Superposition for Fixed Domains

Matthias Horbach and Christoph Weidenbach

Max-Planck-Institut für Informatik
Saarbrücken, Germany
{horbach,weidenb}@mpi2.de

Abstract. Superposition is an established decision procedure for a variety of first-order logic theories represented by sets of clauses. A satisfiable theory, saturated by superposition, implicitly defines a perfect term-generated model for the theory. Proving universal properties with respect to a saturated theory directly leads to a modification of the perfect model’s term-generated domain, as new Skolem functions are introduced. For many applications, this is not desired. Therefore, we propose the first superposition calculus that can explicitly represent existentially quantified variables and can thus compute with respect to a given domain. This calculus is sound and complete for a first-order fixed domain semantics. For some classes of formulas and theories, we can even employ the calculus to prove properties of the perfect model itself, going beyond the scope of known superposition based approaches.

1 Introduction

One of the most powerful calculi for first-order logic with equality is superposition [1, 13, 16]. This is in particular demonstrated by superposition instances effectively deciding almost any known decidable classical subclass of first-order logic, e.g. the monadic class with equality [2] or the guarded fragment with equality [7], as well as a number of decidable first-order classes that have been proven decidable for the first time by means of the superposition calculus [12, 9, 15, 10]. The key to this success is an inherent redundancy notion based on the term-generated minimal model $I_N$ of a clause set $N$. If all inferences from a clause set $N$ are redundant (then $N$ is called saturated) and $N$ does not contain the empty clause, then $I_N$ is a minimal model of $N$.

A formula $\Phi$ is entailed by a clause set $N$ with respect to the standard first-order semantics, written $N \models \Phi$, if $\Phi$ holds in all models of $N$ over all possible domains. For a number of applications, this is not the desired semantics. Instead, only Herbrand models of $N$ over the signature $\mathcal{F}$ should be considered, written $N \models^H \Phi$. Even stronger, the validity of $\Phi$ is considered with respect to the model $I_N$, written $I_N \models \Phi$ or alternatively $N \models^H \Phi$. It holds that $I_N \in \{M \mid M \models^F N\} \subseteq \{M \mid M \models N\}$ and the opposite inclusions hold for the sets of valid formulas: $\{\Phi \mid N \models^H \Phi\} \supseteq \{\Phi \mid N \models^F \Phi\} \supseteq \{\Phi \mid N \models \Phi\}$.

Consider the following small example, demonstrating the differences of the three semantics. The clause set $N = \{ \rightarrow G(s(0), 0), G(x, y) \rightarrow G(s(x), s(y)) \}$
is finitely saturated by superposition, where the domain of \( I_N \) is isomorphic to the naturals and \( G_{I_N} \) is a subset of the greater relation. Now for the different entailment relations the following holds:

\[
\begin{align*}
N & = G(s(s(0)), s(0)) \quad N \models G(s(s(0)), s(0)) \quad N \models_{\text{ind}} G(s(s(0)), s(0)) \\
N & \neq \forall x. G(s(x), x) \quad N \models \forall x. G(s(x), x) \quad N \models_{\text{ind}} \forall x. G(s(x), x) \\
N & \neq \forall x. \neg G(x, x) \quad N \models \forall x. \neg G(x, x) \quad N \models_{\text{ind}} \forall x. \neg G(x, x)
\end{align*}
\]

Superposition is a sound and complete calculus for the standard semantics \( \models \). In this paper, we develop a sound and complete calculus for \( \models_{\text{f}} \). Given a clause set \( N \) and a purely existentially quantified conjecture, standard superposition is also complete for \( \models_{\text{f}} \). The problem arises with universally quantified conjectures that become existentially quantified after negation. Then, as soon as these existentially quantified variables are Skolemized, the standard superposition calculus applied afterwards no longer computes modulo \( \models_{\text{f}} \), but modulo \( \models_{\text{f} \cup \{f_1, \ldots, f_n\}} \) where \( f_1, \ldots, f_n \) are the introduced Skolem functions. The idea behind our new calculus is not to Skolemize existentially quantified variables, but to treat them explicitly by the calculus. This is represented by an extended clause notion, containing a constraint for the existentially quantified variables. For example, the above conjecture \( \forall x. G(s(x), x) \) results after negation in the clause \( u \approx x \mid G(s(x), x) \to x \). In addition to standard first-order equational reasoning, the inference and reduction rules of the new calculus take also care of the constraint (see section 3).

In general, a \( \models_{\text{f}} \) unsatisfiability proof of a constrained clause set requires the computation of infinitely many empty clauses. This does not come as a surprise because we have to show that an existentially quantified clause cannot be satisfied by a term-generated infinite domain. In order to represent this infinite set of empty clauses finitely, a further induction rule, based on the minimal model semantics \( \models_{\text{ind}} \), can be employed. We prove the new rule sound in section 4 and show its potential. In general, our calculus can cope with (conjecture) formulas of the form \( \forall x. \exists \Phi \) and does not impose special conditions on \( N \) (except saturation for \( \models_{\text{ind}} \)), which is beyond any known result on superposition based calculi proving properties of \( \models_{\text{f}} \) or \( \models_{\text{ind}} \) [11, 4, 8, 3, 6, 14]. This, together with potential extensions and directions of research, is discussed in the final section 5.

2 Preliminaries

We build on the notions of [1, 16] and shortly recall here the most important concepts as well as the specific extensions needed for the new superposition calculus. Let \( \mathcal{F} \) be a signature, i.e., a set of function symbols of fixed arity, and \( X \) an infinite set of variables. We denote by \( \mathcal{T} (\mathcal{F}, X) \) the set of all terms over \( \mathcal{F} \) and \( X \) and by \( \mathcal{T} (\mathcal{F}) \) the set of ground terms over \( \mathcal{F} \). A (standard universal) clause is a pair of multisets of equations, written \( \Gamma \to \Delta \), interpreted as the conjunction of all atoms in \( \Gamma \) implying the disjunction of all atoms in \( \Delta \). The empty clause is denoted by \( \Box \). Any (reduction) ordering \( \prec \) on terms can be lifted to clauses in the usual way as its twofold multiset extension over equations and
clauses (cf. [1]). Predicates can be encoded in this setting as equations with a special "true" constant on the right hand side as usual. Please note that in this case we consider a many-sorted framework where the predicative sort is separated from the sort of all other terms. As there are no variables of the predicative sort, we never explicitly express the sorting.

By \( t[\sigma] \) we denote the subterm of \( t \) at position \( p \). The term that arises from \( t \) by replacing the subterm at position \( p \) by the term \( r \) is \( t[r]^\sigma \). A substitution \( \sigma \) is a map from a set \( X' \subseteq X \) of variables to \( T(F, X) \), where the domain \( \text{dom}(\sigma) = \{x \in X' \mid x \sigma \neq x\} \) is finite. The most general unifier of two terms \( s, t \in T(F, X) \) is denoted by \( \text{mgu}(s, t) \). Remark that, even if we consider predicates, there are no variables of the predicative sort and hence substitutions do not introduce symbols of this sort.

