UPMAIL Technical Report No. 121
January 12, 1996
revised June 4, 1996
ISSN 1100-0686

On Proof-Search in Intuitionistic Logic with Equality, or Back to Simultaneous Rigid E-Unification

Andrei Voronkov*

Computing Science Department
Uppsala University
Box 311, S-751 05 Uppsala,
Sweden

email voronkov@csd.uu.se

*Supported by a TFR grant

Abstract

We characterize provability in intuitionistic logic with equality in terms of a constraint calculus. This characterization uncovers close connections between provability in intuitionistic logic with equality and solutions to simultaneous rigid E-unification. We show that the problem of existence of a sequent proof with a given skeleton is polynomial-time equivalent to simultaneous rigid E-unifiability. This gives us a proof procedure for intuitionistic logic with equality modulo simultaneous rigid E-unification. We also show that simultaneous rigid E-unifiability is polynomial-time reducible to intuitionistic logic with equality. Thus, any proof procedure for intuitionistic logic with equality can be considered as a procedure for simultaneous rigid E-unifiability. In turn, any procedure for simultaneous rigid E-unifiability gives a procedure for establishing provability in intuitionistic logic with equality.[2]

Section 1

Introduction

Any automated theorem proving method for predicate logic provides a way of instantiating variables in proofs. In modern theorem proving methods, the variable instantiation is usually controlled by a suitable unification algorithm. In this paper we analyze the problem of variable instantiation in intuitionistic logic with equality. Our analysis shows close connections between the variable instantiation problem and simultaneous rigid E-unification introduced by Gallier, Raatz and Snyder [13]. Furthermore, our results imply that handling simultaneous rigid E-unification is unavoidable in automatic proof procedures for intuitionistic logic with equality.

For classical logic, there are many methods of variable instantiation depending on the proof procedure. The main methods (in the chronological order) are the following.

1. The early methods used saturation algorithms: substitutions of all possible (ground) terms for variables. The same effect is achieved by the use of the *functional reflexivity axiom* $t \simeq t$ (Robinson and Wos [31], also Loveland [21] in the context of model elimination and Fitting [12] in the context of the tableau method) or by the *functional substitutivity axioms:* both axioms allow us to replace variables by arbitrary terms. This way of instantiation is applicable to arbitrary theorem proving procedures, for example resolution-based or tableau-based procedures.

2. Kanger [15, 16] proposed to instantiate variables by subterms of terms already occurring in the (partial) derivation. This method was characterized as *minus-normalization* by Matulis [24] and Maslov [23]. The applicability of minus-normalization has been demonstrated for proof procedures based on sequent calculi, but it can as well be applied to resolution- and paramodulation-based proof procedures.

3. Resolution and *paramodulation* originally introduced by Robinson and Wos [31], or *superposition* use most-general unifiers to instantiate variables. However, most general unifiers have been shown useful only in indirect proof procedures: resolution and the inverse method (see Voronkov [38], Degtyarev and Voronkov [9])[1].

4. Plotkin [30] proposed to use *E-unification.* However, E-unification is applicable only in very restricted cases.

5. Gallier, Raatz and Snyder [13] proposed to use *simultaneous rigid E-unification* to instantiate variables in matrix-based methods, including the connection (or the mating) method and

[1] The inverse method was originally described by Maslov [22], but Maslov has never explicitly considered how to instantiate variables.

semantic tableaux. However, our recent results on the undecidability of simultaneous rigid E-unification by Degtyarev and Voronkov [5, 6] show that this approach can hardly be an advantage over methods using most general unifiers.

6. Degtyarev and Voronkov [4, 7, 8] proposed a combination of two kinds of unification for matrix methods based on so-called *equality elimination*. This approach consists of using most general unifiers in the superposition rules and *subset unification* to close tableau branches (subset unifiability is NP-complete).

For intuitionistic logic with equality, no machine-oriented characterization of provability is known. Of course, we can characterize provability in terms of arbitrary substitutions or the functional reflexivity axiom but this is hardly efficient. There are no analogues of resolution for intuitionistic logic. The inverse method augmented with paramodulation is incomplete, as implied by Example 2.2 below. This example also demonstrates non-applicability of equality elimination to intuitionistic logic.

The aim of this paper is to give a machine-oriented characterization of provability for intuitionistic logic with equality. Our characterization is based on simultaneous rigid E-unification. Using a description of provability in terms of derivation skeletons and constraints, we show that the existence of a derivation with a given skeleton is polynomial-time equivalent to simultaneous rigid E-unifiability. We also show that simultaneous rigid E-unifiability is polynomial-time reducible to intuitionistic logic with equality. These two observations show that a (semi-decision) algorithm for simultaneous rigid E-unifiability is "necessary and sufficient" for designing automated reasoning procedures for intuitionistic logic with equality.

This paper is structured as follows. Section 2 introduces main notions and defines simultaneous rigid E-unification. Section 3 defines a sequent calculus $\mathbf{LJ}^{\simeq}$ for intuitionistic logic with equality. In Section 3.1 we introduce derivation skeletons and the skeleton instantiation problem: the problem of the existence of a derivation with a given skeleton. We show that simultaneous rigid E-unifiability is polynomial-time reducible to intuitionistic logic with equality and to the skeleton instantiation problem. In Section 4 we introduce the constraint calculus $\mathbf{LJ}^{\simeq}_c$ which is a constraint-based modification of $\mathbf{LJ}^{\simeq}$. We also prove a general theorem about the connection between derivability in $\mathbf{LJ}^{\simeq}$ and that in $\mathbf{LJ}^{\simeq}_c$. In Section 5 we prove that the skeleton instantiation problem is polynomial-time equivalent to simultaneous rigid E-unifiability. In Section 6 we briefly consider related work.

Section 2

Preliminaries

Formulas are defined as usual, using atomic formulas, the constant Λ, the connectives $\wedge, \vee, \supset$ and the quantifiers $\forall, \exists$. Negation $\neg\varphi$ can be introduced as $\varphi \supset \Lambda$. A *sequent* is an expression of the form $\Gamma \rightarrow \varphi$ where Γ is a finite sequence of formulas and φ is a formula. A formula is *closed* iff it has no free variables. A sequent $\Gamma \rightarrow \varphi$ is *closed* iff all formulas in Γ, φ are closed. We assume that all free variables in formulas are different from all bound variables.

The notation $\rightleftharpoons$ stands for "equal by definition". We denote the formal equality symbol by $\simeq$. An *equation* is a formula of the form $s\simeq t$. An expression is *ground* iff it has no variables.

By X we denote a countable infinite set of variables. The set of all terms in the signature Σ with variables in X is denoted by $T_\Sigma(X)$. By T_Σ we denote $T_\Sigma(\emptyset)$, i.e. the set of all ground terms in the signature Σ. *Constants* are regarded as function symbols of arity 0. Variables are denoted by u, v, w, x, y, z, maybe with indices. We assume that all formulas use variables in the set X.

A *substitution* is any mapping θ from X to $T_\Sigma(X)$ such that there is only a finite number of variables x such that $\theta(x) \neq x$. The *domain* $dom(\theta)$ of the substitution θ is the set $\{x \mid x\theta \neq x\}$. The *range* $ran(\theta)$ of the substitution θ is defined by $ran(\theta) \rightleftharpoons \{x\theta \mid x \in dom(\theta)\}$. Substitutions θ with the domain $x_1, \ldots, x_n$ are denoted by $\{x_1\theta/x_1, \ldots, x_n\theta/x_n\}$. Let E be a term, formula, sequence of formulas or sequent. For a substitution $\theta = \{t_1/x_1, \ldots, t_n/x_n\}$, $E\theta$ denotes the result of *applying* θ *to* E, i.e. renaming of those bound variables in E that coincide with a variable occurring in any t_i and the replacement of all free occurrences of x_i by t_i.

Let φ be a formula all whose free variables are $x_1, \ldots, x_n$, in the order of their occurrences in φ. By $\forall\varphi$ we denote the formula $\forall x_1 \ldots \forall x_n \varphi$, and similar for $\exists\varphi$. We identify formulas equal up to renaming of bound variables.

2.1 Simultaneous rigid E-unification

In this section we define simultaneous rigid E-unification originally introduced by Gallier, Raatz and Snyder [13].

Definition 2.1 (Simultaneous rigid E-unification)
A *rigid equation* is an expression $E \vdash_\forall s\simeq t$, where E is a finite set of equations. A *solution to a rigid equation* $\{s_1\simeq t_1, \ldots, s_n\simeq t_n\} \vdash_\forall s\simeq t$ is any substitution σ such that the formula $\forall(s_1\sigma\simeq t_1\sigma \wedge \ldots \wedge s_n\sigma\simeq t_n\sigma \supset s\sigma\simeq t\sigma)$ is true[1]. A *system of rigid equations* is a finite set of rigid equations. A *solution to a system of rigid equations* S is any substitution that is a solution to every rigid

[1] I.e. this formula is provable in first-order (classical or intuitionistic) logic. Equivalently, we can say that $s\sigma$ and $t\sigma$ lie in the same class of the congruence generated by $\{s_1\sigma\simeq t_1\sigma, \ldots, s_n\sigma\simeq t_n\sigma\}$.

equation in S. The problem of solvability of rigid equations is known as *rigid E-unification*. The problem of solvability of systems of rigid equations is known as *simultaneous rigid E-unification*[2].

We shall sometimes write the left-hand side of a rigid equation as a *sequence* of equations, for example $x \simeq a \vdash_\forall g(x) \simeq x$ instead of $\{x \simeq a\} \vdash_\forall g(x) \simeq x$.

Consider two examples.

Example 2.2 The system of two rigid equations[3]

$$\begin{array}{c} a \simeq b \vdash_\forall g(x,u,v) \simeq g(y,f(c),f(d)) \\ c \simeq d \vdash_\forall g(u,x,y) \simeq g(v,f(a),f(b)) \end{array}$$

has one solution $\{f(a)/x, f(b)/y, f(c)/u, f(d)/v\}$. This system of rigid equations has an interesting property: we cannot find its solution using V-paramodulation of Chang and Lee [17] (later described as rigid paramodulation by Plaisted [29]) and most general solutions to the equations in the right-hand sides of $\vdash_\forall$.

Example 2.3 The system of two rigid equations

$$\begin{array}{c} h(x_1) \simeq a, h(x_2) \simeq a, h(a) \simeq y \vdash_\forall y \simeq g(h(y)) \\ h(x_1) \simeq a, h(x_2) \simeq a, h(b) \simeq f(y) \vdash_\forall y \simeq g(f(y)) \end{array}$$

has an infinite number of solutions. Among these solutions are the substitutions of the form $\{a/x_1, b/x_2, g(h^n(a))/y\}$, for every $n \geq 0$.

The following result is proven by Degtyarev and Voronkov [5, 6]:

Theorem 2.4 Simultaneous rigid E-unifiability is undecidable.

In view of this result, when we mention procedures or algorithms for simultaneous rigid E-unification, we mean semi-decision procedures or algorithms.

A more precise formulation of the undecidability results is the following (see Veanes [36]):

Theorem 2.5 Simultaneous rigid E-unifiability in the signature with one function symbol of arity ≥ 2 and at least one constant is undecidable.

The decidability of simultaneous rigid E-unification in the signatures with unary function symbols is an open problem (Degtyarev, Matiyasevich and Voronkov [3]).

[2] We slightly changed the terminology compared to Gallier, Raatz and Snyder [13]. Our notion of a rigid equation corresponds to the notion of a rigid E-unification problem of [13]. Our notion of a system of rigid equations corresponds to the notion of a simultaneous rigid E-unification problem of [13]. We introduced a new terminology to avoid the ambiguous use of the word "problem" that can also be understood as the algorithmic problem of finding a solution to a rigid equation.

[3] This system was proposed by Anatoli Degtyarev to show that paramodulation-based methods are incomplete for simultaneous rigid E-unification.

