Order-Sorted Congruence Closure

Jean H. Gallier  
*University of Pennsylvania, jeanmarc@cis.upenn.edu*

Tomas Isakowitz  
*University of Pennsylvania*

Follow this and additional works at: https://repository.upenn.edu/cis_reports

**Recommended Citation**


This paper is posted at ScholarlyCommons. https://repository.upenn.edu/cis_reports/686
For more information, please contact repository@pobox.upenn.edu.
Order-Sorted Congruence Closure

Abstract
In this paper, an algorithm for testing the unsatisfiability of a set of ground order-sorted equational Horn clauses (for coherent signatures) is presented. This result follows from the fact that the concept of congruence closure extends to finite sets of ground order-sorted equational Horn clauses. We show how to compute the order-sorted congruence closure and obtain an algorithm running in $O(\eta^2)$.

Comments

This technical report is available at ScholarlyCommons: https://repository.upenn.edu/cis_reports/686
ORDER-SORTED
CONGRUENCE CLOSURE
Tomas Isakowitz
Jean H. Gallier
MS-CIS-88-07
LINC LAB 96

Department of Computer and Information Science
School of Engineering and Applied Science
University of Pennsylvania
Philadelphia, PA 19104
January 1988

Acknowledgements: This research was supported in part by DARPA grant NOOO14-85-K-0018, NSF grants DCR-86-07156 and DCS-8219196-CER and U.S. Army grants DAA29-84-K-0061, DAA29-84-9-0027.
In this paper, an algorithm for testing the unsatisfiability of a set of ground order-sorted equational Horn clauses (for coherent signatures) is presented. This result follows from the fact that the concept of congruence closure extends to finite sets of ground order-sorted equational Horn clauses. We show how to compute the order-sorted congruence closure and obtain an algorithm running in $O(n^2)$. 
Contents

1 Introduction

2 Order-Sorted Algebras
   2.1 Signatures
   2.2 Algebras
   2.3 Order-sorted term algebra
   2.4 Equations
   2.5 Order-sorted Logic
   2.6 Transforming Horn clauses into equational form
   2.7 Order-sorted relations
   2.8 Order-sorted congruences
   2.9 The top algebra
   2.10 Least Order-sorted congruences

3 Congruences Associated With Order-sorted Horn Clauses
   3.1 The Graph $GT(H)$
   3.2 Order-sorted Graph Congruence Closure
   3.3 A Method For Testing Unsatisfiability
   3.4 Finite models

4 Existence of the Order-sorted Graph Congruence Closure
   4.1 Equational Order-sorted Graph Congruence Closure
   4.2 Implicational Closure
   4.3 Order-sorted Congruence Closure For Horn Clauses
   4.4 A more efficient Order-sorted Graph Congruence closure

5 Conclusion
1 Introduction

Order-sorted algebras were first introduced by Goguen and Meseguer [6], in order to deal with the notion of subtype and the notion of error in abstract data types. They constitute an interesting extension of many-sorted algebras, and their properties have been investigated recently by Goguen and Meseguer [5], Nutt, Smolka, Goguen, and Meseguer [14], and by Ait-Kaci and Smolka [15], where they are used to provide a semantics for inheritance.

In spite of this recent interest, some basic logical properties of these algebras have been neglected, in particular, the notion of congruence closure [8,9,13]. In this paper, it is shown that the notion of congruence closure extends to finite sets of ground order-sorted equations. Actually, extending a result of Gallier [2], it is shown that congruence closure extends to finite sets of ground order-sorted equational Horn clauses. More specifically, we prove that congruence closure is sound and complete for showing the unsatisfiability of sets of ground order-sorted equational Horn clauses (for coherent signatures). As a consequence, adapting results from Gallier [2], an unsatisfiability algorithm running in $O(n^2)$ is obtained.

Due to the nature of subtypes in order-sorted algebras, the proof that the method is complete is surprisingly nontrivial. This is because the approach used in the many-sorted case does not work. An approach using rewriting (as in Kozen [9]) fails, due to the well known problem that rewriting with order-sorted rewrite rules may create ill-typed terms. Also, the construction of a finite counter example as in Gallier [2] does not quite work, because it does not seem possible to define directly a finite algebra and respect the type structure at the same time. Our solution is to define a counter example by taking the quotient of the initial order-sorted algebra by the least congruence $\simeq$ containing the graph congruence closure $\rightarrow^*_E$ of the set of clauses. But then, we run into the problem that it is not obvious that congruence modulo $\simeq$ is conservative over congruence modulo $\rightarrow^*_E$ for terms occurring in the clauses. However, we are able to prove this result by characterizing congruence modulo $\simeq$ in a way that imitates congruence closure. Thus, we are able to prove the completeness (and soundness) of this congruence closure method (for ground Horn clauses).

2 Order-Sorted Algebras

2.1 Signatures

Our definition of an order-sorted algebra is equivalent to that given by Goguen and Meseguer [6] and by Kirchner and Kirchner [7], but we believe that it is slightly easier to grasp.

Given an index set $S$, an $S$-sorted set $A$ is just a family $(A_s)_{s \in S}$ of sets, one set $A_s$ for each $s \in S$. Similarly, given two $S$-sorted sets $A$ and $B$, an $S$-sorted function $f : A \rightarrow B$ is an $S$-indexed family $(f_s : A_s \rightarrow B_s)_{s \in S}$ of functions $f_s : A_s \rightarrow B_s$, and an $S$-sorted relation $R$ is an $S$-indexed family $(R_s)_{s \in S}$ of relations $R_s \subseteq A_s \times B_s$. Let us assume a fixed set $S$ called the sort set, with a partial order $\leq$. 

Definition 2.1 A many-sorted signature is defined as a triple $(S, \Sigma, \rho)$, where $S$ is a sort set and $\rho: \Sigma \rightarrow 2^{\mathbb{S} \times \mathbb{S}}$ is a rank function assigning a set $\rho(f)$ of ranks $(w, s)$ to each symbol in $\Sigma$. The elements of the sets $\Sigma$ are called operators or function symbols. The set $\Sigma$ can be viewed as an indexed family if for every $(w, s) \in S^* \times S$ we let $\Sigma_{w,s} = \{ f \in \Sigma \mid (w, s) \in \rho(f) \}$.

Note that $\Sigma_{w,s}$ and $\Sigma_{w',s'}$ are not necessarily disjoint, since a symbol in $\Sigma$ may have several ranks. Whenever convenient, we omit the function $\rho$, and view $\Sigma$ as family of sets $(\Sigma_{w,s})_{(w,s) \in S \times S^*}$.

Definition 2.2 An order-sorted signature is a quadruple $(S, \leq, \Sigma, \rho)$, such that $(S, \Sigma, \rho)$ is a many-sorted signature and $(S, \leq)$ is a partially ordered set.

Example 2.1 Let the set of sorts be $S = \{ \text{zero}, \text{rat}^+, \text{rat} \}$, and let the partial order be: $\text{zero} \leq \text{rat}, \text{rat}^+ \leq \text{rat}$
The following is an order-sorted $\Sigma$-signature:  
$\Sigma_{\text{rat}.\text{rat}.\text{rat}} = \{+\}$ 
$\Sigma_{\text{rat}.\text{rat}^+.\text{rat}} = \{/\}$

Notice that the second argument of / is of sort $\text{rat}^+$, which is intended to exclude zero. Hence we trying to formalize the idea of disallowing a division by zero.

In order that the standard construction of an initial algebra as a term algebra holds, we restrict ourselves to a special class of signatures called regular. Essentially, regularity asserts that overloaded operations are consistent under restrictions to subsorts. Note that the ordering $\leq$ on $S$ extends to an ordering on strings of equal length in $S^*$ as follows: $s_1 \ldots s_n \leq s'_1 \ldots s'_n$ iff $s_i \leq s'_i$ for $1 \leq i \leq n$. Similarly, $\leq$ extends to pairs in $S^* \times S$ by stating that $(w, s) \leq (w', s')$ iff $w \leq w'$ and $s \leq s'$.

Definition 2.3 An order-sorted signature $S$ is regular iff for every $f \in \Sigma$, every $w^0 \in S^*$, and every $(w, s) \in \rho(f)$, if $w^0 \leq w$, then the set $\{(w', s') \in \rho(f) \mid w^0 \leq w'\}$ has a least element.

When the set of sorts is finite (or well founded), regularity is captured by a combinatorial condition (see the paper by Kirchner and Kirchner [7]).
2.2 Algebras

Lemma 2.1 An order-sorted signature $\Sigma$ over a finite (or well founded) sort set $S$ is regular iff for every every $f \in \Sigma$, every $w^0 \in S^*$, and every pair of ranks $(w, s), (w', s') \in \rho(f)$, if $w^0 \leq w, w'$, then the set $\{(w, s), (w', s')\}$ has a lower bound $(w_l, s_l)$ such that $(w_l, s_l) \in \rho(f)$, and $w^0 \leq w_l$.

Let $\equiv = (\leq \cup \leq^{-1})^+$ be the equivalence relation induced by the partial order $\leq$. We will say that to sorts $s$ and $s'$ are connected if $s \equiv s'$.

Notice that being connected is an equivalence relation that splits the set of sorts into connected components. The concept of connected sorts is important for defining quotient algebras. Indeed, in order for the usual construction of the quotient of an algebra by a congruence to hold, we need a condition on signatures called coherence.

Definition 2.4 A regular order-sorted signature is coherent if every connected component has a greatest element called the top sort of the connected component.

2.2 Algebras

For any string $w = s_1, \ldots, s_n$ $(n \geq 1)$, let $A_w = A_{s_1} \times \ldots \times A_{s_n}$, with $A_{s} = \{s\}$ (a one element set).

Definition 2.5 Let $(S, \leq, \Sigma, \rho)$ be an order-sorted signature. An order sorted $(S, \leq, \Sigma, \rho)$-algebra $A$ is a pair $(A, I)$ consisting of an $S$-sorted family $A = (A_s)_{s \in S}$ called the carrier of $A$, and a function $I$ called the interpretation function of $A$, where $I$ assigns to every $f \in \Sigma$ an indexed family of functions $I(f) = (I^w_s : A_w \to A_s)_{(w, s) \in \rho(f)}$. In particular, when $w = \lambda$, $I^w_s$ is an element of $A_s$. For each sort $s$, $A_s$ is the carrier of sort $s$. Note that the carrier of sort $s$ may be empty. We also denote $I^w_s$ as $f^w_{A,s}$. Moreover, the following conditions hold:

1. $A_s \subseteq A_{s'}$ whenever $s \leq s'$, and

2. If $(w, s) \in \rho(f)$ and $(w', s') \in \rho(f)$, $s \leq s'$, and $w \leq w'$, then $f^w_{A,s} : A_w \to A_s$ is equal to the restriction of $f^{w'}_{A,s'} : A_{w'} \to A_{s'}$ to $A_w$. That is, for any $\overline{x} \in A_w, f^w_{A,s}(\overline{x}) = f^{w'}_{A,s'}(\overline{x})$.