A Herbrand interpretation over the signature \( F \) is a congruence on the ground terms \( T(F) \). We recall the construction of the special Herbrand interpretation \( \mathcal{I}_N \) derived from a clause set \( N \) in [1]. If \( N \) is consistent and saturated with respect to a certain inference system, then \( \mathcal{I}_N = N \) and \( \mathcal{I}_N \) is called a minimal model of \( N \). Let \( \prec \) be a well-founded reduction ordering that is total on ground terms. We use induction on the clause ordering \( \prec \) to define sets of equations \( E_C \), \( R_C \) and \( I_C \) for all ground clauses over \( T(F) \) by \( R_C = \bigcup_{C \subseteq C'} E_C \), and \( I_C = R_C \), i.e. the reflexive, transitive closure of \( R_C \). Moreover \( E_C = \{s \preceq t\} \) (and we say that \( C \) produces \( s \preceq t\), if \( C \rightarrow \Delta, s \preceq t \) is a ground instance of a clause from \( N \) such that (i) \( s \succ t \) and \( s \preceq t \) is a strictly maximal occurrence of an equation in \( C \), (ii) \( s \) is irreducible by \( R_C \), (iii) \( \Gamma \subseteq I_C \), and (iv) \( \Delta \cap I_C = \emptyset \). Otherwise \( E_C = \emptyset \). Finally, we define the confluent and terminating ground rewrite system \( R = \bigcup C E_C \) as the set of all produced equations and set \( \mathcal{I}_N = R^* \) over the domain \( T(F) \).

We distinguish a finite set \( V \subseteq X \) of existential variables. Elements of \( V \) are denoted as \( u, v \) and elements of \( X \setminus V \) as \( x, y, z \). A constrained clause \( v_1 \approx t_1, \ldots, v_n \approx t_n \mid C \) consists of a sequence of equations \( v_1 \approx t_1, \ldots, v_n \approx t_n \), called the constraint and a clause \( C \), such that \( V = \{v_1, \ldots, v_n\} \), \( v_i \neq v_j \) for \( i \neq j \), and neither \( C \) nor \( t_1, \ldots, t_n \) contain an existential variable. In particular, constraints always constitute a solved unification problem. The constrained clause is called ground if \( C \) and \( t_1, \ldots, t_n \) are ground. A constraint \( \alpha \) induces a substitution \( \mathbb{V} \rightarrow T(F, X) \), which we will denote by \( \sigma_n \).

Constrained clauses are considered equal up to renaming of non-existential variables. For example, the clauses \( u \approx x, v \approx y \mid P(x) \) and \( u \approx x, v \approx y \mid P(y) \) are considered equal, but they are both different from \( u \approx x, v \approx y \mid P(x) \). If the universal variable \( x \) does not appear in \( C \), we abbreviate \( v_1 \approx t_1, \ldots, v_n \approx t_n, v \approx x \mid C \) as \( v_1 \approx t_1, \ldots, v_n \approx t_n \mid C \). A clause \( \mid C \) is unconstrained. If \( V = \{v_1, \ldots, v_n\} \), and \( x_1, \ldots, x_m \) are the non-existential variables in a clause set \( N \), the semantics of \( N \) is \( \exists \mathbb{V} \forall \mathbb{V} \bigwedge_{\{C \mid C \in N \}} \alpha \rightarrow C \). i.e. an interpretation \( M \) is said to model \( N \), written \( M \models N \) iff the formula \( \exists \mathbb{V} \forall \mathbb{V} \bigwedge_{\{C \mid C \in N \}} \alpha \rightarrow C \) is valid in \( M \).

We extend \( \prec \) to constraints by \( v_1 \approx s_1, \ldots, v_n \approx s_n \prec v_1 \approx t_1, \ldots, s_n \approx t_n \) if \( s_1 \prec t_1 \wedge \ldots \wedge s_n \prec t_n \) and \( s_1 \neq t_1 \vee \ldots \vee s_n \neq t_n \). Constrained clauses are ordered lexicographically with priority on the constraint, i.e. \( \alpha \mid C \prec \beta \mid D \) iff \( \alpha \prec \beta \),
or $\alpha = \beta$ and $C < D$. This ordering is not total on ground clauses, but strong enough to support our completeness result and the usual notion of redundancy.

We use the symbols $\forall$ and $3$ both in first-order formulas and on the meta level, where they are also used for higher-order quantification.

3 First-Order Reasoning in Fixed Domains

In this section, we will give a saturation procedure for sets of constrained clauses over a domain $\mathcal{T}(F)$ and show how it is possible to decide whether a saturated clause set possesses a Herbrand model over $\mathcal{F}$.

We consider the following inference rules, which are defined with respect to a reduction ordering $< \text{ on } \mathcal{T}(\mathcal{F}, X)$ that is total on ground terms. Most of the rules are quite similar to the usual superposition rules, just generalizad to constrained clauses. However, they also require additional treatments of the constraints. To simplify the presentation below we do not enrich the calculus by the use of a negative literal selection function, although this is also possible. As usual, we consider the universal variables in different appearing clauses to be renamed apart. If $\alpha_1 = s_1 \approx t_1, \ldots, s_n \approx t_n$ and $\alpha_2 = s_1' \approx t_1', \ldots, s_n' \approx t_n'$ are two constraints, then we write $\alpha_1 \approx \alpha_2$ for the equations $s_1 \approx t_1, \ldots, s_n \approx t_n$, which do not contain any existential variables, and we write $\text{mgu}(\alpha_1, \alpha_2)$ for the most general common unifier of $(s_1, t_1), \ldots, (s_n, t_n)$.

Equality Resolution:
\[
\frac{\alpha \parallel (\Gamma, s \approx t) \rightarrow \Delta}{(\alpha \parallel (\Gamma \rightarrow \Delta) \sigma}
\]
where (i) $\sigma = \text{mgu}(s, t)$ and (ii) $(s \approx t) \sigma$ is maximal in $(\Gamma, s \approx t) \rightarrow \Delta) \sigma$.

Equality Factoring:
\[
\frac{\alpha \parallel (\Gamma \rightarrow \Delta, s \approx t, s' \approx t')}{(\alpha \parallel (\Gamma, t \approx t', \rightarrow \Delta, s \approx t') \sigma}
\]
where (i) $\sigma = \text{mgu}(s, s')$, (ii) $(s \approx t) \sigma$ is maximal in $(\Gamma \rightarrow \Delta, s \approx t, s' \approx t') \sigma$, and (iii) $t \sigma \not\approx s \sigma$.