Section 3

The calculus $\mathbf{LJ}^{\simeq}$

In this section we define the sequent calculus $\mathbf{LJ}^{\simeq}$ for intuitionistic logic with equality and two notions of derivation skeletons. We also prove some properties of derivations in $\mathbf{LJ}^{\simeq}$.

Definition 3.1 (Calculus $\mathbf{LJ}^{\simeq}$)
The calculus $\mathbf{LJ}^{\simeq}$ for intuitionistic logic with equality derives sequents. The rules of the calculus are shown in Figure 3.1. Derivations in $\mathbf{LJ}^{\simeq}$ are trees defined as usual.

We formulate $\mathbf{LJ}^{\simeq}$ as a system without the cut rule. It is not difficult to prove that cut is admissible in $\mathbf{LJ}^{\simeq}$ using the general cut-elimination theorem given in Sazonov [33], Buss [1], or Girard [14].

There are two major kinds of automated theorem proving methods based on the proof-search in sequent calculi: the tableau method and the inverse method. The inverse method tries to construct proofs in the direction from axioms to the goal. The tableau method tries to construct proofs in the direction from the goal to axioms. The calculus $\mathbf{LJ}^{\simeq}$ is formulated in a way more suitable for a tableau proof procedure. We can also define a similar calculus for the inverse method, but designing a particular *procedure* is not the aim of this paper.

The following simple statement connects the derivability in $\mathbf{LJ}^{\simeq}$ with solutions to rigid equations.

Lemma 3.2 Let σ be a substitution. The following conditions are equivalent:

1. The sequent $s_1\sigma\simeq t_1\sigma, \ldots, s_n\sigma\simeq t_n\sigma \to s\sigma\simeq t\sigma$ is derivable in $\mathbf{LJ}^{\simeq}$;
2. The sequent $s_1\sigma\simeq t_1\sigma, \ldots, s_n\sigma\simeq t_n\sigma \to s\sigma\simeq t\sigma$ is derivable in $\mathbf{LJ}^{\simeq}$ using only $(\simeq)$, $(\simeq_1)$ and $(\simeq_2)$;
3. σ is a solution to the rigid equation $s_1\simeq t_1, \ldots, s_n\simeq t_n \vdash_\forall s\simeq t$.

Proof. Standard. □

Note. To prove this lemma, it is enough to have a restricted system where the rules $(\simeq_1)$ and $(\simeq_2)$ only replace terms in the succedents of the sequents. The completeness of the system with such restricted rules for intuitionistic logic with equality is proven by a number of authors (e.g. by Orevkov [26]).

$$\frac{}{\Gamma, A, \Delta \to A}\ (Ax) \qquad \frac{}{\Gamma, \Lambda, \Delta \to \varphi}\ (\Lambda) \qquad \frac{}{\Gamma \to t{\simeq}t}\ (\simeq)$$

$$\frac{\Gamma\{t/x\}, s{\simeq}t, \Delta\{t/x\} \to \chi\{t/x\}}{\Gamma\{s/x\}, s{\simeq}t, \Delta\{s/x\} \to \chi\{s/x\}}\ (\simeq_1) \qquad \frac{\Gamma\{s/x\}, s{\simeq}t, \Delta\{s/x\} \to \chi\{s/x\}}{\Gamma\{t/x\}, s{\simeq}t, \Delta\{t/x\} \to \chi\{t/x\}}\ (\simeq_2)$$

$$\frac{\Gamma, \varphi, \psi, \Delta \to \chi}{\Gamma, \varphi \land \psi, \Delta \to \chi}\ (\land \to) \qquad \frac{\Gamma \to \varphi \quad \Gamma \to \psi}{\Gamma \to \varphi \land \psi}\ (\to \land)$$

$$\frac{\Gamma, \varphi, \Delta \to \chi \quad \Gamma, \psi, \Delta \to \chi}{\Gamma, \varphi \lor \psi, \Delta \to \chi}\ (\lor \to) \qquad \frac{\Gamma \to \varphi}{\Gamma \to \varphi \lor \psi}\ (\to \lor_1) \qquad \frac{\Gamma \to \psi}{\Gamma \to \varphi \lor \psi}\ (\to \lor_2)$$

$$\frac{\Gamma, \psi, \Delta \to \chi \quad \Gamma, \varphi \supset \psi, \Delta \to \varphi}{\Gamma, \varphi \supset \psi, \Delta \to \chi}\ (\supset\to) \qquad \frac{\varphi, \Gamma \to \psi}{\Gamma \to \varphi \supset \psi}\ (\to\supset)$$

$$\frac{\Gamma, \varphi\{t/x\}, \forall x\varphi, \Delta \to \chi}{\Gamma, \forall x\varphi, \Delta \to \chi}\ (\forall \to) \qquad \frac{\Gamma \to \varphi\{y/x\}}{\Gamma \to \forall x\varphi}\ (\to \forall)$$

$$\frac{\Gamma, \varphi\{y/x\}, \Delta \to \chi}{\Gamma, \exists x\varphi, \Delta \to \chi}\ (\exists \to) \qquad \frac{\Gamma \to \varphi\{t/x\}}{\Gamma \to \exists x\varphi}\ (\to \exists)$$

In this figure, A ranges over atomic formulas, φ, ψ, χ range over arbitrary formulas and Γ, Δ range over finite sequences of formulas. In the rules $(\to \forall)$ and $(\exists \to)$ the variable y has no free occurrences in the conclusions of the rules. The variable y is called the *eigenvariable* of these rules.

Figure 3.1: Calculus $\mathbf{LJ}^{\simeq}$

3.1 Derivation skeletons

In this section we study two kinds of skeletons of $\mathbf{LJ}^{\simeq}$-derivations. The notion of a skeleton provides an abstraction of a family of derivations.

Definition 3.3 (Weak skeleton)
A *weak derivation skeleton* is a tree such that

1. Its nodes are labelled by the names of inference rules in $\mathbf{LJ}^{\simeq}$, except for $(\simeq_1)$ and $(\simeq_2)$;

2. The number of parents of a node labelled by a name of an inference rule is equal to the number of the premises in such a rule in $\mathbf{LJ}^{\simeq}$.

We display derivation skeletons as derivations with omitted sequents, nodes are denoted by horizontal bars with labels displayed to the right of the bar.

Example 3.4 The following is a weak derivation skeleton. This weak skeleton corresponds to derivations of Example 3.10 in some precise sense defined below (Definition 3.6).

$$
\AxiomC{}
\RightLabel{$(\simeq)$}
\UnaryInfC{}
\RightLabel{$(\rightarrow \exists)$}
\UnaryInfC{}
\RightLabel{$(\exists \rightarrow)$}
\UnaryInfC{}
\AxiomC{}
\RightLabel{$(\simeq)$}
\UnaryInfC{}
\RightLabel{$(\rightarrow \vee_2)$}
\UnaryInfC{}
\RightLabel{$(\supset\rightarrow)$}
\BinaryInfC{}
\RightLabel{$(\forall \rightarrow)$}
\UnaryInfC{}
\RightLabel{$(\rightarrow \exists)$}
\UnaryInfC{}
\RightLabel{$(\exists \rightarrow)$}
\UnaryInfC{}
\AxiomC{}
\RightLabel{$(\simeq)$}
\UnaryInfC{}
\RightLabel{$(\rightarrow \vee_1)$}
\UnaryInfC{}
\RightLabel{$(\supset\rightarrow)$}
\BinaryInfC{}
\RightLabel{$(\forall \rightarrow)$}
\UnaryInfC{}
\RightLabel{$(\rightarrow \exists)$}
\UnaryInfC{}
\RightLabel{$(\rightarrow\supset)$}
\UnaryInfC{}
\DisplayProof
$$

The following are *not* weak derivation skeletons:

$$
\AxiomC{}
\RightLabel{$(\simeq)$}
\UnaryInfC{}
\RightLabel{$(\rightarrow \wedge)$}
\UnaryInfC{}
\DisplayProof
\qquad \text{and} \qquad
\AxiomC{}
\RightLabel{$(\simeq)$}
\UnaryInfC{}
\RightLabel{$(\simeq_2)$}
\UnaryInfC{}
\DisplayProof
$$

In the first figure, the node labeled $(\rightarrow \wedge)$ has one parent instead of two. The second figure contains a node labeled $(\simeq_2)$ that is not allowed in skeletons.

We introduce a stronger notion of skeletons:

Definition 3.5 (Skeleton)
A *skeleton* is defined similar to the weak skeleton with the following difference: all nodes labelled by antecedent rules or (Ax) are additionally labelled by a natural number.

Derivation skeletons are abstractions of derivations that encode information about the structures of derivations. They abstract from the following information:

1. The instantiation of variables in quantifier rules;

2. The order of applications of the equality rules $(\simeq_1)$ and $(\simeq_2)$.

We shall illustrate this in Examples 3.7–3.10 below.

The natural number in an antecedent rule or in an axiom (Ax) represents the index of the main formula (counting from 0) of this rule in the antecedent of the conclusion of the rule. In other words, this number is the number of formulas in Γ in the corresponding rules of $\mathbf{LJ}^{\simeq}$ (Figure 3.1). We always display the number as an index.

The weak skeleton of a derivation Π is obtained from Π by removing all sequents and all applications of rules $(\simeq_1)$ and $(\simeq_2)$. More formally, the skeleton and the weak skeleton of a derivation are defined as follows:

Definition 3.6 (Skeleton of a derivation)
Let Π be a derivation in $\mathbf{LJ}^{\simeq}$. *The weak skeleton* Π' *of* Π and *the skeleton* Π'' *of* Π are defined inductively as follows:

1. If Π has the form $\dfrac{}{\Gamma, A, \Delta \rightarrow A}\,(Ax)$ then Π' and Π'' are $\overline{}\;(Ax)$ and $\overline{}\;(Ax_n)$ respectively, where n is the number of formulas in Γ.

2. If Π has the form $\dfrac{}{\Gamma,\Lambda,\Delta\to\varphi}\,(\Lambda)$ then both Π' and Π'' are $\dfrac{}{}\,(\Lambda)$.

3. If Π has the form $\dfrac{}{\Gamma\to t\simeq t}\,(\simeq)$ then both Π' and Π'' are $\dfrac{}{}\,(\simeq)$.

4. If Π has the form $\dfrac{\begin{matrix}\Pi_1\\ \Gamma\{t/x\},s\simeq t,\Delta\{t/x\}\to\chi\{t/x\}\end{matrix}}{\Gamma\{s/x\},s\simeq t,\Delta\{s/x\}\to\chi\{s/x\}}\,(\simeq_1)$ and Π_1' and Π_1'' are, respectively, the weak skeleton and the skeleton of Π_1, then $\Pi'\rightleftharpoons\Pi_1'$ and $\Pi''\rightleftharpoons\Pi_1''$, and similar for the $(\simeq_2)$-rule.

5. If Π has the form $\dfrac{\begin{matrix}\Pi_1\\ \varphi,\Gamma\to\psi\end{matrix}}{\Gamma\to\varphi\supset\psi}\,(\to\supset)$ and Π_1' and Π_1'' are, respectively, the weak skeleton and the skeleton of Π_1, then Π' and Π'' are $\dfrac{\Pi_1'}{}\,(\to\supset)$ and $\dfrac{\Pi_1''}{}\,(\to\supset)$ respectively, and similar for all other succedent rules.

6. If Π has the form $\dfrac{\begin{matrix}\Pi_1\\ \Gamma,\psi,\Delta\to\chi\end{matrix}\quad\begin{matrix}\Pi_2\\ \Gamma,\varphi\supset\psi,\Delta\to\varphi\end{matrix}}{\Gamma,\varphi\supset\psi,\Delta\to\chi}\,(\supset\to)$ and Π_1',Π_2' and Π_1'',Π_2'' are, respectively, the weak skeletons and the skeletons of Π_1,Π_2, then Π' and Π'' are $\dfrac{\Pi_1'\quad\Pi_2'}{}\,(\supset\to)$ and $\dfrac{\Pi_1''\quad\Pi_2''}{}\,(\supset\to_n)$ respectively, where n is the number of formulas in Γ, and similar for all other antecedent rules.