By abuse of notation, we may denote an algebra and its carrier by the same name unless confusions arise. For example in the the previous definition we might use $A$ for both the carrier (which is $A$) and for the algebra (which is $A$). We may also drop some of the components in $(S, \leq, \Sigma, \rho)$ when talking about order-sorted algebras, or drop the superscript $(w, s)$ when referring to a function $f^w_{A,s}$.

Example 2.2 Consider the signature presented in example 2.1, an order-sorted $\Sigma$-algebra $A$ is:

- $A_{\text{rat}} = Q$ (the set of rational numbers),
2 ORDER-SORTED ALGEBRAS

- \( A_{\text{rat}}^+ = \mathbb{Q} - \{0\} \) (the set of non-zero rationals), and
- \( A_{\text{zero}} = \{0\}\).

The functions have their natural interpretations:

- \(+_A\) is addition of rational numbers,
- \(/_A\) is division of rational numbers.

For any \( w = s_1 \ldots s_n \neq \lambda \) and \( \bar{a} = (a_1, \ldots, a_n) \in A_w \), let \( h_w(\bar{a}) = (h_{s_1}(a_1), \ldots, h_{s_n}(a_n)) \).

**Definition 2.6** Let \((S, \leq, \Sigma, \rho)\) be an order-sorted signature, and let \( A \) and \( B \) be \((S, \leq, \Sigma, \rho)\)-order-sorted algebras. A \((S, \leq, \Sigma, \rho)\)-homomorphism \( h : A \rightarrow B \) is an \( S \)-sorted function such that

1. for every constant \( c \) of sort \( s \), \( h_s(c_A) = c_B \),
2. for every \( f \in \Sigma \), every \((w, s) \in \rho(f)\), and every \( \bar{a} \in A_w \),
   \[ h_s(f^w_s(\bar{a})) = f^w_s(h_\Sigma(\bar{a})) \]
3. \( w \leq w' \) and \( \bar{a} \in A_w \) implies \( h_w(\bar{a}) = h_{w'}(\bar{a}) \).

When the partially ordered set is clear, \((S, \leq, \Sigma, \rho)\)-homomorphisms are called order-sorted \( \Sigma \)-homomorphisms. We may also drop some of the components in \((S, \leq, \Sigma, \rho)\) when talking about order-sorted homomorphisms.

### 2.3 Order-sorted term algebra

Following [6], we now define the order-sorted \( \Sigma \)-term algebra \( T_\Sigma \) as the least family \( \{T_{w,s} \mid s \in S\} \) of sets satisfying the following conditions:

1. \( \Sigma_{\lambda,s} \subseteq T_{\Sigma,s} \) for \( s \in S \);
2. \( T_{\Sigma,s} \subseteq T_{\Sigma,s'} \) whenever \( s \leq s' \);
3. if \( f \in \Sigma_{w,s} \), and if \( t_i \in T_{\Sigma,s_i} \), where \( w = s_1, \ldots, s_i \neq \lambda \), then the string \( f t_1 \ldots t_n \) is in \( T_{\Sigma,s} \)

In addition, the function symbols are interpreted as string constructors as follows: for \( f \in \Sigma_{w,s} \), \( f^w_s(t_1, \ldots, t_n) = ft_1 \ldots t_n \).

**Definition 2.7** Let \( \Sigma \) be an order-sorted signature. An order-sorted algebra \( A \) is initial in the class of all \( \Sigma \)-algebras if there is a unique order-sorted \( \Sigma \)-homomorphism from \( A \) to any other \( \Sigma \)-algebra.

We state the following theorems, whose proofs can be found in [6].
2.4 Equations

Theorem 2.2 Let $\Sigma$ be a regular order-sorted signature. Then $T_\Sigma$ is an initial order-sorted $\Sigma$-algebra. This means that for every order-sorted $\Sigma$-algebra $A$, there is a unique order-sorted homomorphism $h_A : T_\Sigma \rightarrow A$.

Theorem 2.3 Let $\Sigma$ be a regular order-sorted signature. Then every term $t$ in $T_\Sigma$ has a least sort denoted by $LS(t)$.

2.4 Equations

An equation can be stated between two terms if they belong to the same top sort. Viewed as terms in $T_\Sigma$ we can say that two terms can be equated if their least sorts are in the same connected component, because then they both belong to the same top sort $t$ and the equality symbol is to be seen as that of sort $t.t$.

Definition 2.8 Given a coherent order-sorted signature $\Sigma$, an equation or equational atom is a pair $(u, v)$ of terms in $T_\Sigma$ such that the least sorts $LS(u)$ and $LS(v)$ of $u$ and $v$ are connected. An equation is also denoted as $u \doteq v$.

The concept of validity of an equation is defined using the initiality property of $T_\Sigma$.

Definition 2.9 Given a coherent order-sorted signature $\Sigma$, we say that an equation $u \doteq v$ is valid in some order-sorted $\Sigma$-algebra $A$ (denoted $A \models u \doteq v$) if and only if

$$h_{A,LS(u)}(u) = h_{A,LS(v)}(v),$$

where $h_A : T_\Sigma \rightarrow A$ is the unique order-sorted homomorphism given by initiality. We say that $u \doteq v$ is universally valid, or valid, and (denoted $\models u \doteq v$) iff $u \doteq v$ is valid in every order-sorted $\Sigma$-algebra $A$.

2.5 Order-sorted Logic

A logic language consists of terms and predicates. We extend the notion of an order-sorted signature to include predicates.

Definition 2.10 Given a coherent order-sorted signature $(S, \leq, \Sigma, \rho_\Sigma)$, an order-sorted signature with predicates is a quintuple $(S, \leq, \Sigma, \Pi, \rho)$, where $\Pi$ is a family of predicate symbols. The function $\rho$ assigns ranks to the elements of $\Sigma$ and $\Pi$ so that

1. for $f \in \Sigma, \rho(f) = \rho_\Sigma(f)$, and
2. for $P \in \Pi, \rho(P) \in 2^{S*}$, i.e. $P$ might have more than one rank (even different number of arguments).
We also demand that the following regularity condition be satisfied:

For each \( P \in \Pi, \) every \( w^0 \in S^* \), and every \( w \in \rho(P) \), if \( w^0 \leq w \), then the set 
\[ \{ w' \in \rho(P) \mid w^0 \leq w' \} \]
has a least element.

Notice that an order-sorted signature with predicates is by definition coherent. As in the case of order-sorted signature, we can regard \( I^3 \) as an \( S^* \)-indexed family \( \{I^i\}_{s \in S^*} \). When the sort set \( S \), the partial order \( \leq \) and the rank function \( p \) are clear, we write \( (S, \leq, \Sigma, \Pi, \rho) \) for \( (S, \leq, \Sigma, \Pi, \rho) \). A predicate with empty rank, i.e. \( x \in \rho(P) \), is a propositional letter.

**Definition 2.11** Let \( (S, \leq, \Sigma, \Pi, \rho) \) be an order-sorted signature with predicates. Then an \( (S, \leq, \Sigma, \Pi, \rho) \)-structure is a \( (S, \leq, \Sigma, \Pi, \rho) \)-algebra \( M \) together with an interpretation 
\[ P_{s_1 \ldots s_n}^M : M_{s_1 \ldots s_n} \mapsto BOOL, \]
and

1. \( P_{s_1 \ldots s_n}^M : M_{s_1 \ldots s_n} \mapsto BOOL, \)

2. whenever \( w_1, w_2 \in \rho(P) \) with \( w_1 \leq w_2 \) and \( x \in M_{w_1} \), \( P_{s_1 \ldots s_n}^{w_1}(x) = P_{s_1 \ldots s_n}^{w_2}(x) \).

The second condition states that the interpretation is consistent under subsorts. Notice that for a propositional letter \( A \), \( A_M \) is a constant, either \text{true} or \text{false}.

Atoms are expressions of the form \( P t_1 \ldots t_n \) such that \( P \) is a predicate symbol and \( t_1, \ldots, t_n \) are \( \Sigma \)-terms of sort \( s_1, \ldots, s_n \) for \( s_1 \ldots s_n \in \rho(P) \). The notion of satisfaction is as in the many-sorted case:

**Definition 2.12** Let \( \Sigma, \Pi \) be an order-sorted signature with predicates and let \( M \) be a \( \Sigma, \Pi \)-structure. Given a \( \Sigma, \Pi \)-atom \( P t_1 \ldots t_n \) with \( t_i \) of sort \( w_i \) and \( w = w_1 \ldots w_n \in \rho(P) \), we say that \( M \) satisfies \( P t_1 \ldots t_n \) (written \( M \models P t_1 \ldots t_n \)) if \( P_{s_1 \ldots s_n}^{w_1}(t_1, \ldots, t_n) = \text{true} \).

We now introduce additional notation for Horn clauses. Let \( \Sigma, \Pi \) be an order-sorted signature with predicates and equality.

**Definition 2.13** A \( \Sigma, \Pi \)-Horn clause is an expression of the form 
\[ A : B_1, \ldots, B_n \]
where each of \( A, B_1, \ldots, B_n \) is either an atom or an equational atom. \( A \) is called the head and \( B_1, \ldots, B_n \) the body. When the body is empty, the Horn clause is called a unit clause and written \( A \) instead of \( A : - \). If the head of a clause is empty, it is a negative clause.

The notion of satisfaction of ground Horn clauses is the usual one:
2.6 Transforming Horn clauses into equational form

Definition 2.14 Given a ground $\Sigma, \Pi$-Horn clause $A : -B_1, \ldots, B_n$, $M$ satisfies it if $M \models B_i$ for $i = 1, \ldots, n$ implies $M \models A$.

For $H$ a set of ground Horn clauses, we say that $M$ is a model of $H$, and we write $M \models H$ if $M$ satisfies every Horn clause in $H$.

Notice that $M$ satisfies a negative clause $-B_1, \ldots, B_n$ if and only if $M \not\models B_i$ for $i = 1 \ldots n$.

The syntax and semantics for the logical connectives $\neg, \lor, \land, \equiv$ and $\equiv$ are as in the unsorted case. Since there are no variables in our discussion, all terms are ground. That is the reason no assignment is needed in defining satisfaction.

2.6 Transforming Horn clauses into equational form

For the purpose of our discussion later on, it is useful to regard arbitrary Horn clauses as equational ones. This is done by replacing each occurrence of a non-equational atom $P_{t_1} \ldots t_n$ by the equation $P_{t_1} \ldots t_n \equiv \top$. If we add to our language a special sort bool, a constant $\top$ interpreted as true, and for every structure, the domain BOOL of sort bool is the set of truth values $\{\text{true}, \text{false}\}$, every atomic formula $P_{t_1} \ldots t_k$ is logically equivalent to $P_{t_1} \ldots t_k \equiv \top$, in the sense that $P_{t_1} \ldots t_k \equiv (P_{t_1} \ldots t_k \equiv \top)$ is valid. But then, this means that $\equiv$ behaves semantically exactly as the identity relation on BOOL. Hence, we can treat $\equiv$ as the equality symbol $=$ of sort bool.