Superposition, Right:
\[
\frac{\alpha_1 \parallel \Gamma_1 \rightarrow \Delta_1, t \approx r \quad \alpha_2 \parallel \Gamma_2 \rightarrow \Delta_2, s[l'] \approx t}{(\alpha_1 \parallel (\Gamma_1, \Gamma_2 \rightarrow \Delta_1, \Delta_2, s[r] \approx t) \sigma_1 \sigma_2}
\]
where (i) $\sigma_1 = \text{mgu}(l, l')$, $\sigma_2 = \text{mgu}(s_1 \sigma_1, s_2 \sigma_1)$, (ii) $(s \approx t) \sigma_1 \sigma_2$ is strictly maximal in $(\Gamma_1 \rightarrow \Delta_1, t \approx r) \sigma_1 \sigma_2$ and $(s \approx t) \sigma_1 \sigma_2$ is strictly maximal in $(\Gamma_2 \rightarrow \Delta_2, s \approx t) \sigma_1 \sigma_2$, (iii) $r \sigma_1 \sigma_2 \not\approx t \sigma_1 \sigma_2$ and $t \sigma_1 \sigma_2 \not\approx r \sigma_1 \sigma_2$, and (iv) $l'$ is not a variable.

Superposition, Left:
\[
\frac{\alpha_1 \parallel \Gamma_1 \rightarrow \Delta_1, t \approx r \quad \alpha_2 \parallel \Gamma_2, s[l'] \approx t \rightarrow \Delta_2}{(\alpha_1 \parallel (\Gamma_1, \Gamma_2 \rightarrow \Delta_1, \Delta_2) \sigma_1 \sigma_2}
\]
where (i) $\sigma_1 = \text{mgu}(l, l')$, $\sigma_2 = \text{mgu}(\alpha_1\sigma_1, \alpha_2\sigma_1)$, (ii) $(l \preccurlyeq \sigma)\sigma_1\sigma_2$ is strictly maximal in $(I_1 \rightarrow \Delta_1, l \preccurlyeq \sigma)\sigma_1\sigma_2$, (iii) $\sigma_1\sigma_2 \not\preccurlyeq l_1\sigma_2$ and $l_1\sigma_2 \not\preccurlyeq \sigma_1\sigma_2$, and (iv) $l'$ is not a variable.

Constraint Superposition:

$$
\frac{\alpha_1 \parallel I_1 \rightarrow \Delta_1, l \preccurlyeq \tau \parallel r' \parallel I_2 \rightarrow \Delta_2}{\alpha_2 \parallel (\varnothing \parallel \tau \parallel r') \parallel \alpha_2 \parallel I_1, I_2 \rightarrow \Delta_1, \Delta_2, \sigma_1\sigma_2}
$$

where (i) $\sigma = \text{mgu}(l, l')$, (ii) $(l \preccurlyeq \sigma)\sigma_1\sigma_2$ is strictly maximal in $(I_1 \rightarrow \Delta_1, l \preccurlyeq \sigma)\sigma_1\sigma_2$, (iii) $\sigma_1\sigma_2 \not\preccurlyeq l_1\sigma_2$ and (iv) $r'$ is not a variable.

Equality Elimination:

$$
\frac{\alpha_1 \parallel I \rightarrow \Delta, l \preccurlyeq \tau \parallel \alpha_2 \parallel I \rightarrow \Delta_2, \sigma_1\sigma_2}{\alpha_1 \parallel I \rightarrow \Delta, \tau \parallel \alpha_2 \parallel I \rightarrow \Delta_2, \sigma_1\sigma_2}
$$

where (i) $\sigma_1 = \text{mgu}(r, r')$, $\sigma_2 = \text{mgu}(\alpha_1\sigma_1, (\varnothing \preccurlyeq \tau r') \parallel \alpha_2)$, (ii) $(l \preccurlyeq \sigma)\sigma_1\sigma_2$ is strictly maximal in $(I \rightarrow \Delta, l \preccurlyeq \tau)\sigma_1\sigma_2$, (iii) $\sigma_1\sigma_2 \not\preccurlyeq l_1\sigma_2$, and (iv) $r'$ is not a variable.

While the other rules keep clauses with different constraints strictly separate, constraint superposition and equality elimination transfer information across these bounds, allowing to derive, e.g., $u \approx b \parallel \Box$ from $u \approx b \parallel \Box \rightarrow a \approx b$ and $u \approx a \parallel \Box$ where $a \gg b$.

This inference system contains the standard universal superposition calculus as the special case when there are no existential variables at all present, i.e., $V = \emptyset$ and all constraints are empty. The rules equality resolution, equality factoring, and superposition right and left reduce to their non-constrained counterparts and the constraint superposition and equality elimination rules become obsolete.

A ground constrained clause $\alpha \parallel C$ is called \textit{redundant} with respect to a set $N$ of constrained clauses if there are ground instances $\alpha \parallel C_1, \ldots, \alpha \parallel C_k$ of clauses in $N$, such that $C_1, \ldots, C_k \models C$ and $C_i \prec C$ for all $i$. As an alternative, we could choose $\models_{\mathcal{P}}$ for defining redundancy. A non-ground constrained clause is redundant if all its ground instances are redundant. A ground inference with conclusion $\beta \parallel B$ is called \textit{redundant} with respect to $N$ if either some premise is redundant or if there are ground instances $\beta \parallel C_1, \ldots, \beta \parallel C_k$ of clauses in $N$, such that $C_1, \ldots, C_k \models B$ and $C_1, \ldots, C_n$ are smaller than the maximal premise of the ground inference. A non-ground inference is redundant if all its ground instances are redundant. A clause set $N$ is \textit{saturated} if each inference with premises in $N$ is redundant with respect to $N$.

As constrained clauses are just special classes of clauses, the construction of a Herbrand model of $N$ is almost identical to the one for universal clause sets [1]. The main difference is that we now have to account for existential variables before starting the construction. To define a Herbrand interpretation $I_N$ of a set $N$ of constrained clauses, we proceed in two steps:

1. Let $A_N = \{ \alpha \mid (\alpha \parallel \Box) \in N \}$. Let $\alpha_N$ be a minimal ground constraint with respect to $\prec$ such that $\alpha_N$ is not an instance of any $\alpha \in A_N$ if such a
constraint exists. Otherwise we say that \( A_N \) is covering. In this case let \( \alpha_N \) be an arbitrary ground constraint.

2. The Herbrand interpretation \( I_N \) is defined as the (classical) minimal model of the unconstrained clause set \( \{ C \sigma \mid \sigma \in N \land \alpha \sigma = \alpha_N \} \).

Note that even if \( A_N \) is not covering, \( \alpha_N \) is usually not uniquely defined, e.g. \( \alpha_N = \{ u \approx s(0), v \approx s(0) \} \) or \( \alpha_N = \{ u \approx s(0), v \approx 0 \} \) for \( F = \{ 0, s \} \) and the clause set \( N = \{ u \approx 0, v \approx 0 \} \), which results in \( A_N = \{ (u \approx 0, v \approx 0) \} \).

