C_g[C[r]\sigma_g]$, $v_g \equiv C_g[t\sigma_g]$), $\sigma = \text{mgu}(u, l)$ and $s \equiv C[u]$. Then we have $v_g \equiv C_g[C[r]\sigma_g] \leftarrow_{\mathcal{R}} C_g[C[l]\sigma_g] \equiv C_g[C\sigma[l\sigma_g]] \equiv C_g[C\sigma[u\sigma_g]] \equiv C_g[C[u]\sigma_g] \equiv C_g[s\sigma_g] \leftrightarrow_{\{s \doteq t\}} C_g[t\sigma_g] \equiv$

w_g . □

4. Simplification by Conjectures

Simplification by (yet unproved) conjectures is one of basic refinements used in many extended rewriting induction systems^{5)~7),9)}. In this section, we introduce a rewriting induction system with a general simplification-by-conjectures rule and an abstract principle that is used to prove the soundness of this new rewriting induction system.

Figure 3 describes our new inference system cRI which is obtained by adding an inference rule *Simplify-C* to RI . In *Simplify-C*, an equation of E is reduced using other equations of E if an indicated condition is satisfied.

Definition 6 If $\langle E', H' \rangle$ is obtained from $\langle E, H \rangle$ by applying one of the inference rules from **Fig. 3**, we write $\langle E, H \rangle \rightsquigarrow_{\text{cRI}} \langle E', H' \rangle$. The reflexive transitive closure of $\rightsquigarrow_{\text{cRI}}$ is denoted by $\overset{*}{\rightsquigarrow}_{\text{cRI}}$. We sometimes write $\rightsquigarrow_{\text{cRI}}^s$, $\rightsquigarrow_{\text{cRI}}^{\text{sc}}$, $\rightsquigarrow_{\text{cRI}}^d$, or $\rightsquigarrow_{\text{cRI}}^e$ to indicate which inference rule is used.

Koike and Toyama¹⁶⁾ extracted the following abstract principle from the proof of the soundness of rewriting induction¹⁸⁾.

Proposition 7 (Koike and Toyama¹⁶⁾)

Let $\rightarrow_1, \rightarrow_2$ be binary relations and $>$ a well-founded partial order on a set A . Suppose that (i) $\rightarrow_{1 \cup 2} \subseteq >$ and (ii) if $a \rightarrow_2 b$ then there exists c such that (ii-a) $a \rightarrow_1 c$ and (ii-b) $c \downarrow_{1 \cup 2} b$. Then, $\overset{*}{\rightarrow}_1 = \overset{*}{\rightarrow}_{1 \cup 2}$.

$$\begin{array}{l}
\text{Expand} \\
\frac{\langle E \uplus \{s \doteq t\}, H \rangle}{\langle E \cup \text{Expd}_u(s, t), H \cup \{s \rightarrow t\} \rangle} \quad u \in \mathcal{B}(s), s > t \\
\text{Simplify} \\
\frac{\langle E \uplus \{s \doteq t\}, H \rangle}{\langle E \cup \{s' \doteq t\}, H \rangle} \quad s \rightarrow_{\mathcal{R} \cup H} s' \\
\text{Simplify-C} \\
\frac{\langle E \uplus \{s \doteq t\}, H \rangle}{\langle E \cup \{s' \doteq t\}, H \rangle} \quad s \leftrightarrow_E s', (s \geq s') \vee (t \geq s') \\
\text{Delete} \\
\frac{\langle E \uplus \{s \doteq s\}, H \rangle}{\langle E, H \rangle}
\end{array}$$

Fig. 3 Inference rules of cRI

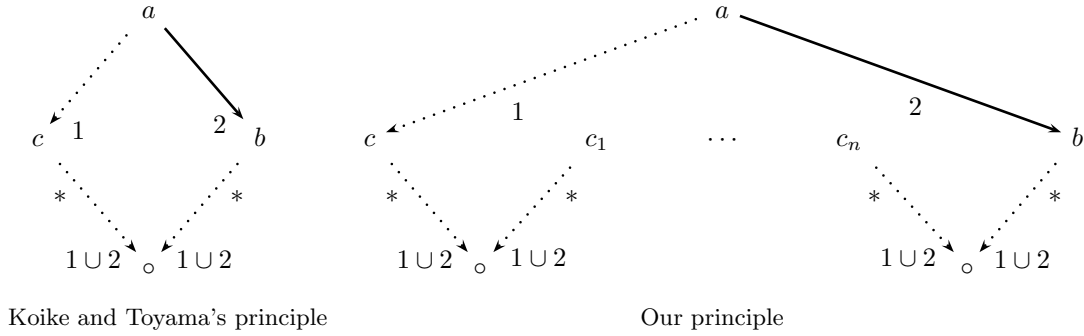


Fig. 4 Difference of principles

Based on this principle, the soundness of the original rewriting induction system RI can be proved¹). The principle, however, is not general enough to show the soundness of cRI.

We now give a new abstract principle that allows us to prove the soundness of cRI. It is easy to see that our new abstract principle is an extension of Koike and Toyama's principle (Fig.4).

Lemma 8 *Let $\rightarrow_1, \rightarrow_2$ be binary relations and $>$ a well-founded partial order on a set A . Suppose that (i) $\rightarrow_{1 \cup 2} \subseteq >$ and (ii) if $a \rightarrow_2 b$ then there exist c, c_1, \dots, c_n ($n \geq 0$) such that (ii-a) $a \rightarrow_1 c$, (ii-b) for each $1 \leq i \leq n$, either $c_i \leq c$ or $c_i \leq b$, and (ii-c) $c \downarrow_{1 \cup 2} c_1, c_1 \downarrow_{1 \cup 2} c_2, \dots, c_{n-1} \downarrow_{1 \cup 2} c_n$, and $c_n \downarrow_{1 \cup 2} b$. Then, $\overset{*}{\leftrightarrow}_1 = \overset{*}{\leftrightarrow}_{1 \cup 2}$.*

