UPMAIL Technical Report No. 151
February 11, 1998

Herbrand's theorem, automated reasoning and semantic tableaux

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 overview recent results related to Herbrand's theorem and tableau-like methods of automated deduction. Based on an analysis and discussion of these results, open problems are posed and new research directions are suggested.

Section 1

Introduction

Numerous results related to the Herbrand theorem and the foundations of semantics tableaux were obtained recently. These results shed a new light on the nature of such methods and computational complexity of several problems related to the Herbrand theorem. The aim of this paper is to overview these results, sketch new research directions and pose some open problems. We also prove several new results.

The main questions we ask in the paper are the following.

- Are tableaux and related methods inherently inefficient?
- In what cases are these methods efficient?
- In what cases and how can we increase efficiency of these methods?

This paper is structured as follows. In Section 3 we give a short description of the tableau and related method and consider a typical proof-search procedure for such methods. We analyze this procedure and point out two problems, instantiation of a quantifier-free formula to a valid formula, and strategies for selecting multiplicity. In Section 4 we prove several results on the complexity of the formula instantiation problem. Section 5 discusses some results about strategies for multiplicity. Both in Section 4 and Section 5 we mention some related open problems. Finally, Section 6 indicates some interesting research directions and defines more open problems in connections with these directions.

This paper does not pretend to be a historical survey. When we cite particular results, we try to choose most accessible publications which are often not the earliest ones. However, we always put the authors of a result first in the citation list for this result. When a result is new, it has no citations and is provided with a proof or a reference to the full text of the proof.

By semantic tableaux and related methods we understand:

1. the tableau method (Fitting 1996);
2. the method of matings (Andrews 1981, Gallier 1986), or the connection method (Bibel 1981, Bibel & Eder 1993);
3. model elimination (Loveland 1968, Loveland 1978).

There is no unifying name for these kind of methods. They may be called matrix methods (Degtyarev & Voronkov 1995) due to Prawitz (Prawitz 1970), extension methods (Bibel 1987, Petermann 1993), non-local methods (Maslov, Mints & Orevkov 1983) or rigid-variable methods (Voronkov 1997b). We shall call them *tableau-like methods* and use matings for illustration.

Section 2

Preliminaries

In this section we introduce some notation and terminology. We use boldface notation to denote sequences of symbols. For example, t is used to denote terms and $\mathbf{t}$ is used to denote sequences of terms. The equality predicate is denoted $\approx$. The symbol $\vdash$ denotes provability in classical logic. An expression (e.g. a term or a set of terms) is called *ground* if it contains no variables.

Substitutions. By $[x_1 \mapsto t_1, \ldots, x_n \mapsto t_n]$ we denote the substitution that replaces variables x_i by terms t_i. If θ is a substitution and t is a term, $t\theta$ denotes the term obtained from t by applying θ. We shall also apply substitution to formulas. When applying a substitution θ to a formula φ, we rename, if necessary, bound variables of φ. The domain of a substitution θ is denoted $dom(\theta)$. The *variable range of* θ, denoted $vran(\theta)$, is the set of variables occurring in $(dom(\theta))\theta$.The restriction of a substitution θ to a set of variables X is denoted $\theta\restriction_X$.

Formulas. By formulas we mean first-order formulas. For every formula φ, we denote by $\exists\varphi$ the *existential closure* of φ. A *literal* is either an atomic formula or the negation of an atomic formula. A formula is in *negation normal form* if it is constructed from literals using $\wedge, \vee, \forall, \exists$.

Signatures. We assume that every signature considered in this article contains at least one constant. The *signature of a formula* φ is the signature consisting of all symbols occurring in φ, plus one fixed constant if φ contains no constants. Our results will depend on the signature and logic in which formulas are written. We consider two logics: classical logics with and without equality. If a signature Σ consists of k constants, l unary function symbols, and m function symbols of arity ≥ 2, we shall denote such a signature by (k, l, m). In the case of logic with equality, the corresponding signature will be denoted $(k, l, m)^{\approx}$. We shall also use ordinals and wildcards in the notation for signatures. For example, $(\omega, \_, 3)$ denotes any signature with infinitely many constants, any number of unary function symbols, and 3 function symbols of arity ≥ 2. Similarly, $(< \omega, 0, 0)^{\approx}$ denotes a signature with any finite number of constants and no function symbols of arity ≥ 1, considered in logic with equality.

Theories. A *theory* is any set of first-order sentences. We denote by $\vdash \varphi$ (respectively, $\mathcal{T} \vdash \varphi$) provability of φ (respectively from $\mathcal{T}$) in first-order classical logic.

Section 3

Tableaux and related methods

We assume that formulas to be checked for provability are prenex existential sentences, i.e. formulas of the form

$$\exists x_1 \ldots \exists x_n \varphi(x_1, \ldots, x_n), \tag{3.1}$$

where $\varphi(x_1, \ldots, x_n)$ is a quantifier-free formula all whose free variables are among $x_1, \ldots, x_n$.

Given a formula (3.1), the method of matings constructs a *matrix*, using an appropriate *multiplicity*. Multiplicity is, intuitively, the number of copies of $\varphi(x_1, \ldots, x_n)$ that can be used in the search for a proof.

For example, for the input formula

$$\exists x (P(x) \vee (\neg P(a) \wedge \neg P(b))), \tag{3.2}$$

using two copies of $\exists x$ we get the following matrix

$$\left[\begin{array}{c} P(x_1) \\ \\ \left[\begin{array}{cc} \neg P(a) & \qquad \neg P(b) \end{array}\right] \\ \\ P(x_2) \\ \\ \left[\begin{array}{cc} \neg P(a) & \qquad \neg P(b) \end{array}\right] \end{array}\right]$$

This matrix represents two variable-disjoint copies of $P(x) \vee (\neg P(a) \wedge \neg P(b))$, namely

$$P(x_1) \vee (\neg P(a) \wedge \neg P(b)) \text{ and}$$
$$P(x_2) \vee (\neg P(a) \wedge \neg P(b)),$$

with disjunctions displayed vertically and conjunctions displayed horizontally.

The method of matings is based on the following characterization of provability.

Theorem 3.1 A formula φ is provable if there exist a multiplicity μ and a substitution θ so that every vertical path in $M\theta$ is a tautology, where M is the matrix constructed by φ and μ.

The tableau method uses trees instead of matrices. The notion of a multiplicity is representation-dependent and may vary. For example, model elimination provers often use bounded-depth search. The depth bound is an example of another notion of multiplicity. For nonprenex formulas, the multiplicity can be a tree of integers, because we can use different subformulas a different number of times.

The results of this paper can be reformulated for different notions of multiplicity and different characterizations of provability similar to Theorem 3.1. We choose one particular characterization and the corresponding representation-independent notion. This characterization is nothing but Herbrand's theorem.

Theorem 3.2 (Herbrand 1972) A formula $\exists \mathbf{x} \varphi(\mathbf{x})$, where $\varphi(\mathbf{x})$ is quantifier-free, is provable iff there exists a positive integer μ and a substitution θ such that $(\varphi(\mathbf{x}_1) \vee \ldots \vee \varphi(\mathbf{x}_\mu))\theta$ is provable.

The matrix characterization of provability of Theorem 3.1 is just a reformulation of Herbrand's theorem. Now we call *multiplicity* any positive integer and *matrix* any quantifier-free formula.

Given as input a prenex existential formula $\exists \mathbf{x} \varphi(\mathbf{x})$, implementations of matrix methods usually follow the following loop or its variations:

1. Choose an initial multiplicity μ.

2. Consider the matrix $\varphi_\mu = (\varphi(\mathbf{x}_1) \vee \ldots \vee \varphi(\mathbf{x}_\mu))$ and check whether there exists a substitution θ such that the formula $\varphi_\mu \theta$ is provable.

3. If such a substitution exists, then the goal formula $\exists \mathbf{x} \varphi(\mathbf{x})$ is provable. Otherwise, increase μ and come back to step 2.

We refer to this loop in the sequel as the loop. Our aim is to understand the efficiency of methods based on this loop and ways to improve performance of such methods. To this end we analyze the following two problems.

1. How difficult is the check for the existence of the substitution θ (step 2)?

2. What kind of strategies for increasing multiplicity should be used? Are some strategies more efficient than the other?

Some analysis of these two problems is made in the next two sections.

Section 4

Formula instantiation

The problem that should be solved at step 2 of the loop gives rise to the following decision problem.

Definition 4.1 (Formula Instantiation) *Formula Instantiation* is the following decision problem. Given a quantifier-free formula $\varphi(\mathbf{x})$, is there a term sequence $\mathbf{t}$ such that $\varphi(\mathbf{t})$ is provable?