While it is well known how the second step works, it is not that obvious that one can decide whether \( A_N \) is covering and, if it is not, effectively compute \( \alpha_N \). This is, however, possible for finite \( N \): Let \( \{ x_1, \ldots, x_m \} \subseteq X \setminus V \) be the set of non-existent variables appearing in \( A_N \). \( A_N \) is covering if and only if the formula \( \forall x_1, \ldots, x_m. \alpha_{\sigma \in A_N} \sigma \) is satisfiable in \( T(F) \). Such so-called disunification problems have been studied among others by Comon and Lescanne [5], who gave a terminating algorithm that eliminates the universal quantifiers from this formula and transforms the initial problem into an equivalent formula from which the set of solutions can easily be read off.

We will now show that a saturated constrained clause set \( N \) has a Herbrand model over \( F \) (namely \( I_N \)) if and only if \( A_N \) is not covering, and call \( I_N \) a minimal model of \( N \) in this case. Since \( I_N \) is defined via a set of unconstrained clauses, it inherits all properties of models of purely universal clause sets. Above all, we will use the property that the rewrite system \( R \) constructed in parallel with this interpretation is confluent and terminating. We write \( s \rightarrow_R r \) if there is a rule \( l \approx r \in R \), also written \( l \rightarrow \sigma \in R \), and a position \( p \) of \( s \) such that \( s = s[l]'_p \) and \( t = s[r]'_p \). In this case, \( s \) is called reducible by \( R \). The notions of positions, \( \rightarrow_R \) and reducibility lift naturally to constraints.

**Lemma 1.** Let \( N \) be saturated. If \( A_N \) is not covering then \( \alpha_N \) is irreducible by \( R \).

**Proof.** Assume that there is a position \( s \) and a rule \( l \sigma \rightarrow r \sigma \in R \) produced by a ground instance \( (\beta \mid A \rightarrow P, l \approx r) \sigma \) of a clause \( \beta \mid A \rightarrow P, l \approx r \in N \), such that \( l \sigma = \alpha_N \sigma \).

Because of the minimality of \( \alpha_N \), there must be a clause \( \gamma \parallel \Box \in N \) with \( \gamma' \models A_N \sigma \). Since by definition \( \alpha_N \) is not an instance of \( \gamma \), the position \( s \) is a non-variable position of \( \gamma \). Since furthermore \( \beta \sigma = \alpha_N = \gamma' \mid [l]'_p \), there is an equality elimination inference

\[
\frac{\beta \mid A \rightarrow P, l \approx r, \gamma \equiv \Box}{(\beta \mid A \rightarrow P)^{s_1 \sigma_1} \sigma_2 \sigma_2 = \text{mgu}(\gamma \mid \text{r}, \sigma_2)}
\]

with \( \text{dom}(\sigma_2) \cap V = \emptyset \). The instance \( (\beta \mid A \rightarrow P) \sigma \) of the result clause prevents the production of \( l \sigma \approx r \sigma \) by the above clause, which is a contradiction.

**Lemma 2.** Let \( N \) be saturated, \( A_N \) not covering and \( I_N \not\models \sigma \). If \( (\alpha \parallel C) \sigma \) is a minimal ground instance of a clause in \( N \) such that \( I_N \not\models (\alpha \parallel C) \sigma \), then \( \alpha \sigma = \alpha_N \).
Proof. Let $C = \Gamma \rightarrow \Delta$. By definition of entailment, $I_N \models \alpha_N \Rightarrow \sigma$, which is equivalent to $\alpha_N \Rightarrow_R \alpha \sigma$. We have already seen in lemma 1 that $\alpha_N$ is irreducible. Because of the confluence of $R$, either $\alpha_N = \alpha \sigma$ or $\alpha \sigma$ must be reducible.

Assume the latter, i.e., that $\alpha \sigma[p] = l\sigma'$ for a position $p$ and a rule $l \sigma' \rightarrow r \sigma' \in R$ that is produced by a class $\beta \parallel \Pi, l \sigma r \in N$. If $p$ is not a non-variable position in $\alpha$, then the rule actually reduces $\sigma$, which contradicts the minimality of $(\alpha \parallel C)\sigma$. Otherwise there is a constraint superposition inference

$$\frac{\beta \parallel \Pi, l \sigma r \quad \alpha \parallel \Gamma \rightarrow \Delta}{(\alpha \parallel [\sigma], l \sigma') \rightarrow (\beta \parallel \Pi, l \sigma r)}$$

The ground instance $\delta \| D := (\alpha \parallel [\sigma], l \sigma') \rightarrow (\beta \parallel \Pi, l \sigma r)\sigma' \in R$, of the conclusion is not true in $I_N$. On the other hand, as the inference is redundant, so is the clause $\delta \| D$, i.e., it follows from ground instances of clauses of $N$ all of which are smaller than $\delta \| D$. Since moreover $\delta \| D \prec (\alpha \parallel C)\sigma$ (remember that the ordering prioritizes constraints), all these ground instances hold in $I_N$, hence $I_N \models \delta \| D$ by minimality of $(\alpha \parallel C)\sigma$. This is a contradiction to $I_N \not\vDash \delta \| D$.

**Proposition 1.** Let $N$ be a saturated set of constrained clauses such that $A_N$ is not covering. Then $I_N \vDash N$.

**Proof.** Assume, contrary to the proposition, that $N$ is not modeled by $I_N$. Then there is a minimal ground instance $(\alpha \parallel C)\sigma$ of a clause $\alpha \parallel C \in N$ that is not modeled by $I_N$. We will refute this minimality. We proceed by a case analysis of the position of the maximal literal in $C\sigma$.

$C\sigma$ does not contain any maximal literal at all, i.e., $C = \Box$. Since $\alpha \sigma = \alpha_N$ by lemma 2, but $I_N \not\vDash \alpha \sigma \Rightarrow_{\alpha_N}$ by definition of $\alpha_N$, this cannot happen.

$C = \Gamma \rightarrow \Delta$, s\text{at} and $s\text{at} \sigma$ is maximal in $C\sigma$ with $\sigma = l\sigma$. This cannot happen because then $C\sigma$ would be a tautology.

$C = \Gamma, s\text{at} \rightarrow \Delta$ and $s\text{at} \Rightarrow \sigma$ is maximal in $C\sigma$ with $\sigma \Rightarrow \sigma$. Since $I_N \not\vDash C\sigma$, we know that $s\text{at} \sigma \Rightarrow \sigma$ is true in $I_N$, and because $R$ only rewrites larger to smaller terms $s\text{at}$ must be reducible by a rule $l\sigma' \rightarrow r\sigma' \in R$ produced by a clause $\beta \parallel \Pi, l \sigma r \in N$. So $s\text{at}[p] = l\sigma'$ for some position $p$ in $s\text{at}$.