Proof (\subseteq) is obvious. To show (\supseteq), we show by noetherian induction on $>$ that

$$\forall y \in A. (x \overset{*}{\rightarrow}_{1 \cup 2} y \Rightarrow x \overset{*}{\leftrightarrow}_1 y)$$

for any $x \in A$. (Base Step) We have $x = y$ and

thus $x \overset{*}{\leftrightarrow}_1 y$. (Induction Step) Let $x \overset{*}{\rightarrow}_{1 \cup 2} y$. The case $x = y$ is obvious. Let $x \rightarrow_{1 \cup 2} z \overset{*}{\rightarrow}_{1 \cup 2} y$. Then $x > z$ follows by condition (i), and hence $z \overset{*}{\leftrightarrow}_1 y$ by the induction hypothesis. If $x \rightarrow_1 z$ then we have $x \rightarrow_1 z \overset{*}{\leftrightarrow}_1 y$, and thus $x \overset{*}{\leftrightarrow}_1 y$. Otherwise, $x \rightarrow_2 z$. By condition (ii), there exist c, c_1, \dots, c_n such that (a) $x \rightarrow_1 c$, (b) for each $1 \leq i \leq n$, either $c_i \leq c$ or $c_i \leq z$ (c) $c \overset{*}{\rightarrow}_{1 \cup 2} c_1, c_1 \overset{*}{\rightarrow}_{1 \cup 2} c_2, \dots, c_{n-1} \overset{*}{\rightarrow}_{1 \cup 2} c_n$, and $c_n \overset{*}{\rightarrow}_{1 \cup 2} z$. By condition (i), $x > c$ follows from (a). Thus, together with $x > z$, it follows from (b) that $c_i < x$ for all $1 \leq i \leq n$. Hence one can apply the induction hypothesis to z, c, c_1, \dots, c_n and obtain from (c) that $c \overset{*}{\leftrightarrow}_1 c_1, c_1 \overset{*}{\leftrightarrow}_1 c_2, \dots, c_{n-1} \overset{*}{\leftrightarrow}_1 c_n, c_n \overset{*}{\leftrightarrow}_1 z$. Thus, $x \rightarrow_1 c \overset{*}{\leftrightarrow}_1 z \overset{*}{\leftrightarrow}_1 y$. \square

In the remaining lemmas of this section, we assume that \mathcal{R} is a quasi-reducible TRS and $>$ is a reduction order satisfying $\mathcal{R} \subseteq >$.

Lemma 9 *If $\langle E_n, H_n \rangle \rightsquigarrow_{\text{cRI}} \langle E_{n+1}, H_{n+1} \rangle$, then $\overset{*}{\leftrightarrow}_{\mathcal{R} \cup E_n \cup H_n} = \overset{*}{\leftrightarrow}_{\mathcal{R} \cup E_{n+1} \cup H_{n+1}}$ on $\mathbb{T}(\mathcal{F})$.*

Proof We distinguish cases according to the inference rule applied in the derivation step $\langle E_n, H_n \rangle \rightsquigarrow_{\text{CRI}} \langle E_{n+1}, H_{n+1} \rangle$. The cases $\langle E_n, H_n \rangle \rightsquigarrow_{\text{CRI}}^{s,sc,d} \langle E_{n+1}, H_{n+1} \rangle$ easily follow. Consider the case $\langle E_n, H_n \rangle \rightsquigarrow_{\text{CRI}}^e \langle E_{n+1}, H_{n+1} \rangle$. Then one can let $E_n = E \uplus \{s = t\}$, $E_{n+1} = E \cup \text{Expd}_u(s, t)$, $H_{n+1} = H_n \cup \{s \rightarrow t\}$, and $u \in \mathcal{B}(s)$. The inclusion $\overset{*}{\leftarrow} \mathcal{R} \cup E_n \cup H_n \subseteq \overset{*}{\leftarrow} \mathcal{R} \cup E_{n+1} \cup H_{n+1}$ is obvious. To show $\overset{*}{\leftarrow} \mathcal{R} \cup E_n \cup H_n \supseteq \overset{*}{\leftarrow} \mathcal{R} \cup E_{n+1} \cup H_{n+1}$, it suffices to show $u_g \leftrightarrow_{\text{Expd}_u(s,t)} v_g$ implies $u_g \overset{*}{\leftarrow} \mathcal{R} \cup E_n \cup H_n v_g$ for any ground terms u_g, v_g . This follows from **Lemma 5** (2), since $s = t \in E_n$. \square

Lemma 10 Let $\langle E_n, H_n \rangle \rightsquigarrow_{\text{CRI}}^* \langle \emptyset, H^\# \rangle$. For any $s_g, t_g \in \mathbb{T}(\mathcal{F})$ such that $s_g \leftrightarrow_{E_n} t_g$, there exist $u_1, \dots, u_k \in \mathbb{T}(\mathcal{F})$ satisfying (1) for any $1 \leq i \leq k$ either $u_i \leq s_g$ or $u_i \leq t_g$ and (2) $s_g \downarrow_{\mathcal{R} \cup H^\#} u_1, u_1 \downarrow_{\mathcal{R} \cup H^\#} u_2, \dots, u_{k-1} \downarrow_{\mathcal{R} \cup H^\#} u_k, u_k \downarrow_{\mathcal{R} \cup H^\#} t_g$

Proof By induction on the length k of the derivation $\langle E_n, H_n \rangle \rightsquigarrow_{\text{CRI}}^* \langle \emptyset, H^\# \rangle$. The case $k = 0$ is obvious. Suppose $k > 0$. Then one can let $\langle E_n, H_n \rangle \rightsquigarrow_{\text{CRI}} \langle E_{n+1}, H_{n+1} \rangle \rightsquigarrow_{\text{CRI}}^* \langle \emptyset, H^\# \rangle$. We distinguish cases according to the inference rule applied in the derivation step $\langle E_n, H_n \rangle \rightsquigarrow_{\text{CRI}} \langle E_{n+1}, H_{n+1} \rangle$. The cases $\langle E_n, H_n \rangle \rightsquigarrow_{\text{CRI}}^{d,e} \langle E_{n+1}, H_{n+1} \rangle$ are shown easily.

- Case $\langle E_n, H_n \rangle \rightsquigarrow_{\text{CRI}}^s \langle E_{n+1}, H_{n+1} \rangle$. Then one can let $E_n = E \uplus \{s = t\}$, $E_{n+1} = E \cup \{s' = t\}$, $H_n = H_{n+1}$, $s \rightarrow_{\mathcal{R} \cup H_n} s'$. If $s_g \leftrightarrow_E t_g$, the claim follows immediately from the induction hypothesis. Let $s_g \leftrightarrow_{\{s=t\}} t_g$. Then we have $s_g \equiv C_g[s\sigma_g]$, $t_g \equiv C_g[t\sigma_g]$ (or $s_g \equiv C_g[t\sigma_g]$, $t_g \equiv C_g[s\sigma_g]$). Since $s'_g \equiv C_g[s'\sigma_g] \leftrightarrow_{E_{n+1}} t_g$, by the induction hypothesis, there exist u_1, \dots, u_k such that (1) for all $1 \leq i \leq k$, either $u_i \leq s'_g$ or $u_i \leq t_g$ holds and (2) $s'_g \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# u_1, u_1 \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# u_2, \dots, u_k \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# t_g$.