In fact, we have a family of Formula Instantiation problems, depending on the signature and presence of equality. Formula Instantiation for the formulas of a signature Σ will be denoted $FI(\Sigma)$ for logic without equality, and $FI(\Sigma)^{\approx}$ for logic with equality.

To consider some particular theories as built-in, we introduce a more general Formula Instantiation.

Definition 4.2 *Formula Instantiation* with respect to a theory T is the following decision problem. Given a quantifier-free formula $\varphi(\mathbf{x})$, is there a term sequence $\mathbf{t}$ such that $T \vdash \varphi(\mathbf{t})$.

When we consider a provability in a particular theory instead of provability in first-order logic, we do not necessarily have an analogue of Herbrand's theorem. Herbrand's theorem takes place for theories axiomatized by universally quantified formulas. Automated deduction with respect to a particular theory is considered in a number of papers, for example in (Stickel 1985).

As a particular example we can consider the theory of transitive relations that plays an important role in automated reasoning (Bachmair & Ganzinger 1994) in connection with axiomatization of orderings.

First, we note a trivial but useful property of Formula Instantiation.

Lemma 4.3 Let $\varphi(\mathbf{x})$ be a quantifier-free formula. If there exists a term sequence $\mathbf{t}$ such that $\varphi(\mathbf{t})$ is provable, then there exists such a term sequence in the signature of φ. $\Box$

Of course this lemma does not hold when provability is replaced by provability in a particular theory. To make it hold for a theory T, it is enough to require that T is axiomatized by universally quantified formulas, and consider the signature of T and φ instead of the signature of φ.

4.1 Logic without equality

There exist several procedures for solving Formula Instantiation in logic without equality. Usually, they are presented in the form of searching for a substitution making all paths in a matrix tautologies (Gallier 1986, Bibel & Eder 1993) or closing all branches in a tableau (Fitting 1996). The following theorem shows the complexity of Formula Instantiation for logic without equality.

Theorem 4.4 For every signature Σ with at least two symbols, $FI(\Sigma)$ is decidable and Σ_2^p-complete.

Proof. First, we show that Formula Instantiation is in Σ_2^p. Let $\varphi(\mathbf{x})$ be an instance of Formula Instantiation. Let us call a *split* of $\varphi(\mathbf{x})$ any equivalence relation on the set of atomic subformulas of $\varphi(\mathbf{x})$. We shall identify such equivalence relations with the sets of corresponding equivalence classes. Thus, any split can be considered as a set of sets of atomic subformulas of $\varphi(\mathbf{x})$.

Given a split S we obtain from $\varphi(\mathbf{x})$ a propositional formula φ_S as follows. Replace all atomic subformulas by propositional variables so that subformulas belonging to the same equivalence class of S are replaced by the same symbol, and subformulas belonging to different equivalence classes are replaced by different symbols.

A split is called a *justification* of $\varphi(\mathbf{x})$ if

1. φ_S is a tautology;
2. there exists a substitution θ such that for every equivalence class $E \in S$ and for every two formulas $A, B \in E$ we have $A\theta = B\theta$.

Consider an example, developed from formula (3.2). Suppose that $\varphi(x_1, x_2)$ is the formula

$$\begin{array}{l}\big(P(x_1) \vee (\neg P(a) \wedge \neg P(b))\big) \vee \\ \big(P(x_2) \vee (\neg P(a) \wedge \neg P(b))\big).\end{array}$$

Consider the split S with two equivalence classes:

$$\{P(a), P(x_1)\} \quad \text{and} \quad \{P(b), P(x_2)\}.$$

This split is a justification. Indeed, if we replace the atoms $P(a), P(x_1)$ by a propositional letter A and the atoms $P(b), P(x_2)$ by a propositional letter B, we obtain the tautology

$$\varphi_S = \big(A \vee (\neg A \wedge \neg B)\big) \vee \big(B \vee (\neg A \wedge \neg B)\big).$$

The corresponding substitution θ is $[x_1 \mapsto a, x_2 \mapsto b]$.

Is not hard to argue that the instance $\varphi(\mathbf{x})$ of Formula Instantiation holds if and only if there exists a justification of $\varphi(\mathbf{x})$. Let us now prove that the problem of existence of a justification is in Σ_2^p. This follows from the following observations:

1. All splits can be found by a nondeterministic polynomial-time algorithm.
2. The problem of checking, given a split S, whether φ_S is a tautology, is coNP-complete (by obvious reductions to and of the propositional provability problem).
3. The problem of the existence of an appropriate substitution θ can be solved in polynomial time (it is the so-called *simultaneous unification problem* proved P-complete in (Dwork, Kanellakis & Mitchell 1984, Yasuura 1984, Dwork, Kanellakis & Stockmeyer 1988)).

It remains to prove that Formula Instantiation is Σ_2^p-hard. We prove this for the signature $(2, 0, 0)$, but the proof is valid for every other signature with at least two symbols, by replacing two constants of this signature with any two distinct ground terms. We use reduction of the QBF_2 problem known to be Σ_2^p-complete, see e.g. (Papadimitriou 1994). This problem can be formulated as follows. Consider the algebra **2** with two elements $0, 1$ in the signature with two constants $0, 1$ representing these elements. Given a sentence of this signature

$$\exists x_1 \dots \exists x_n \forall y_1 \dots \forall y_m \Phi(x_1, \dots, x_n, y_1, \dots, y_m), \tag{4.1}$$

whose atomic formulas are of the form $x_i \approx 0, x_i \approx 1, y_j \approx 0, y_j \approx 1$, is this formula true in $\mathbf{2}$?

Given an instance (4.1) of QBF_2, we construct the corresponding instance of Formula Instantiation as follows. The instance uses unary predicate symbols $P_1, \dots, P_n$ and propositional symbols $Q_1, \dots, Q_m$. Denote by Φ' the formula obtained from Φ by replacing

- each occurrence of $x_i \approx 0$ by $\neg P_i(x_i)$;
- each occurrence of $x_i \approx 1$ by $P_i(x_i)$;
- each occurrence of $y_j \approx 0$ by $\neg Q_j$;
- each occurrence of $y_j \approx 1$ by Q_j.

Consider the instance of Formula Instantiation

$$\bigwedge_{1 \le i \le n} (\neg P_i(0) \wedge P_i(1)) \supset \Phi'. \tag{4.2}$$

We claim that (4.1) holds if and only if (4.2) does.

By Lemma 4.3, if an instance of Formula Instantiation is satisfied by a substitution, then it is also satisfied by a substitution θ such that θ maps each variable to 0 or 1. Let θ be such a substitution.

It is not hard to argue that θ satisfies (4.2) if and only if

$$\mathbf{2} \models \forall y_1 \dots \forall y_m \Phi(x_1\theta, \dots, x_n\theta, y_1, \dots, y_m).$$

This proves the equivalence of (4.1) and (4.2). □

When the signature contains only one constant and no function symbols, the complexity is characterized by the following statement.

Theorem 4.5 *FI*$(1,0,0)$ and *FI*$(1,0,0)^{\approx}$ are coNP-complete.

Proof. Consider any instance $\varphi(x_1, \dots, x_n)$ of Formula Instantiation in the signature with one constant a. By Lemma 4.3, this instance is a yes-instance if and only if the formula $\varphi(a, \dots, a)$ is provable. All equalities in $\varphi(a, \dots, a)$ have the form $a \approx a$, so we can assume that $\varphi(a, \dots, a)$ has no occurrences of equality. Then, *FI*$(1,0,0)$ is equivalent to the provability problem of propositional formulas. □

4.2 Equality and other relations

For logic with equality, Formula Instantiation is decidable for formulas of a signature Σ if and only if simultaneous rigid E-unification (Gallier, Raatz & Snyder 1987) is decidable for formulas of this signature. Most (un)decidability results cited below were proved about simultaneous rigid E-unification, we reformulate them for Formula Instantiation.

Theorem 4.6 (Degtyarev & Voronkov 1996*c*, Degtyarev & Voronkov 1996*d*) $FI(\_,\_,\geq 1)^{\approx}$ is undecidable. It is undecidable already for formulas with two variables (Veanes 1997). □

As for the number of variables, this undecidability result is sharp, as the following theorem shows.

Theorem 4.7 (Degtyarev, Gurevich, Narendran, Veanes & Voronkov 1997) $FI(\_,\_,\_)^{\approx}$ is decidable for formulas with one variable. □

(Degtyarev et al. 1997) prove that simultaneous rigid E-unification with one variable in the signature $(\_,\_,\geq 1)$ is EXPTIME-complete. This gives the 2-NEXPTIME upper bound and EXPTIME lower bound on the complexity of $FI(\_,\_,\leq 1)^{\approx}$ for formulas with one variable. The precise complexity is however not known:

Open problem 1 What is the complexity of $FI(\_,\_,\geq 1)^{\approx}$? for formulas with one variable?