For every predicate letter $P$ of rank $\rho(P) = \{s_1^{n_1}, \ldots, s_k^{n_k}\}$ a new function symbol $P$ of sort $\{(s_1^{n_1}, \text{bool}), \ldots, (s_k^{n_k}, \text{bool})\}$ is introduced. Hence, every set $H$ of order-sorted Horn clauses is equivalent to a set $H'$ of order-sorted Horn clauses, in which every atomic formula $P_{t_1} \ldots t_k$ is replaced by the equation $P_{t_1} \ldots t_k \equiv \top$. Formally we proceed as follows.

Definition 2.15 An order-sorted signature with boolean symbols is an order-sorted signature where the set of sorts $S$ contains the special sort bool, which can only be the target type (or co-arity) of a function symbol. In addition we require the constants $\top$ and $\bot$ of rank bool to be in the signature. (There might also exist other function symbols of co-arity bool).

The semantics of these signatures is given by order-sorted algebras that interpret the objects related to bool in a specific way.

Definition 2.16 An order-sorted-$\Sigma$-bool algebra is an order-sorted-$\Sigma$ algebra $A$ such that:

- $A_{\text{bool}} = \{\text{true}, \text{false}\}$,
- $\top_A = \text{true}$, and
- $\bot_A = \text{false}$.
One can define equations, equational Horn clauses and the notion of satisfaction as in the case of normal order-sorted signature, except that the models now have a fixed interpretation for the sort \( \text{bool} \) and its related function symbols.

Given an order-sorted signature with predicates \((S, \leq, \Sigma, \Pi, \rho)\), we transform it into an order-sorted signature with boolean symbols (but without predicates) \((S, \leq, \Sigma \cup \Pi, \rho^*)\) by letting \(\rho^*\) be:

- for \( f \in \Sigma, \rho^*(f) = \rho(f), \) and
- for \( P \in \Pi, \rho^*(P) = (\rho(P), \text{bool}).\)

Let \( H \) be a set of Horn clauses over \( T_{(S, \leq, \Sigma, \Pi, \rho)} \), we transform it into a set \( H' \) of equational Horn clauses over \( T_{(S, \leq, \Sigma \cup \Pi, \rho^*)} \) by replacing every occurrence of an atomic formula \( Pt_1 \ldots t_n \) in \( H \) by the equation \( Pt_1 \ldots t_n \models \top \) in \( H' \). Then the following lemma holds:

**Lemma 2.4** \( H \) is satisfiable if and only if \( H' \) is satisfiable.

### 2.7 Order-sorted relations

**Definition 2.17** We say that an \( S \)-sorted relation \( R \) on an order-sorted algebra is order-sorted iff given elements \( u \) and \( v \) of sort \( s \), and given a sort \( t \) such that \( s \leq t \),

\[
\text{u}_R_s \text{v} \quad \text{iff} \quad \text{u}_R_t \text{v}.
\]

Informally this means that the relation is independent of the specific sort within a connected component.

Not every relation is order-sorted but it can be made into one by simply adding the missing pairs.

**Definition 2.18** Given a relation \( R \), the order-sorted completion of \( R \) is the family \( \{R'_s\}_{s \in S} \):

\[
R'_s = \{(u, v) \in A_s \times A_s \mid (u, v) \in R_t \text{ for some } t \text{ such that } t \geq s \text{ or } s \geq t \}
\]

We can ask ourselves the following question. Given an order-sorted algebra and an order-sorted relation \( R \), can it occur that \( uR_s v \) for some sort \( s \) but \( \neg uR_{s'} v \) for a different sort \( s' \)? It turns out that for initial algebras of a coherent signature this is impossible.

**Lemma 2.5** Let \( \Sigma \) be a coherent signature. Consider the term algebra \( T_\Sigma \). A relation \( \sim \) on \( T_\Sigma \) is order-sorted if and only if for every pair of terms \( u \) and \( v \) and every pair of sort \( \tau, \sigma \) such that both \( u \) and \( v \) are of sort \( \tau \) and \( \sigma \),

\[
u \sim_\tau v \quad \text{iff} \quad u \sim_\sigma v
\]

**Proof:** Since \( \Sigma \) is regular and \( u \) is of sort \( \sigma \) and \( \tau, \sigma \) and \( \tau \) are connected via the least sort of \( u \). Since \( \Sigma \) is coherent, there is a top element \( \delta \) in the connected component of \( \tau \) and \( \sigma \), i.e. \( \tau \leq \delta \) and \( \sigma \leq \delta \). If \( \sim \) is order-sorted, \( u \sim_\tau v \) iff \( u \sim_\delta v \) iff \( u \sim_\sigma v \).

The converse direction is trivial. \( \square \)
2.8 Order-sorted congruences

Since every initial algebra is isomorphic to a term algebra, we have as a corollary that any initial algebra satisfies the above property. Thus when dealing with order-sorted relations over an initial algebra of a coherent signature, we can drop the subscripts from the relation symbol without causing any confusion. That is, $uR_su$ can be written as $uRv$, since we are guaranteed that whenever this last expression makes sense, it holds.

2.8 Order-sorted congruences

Congruences are equivalence relations which are preserved under function application. They are useful because just as one can define a quotient of a set by an equivalence relation, it is possible to define the quotient of an algebra by a congruence.

**Definition 2.19** For $(S, \Sigma)$ a many-sorted signature and $A$ a $\Sigma$-algebra, a relation $\sim$ is a many-sorted congruence if the following conditions are satisfied:

1. $\sim$ is an equivalence relation
2. For every $f \in \Sigma_{s_1, \ldots, s_n}$, if $u_i \sim_{s_i} v_i$ for every $i$, $1 \leq i \leq n$, then $f_A(u_1, \ldots, u_n) \sim_{s} f_A(v_1, \ldots, v_n)$.

**Definition 2.20** For $(S, \leq, \Sigma)$ an order-sorted signature and $A$ an order-sorted $\Sigma$-algebra, a many-sorted congruence $\sim$ is an order-sorted congruence if it is an order-sorted relation. That is, if it satisfies:

for every $s, s' \in S$ and $a, b \in A$, if $s \leq s'$ then $a \sim_{s} b$ iff $a \sim_{s'} b$.

We proceed to define the quotient algebra.

**Definition 2.21** For $(S, \leq, \Sigma)$ a coherent order-sorted signature, $A$ an order-sorted $\Sigma$-algebra, and $\sim$ an order-sorted $\Sigma$-congruence, the quotient of $A$ by $\sim$ is the order-sorted $\Sigma$-algebra $A/\sim$ defined as follows:

- for each top sort $t$, the carrier $(A/\sim)_t$ is $A_t/\sim$,
- for each other sort $s$ whose connected component has top sort $\text{max}(s)$, the carrier $(A/\sim)_s$ is $\pi_{\text{max}(s)}(A_s)$, where $\pi_{\text{max}(s)} : A_{\text{max}(s)} \mapsto (A/\sim)_{\text{max}(s)}$ is the natural projection $a \mapsto [a]$ of each element $a$ to its $\sim_{\text{max}(s)}$ equivalence class.
- The interpretation of each function symbol $f$ of rank $(\sigma, s)$ is given by:

$$f^\sigma_{(A/\sim)}([a_1], \ldots, [a_n]) = [f^\sigma_{A}(a'_1, \ldots, a'_n)]$$

where $\sigma = \sigma_1, \ldots, \sigma_n$ and $a'_i \in [a_i] \cap A_{\sigma_i}$. The interpretation is well defined since $\sim$ is an order-sorted $\Sigma$-congruence.
Notice that the carrier for a sort $s$ is not simply $A_s/\sim$, but the restriction of the quotient map on the top sort of $s$. This is to ensure that $(A/\sim)_s \subseteq (A/\sim)_{s'}$ whenever $s \leq s'$.

The elements $a'_i$, in 1 above, are needed because not every member of $[a_i]$ is of sort $\sigma_i$, hence some of them might not belong to the domain of $f_A$. As an example consider the following case.

**Example 2.3** Let the signature be such that the sort structure is $S = \{s_1, s_2, s_3, s\}$ with $s_1, s_2, s_3 \leq s$, $\Sigma = \{a, b, c, f\}$, $a, b$ and $c$ are constants of rank $s_1$, $s_2$ and $s_3$ respectively, and $f$ has rank $\{(s_1, s_1), (s_3, s_3)\}$. The situation is depicted in figure 1.

Consider the initial algebra $T$. Notice that $s_2$ is not in the arity of $f$, hence $fb$ is not in $T$. Let $f^{(i)}x$ denote the term $x$, and for $i > 0$, let $f^{(i)}x$ denote the term $f f \ldots f x$ where $f$ occurs $i$ times.

Let $\sim$ be the reflexive, symmetric and transitive closure of the relation $R$ given by:

$$R_s = \{(a, b), (b, c)\} \cup \bigcup_{i \geq 0} \{(f^{(i)}a, f^{(i)}c)\} \text{ and } R_{s_1} = R_{s_2} = R_{s_3} = \emptyset.$$ 

Clearly, $\sim$ is an order-sorted congruence. Let $A$ denote the quotient $\Sigma$-algebra $T_s/\sim$. We have $[a] = [b] = [c] = \{a, b, c\}$, $[f^{(i)}a] = [f^{(i)}c] = \{f^{(i)}a, f^{(i)}c\}$. The carrier of sort $s_1$ and $s_3$ is $\{[a], [fa], [ffa], \ldots, [f^{(i)}a], \ldots\}$, the carrier of sort $s_2$ is $\{[a]\}$.

How does one define $f_{\Sigma, s_1}^A([a])$? From one point of view since $a \in [a]$, we can say $f_{\Sigma, s_1}^A([a]) = [fa] = \{fa, fc\}$. But since $[a] = [b]$, we could let $f_{\Sigma, s_1}^A([a]) = [fb]$ which is undefined. Definition 2.21 takes care of this since it demands that $f_{\Sigma, s_1}^A([a]) = [fa']$ for some $a'$ of sort $s_1$ such that $a' \in [a]$. This forces $a' = a$, and rules $f_{\Sigma, s_1}^A([a]) = [fb]$ out. It also rules the choice of $c$ for $a'$ since $c$ is not of sort $s_1$. However, $fc \in [fa]$ implies that $[fa] = [fc]$ hence $f_{\Sigma, s_1}^A([a]) = [fc]$ is correct.

### 2.9 The top algebra

As described above, order-sorted congruences are used in defining quotient algebras. The construction of such congruences is somewhat a delicate process because of their order-
sorted characteristic. If the signature is coherent, one can define a special kind of many-sorted congruence which is simpler to construct and which naturally extends to an order-sorted congruence. This congruence is therefore a useful tool for the construction of order-sorted quotient algebras as shown in section 3.3 where it is used to construct a model. The many-sorted congruence is defined on the top sorts which constitute a many-sorted algebra which we call the top algebra.