By $s \rightarrow_{\mathcal{R} \cup H_n} s'$, $s_g \equiv C_g[s\sigma_g] \rightarrow_{\mathcal{R} \cup H_n} C_g[s'\sigma_g] \equiv s'_g$ and thus $s_g > s'_g$. Hence, from (1), for all $1 \leq i \leq k$, we have either $u_i \leq s_g$ or $u_i \leq t_g$. By $s_g \rightarrow_{\mathcal{R} \cup H_n} s'_g$ and $H_n \subseteq H^\#$, we have $s_g \rightarrow_{\mathcal{R} \cup H^\#} s'_g$. Thus, it follows from (2) that $s_g \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# u_1, u_1 \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# u_2, \dots, u_k \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# t_g$.

- Case $\langle E_n, H_n \rangle \rightsquigarrow_{\text{CRI}}^{sc} \langle E_{n+1}, H_{n+1} \rangle$. Then one can let $E_n = E \uplus \{s = t\}$, $E_{n+1} = E \cup \{s' = t\}$, $H_n = H_{n+1}$, $s \leftrightarrow_E s'$, and $s' \leq s$ or $s' \leq t$. The case $s_g \leftrightarrow_E t_g$ follows immediately from the induction hy-

pothesis. Let $s_g \leftrightarrow_{\{s=t\}} t_g$. Then we have $s_g \equiv C_g[s\sigma_g]$, $t_g \equiv C_g[t\sigma_g]$ (or $s_g \equiv C_g[t\sigma_g]$, $t_g \equiv C_g[s\sigma_g]$). Because we have $s'_g \equiv C_g[s'\sigma_g] \leftrightarrow_{E_{n+1}} t_g$, by the induction hypothesis, there exist $u_1, \dots, u_k \in \mathbb{T}(\mathcal{F})$ such that (1) for any $1 \leq i \leq k$, either $u_i \leq s'_g$ or $u_i \leq t_g$ holds and (2) $s'_g \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# u_1, u_1 \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# u_2, \dots, u_k \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# t_g$. Further, since $s_g \equiv C_g[s\sigma_g] \leftrightarrow_{E_{n+1}} C_g[s'\sigma_g] \equiv s'_g$, by the induction hypothesis, there exist $v_1, \dots, v_l \in \mathbb{T}(\mathcal{F})$ such that (1') for any $1 \leq i \leq l$, either $v_i \leq s_g$ or $v_i \leq s'_g$ holds and (2') $s_g \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# v_1, v_1 \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# v_2, \dots, v_l \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# s'_g$. Since $s' \leq s$ implies $s'_g \leq s_g$ and $s' \leq t$ implies $s'_g \leq t_g$, we have (1'') for $1 \leq j \leq l$, either $v_j \leq s_g$ or $v_j \leq t_g$, and for $1 \leq i \leq k$, either $u_i \leq s_g$ or $u_i \leq t_g$. Combining (2) and (2'), we have (2'') $s_g \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# v_1, v_1 \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# v_2, \dots, v_l \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# s'_g, s'_g \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# u_1, u_1 \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# u_2, \dots, u_k \overset{*}{\leftarrow} \mathcal{R} \cup H^\# \circ \overset{*}{\leftarrow} \mathcal{R} \cup H^\# t_g$. Now, it remains to show either $s'_g \leq s_g$ or $s'_g \leq t_g$ holds—this follows because we have either $s' \leq s$ or $s' \leq t$. \square

Lemma 11 Let $\langle E_n, H_n \rangle \rightsquigarrow_{\text{CRI}}^* \langle \emptyset, H^\# \rangle$. For any $s_g, t_g \in \mathbb{T}(\mathcal{F})$ such that $s_g \rightarrow_{H^\#} t_g$, there exist $w_g, u_1, \dots, u_k \in \mathbb{T}(\mathcal{F})$ satisfying (1) $s_g \rightarrow_{\mathcal{R}} w_g$, (2) for any i , either $u_i \leq w_g$ or $u_i \leq t_g$, and (3) $w_g \downarrow_{\mathcal{R} \cup H^\#} u_1, u_1 \downarrow_{\mathcal{R} \cup H^\#} u_2, \dots, u_{k-1} \downarrow_{\mathcal{R} \cup H^\#} u_k, u_k \downarrow_{\mathcal{R} \cup H^\#} t_g$.

Proof Suppose $s \rightarrow t \in H^\#$ and $s_g \rightarrow_{\{s \rightarrow t\}} t_g$. Let $s_g \equiv C_g[s\sigma_g]$ and $t_g \equiv C_g[t\sigma_g]$.

We first claim that one may assume w.l.o.g. that $\sigma_g(x) \in \text{NF}(\rightarrow_{\mathcal{R}})$ for any $x \in V(s)$. By $\text{SN}(\rightarrow_{\mathcal{R}})$, there exists a substitution $\hat{\sigma}_g$ such that for any $x \in V(s)$, $\sigma_g(x) \overset{*}{\leftarrow} \mathcal{R} \hat{\sigma}_g(x) \in \text{NF}(\rightarrow_{\mathcal{R}})$. Let $\hat{s}_g \equiv C_g[s\hat{\sigma}_g]$ and $\hat{t}_g \equiv C_g[t\hat{\sigma}_g]$, and suppose that there exist $w_g, u_1, \dots, u_k \in \mathbb{T}(\mathcal{F})$ such that (1) $\hat{s}_g \rightarrow_{\mathcal{R}} w_g$, (2) for any i , either $u_i \leq w_g$ or $u_i \leq t_g$ holds, and (3) $w_g \downarrow_{\mathcal{R} \cup H^\#} u_1, u_1 \downarrow_{\mathcal{R} \cup H^\#} u_2, \dots, u_{k-1} \downarrow_{\mathcal{R} \cup H^\#} u_k, u_k \downarrow_{\mathcal{R} \cup H^\#} \hat{t}_g$. Then by $s_g \equiv C_g[s\sigma_g] \overset{*}{\leftarrow} \mathcal{R} C_g[s\hat{\sigma}_g] \equiv \hat{s}_g$ and $t_g \equiv C_g[t\sigma_g] \overset{*}{\leftarrow} \mathcal{R} C_g[t\hat{\sigma}_g] \equiv \hat{t}_g$, we have $s_g \geq \hat{s}_g$ and $t_g \geq \hat{t}_g$. By $s_g \overset{*}{\leftarrow} \mathcal{R} \hat{s}_g \rightarrow_{\mathcal{R}} w_g$ one can take w'_g such that $s_g \rightarrow_{\mathcal{R}} w'_g \overset{*}{\leftarrow} \mathcal{R} w_g$. Then it follows that (1) $s_g \rightarrow_{\mathcal{R}} w'_g$, (2) for any i , either $u_i \leq w_g \leq w'_g$ (since $w'_g \overset{*}{\leftarrow} \mathcal{R} w_g$) or $u_i \leq \hat{t}_g \leq t_g$, and (3) $w'_g \overset{*}{\leftarrow} \mathcal{R} \cup H^\# w_g \overset{*}{\leftarrow} \mathcal{R} \cup H^\# u_1, u_1 \downarrow_{\mathcal{R} \cup H^\#} u_2, \dots, u_{k-1} \downarrow_{\mathcal{R} \cup H^\#} u_k,$