All proofs of Theorem 4.6 essentially use a function symbol of arity ≥ 2. For Monadic Formula Instantiation, i.e. Formula Instantiation with unary function symbols only, the decidability is an open problem. Some known results are the following. In the case of one unary function symbol, we have

Theorem 4.8 (Degtyarev, Matiyasevich & Voronkov 1996) $FI(\_,1,0)^{\approx}$ is decidable. □

The decidability proof of this theorem essentially uses the decidability of the so-called *Diophantine problem for addition and divisibility* proved in (Beltyukov 1976, Mart'janov 1977, Lipshitz 1978), i.e. solving equations over natural numbers in the signature consisting of the function $+$ and the divisibility predicate $|$. Establishing complexity of $FI(\_,1,0)^{\approx}$ will most likely require a complexity result for the Diophantine problem for addition and divisibility. The complexity of the latter problem was investigated in (Lipshitz 1981), but it is only known that the problem is NP-hard. Thus, we have

Open problem 2 What is the complexity of $FI(\_,1,0)^{\approx}$?

For Monadic Formula Instantiation with more than one function symbol, the following results are known. Using a standard encoding of words on an arbitrary alphabet by words on a two-letter alphabet, one can easily prove

Theorem 4.9 (Degtyarev, Matiyasevich & Voronkov 1996) $FI(\_,2,0)^{\approx}$ is polynomial-time equivalent to $FI(\_,\geq 2,0)^{\approx}$. □

Moreover, (Degtyarev, Matiyasevich & Voronkov 1996) noted that there is a polynomial-time reduction of word equations to $FI(\_,2,0)^{\approx}$. The complexity of word equations is between NP and 3-NEXPTIME (Kościelski & Pacholski 1996). A more precise correspondence between word equations is described in (Gurevich & Voronkov 1997*a*, Gurevich & Voronkov 1997*b*) and described below.

Let $\mathbf{A}$ be any alphabet with more than one symbol. Denote by $\mathbf{W}$ the set of pairs of words on $\mathbf{A}$. Introduce on $\mathbf{W}$ a binary function $*$, a unary function ^{r} and a binary relation $\leq$ in the following way:

$$(U_1, U_2) * (V_1, V_2) = \begin{cases} (U_1, V_2), & \text{if } U_2 = V_1; \\ (V_1, V_2), & \text{otherwise;} \end{cases}$$

$$(U_1, U_2)^r = (U_2, U_1);$$

$$(U_1, U_2) \leq (V_1, V_2) = \text{there is a word } W \text{ such that } (V_1, V_2) = (U_1 W, U_2 W).$$

An *ideal* on $\mathbf{W}$ is any set of pairs containing the pair $(\varepsilon, \varepsilon)$ of empty words, closed under functions $*$ and ^{r} and upward closed under $\leq$. The *ideal generated by a set of pairs* S, denoted *ideal*(S) is defined as the least ideal containing S.

An ideal membership equation is an expression

$$(U, V) \in ideal(\{(U_1, V_1), \ldots, (U_n, V_n)\}),$$

where $n \geq 0$ and $U, V, U_1, \ldots, U_n, V_1, \ldots, V_n$ are words built from $\mathbf{A}$ and a set of word variables. A *solution* to such ideal membership equation is any substitution σ of words for word variables such that the word $(U\sigma, V\sigma)$ belongs to the ideal generated by

$$\{(U_1\sigma, V_1\sigma), \ldots, (U_n\sigma, V_n\sigma)\}.$$

A *system of ideal membership equations* is any finite set of ideal membership equations. A *solution* to a system of ideal membership equations is any word substitution that solves each equation in the system. The *ideal membership problem* is the decision problem of solvability of systems of ideal membership equations.

Theorem 4.10 (Gurevich & Voronkov 1997*a*, Gurevich & Voronkov 1997*b*) The ideal membership equation is decidable if and only if $FI(\_, \geq 2, 0)^{\approx}$ is decidable. □

It is known that the if ideal membership problem is decidable, then it is also decidable with regular constraints (every word variable ranges over a regular set) (Gurevich & Voronkov 1997*a*). However, this does not give the undecidability result for $FI(\_, \geq 2, 0)^{\approx}$, since word equations with regular constraints are decidable (Schulz 1990). Thus, we have

Open problem 3 Is $FI(\_, \geq 2, 0)^{\approx}$ decidable?

This problem is also related to the classification of decidable prenex fragments of intuitionistic logic depending on the signature and the quantifier prefix (Degtyarev & Voronkov 1996*a*, Degtyarev, Gurevich & Voronkov 1996).

As for Formula Instantiation with equality but no function symbols, we shall establish its complexity after proving some quite general results.

Denote by R, S, T axioms of reflexivity, symmetry and transitivity, respectively, for some predicate.

Theorem 4.11 Let $\mathcal{T}$ be a theory in logic without equality axiomatized by any combination of R, S, T for any number of predicates. Then Formula Instantiation with respect to $\mathcal{T}$ is Σ_2^p-complete.

Proof. When we have a predicate symbol for which no axioms are specified, Σ_2^p-hardness follows from Theorem 4.4. When every predicate symbol of the language has one or more axioms R, S, T, the proof of Σ_2^p-hardness can still be modified and we do not consider details here. We only prove containment in Σ_2^p.

For simplicity, but without loss of generality, we assume that the language contains only one predicate P and the theory $\mathcal{T}$ consists of the transitivity axiom for P:

$$\forall x \forall y \forall z (P(x, y) \wedge P(y, z) \supset P(x, z)).$$

Let φ be any quantifier-free formula. First, we characterize Formula Instantiation for φ in terms of so-called *argument splits*.

Denote by T the set of terms occurring as arguments to a predicate occurring in φ. For example, if φ contains the subformula $P(a, f(x))$, then the terms a and $f(x)$ are members of T. We call an *argument split* any equivalence relation on T. Given an argument split S, we obtain from φ a formula φ_S as follows. Replace arguments of predicates in φ by constants so that terms belonging to the same equivalence class of S are replaced by the same constant and terms belonging to different equivalence classes are replaced by different constants.

Let θ be any substitution. The *split by* θ, denoted $S(\theta)$, is defined as follows. Two terms $s, t \in T$ are equivalent w.r.t. $S(\theta)$ if and only if $s\theta = t\theta$.

Lemma 4.12 $\mathcal{T} \vdash \varphi\theta$ if and only if $\mathcal{T} \vdash \varphi_{S(\theta)}$.

Proof. Without loss of generality we can assume that $\varphi\theta$ has no variables. We show that $\neg\varphi\theta$ has a model in which P is a transitive relation if and only if $\neg\varphi_{S(\theta)}$ has a model in which P is a transitive relation. We shall prove it only in one direction, in the other direction the proof is more complex but similar.

Let $t_1, \ldots, t_n$ be all different arguments to predicates in $\varphi\theta$ and $c_1, \ldots, c_n$ be constants. Then $\varphi_{S(\theta)}$ is obtained from $\varphi\theta$ by replacement of all t_i by c_i.

Suppose $\mathfrak{M}$ is any model of $\neg\varphi\theta$ in which P is a transitive relation. We define $\mathfrak{M}'$ as a model whose signature consists of one predicate symbol P and constants $c_1, \ldots, c_n$ as follows. The domain of $\mathfrak{M}'$ is the same as the domain of $\mathfrak{M}$ and the interpretation of P in $\mathfrak{M}'$ is the same as in $\mathfrak{M}$. For every constant c_i we define $c_i^{\mathfrak{M}'}$ as $t_i^{\mathfrak{M}}$. It is straightforward to check that $\mathfrak{M} \models \neg\varphi\theta$ if and only if $\mathfrak{M}' \models \neg\varphi_{S(\theta)}$.

□

For splits S and S', we write $S \leq S'$ if every equivalence class by S is a subset of an equivalence class by S'. For example, for three splits

$$S_1 = \{\{a\}, \{b, c\}\},\ S_2 = \{\{a, b\}, \{c\}\},\ S_3 = \{\{a, b, c\}\}$$

we have $S_1 \leq S_3$ and $S_2 \leq S_3$, but S_1 and S_2 are incomparable w.r.t. $\leq$.

Lemma 4.13 If $S \leq S'$ and $\mathcal{T} \vdash \varphi_S$, then $\mathcal{T} \vdash \varphi_{S'}$.