Case 1: $p$ is a non-variable position in $s$. Since $\beta \sigma' = \alpha N = \alpha \sigma$ and $l\sigma' = l\sigma'$, there is an inference by superposition (left) as follows:

$$\frac{\beta \parallel \Pi, l \sigma r \quad \alpha \parallel \Gamma, s\text{at} \rightarrow \Delta}{(\alpha \parallel [\sigma], l \sigma') \rightarrow (\beta \parallel \Pi, l \sigma r)}$$

The ground instance $\delta \| D := (\alpha \parallel \Gamma, s\text{at} \rightarrow \Pi, \Delta) \sigma := \text{mgu}(s\text{at}[p], \sigma), \sigma_2 = \text{mgu}(\beta \sigma, \alpha \sigma)$ of the result clause is not modeled by $I_N$.

On the other hand, as the inference is redundant, so is the clause $\delta \| D$, i.e., it follows from ground instances of clauses of $N$ all of which are smaller than $\delta \| D$. Since moreover $\delta \| D \prec (\alpha \parallel C)\sigma$, all these ground instances hold in $I_N$, whence $I_N \not\vDash \delta \| D$. A contradiction.

Case 2: $p = \beta \parallel \beta''$, where $s\text{at}[p] = x$ is a variable. Then $(x\sigma)[p] = l\sigma$. If $\tau$ is the substitution that coincides with $\sigma$ except that $x\tau = x\sigma[p']$, then $I_N \not\vDash C\tau$ and $C\tau$ contradicts the minimality of $C\sigma$. 


The other cases are handled analogously.

For the construction of $I_N$, we choose $a_N$ to be minimal. For non-minimal $a_N$, the proposition does not hold: If, e.g., $N = \{u \approx a \rightarrow a \approx b, u \approx b \rightarrow a \approx b\}$ and $a \succ b$, then $N$ is saturated, but $N$ implies $u \approx a \not\models \square$. So the model constructed with $a_N' = \{u \approx a\}$ is not a model of $N$. On the other hand, $A_N$ is not covering whenever $N$ has any Herbrand model over $\mathcal{F}$:

**Proposition 2.** Let $N$ be a set of clauses such that $A_N$ is covering. Then $N$ does not have any Herbrand model over $\mathcal{F}$.

**Proof.** Let $M$ be a Herbrand model of $N$ over $\mathcal{F}$. Then

$$
M \models \{ (\alpha \not\models \square) \mid (\alpha \not\models \square) \in N \} \\
\iff \exists \tau \forall (\alpha \not\models \square) \in N. \tau(T(\mathcal{F}) \not\models \alpha \not\models \tau \not\models \square) \\
\iff \exists \tau \forall (\alpha \not\models \square) \in N. M \models \alpha \not\models \tau \\
\iff \exists \tau \forall (\alpha \not\models \square) \in N. T(\mathcal{F}) \not\models \alpha \not\models \tau 
$$

where $\alpha : V \rightarrow T(\mathcal{F})$ and $\tau : X \rightarrow T(\mathcal{F})$. But then the constraint $\bigwedge_{v \in V} v \approx w \not\models \square$ is not an instance of the constraint of any clause of the form $\alpha \not\models \square$, so $A_N$ is not covering.

A saturated clause set $N$ for which $A_N$ is covering may nevertheless have both non-Herbrand models and Herbrand models over an extended signature: If $\mathcal{F} = \{a\}$ and $N = \{u \approx a \not\models \square\}$, then $A_N$ is covering, but any standard first-order interpretation with a universe of at least two elements is a model of $N$.

Propositions 1 and 2 constitute the following theorem:

**Theorem 1.** Let $N$ be a saturated set of constrained clauses. Then $N$ has a Herbrand model over $\mathcal{F}$ iff $A_N$ is not covering.

Moreover, the classical notions of theorem proving derivations and fairness from $\vdash$ carry over to our setting. A finite or countably infinite theorem proving derivation is a sequence $N_0, N_1, \ldots$ of constrained clause sets, written $N_0 \vdash N_1 \vdash \ldots$, such that either

- (Deduction) $N_{i+1} = N_i \cup \{C\}$ and $N_i \vdash \tau \vdash N_{i+1}$, or
- (Deletion) $N_{i+1} = N_i \setminus \{C\}$ and $C$ is redundant with respect to $N_i$.

We may use our existential superposition calculus for deductions in a theorem proving derivation:

**Proposition 3.** Let $\alpha \not\models C$ be the conclusion of an inference with premises in $N$. Then $N \not\models \{\alpha \not\models C\}$. More precisely: if $\tau : V \rightarrow T(\mathcal{F})$ is a substitution then $N\tau \models N\tau \cup \{\alpha \not\models \tau \rightarrow C\tau\}$.

**Proof.** Let $\alpha \not\models C$ be the conclusion of an inference from $\alpha_1 \not\models C_1, \alpha_2 \not\models C_2 \in N$. Then $\alpha_1 \not\models C\tau$ is (modulo (unconstrained) equality resolution) an instance of the conclusion of a standard paramodulation inference from $\alpha_1 \tau \rightarrow C_1\tau$ and $\alpha_2 \tau \rightarrow C_2\tau$. Because of the soundness of the paramodulation rules, we have $N\tau \models N\tau \cup \{\alpha \not\models \tau \rightarrow C\tau\}$. 


A derivation using our calculus is fair if every inference with premises in \( \bigcup_{j \geq 2} N_j \) is redundant with respect to \( \bigcup_{j} N_j \). As usual, fairness can be ensured by systematically adding conclusions of non-redundant inferences, making this inference redundant.

As it relies on redundancy and fairness rather than a concrete inference system, the proof of the next theorem is exactly as in the unconstrained case:

**Theorem 2.** Let \( N_0, N_1, \ldots \) be a fair theorem proving derivation. \( \bigcup_{j \geq 2} N_j \) is saturated, and this set has a Herbrand model over \( \mathcal{F} \) if and only if \( N_0 \) does.

## 4 Finite Domain and Minimal Model Validity of Constrained Clauses

Given a clause set \( N \), we are often not only interested in the (un)satisfiability of \( N \) (with or without respect to a fixed domain), but also in properties of Herbrand models of a satisfiable clause set \( N \) over \( \mathcal{F} \), especially of the model \( I_N \).

These are not always disjoint problems: For some \( N \), whole classes of first-order properties and properties of \( I_N \) coincide, so that we can explore the latter with first-order techniques:

**Proposition 4.** If \( N \) is a saturated set of unconstrained Horn clauses and \( \Gamma \) is a conjunction of positive literals with existential closure \( \exists \forall \Gamma \), then

\[
N \models \exists \forall \Gamma \iff N \models \exists \forall \Gamma
\]

**Proof.** \( N \models \exists \forall \Gamma \) holds iff the set \( N \cup \{ \forall \exists, \neg \Gamma \} \) is unsatisfiable. \( N \) is Horn, so during saturation of \( N \cup \{ \neg \Gamma \} \) using a set-of-support strategy (which is complete as \( N \) is saturated), only purely negative, hence non-productive, clauses can appear. So \( N \cup \{ \forall \exists, \neg \Gamma \} \) is unsatisfiable iff \( N \not\models \exists \forall \neg \exists, \neg \forall \Gamma \), which is in turn equivalent to \( N \not\models \exists \forall \Gamma \).