$u_k \xrightarrow{*} \mathcal{R} \cup H^\# \circ \xleftarrow{*} \mathcal{R} \cup H^\# \hat{t}_g \xleftarrow{*} \mathcal{R} \cup H^\# t_g$. Thus the claim follows.

Thus let us assume w.l.o.g. that for any $x \in V(s)$, $\sigma_g(x) \in \text{NF}(\rightarrow_{\mathcal{R}})$. Then by the quasi-reducibility of \mathcal{R} , σ_g is a constructor substitution. Since the only inference rule that adds equations to $H^\#$ is *Expand*, we have a derivation of the form $\langle E_0, \emptyset \rangle \xrightarrow{*}_{\text{cRI}} \langle E_n, H_n \rangle \xrightarrow{\sim}_{\text{cRI}} \langle E_{n+1}, H_{n+1} \rangle \xrightarrow{*}_{\text{cRI}} \langle \emptyset, H^\# \rangle$ such that $H_{n+1} = H_n \cup \{s \rightarrow t\}$, $E_n = E \uplus \{s \doteq t\}$, $E_{n+1} = E \cup \text{Expd}_u(s, t)$, $u \in \mathcal{B}(s)$, and $s > t$. By **Lemma 5** (1), we have $s\sigma_g \rightarrow_{\mathcal{R}} \circ \leftrightarrow_{\text{Expd}_u(s, t)} t\sigma_g$. Thus, $s_g \equiv C_g[s\sigma_g] \rightarrow_{\mathcal{R}} \circ \leftrightarrow_{E_{n+1}} C_g[t\sigma_g] \equiv t_g$. Hence the statement follows from **Lemma 10**. \square

Theorem 12 *Let \mathcal{R} be a quasi-reducible TRS, E a set of equations, and $>$ a reduction order such that $\mathcal{R} \subseteq >$. If $\langle E, \emptyset \rangle \xrightarrow{*}_{\text{cRI}} \langle \emptyset, H^\# \rangle$ for some set $H^\#$ of rewrite rules, then the equations of E are inductive theorems of \mathcal{R} .*

Proof By applying **Lemma 9** repeatedly, we know $\xrightarrow{*}_{E \cup \mathcal{R}} = \xrightarrow{*}_{\mathcal{R} \cup H^\#}$ holds on $\text{T}(\mathcal{F})$. Thus it remains to show $\xrightarrow{*}_{\mathcal{R} \cup H^\#} = \xrightarrow{*}_{\mathcal{R}}$ on $\text{T}(\mathcal{F})$. For this, we apply **Lemma 8** with $\rightarrow_1 := \rightarrow_{\mathcal{R}}$, $\rightarrow_2 := \rightarrow_{H^\#}$, and $A := \text{T}(\mathcal{F})$. By the facts that $\mathcal{R} \cup H^\# \subseteq >$ and $>$ is a reduction order, condition (i) of the lemma is satisfied. Condition (ii) follows from **Lemma 11**. Therefore, $\xrightarrow{*}_{\mathcal{R}} = \xrightarrow{*}_{\mathcal{R} \cup H^\#}$. \square

5. Extension to ordered rewriting

The notion of ordered rewriting was introduced originally for the Knuth-Bendix completion algorithm to deal with non-orientable equations^{(3), (11)}. Rewriting induction systems in^{(5)~(7), (9)} are based on ordered rewriting. In this section, we present a variant oRI of the system cRI based on ordered rewriting and prove its soundness using the same abstract principle.

We first present some preliminary definitions related to ordered rewriting. Let $>$ be a reduction order. For a set E of equations, its ordered rewrite relation \rightarrow_E is defined as: $s \rightarrow_E t$ iff there exist an equation $l \doteq r \in E$, a context C and a substitution θ such that $s \equiv C[l\theta]$, $t \equiv C[r\theta]$, and $l\theta > r\theta$. Clearly, \rightarrow_E is well-founded. We write $s \vdash_E t$ if there exists $l \doteq r \in E$, a context C , and a substitution θ such that $s \equiv C[l\theta]$, and $t \equiv C[r\theta]$. Note that in general \leftrightarrow_E (the symmetric closure of \rightarrow_E) and \vdash_E may be different. Moreover, if $>$ is ground-total, $\vdash_E = \leftrightarrow_E$ on $\text{T}(\mathcal{F})$.

Let \mathcal{D}, \mathcal{C} be disjoint sets of function symbols, \mathcal{E} a set of equations over $\text{T}(\mathcal{D} \cup \mathcal{C}, V)$. Then

the triple $\langle \mathcal{D}, \mathcal{C}, \mathcal{E} \rangle$ is called an *equational system* (ES). If \mathcal{D}, \mathcal{C} are known or irrelevant, we identify $\langle \mathcal{D}, \mathcal{C}, \mathcal{E} \rangle$ with \mathcal{E} . For ESs, the notions such as defined symbols, constructor symbols, are adapted by regarding $\mathcal{D}_{\mathcal{R}}$ and $\mathcal{C}_{\mathcal{R}}$ as \mathcal{D} and \mathcal{C} , respectively. An ES \mathcal{E} is said to be *quasi-reducible* if all ground basic terms are reducible by $\rightarrow_{\mathcal{E}}$, i.e. for any ground basic term s_g there exist $l \doteq r \in \mathcal{E}$ and σ_g such that $l\sigma_g \equiv s_g$ and $l\sigma_g > r\sigma_g$. An *inductive theorem* of an ES \mathcal{E} is an equation that is valid on $\text{T}(\mathcal{F})$, i.e. $s \doteq t$ is an inductive theorem iff $s\sigma_g \vdash_{\mathcal{E}}^* t\sigma_g$ holds for any ground instance $s\sigma_g \doteq t\sigma_g$.