Given a coherent order-sorted algebra \(A\), the carriers for the top sorts in \(S\) and the functions defined on those sorts form a many-sorted algebra \(\text{top}(A)\). More formally

**Definition 2.22** Given a coherent order-sorted algebra \(A\) with signature \((S, \leq, \Sigma, \rho)\), the many-sorted signature \((S', \Sigma', \rho')\) is defined by considering the top sorts in \(\Sigma\):

\[
S' = \{ \omega \in S \mid \omega \text{ is a top sort} \}
\]

\[
\Sigma' = \{ f \in \Sigma \mid \rho(f) \cap (S')^* \times S' \neq \emptyset \}
\]

\[
\rho'(f) = \rho(f) \cap (S')^* \times S'
\]

Alternatively, one can look at \(\Sigma'\) as the family \(\Sigma_{(\omega, s)}\) where \(\omega\) and \(s\) are top sorts. From a \((S, \leq, \Sigma, \rho)\)-algebra \(A\) one obtains a \((S', \Sigma', \rho')\)-algebra \(\text{top}(A)\) by restricting \(A\) to the top sorts:

- for \(s\) a top sort, \(\text{top}(A)_s = A_s\)
- for \(f \in \Sigma', (\omega, s) \in \rho'(f)\), \(f_{\text{top}}^{\omega, s} = f^{\omega, s}_A\)

The algebra \(\text{top}(A)\) is called the top algebra of \(A\).

**Example 2.4** Consider the signature presented in example 2.1 and the algebra presented in example 2.2. For completeness, we present them once more.

The partially ordered set of sorts is \(S = \{\text{zero}, \text{rat}^+, \text{rat}\}\) with \(\text{zero} \leq \text{rat}, \text{rat}^+ \leq \text{rat}\).

The signature \(\Sigma\) is:

\[
\Sigma_{\text{rat-rat}, \text{rat}} = \{+\}
\]

\[
\Sigma_{\text{rat-rat}, \text{rat}^+} = \{/\}
\]

The order-sorted \(\Sigma\)-algebra \(A\) is: \(A_{\text{rat}} = \mathbb{Q}\) (the set of rational numbers), \(A_{\text{rat}^+} = \mathbb{Q} - \{0\}\) (the set of non-zero rationals), and \(A_{\text{zero}} = \{0\}\). The functions have their natural interpretations: \(+ is addition of rational numbers, \(/ is division.

Division is missing from the algebra \(\text{top}(A)\) which is as follows: \(\text{top}(A)_{\text{rat}} = \mathbb{Q}\), \(+ is addition. The set \(S'\) of top sorts is \(\{\text{rat}\}\) and the signature of this top algebra is \(\Sigma'_{\text{rat-rat}, \text{rat}} = \{+\}\).

**Definition 2.23** We say that a many-sorted congruence \(\sim\) on \(\text{top}(A)\) has the lower sorts property iff \(x_1 \sim_{t_1} y_1, \ldots, x_n \sim_{t_n} y_n\) implies that for any function symbol \(f \in \Sigma\) of rank \((\sigma, \omega)\) where \(\sigma = \sigma_1 \ldots \sigma_n\) with \(\sigma_i \leq t_i\), if \(x_i\) and \(y_i\) are also of sort \(\sigma_i\) then

\[
f_A^{\sigma, \omega}(x_1, \ldots, x_n) \sim_{t_1} f_A^{\sigma, \omega}(y_1, \ldots, y_n)
\]

for \(\omega_i\) the top sort of the connected component of \(\omega\).
Notice in the above definition that \( f \) is not required to be a member of \( \Sigma' \), the signature of \( \text{top}(A) \). However \( f^\omega_t(x_1, \ldots, x_n) \) is an element of \( A_t \) for every sort \( t \geq \omega \), in particular of \( A_\omega = (\text{top}(A))_\omega \), hence the definition makes sense. Also notice that in the case of initial algebras, by lemma 2.5, if two elements are congruent in some sort, they are congruent in every sort to which both belong. This allows us to strengthen the lower sorts condition on initial order-sorted algebras as follows.

**Lemma 2.6** A congruence \( \sim \) on the top algebra of an initial algebra has the lower sorts property if and only if
\[
  x_1 \sim y_1, \ldots, x_n \sim y_n \text{ implies that for any function symbol } f \in \Sigma \text{ such that } f_A(x_1, \ldots, x_n) \text{ and } f_A(y_1, \ldots, y_n) \text{ are defined and are of the same sort, } f_A(x_1, \ldots, x_n) \sim f_A(y_1, \ldots, y_n).
\]

**Example 2.5** On the top algebra of the previous example, define \( x \sim y \) iff \( |x - y| \) is even. Since the only function symbol on \( \text{top}(A) \) is \(+\), clearly \( \sim \) is a \( \text{top}(A) \)-congruence. However, it does not satisfy the lower sorts property. For example \( 1 \sim 3 \) and \( 2 \sim 4 \) but \( 1/2 \not\sim 3/4 \) even though \( 1/2 \) and \( 3/4 \) are in \( \text{top}(A) \).

In this previous example \( \sim \) is not an \( A \)-congruence. As the following lemma shows, this is not a coincidence.

**Lemma 2.7** The restriction of an \( A \)-order-sorted congruence to \( \text{top}(A) \) has the lower sorts property.

**Proof:** Let \( \simeq \) be an order-sorted congruence on \( A \) and let \( \sim \) be its restriction to \( \text{top}(A) \).
Suppose \( x_i, y_i \in \text{top}(A)_{t_i} \) and \( x_i \simeq_{t_i} y_i \) for \( 1 \leq i \leq n \). By definition of \( \simeq \), it must be the case that \( x_i \simeq_{t_i} y_i \) as well. Let \( (\sigma_1 \ldots \sigma_n, \omega) \in \rho(f) \) with \( \sigma_i \leq t_i \). If \( x_i \) and \( y_i \) are also of sort \( \sigma_i \), by the order sorted nature of \( \simeq \), we must have \( x_i \simeq_{\sigma_i} y_i \). Since \( \simeq \) is a congruence, \( f_A(x_1, \ldots, x_n) \simeq_{\omega} f_A(y_1, \ldots, y_n) \) which by order-sortedness implies \( f_A(x_1, \ldots, x_n) \sim_{\omega t} f_A(y_1, \ldots, y_n) \) for \( \omega_t \) the top element of the connected component of \( \omega \).

The converse is true as well, namely that from a many-sorted congruence on the top algebra one can obtain an order-sorted congruence on the order-sorted algebra.

**Lemma 2.8** Let \( \sim \) be a many-sorted congruence on \( \text{top}(A) \) that satisfies the lower sorts property, then the \( S \)-indexed relation \( \simeq \) defined by
\[
  \simeq_s = \{(x, y) \mid x \sim_t y \text{ for } t \geq s\}
\]
is an \( A \)-order-sorted congruence.

**Proof:** Clearly, \( \simeq \) is an equivalence relation, we show that it is a congruence. Let \( x_i \simeq_{\sigma_i} y_i \) for \( 1 \leq i \leq n \), and let \( f \) be a function symbol with \( (\sigma_1 \ldots \sigma_n, \omega) \) in its rank. We have to show that \( f_A(x_1, \ldots, x_n) \simeq_{\omega} f_A(y_1, \ldots, y_n) \). Indeed, by the definition of \( \simeq \), \( x_i \sim_{t_i} y_i \) for \( t_i \) the top sort of the connected component of \( \sigma_i \). Let \( \omega_t \) be the top sort in the component of \( \omega \), by the lower sorts property, \( f_A(x_1, \ldots, x_n) \sim_{\omega_t} f_A(y_1, \ldots, y_n) \). Hence by definition \( f_A(x_1, \ldots, x_n) \simeq_{\omega} f_A(y_1, \ldots, y_n) \) as wanted.

It is easy to see that \( \simeq \) is order-sorted, therefore it is an order-sorted congruence. \( \square \)
These two lemmas actually show the existence of a one to one correspondence between the order-sorted congruences of an order-sorted algebra and the many-sorted congruences on its top algebra satisfying the lower sorts property. In the first lemma, from an order-sorted congruence \( \sim_1 \) one obtains a many-sorted congruence \( \sim_2 \) on the top algebra which satisfies the lower sorts property. Applying the second lemma, an order-sorted congruence \( \sim_3 \) is obtained. Since we are dealing with extensions and restrictions of a relation, it is easy to see that \( \sim_1 \) and \( \sim_3 \) are the same. Similarly if we start from a many-sorted congruence satisfying the lower sorts property, we obtain an order-sorted congruence whose restriction to the top algebra is the congruence with which we started.

This correspondence is useful when one wishes to construct order-sorted congruences since it is simpler to construct a many-sorted congruence for the many sorted top algebra than dealing directly with the order-sorted algebra itself. We use this result in the next section in order to construct an infinite model. Notice that this correspondence is monotonic in the following sense. Let \( \sim_1 \) and \( \sim_2 \) be many-sorted congruences on the top algebra, and let \( \sim_1^* \) and \( \sim_2^* \) be the corresponding order-sorted congruences. Then

\[
\sim_1 \subseteq \sim_2 \iff \sim_1^* \subseteq \sim_2^*
\]

We thus have as a corollary:

**Corollary 2.9** Given a coherent order-sorted signature \( \Sigma \) and a \( \Sigma \)-algebra \( A \), the least many-sorted congruence with the lower sorts property on \( \text{top}(A) \) exists if and only if the least order-sorted congruence on \( A \) exists. Furthermore, if they exist, they correspond to each other under the correspondence described above.

### 2.10 Least Order-sorted congruences

**Definition 2.24** Given an \( S \)-sorted relation \( R \) on an \( < S, \leq, \Sigma, \rho > \)-algebra \( A \), the least order-sorted congruence of \( R \) on \( A \), written \( \simeq_R \), is the least (with respect to inclusion) order-sorted congruence containing \( R \).

One way to show the existence of \( \simeq_R \) is to realize that it is the intersection of all the order-sorted congruences containing \( R \). Since there is at least one such congruence, namely \( \{(u,v) \mid u,v \in A\} \), and all of them contain \( R \), it is clear that this intersection is not empty. Another way is to give an inductive construction, as for the many-sorted case, and then prove that the congruence is order-sorted.

If the signature is coherent, we can use the results of section 2.9 on top algebras as follows. Let \( R^t \) be the restriction to the top sorts of the completion of \( R \), that is: for a top sort \( \sigma \), \( R^t_\sigma = \{(u,v) \mid (u,v) \in R_s \text{ for some } s \leq \sigma\} \). The least congruence containing \( R^t \) with the lower sorts property on \( \text{top}(A) \) induces, by virtue of corollary 2.9, the least order-sorted congruence \( \simeq_R \) of \( R \) on \( A \).