If \( N \) and \( \Gamma \) additionally belong to the Horn fragment of a first-order logic (clause) class decidable by (unconstrained) superposition, such as the monadic class with equality [2] or the guarded fragment with equality [7], it is thus decidable whether \( N \models \exists \forall \Gamma \).

Our goal in this section is to extend these results further. We will first show how to use our superposition calculus to prove or refute the validity of a set \( H \) of constrained clauses with respect to a Herbrand model \( \mathcal{M} \) over \( \mathcal{F} \) of a saturated clause set \( N \), i.e. to decide whether or not \( \mathcal{M} \models H \) (Theorem 3). Moreover, we will demonstrate classes of clause sets \( N \) and properties \( H \) for which \( \models \exists \forall H \) and \( N \models \exists \forall H \) coincide (Proposition 5). Finally, we will look at ways to improve the termination of our approach for properties of \( I_N \) (Theorem 4).

Since existential variables of \( N \) and \( H \) can be renamed apart and then do not interact in our inference system, we can and will assume that \( N \) consists only of unconstrained clauses.

As in the unconstrained context, a set-of-support strategy is complete for our calculus if the support set is saturated. We write \( H \vdash^* N \) if \( N \cup H \vdash^* N \cup H' \) using \( N \) as set of support.
Theorem 3. Let $N$ be saturated and let $H \models \gamma$ for each Herbrand model $M$ of $N$ over $\mathcal{F}$.

Proof. This is a direct consequence of theorem 2 in the context of a set-of-support strategy for $N$.

Example 1. We consider the partial definition of the usual ordering on the naturals given by $N = \{ \rightarrow G(s(0),0), \rightarrow G(x,y) \rightarrow G(s(x),s(y)) \}$, as shown in the introduction. We want to check whether or not $N \not\models \forall x. G(s(x), x)$. The first steps of a possible derivation are as follows:

\[
\begin{align*}
\text{clauses in } N: & \quad 1 : \quad G(s(0),0) \\
& \quad 2 : \quad G(x,y) \rightarrow G(s(x),s(y)) \\
\text{negated conjecture: } & \quad 3 : \quad \neg G(s(x),x) \\
\text{superposition(1,3) } & \quad 4 : \quad u \neg s(0) \\
\text{superposition(2,3) } & \quad 5 : \quad u \neg s(x) \\
\text{superposition(1,5) } & \quad 6 : \quad u \neg s(0) \\
\text{superposition(2,5) } & \quad 7 : \quad u \neg s(s(z))
\end{align*}
\]

If the sequel, we repeatedly superpose clauses 1 and 2 into (descendants of) clause 5 and successively derive all clauses of the forms $u \neg s^n(0) \parallel \square$ and $u \neg s^n(x) \parallel G(s(x),x) \rightarrow$, where, e.g., $s^n(0)$ denotes the $n$-fold application $s(\ldots(s(0))\ldots)$ of $s$ to 0. Since the constraints of the derived $\square$ clauses are covering, we know that $N \not\models \forall x. G(s(x), x)$.

Given our superposition calculus for fixed domains, we can show that a result similar to proposition 4 holds for positive universal clauses.

Proposition 5. If $N$ is a saturated set of (unconstrained) Horn clauses and $\Gamma$ is a conjunction of positive literals with universal closure $\forall \mathbf{v}. \Gamma$, then

$N \models \forall \mathbf{v}. \Gamma \iff N \models \forall \mathbf{v}. \Gamma$

Proof. $N \models \forall \mathbf{v}. \Gamma$ holds iff $N \cup \{ \exists \mathbf{v}. \neg \Gamma \}$ does not have a Herbrand model over $\mathcal{F}$. If $N \cup \{ \exists \mathbf{v}. \neg \Gamma \}$ does not have a Herbrand model over $\mathcal{F}$, then obviously $N \not\models \forall \mathbf{v}. \Gamma$. Otherwise, the minimal models of $N$ and $N \cup \{ \exists \mathbf{v}. \neg \Gamma \}$ are identical, since during the saturation of $N \cup \{ \parallel \Gamma \rightarrow \}$ with our algorithm using a set-of-support strategy (which again is complete as $N$ is saturated), only purely negative, hence non-productive, clauses can appear. This in turn just means that $N \equiv \forall \mathbf{v}. \neg \Gamma$.

Using proposition 5, we can decide properties of minimal models for which neither the approach of Ganzinger and Stuber [8] nor the one of Comon and Nieuwenhuis [6] works.

Example 2. Consider yet another partial definition of the usual ordering on the naturals given by the saturated set $N = \{ \rightarrow G(s(x),0), \rightarrow G(x,y) \rightarrow G(x,0) \}$ over the signature $\mathcal{F} = \{ 0, s \}$. We want to prove both $N \not\models \forall x, y. G(x, y)$ and
\[ N \not\equiv_{\text{ind}} \forall x, y. G(x, y) \]. We start with the clause \( u \approx x, v \approx y \parallel G(x, y) \) and do the following one step derivation:

\[
\begin{align*}
\text{clauses in } N: & \quad 1: \quad u \approx x, v \approx y \parallel G(s(x), 0) \\
& \quad 2: \quad G(x, s(y)) \parallel G(x, 0) \\
\text{negated conjecture: } 3: & \quad u \approx x, v \approx y \parallel G(x, y) \\
\text{superposition(1,3) = } 4: & \quad u \approx s(x), v \approx 0 \parallel \square 
\end{align*}
\]

All further inferences are redundant, thus the counter examples to the query are exactly those for which no \( \square \) clause was derived, i.e. instantiations of \( u \) and \( v \) which are not an instance of \( \{ u \mapsto s(x), v \mapsto 0 \} \). Hence these counter examples take on exactly the form \( \{ u \mapsto 0, v \mapsto t_2 \} \) or \( \{ u \mapsto t_1, v \mapsto s(t_2) \} \) for any \( t_1, t_2 \in T(F) \). Thus we know that \( N \not\equiv_{\mathcal{F}} \forall x, y. G(x, y) \), but since the query is positive, we also know that \( N \not\equiv_{\text{ind}} \forall x, y. G(x, y) \).

In comparison, the base approach by Ganzinger and Stuber starts a derivation with the clause \( G(x, y) \), derives in one step the potentially productive clause \( G(x, 0) \) and finishes with the answer “don’t know”. The extended approach that uses the predicate gnd defined by \( \{ \rightarrow \, \text{gnd}(0), \text{gnd}(x) \rightarrow \text{gnd}(s(x)) \} \) starts the derivation with the clause \( \text{gnd}(x), \text{gnd}(y) \rightarrow G(x, y) \), where at least one of \( \text{gnd}(x) \) and \( \text{gnd}(y) \) is selected, and diverges.