Figure 5 describes our inference system oRI of rewriting induction based on ordered rewriting. The *Simplify* rule and the *Simplify-C* rule of cRI are integrated into the *O-Simplify* rule of the new inference system. The operator OExpd in the figure is defined as:

$$\begin{aligned} \text{OExpd}_u(s, t) = \{ & C[r]\sigma \doteq t\sigma \mid s \equiv C[u], \\ & \sigma = \text{mgu}(u, l), l \doteq r \in \mathcal{E}, \\ & l : \text{basic}, r\sigma \not\geq l\sigma \} \end{aligned}$$

Note that by the condition $r\sigma \not\geq l\sigma$ and the fact that $>$ is a reduction order, it follows that $\text{OExpd}_u(s, t) = \text{Expd}_u(s, t)$ when $l > r$ for any $(l, r) \in \mathcal{E}$.

Definition 13 *If $\langle E', H' \rangle$ is obtained from $\langle E, H \rangle$ by applying one of the inference rules from **Fig. 5**, we write $\langle E, H \rangle \xrightarrow{\sim}_{\text{oRI}} \langle E', H' \rangle$. The reflexive transitive closure of $\xrightarrow{\sim}_{\text{oRI}}$ is denoted by $\xrightarrow{*}_{\text{oRI}}$. We sometimes write $\xrightarrow{\sim}_{\text{oRI}}^{\text{os}}$, $\xrightarrow{\sim}_{\text{oRI}}^{\text{oe}}$, or $\xrightarrow{\sim}_{\text{oRI}}^{\text{oc}}$ to indicate which inference rule is used.*

OExpd has two properties similar to Expd .

Lemma 14 *Let \mathcal{E} be a quasi-reducible ES and $u \in \mathcal{B}(s)$. Then (1) $s\sigma_g \rightarrow_{\mathcal{E}} \circ \vdash_{\text{OExpd}_u(s, t)}^* t\sigma_g$ for any ground constructor substitution σ_g and (2) $v_g \vdash_{\text{OExpd}_u(s, t)} w_g$ implies $v_g \vdash_{\mathcal{E} \cup \{s \doteq t\}}^* w_g$ for any ground terms v_g, w_g .*

Proof (1) Since u is basic and σ_g is a ground constructor substitution, $u\sigma_g$ is a basic ground term. Thus, by the quasi-reducibility of \mathcal{E} , there exists $l \doteq r \in \mathcal{E}$ such that $u\sigma_g$ is an instance of l and $u\sigma_g$ is greater than the corresponding instance of r . Because $u\sigma_g$ is basic, l is basic. W.l.o.g. we may assume $V(l) \cap V(s) = \emptyset$ and thus by extending σ_g one can let $u\sigma_g \equiv l\sigma_g$ such that $l\sigma_g > r\sigma_g$. Then σ_g is a unifier of u and l and thus we have $\sigma_g = \theta_g \circ \sigma$ for some substitution θ_g , where $\sigma = \text{mgu}(u, l)$. If we have $r\sigma \geq l\sigma$, then $r\sigma_g \geq l\sigma_g$, contradicting $l\sigma_g > r\sigma_g$. Thus we may assume $r\sigma \not\geq l\sigma$. Then by letting $s \equiv C[u]$, we have

O-Expand

$$\frac{\langle E \uplus \{s \doteq t\}, H \rangle}{\langle E \cup \text{OExpd}_u(s, t), H \cup \{s \doteq t\} \rangle} \quad u \in \mathcal{B}(s)$$

O-Simplify

$$\frac{\langle E \uplus \{s \doteq t\}, H \rangle}{\langle E \cup \{s' \doteq t\}, H \rangle} \quad s \vdash_{\mathcal{E} \cup H \cup E} s', (s \geq s') \vee (t \geq s')$$

O-Delete

$$\frac{\langle E \uplus \{s \doteq s\}, H \rangle}{\langle E, H \rangle}$$

Fig. 5 Inference rules of oRI

$s\sigma_g \equiv C[u]\sigma_g \equiv C\sigma_g[u\sigma\theta_g] \equiv C\sigma_g[l\sigma_g] \rightarrow_{\mathcal{R}} C\sigma_g[r\sigma_g] \equiv C[r]\sigma\theta_g \vdash_{\text{OExpd}_u(s, t)} t\sigma\theta_g \equiv t\sigma_g$.
 (2) Similar to the proof of **Lemma 5** (2). \square

The soundness of oRI is proved in a way almost similar to the proof of soundness of cRI. Below, proofs are explicitly presented only when a different situation is involved. In the remaining lemmas in this section, we assume that \mathcal{E} is a quasi-reducible ES and $>$ is a reduction order that is ground-total.

Lemma 15 *If $\langle E_n, H_n \rangle \rightsquigarrow_{\text{oRI}} \langle E_{n+1}, H_{n+1} \rangle$ then $\vdash_{\mathcal{R} \cup E_n \cup H_n}^* = \vdash_{\mathcal{R} \cup E_{n+1} \cup H_{n+1}}^*$ on $\mathbb{T}(\mathcal{F})$.*

Lemma 16 *Let $\langle E_n, H_n \rangle \rightsquigarrow_{\text{oRI}} \langle \emptyset, H^\# \rangle$. For any $s_g, t_g \in \mathbb{T}(\mathcal{F})$ such that $s_g \vdash_{E_n} t_g$, there exist $u_1, \dots, u_k \in \mathbb{T}(\mathcal{F})$ satisfying (1) for any $1 \leq i \leq k$ either $u_i \leq s_g$ or $u_i \leq t_g$ and (2) $s_g \downarrow_{\mathcal{E} \cup H^\#} u_1, u_1 \downarrow_{\mathcal{E} \cup H^\#} u_2, \dots, u_{k-1} \downarrow_{\mathcal{E} \cup H^\#} u_k, u_k \downarrow_{\mathcal{E} \cup H^\#} t_g$.*