The following example shows that the notion of a weak skeleton abstracts from some details of the structure of derivations which is explicitly presented in skeletons.

Example 3.7 Consider the following two derivations of the propositional formula $((A\supset\Lambda)\wedge(B\supset\Lambda)\wedge A\wedge B)\supset\Lambda$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Lambda,(B\supset\Lambda),A,B\to\Lambda}\,(\Lambda)\quad\dfrac{}{(A\supset\Lambda),(B\supset\Lambda),A,B\to A}\,(Ax)}{(A\supset\Lambda),(B\supset\Lambda),A,B\to\Lambda}\,(\supset\to)}{(A\supset\Lambda),(B\supset\Lambda),A\wedge B\to\Lambda}\,(\wedge\to)}{(A\supset\Lambda),(B\supset\Lambda)\wedge A\wedge B\to\Lambda}\,(\wedge\to)}{(A\supset\Lambda)\wedge(B\supset\Lambda)\wedge A\wedge B\to\Lambda}\,(\wedge\to)}{\to((A\supset\Lambda)\wedge(B\supset\Lambda)\wedge A\wedge B)\supset\Lambda}\,(\to\supset)$$

and

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{(A\supset\Lambda),\Lambda,A,B\to\Lambda}\,(\Lambda)\quad\dfrac{}{(A\supset\Lambda),(B\supset\Lambda),A,B\to B}\,(Ax)}{(A\supset\Lambda),(B\supset\Lambda),A,B\to\Lambda}\,(\supset\to)}{(A\supset\Lambda),(B\supset\Lambda),A\wedge B\to\Lambda}\,(\wedge\to)}{(A\supset\Lambda),(B\supset\Lambda)\wedge A\wedge B\to\Lambda}\,(\wedge\to)}{(A\supset\Lambda)\wedge(B\supset\Lambda)\wedge A\wedge B\to\Lambda}\,(\wedge\to)}{\to((A\supset\Lambda)\wedge(B\supset\Lambda)\wedge A\wedge B)\supset\Lambda}\,(\to\supset)$$

They have the same weak skeleton

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{}\,(\Lambda)\qquad\dfrac{}{}\,(Ax)}{}\,(\supset\to)}{}\,(\wedge\to)}{}\,(\wedge\to)}{}\,(\wedge\to)}{}\,(\to\supset)$$

but different skeletons:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{}\,(\Lambda)\qquad\dfrac{}{}\,(Ax_2)}{}\,(\supset\to_0)}{}\,(\wedge\to_2)}{}\,(\wedge\to_1)}{}\,(\wedge\to_0)}{}\,(\to\supset) \qquad\qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{}\,(\Lambda)\qquad\dfrac{}{}\,(Ax_3)}{}\,(\supset\to_1)}{}\,(\wedge\to_2)}{}\,(\wedge\to_1)}{}\,(\wedge\to_0)}{}\,(\to\supset)$$

Skeletons uniquely identify derivations of propositional formulas. However, there may be many derivations of the same non-propositional formula (even without equality) with the same skeleton due to different instantiations of terms in the quantifier rules.

Example 3.8 The following two different derivations of the formula $\forall xA(x) \supset \exists xA(x)$ have the same skeleton:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A(x),\forall xA(x)\to A(x)}\,(Ax)}{\forall xA(x)\to A(x)}\,(\forall\to)}{\forall xA(x)\to\exists xA(x)}\,(\to\exists)}{\to\forall xA(x)\supset\exists xA(x)}\,(\to\supset) \qquad\qquad \dfrac{\dfrac{\dfrac{\dfrac{}{A(f(a)),\forall xA(x)\to A(f(a))}\,(Ax)}{\forall xA(x)\to A(f(a))}\,(\forall\to)}{\forall xA(x)\to\exists xA(x)}\,(\to\exists)}{\to\forall xA(x)\supset\exists xA(x)}\,(\to\supset)$$

Finally, skeletons abstract from the order of applications of the rules $(\simeq_1)$ and $(\simeq_2)$. Before giving an example, we introduce an important notion:

Definition 3.9 (Regular derivation)
A derivation in $\mathbf{LJ}^{\simeq}$ is called *regular* iff above any application of $(\simeq_1)$ or $(\simeq_2)$ there can only be applications of the rules $(\simeq_1)$, $(\simeq_2)$, (Ax), (Λ) and $(\simeq)$.

Example 3.10 Below we show two derivations of the formula $\forall x(x\simeq a \vee x\simeq b \supset \exists y(f(x,y)\simeq b)) \supset \exists u\exists v\exists w(f(f(u,v),w)\simeq b)$. Both derivations have the weak skeleton of Example 3.4. They have the same skeleton and use the same instantiation of variables. We denote by φ the formula $\forall x(x\simeq a \vee x\simeq b \supset \exists y(f(x,y)\simeq b))$. We also denote by $\cdots$ some irrelevant parts of the sequents.

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{$(\simeq)$}
\UnaryInfC{$f(a,y)\simeq b, f(b,z)\simeq b, \varphi \rightarrow f(b,z)\simeq f(b,z)$}
\RightLabel{$(\simeq_2)$}
\UnaryInfC{$f(a,y)\simeq b, f(b,z)\simeq b, \varphi \rightarrow f(b,z)\simeq b$}
\RightLabel{$(\simeq_1)$}
\UnaryInfC{$f(a,y)\simeq b, f(b,z)\simeq b, \varphi \rightarrow f(f(a,y),z)\simeq b$}
\RightLabel{$(\rightarrow \exists)$}
\UnaryInfC{$f(a,y)\simeq b, f(b,z)\simeq b, \varphi \rightarrow \exists w(f(f(a,y),w)\simeq b)$}
\RightLabel{$(\exists \rightarrow)$}
\UnaryInfC{$f(a,y)\simeq b, \exists y(f(b,y)\simeq b), \varphi \rightarrow \exists w(f(f(a,y),w)\simeq b)$}
\AxiomC{}
\RightLabel{$(\simeq)$}
\UnaryInfC{$\cdots \rightarrow b\simeq b$}
\RightLabel{$(\rightarrow \vee_2)$}
\UnaryInfC{$\cdots \rightarrow b\simeq a \vee b\simeq b$}
\RightLabel{$(\supset\rightarrow)$}
\BinaryInfC{$f(a,y)\simeq b, b\simeq a \vee b\simeq b \supset \exists y(f(b,y)\simeq b), \varphi \rightarrow \exists w(f(f(a,y),w)\simeq b)$}
\RightLabel{$(\forall \rightarrow)$}
\UnaryInfC{$f(a,y)\simeq b, \varphi \rightarrow \exists w(f(f(a,y),w)\simeq b)$}
\RightLabel{$(\rightarrow \exists)$}
\UnaryInfC{$f(a,y)\simeq b, \varphi \rightarrow \exists v\exists w(f(f(a,v),w)\simeq b)$}
\RightLabel{$(\exists \rightarrow)$}
\UnaryInfC{$\exists y(f(a,y)\simeq b), \varphi \rightarrow \exists v\exists w(f(f(a,v),w)\simeq b)$}
\AxiomC{}
\RightLabel{$(\simeq)$}
\UnaryInfC{$\cdots \rightarrow a\simeq a$}
\RightLabel{$(\rightarrow \vee_1)$}
\UnaryInfC{$\cdots \rightarrow a\simeq a \vee a\simeq b$}
\RightLabel{$(\supset\rightarrow)$}
\BinaryInfC{$a\simeq a \vee a\simeq b \supset \exists y(f(a,y)\simeq b), \varphi \rightarrow \exists v\exists w(f(f(a,v),w)\simeq b)$}
\RightLabel{$(\forall \rightarrow)$}
\UnaryInfC{$\varphi \rightarrow \exists v\exists w(f(f(a,v),w)\simeq b)$}
\RightLabel{$(\rightarrow \exists)$}
\UnaryInfC{$\varphi \rightarrow \exists u\exists v\exists w(f(f(u,v),w)\simeq b)$}
\RightLabel{$(\rightarrow\supset)$}
\UnaryInfC{$\rightarrow \varphi \supset \exists u\exists v\exists w(f(f(u,v),w)\simeq b)$}
\end{prooftree}
$$

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{$(\simeq)$}
\UnaryInfC{$f(a,y)\simeq b, f(b,z)\simeq b, \varphi \rightarrow b\simeq b$}
\RightLabel{$(\simeq_2)$}
\UnaryInfC{$f(a,y)\simeq b, f(b,z)\simeq b, \varphi \rightarrow f(b,z)\simeq b$}
\RightLabel{$(\rightarrow \exists)$}
\UnaryInfC{$f(a,y)\simeq b, f(b,z)\simeq b, \varphi \rightarrow \exists w(f(b,w)\simeq b)$}
\RightLabel{$(\exists \rightarrow)$}
\UnaryInfC{$f(a,y)\simeq b, \exists y(f(b,y)\simeq b), \varphi \rightarrow \exists w(f(b,w)\simeq b)$}
\AxiomC{}
\RightLabel{$(\simeq)$}
\UnaryInfC{$\cdots \rightarrow b\simeq b$}
\RightLabel{$(\rightarrow \vee_2)$}
\UnaryInfC{$\cdots \rightarrow b\simeq a \vee b\simeq b$}
\RightLabel{$(\supset\rightarrow)$}
\BinaryInfC{$f(a,y)\simeq b, b\simeq a \vee b\simeq b \supset \exists y(f(b,y)\simeq b), \varphi \rightarrow \exists w(f(b,w)\simeq b)$}
\RightLabel{$(\forall \rightarrow)$}
\UnaryInfC{$f(a,y)\simeq b, \varphi \rightarrow \exists w(f(b,w)\simeq b)$}
\RightLabel{$(\simeq_1)$}
\UnaryInfC{$f(a,y)\simeq b, \varphi \rightarrow \exists w(f(f(a,y),w)\simeq b)$}
\RightLabel{$(\rightarrow \exists)$}
\UnaryInfC{$f(a,y)\simeq b, \varphi \rightarrow \exists v\exists w(f(f(a,v),w)\simeq b)$}
\RightLabel{$(\exists \rightarrow)$}
\UnaryInfC{$\exists y(f(a,y)\simeq b), \varphi \rightarrow \exists v\exists w(f(f(a,v),w)\simeq b)$}
\AxiomC{}
\RightLabel{$(\simeq)$}
\UnaryInfC{$\cdots \rightarrow a\simeq a$}
\RightLabel{$(\rightarrow \vee_1)$}
\UnaryInfC{$\cdots \rightarrow a\simeq a \vee a\simeq b$}
\RightLabel{$(\supset\rightarrow)$}
\BinaryInfC{$a\simeq a \vee a\simeq b \supset \exists y(f(a,y)\simeq b), \varphi \rightarrow \exists v\exists w(f(f(a,v),w)\simeq b)$}
\RightLabel{$(\forall \rightarrow)$}
\UnaryInfC{$\varphi \rightarrow \exists v\exists w(f(f(a,v),w)\simeq b)$}
\RightLabel{$(\rightarrow \exists)$}
\UnaryInfC{$\varphi \rightarrow \exists u\exists v\exists w(f(f(u,v),w)\simeq b)$}
\RightLabel{$(\rightarrow\supset)$}
\UnaryInfC{$\rightarrow \varphi \supset \exists u\exists v\exists w(f(f(u,v),w)\simeq b)$}
\end{prooftree}
$$

However, the proofs are different because of the order of applications of the rules $(\simeq_1)$ and $(\simeq_2)$. Moreover, the first derivation is regular while the second is not regular.