Proof. The formula $\varphi_{S'}$ is obtained from φ_S by replacement of some constants c_i by other constants c_j. It is not hard to argue that every model of $R + \neg\varphi_{S'}$ can be made into a model of $R + \neg\varphi_S$. □

An argument split S is called a *justification of* φ if (i) $\mathcal{T} \vdash \varphi_S$; and (ii) there exists a substitution θ such that for every equivalence class E by S and every terms $s, t \in E$ we have $s\theta = t\theta$.

Lemma 4.14 There exists a substitution θ such that $\mathcal{T} \vdash \varphi\theta$ if and only if there exists a justification of φ.

Proof.

- $\Rightarrow$ Suppose $\mathcal{T} \vdash \varphi\theta$. By Lemma 4.12 $\mathcal{T} \vdash \varphi_{S(\theta)}$. Evidently, $S(\theta)$ is a justification.
- $\Leftarrow$ Suppose that S is a justification of φ. Then $\mathcal{T} \vdash \varphi_S$. Consider any substitution θ such that for every equivalence class E by S and every terms $s, t \in E$ we have $s\theta = t\theta$. By the definition of θ we have $S \leq S(\theta)$. By Lemma 4.13, $\mathcal{T} \vdash \varphi_{S(\theta)}$. By Lemma 4.12, $\mathcal{T} \vdash \varphi\theta$.

□

Lemma 4.15 Let U be a finite set of ground literals. The problem of checking whether U has a model where P is a transitive relation, can be checked in polynomial time.

Proof. Consider the set of pairs

$$V = \{(s,t) \mid P(s,t) \in U\}$$

and let W be the transitive closure of V. It is not hard to argue that U is inconsistent if and only if there exists a pair of terms $(s,t) \in W$ such that $(\neg P(s,t)) \in U$. Then use the fact that the transitive closure can be constructed in polynomial time. □

Lemma 4.16 Let ψ be a quantifier-free ground formula. The problem of checking whether $\mathcal{T} \vdash \psi$ is in coNP.

Proof. The formula ψ is equivalent to its conjunctive normal form, i.e. a formula $\psi' = \psi_1 \wedge \ldots \wedge \psi_n$ where each ψ_i is a disjunction of literals. It is not hard to argue that all disjunctions ψ_i can be found by a nondeterministic polynomial-time algorithm and that $\mathcal{T} \vdash \psi$ if and only if for every ψ' we have $\mathcal{T} \vdash \psi'$. Evidently, $\mathcal{T} \nvdash \psi'$ if there exists a model of $\neg\psi'$ in which P is a transitive relation. Using Lemma 4.15, the existence of such a model can be checked in polynomial time. □

Lemma 4.17 The problem of checking, given φ and a split S, that S is a justification of φ, is in coNP.

Proof. The check $\mathcal{T} \vdash \varphi_S$, is in co-NP, by Lemma 4.16. The existence of a substitution θ such that for every equivalence class E by S and every terms $s, t \in E$ we have $s\theta = t\theta$ can be made in polynomial time by a simultaneous unification algorithm. □

Now we can complete the proof of Theorem 4.11. By Lemma 4.14, there exists a substitution θ such that $\mathcal{T} \vdash \varphi\theta$ if and only if there exists a justification of φ. All splits can be generated using a nondeterministic polynomial-time algorithm. By Lemma 4.17, the problem whether a split is a justification is in coNP. Hence, Formula Instantiation with respect to $\mathcal{T}$ is in Σ_2^p. □

Theorem 4.18 *FI*$(\geq 2, 0, 0)^{\approx}$ is Σ_2^p-complete.

Proof. In the absence of function symbols, the theory of equality $\mathcal{T}$ equality is axiomatized as an equivalence relation, i.e. by reflexivity, transitivity and symmetry axioms. In addition, for every predicate symbol P different from equality, $\mathcal{T}$ contains the formula

$$x_1 \approx y_1 \wedge \ldots \wedge x_n \approx y_n \wedge P(x_1, \ldots, x_n) \supset P(y_1, \ldots, y_n).$$

The proof is the same as that of Theorem 4.11. □

Theorem 4.6 on the undecidability of Formula Instantiation for logic with equality buried hopes for handling equality in tableau-like methods in the ordinary way. After this theorem was proved, several papers with nonstandard approaches to equality appeared, for example

- The equality elimination method: a combination of tableaux and resolution (Degtyarev & Voronkov 1995, Degtyarev & Voronkov 1996*b*).
- A goal-oriented strategy for model elimination (Moser, Lynch & Steinbach 1995).
- Incomplete but terminating procedures for Formula Instantiation (Plaisted 1995, Degtyarev & Voronkov 1998).
- Optimized translations of logic with equality into logic without equality (Bachmair, Ganzinger & Voronkov 1998).

4.3 Function symbols introduced by Skolemization

Sometimes, formulas to be proved do not have function symbols, but function symbols are introduced by Skolemization. There are at least two approaches for getting around Theorem 4.6 in this case.

Tableaux without Skolemization. One possible approach was introduced in (Voronkov 1996) for intuitionistic logic, but it works for classical logic as well. A matrix characterization of validity based on similar ideas appeared already in (Lyaletski 1981, Bibel 1982*b*). The idea is to augment Formula Instantiation with *non-occurrence constraints*. Any such constraint have the form "c does not occur in t", where c is a constant and t is an arbitrary term. A substitution θ is a solution to such a constraint if c does not occur in $t\theta$.

For example, consider the formula $\exists x \forall y(P(x) \supset P(y))$. Skolemizing would give a formula with function symbols. Consider the following "pseudo-proof" of this formula in a sequent calculus.

$$\cfrac{\cfrac{P(t) \supset P(c)}{\forall y(P(t) \supset P(y))}}{\exists x \forall y(P(x) \supset P(y))}$$

This can be extended to a proof if there exist a term t such that (i) $\vdash P(t) \supset P(c)$, and (ii) c does not occur in t? Similar, we can establish that $\exists x \forall y(P(x) \supset P(y))$ is provable if there exist terms t_1, t_2 such that (i) $\vdash (P(t_1) \supset P(c_1)) \vee (P(t_2) \supset P(c_2))$, and (ii) c_1 does not occur in t_1, and c_2 does not occur in t_1, t_2?

In the second case we have the instance $(P(x_1) \supset P(c_1)) \vee (P(x_2) \supset P(c_2))$ of Formula Instantiation with non-occurrence constraints "c_1 does not occur in x_1", and "c_2 does not occur in x_1, x_2".

Theorem 4.19 Let $\mathcal{T}$ be a theory axiomatized by any combination of R, S, T. Then Formula Instantiation with non-occurrence constraints with respect to $\mathcal{T}$ is Σ_2^p-complete.

Proof. Similar to the proof of Theorem 4.11. The only difference is that we change the notion of a justification to satisfy the non-occurrence constraints. □

In a similar way, we can establish

Theorem 4.20 $FI(\geq 2, 0, 0)^{\approx}$ with non-occurrence constraints is Σ_2^p-complete.

A substitute for the theory of equality. In general, the theory of equality for a signature Σ consists of universal closures of the following axioms

$$x \approx x;$$
$$x \approx y \supset y \approx x;$$
$$x \approx y \wedge y \approx z \supset x \approx z.$$

plus the following axioms for every function symbol f and every predicate symbol P of the signature:

$$x_1 \approx y_1 \wedge \ldots \wedge x_n \approx y_n \supset f(x_1, \ldots, x_n) \approx f(y_1, \ldots, y_n);$$
$$x_1 \approx y_1 \wedge \ldots \wedge x_n \approx y_n \wedge P(x_1, \ldots, x_n) \supset P(y_1, \ldots, y_n.$$

For a signature Σ, denote the theory of equality for Σ by $\mathcal{E}_\Sigma$.

Introduce a new binary predicate symbol E. For every formula φ, denote by φ^E the formula obtained from φ by the replacement of every occurrence of the equality predicate $\approx$ by E. Note that φ^E is a formula without equality.

Lemma 4.21 Let φ be a formula with equality in a signature Σ. Then $\vdash \varphi$ if and only if $\mathcal{E}_\Sigma \vdash \varphi^E$. □

Let φ be a formula. Denote by φ_{Sk} a "standard" Skolem normal form of φ. In fact, we require of φ_{Sk} the following property.

Lemma 4.22 Let $\mathcal{T}$ be any theory consisting of universal sentences, i.e. sentences $\forall \mathbf{x} \psi$, where ψ is quantifier-free. Then $\mathcal{T} \vdash \varphi$ if and only if $\mathcal{T} \vdash \psi_{Sk}$. □

Let now Σ be a signature $(\_, 0, 0)$ and φ be a formula with equality in this signature. The formula φ_{Sk} may contain function symbols. Denote by Σ' the signature of φ_{Sk}.