Proof By induction on the length k of the derivation $\langle E_n, H_n \rangle \rightsquigarrow_{\text{oRI}} \langle \emptyset, H^\# \rangle$. The case $k = 0$ is obvious. Suppose $k > 0$. Then one can let $\langle E_n, H_n \rangle \rightsquigarrow_{\text{oRI}} \langle E_{n+1}, H_{n+1} \rangle \rightsquigarrow_{\text{oRI}} \langle \emptyset, H^\# \rangle$. We distinguish cases according to the inference rule applied in the derivation step $\langle E_n, H_n \rangle \rightsquigarrow_{\text{oRI}} \langle E_{n+1}, H_{n+1} \rangle$. We only show the case $\langle E_n, H_n \rangle \rightsquigarrow_{\text{oRI}}^{\text{OS}} \langle E_{n+1}, H_{n+1} \rangle$ and $s \vdash_{\mathcal{E} \cup H} s'$. Other cases are shown in the ways similar to **Lemma 10**. Suppose $E_n = E \uplus \{s \doteq t\}$, $E_{n+1} = E \cup \{s' \doteq t\}$, $H_n = H_{n+1}$, and $s \geq s'$ or $t \geq s'$. The case $s_g \vdash_E t_g$ follows immediately from the induction hypothesis. Let $s_g \vdash_{\{s \doteq t\}} t_g$. W.l.o.g. let $s_g \equiv C_g[s\sigma_g]$, $t_g \equiv C_g[t\sigma_g]$. Since $s'_g \equiv C_g[s'\sigma_g] \vdash_{E_{n+1}} t_g$, by the induction hypothesis, there exist u_1, \dots, u_k such that (1) for all $1 \leq i \leq k$, either $u_i \leq s'_g$ or $u_i \leq t_g$ and (2) $s'_g \downarrow_{\mathcal{E} \cup H^\#} u_1, \dots, u_k \downarrow_{\mathcal{E} \cup H^\#} t_g$.

By $s \vdash_{\mathcal{E} \cup H_n} s'$ and the ground-totality of $>$, we have $s_g \leftrightarrow_{\mathcal{E} \cup H_n} s'_g$. The case $s_g \rightarrow_{\mathcal{E} \cup H^\#} s'_g$ follows easily. Otherwise, $s'_g \rightarrow_{\mathcal{E} \cup H^\#} s_g$ and thus $t \geq s'$. Let $u'_1 := s'_g, u'_{i+1} := u_i$ for $i \leq k$ and it follows that (1) $u'_i \leq t_g$ for any $1 \leq i \leq$

$k + 1$ and (2) $s_g \xrightarrow{*}_{\mathcal{E} \cup H^\#} s_g \xleftarrow{*}_{\mathcal{E} \cup H^\#} s'_g \equiv u'_1, u'_1 \downarrow_{\mathcal{E} \cup H^\#} u'_2, \dots, u'_{k+1} \downarrow_{\mathcal{E} \cup H^\#} t_g$. \square

Lemma 17 *Let $\langle E_n, H_n \rangle \rightsquigarrow_{\text{oRI}} \langle \emptyset, H^\# \rangle$. For any $s_g, t_g \in \mathbb{T}(\mathcal{F})$ such that $s_g \rightarrow_{H^\#} t_g$, there exist $w_g, u_1, \dots, u_k \in \mathbb{T}(\mathcal{F})$ satisfying (1) $s_g \rightarrow_{\mathcal{E}} w_g$, (2) for any i , either $u_i \leq w_g$ or $u_i \leq t_g$, and (3) $w_g \downarrow_{\mathcal{E} \cup H^\#} u_1, u_1 \downarrow_{\mathcal{E} \cup H^\#} u_2, \dots, u_{k-1} \downarrow_{\mathcal{E} \cup H^\#} u_k, u_k \downarrow_{\mathcal{E} \cup H^\#} t_g$.*

Theorem 18 *Let \mathcal{E} be a quasi-reducible ES, E a set of equations, and $>$ a reduction order that is ground-total. If $\langle E, \emptyset \rangle \rightsquigarrow_{\text{oRI}} \langle \emptyset, H^\# \rangle$ for some set $H^\#$ of rewrite rules, then the equations of E are inductive theorems of \mathcal{E} .*

Proof By applying **Lemma 15** repeatedly, we know $\vdash_{E \cup \mathcal{E}}^* = \vdash_{\mathcal{E} \cup H^\#}^*$ holds on $\mathbb{T}(\mathcal{F})$. Thus it remains to show $\vdash_{\mathcal{E} \cup H^\#}^* = \vdash_{\mathcal{E}}^*$ on $\mathbb{T}(\mathcal{F})$. By the ground-totality of $>$, this is equivalent to showing $\leftrightarrow_{\mathcal{E} \cup H^\#}^* = \leftrightarrow_{\mathcal{E}}^*$ on $\mathbb{T}(\mathcal{F})$. This follows from **Lemma 8** with $\rightarrow_1 := \rightarrow_{\mathcal{E}}, \rightarrow_2 := \rightarrow_{H^\#}$, and $A := \mathbb{T}(\mathcal{F})$ using **Lemma 17**. \square

6. Comparison

In this section, we compare our system and some major systems from the literature.

Firstly, in the original rewriting induction system I by Reddy¹⁸, a slightly different expand rule is used:

$$\text{Expand} \quad \frac{\langle E \uplus \{s \doteq t\}, H \rangle}{\langle E \cup E', H \cup \{s \rightarrow t\} \rangle} \quad s > t$$

where $E' = \bigcup_{i \in I} \{b \doteq t\sigma_i \mid s\sigma_i \rightarrow_{\mathcal{R}} b\}$ and $\{\sigma_i \mid i \in I\}$ is a $>$ -cover set of substitutions for s , that is, for any ground term s_g , there exists $i \in I$ such that $s\sigma_i \leftrightarrow_{\mathcal{R}} s_g$ and $s\sigma_i \leq s_g$. Many systems employ essentially the same but differently formulated expand rules—the differences are out of the scope of this paper and below we omit these differences. Our version based on the quasi-reducibility of \mathcal{R} and the notion of basic subterms is originally used in 19). Other

methods do not assume the quasi-reducibility; instead, some properties of the data structure on which the TRS \mathcal{R} acts on are assumed or induced from \mathcal{R} .

Dershowitz and Reddy⁹⁾ incorporate ordered rewriting extension into rewriting induction; their system also includes simplification by conjectures. In **Fig.6**, we present their system in our formulation. The system is based on a ground-total simplification order. It is readily seen that the rule *Simplify* is a part of *O-Simplify*. Each application of *Subsume* can be simulated by an application of *O-Simplify* and a successive application of *O-Delete*. The rule *Hypothesis* is not derived in oRI but it is easily seen that this rule can be added without losing soundness. Thus, Dershowitz and Reddy's system is essentially subsumed by oRI.