Thus we proceed to show how we can construct \( \simeq_Q \), the least congruence of a relation \( Q \) with the lower sorts property on \( \text{top}(A) \). In our case \( Q = R^t \). For a relation \( Q \), let \( Q^{-1} = \{(v,u) \mid (u,v) \in Q\} \). The construction is in stages as follows:
Construction 2.10

$$\simeq_{0,s} = \{ (u, u) \mid u \in \text{top}(A) \}_s \cup Q_s \cup Q_s^{-1}$$

for \( i > 0 \),

$$\simeq_{i,s} = \simeq_{i-1,s} \cup \{ (u, w) \mid \exists v \ (u \simeq_{i-1,s} v \simeq_{i-1,s} w) \} \cup \{ (f_A(u_1, \ldots, u_n), f_A(v_1, \ldots, v_n)) \mid f \in \Sigma, (\sigma_1 \ldots \sigma_n, \omega) \in \rho(f), \omega \leq s, \text{ and for } 1 \leq j \leq n, u_j \simeq_{i-1,\sigma_j} v_j \}$$

Notice that we use the functions \( f_A \) (on \( A \)) and not \( f_{\text{top}}(A) \) (on \( \text{top}(A) \)), this is what ensures the lower sorts property. The third member of the union can be more informally expressed as

$$\{ (f_A(u_1, \ldots, u_n), f_A(v_1, \ldots, v_n)) \mid f_A(u_1, \ldots, u_n) \text{ and } f_A(v_1, \ldots, v_n) \text{ are well defined and for } 1 \leq j \leq n, u_j \simeq_{i-1,\sigma_j} v_j \}$$

Finally, let \( \simeq_Q = \bigcup_{i \geq 0} \simeq_i \).

One can see that \( \simeq_Q \) is a many-sorted congruence on \( \text{top}(A) \). It is clearly reflexive, symmetry follows from the fact that \( Q \) and \( Q^{-1} \) are in \( \simeq_0 \), and transitivity is ensured by the second member of the union in the construction of \( \simeq_i \). Thus \( \simeq_Q \) is an equivalence relation. Furthermore \( \simeq_Q \) is preserved under function application by virtue of the third member of this union. Actually in that case we are adding more than is needed for a simple \( \text{top}(A) \) congruence, namely we are causing it to satisfy the lower sorts property.

That \( \simeq_Q \) is minimal can be shown by inductively proving \( \simeq_i \subseteq R \) for any other many-sorted congruence \( R \) with the lower sorts property. Therefore \( \simeq_Q \) is the least congruence on \( \text{top}(A) \) with the lower sorts property containing \( Q \).

What are the ways in which two elements become congruent? It is clearly by propagation of \( Q \) and \( Q^{-1} \) via transitivity and function application. Thus whenever \( u \simeq v \) there should be a way of specifying exactly which pairs in \( Q \) have been used. We now formalize this intuition.

Definition 2.25 Based on the least congruence \( \simeq \), the relation \( \sim \) is defined as follows:

- \( u \sim_0 v \) if and only if \( u = v \)
- \( u \sim_i v \) if and only if either \( u = v \) or \( u = f_A(u_1, \ldots, u_n), v = f_A(v_1, \ldots, v_n), \text{ and for } 1 \leq j \leq n, u_j \simeq_{i-1,\sigma_j} v_j \).

Notice that \( u \sim_i v \) implies \( u \simeq_i v \), hence \( \sim_i \) is a weaker notion. Also, \( u \sim_i v \) implies \( u \sim_{i+1} v \).

Lemma 2.11 If \( u \sim_i v \sim_i w \) then \( u \sim_{i+1} w \).
Proof: If either \( u = v \) or \( v = w \), the claim clearly holds. Suppose \( u = v \), then \( v \sim_i w \)
implies $v \sim_{i+1} w$. Similarly for $v = w$.

Otherwise, $u = f_A(u_1, \ldots, u_n), v = f_A(v_1, \ldots, v_n), w = f_A(w_1, \ldots, w_n)$ and for $1 \leq j \leq n$, $u_j \sim_{i-1} v_j \sim_{i-1} w_j$. By definition of $\sim_i$, we have $u_j \sim_i w_j$, which forces $u = f_A(u_1, \ldots, u_n) \sim_{i+1} f_A(w_1, \ldots, w_n) = w$ as wanted. □

We are now ready to prove the lemma that relates two congruent terms to the pairs in $Q$ which make them congruent.

**Lemma 2.12** If $u \sim_i v$, then either

1. $u = v$ or,
2. $u \sim_i v$ (and $u \neq v$) or,
3. There exist $(l_1, r_1), \ldots, (l_n, r_n)$ in $Q \cup Q^{-1}$ such that $u \sim_{i-l_1, r_1} \ldots \sim_{i-1} r_j \sim_{i-l_{j+1}, r_{j+1}} \ldots \sim_{i} v$.

**Proof:** The claim is clearly true for $\sim_0$ for either $u = v$ or $(u, v) \in Q \cup Q^{-1}$ in which case $l_1 = u, r_1 = v$ and $u \sim_0 l_1, r_1 \sim_0 v$, so that $(u, v)$ is a chain of length 1 that satisfies 3.

Assume that the claim holds for $0 \leq k < i$. Suppose that $u \sim_i v$ and that $i$ is minimal.

There are two ways in which $u$ and $v$ can become congruent:

1. Function application: for $1 \leq j \leq n$ $u_j \sim_{i-1} v_j$ and $u = f_A(u_1, \ldots, u_n), v = f_A(v_1, \ldots, v_n)$. Therefore $u \sim_i v$; or

2. Transitivity: there exists $y$ such that $u \sim_{i-1} y \sim_{i-1} v$. By inductive hypothesis, we can say that one of the following cases occurs for $u$ and $y$:
   a1) $u = y$ or
   a2) $u \sim_{i-1} y$ or
   a3) $u \sim_{i-1} l_1, r_1 \sim_{i-1} l_2, r_2, \ldots, r_n \sim_{i-1} y$ for some $(l_1, r_1), \ldots, (l_n, r_n)$ in $Q \cup Q^{-1}$.
   Similarly $y \sim_{i-1} v$ implies that
   b1) $y = v$ or
   b2) $y \sim_{i-1} v$ or
   b3) $y \sim_{i-1} l_1, r_1 \sim_{i-1} l_2, r_2, \ldots, r_n \sim_{i-1} v$ for some $(l_1, r_1), \ldots, (l_n, r_n)$ in $Q \cup Q^{-1}$.

Case a1 would violate the minimality condition as would case b1. If case a2 and b2 occur then, by lemma 2.11 we have that $u \sim_{i-1} y \sim_{i-1} v$, that is $u \sim_i v$.

Suppose now that a2 and b3 occur. Then $u \sim_{i-1} y \sim_{i-1} l_1$. By lemma 2.11 we have $u \sim_i l_1$, hence the pairs $(l_1, r_1), \ldots, (l_n, r_n)$ are such that $u \sim_i l_1, r_1, r_2, \ldots, r_n \sim_i v$ as wanted.

The case a3 and b3 is handled similarly. Notice that $r_n \sim_{i-1} y \sim_{i-1} l_1$, hence $r_n \sim_{i} l_1$, and $(l_1, r_1), \ldots, (l_n, r_n)$ are pairs with property 3. □
3 Congruences Associated With Order-sorted Horn Clauses

Let \((S, \leq, \Sigma, \rho)\) be a coherent signature, and let \(T = T_{(S, \leq, \Sigma, \rho)}\) be the order-sorted term algebra on that signature. Let \(H_1\) be a set of ground order-sorted Horn clauses over \(T\), possibly with equational atoms, and let \(H\) be the set of equational Horn clauses obtained as described in section 2.6.

3.1 The Graph \(GT(H)\)

In order to obtain efficiency and to avoid empty carriers, we restrict our attention to the sorts which actually appear in the set of clauses, as opposed to the set of all sorts in the logic language to which the clauses belong.

**Definition 3.1** Given a set \(H\) of ground Horn clauses over the term algebra of a coherent order-sorted signature \((S, \leq, \Sigma, \rho)\), let

- \(TERM(H)\) be the set of all subterms of terms occurring in the atomic formulae in \(H\); and
- \(S(H)\) be the set of sorts of all terms in \(TERM(H)\), partially ordered by the restriction of \(\leq\) to \(S(H)\).

The graph \(GT(H)\) represents subterm dependencies, and it is used to propagate congruential information. This graph was first defined by Kozen (under a different name) to study the properties of finitely presented algebras, [8,9,10,11].

For every sort \(s\) in \(S(H)\), let \(TERM(H)_s\) be the set of all terms of sort \(s\) in \(TERM(H)\). Note that by the definition, each set \(TERM(H)_s\) is nonempty. Let \(\Sigma(H)\) be the \(S(H)\)-ranked alphabet consisting of all constant and function symbols occurring in \(TERM(H)\) and let \(\rho(H)\) be the restriction of \(\rho\) to \(\Sigma(H)\).

Consider the signature \((S(H), \leq, \Sigma(H), \rho(H))\). Notice that \(\Sigma(H) \subseteq \Sigma\) and if \(\Sigma\) is coherent, so is \(\Sigma(H)\).

The graph \(GT(H)\) has the set \(TERM(H)\) as its set of nodes, its edges and the function \(\Lambda\) labeling its nodes are defined as follows:

- For every node \(t\) in \(TERM(H)\), if \(t\) is a constant, then \(\Lambda(t) = t\), else \(t\) is of the form \(fy_1 \ldots y_k\) and \(\Lambda(t) = f\);

- For every node \(t\) in \(TERM(H)\), if \(t\) is of the form \(f y_1 \ldots y_k\), then \(t\) has exactly \(k\) successors \(y_1 \ldots y_k\), else \(t\) is a constant and it is a terminal node of \(GT(H)\).

Given a node \(u \in TERM(H)\), if \(u\) has \(n\) successors, \(n > 0\), then the \(i\)-th successor of \(u\) is denoted by \(u[i]\).
3.2 Order-sorted Graph Congruence Closure

Example 3.1 Consider the signature in which $S = \{ i, s \}$, $\Sigma = \{ f, g, a, b, c \}$, with $\rho(f) = (i, s)$, $\rho(g) = (s, s)$, $\rho(a) = i$, $\rho(b) = \rho(c) = s$. Let $H$ be the set of Horn clauses

$$\{ f(a, b) \equiv c, : -g(f(a, b), a) \equiv g(c, a) \}.$$  

Then, $TERM(H)_i = \{ a \}$, $TERM(H)_s = \{ b, c, f(a, b), g(c, a), g(f(a, b), a) \}$, and $E = \{(f(a, b), c)\}$. The graph $GT(H)$ is shown in figure 2.

3.2 Order-sorted Graph Congruence Closure

The crucial concept in showing the decidability of unsatisfiability for ground equational Horn clauses is a certain kind of equivalence relation on the graph $GT(H)$ called an order-sorted graph congruence.