Theorem 4.23 $\vdash \varphi$ if and only if $\mathcal{E}_\Sigma \vdash \varphi_{Sk}^E$.

Proof.

($\Rightarrow$) Suppose $\vdash \varphi$. By Lemma 4.21, $\mathcal{E}_\Sigma \vdash \varphi^E$. By Lemma 4.22, $\mathcal{E}_\Sigma \vdash \varphi_{Sk}^E$.

($\Leftarrow$) Suppose $\mathcal{E}_\Sigma \vdash \varphi_{Sk}^E$. Since Σ' extends Σ, we have $\mathcal{E}_{\Sigma'} \vdash \varphi_{Sk}^E$. By Lemma 4.21, $\vdash \varphi_{Sk}$. By Lemma 4.22, $\vdash \varphi$.

□

The proof of Theorem 4.18 implies that Formula Instantiation with respect to $\mathcal{E}_\Sigma$ is decidable. At the same time, Formula Instantiation with respect to $\mathcal{E}_{\Sigma'}$ may be undecidable. Therefore, this theorem shows how an undecidable special case of Formula Instantiation can be replaced by a decidable one.

Section 5

Strategies for multiplicity

In this section we present in a unified framework some previously published results about strategies for multiplicity and prove some new results.

Informally, a strategy for multiplicity is any procedure that selects the initial multiplicity and increases multiplicity in `the loop`. Therefore, such a strategy can be formalized as a function producing, by a given formula, an increasing sequence of multiplicities. Since a sequence it itself a function on positive integers, we define strategies for multiplicity as follows.

Definition 5.1 (Strategy for multiplicity) A *strategy for multiplicity* is a computable binary function $\mathfrak{S}$, whose first argument ranges over quantifier-free formulas and second argument ranges over positive integers. The range of $\mathfrak{S}$ is the set of positive integers and $\mathfrak{S}$ is strictly monotone on the second argument, i.e. $\mathfrak{S}(\varphi, n) > \mathfrak{S}(\varphi, m)$ whenever $n > m$.

The monotonicity requirement is due to the fact that the multiplicity in `the loop` increases with every iteration. When we fix a strategy $\mathfrak{S}$, we can reformulate `the loop` as follows. Given as the input a prenex existential formula $\exists \mathbf{x} \varphi(\mathbf{x})$, do the following.

1. Let $i = 1$ (to denote the iteration step).
2. Define $\mu = \mathfrak{S}(\varphi(\mathbf{x}), i)$. Consider the matrix $\varphi_\mu = (\varphi(\mathbf{x}_1) \vee \ldots \vee \varphi(\mathbf{x}_\mu))$ and check whether there exists a substitution θ such that the formula $\varphi_\mu \theta$ is provable.
3. If such a substitution exists, then the goal formula $\exists \mathbf{x} \varphi(\mathbf{x})$ is provable. Otherwise, increase i by 1 and come back to step 2.

Now we can investigate decidability and complexity problems for this loop, depending on the strategy $\mathfrak{S}$.

We introduce one special kinds of strategies.

Definition 5.2 A strategy $\mathfrak{S}$ is called *formula-independent* if for every formulas φ, ψ and a natural number n we have $\mathfrak{S}(\varphi, n) = \mathfrak{S}(\psi, n)$. The *standard strategy* $\mathfrak{S}$ is defined by $\mathfrak{S}(\varphi, n) = n$, for every φ.

Thus, a strategy is formula-independent if it does not depend on the input formula. The standard strategy sets multiplicity initially to 1 and increments it by 1 at any further step. Evidently, the standard strategy is formula-independent.

If we choose multiplicity using a strategy, we can consider the following family of decision problems.

Definition 5.3 (Herbrand Instantiation) Let $\mathfrak{S}$ be a strategy. *Herbrand Instantiation using* $\mathfrak{S}$, denoted $HI(\mathfrak{S})$, is the following decision problem. Given a quantifier-free formula $\varphi(\mathbf{x})$ and a positive integer i (written in unary notation), are there term sequences $\mathbf{t}_1, \dots, \mathbf{t}_{\mathfrak{S}(\varphi(\mathbf{x}),i)}$ such that the formula $\varphi(\mathbf{t}_1) \vee \dots \vee \varphi(\mathbf{t}_{\mathfrak{S}(\varphi(\mathbf{x}),i)})$ is provable? Similarly, we denote by $HI(\mathfrak{S})^{\approx}$ Herbrand Instantiation using $\mathfrak{S}$ for logic with equality.

We shall always denote the arguments of a strategy $\mathfrak{S}$ by φ and n and denote the size of φ of $|\varphi|$.[1] For example, $HI(2^{n|\varphi|})$ denotes Herbrand Instantiation using the strategy $\mathfrak{S}(\varphi, n) = 2^{n|\varphi|}$.

Evidently, for every signature in which $FI(\Sigma)^{\approx}$ is decidable, the problem $HI(\mathfrak{S})^{\approx}$ is also decidable.

(Voda & Komara 1995) introduced a decision problem called Herbrand Skeleton.

Definition 5.4 (Herbrand Skeleton) Let k be a positive integer. Herbrand Skeleton for multiplicity k, denoted HS_k (and $HS_k^{\approx}$ for logic with equality), is the following decision problem. Given a quantifier-free formula $\varphi(\mathbf{x})$, is there a substitution θ such that the formula $\big(\varphi(\mathbf{x}_1) \vee \dots \vee \varphi(\mathbf{x}_k)\big)\theta$ is provable?

Note that Formula Instantiation can be described as HS_1 (or $HS_1^{\approx}$ for formulas with equality). (Gurevich & Veanes 1997) also give a reduction of $HS_1^{\approx}$ to $HS_k^{\approx}$. This reduction also works for many fragments of predicate calculus.

(Voda & Komara 1995) prove that $HS_k^{\approx}$ is undecidable, for every k, for formulas with equality. They note that the Herbrand Skeleton problem plays an important role in automated deduction in tableau-like methods. As we shall see from the following theorem, this problem can be reformulated as a statement about formula-independent strategies.

Theorem 5.5 If $HS_k^{\approx}$ for a class Φ of quantifier-free formulas is undecidable for every k, then $HI(\mathfrak{S})^{\approx}$ for the class Φ is undecidable for every formula-independent strategy $\mathfrak{S}$.

Proof. Suppose, by contradiction, that $\mathfrak{S}$ is a formula-independent strategy such that $HI(\mathfrak{S})^{\approx}$ is decidable. Define the function f by $f(n) = \mathfrak{S}(\varphi, n)$, where φ is an arbitrary formula. The problem $HI(\mathfrak{S})^{\approx}$ can be reformulated as the following decision problem. Given a quantifier-free formula $\varphi(\mathbf{x})$ and a positive integer i, are there term sequences $\mathbf{t}_1, \dots, \mathbf{t}_{f(i)}$ such that the formula $\varphi(\mathbf{t}_1) \vee \dots \vee \varphi(\mathbf{t}_{f(i)})$ is provable? Since this problem is decidable, its specialization for each particular i is also decidable. By specializing this problem for $i = 0$ we obtain $HS_{f(0)}^{\approx}$. Therefore, $HS_{f(0)}^{\approx}$ is undecidable. Contradiction. $\square$

As a consequence, we have

Theorem 5.6 $HI(\mathfrak{S})^{\approx}$ is undecidable for every formula-independent strategy $\mathfrak{S}$. $\square$

When we proved the undecidability of Formula Instantiation for logic with equality, we received comments that predicate logic in undecidable in any case, so the undecidability of Formula Instantiation does not add much complexity to tableau-like methods.

Let us now consider how Formula Instantiation and Herbrand Instantiation behave on a *decidable* class of so-called ground-negative formulas. A formula φ is ground-negative (Voronkov 1997*b*) if all negative atomic subformulas of φ are ground (i.e. variable-free). The class of ground-negative formulas is decidable.

[1] At the moment any reasonable definition of the size of a formula is enough for our purpose.

Theorem 5.7 (Voronkov 1997*a*) The provability problem for ground-negative formulas is decidable and Π_2^p-complete, with or without function symbols and with or without equality. $\Box$

Theorem 5.8 (Voronkov 1997*b*) For all formula-independent strategies $\mathfrak{S}$, the problem $HI(\mathfrak{S})^{\approx}$ is undecidable for the class of ground-negative formulas. $\Box$

This theorem is a consequence of Theorem 5.5 and the undecidability of all $HS_k^{\approx}$ for ground-negative formulas (Gurevich & Veanes 1997).