In **Fig.7**, we present a part of the inference system I in 6). The full part of inference system I is used as a basis for the inductive theorem prover SPIKE. Here $s \mid t$ means neither $s > t$, $t < s$, nor $t \equiv s$. The presented inference system is obtained from the original system by restricting to first-order term rewriting and proof of equations. A failure detection rule is also removed. The *Generate* rule corresponds to the *O-Expand* rule. Since $>$ is a reduction order, $s/u > s'/u$ in *Simplify*₁₋₄ is more restrictive than $s > s'$. Then it is readily seen that *Simplify*₁₋₄ are part of the *O-Simplify* rule. Thus the equation-proving part of first-order term rewriting fragment of the inference system I is subsumed by our system provided that the underlying order is ground-total.

In 8), 20), general frameworks for proving induction theorems are proposed. Rewriting induction⁸⁾ (Procedure 4) involves the following simplification rule:

$$\frac{\text{Simplify} \quad \langle E \cup \{s \doteq t\}, H \rangle}{\langle E \cup \{s' \doteq t\}, H \rangle} \text{cond}$$

where *cond* equals $s\sigma_g \vdash^*_{\mathcal{E} \cup E \cup \{s'=t\} \cup H} t\sigma_g$ for all ground substitutions σ_g . Here, $\vdash^*_{\mathcal{S}} \leq_e \{u_g, v_g\}$ is the equivalence closure of the relation $\{\langle s'_g, t'_g \rangle \mid \exists p. (s'_g \vdash^*_S t'_g \wedge \{s'_g/p, t'_g/p\} \leq_e \{u_g, v_g\})\}$ and \leq_e is a fixed reduction order over equations. The system A in 20) also includes a more general simplification rule using the notion of contextual cover sets (CCSs). These simplification rules are not simulated by our system and vice versa. Both rules request the

derived equation to be used as smaller or equal instantiations, but our system does not necessarily require such a restriction, viz. when $s < s' = t$ in *O-Simplify* we have $\{s', t\} \not\leq_e \{s, t\}$ by orderings on equations such as the multiset extension and the max-extension^{8),20)}.

We end this section with an example.

Example 19 *Let us consider the following equations for the addition and multiplication of natural numbers.*

$$\mathcal{E} \left\{ \begin{array}{l} 0 + y \quad \doteq \quad y \\ s(x) + y \quad \doteq \quad s(x + y) \\ 0 \times y \quad \doteq \quad 0 \\ s(x) \times y \quad \doteq \quad (x \times y) + y \end{array} \right.$$

Let us prove the following set of conjectures using the lexicographic path order²⁾ based on a precedence $\times > + > s > 0$.

$$E \left\{ \begin{array}{l} (1) \quad x + y \quad \doteq \quad y + x \\ (2) \quad (x + y) + z \quad \doteq \quad x + (y + z) \\ (3) \quad x \times 0 \quad \doteq \quad 0 \\ (4) \quad x \times s(y) \quad \doteq \quad (x \times y) + x \\ (5) \quad (x + y) \times z \quad \doteq \quad (x \times z) + (y \times z) \\ (6) \quad x \times y \quad \doteq \quad y \times x \\ (7) \quad (x \times y) \times z \quad \doteq \quad (y \times z) \times x \\ (8) \quad s(x) \times x \quad \doteq \quad x \times s(x) \end{array} \right.$$

In the presented rewriting induction system based on ordered rewriting, equations (1)–(4) are proved without difficulties; using these equations equations (5) and (6) are proved. To prove equation (7) in oRI, the step $\langle E \uplus \{(x \times y) \times z \doteq (y \times z) \times x\}, H \cup \{(6)\} \rangle \rightsquigarrow_{\text{oRI}} \langle E \uplus \{(x \times y) \times z \doteq x \times (y \times z)\}, H \cup \{(6)\} \rangle$ is performed and successively the obtained equation is proved using equations (1),(2),(6); in Dershowitz and Reddy's system, in contrast, this step is impossible. To prove equation (8), in oRI, the step $\langle E \uplus \{s(x) \times x \doteq x \times s(x)\}, H \cup \{(6)\} \rangle \rightsquigarrow_{\text{oRI}} \langle E \uplus \{x \times s(x) \doteq x \times s(x)\}, H \cup \{(6)\} \rangle$ is performed and successively the proof succeeds; but in Bouhoula et. al.'s system I this step is impossible.

7. Conclusion

We have given an abstract principle for rewriting induction that extends the principle introduced in 16). Based on this principle, we have proved the soundness of a rewriting induction system cRI which extends the basic rewriting induction system RI by a general rule of simplification by conjectures. We have presented a variant oRI of the system cRI based on ordered rewriting and proved the soundness of it under the assumption that its base order is ground-total. We have compared our system

<i>Expand</i>	$\frac{\langle E \cup \{s \doteq t\}, H \rangle}{\langle E \cup E', H \cup \{s \doteq t\} \rangle} E' \text{ is a cover set of } s \doteq t$
<i>Simplify</i>	$\frac{\langle E \uplus \{s \doteq t\}, H \rangle}{\langle E \cup \{s' \doteq t\}, H \rangle} s \vdash_{\mathcal{E} \cup H \cup E} s', s > s'$
<i>Subsume</i>	$\frac{\langle E \cup \{C[s\theta] \doteq C[t\theta]\}, H \rangle}{\langle E, H \rangle} s \doteq t \in H$
<i>Hypothesis</i>	$\frac{\langle E, H \rangle}{\langle E \cup \{s \doteq t\}, H \rangle}$
<i>Delete</i>	$\frac{\langle E \cup \{s \doteq s\}, H \rangle}{\langle E, H \rangle}$