Definition 3.2 Given the graph $GT(H)$ associated with the set $H$ of ground Horn clauses, an $S(H)$-indexed family $R$ of relations $R_s$ over $TERM(H)_s$ is an order-sorted graph congruence on $GT(H)$ iff:

1. Each $R_s$ is an equivalence relation;
2. For every pair $(u, v) \in TERM(H)^2_s$, if $\Lambda(u) = \Lambda(v), (w_1 \ldots w_n, s) \in \rho(\Lambda(u))$, and for every $i$, $1 \leq i \leq n$, $u[i]R_{w_i}v[i]$, then $uR_s v$.
3. For every pair $(u, v) \in TERM(H)^2_s$, if $s_1 \in co-arity(\Lambda(u)) \cap co-arity(\Lambda(v))$ and $s_1 \leq s_2$ then $uR_{s_1} v \iff uR_{s_2} v$.
4. For every pair $(u, v)$ of nodes in $TERM(H)^2_s$:
   - If $u \equiv v \in H$, then $uR_s v$; and
   - if $u \equiv v$ is the head of a clause $u \equiv v : -u_1 \equiv v_1, \ldots, u_n \equiv v_n$ in $H$, and for every $i$, $1 \leq i \leq n$, $u_iR_{s_i}v_i$, then $uR_s v$. 

Figure 2: The graph $GT(H)$
Given an $S(H)$ indexed family of relations $E_s$ on $TERM(H)$, the order-sorted graph congruence closure of $E_s$, denoted $\leftrightarrow_{E_s}$, is the least order-sorted graph congruence on $GT(H)$ containing $E_s$. In section 4 we prove the existence of $\leftrightarrow_E$ and provide a construction for it.

We now concentrate on the relationship between the graph congruence closure and the least order-sorted congruence. Let $\Sigma(H)$ be the set of all function and constant symbols appearing in $H$. Consider the (free) order-sorted $\Sigma(H)$-term algebra $\mathcal{T}_\Sigma$. Every function symbol is interpreted as a term constructor. Notice that $TERM(H) \subseteq \mathcal{T}_\Sigma$ and $\leftrightarrow_{E_s}$ is a graph congruence which is not necessarily a $\mathcal{T}_\Sigma$-congruence, mainly because $TERM(H)$ is finite and not closed under function application. If we want to make $\leftrightarrow_{E_s}$ into an order-sorted-$\Sigma(H)$ congruence we can consider $\simeq$ (which we denote by $\simeq$), the least order-sorted congruence containing $\leftrightarrow_{E_s}$. What is the relationship between $\leftrightarrow_{E_s}$ and $\simeq$?

As we now show, $\leftrightarrow_{E_s}$ is a conservative extension of $\leftrightarrow_E$.

**Lemma 3.1** [Conservativeness] For any $u, v \in TERM(H)$, $u \leftrightarrow_{E_s} v$ if and only if $u \simeq v$.

**Proof:** Recall that $\simeq$ was constructed in stages (construction 2.10 on page 14). We show by induction on $i$ that for any $u, v \in TERM(H)$, $u \simeq_i v$ implies $u \leftrightarrow_{E_s} v$.

This is clearly the case for $i = 0$.

Let $i > 0$ be the least number satisfying $u \simeq_i v$. By lemma 2.12 we have one of the following cases:

1. $u = v$ which cannot occur because of the minimality of $i$, or
2. $u \simeq_i v$. Then $u = f(u_1, \ldots, u_n), v = f(v_1, \ldots, v_n)$ and for $1 \leq j \leq n$, $u_j \simeq_{i-1} v_j$. Since $TERM(H)$ is closed under subterms, $u_j, v_j \in TERM(H)$ and the inductive hypothesis can be applied to conclude $u_j \leftrightarrow_{E_s} v_j$. Since $\leftrightarrow_{E_s}$ is closed under function application we have: $u = f(u_1, \ldots, u_n) \leftrightarrow_{E_s} v = f(v_1, \ldots, v_n)$;
3. There exist $(l_1, r_1), \ldots, (l_n, r_n) \in \leftrightarrow_{E_s}$ such that $u \simeq_i l_1 \leftrightarrow_{E_s} r_1 \simeq_i l_2 \leftrightarrow_{E_s} r_2, \ldots, r_j \simeq_i l_{j+1} \leftrightarrow_{E_s} r_{j+1}, \ldots, l_n \leftrightarrow_{E_s} r_n \simeq_i v$. As in the previous case, since $u$ and $l_1$ are in $TERMS(H)$ and $u \simeq_i l_1$, we can prove $u \leftrightarrow_{E_s} l_1$. The same argument applies to show that $r_j \leftrightarrow_{E_s} l_{j+1}$ for $1 \leq j < n$ and $r_n \leftrightarrow_{E_s} v$. Hence we have that $u \leftrightarrow_{E_s} l_1 \leftrightarrow_{E_s} \ldots \leftrightarrow_{E_s} r_n \leftrightarrow_{E_s} v$. Since $\leftrightarrow_{E_s}$ is an equivalence relation it is transitively closed, and therefore $u \leftrightarrow_{E_s} v$.

A more formal treatment of this case would use and inductive argument on pairs $<i, n>$ ordered lexicographically.

\[\square\]

### 3.3 A Method For Testing Unsatisfiability

For every top sort $s \in S(H)$, let $E_s$ be the set of all pairs $(l, r)$ such that $s$ is the top sort of the connected component to which $l$ and $r$ belong and $l \equiv r$ is an equation in $H$. Notice that the above definition makes sense because $l \equiv r$ can occur in $H$ provided the sorts of $l$ and $r$ have a common element. Since the signature is coherent, all the sorts of a term
are in one connected component, hence all the sorts of \( l \) and \( r \) are in the same connected component. Let \( E \) be the \( S(H) \)-indexed family \((E_s)_{s \in S(H)}\). The key to the method is that \( \leftrightarrow_E \), the order-sorted congruence closure of \( E \), exists and that there is an algorithm for computing it.

The proof is somewhat more complex than the one given by Gallier in [2] where a finite model is presented. There, a finite algebra is constructed from the elements in \( TERM(H) \). The interpretation of a function symbol \( f \) of rank \( \rho(f) = (\sigma_1, \ldots, \sigma_n, s) \) on \( x_1, \ldots, x_n \) (where \( x_i \) is of sort \( \sigma_i \)), is defined to be either

1. \( f x_1 \ldots x_n \) if \( f x_1 \ldots x_n \in TERM(H) \), or
2. \( f z_1 \ldots z_n \) if \( \exists z_1, \ldots, z_n \) such that for \( 1 \leq j \leq n \), \( x_j \leftrightarrow_E z_j \) and \( f z_1 \ldots z_n \in TERM(H) \), or
3. \( c \) for some element \( c \in TERM(H)_s \), otherwise.

In the order-sorted case, case 3 causes trouble as can be seen in the following example.

**Example 3.2** Let the sort structure be: \( s_1, s_2 \leq s \) and \( t_1 \leq t \). Suppose \( \Sigma \) consists of the constants \( a \) of sort \( s_1 \), \( b \) of sort \( s_2 \) and \( c \) of sort \( t_1 \), in addition there is a function symbol \( f \) of rank \( \rho(f) = ((s, t), (s_2, t_1)) \). Figure 3 depicts the situation.

Let the set \( H \) of Horn clauses be \( \{a \equiv b, fa \equiv fa, c \equiv c\} \). The formulae \( fa \equiv fa \) and \( c \equiv c \) are present just to force \( fa \) and \( c \) to be in \( TERM(H) \).

Since \( fb \notin TERM(H) \) and \( c \) is the only element of sort \( t_1 \), we would define \( f_M^{s_2, t_1}(b) = c \). Hence by order-sortedness \( f_M^{s_2, t_1}(b) = c \) as well.

On the other hand, since \( fa \in TERM(H) \), \( f_M^{s_2, t_1}(a) = fa \). Since \( a \equiv b \), \( f_M^{s_2, t_1}(a) \) and \( f_M^{s_2, t_1}(b) \) would have to be congruent, i.e. \( fa \) congruent to \( c \). However, clearly \( fa \) and \( c \) are not congruent modulo \( \leftrightarrow_E \).

Our construction is therefore different in that we deal with an infinite model containing \( TERM(H) \) and a congruence which is conservative over \( \leftrightarrow_E \). From the infinite model we present, one can then extract a finite one.
Theorem 3.2 [Soundness and completeness] Let $H$ be a set of order-sorted ground Horn clauses (with equality), and let $E$ be as defined above. If $\leftrightarrow^*_E$ is the order-sorted congruence closure on $GT(H)$ of $E$, then

$$H \text{ is unsatisfiable}$$

iff

for some clause $:- u_1 \equiv v_1, \ldots, u_n \equiv v_n$ in $H$,

for every $i$, $1 \leq i \leq n$, we have $u_i \leftrightarrow^*_E v_i$.

Proof: The proof is obtained by combining and generalizing the techniques used by Gallier in [2]. Let $S$ be the subset of $H$ consisting of the set of definite clauses in $H$.

First, we show that the $S(H)$-indexed family $R$ of relations $R_s$ on $TERM(H)$ defined such that

$$t R_s u \iff S \models t \equiv u,$$

is a congruence on $GT(H)$ containing $E$. The details are straightforward and are left to the reader.

Since $\leftrightarrow^*_E$ is the least congruence on $GT(H)$ containing $E$, for any terms $l, r \in TERM(H)$,

$$l \leftrightarrow^*_E r \iff S \models l \equiv r.$$

Then, if for some negative clause $:- u_1 \equiv v_1, \ldots, u_n \equiv v_n$ in $H$, we have $u_i \leftrightarrow^*_E v_i$ for every $i$, $1 \leq i \leq n$, then $S \models u_1 \equiv v_1 \land \ldots \land u_n \equiv v_n$ holds, which implies that the set $S \cup \{- u_1 \equiv v_1, \ldots, u_n \equiv v_n\}$ is unsatisfiable. Consequently, $H$ is unsatisfiable. Notice that as a matter of fact only the top sort components of $\leftrightarrow^*_E$ are needed here since every $l$ and $r$ belong to some top sort $t$ and $l \leftrightarrow^*_E t r$.

Conversely, assume that there is no negative clause $:- u_1 \equiv v_1, \ldots, u_n \equiv v_n$ in $H$ such that, $u_i \leftrightarrow^*_E v_i$ for every $i$, $1 \leq i \leq n$. We shall construct a model $M$ of $H$.

Let $\Sigma_1$ be the set of all function and constant symbols excluding the ones which represent predicate letters (notice that $\Sigma_1 \subseteq \Sigma$). Consider the initial order-sorted $\Sigma_1$-term algebra $T_{\Sigma_1}$. Every function symbol is interpreted as a term constructor. We will construct the model $M$ by first defining a congruence on $T_{\Sigma_1}$ and then giving an interpretation for the predicate symbols on the quotient algebra.