The approach by Comon and Nieuwenhuis fails as well. Before starting the actual derivation, a so-called I-axiomatization of the negation of \( G \) has to be computed. This involves a quantifier elimination procedure as in [5], that fails since \( G \) is not universally reductive (because, e.g., the head of one clause does not contain all variables of the clause): \( G \) is defined in the minimal model \( I_N \) by \( G(x, y) \iff (y \neq 0 \land \exists u. x = s(u)) \lor (y = 0 \land \exists v. G(x, s(v))) \), so its negation is defined by \( \neg G(x, y) \iff (y \neq 0 \lor \forall u. x \neq s(u)) \land (y \neq 0 \lor \forall v. \neg G(x, s(v))) \).

Quantifier elimination simplifies this to \( \neg G(x, y) \iff (y \neq 0 \lor x = 0) \land (y \neq 0 \lor \forall v. \neg G(x, s(v))) \) but cannot get rid of the remaining universally quantified.

As we have seen in example 1, a proof of \( \equiv_{\mathcal{F}} \) validity often requires the computation of infinitely many empty clauses. This is not surprising, because we have to show that an existentially quantified clause cannot be satisfied by a term-generated infinite domain. In the context of a concrete model \( M \) of \( N \), we can make use of additional structure provided by this model. To do so, we introduce a further inference rule that often drastically decreases the number of possibly non-implied query instances to be considered and allows more derivations to terminate. This rule is not sound for \( \equiv_{\mathcal{F}} \) but always glued to the currently considered model \( M \). While the results in this section hold for all (sets of) Herbrand models of \( N \), they are most likely to be used for the minimal model \( I_N \) of a saturated clause set and hence presented in the context of \( \equiv_{\text{ind}} \) only.

Over any domain where the induction theorem holds, i.e. a domain on which a well-founded ordering can be defined, we can exploit this structure to concentrate on finding minimal solutions. We do this by adding a form of induction hypothesis to the clause set. If e.g. \( P \) is a unary predicate over the natural numbers and \( n \) is the minimal number such that \( P(n) \) holds, then we know that at
the same time \(P(n - 1), P(n - 2), \ldots \) do not hold. This idea will now be cast into an inference rule that can be used during a theorem proving derivation.

Let \( \leq \leq^* \) be a well-founded partial ordering on the elements of \( \mathcal{X}_N \). If \( s, t \) are non-ground terms with equivalence classes \([s]\) and \([t]\), then we define \([s] \leq [t]\) iff \([\sigma \rho] \leq [\tau \rho]\) for all grounding substitutions \(\sigma : X \to \mathcal{T}(\mathcal{F})\). The definition lifts pointwise to substitutions \([\rho] : X' \to \mathcal{T}(\mathcal{F})/\mathcal{X}_N\), where we say that \([\rho] \leq \sigma\) iff \([\rho \sigma] \leq [\tau \rho]\) for all \(x \in X'\).

**Lemma 3.** Let \(\alpha = \varphi_1 \wedge \ldots \wedge \varphi_k\) be a constraint containing only variables, \(X_\alpha = \{x_1, \ldots, x_k\}\), and let \(H = \{\varphi_1 \supset C_1, \ldots, \varphi_k \supset C_n\}\) be a set of clauses where only variables of \(\mathcal{V} \cup X_\alpha\) occur. Furthermore, let \(\sigma, \tau : X_\alpha \to \mathcal{T}(\mathcal{F}, X)\) be substitutions with \([\rho] \leq [\sigma]\). If \(N \models_{\text{ind}} H\), then also \(N \models_{\text{ind}} \alpha \sigma \tau \to (\neg C_1 \rho \lor \ldots \lor \neg C_n \rho)\).

**Proof.** Let \([\sigma_0] : V \to \mathcal{T}(\mathcal{F})/\mathcal{X}_N\) be a minimal substitution with respect to \(\leq\) such that \(N \models_{\text{ind}} \{\varphi_1 \supset C_1(\sigma_0), \ldots, \varphi_k \supset C_n(\sigma_0)\}\). Furthermore, let \(X_\alpha\) be the set of non-constant variables in \(\alpha\) and \(\tau : X_\alpha \to \mathcal{T}(\mathcal{F})/\mathcal{X}_N\) such that \(N \models_{\text{ind}} \alpha \sigma_0 \tau\). We have to show that \(N \models_{\text{ind}} \neg C_1 \rho \lor \ldots \lor \neg C_n \rho\).

The restriction of a substitution to the set \(V\) of existential variables is denoted by \(\cdot \rceil V\). In the next line below, we use that \(\alpha\) is a conjunction of equations \(v \approx v \sigma_\alpha\) and that \(\tau\) and \(\sigma_\alpha \rho \tau\) affect different sides of each such equation.

\[
\begin{align*}
[\rho] \leq [\sigma] & \iff [\sigma_\alpha \rho \tau] \leq [\sigma_\alpha] \\
& \iff [\sigma_\alpha \rho \tau] \leq [\sigma_\alpha] \\
& \iff \exists \tau'. N \models_{\text{ind}} \alpha(\sigma_\alpha \rho \tau) \rceil V = \tau' \quad \text{and} \quad N \models_{\text{ind}} C_1 \tau' \land \ldots \land C_n \tau' \\
& \iff \exists \tau'. \forall \tau' \in V. N \models_{\text{ind}} \nu \sigma_\alpha \rho \tau \approx \nu \sigma_\alpha \tau' \quad \text{and} \quad N \models_{\text{ind}} C_1 \tau' \land \ldots \land C_n \tau' \\
& \iff \exists \tau'. \forall x \in X_\alpha. N \models_{\text{ind}} x \rho \approx x \tau' \quad \text{and} \quad N \models_{\text{ind}} C_1 \tau' \land \ldots \land C_n \tau' \\
& \iff \nu \sigma_\alpha \rho \tau \approx \nu \sigma_\alpha \tau' \quad \text{for} \quad \tau' : X \setminus V \to \mathcal{T}(\mathcal{F}).
\end{align*}
\]

Since the preserved solution \([\sigma_0]\) is independent of the choices of \(\sigma\) and \(\rho\), any clauses derived by this lemma will have a common solution with \(\alpha \supset C\).

**Example 3.** Let \(\mathcal{F} = \{0, s\}, N = \{P(s(s(x)))\}\) and \(H = \{u \approx x \supset P(x)\}\). The formulas derivable by the lemma are of the form \(u \approx s^n(0) \to P(s^{n+m}(0))\), \(u \approx s^n(0) \to \neg P(s^{n+m}(0))\) or \(u \approx s^n(z) \to \neg P(s^{n+m}(z))\) for natural numbers \(n, m\) with \(m > 0\). All these formulas and the initial clause \(u \approx x \supset P(x)\) have the common solution \(\{u \to s(s(0))\}\) in \(I_N\).