Theorem 5.8 shows that for a "simply decidable" fragment of predicate calculus we have to solve undecidable subproblems, when the traditional loop is used. Note that (Fermüller & Leitsch 1997) proved that the class of ground-negative formulas can be decided by traditional resolution-based methods, namely by positive hyperresolution with ordered paramodulation.

The next question we address is the following. Can formula-dependent strategies be better than formula-independent ones? We shall prove that this is the case for the ground-negative formulas.

Theorem 5.9 (Voronkov 1997*b*) $HI(2^{|\varphi|} + n)$ is Π_2^p-complete for ground-negative formulas.

Instead of $2^{|\varphi|} + n$ we could take any strategy that chooses the initial multiplicity $\geq 2^p$, where p is the number of negative atomic subformulas in φ. This theorem shows that more intelligent strategies can lead to much simpler problems (at least for some classes of formulas).

Section 6

Open problems

It will be of a great importance for automated reasoning by tableau-like methods to find intelligent strategies for multiplicity. The problem of finding such strategies was noted as early as in (Bibel 1980). Theorems 5.8 and 5.9 show that such intelligent strategies exist at least for some decidable classes of predicate logic.

Theorem 5.6 shows that $HI(\mathfrak{S})^{\approx}$ is undecidable for every formula-independent strategy $\mathfrak{S}$. The following problem is open.

Open problem 4 Is there a strategy for multiplicity $\mathfrak{S}$ such that $HI(\mathfrak{S})^{\approx}$ is decidable?

The answer is most likely "no", but we could not find a proof. One can easily show that such a strategy exists for every decidable class of formulas.

Theorem 6.1 For every decidable class Φ of formulas there exists a strategy for multiplicity $\mathfrak{S}$ such that $HI(\mathfrak{S})^{\approx}$ is decidable for the class Φ.

Proof. We only define such a strategy $\mathfrak{S}(\varphi, n)$ leaving the proof of the decidability to the reader. Using a decision algorithm for the class Φ, check whether $\exists\varphi$ is provable. If not, define $\mathfrak{S}(\varphi, n) = n$, for all n. If $\exists\varphi$ is provable, find any proof of this formula (for example by the enumeration of all possible proofs in predicate calculus or all resolution refutations of $\neg\varphi$). Extract, using some algorithm, from this proof a number μ such that $\varphi(\mathbf{x}_1) \vee \ldots \vee \varphi(\mathbf{x}_\mu)$ is provable and define $\mathfrak{S}(\varphi, n) = \mu + n$. $\square$

This proof does not expose any *efficient* (in whatever sense) strategy $\mathfrak{S}$, it just shows that $HI(\mathfrak{S})^{\approx}$ can be made decidable for any decidable class. An interesting relevant question is the following.

Open problem 5 What is the complexity of Formula Instantiation for known decidable classes of predicate logic with/out equality? What is the complexity of $HI(\mathfrak{S})$ (or $HI(\mathfrak{S})^{\approx}$), where $\mathfrak{S}$ is the standard strategy, for these classes?

We can ask similar questions for other natural strategies. If we get some complexity results, it would be quite interesting to compare them with the complexity of known resolution-based decision procedures (Joyner jr 1976, Fermüller, Leitsch, Tammet & Zamov 1993, Leitsch 1997). Some comparison of resolution and tableau-like methods was done in (Bibel 1982*a*, Eder 1988, Eder 1991).

The aim of Problem 5 is to compare resolution and tableau-like methods in the cases when they can be compared. However, the ultimate goal of automated reasoning is to find "more efficient" semi-decision procedures for predicate logic as a whole. In order to understand the inherent efficiency (or inefficiency) of tableau-like methods in general, we should understand what happens when we work with large multiplicities.

For classes of formulas for which Formula Instantiation is undecidable, a relevant question is asked in Problem 4. Consider now theories for which Formula Instantiation is decidable (e.g. logic without equality or the theory of a transitive relation). An example problem is

Open problem 6 What is the complexity of $HI(2^{2^{2^{2^{2^{2^{n|\varphi|}}}}}})$ for logic without equality?

Posing of this problem does not mean that we propose to work with so large multiplicities as $2^{2^{2^{2^{2^{2^{n|\varphi|}}}}}}$. The problem is interesting for the following reason. If the complexity is still 6 or 7 exponents in the size of φ and n, then we probably cannot gain of using large multiplicities, which means that the standard loop and strategy (or some modifications thereof) can be used. If the complexity collapses (for example becomes 2 exponents), we should try to identify the reason for such a collapse. After identification, we may reconsider the standard approaches to tableau-like methods.

Several authors proposed to use "universal variables" in tableaux in addition to the rigid ones (Beckert & Hähnle 1992). Logically speaking, this means that instead of solving Formula Instantiation for quantifier-free formulas, we solve it for more general classes of formulas. Consider an example "matrix" that contains quantified formulas.

$$\begin{bmatrix} \vdots \\ \neg P(x,y) \\ \vdots \\ \exists z P(y,z) \\ \vdots \end{bmatrix}$$

The substitution $[x \mapsto y]$ makes this path contain $\neg P(y,y) \vee \exists z P(y,z)$, which is a tautology. Some tableau-based procedures would identify z as a "universal variable"[1], and instead of solving two equations $x \approx y, y \approx z$ would just solve $x \approx y$. This observation can be formalized as follows.

Definition 6.2 (General Formula Instantiation) *General Formula Instantiation* is the following decision problem. Given a formula $\varphi(\mathbf{x})$ (not necessarily quantifier-free), is there a term sequence $\mathbf{t}$ such that $\varphi(\mathbf{t})$ is provable?

Of course General Formula Instantiation is, in general, undecidable even for logic without equality, since the provability problem for first order logic is a special case of General Formula Instantiation.

However, we can show that the complexity of Formula Instantiation does not grow when we allow quantifiers applied to "simple" formulas.

Theorem 6.3 Let Φ be the class of formulas without equality in negation normal form such that in every formula in Φ all occurrences of quantifiers have the form $\exists x_1 \dots \exists x_n L$, where L is a literal. General Formula Instantiation for Φ is decidable and Σ_2^p-complete.

[1]The term "universal variable" is due to the fact that tableau-like methods are usually represented as refutation methods, in which case z would be universally quantified inside the matrix.

Proof. Σ_2^p-hardness follows from Theorem 4.4.

To prove inclusion in Σ_2^p, we introduce several notions in the style of (Gallier 1986) and prove several simple lemmas. A formula φ is called *rectified* if all free variables of φ are different from all bound variables of φ and each distinct occurrences of quantifiers in φ bind distinct variables. For example, the formulas $\exists x P(x) \vee \exists x \neg P(x)$ or $P(x) \vee \exists x \neg P(x)$ are not rectified. Without loss of generality, we only consider rectified formulas of Φ.

We call an $\exists$-*literal* any formula of the form $\exists x_1 \ldots \exists x_n L$, where L is a literal. Two $\exists$-literals E_1 and E_2 are called *complementary under a substitution* σ if $\vdash E_1\sigma \vee E_2\sigma$.

By an immediate application of Herbrand's theorem we can prove the following lemma.

Lemma 6.4 Let A, B be atoms, $E_1 = \exists \mathbf{x} A$ and $E_2 = \exists \mathbf{y} \neg B$ be two $\exists$-literals, and Z be the set of free variables of $E_1 \vee E_2$. Let σ be a substitution such that (i) $dom(\sigma) \subseteq Z$ and (ii) $vran(\sigma)$ contains no variables in $\mathbf{x}, \mathbf{y}$. Then E_1, E_2 are complementary under σ if and only if there exists a substitution θ such that $A\theta = B\theta$ and $\sigma = \theta \restriction_Z$. □

Using this lemma and Herbrand's theorem we can prove the following lemma.

Lemma 6.5 Let $E_1, \ldots, E_n$ be $\exists$-literals and σ be a substitution. Then $\vdash (E_1 \vee \ldots \vee E_n)\sigma$ if and only if for some i, j, the $\exists$-literals E_i and E_j are complementary under σ. □

Let $\varphi \in \Phi$. The set of $\exists$-*literals of* φ is the smallest set S of $\exists$-literals so that φ is constructed from $\exists$-literals in S using $\vee$ and $\wedge$. For example, if φ is the formula

$$\neg P(x, y) \vee \exists z \exists u P(y, f(z, u)),$$

then $\neg P(x, y)$ and $\exists z \exists u P(y, f(z, u))$ are the only $\exists$-literals of φ. Note that the formulas $P(x, y)$ and $\exists u P(y, f(z, u))$ are $\exists$-literals and subformulas of φ, but none of them is an $\exists$-literal of φ.