Let $\Sigma_1$ be the set of all function and constant symbols excluding the ones which represent predicate letters (notice that $\Sigma_1 \subseteq \Sigma$). Consider the initial order-sorted $\Sigma_1$-term algebra $T_{\Sigma_1}$. Every function symbol is interpreted as a term constructor. We will construct the model $M$ by first defining a congruence on $T_{\Sigma_1}$ and then giving an interpretation for the predicate symbols on the quotient algebra.

Let $\simeq$ be the least order-sorted congruence containing $\leftrightarrow^*_E$ on $T_{\Sigma_1}$. By the conservativity lemma 3.1, we have that for $u, v \in TERM(H)$ of sort $s \neq \text{bool}$,

$$u \leftrightarrow^*_E, v \iff u \simeq, v.$$  \hspace{1cm} (2)

This property is important because it shows that incongruences on the graph are preserved by the algebra congruence. This is needed to show that our algebra is indeed a model.

Consider the quotient $T_{\Sigma_1} / \simeq$ which is itself an order-sorted algebra. Notice that (2) implies that for nodes $u, v$ of sort $s \neq \text{bool}$ in $TERM(H)$,

$$[u] \simeq = [v] \simeq \iff u \leftrightarrow^*_E v.$$  \hspace{1cm} (3)
3.3 A Method For Testing Unsatisfiability

We now provide an interpretation for the predicate symbols, thereby making the \(T_{\Sigma_1}/\simeq\) into a \(\Sigma\)-algebra \(M\). The symbol \(\top\) is interpreted as \(\text{true}\). For every predicate symbol \(P\), if \((\sigma_1 \ldots \sigma_n) \in \rho(f)\), and \([u_1], \ldots, [u_n]\) are of sort \(\sigma_1 \ldots \sigma_n\), then

\[
P_M([u_1], \ldots, [u_n]) \overset{df}{=} \begin{cases} 
\text{true} & \text{iff for every } i, 1 \leq i \leq n \text{ there exists a } z_i \in [u_i] \\
& \text{s.t. } P_{z_1} \ldots z_n \leftrightarrow_{E,\text{bool}} \top \\
\text{false} & \text{otherwise}
\end{cases}
\]

It is obvious from the definition that if \(P\) is of ranks \((\tau, \text{bool})\) and \((\sigma, \text{bool})\) with \(\sigma \leq \tau\), then \(P^\sigma_{M^\tau\text{bool}}([u_1], \ldots, [u_n]) = \text{true} \iff P^\tau_{M\text{bool}}([u_1], \ldots, [u_n]) = \text{true}\). Hence this is an order-sorted \(\Sigma\)-algebra, which we denote by \(M\). The graph congruence is preserved in \(M\), i.e. given terms \(u_1, \ldots, u_n\) in \(\text{TERM}(H)\),

\[
P_M([u_1], \ldots, [u_n]) = \text{true} \iff Pu_1 \ldots u_n \leftrightarrow_{E,\text{bool}} \top.
\]

Clearly, \(Pu_1 \ldots u_n \leftrightarrow_{E,\text{bool}} \top\) implies \(P_M([u_1], \ldots, [u_n]) = \text{true}\) since \(u_i \in [u_i]\). For the converse, assume \(P_M([u_1], \ldots, [u_n]) = \text{true}\). Then there exist \(z_1, \ldots, z_n\) such that \(z_i \simeq u_i\) and \(Pz_1 \ldots z_n \leftrightarrow_{E,\text{bool}} \top\). Since \(u_i\) and \(z_i\) are in \(\text{TERM}(H)\), by property 3 above we conclude that \(u_i \leftrightarrow_E z_i\). Since \(\leftrightarrow_E\) is a congruence, this implies \(Pu_1 \ldots u_n \leftrightarrow_E Pz_1 \ldots z_n \leftrightarrow E \top\).

If every non-boolean constant \(c\) is interpreted as \([c]\), it can easily be seen that every non-boolean term \(t\) is mapped onto \([t]\). Every boolean term is mapped into \(\text{true}\) or \(\text{false}\). By 3 and 4 above we have:

\[
M \models u \equiv v \iff u \leftrightarrow_E v.
\]

We now prove that \(M\) with this interpretation is a model of \(H\).

For every clause \(u \equiv v \in H\), we have \((u, v) \in E_s\) for the top sort \(s\) of the component to which the sorts of \(u\) and \(v\) belong. Since \(\leftrightarrow_E\) is a congruence containing \(E\), we have \(u \leftrightarrow_E v\). But then, by 5, we have \(M \models u \equiv v\).

For every clause \(u \equiv v : - u_1 \equiv v_1, \ldots, u_n \equiv v_n\) in \(H\), if \(M \models u_i \equiv v_i\) for every \(i, 1 \leq i \leq n\), by 5, we have \(u_i \leftrightarrow_E v_i\) for \(1 \leq i \leq n\). Since \(\leftrightarrow_E\) is a congruence on \(\text{GT}(H)\), we have \(u \leftrightarrow_E v\). By 5, this is equivalent to \(M \models u \equiv v\). Hence,

\[
M \models u \equiv v : - u_1 \equiv v_1, \ldots, u_n \equiv v_n.
\]

Finally, given any negative clause \(- u_1 \equiv v_1, \ldots, u_n \equiv v_n\) in \(H\), recall that it is assumed that we cannot have \(u_i \leftrightarrow_E v_i\) for every \(i, 1 \leq i \leq n\). Then, for some \(j, 1 \leq j \leq n\), \(u_j\) and \(v_j\) are not \(\leftrightarrow_E\) congruent, and by 5, this implies that \(M \not\models u_j \equiv v_j\), that is, \(M \models \neg u_j \equiv v_j\). But this implies that

\[
M \models : - u_1 \equiv v_1, \ldots, u_n \equiv v_n.
\]

Hence, \(M\) is a model of every clause in \(H\). This concludes the proof.

It is interesting to note that the soundness part of theorem 3.2 follows from the fact that \(\leftrightarrow_E\) is the least congruence on \(\text{GT}(H)\) containing \(E\), and that the completeness part follows from the fact that \(\leftrightarrow_E\) is a graph congruence. It only remains to prove that \(\leftrightarrow_E\) exists and to give an algorithm for computing it.
Example 3.3 Consider the signature of example 2.3 on page 10 where the sort structure is $S = \{s_1, s_2, s_3, s\}$ with $s_1, s_2, s_3 \leq s$, $\Sigma = \{a, b, c, f\}$, $a, b, c$ are constants of rank $s_1, s_2$ and $s_3$ respectively, and $f$ has rank $\{(s_1, s_1), (s_3, s_3)\}$. Notice that the signature is coherent and has one connected component: $\{s_1, s_2, s_3, s\}$. Given $H = \{a = b, b = c\}$. It turns out that $fa = fc$ is not a consequence of $H$, the reason being that for any $\Sigma$-algebra $A$, the $f$ appearing in $fa$ and that appearing on $fc$ do not denote the same function. The first denotes a function from $A_{s_1}$ into itself, while the latter a function from $A_{s_3}$ into itself.

To disprove $fa = fc$, construct the set $H' = \{a = b, b = c, \Box - fa = fc\}$ and show it is satisfiable. The model $M$ is given by theorem 3.2. The congruence classes are as follows:

- $[a] = [b] = [c] = \{a, b, c\}$
- Let $f^{(0)}x$ denote the term $x$, and for $i > 0$, let $f^{(i)}x$ denote the term $ff\ldots fx$ where $f$ occurs $i$ times. Then $[f^{(i)}a] = \{f^{(i)}a\}$ and $[f^{(i)}c] = \{f^{(i)}c\}$.

The carriers are:

- $M_s = \bigcup_{i \geq 0} \{[f^{(i)}a]\} \cup \bigcup_{i \geq 0} \{[f^{(i)}c]\}$
- $M_{s_1} = \bigcup_{i \geq 0} \{[f^{(i)}a]\}$
- $M_{s_2} = \{[a]\}$
- $M_{s_3} = \bigcup_{i \geq 0} \{[f^{(i)}c]\}$

The function symbol $f$ is interpreted as $f_M([x]) = [fx]$ for $x$ of sort $s_1$ or $s_3$ (notice that these are two different functions). $M$ satisfies $H'$ because $fa$ and $fc$ are in different congruence classes.

3.4 Finite models

In the last example, the model for $H'$ is infinite. In a sense it is too big. For example, the congruence class of $f^{100}a$ will never be used in proving $\neg fa = fc$.

We pointed out earlier certain difficulties in constructing a finite model. Using $M$, the infinite model of theorem 3.2, we are now in a position to construct a finite model.

For every top sort $t$ a representative element $c_t$ is chosen from $M_t$ (note that $c_t$ is an equivalence class). These elements are to be used for the value of $f[t]$ whenever $ft \notin \text{TERM}(H)$. Given a sort $s$, let $\text{top}(s)$ denote the top sort of its connected component.

The finite model $M'$ is defined as follows. The carrier for the sort $\text{bool}$ and the boolean functions are as in $M$. For a sort $s \neq \text{bool}$, its carrier is defined by

- $M'_s = \{[u] \in M_s \mid [u] \cap \text{TERM}(H)_s \neq \emptyset\} \cup \{c_{\text{top}(s)}\}$.

Note that $M'_s$ has at most as many elements as $\text{TERM}(H)_s$, hence each carrier is finite.

The interpretation for the function symbols uses the representative elements as follows. Let $\sigma = \sigma_1\ldots \sigma_n$, given a function symbol $f$ of rank $(\sigma, s)$ ($s \neq \text{bool}$) and terms $t_1, \ldots, t_n$ of sort $\sigma_1, \ldots, \sigma_n$,

$$f_{M'}^{\sigma,s}([t_1], \ldots, [t_n]) \triangleq \begin{cases} [ft_1 \ldots t_n] & \text{if } [ft_1 \ldots t_n] \cap \text{TERM}(H)_s \neq \emptyset, \\ c_{\text{top}(s)} & \text{otherwise} \end{cases}$$

We now have the following lemma.
Lemma 3.3 If $H$ is satisfiable then $M'$ is a finite model for it.

Notice that $M'$ is not unique since it depends upon the choice of the elements $c_t$.

Example 3.4 Consider the previous example. A finite model $M'$ for $H' = \{a \equiv b, b \equiv c, : -fa \equiv a\}$ is given as follows. First, choose $[f a]$ to be the representative for $M'_s$, i.e. $c_s = [f a]$. Then add $[f a]$ to all the carriers of sorts below $s$ to obtain:

$$
M_s = \{[a], [f a], [f c]\}
M_{s_1} = \{[a], [f a]\}
M_{s_2} = \{[a], [f a]\}
M_{s_3} = \{[a], [f a], [f c]\}
$$

The functions $f_{M'}$ are therefore given by:

$$
\begin{align*}
&f_{M'}^{s_1}( [a]) = [f a] \\
&f_{M'}^{s_1}( [f a]) = [f a] \\
&f_{M'}^{s_2}( [a]) = [f a] \\
&f_{M'}^{s_2}( [f a]) = c_s = [f a] \\
&f_{M'}^{s_3}( [f c]) = [f c] \\
\end{align*}
$$

4 Existence of the Order-sorted Graph Congruence Closure

We now prove that the order-sorted graph congruence closure of a relation $R$ on the graph $GT(H)$ exists. This can be done by interleaving steps in which a purely equational congruence closure is computed, and steps in which a purely implicational kind of closure is computed. The advantage of this method (even though it is not the most direct) is that it justifies the correctness of the algorithm for computing the graph congruence closure of $R$ on $GT(H)$.