The following theorem shows that the order of applications of $(\simeq_1)$ and $(\simeq_2)$ is, in some sense, unimportant. Similar theorems for various formalizations of intuitionistic logic with equality were stated and/or proven by Kanger [16] and Lifschitz [19].

Theorem 3.11 Let S be a sequent and $\mathcal{S}$ be a skeleton (respectively, a weak skeleton). The following conditions are equivalent:

1. There is a derivation of S with the skeleton (respectively, the weak skeleton) $\mathcal{S}$;
2. There is a regular derivation of S with the skeleton (respectively, the weak skeleton) $\mathcal{S}$.

As a consequence, any derivable sequent has a regular derivation.

Proof. An application of the rule ($\simeq_1$) or ($\simeq_2$), where the variable x has n occurrences in Γ, Δ, χ of the rule, can be replaced by n applications of the same rule. Thus, we can assume that in any application of ($\simeq_1$) or ($\simeq_2$), the variable x has precisely one occurrence in Γ, Δ, χ. Also, we can assume that x does not occur in the derivation, since otherwise x can be replaced by any variable not occurring in the derivation.

The proof of this theorem is based on proof transformations moving applications of ($\simeq_1$) and ($\simeq_2$) up in the derivation. For simplicity, we only consider one case.

Suppose that an application of ($\simeq_2$) is immediately above an application of ($\rightarrow \exists$), and the occurrence of the variable x is in the succedent of the sequent:

$$\frac{\Gamma, s{\simeq}t, \Delta \rightarrow (\exists y\varphi)\{s/x\}}{\Gamma, s{\simeq}t, \Delta \rightarrow (\exists y\varphi)\{t/x\}}\ (\simeq_2)$$

Without loss of generality we can assume that y does not occur in s, t. Since x does not occur in the derivation, this can be rewritten as

$$\frac{\Gamma, s{\simeq}t, \Delta \rightarrow \exists y(\varphi\{s/x\})}{\Gamma, s{\simeq}t, \Delta \rightarrow (\exists y\varphi)\{t/x\}}\ (\simeq_2)$$

Then the fragment of the derivation consisting of the two rule applications has the form

$$\cfrac{\cfrac{\Gamma, s{\simeq}t, \Delta \rightarrow (\varphi\{s/x\})\{r/y\}}{\Gamma, s{\simeq}t, \Delta \rightarrow \exists y(\varphi\{s/x\})}\ (\rightarrow \exists)}{\Gamma, s{\simeq}t, \Delta \rightarrow (\exists y\varphi)\{t/x\}}\ (\simeq_2)$$

Since x does not occur in the derivation and y does not occur in s, t, the sequent $\Gamma, s{\simeq}t, \Delta \rightarrow (\varphi\{s/x\})\{r/y\}$ is equal to $\Gamma, s{\simeq}t, \Delta \rightarrow (\varphi\{r/y\})\{s/x\}$. Then this fragment of the derivation can be replaced by

$$\cfrac{\cfrac{\Gamma, s{\simeq}t, \Delta \rightarrow (\varphi\{s/x\})\{r/y\}}{\Gamma, s{\simeq}t, \Delta \rightarrow (\varphi\{t/x\})\{r/y\}}\ (\simeq_2)}{\Gamma, s{\simeq}t, \Delta \rightarrow \exists y(\varphi\{t/x\})}\ (\rightarrow \exists)$$

The proof for applications of other rules is similar. □

In this paper, we shall consider the problem of instantiation of a (weak) skeleton to a derivation:

Definition 3.12 The *(weak) skeleton instantiation problem* is the following problem. Given a closed sequent S and a (weak) skeleton $\mathcal{S}$, whether there is a derivation in **LJ** of S with the (weak) skeleton $\mathcal{S}$.

Note that the condition on S to be closed is inessential since one can always replace free variables of a sequent by fresh constants.

In [39] we proved that, for formulas without equality both problems are decidable. In addition, for formulas without equality

1. The weak skeleton instantiation problem is NP-complete;

2. The skeleton instantiation problem is in PTIME.

For formulas with equality both problems are undecidable. This follows from the following statement:

Theorem 3.13 Simultaneous rigid E-unifiability is polynomial-time reducible to any of the following three problems:

1. The problem of derivability in $\mathbf{LJ}^{\simeq}$;
2. The weak skeleton instantiation problem;
3. The skeleton instantiation problem.

Proof. Consider any system R of rigid equations of the form

$$\begin{array}{ccccc} s_{11}\simeq t_{11} & \dots & s_{1n_1}\simeq t_{1n_1} & \vdash_\forall & s'_1\simeq t'_1 \\ \vdots & & \vdots & & \vdots \\ s_{k1}\simeq t_{k1} & \dots & s_{kn_k}\simeq t_{kn_k} & \vdash_\forall & s'_k\simeq t'_k \end{array}$$

Let $x_1, \dots, x_m$ be all variables occurring in R. Denote by φ_R the formula

$$\begin{array}{lll} \exists x_1 \dots \exists x_m(& (s_{11}\simeq t_{11} \wedge \dots \wedge s_{1n_1}\simeq t_{1n_1} \supset s'_1\simeq t'_1) & \wedge \\ & \dots & \wedge \\ & (s_{k1}\simeq t_{k1} \wedge \dots \wedge s_{kn_k}\simeq t_{kn_k} \supset s'_k\simeq t'_k) &) \end{array}$$

(We assume that $\wedge$ associates to the right.) Evidently, φ_R can be constructed from R using a polynomial-time algorithm. By considering all possible derivations of $\to \varphi_R$ in $\mathbf{LJ}^{\simeq}$, it is easy to see that φ_R is derivable in $\mathbf{LJ}^{\simeq}$ iff there is a substitution σ such that the formula ψ of the form

$$\begin{array}{lll} (& (s_{11}\simeq t_{11} \wedge \dots \wedge s_{1n_1}\simeq t_{1n_1} \supset s'_1\simeq t'_1) & \wedge \\ & \dots & \wedge \\ & (s_{k1}\simeq t_{k1} \wedge \dots \wedge s_{kn_k}\simeq t_{kn_k} \supset s'_k\simeq t'_k) &)\sigma \end{array}$$

is derivable in $\mathbf{LJ}^{\simeq}$. Using the fact that the rules $(\to\wedge)$, $(\wedge\to)$ and $(\to\supset)$ are invertible[1] we can prove that ψ is derivable in $\mathbf{LJ}^{\simeq}$ if and only if it has a derivation with the skeleton $\mathcal{S}$ of the form

$$\cfrac{\mathcal{S}_1 \qquad \cfrac{\mathcal{S}_2 \qquad \begin{array}{c} \cfrac{\mathcal{S}_{k-1} \quad \mathcal{S}_k}{\qquad}\,(\to\wedge) \\ \vdots \end{array}}{\qquad}\,(\to\wedge)}{\qquad}\,(\to\wedge)$$

where $\mathcal{S}_j$ are skeletons

[1] A rule is invertible if the derivability of the conclusion of the rule implies the derivability of all premises of the rule.

$$
\begin{array}{l}
\overline{}\ (\simeq) \\
\overline{}\ (\wedge \to_{n_j-1}) \\
\vdots \\
\overline{}\ (\wedge \to_0) \\
\overline{}\ (\to\supset)
\end{array}
$$

It is easy to check that there is a derivation of ψ with the skeleton $\mathcal{S}$ iff for all $j \in \{1, \ldots, k\}$ the sequent $s_{j1}\sigma \simeq t_{j1}\sigma, \ldots, s_{jn_j}\sigma \simeq t_{jn_j}\sigma \to s'_j\sigma \simeq t'_j\sigma$ is derivable in $\mathbf{LJ}^{\simeq}$. By Lemma 3.2 we obtain that there is a derivation of ψ with the skeleton $\mathcal{S}$ iff σ is a solution to R.

This proves that simultaneous rigid E-unifiability is polynomial-time reducible to the derivability in $\mathbf{LJ}^{\simeq}$. By considering the formula φ_R and the skeleton

$$
\left.\begin{array}{l}
\dfrac{\mathcal{S}}{}\ (\to \exists) \\
\vdots \\
\overline{}\ (\to \exists)
\end{array}\right\} m \text{ applications of } (\to \exists)
$$

and using the same arguments as above, we prove that simultaneous rigid E-unifiability is polynomial-time reducible to the skeleton instantiation problem, and similar for the weak skeleton instantiation problem. □

This statement and Theorem 2.5 yield

Theorem 3.14 The weak skeleton instantiation problem and the skeleton instantiation problem for any signature having a function symbol of arity ≥ 2 are undecidable.

Section 4

The Constraint Calculus

In this section we define the constraint calculus $\mathbf{LJ}_c^{\simeq}$. This calculus can be used for defining sequent style proof procedures for intuitionistic logic with equality. The proof procedures based on $\mathbf{LJ}_c^{\simeq}$ consist of two parts: the construction of a derivation skeleton and the constraint satisfaction part. The constraint to be satisfied is computed from the skeleton of a derivation.

In Section 4.1 we define constraints and their semantics. In Section 4.2 we introduce the constrained calculus $\mathbf{LJ}_c^{\simeq}$ and prove its equivalence to $\mathbf{LJ}^{\simeq}$.

4.1 Constraints

Definition 4.1 (Constraints)
Constraints are defined inductively as follows:

1. $\top$ is a constraint;
2. For any terms $t, t_1, \ldots, t_n$, $t \not\preceq \{t_1, \ldots, t_n\}$ is a constraint;
3. Any rigid equation $s_1 \simeq t_1, \ldots, s_n \simeq t_n \vdash_\forall s \simeq t$ is a constraint;
4. If $\mathcal{C}_1, \mathcal{C}_2$ are constraints, then $\mathcal{C}_1 \wedge \mathcal{C}_2$ is a constraint;
5. If $\mathcal{C}$ is a constraint, x is variable, then $\exists x \mathcal{C}$ is a constraint.

Constraints can be regarded as first order formulas using the atomic formulas $\top$, $t \not\preceq \{t_1, \ldots, t_n\}$ and $E \vdash_\forall s \simeq t$ such that $\ldots \not\preceq \{\ldots\}$ and $\ldots \vdash_\forall \ldots$ are considered as a family of predicate symbols of arbitrary arities. Then, we can speak about the set $var(\mathcal{C})$ of *free variables* of a constraint $\mathcal{C}$.