A *mated pair in* φ is a pair of $\exists$-literals of φ of the form $\exists \mathbf{x} P(\mathbf{t}), \exists \mathbf{y} \neg P(\mathbf{s})$. A *premating in* φ is a set of mated pairs in φ. A *mating in* φ is a pair (M, σ), where M is a premating in φ and σ is a substitution so that every pair in M is complementary under σ.

Lemma 6.6 The following problem can be solved in polynomial time: *given a premating M in φ, does there exist a mating (M, σ) in φ?*

Proof. Suppose that M consists of pairs $(\exists \mathbf{x}_i A_i, \exists \mathbf{y}_i \neg B_i)_{i \in \{1,\ldots,n\}}$. By renaming bound variables, we can assume that all variables in $\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{y}_1, \ldots, \mathbf{y}_n$ are pairwise different. Using Lemma 6.5, we can prove that a mating (M, σ) exists if and only if there exists a simultaneous unifier of pairs (A_i, B_i). The existence of such a simultaneous unifier can be checked in polynomial time. □

Lemma 6.7 Let $\psi \in \Phi$ be a formula in conjunctive normal form

$$\psi = \bigwedge_{i \in I} \bigvee_{j \in J_i} E_{i,j}$$

Then ψ is a yes-instance of General Formula Instantiation if and only if there exists a mating (M, σ) in ψ such that for every $i \in I$ there exists $j, k \in J_i$ such that $(E_{i,j}, E_{i,k}) \in M$.

Proof.

($\Rightarrow$) Suppose $\vdash \psi\theta$. Then for all $i \in I$ we have $\vdash \bigvee_{j \in J_i} \exists \mathbf{x}_{i,j} E_{i,j}$. Take an arbitrary $i \in I$. By Lemma 6.5 there exist $j_i, k_i \in J_i$ such that E_{i,j_i} and E_{i,k_i} are complementary under θ. Consider the following premating in ψ

$$M = \{(E_{i,j_i}, E_{i,k_i}) \mid i \in I\}.$$

It is easy to see that (M, θ) is the required mating.

$\Leftarrow$ Suppose (M, σ) is such a mating. Take an arbitrary $i \in I$. Then there exist $j, k \in J_i$ such that $(E_{i,j}, E_{i,k}) \in M$. By the definition of a mating, we have $\vdash E_{i,j}\sigma \vee E_{i,k}\sigma$. Then evidently,

$$\vdash \bigvee_{j \in J_i} E_{i,j}\sigma.$$

Since i was arbitrary, we have

$$\vdash \bigwedge_{i \in I} \bigvee_{j \in J_i} E_{i,j}\sigma,$$

i.e. $\vdash \psi\sigma$.

$\square$

Now we can complete the proof of Theorem 6.3. Let $\varphi \in \Phi$ and $\psi \in \Phi$ be obtained from φ by the standard translation into conjunctive normal form. Then $\vdash \varphi \equiv \psi$, every mating in φ is also a mating in ψ and vice versa. We have

$$\psi = \bigwedge_{i \in I} \bigvee_{j \in J_i} E_{i,j}.$$

By Lemma 6.7 ψ is a yes-instance of General Formula Instantiation if and only if there exists a mating (M, σ) in ψ such that for every $i \in I$ there exists $j, k \in J_i$ such that $(E_{i,j}, E_{i,k}) \in M$.

Using $\vdash \varphi \equiv \psi$ and using that matings in ψ are precisely matings in φ, we have that the following conditions are equivalent:

(i) φ is a yes-instance of General Formula Instantiation;

(ii) there exists a premating M in φ and a substitution σ such that (M, σ) is a mating and for every $i \in I$ there exists $j, k \in J_i$ such that $(E_{i,j}, E_{i,k}) \in M$.

It remains to note that (ii), considered as a decision problem of the given φ, is in Σ_2^p. Indeed, all prematings can be generated by a nondeterministic polynomial-time algorithm. By Lemma 6.6, for every premating M the existence of σ can be checked in polynomial time. Finally, note that all sets

$$\{E_{i,j} \mid j \in J_i\}_{i \in I}$$

can be generated by a nondeterministic polynomial-time algorithm. $\square$

General Formula Instantiation gives rise to a number of other interesting problems.

Open problem 7 Find classes of formulas and/or theories for which Formula Instantiation is of a "reasonable" complexity. Design procedures for checking Formula Instantiation and returning the resulting substitutions.

One particular classification of General Formula Instantiation may be in terms similar to those of the classical decision problem (Börger, Grädel & Gurevich 1997).

Open problem 8 Classify formulas, e.g. depending on a signature, quantifier prefix and the number of free variables, w.r.t. General Formula Instantiation (decidability, complexity, the number of solutions).

In view of Theorem 6.3 and connections between General Formula Instantiation and tableau-based theorem proving, instead of prefix formulas one can consider formulas constructed from prefix ones using $\wedge, \vee$. It is also reasonable to restrict oneself to only existencial quantifiers, since for universally quantified formulas we have no analogue of Herbrand's theorem.

Summary

In this article we undertook a mathematical investigation of problems related to tableau-based theorem proving. We proved/cited relevant results and formulated a number of open problems.

In our opinion, we shall know more about the potentials of tableau-based methods when we obtain more results about the above mentioned problems and try to implement new procedures where the results show possible efficiency.

Acknowledgments

Second part of Section 4.3 has appeared essentially due to a remark of Harald Ganzinger.

Bibliography

Andrews, P. (1981), 'Theorem proving via general matings', *Journal of the Association for Computing Machinery* **28**(2), 193–214.

Bachmair, L. & Ganzinger, H. (1994), Rewrite techniques for transitive relations, *in* 'Proc. IEEE Conference on Logic in Computer Science (LICS)', IEEE Computer Society Press.

Bachmair, L., Ganzinger, H. & Voronkov, A. (1998), Brand's transformation with ordering constraints, *in* 'CADE'98'. To be submitted.

Beckert, B. & Hähnle, R. (1992), An improved method for adding equality to free variable semantic tableaux, *in* D. Kapur, ed., '11th International Conference on Automated Deduction (CADE)', Vol. 607 of *Lecture Notes in Artificial Intelligence*, Springer Verlag, Saratoga Springs, NY, USA, pp. 678–692.

Beltyukov, A. (1976), 'Decidability of the universal theory of natural numbers with addition and divisibility (in Russian)', *Zapiski Nauchnyh Seminarov LOMI* **60**, 15–28. English translation in: Journal of Soviet Mathematics.

Bibel, W. (1980), A theoretical basis for the systematic proof procedure, *in* P. Dembinski, ed., 'Proc. of 9th Symposium on Mathematical Foundations of Computer Science', Vol. 88 of *Lecture Notes in Computer Science*, Rydzzyna, Poland, pp. 154–167.

Bibel, W. (1981), 'On matrices with connections', *Journal of the Association for Computing Machinery* **28**(4), 633–645.

Bibel, W. (1982*a*), 'A comparative study of several proof procedures', *Artificial Intelligence* **18**(3), 269–293.

Bibel, W. (1982*b*), Computationally improved versions of Herbrand's theorem, *in* J. Stern, ed., 'Proceedings of the Herbrand Symposium. Logic Colloquium'81', North Holland, pp. 11–28.

Bibel, W. (1987), *Automated theorem proving*, Vieweg Verlag. 2nd edition.

Bibel, W. & Eder, E. (1993), Methods and calculi for deduction, *in* D. Gabbay, C. Hogger & J. Robinson, eds, 'Handbook of Logic in Artificial Intelligence and Logic Programming', Vol. 1, Oxford University Press, chapter 3, pp. 67–182.

Börger, E., Grädel, E. & Gurevich, Y. (1997), *The Classical Decision Problem*, Springer Verlag.

Degtyarev, A., Gurevich, Y., Narendran, P., Veanes, M. & Voronkov, A. (1997), The decidability of simultaneous rigid E-unification with one variable, UPMAIL Technical Report 139, Uppsala University, Computing Science Department. To appear in Theoretical Computer Science.

Degtyarev, A., Gurevich, Y. & Voronkov, A. (1996), Herbrand's theorem and equational reasoning: Problems and solutions, *in* 'Bulletin of the European Association for Theoretical Computer Science', Vol. 60, pp. 78–95. The "Logic in Computer Science" column.

Degtyarev, A., Matiyasevich, Y. & Voronkov, A. (1996), Simultaneous rigid E-unification and related algorithmic problems, *in* 'Eleventh Annual IEEE Symposium on Logic in Computer Science (LICS'96)', IEEE Computer Society Press, New Brunswick, NJ, pp. 494–502.