First, we define the concept of an equational order-sorted congruence closure.

4.1 Equational Order-sorted Graph Congruence Closure

The notion of many-sorted equational congruence closure was first introduced (under a different name) by Kozen, [8,9]. In fact, Dexter Kozen appears to have given an $O(n^2)$-time algorithm solving the word problem for finitely presented algebras before everyone else [8]. Independently, the concept of congruence closure was defined in Nelson and Oppen, [12]. We have added the qualifier equational in order to distinguish it from the more general notion defined in section refsec-horn-cong that applies to Horn clauses.

For our purpose, we only need to consider the concept of equational order-sorted closure on the graph $GT(H)$ induced by some (fixed) set $H$ of ground Horn clauses. In the rest of this section, it is assumed that a fixed set $H$ of ground Horn clauses is given.
Definition 4.1 An \(S(H)\)-indexed family \(R\) of relations \(R_s\) over \(TERM(H)\), is an equational congruence on \(GT(H)\) iff:

1. Each \(R_s\) is an equivalence relation;
2. For every pair \((u,v)\) \(\in\) \(TERM(H)^2\), if \(\Lambda(u) = \Lambda(v)\), \((w_1 \ldots w_n, s) \in \rho(\Lambda(u))\), and for every \(i\), \(1 \leq i \leq n\), \(u[i]R_w v[i]\), then \(uR_s v\).
3. For every pair \((u,v)\) \(\in\) \(TERM(H)^2\), if \(s_1 \in co-arity(\Lambda(u)) \cap co-arity(\Lambda(v))\) and \(s_1 \leq s_2\) then \(uR_{s_1} v\) iff \(uR_{s_2} v\).

A non order-sorted version of the following lemma was first shown by Kozen, [8,9]. For the sake of completeness our proof is based upon the one presented in Gallier, [2,3].

Lemma 4.1 Given any \(S(H)\)-indexed family \(R\) of relations on \(TERM(H)\), there is a smallest equational order-sorted congruence \(\cong_R\) on the graph \(GT(H)\) containing \(R\).

Proof: Since \(R\) might not be an order-sorted relation, we complete it to \(R'\) (as in definition 2.18):

\[
R'_s = \{(u,v) \in A_s \times A_s \mid (u,v) \in R_i\text{ for some } t\text{ such that } t \geq s \text{ or } s \geq t\}.
\]

We define the sequence \(R^i\) of \(S(H)\)-indexed families of relations inductively as follows: For every sort \(s\) \(\in\) \(S(H)\), for every \(i \geq 0\),

\[
R^0_s = R'_s \cup \{(u,u) \mid u \in TERM(H)_s\},
R^{i+1}_s = R^i_s \cup \{(v,u) \in TERM(H)^2_s \mid (u,v) \in R^i_s\}
\cup \{(u,w) \in TERM(H)^2_s \mid \exists v \in TERM(H), (u,v) \in R^i_s \text{ and } (v,w) \in R^i_s\}
\cup \{(u,v) \in TERM(H)^2_s \mid \Lambda(u) = \Lambda(v), (w_1 \ldots w_n, s) \in \rho(\Lambda(u)),
\text{ and } u[j]R^i_{w'_j} v[j], 1 \leq j \leq n\text{, for some } s'\text{ connected to } s
\text{ such that } (w'_1 \ldots w'_n, s') \in \rho(\Lambda(u))\}.
\]

Let \((\cong_R)_s = \bigcup_{i \geq 0} R^i_s\). Clearly, \(\cong_R\) is a congruence. It is also order-sorted due the use of \(R'\) in \(R^0\) and the fact that the third union in the definition of \(R^{i+1}_s\) deals with a sort connected to \(s\). Since \(s_1 \leq s_2\) implies that \(s_1\) and \(s_2\) are connected, any \(s'\) is connected to \(s_1\) if and only if it is connected to \(s_2\). It is easily shown by induction that every equational order-sorted congruence on \(GT(H)\) containing \(R\) contains every \(R^i\), and that \(\cong_R\) is an equational order-sorted congruence on \(GT(H)\). Hence, \(\cong_R\) is the least equational order-sorted congruence on \(GT(H)\) containing \(R\).

Since the graph \(GT(H)\) is finite, there must exist some integer \(i\) such that \(R^i = R^{i+1}\). Hence, the equational order-sorted congruence closure \(\cong_R\) of \(R\) is computable.
4.2 Implicational Closure

Let $H$ be a set of equational ground Horn clauses.

**Definition 4.2** An $S(H)$-indexed family $R$ of relations $R_s$ over $TERM(H)$ is an implicational relation on $GT(H)$ iff: For every pair $(u, v)$ of nodes in $TERM(H)^2$:

1. If $u = v \in H$, then $uR_s v$ for each sort $s$ such that $u$ and $v$ are of sort $s$.
2. If $u = v$ is the head of a clause $u = v : - u_1 = v_1, \ldots, u_n = v_n$ in $H$, and for every $j$, $1 \leq j \leq n$, there exists a sort $w_j$ such that $u_j$ and $v_j$ are of sort $w_j$ and $u_jR_{w_j} v_j$, then $uR_s v$.

The following result is well known, (for instance, see Van Emden and Kowalski, [16], or Apt and Van Emden, [1], page 845) but a simple proof is worth mentioning.

**Lemma 4.2** Given a set $H$ of equational ground Horn clauses, given any $S(H)$-indexed family $R$ of relations on $TERM(H)$, there is a smallest implicational relation $\hat{\Im}R$ on the graph $GT(H)$ containing $R$. The relation $\hat{\Im}R$ is called the implicational closure of $R$ on $GT(H)$.

**Proof:** We define the sequence $R^i$ of $S(H)$-indexed families of relations inductively as follows:

for every sort $s \in S(H)$, for every $i \geq 0$,

$$R_s^0 = R_s \cup \{(u, v) \in TERM(H)_s^2 \mid u = v \in H\},$$

$$R_s^{i+1} = R_s^i \cup \{(u, v) \in TERM(H)_s^2 \mid$$

there is some clause $u = v : - u_1 = v_1, \ldots, u_n = v_n$ in $H$, such that, $u_jR_{w_j} v_j$, for some sort $w_j$, $1 \leq j \leq n \}.$

Let $(\hat{\Im}R)_s = \bigcup_{i \geq 0} R_s^i$. As in the previous proof, it is easily shown that $\hat{\Im}R$ is the implicational closure of $R$. 

Since $GT(H)$ is finite, there is a least integer $i$ such that $R^i = R^{i+1}$. Hence, the implicational closure $\hat{\Im}R$ of $R$ is computable.

Note that $\hat{\Im}R$ is not necessarily an equivalence relation, but this does not matter because we are going to interleave implicational closure steps, and equational congruence closure steps. Also notice that $\hat{\Im}R$ is an order-sorted relation.

4.3 Order-sorted Congruence Closure For Horn Clauses

The idea is to interleave steps in which the implicational closure is computed, and steps in which the equational order-sorted congruence closure is computed.
Theorem 4.3 Given a set $H$ of equational ground Horn clauses, given any $S(H)$-indexed family $R$ of relations on $TERM(\bar{H})$, there is a smallest order-sorted congruence closure $\leftrightarrow_R$ on the graph $GT(H)$ containing $R$.

Proof: We define the sequence $R^i$ of $S(H)$-indexed families of relations inductively as follows: For every sort $s \in S(H)$, for every $j \geq 0$,

$$R_s^0 = R_s,$$
$$R_s^{2j+1} = \overset{*}{\cup} R_s^j,$$
$$R_s^{2j+2} = \overset{*}{=} R_s^{2j+1}.$$

Let $(\leftrightarrow_R)_s = \bigcup_{i\geq 0} R_s^i$. Since the graph $GT(H)$ is finite, there is some integer $i \geq 2$ such that $R^i = R_i^{i+1}$. If $i = 2j$, since $R_s^{2j+1} = \overset{*}{\cup} R_s^j$ and $j \geq 1$, then $R_s^{2j}$ is an equational order-sorted congruence, and $R_s^{2j+1}$ is an order-sorted congruence on $GT(H)$. If $i = 2j + 1$, since $R_s^{2j+2} = \overset{*}{=} R_s^{2j+1}$ and $j \geq 1$, then $R_s^{2j+1}$ is an implicational order-sorted relation, and $R_s^{2j+2}$ is an order-sorted congruence on $GT(H)$. It can also easily be shown by induction that any order-sorted congruence on $GT(H)$ containing $R$ contains every $R^i$. Hence, $\leftrightarrow_R$ is the order-sorted congruence closure of $R$ on $GT(H)$.

4.4 A more efficient Order-sorted Graph Congruence closure

There is an aspect of the method described above that makes it somehow unnecessarily computationally expensive: it computes the whole family of relations $R_s$. Within a given connected component it is only necessary to compute the $R_t$ for $t$ the top sort of that component since the order-sortedness of the congruence forces the congruences on the lower sorts to hold. If the signature is coherent, as it is in our case, one can definitely drop the subscript from the congruence. Our discussion on top algebras in section 2.9 can be adapted to graph congruences. As a consequence, one can construct a many-sorted congruence on the top sorts which then naturally extends to an order-sorted congruence when taking the rest of the sorts in consideration. For the purpose of our paper however, it is not even necessary to compute this extension, since by virtue of the signature being coherent, one does not need to differentiate between different components of the same congruence.

The methods for computing the order-sorted graph congruence closure in [2] work in a bottom up fashion disregarding the sorts of the terms (it assumes that every term in $H$ is well typed). Hence they yield a graph congruence closure which has the lower sorts property. Thus the algorithm described there computes the order-sorted graph congruence closure in $O(n^2)$. 
5 Conclusion

We have shown that congruence closure extends to finite sets of ground order-sorted equational Horn clauses. We have also proved that congruence closure is sound and complete for showing the unsatisfiability of sets of ground order-sorted equational Horn clauses (for coherent signatures). As a consequence, adapting results from Gallier [2], an unsatisfiability algorithm running in $O(n^2)$ has been obtained. The proof that the method is complete is surprisingly nontrivial and, as a by-product, it yields an interesting characterization of the least order-sorted congruence containing a relation $R$. Elsewhere, we have shown that congruence closure plays a crucial role in generalizing Andrews's method of matings to first-order languages with equality (Gallier, Raatz, Snyder [4]).

We are hoping that the congruence closure algorithm for order-sorted algebras can be used in a similar way for order-sorted logic.

References