Constraints describe the domain of substitutions. If a constraint $\mathcal{C}$ is true on a substitution σ we say that σ *satisfies* $\mathcal{C}$:

Definition 4.2 (Constraint satisfiability)
The notion "a substitution σ satisfies the constraint $\mathcal{C}$" (denoted $\sigma \models \mathcal{C}$) is defined inductively as follows:

1. $\sigma \models \top$ for every substitution σ;
2. $\sigma \models E \vdash_\forall s \simeq t$ iff σ is a solution to the rigid equation $E \vdash_\forall s \simeq t$;
3. $\sigma \models t \not\preceq \{t_1, \ldots, t_n\}$ iff $t\sigma$ is a variable and $t\sigma$ does not occur in $t_1\sigma, \ldots, t_n\sigma$;

$$\overline{\Gamma, A(s_1,\ldots,s_n), \Delta \to A(t_1,\ldots,t_n)\cdot \Gamma_{\simeq}\cup\Delta_{\simeq}\vdash_{\forall} s_1\simeq t_1\wedge\ldots\wedge\Gamma_{\simeq}\cup\Delta_{\simeq}\vdash_{\forall} s_n\simeq t_n}\ (Ax)$$

$$\overline{\Gamma,\Lambda,\Delta\to\varphi\cdot\top}\ (\Lambda) \qquad \overline{\Gamma\to s{\simeq}t\cdot\Gamma_{\simeq}\vdash_{\forall} s{\simeq}t}\ (\simeq)$$

$$\frac{\Gamma,\varphi,\psi,\Delta\to\chi\cdot\mathcal{C}}{\Gamma,\varphi\wedge\psi,\Delta\to\chi\cdot\mathcal{C}}\ (\wedge\to) \qquad \frac{\Gamma\to\varphi\cdot\mathcal{C}_1\quad \Gamma\to\psi\cdot\mathcal{C}_2}{\Gamma\to\varphi\wedge\psi\cdot\mathcal{C}_1\wedge\mathcal{C}_2}\ (\to\wedge)$$

$$\frac{\Gamma,\varphi,\Delta\to\chi\cdot\mathcal{C}_1\quad \Gamma,\psi,\Delta\to\chi\cdot\mathcal{C}_2}{\Gamma,\varphi\vee\psi,\Delta\to\chi\cdot\mathcal{C}_1\wedge\mathcal{C}_2}\ (\vee\to) \qquad \frac{\Gamma\to\varphi\cdot\mathcal{C}}{\Gamma\to\varphi\vee\psi\cdot\mathcal{C}}\ (\to\vee_1) \quad \frac{\Gamma\to\psi\cdot\mathcal{C}}{\Gamma\to\varphi\vee\psi\cdot\mathcal{C}}\ (\to\vee_2)$$

$$\frac{\Gamma,\psi,\Delta\to\chi\cdot\mathcal{C}_1\quad \Gamma,\varphi\supset\psi,\Delta\to\varphi\cdot\mathcal{C}_2}{\Gamma,\varphi\supset\psi,\Delta\to\chi\cdot\mathcal{C}_1\wedge\mathcal{C}_2}\ (\supset\to) \qquad \frac{\varphi,\Gamma\to\psi\cdot\mathcal{C}}{\Gamma\to\varphi\supset\psi\cdot\mathcal{C}}\ (\to\supset)$$

$$\frac{\Gamma,\varphi\{y/x\},\forall x\varphi,\Delta\to\chi\cdot\mathcal{C}}{\Gamma,\forall x\varphi,\Delta\to\chi\cdot\exists y\mathcal{C}}\ (\forall\to) \qquad \frac{\Gamma\to\varphi\{y/x\}\cdot\mathcal{C}}{\Gamma\to\forall x\varphi\cdot\exists y(y\not\preceq\{v_1,\ldots,v_n\}\wedge\mathcal{C})}\ (\to\forall)$$

$$\frac{\Gamma,\varphi\{y/x\},\Delta\to\chi\cdot\mathcal{C}}{\Gamma,\exists x\varphi,\Delta\to\chi\cdot\exists y(y\not\preceq\{v_1,\ldots,v_n\}\wedge\mathcal{C})}\ (\exists\to) \qquad \frac{\Gamma\to\varphi\{y/x\}\cdot\mathcal{C}}{\Gamma\to\exists x\varphi\cdot\exists y\mathcal{C}}\ (\to\exists)$$

In the rule (Ax), A is a predicate symbol different from equality. In the rules $(\forall\to)$–$(\to\exists)$ the variable y has no free occurrences in the sequent in the conclusion of the rules. In the rule $(\to\forall)$, $v_1,\ldots,v_n$ are all free variables of $\Gamma,\forall x\varphi$. In the rule $(\exists\to)$, $v_1,\ldots,v_n$ are all free variables of $\Gamma,\exists x\varphi,\Delta,\chi$.

Figure 4.1: Calculus $\mathbf{LJ}_c^{\simeq}$

4. $\sigma\models\mathcal{C}_1\wedge\mathcal{C}_2$ iff $\sigma\models\mathcal{C}_1$ and $\sigma\models\mathcal{C}_2$;
5. $\sigma\models\exists x\mathcal{C}$ iff there is a substitution τ such that $\tau\models\mathcal{C}$ and $y\tau=y\sigma$ for every variable y different from x.

Constraints $\mathcal{C}_1$ and $\mathcal{C}_2$ are *equivalent* iff for every substitution σ we have $\sigma\models\mathcal{C}_1$ iff $\sigma\models\mathcal{C}_2$. A constraint $\mathcal{C}$ is *satisfiable* iff there is a substitution σ satisfying $\mathcal{C}$.

4.2 The calculus $\mathbf{LJ}_c^{\simeq}$

In this section we introduce the calculus $\mathbf{LJ}_c^{\simeq}$ of *constrained sequents.* Before giving its inference rules, we introduce the following notation. For a sequence of formulas Γ, denote by $\Gamma_{\simeq}$ the set of formulas $\{s\simeq t \mid s\simeq t\in\Gamma\}$.

Definition 4.3 A *constrained sequent* is an expression $S\cdot\mathcal{C}$ where S is a sequent, $\mathcal{C}$ is a constraint. The *constraint calculus* $\mathbf{LJ}_c^{\simeq}$ of constrained sequents is shown in Figure 4.1.

The notions of a skeleton and a weak skeleton for $\mathbf{LJ}_c^{\simeq}$-derivations are similar to those of $\mathbf{LJ}^{\simeq}$-derivations.

Consider two examples of derivations in $\mathbf{LJ}_c^{\simeq}$:

Example 4.4 The following is a derivation in $\mathbf{LJ}_c^{\simeq}$ of the formula $\forall x(x\simeq a \vee x\simeq b \supset \exists y(f(x,y)\simeq b)) \supset \exists u\exists v\exists w(f(f(u,v),w)\simeq b)$ (see Example 3.10) with a suitable constraint. As in Example 3.10, we denote by φ the formula $\forall x(x\simeq a \vee x\simeq b \supset \exists y(f(x,y)\simeq b))$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi \to f(f(u,v),w)\simeq b \cdot \vdash_\forall f(f(u,v),w)\simeq b}\,(\simeq)}{\varphi \to \exists w(f(f(u,v),w)\simeq b) \cdot \exists w(\vdash_\forall f(f(u,v),w)\simeq b)}\,(\to\exists)}{\varphi \to \exists v\exists w(f(f(u,v),w)\simeq b) \cdot \exists v\exists w(\vdash_\forall f(f(u,v),w)\simeq b)}\,(\to\exists)}{\varphi \to \exists u\exists v\exists w(f(f(u,v),w)\simeq b) \cdot \exists u\exists v\exists w(\vdash_\forall f(f(u,v),w)\simeq b)}\,(\to\exists)}{\to \varphi \supset \exists u\exists v\exists w(f(f(u,v),w)\simeq b) \cdot \exists u\exists v\exists w(\vdash_\forall f(f(u,v),w)\simeq b)}\,(\to\supset)$$

The resulting constraint $\exists u\exists v\exists w(\vdash_\forall f(f(u,v),w)\simeq b)$ of this derivation is evidently unsatisfiable.

Example 4.5 Another proof of this formula (with the same skeleton as that of the derivations of Example 3.10) is

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{f(x_1,y_1)\simeq b, f(x_2,y_2)\simeq b, \varphi \to f(f(u,v),w)\simeq b \cdot \mathcal{C}_1}\,(\simeq)}{f(x_1,y_1)\simeq b, f(x_2,y_2)\simeq b, \varphi \to \exists w(f(f(u,v),w)\simeq b) \cdot \mathcal{C}_2}\,(\to\exists)}{f(x_1,y_1)\simeq b, \exists y(f(x_2,y)\simeq b), \varphi \to \exists w(f(f(u,v),w)\simeq b) \cdot \mathcal{C}_4}\,(\exists\to) \quad \dfrac{\dfrac{}{\cdots \to x_2\simeq b \cdot \mathcal{C}_3}\,(\simeq)}{\cdots \to x_2\simeq a \vee x_2\simeq b \cdot \mathcal{C}_3}\,(\to\vee_2)}{f(x_1,y_1)\simeq b, x_2\simeq a \vee x_2\simeq b \supset \exists y(f(x_2,y)\simeq b), \varphi \to \exists w(f(f(u,v),w)\simeq b) \cdot \mathcal{C}_5}\,(\supset\to)}{f(x_1,y_1)\simeq b, \varphi \to \exists w(f(f(u,v),w)\simeq b) \cdot \mathcal{C}_6}\,(\forall\to)}{f(x_1,y_1)\simeq b, \varphi \to \exists v\exists w(f(f(u,v),w)\simeq b) \cdot \mathcal{C}_7}\,(\to\exists)}{\exists y(f(x_1,y)\simeq b), \varphi \to \exists v\exists w(f(f(u,v),w)\simeq b) \cdot \mathcal{C}_9}\,(\exists\to) \quad \dfrac{\dfrac{}{\cdots \to x_1\simeq a \cdot \mathcal{C}_8}\,(\simeq)}{\cdots \to x_1\simeq a \vee x_1\simeq b \cdot \mathcal{C}_8}\,(\to\vee_1)}{x_1\simeq a \vee x_1\simeq b \supset \exists y(f(x_1,y)\simeq b), \varphi \to \exists v\exists w(f(f(u,v),w)\simeq b) \cdot \mathcal{C}_{10}}\,(\supset\to)}{\varphi \to \exists v\exists w(f(f(u,v),w)\simeq b) \cdot \mathcal{C}_{11}}\,(\forall\to)}{\varphi \to \exists u\exists v\exists w(f(f(u,v),w)\simeq b) \cdot \mathcal{C}_{12}}\,(\to\exists)}{\to \varphi \supset \exists u\exists v\exists w(f(f(u,v),w)\simeq b) \cdot \mathcal{C}_{12}}\,(\to\supset)$$

Here the constraints $\mathcal{C}_1$–$\mathcal{C}_{12}$ are as follows:

$$\begin{array}{lcl}
\mathcal{C}_1 & \rightleftharpoons & f(x_1,y_1)\simeq b, f(x_2,y_2)\simeq b \vdash_\forall f(f(u,v),w)\simeq b \\
\mathcal{C}_2 & \rightleftharpoons & \exists w(f(x_1,y_1)\simeq b, f(x_2,y_2)\simeq b \vdash_\forall f(f(u,v),w)\simeq b) \\
\mathcal{C}_3 & \rightleftharpoons & f(x_1,y_1)\simeq b \vdash_\forall x_2\simeq b \\
\mathcal{C}_4 & \rightleftharpoons & \exists y_2(y_2 \not\precsim \{x_1,y_1,x_2,u,v\} \wedge \exists w(f(x_1,y_1)\simeq b, f(x_2,y_2)\simeq b \vdash_\forall f(f(u,v),w)\simeq b)) \\
\mathcal{C}_5 & \rightleftharpoons & \mathcal{C}_4 \wedge \mathcal{C}_3 \\
\mathcal{C}_6 & \rightleftharpoons & \exists x_2(\mathcal{C}_4 \wedge \mathcal{C}_3) \\
\mathcal{C}_7 & \rightleftharpoons & \exists v\exists x_2(\mathcal{C}_4 \wedge \mathcal{C}_3) \\
\mathcal{C}_8 & \rightleftharpoons & \vdash_\forall x_1\simeq a \\
\mathcal{C}_9 & \rightleftharpoons & \exists y_1(y_1 \not\precsim \{x_1,u\} \wedge \exists v\exists x_2(\mathcal{C}_4 \wedge \mathcal{C}_3)) \\
\mathcal{C}_{10} & \rightleftharpoons & \exists y_1(y_1 \not\precsim \{x_1,u\} \wedge \exists v\exists x_2(\mathcal{C}_4 \wedge \mathcal{C}_3)) \wedge \vdash_\forall x_1\simeq a \\
\mathcal{C}_{11} & \rightleftharpoons & \exists x_1(\exists y_1(y_1 \not\precsim \{x_1,u\} \wedge \exists v\exists x_2(\mathcal{C}_4 \wedge \mathcal{C}_3)) \wedge \vdash_\forall x_1\simeq a) \\
\mathcal{C}_{12} & \rightleftharpoons & \exists u\exists x_1(\exists y_1(y_1 \not\precsim \{x_1,u\} \wedge \exists v\exists x_2(\mathcal{C}_4 \wedge \mathcal{C}_3)) \wedge \vdash_\forall x_1\simeq a)
\end{array}$$

The resulting constraint $\mathcal{C}_{12}$ of this derivation is satisfiable. To establish this, we first note that $\mathcal{C}_{12}$ is satisfiable iff such is the following constraint $\mathcal{C}$ obtained from $\mathcal{C}_{12}$ be removing all quantifiers:

$$\begin{array}{l} f(x_1,y_1)\simeq b, f(x_2,y_2)\simeq b \vdash_\forall f(f(u,v),w)\simeq b \wedge \\ f(x_1,y_1)\simeq b \vdash_\forall x_2\simeq b \wedge \\ y_2 \not\preceq \{x_1,y_1,x_2,u,v\} \wedge \\ \vdash_\forall x_1\simeq a \wedge \\ y_1 \not\preceq \{x_1,u\} \end{array}$$

This quantifier-free constraint is satisfied by the substitution $\{a/u, a/x_1, y_1/v, b/x_2, y_2/w\}$.