Degtyarev, A. & Voronkov, A. (1995), Equality elimination for the inverse method and extension procedures, *in* C. Mellish, ed., 'Proc. International Joint Conference on Artificial Intelligence (IJCAI)', Vol. 1, Montréal, pp. 342–347.

Degtyarev, A. & Voronkov, A. (1996*a*), Decidability problems for the prenex fragment of intuitionistic logic, *in* 'Eleventh Annual IEEE Symposium on Logic in Computer Science (LICS'96)', IEEE Computer Society Press, New Brunswick, NJ, pp. 503–512.

Degtyarev, A. & Voronkov, A. (1996*b*), Equality elimination for the tableau method, *in* J. Calmet & C. Limongelli, eds, 'Design and Implementation of Symbolic Computation Systems. International Symposium, DISCO'96', Vol. 1128 of *Lecture Notes in Computer Science*, Karlsruhe, Germany, pp. 46–60.

Degtyarev, A. & Voronkov, A. (1996*c*), Simultaneous rigid E-unification is undecidable, *in* H. Kleine Büning, ed., 'Computer Science Logic. 9th International Workshop, CSL'95', Vol. 1092 of *Lecture Notes in Computer Science*, Paderborn, Germany, September 1995, pp. 178–190.

Degtyarev, A. & Voronkov, A. (1996*d*), 'The undecidability of simultaneous rigid E-unification', *Theoretical Computer Science* **166**(1–2), 291–300.

Degtyarev, A. & Voronkov, A. (1998), 'What you always wanted to know about rigid E-unification', *Journal of Automated Reasoning* **20**(1), 47–80.

Dwork, C., Kanellakis, P. & Mitchell, J. (1984), 'On the sequential nature of unification', *Journal of Logic Programming* **1**, 35–50.

Dwork, C., Kanellakis, P. & Stockmeyer, L. (1988), 'Parallel algorithms for term matching', *SIAM Journal of Computing* **17**(4), 711–731.

Eder, E. (1988), A comparison of the resolution calculus and the connection method, and a new calculus generalizing both methods, *in* E. Börger, G. Jäger, H. Kleine Büning & M. Richter, eds, 'CSL'88 (Proc. 2nd Workshop on Computer Science Logic)', Vol. 385 of *Lecture Notes in Computer Science*, Springer Verlag, pp. 80–98.

Eder, E. (1991), Consolution and its relation with resolution, *in* 'Proc. International Joint Conference on Artificial Intelligence (IJCAI)', pp. 132–136.

Fermüller, C. & Leitsch, A. (1997), 'Decision procedures and model building in equational clause logic', *Journal of the IGPL* . To appear.

Fermüller, C., Leitsch, A., Tammet, T. & Zamov, N. (1993), *Resolution Methods for the Decision Problem*, Vol. 679 of *Lecture Notes in Computer Science*, Springer Verlag.

Fitting, M. (1996), *First Order Logic and Automated Theorem Proving*, Springer Verlag, New York. Second edition.

Gallier, J. (1986), *Logic for Computer Science: Foundations of Automatic Theorem Proving*, Harper and Row, New York.

Gallier, J., Raatz, S. & Snyder, W. (1987), Theorem proving using rigid E-unification: Equational matings, *in* 'Proc. IEEE Conference on Logic in Computer Science (LICS)', IEEE Computer Society Press, pp. 338–346.

Gurevich, Y. & Veanes, M. (1997), Some undecidable problems related to the Herbrand theorem, UPMAIL Technical Report 138, Uppsala University, Computing Science Department.

Gurevich, Y. & Voronkov, A. (1997*a*), Monadic simultaneous rigid E-unification and related problems, UPMAIL Technical Report 137, Uppsala University, Computing Science Department. Revised June 20, 1997. To appear in Theoretical Computer Science.

Gurevich, Y. & Voronkov, A. (1997*b*), Monadic simultaneous rigid E-unification and related problems, *in* P. Degano, R. Corrieri & A. Marchetti-Spaccamella, eds, 'Automata, Languages and Programming. 24th International Colloquium, ICALP'97', Vol. 1256 of *Lecture Notes in Computer Science*, Bologna, Italy, pp. 154–165.

Herbrand, J. (1972), *Logical Writings*, Harvard University Press.

Joyner jr, W. (1976), 'Resolution strategies as decision procedures', *Journal of the Association for Computing Machinery* **23**, 398–417.

Kościelski, A. & Pacholski, L. (1996), 'Complexity of Makanin's algorithm', *Journal of the Association for Computing Machinery* **43**(4), 670–684.

Leitsch, A. (1997), *The Resolution Calculus*, Springer Verlag.

Lipshitz, L. (1978), 'The Diophantine problem for addition and divisibility', *Transactions of the American Mathematical Society* **235**, 271–283.

Lipshitz, L. (1981), 'Some remarks on the Diophantine problem for addition and divisibility', *Bull. Soc. Math. Belg. Sér. B* **33**(1), 41–52.

Loveland, D. (1968), 'Mechanical theorem proving by model elimination', *Journal of the Association for Computing Machinery* **15**, 236–251.

Loveland, D. (1978), *Automated Theorem Proving: a Logical Basis*, North Holland.

Lyaletski, A. (1981), 'A variant of Herbrand's theorem for prenex formulas', *Cybernetics* **17**, 112–116.

Mart'janov, V. (1977), 'Universal extended theories of integers', *Algebra i Logika* **16**(5), 588–602.

Maslov, S., Mints, G. & Orevkov, V. (1983), Mechanical proof-search and the theory of logical deduction in the USSR, *in* J.Siekmann & G.Wrightson, eds, 'Automation of Reasoning (Classical papers on Computational Logic)', Vol. 1, Springer Verlag, pp. 29–38.

Moser, M., Lynch, C. & Steinbach, J. (1995), Model elimination with basic ordered paramodulation, Technical Report AR-95-11, Fakultät für Informatik, Technische Universität München, München.

Papadimitriou, C. (1994), *Computational Complexity*, Addison-Wesley.

Petermann, U. (1993), A framework for integrating equality reasoning into the extension procedure, *in* D. Basin, R. Hähnle, B. Fronhöfer, J. Posegga & C. Schwind, eds, 'Proc. Workshop on Theorem Proving with Analytic Tableaux and Related Methods', pp. 195–207.

Plaisted, D. (1995), Special cases and substitutes for rigid E-unification, Technical Report MPI-I-95-2-010, Max-Planck-Institut für Informatik.

Prawitz, D. (1970), A proof procedure with matrix reduction, *in* M. Laudet, L. Lacombe, L. Nolin & M. Schutzenberger, eds, 'Symp. on Automatic Demonstration', Vol. 125 of *Lecture Notes in Mathematics*, Springer Verlag, pp. 207–213.

Schulz, K. (1990), Makanin's algorithm: Two improvements and a generalization, *in* K. Schulz, ed., 'Proceedings of the First International Workshop on Word Equations and Related Topics, Tübingen', number 572 *in* 'Lecture Notes in Computer Science'.

Stickel, M. (1985), 'Automated deduction by theory resolution', *Journal of Automated Reasoning* **1**, 333–355.

Veanes, M. (1997), The undecidability of simultaneous rigid E-unification with two variables, *in* G. Gottlob, A. Leitsch & D. Mundici, eds, 'Computational Logic and Proof Theory. 5th Kurt Gödel Colloquium, KGC'97', Vol. 1289 of *Lecture Notes in Computer Science*, Vienna, Austria, pp. 305–318.

Voda, P. & Komara, J. (1995), On Herbrand skeletons, Technical report, Institute of Informatics, Comenius University Bratislava.

Voronkov, A. (1996), Proof search in intuitionistic logic based on constraint satisfaction, *in* P. Miglioli, U. Moscato, D. Mundici & M. Ornaghi, eds, 'Theorem Proving with Analytic Tableaux and Related Methods. 5th International Workshop, TABLEAUX '96', Vol. 1071 of *Lecture Notes in Artificial Intelligence*, Terrasini, Palermo Italy, pp. 312–329.

Voronkov, A. (1997*a*), The ground-negative fragment of first-order logic is Π_2^p-complete, UPMAIL Technical Report 144, Uppsala University, Computing Science Department. To appear in the Journal of Symbolic Logic.

Voronkov, A. (1997*b*), Strategies in rigid-variable methods, *in* M. Pollack, ed., 'Proc. of the Fifteenth International Joint Conference on Artificial Intelligence (IJCAI-97)', Vol. 1, Nagoya, Japan, pp. 114–119.

Yasuura, H. (1984), On parallel computational complexity of unification, *in* 'Proc. of the Conference on Fifth Generation Computer Systems', ICOT, pp. 235–243.