The formula \(\alpha \sigma \tau \to (\neg C_1 \rho \lor \ldots \lor \neg C_n \rho)\) can usually not be written as a single equivalent constrained clause if some \(C_i\) contains more than one literal.
However, if $D_1 \land \ldots \land D_m$ is a conjunctive normal form of $-C_1 \lor \ldots \lor -C_n$, then each $D_j$ is a disjunction of literals and so $\sigma \cdot \| D_j \rho$ is a constrained clause.

We can thus, to decide the validity of $\{ \sigma \cdot \| C_1, \ldots, C_n \}$ in $T_N$, use information taken from the lemma in the theorem proving derivation:

**Theorem 4.** Let $N$ be a saturated set of clauses, let $\alpha = v_1 \approx x_1, \ldots, v_k \approx x_k$ be a constraint containing only variables, $X_\alpha = \{ x_1, \ldots, x_k \}$, and let $H = \{ \alpha \cdot \| C_1, \ldots, \alpha \cdot \| C_n \}$ be a set of clauses where only variables of $V \cup X_\alpha$ occur. Moreover, let $D_1 \land \ldots \land D_m$ be a conjunctive normal form of $-C_1 \lor \ldots \lor -C_n$. Consider the inference rule

$$\frac{\sigma \cdot \| D_j \rho}{\sigma, \rho : X_\alpha \rightarrow T(\mathcal{F}, X)}$$

which is specialized for the one fixed clause set $H$, and the theorem proving system combining this rule and $\mathcal{F}$. If $H'$ is derived from $H$ using this combined inference system, then $N \models_{\text{ind}} H' \iff N \not\models_{\text{ind}} H$.

**Proof.** This follows directly from proposition 3 and lemma 3.

**Example 4.** Consider the following theory of the addition on the naturals: $N = \{ \rightarrow 0 + y \approx y, \rightarrow s(x) + y \approx s(x + y) \}$. The proof of $N \models_{\text{ind}} \forall x. x + 0 \approx x$ with the induction inference rule terminates quickly:

- clauses in $N$:
  - 1: $\|$ $\rightarrow 0 + y \approx y$
  - 2: $\|$ $\rightarrow s(x) + y \approx s(x + y)$
- negated conjecture: 3: $u \approx x$
- superposition(1,3) = 4: $u \approx 0$
- equality res.(4) = 5: $u \approx 0$
- superposition(2,3) = 6: $u \approx s(y)$
- induction rule(3) = 7: $u \approx s(z)$
- superposition(7,6) = 8: $u \approx s(z)$
- equality res.(8) = 9: $u \approx s(z)$

At this point, the clauses $u \approx 0 \| \Box$ and $u \approx s(z) \| \Box$ have been derived. Their constraints cover all of $T(\mathcal{F})$, which means that $N \not\models_{\text{ind}} u \approx x \| x + 0 \approx x \rightarrow$, i.e. $N \models_{\text{ind}} \forall x. x + 0 \approx x$.

**Example 5.** Given the theory $N = \{ \rightarrow E(0), E(x) \rightarrow E(s(s(x))) \}$ of the natural numbers together with a predicate describing the even numbers, we check whether $N \models_{\text{ind}} \forall x. E(x)$. A possible derivation runs as follows:

- clauses in $N$:
  - 1: $\| \rightarrow E(0)$
  - 2: $\| E(x) \rightarrow E(s(s(x)))$
- negated conjecture: 3: $u \approx x$
- superposition(1,3) = 4: $u \approx 0$
- superposition(2,3) = 5: $u \approx s(y)$
- induction rule(3) = 6: $u \approx s(s(z))$
- superposition(6,5) = 7: $u \approx s(s(z))$

This set is saturated. The derived contradictions are $u \approx 0 \| \Box$ and $u \approx s(s(z)) \| \Box$. Their constraints are not covering, and in fact $N \models_{\text{ind}} E(s(0) \rightarrow$. 

5 Conclusion

We have presented a sound and complete superposition calculus for a fixed domain semantics. Compared to other approaches in model building over fixed domains, our approach is applicable to a larger class of clause sets. While most works in the tradition of Caferra and Zabel [4] consider only very restricted forms of equality literals and even more recent publications by Peltier [14] pose strong restrictions on the clause sets (e.g. that they have a unique Herbrand model), we do not have such restrictions.

Moreover, we presented a way to prove the validity of minimal model properties by using a specific induction rule. We even showed that standard first-order and fixed domain superposition based reasoning, respectively, delivers minimal model results for some cases. The most general methods based on saturation so far are those by Ganzinger and Stuber [8] and Comon and Nieuwenhuis [6]. Both approaches work only on sets of purely universal and universally reductive (Horn) clauses. We gave an example of a purely universal problem that our algorithm can solve while neither of the above approaches works. Additionally, we showed how we can also prove the validity of $\forall^+$-quantified formulas.

Another intensely studied approach is via test sets [11,3]. Test sets rely on the existence of a set of constructor symbols that are either free or specified by unconditional equations only. Again, such properties are not needed for the applicability of our calculus. Example 1 is not solvable via test sets, whereas Example 2 is.

In analogy to the work of Bachmair and Ganzinger [1], it is also possible to extend the new superposition calculus by negative literal selection, with the restriction that no constraint literals may be selected, still hold in this setting. Theorem 1 still holds in this setting. For universally reductive clause sets $N$, is also possible to make the inductive theorem proving algorithm (with selection) refutationally complete, following the approach of Ganzinger and Stuber [8].

In summary, our approach does not need many of the prerequisites required by previous approaches, like solely universally reductive clauses in $N$, solely Horn clauses, solely purely universal clauses, solely non-equational clauses, the existence of an “$A$” set fixing the standard first-order interpretation to the minimal model, or the existence of explicit constructor symbols. Its success is build on a superposition based saturation concept.

Our hope is that the success of the superposition based saturation approach on identifying decidable classes with respect to the classical first-order semantics can be extended to some new classes for the fixed domain or minimal model semantics. In case we can finitely saturate a clause set, the ordering $<$ on $Zv$ elements may become effective and hence the induction rule of theorem 4 can then be effectively used to finitely saturate clause sets that otherwise have an infinite saturation. Decidability results for the fixed domain semantics are hard to obtain for infinite Herbrand domains but the problem can now be attacked using the sound and complete calculus presented in this paper. They will require in addition the extension of the redundancy notion suggested in section 3 possibly.
using more expressive languages of existential constraints. Here, concepts and results from tree automata could play a role.

Acknowledgements: We thank our reviewers for their detailed and valuable comments. Matthias Horbach and Christoph Weidenbach are supported by the German Transregional Collaborative Research Center SFB/TR 14 AVACS.

References