The following statement connects the derivability in $\mathbf{LJ}^{\simeq}$ with the derivability in $\mathbf{LJ}_c^{\simeq}$:

Theorem 4.6 Let $\Gamma \to \varphi$ be a sequent, θ be a substitution and $\mathcal{S}$ be a skeleton (respectively, weak skeleton). Then the following conditions are equivalent:

1. There is a derivation of $\Gamma\theta \to \varphi\theta$ in $\mathbf{LJ}^{\simeq}$ with the skeleton (respectively, weak skeleton) $\mathcal{S}$;
2. There is a constraint $\mathcal{C}$ and a derivation of $\Gamma \to \varphi \cdot \mathcal{C}$ in $\mathbf{LJ}_c^{\simeq}$ with the skeleton (respectively, weak skeleton) $\mathcal{S}$ such that $\theta \models \mathcal{C}$.

Proof. We only prove the claim for skeletons, then the result for weak skeletons will be a straightforward consequence. By Theorem 3.11, we can restrict ourselves to regular $\mathbf{LJ}^{\simeq}$-derivations. The proof is carried out by induction on the regular derivations in $\mathbf{LJ}^{\simeq}$ (respectively, derivations in $\mathbf{LJ}_c^{\simeq}$). Consider several cases depending on the last inference rule applied. In all cases the condition on the skeletons to be the same is straightforward.

1. The $\mathbf{LJ}^{\simeq}$-derivation of a sequent $\Gamma\theta \to s\theta\simeq t\theta$ consists of an application of the rule $(\simeq)$ followed by any number of $(\simeq_1)$ or $(\simeq_2)$. By Lemma 3.2, θ is a solution to the rigid equation $\Gamma_{\simeq} \vdash_\forall s\simeq t$. The following is the required $\mathbf{LJ}_c^{\simeq}$-derivation:

$$\frac{}{\Gamma \to s\simeq t \cdot \Gamma_{\simeq} \vdash_\forall s\simeq t}\ (\simeq)$$

2. The $\mathbf{LJ}_c^{\simeq}$-derivation consists of one application of $(\simeq)$:

$$\frac{}{\Gamma \to s\simeq t \cdot \Gamma_{\simeq} \vdash_\forall s\simeq t}\ (\simeq)$$

   Suppose $\theta \models \Gamma_{\simeq} \vdash_\forall s\simeq t$. It follows from Lemma 3.2 that there is an $\mathbf{LJ}^{\simeq}$-derivation of the sequent $\Gamma\theta \to s\theta\simeq t\theta$ consisting only of applications of the rules $(\simeq)$, $(\simeq_1)$ and $(\simeq_2)$.

3. The last rule applied in the $\mathbf{LJ}^{\simeq}$-derivation is $(\to \wedge)$. Then the $\mathbf{LJ}^{\simeq}$-derivation has the form

$$\frac{\begin{array}{c}\Pi_1\\ \Gamma\theta \to \varphi\theta\end{array} \quad \begin{array}{c}\Pi_2\\ \Gamma\theta \to \psi\theta\end{array}}{\Gamma\theta \to \varphi\theta \wedge \psi\theta}\ (\to \wedge)$$

   By the induction hypothesis, there are $\mathbf{LJ}_c^{\simeq}$-derivations Π_1' and Π_2' of constrained sequents $\Gamma \to \varphi \cdot \mathcal{C}_1$ and $\Gamma \to \psi \cdot \mathcal{C}_2$, respectively, such that $\theta \models \mathcal{C}_1$ and $\theta \models \mathcal{C}_2$. By the definition of the constraint satisfaction, $\theta \models \mathcal{C}_1 \wedge \mathcal{C}_2$. Define $\mathcal{C}$ as $\mathcal{C}_1 \wedge \mathcal{C}_2$. Then the required $\mathbf{LJ}_c^{\simeq}$-derivation is

$$\frac{\begin{array}{cc}\Pi_1' & \Pi_2' \\ \Gamma \to \varphi \cdot \mathcal{C}_1 & \Gamma \to \psi \cdot \mathcal{C}_2\end{array}}{\Gamma \to \varphi \wedge \psi \cdot \mathcal{C}_1 \wedge \mathcal{C}_2}\ (\to \wedge)$$

4. The last rule applied in the $\mathbf{LJ}_c^{\simeq}$-derivation is $(\to \wedge)$. Then the $\mathbf{LJ}_c^{\simeq}$-derivation has the form

$$\frac{\begin{array}{cc}\Pi_1 & \Pi_2 \\ \Gamma \to \varphi \cdot \mathcal{C}_1 & \Gamma \to \psi \cdot \mathcal{C}_2\end{array}}{\Gamma \to \varphi \wedge \psi \cdot \mathcal{C}_1 \wedge \mathcal{C}_2}\ (\to \wedge)$$

Let $\theta \models \mathcal{C}_1 \wedge \mathcal{C}_2$. Then $\theta \models \mathcal{C}_1$ and $\theta \models \mathcal{C}_2$. By the induction hypothesis, there are $\mathbf{LJ}^{\simeq}$-derivations Π_1' and Π_2' of the sequents $\Gamma\theta \to \varphi\theta$ and $\Gamma\theta \to \psi\theta$, respectively. Then the required $\mathbf{LJ}^{\simeq}$-derivation is

$$\frac{\begin{array}{cc}\Pi_1' & \Pi_2' \\ \Gamma\theta \to \varphi\theta & \Gamma\theta \to \psi\theta\end{array}}{\Gamma\theta \to \varphi\theta \wedge \psi\theta}\ (\to \wedge)$$

5. The last rule applied in the $\mathbf{LJ}^{\simeq}$-derivation is $(\to \forall)$. Let y be the eigenvariable of this rule and $\Sigma \to \psi$ be the premise of the rule. Then it is easy to see that for any variable z not occurring in Σ or ψ, the sequent $\Sigma\{y/z\} \to \psi\{y/z\}$ is also derivable in $\mathbf{LJ}^{\simeq}$ with the same skeleton. Hence, without loss of generality we can assume that the eigenvariable does not occur in Γ or φ. Then the $\mathbf{LJ}^{\simeq}$-derivation has the form

$$\frac{\begin{array}{c}\Pi \\ \Gamma\theta' \to \varphi\{y/x\}\theta'\end{array}}{\Gamma\theta \to (\forall x\varphi)\theta}\ (\to \forall)$$

where θ' is a substitution such that $v\theta = v\theta'$ for all variables v different from y and $y\theta' = y$. By the induction hypothesis, there is an $\mathbf{LJ}_c^{\simeq}$-derivation Π' of a constrained sequent $\Gamma \to \varphi\{y/x\} \cdot \mathcal{C}$ such that $\theta' \models \mathcal{C}$. Let $v_1, \ldots, v_m$ be all free variables of $\Gamma, \forall x\varphi$. Since y does not occur in Γ, φ and $y\theta' = y$, then $\theta' \models y \not\preceq \{v_1, \ldots, v_m\} \wedge \mathcal{C}$. It follows that $\theta \models \exists y(y \not\preceq \{v_1, \ldots, v_m\} \wedge \mathcal{C})$. The required $\mathbf{LJ}_c^{\simeq}$-derivation is

$$\frac{\begin{array}{c}\Pi' \\ \Gamma \to \varphi\{y/x\} \cdot \mathcal{C}\end{array}}{\Gamma \to \forall x\varphi \cdot \exists y(y \not\preceq \{v_1, \ldots, v_m\} \wedge \mathcal{C})}\ (\to \forall)$$

6. The last rule applied in the $\mathbf{LJ}_c^{\simeq}$-derivation is $(\to \forall)$. Then the $\mathbf{LJ}_c^{\simeq}$-derivation has the form

$$\frac{\begin{array}{c}\Pi \\ \Gamma \to \varphi\{y/x\} \cdot \mathcal{C}\end{array}}{\Gamma \to \forall x\varphi \cdot \exists y(y \not\preceq \{v_1, \ldots, v_n\} \wedge \mathcal{C})}\ (\to \forall)$$

Let $\theta \models \exists y(y \not\preceq \{v_1, \ldots, v_n\} \wedge \mathcal{C})$. By the definition of the constraint satisfaction, there is a substitution θ' such that $v\theta' = v\theta$ for all variables different from y and $\theta' \models y \not\preceq \{v_1, \ldots, v_m\} \wedge \mathcal{C}$. It means that $\theta' \models \mathcal{C}$ and $y\theta'$ is a variable not occurring in $v_1\theta', \ldots, v_m\theta'$. By the induction hypothesis, there is derivation Π' in $\mathbf{LJ}^{\simeq}$ of the sequent $\Gamma\theta' \to \varphi\{y/x\}\theta'$. Then the required $\mathbf{LJ}^{\simeq}$-derivation is

$$\frac{\begin{matrix}\Pi' \\ \Gamma\theta' \to \varphi\{y/x\}\theta'\end{matrix}}{\Gamma\theta \to (\forall x\varphi)\theta}$$

The other cases are similar.

□

The following two theorems are straightforward consequences of Theorem 4.6:

Theorem 4.7 Let S be a closed sequent and $\mathcal{S}$ be a skeleton (respectively, a weak skeleton). Then S has a derivation in $\mathbf{LJ}^{\simeq}$ with the skeleton (respectively, the weak skeleton) $\mathcal{S}$ iff there is a satisfiable constraint $\mathcal{C}$ such that $S \cdot \mathcal{C}$ has a derivation in $\mathbf{LJ}_c^{\simeq}$ with the skeleton (respectively, the weak skeleton) $\mathcal{S}$.

Theorem 4.8 Let S be a closed sequent. Then S is derivable in $\mathbf{LJ}^{\simeq}$ iff there is a satisfiable constraint $\mathcal{C}$ such that $S \cdot \mathcal{C}$ is derivable in $\mathbf{LJ}_c^{\simeq}$.

Note that the set of constraints $\mathcal{C}$ such that $S \cdot \mathcal{C}$ is derivable in $\mathbf{LJ}_c^{\simeq}$ with a skeleton $\mathcal{S}$ is uniquely defined by the skeleton $\mathcal{S}$ up to renaming of bound variables. Thus, the proof-search in intuitionistic logic can be considered as consisting of two parts: constructing a skeleton and the constraint satisfaction. The two parts should not necessarily be processed in this order, as the constraint satisfaction algorithm can try to check constraints after each step of the skeleton construction.

According to Theorem 3.14, the skeleton instantiation problem is undecidable which causes doubts about the efficiency of such procedures. In classical logic, there are many complete methods for reasoning with equality which do not use simultaneous rigid E-unification. However, for intuitionistic logic, there is a simple reduction of simultaneous rigid E-unifiability to the derivability problem, and hence handling of simultaneous rigid E-unification is inevitable for designing a complete procedure. In addition, some special cases of simultaneous rigid E-unification are decidable (see Degtyarev, Matiyasevich and Voronkov [3]) (for example, the function-free case is NP-complete) which allows one to use decision procedures for these fragments.