Fig. 6 Inference rules by Dershowitz and Reddy⁹⁾

<i>Generate</i>	$\frac{\langle E \cup \{s \doteq t\}, H \rangle}{\langle E \cup \bigcup_{\sigma} E_{\sigma}, H \cup \{s \doteq t\} \rangle}$	for any test-instance $s\sigma \doteq t\sigma$ there exists b such that either (a) $\neg(s < t)$, $s\sigma \vdash_{\mathcal{E}}^p b$, $s\sigma/p > b/p$, $E_{\sigma} = \{b \doteq t\sigma\}$, (b) $s \mid t$, $t\sigma \vdash_{\mathcal{E}}^p b$, $t\sigma/p > b/p$, $E_{\sigma} = \{s\sigma \doteq b\}$, or (c) $s\sigma \equiv t\sigma$ and $E_{\sigma} = \emptyset$
<i>Simplify₁</i>	$\frac{\langle E \cup \{s \doteq t\}, H \rangle}{\langle E \cup \{s' \doteq t\}, H \rangle} s \vdash_{\mathcal{E}}^p s', s/p > s'/p$	
<i>Simplify₂</i>	$\frac{\langle E \cup \{s \doteq t\}, H \rangle}{\langle E \cup \{s' \doteq t\}, H \rangle} s \vdash_{\mathcal{E}}^{p, g \doteq h} s', g \doteq h \in H, s/p > s'/p,$	
<i>Simplify₃</i>	$\frac{\langle E \cup \{s \doteq t\}, H \rangle}{\langle E \cup \{s' \doteq t\}, H \rangle} s \vdash_E^p s', s/p > s'/p, p \neq \epsilon, s > s/p$	$(p \neq \epsilon \wedge s > s/p) \vee (g > h)$
<i>Simplify₄</i>	$\frac{\langle E \cup \{s \doteq t\}, H \rangle}{\langle E \cup \{s' \doteq t\}, H \rangle} s \vdash_H^p s', s/p \mid s'/p, s \mid t, s' \leq t$	
<i>Delete</i>	$\frac{\langle E \cup \{s \doteq s\}, H \rangle}{\langle E, H \rangle}$	

Fig. 7 Inference rules of (a part of) system I ⁶⁾

and other major systems in the literature. The proposed inference rule of simplification by conjectures essentially subsumes those of the corresponding fragments of some well-known inference systems. As our future work, we intend to implement the proposed method and experimentally evaluate the effectiveness of our approach.

References


- 1) Aoto, T.: Dealing with non-orientable equations in rewriting induction, *Proc. of the 17th International Conference on Rewriting Tech-*
- niques and Applications*, LNCS, Vol. 4098, Springer-Verlag, pp. 242–256 (2006).
- 2) Baader, F. and Nipkow, T.: *Term Rewriting and All That*, Cambridge University Press (1998).
- 3) Bachmair, L., Dershowitz, N. and Plaisted, D. A.: Completion without failure, *Resolution of Equations in Algebraic Structures*, Vol. 2, Academic Press, pp. 1–30 (1989).
- 4) Barthe, G. and Stratulat, S.: Validation of the JavaCard Platform with implicit induction techniques, *Proc. of the 14th International Conference on Rewriting Techniques and Applica-*

- tions, LNCS, Vol. 2706, Springer-Verlag, pp. 337–351 (2003).
- 5) Bouhoula, A.: Automated theorem proving by test set induction, *Journal of Symbolic Computation*, Vol. 23, pp. 47–77 (1997).
 - 6) Bouhoula, A., Kounalis, E. and Rusinowitch, M.: Automated mathematical induction, *Journal of Logic and Computation*, Vol. 5, No. 5, pp. 631–668 (1995).
 - 7) Bouhoula, A. and Rusinowitch, M.: Implicit induction in conditional theories, *Journal of Automated Reasoning*, Vol. 14, pp. 189–235 (1995).
 - 8) Bronsard, R., Reddy, U. S. and Hasker, R. W.: Induction using term orders, *Journal of Automated Reasoning*, Vol. 16, pp. 3–37 (1996).
 - 9) Dershowitz, N. and Reddy, U. S.: Deductive and inductive synthesis of equational programs, *Journal of Symbolic Computation*, Vol. 15, pp. 467–494 (1993).
 - 10) Falke, S. and Kapur, D.: Inductive decidability using implicit induction, *Proc. of the 13th International Conference on Logic for Programming, Artificial Intelligence and Reasoning*, LNAI, Vol. 4246, Springer-Verlag, pp. 45–59 (2006).
 - 11) Hsiang, J. and Rusinowitch, M.: On word problems in equational theories, *Proc. of the 14th International Colloquium on Automata, Languages and Programming*, LNCS, Vol. 267, Springer-Verlag, pp. 54–71 (1987).
 - 12) Huet, G. and Hullot, J.-M.: Proof by induction in equational theories with constructors, *Journal of Computer and System Sciences*, Vol. 25, No. 2, pp. 239–266 (1982).
 - 13) Jouannaud, J.-P. and Kounalis, E.: Automatic proofs by induction in theories without constructors, *Information and Computation*, Vol. 82, pp. 1–33 (1989).
 - 14) Kapur, D., Giesl, J. and Subramaniam, M.: Induction and decision procedures, *Revista de la real academia de ciencias (RACSAM) Serie A: Matematicas*, Vol. 98, No. 1, pp. 154–180 (2004).
 - 15) Kapur, D., Narendran, P. and Zhang, H.: Automating inductionless induction using test sets, *Journal of Symbolic Computation*, Vol. 11, No. 1–2, pp. 81–111 (1991).
 - 16) Koike, H. and Toyama, Y.: Inductionless induction and rewriting induction, *Computer Software*, Vol. 17, No. 6, pp. 1–12 (2000). In Japanese.
 - 17) Musser, D. R.: On proving inductive properties of abstract data types, *Proc. of the 7th Annual ACM Symposium on Principles of Programming Languages*, ACM Press, pp. 154–162 (1980).
 - 18) Reddy, U. S.: Term rewriting induction, *Proc. of the 10th International Conference on Automated Deduction*, LNAI, Vol. 449, Springer-Verlag, pp. 162–177 (1990).
 - 19) Sakamoto, K., Aoto, T. and Toyama, Y.: Fusion transformation based on rewriting induction, *Proc. of the 21st JSSST Annual Conference* (2B-3, 2004). In Japanese.
 - 20) Stratulat, S.: A general framework to build contextual cover set induction provers, *Journal of Symbolic Computation*, Vol. 32, pp. 403–445 (2001).
 - 21) Terese: *Term Rewriting Systems*, Cambridge University Press (2003).
 - 22) Toyama, Y.: How to prove equivalence of term rewriting systems without induction, *Theoretical Computer Science*, Vol. 90, No. 2, pp. 369–390 (1991).

Acknowledgments Thanks are due to Yoshihito Toyama, Jeroen Ketema, Yuki Chiba, and an anonymous referee for valuable comments. This work was partially supported by a grant from JSPS, No. 17700002.

(Received May 07, 19)

(Accepted August 01, 19)



Takahito Aoto received his M.S. and Ph.D. from Japan Advanced Institute for Science and Technology (JAIST). He was at JAIST from 1997 to 1998 as an associate, at Gunma University from 1998 to 2002 as an assistant professor, and at Tohoku University from 2003 to 2004 as a lecturer. He has been in Tohoku University from 2004 as an associate professor. His current research interests include term rewriting, automated theorem proving, and foundation of software. He is a member of IPSJ, JSSST, EATCS, and ACM.