Section 5

Constraint satisfiability and simultaneous rigid E-unification

The main result of this section is that the skeleton instantiation problem is polynomial-time equivalent to simultaneous rigid E-unifiability. Since both problems are undecidable, it shows close relationships between the two problems. In fact, we give structure-preserving translations between the two problems.

We start with several technical definitions and statements. Let Σ be any signature containing at least one constant. *We assume that all terms of this section are terms in* Σ. For any signature Δ, we denote by Δ^* an extension of Δ by a countable set of new constants $c_1, c_2 \ldots$.

Note that any system or rigid equations $\{R_1, \ldots, R_n\}$ is equivalent to the constraint $R_1 \wedge \ldots \wedge R_n$ in the sense that any solution to $\{R_1, \ldots, R_n\}$ satisfies $R_1 \wedge \ldots \wedge R_n$ and vice versa. Thus, simultaneous rigid E-unification can be regarded as a special case of constraint satisfaction.

We call a constraint $\mathcal{C}$ *refined* iff for any two different occurrences of quantifiers $\exists x$ and $\exists y$ in $\mathcal{C}$ we have $x \neq y$. Evidently, any constraint can be transformed to an equivalent refined one by renaming bound variables. *For the rest of this section we assume that all constraints we consider are refined.*

We say that a constraint $\mathcal{C}'$ is obtained from a constraint $\mathcal{C}$ be *quantifier removal* iff $\mathcal{C}'$ is a quantifier-free constraint obtained from $\mathcal{C}$ by removal of all quantifiers $\exists x$. For example, if $\mathcal{C}$ is $\exists z(z \simeq a \wedge \exists y(y \simeq f(u)))$, then after quantifier removal we obtain $z \simeq a \wedge y \simeq f(u)$.

Lemma 5.1 Let $\mathcal{C}$ be a refined constraint and $\mathcal{C}'$ be obtained from $\mathcal{C}$ by quantifier removal. Then $\mathcal{C}$ and $\mathcal{C}'$ are equi-satisfiable.

Proof. Straightforward. □

We implicitly used this lemma when we established the constraint satisfiability in Example 4.5.

Definition 5.2 (Special constraint)
A constraint $\mathcal{C}$ is called *special* iff any occurrence of $\ldots \not\preceq \{\ldots\}$ in $\mathcal{C}$ is an occurrence in a subformula of $\mathcal{C}$ of the form $\exists x(x \not\preceq \{v_1, \ldots, v_n\} \wedge \mathcal{C}')$, where $v_1, \ldots, v_n$ are variables and all free variables of $\mathcal{C}'$ are among $x, v_1, \ldots, v_n$.

Note that for any constraint sequent $S \cdot \mathcal{C}$ derivable in $\mathbf{LJ}_c^{\simeq}$, the constraint $\mathcal{C}$ is special.

We shall introduce some technical definitions and prove several technical lemmas.

Definition 5.3 (Equivalent substitutions)
Let X be a set of variables and θ_1, θ_2 be substitutions. Then θ_1 and θ_2 are called *equivalent w.r.t. X*, denoted $\theta_1 \equiv_X \theta_2$, iff there are two substitutions τ_1, τ_2 such that for every variable $x \in X$ we have $x\theta_1 = x\theta_2\tau_2$ and $x\theta_1\tau_1 = x\theta_2$.

Lemma 5.4 Let $\theta_1 \equiv_X \theta_2$ and $\mathcal{C}$ be a constraint all whose free variables are among X. Then $\theta_1 \models \mathcal{C}$ iff $\theta_2 \models \mathcal{C}$.

Proof. By straightforward induction on the structure of $\mathcal{C}$. □

Lemma 5.5 Let $\mathcal{C}$ be a constraint all whose free variables are among $x, v_1, \ldots, v_n$ and θ be any substitution such that $\theta \models x \not\preceq \{v_1, \ldots, v_n\} \wedge \mathcal{C}$. Let y be any variable not occurring in $x\theta, v_1\theta, \ldots, v_n\theta$ and the substitution θ' be defined as follows:

$$\theta'(z) \rightleftharpoons \begin{cases} \theta(z), & \text{if } z \neq x \\ y & \text{otherwise} \end{cases}$$

Then $\theta' \models x \not\preceq \{v_1, \ldots, v_n\} \wedge \mathcal{C}$.

Proof. Since $x\theta$ is a variable not occurring in $v_1\theta, \ldots, v_n\theta$, we have $\theta \equiv_{\{x, v_1, \ldots, v_n\}} \theta'$. Then apply Lemma 5.4. □

Lemma 5.6 Let $\mathcal{C}$ be a satisfiable special refined constraint. Let $\mathcal{C}'$ be the quantifier-free constraint obtained from $\mathcal{C}$ by quantifier removal. Let $\{x_1, \ldots, x_m\}$ be the set of all variables x such that $\mathcal{C}'$ contains a constraint of the form $x \not\preceq \{t_1, \ldots, t_n\}$. Then $\mathcal{C}'$ has a solution θ with the following property:

1. For any variable y occurring in $\mathcal{C}'$ we have $y\theta \in T_\Sigma(\{x_1, \ldots, x_m\})$;
2. For every $i \in \{1, \ldots, m\}$ we have $x_i\theta = x_i$.

Proof. Let σ be any substitution satisfying $\mathcal{C}'$. Define $Y \rightleftharpoons \{x_1\sigma, \ldots, x_m\sigma\}$. Since $\sigma \models \mathcal{C}'$, all terms in Y are variables. By Lemma 5.5 we can assume that the variables $x_1\sigma, \ldots, x_m\sigma$ are pairwise disjoint. Let $Y = \{y_1, \ldots, y_m\}$. Take any constant $c \in \Sigma$ and define the substitution τ as follows: for any variable x,

$$x\tau \rightleftharpoons \begin{cases} x_i, & \text{if } x = y_i \\ c, & \text{if } x \in var(\mathcal{C}') \cup var(ran(\sigma)) \setminus Y \\ x, & \text{otherwise} \end{cases}$$

Finally, define $\theta \rightleftharpoons \sigma\tau$. It is easy to check that θ satisfies the claim. □

Let Δ be any finite set of function symbols with at least one constant, c be any constant in Δ and t be a term not necessarily in the signature Δ. Define the rigid equation

$$\mathcal{R}_{t,\Delta} \rightleftharpoons \{f(c, \ldots, c) \simeq c \mid f \in \Delta\} \vdash_\forall t \simeq c$$

Lemma 5.7 For every substitution θ, θ is a solution to $\mathcal{R}_{t,\Delta}$ iff $t\theta \in T_\Delta$.

Proof. Obvious. □

Theorem 5.8 Simultaneous rigid E-unifiability in the signature Σ^* is polynomial-time equivalent to the satisfiability problem for special constraints in the signature Σ^*.

Proof. As we noted, simultaneous rigid E-unifiability is a special case of constraint satisfiability. It remains to show a polynomial-time reduction of constraint satisfiability to simultaneous rigid E-unifiability.

Let $\mathcal{C}$ be a special constraint. Without loss of generality we can assume that $\mathcal{C}$ is refined. By Lemma 5.1 we can assume that $\mathcal{C}$ is quantifier-free. Let $\{x_1, \dots, x_m\}$ be the set of all variables x such that $\mathcal{C}$ contains a constraint of the form $x \not\preceq \{t_1, \dots, t_n\}$. Let $c_1, \dots, c_m$ be constants occurring in Σ^* but not in Σ. For any $i \in \{1, \dots, n\}$ denote by Σ_{-i} the signature $\Sigma \cup \{c_1, \dots, c_{i-1}, c_{i+1}, \dots, c_n\}$.

Let $R_\mathcal{C}$ be the system of rigid equations consisting of

1. All rigid equations occurring in $\mathcal{C}$;
2. For every $i \in \{1, \dots, m\}$, the rigid equation $\vdash_\forall x_i \simeq c_i$;
3. For every constraint $x_i \not\preceq \{v_1, \dots, v_n\}$ occurring in $\mathcal{C}$, the set of rigid equations $\mathcal{R}_{v_j, \Sigma_{-i}}$, where $j \in \{1, \dots, n\}$.

Obviously, $R_\mathcal{C}$ can be constructed by $\mathcal{C}$ in polynomial time. We prove that $\mathcal{C}$ is satisfiable iff $R_\mathcal{C}$ is solvable.

Define the substitution $\tau \rightleftharpoons \{c_1/x_1, \dots, c_m/x_m\}$. We prove the following claim:

(I) For any substitution θ the following conditions are equivalent:

 (a) $\theta \models \mathcal{C}$ and θ satisfies the conditions of Lemma 5.6;
 (b) $\theta\tau$ is a solution to $R_\mathcal{C}$.

 We only prove the ($\Rightarrow$) direction. The reverse direction is similar. Suppose that $\theta \models \mathcal{C}$ and θ satisfies the conditions of Lemma 5.6.

 (a) Since $\theta \models \mathcal{C}$, evidently $\theta\tau$ satisfies all rigid equations in $\mathcal{C}$.
 (b) Consider any $i \in \{1, \dots, m\}$. Since θ satisfies the conditions of Lemma 5.6, we have $x_i\theta = x_i$. Hence, $x_i\theta\tau = c_i$. Then $\theta\tau \models\vdash_\forall x_i \simeq c_i$.
 (c) Let $x_i \not\preceq \{v_1, \dots, v_n\}$ be a constraint occurring in $\mathcal{C}$. Since θ satisfies the conditions of Lemma 5.6, we have $x_i\theta = x_i$. Hence, x_i does not occur in $v_1\theta, \dots, v_n\theta$. Since all $v_j\theta$ are terms in $T_\Sigma(\{x_1, \dots, x_m\})$, we have that c_i does not occur in $v_1\theta\tau, \dots, v_n\theta\tau$. Hence, for any $j \in \{1, \dots, n\}$ we have $v_i\theta\tau \in T_{\Sigma_{-i}}$. By Lemma 5.7, $\theta\tau \models \mathcal{R}_{v_j, \Sigma_{-i}}$.

Claim (I) is proven.

Suppose now that $\mathcal{C}$ is satisfiable. By Lemma 5.6, there is substitution θ satisfying conditions of this lemma and such that $\theta \models \mathcal{C}$. By claim (I), $R_\mathcal{C}$ is solvable.

Let $R_\mathcal{C}$ be solvable and σ be any solution to $R_\mathcal{C}$. Take any substitution θ such that $\theta\tau = \sigma$. By claim (I) we have $\theta \models \mathcal{C}$. We have shown that $\mathcal{C}$ is satisfiable iff $R_\mathcal{C}$ is solvable. Thus, the satisfiability problem for special constraints is polynomial-time reducible to simultaneous rigid E-unifiability. □

The aim of this theorem was to show the close connection between constraint satisfaction and simultaneous rigid E-unification. Of course in practice, instead of reduction of constraint satisfaction to simultaneous rigid E-unification, one can develop special algorithms for constraint satisfaction hoping that they may be more "efficient" or more intuitive compared to the one using the above reduction to simultaneous rigid E-unification.

Combining Theorems 4.6 and 5.8, we obtain

Theorem 5.9 The skeleton instantiation problem in the signature Σ^* is polynomial-time equivalent to simultaneous rigid E-unifiability in the signature Σ^*.

This theorem is also true for classical logic, if we change the system $\mathbf{LJ}^{\simeq}$ to the corresponding classical system allowing for more than one formula in the succedent. However, for classical logic we cannot show a straightforward reduction of simultaneous rigid E-unification to the provability problem. Indeed, there are many methods of automatic theorem proving in classical logic with equality not using simultaneous rigid E-unification. Our results show that the (direct or indirect) use of simultaneous rigid E-unification is unavoidable in theorem proving in intuitionistic logic with equality.

Theorem 5.9 has several important consequences related to the skeleton instantiation problem. Although simultaneous rigid E-unifiability is, in general, undecidable, its undecidability is only known for the case when the signature Σ in which formulas are written contains binary function symbols (see proofs of the undecidability by Degtyarev and Voronkov [5, 6], Plaisted [29] and Veanes [36] for an overview of such proofs). In [2, 3] Degtyarev, Matiyasevich and Voronkov proved that simultaneous rigid E-unifiability in the signatures having at most one unary function symbol and no function symbols of arity ≥ 2 is decidable which implies the following result:

Theorem 5.10 Let Σ be a signature consisting of any number of constants and at most one unary function symbol. The following problems restricted to formulas of the signature Σ are decidable:

1. Simultaneous rigid E-unifiability;
2. The weak skeleton instantiation problem;
3. The skeleton instantiation problem.

Proof. For simultaneous rigid E-unifiability in Σ^* it was proven in Degtyarev, Matiyasevich and Voronkov [2, 3]. Theorem 5.9 implies that the skeleton instantiation problem in this signature is decidable. Since any instance of the weak skeleton instantiation problem can be effectively reduced to a disjunction of instances of the skeleton instantiation problem, the weak skeleton instantiation problem for this signature is decidable. □

Section 6

Conclusion and related work

There are not so many papers on intuitionistic logic with equality. The decidability problems for intuitionistic logic with equality are studied in Lifschitz [18], Mints [25], and Orevkov [27]. Lifschitz [18] proves the undecidability of some systems of intuitionistic equality. Mints [25] introduces a system of Skolem functions for formulas of intuitionistic logic restricting the application of quantifier rules. Orevkov [27] gives a partial classification of decidable pseudo-prenex[1] fragments of intuitionistic logic with and without equality. All these papers do not use function symbols, except for constants. In [10] Degtyarev and Voronkov prove some decidability and complexity results for prenex formulas of intuitionistic logic with and without equality.

Voda and Komara [37] consider so-called *Herbrand skeletons* (formulas obtained after a fixed number of quantifier duplications in a prenex skolemized formula) and claim that the corresponding skeleton instantiation problem is undecidable.

Tammet [35] implemented a theorem prover for intuitionistic logic based on the inverse method. Currently, the prover does not have equality, but Tammet is going to include equality as well (private communication). Our results provide a basis for including equality in such provers. Sahlin, Franzén and Haridi [32] implemented a theorem prover for intuitionistic logic where a non-standard formalization of equality is used. For example, in their logical system the formula $a \simeq b \supset c \simeq d$ is provable.

The results of our paper explain the (so far) unsuccessful attempts to incorporate equality in intuitionistic logic. To add equality to proof procedures for intuitionistic logic one has to develop algorithms for simultaneous rigid E-unifiability. No such algorithms are known yet, except for ones based on a straightforward enumeration (see Petermann [28]).

Our results also show a fundamental difference between handling equality in proof procedures for classical and non-classical logics. For classical logic, a number of methods not using simultaneous rigid E-unification have been developed. For methods based on sequent calculi, the equality elimination method has been developed by Degtyarev and Voronkov [4, 8, 9]. Recently, Degtyarev and Voronkov [11] proved that an incomplete but terminating procedure for rigid E-unification gives a complete procedure for classical logic with equality [11]. It follows from the results of this paper that none of these methods is applicable to intuitionistic logic.

We did not give any concrete procedure for proof search modulo simultaneous rigid E-unification. In fact, it is easy to construct such a procedure using rules of our constraint calculus in the backward direction. Such procedures are standard in tableau-based theorem provers, see e.g. Shankar [34] or Lincoln and Shankar [20], with the exception that in presence of equality we cannot

[1] A *pseudo-prenex* is a finite sequence of $\forall x_i$, $\exists x_i$ and $\neg\neg$.

use (even dynamic) skolemization.

Our technique is applicable to non-classical logics, for example some modal logics.

Acknowledgments

I thank Anatoli Degtyarev for many helpful comments.

Bibliography

[1] S.R. Buss. *Bounded Arithmetic*, volume 3 of *Studies in Proof Theory.* Bibliopolis, Napoly, 1986.

[2] A. Degtyarev, Yu. Matiyasevich, and A. Voronkov. Simultaneous rigid E-unification is not so simple. UPMAIL Technical Report 104, Uppsala University, Computing Science Department, April 1995.

[3] A. Degtyarev, Yu. Matiyasevich, and A. Voronkov. Simultaneous rigid E-unification and related algorithmic problems. To appear in *LICS'96*, 9 pages, 1996.

[4] A. Degtyarev and A. Voronkov. Equality elimination for semantic tableaux. UPMAIL Technical Report 90, Uppsala University, Computing Science Department, December 1994. To appear in *DISCO'96.*

[5] A. Degtyarev and A. Voronkov. Simultaneous rigid E-unification is undecidable. UPMAIL Technical Report 105, Uppsala University, Computing Science Department, May 1995. To appear in Theoretical Computer Science.

[6] A. Degtyarev and A. Voronkov. Reduction of second-order unification to simultaneous rigid E-unification. UPMAIL Technical Report 109, Uppsala University, Computing Science Department, June 1995.

[7] A. Degtyarev and A. Voronkov. A new procedural interpretation of Horn clauses with equality. In Leon Sterling, editor, *Proceedings of the Twelfth International Conference on Logic Programming*, pages 565–579. The MIT Press, 1995.

[8] A. Degtyarev and A. Voronkov. General connections via equality elimination. In M. De Glas and Z. Pawlak, editors, *Second World Conference on the Fundamentals of Artificial Intelligence (WOCFAI-95)*, pages 109–120, Paris, July 1995. Angkor.

[9] A. Degtyarev and A. Voronkov. Equality elimination for the inverse method and extension procedures. In C.S. Mellish, editor, *Proc. International Joint Conference on Artificial Intelligence (IJCAI)*, volume 1, pages 342–347, Montréal, August 1995.

[10] A. Degtyarev and A. Voronkov. Decidability problems for the prenex fragment of intuitionistic logic. To appear in *LICS'96*, 10 pages, 1996.

[11] A. Degtyarev and A. Voronkov. What you always wanted to know about rigid E-unification. To appear in *JELIA'96*, 20 pages, 1996.

[12] M. Fitting. *First Order Logic and Automated Theorem Proving.* Springer Verlag, New York, 1990.

[13] J.H. Gallier, S. Raatz, and W. Snyder. Theorem proving using rigid E-unification: Equational matings. In *Proc. IEEE Conference on Logic in Computer Science (LICS)*, pages 338–346. IEEE Computer Society Press, 1987.

[14] J.-Y. Girard. *Proof Theory and Logical Complexity.* Studies in Proof Theory. Bibliopolis, Napoly, 1987.

[15] S. Kanger. *Provability in Logic*, volume 1 of *Studies in Philosophy.* Almqvist and Wicksell, Stockholm, 1957.

[16] S. Kanger. A simplified proof method for elementary logic. In J. Siekmann and G. Wrightson, editors, *Automation of Reasoning. Classical Papers on Computational Logic*, volume 1, pages 364–371. Springer Verlag, 1983. Originally appeared in 1963.

[17] R.C.T. Lee and C.L. Chang. *Symbolic Logic and Mechanical Theorem Proving.* Academic Press, 1973.

[18] V. Lifschitz. The decidability problem for some constructive theories of equality (in Russian). *Zapiski Nauchnyh Seminarov LOMI*, 4:78–85, 1967.

[19] V. Lifschitz. Specialized forms of derivation in predicate calculus with equality and function symbols (in Russian). In *Trudy MIAN*, volume 98, pages 5–25. 1968. English translation in: Proc. Steklov Institute of Math., AMS, Providence, RI, 1971.

[20] P.D. Lincoln and N. Shankar. Proof search in first-order linear logic and other cut-free sequent calculi. In S. Abramski, editor, *Ninth Annual Symposium on Logic in Computer Science*, pages 282–291, Paris, France, 1994. IEEE Computer Society Press.

[21] D.W. Loveland. *Automated Theorem Proving: a Logical Basis.* North Holland, 1978.

[22] S.Yu. Maslov. An inverse method for establishing deducibility of nonprenex formulas of the predicate calculus. In J.Siekmann and G.Wrightson, editors, *Automation of Reasoning (Classical papers on Computational Logic)*, volume 2, pages 48–54. Springer Verlag, 1983.

[23] S.Yu. Maslov. An invertible sequential variant of constructive predicate calculus (in Russian). *Zapiski Nauchnyh Seminarov LOMI*, 4, 1967. English Translation in: Seminars in Mathematics: Steklov Math. Inst. 4, Consultants Bureau, NY-London, 1969, p.36–42.

[24] V.A. Matulis. On variants of classical predicate calculus with the unique deduction tree (in Russian). *Soviet Mathematical Doklady*, 148:768–770, 1963.

[25] G.E. Mints. Collecting terms in the quantifier rules of the constructive predicate calculus (in Russian). *Zapiski Nauchnyh Seminarov LOMI*, 4:78–85, 1967.

[26] V.P. Orevkov. A specialized form of derivation in Gentzen calculi and its applications (in Russian). *Zapiski Nauchnyh Seminarov LOMI*, 32:110–118, 1974.

[27] V.P. Orevkov. Solvable classes of pseudo-prenex formulas (in Russian). *Zapiski Nauchnyh Seminarov LOMI*, 60:109–170, 1976. English translation in: Journal of Soviet Mathematics.

[28] U. Petermann. A complete connection calculus with rigid E-unification. In *JELIA'94*, volume 838 of *Lecture Notes in Computer Science*, pages 152–166, 1994.

[29] D.A. Plaisted. Special cases and substitutes for rigid E-unification. Technical Report MPI-I-95-2-010, Max-Planck-Institut für Informatik, November 1995.

[30] G. Plotkin. Building-in equational theories. In B. Meltzer and D. Michie, editors, *Machine Intelligence*, volume 7, pages 73–90. Edinburgh University Press, 1972.

[31] G. Robinson and L.T. Wos. Paramodulation and theorem-proving in first order theories with equality. In Meltzer and Michie, editors, *Machine Intelligence*, volume 4, pages 135–150. Edinburgh University Press, Edinburgh, 1969.

[32] D. Sahlin, T. Franzén, and S. Haridi. An intuitionistic predicate logic theorem prover. *Journal of Logic and Computation*, 2(5):619–656, 1992.

[33] V.Yu. Sazonov. A logical approach to the problem "P=NP?". In *Mathematical Foundations of Computer Science*, volume 88 of *Lecture Notes in Computer Science*, pages 562–575, 1980.

[34] N. Shankar. Proof search in the intuitionistic sequent calculus. In D. Kapur, editor, *11th International Conference on Automated Deduction*, volume 607 of *Lecture Notes in Artificial Intelligence*, pages 522–536, Saratoga Springs, NY, USA, June 1992. Springer Verlag.

[35] T. Tammet. A resolution theorem prover for intuitionistic logic. To appear in *CADE'96*.

[36] M. Veanes. Uniform representation of recursively enumerable sets with simultaneous rigid E-unification. UPMAIL technical report, Uppsala University, Computing Science Department, 1996. To appear.

[37] P.J. Voda and J. Komara. On Herbrand skeletons. Technical report, Institute of Informatics, Comenius University Bratislava, July 1995.

[38] A. Voronkov. Theorem proving in non-standard logics based on the inverse method. In D. Kapur, editor, *11th International Conference on Automated Deduction*, volume 607 of *Lecture Notes in Artificial Intelligence*, pages 648–662, Saratoga Springs, NY, USA, June 1992. Springer Verlag.

[39] A. Voronkov. Proof-search in intuitionistic logic based on the constraint satisfaction. UPMAIL Technical Report 120, Uppsala University, Computing Science Department, January 1996.