G22.3033-003 Logic and Verification

Spring 2004

Lecture 12
Review

- Gröbner bases
Outline

- Real Algebra
- Combining Decision Procedures

Sources:

Harrison, John. *Introduction to Logic and Automated Theorem Proving*. Unpublished manuscript. Used by permission.


Real Algebra

Our final decision procedure for arithmetic is for the theory of real numbers with addition and multiplication.

In fact, this is a special case of a more general decision procedure for real closed fields.

Real closed fields are axiomatized by the field axioms plus the following additional axioms:

**Ordered field axioms**

- $\forall x y. x = y \lor x < y \lor y < x$
- $\forall x y z. x < y \lor y < z \rightarrow x < z$
- $\forall x. x \not< x$
- $\forall y z. y < z \rightarrow \forall x. x + y < x + z$
- $\forall x y. 0 < x \land 0 < y \rightarrow 0 < xy$
Real Algebra

Real-closed axioms

- $\forall x. x \geq 0 \rightarrow \exists y. x = y^2$
- for each odd $n$:

  $$\forall a_0 \ldots a_n. a_n \neq 0 \rightarrow \exists x. a_n x^n + \cdots + a_1 x + a_0 = 0$$

Clearly, the real numbers with their standard operations are a model of these axioms.

In the following, we will typically appeal directly to properties of the reals rather than these axioms.

With a bit of work, our approach can be generalized to arbitrary real closed fields.

Decidability was first shown by Tarski in 1951. Subsequent decision procedures were proposed by Seidenberg in 1954, Cohen in 1969, Collins in 1976, Kreisel and Krivine in 1971, and Hörmander in 1983.

Collins’ Cylindrical Algebraic Decomposition (CAD) is probably the most efficient.

We will follow Hörmander’s approach (based on a manuscript by Cohen). This approach is simpler, but still relatively efficient.
Real Algebra

Why not use same approach as with complex numbers?

Recall that a crucial step in the decision procedure for complex numbers was to consider a formula of the form:

$$\forall x. p(x) = 0 \rightarrow q(x) = 0,$$

and rewrite it as $p(x)|a_0q(x)^n$, where $a_0$ is the leading coefficient of $p(x)$ and $n$ is the degree of $p(x)$.

However, in real closed fields, this is no longer true. Consider the formula:

$$\forall x. x^2 + 1 = 0 \rightarrow x + 2 = 0.$$

This formula is valid, yet there is no simple divisibility relationship between the two polynomials.

Instead, we will use facts from real analysis. As noted, more work would be required to show that these facts are derivable from the real closed field axioms.
Real Algebra

Sign Matrices

A key component of the algorithm is a procedure to obtain a sign matrix for a set of polynomials.

A sign matrix is a division of the real line into an ordered sequence of $m$ points $x_1 < x_2 < \cdots < x_m$ representing precisely the zeros of the polynomials:

1. Each column of the matrix is labeled with one of the polynomials.

2. Each row is labeled by either a point or an interval between two consecutive points. There are two additional rows for the intervals $(-\infty, x_1)$ and $(x_m, +\infty)$.

3. Each entry in the matrix is either $+$, $-$, or $0$, corresponding to whether the polynomial for the current column is positive, negative, or equal to zero for the point or interval corresponding to the current row.
Consider the two polynomials:

\[ p_1(x) = x^2 - 3x + 2 \]
\[ p_2(x) = 2x - 3. \]

The sign matrix is:

<table>
<thead>
<tr>
<th>Point/Interval</th>
<th>( p_1 )</th>
<th>( p_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>((-\infty, x_1))</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>(x_1)</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>((x_1, x_2))</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>(x_2)</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>((x_2, x_3))</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>(x_3)</td>
<td>0</td>
<td>+</td>
</tr>
<tr>
<td>((x_3, +\infty))</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

Notice that in this case we know \( x_1 = 1 \), \( x_2 = 1.5 \), and \( x_3 = 2 \). However, the sign matrix does not contain this information.
Real Algebra

As usual, our goal is to eliminate an existential quantifier from a formula of the form \( \exists x. \phi[x] \), where \( \phi[x] \) is quantifier-free.

Suppose that the atomic formulas of \( \phi[x] \) are all of the form:

\[
p_i(x) \circ 0,
\]

where \( \circ \) is any of the relations \( =, <, >, \leq, \geq \), and \( 1 \leq i \leq n \).

Then, if we have a correct sign matrix for \( p_1(x), \ldots, p_n(x) \), we can easily determine the truth of \( \exists x. \phi[x] \) simply by evaluating it for each row of the sign matrix.

If one of the rows makes \( \phi[x] \) true, then the formula is true. If none of the rows makes \( \phi[x] \) true, the formula is false.

For an example, we look at \textit{real.ml}. 
Real Algebra

Thus, we can eliminate quantifiers by finding the sign matrix for a set of polynomials.

A fairly simple algorithm for doing so is based on the following observation

Let \( P = \{p, p_1, \ldots, p_n \} \) be a set of polynomials. In order to find the sign matrix for \( P \), it suffices to find the sign matrix for:

\[ Q = \{p_0, p_1, \ldots, p_n, q_0, q_1, \ldots, q_n \}, \]

where \( p_0 = p' \), the derivative of \( p \), and \( q_i \) is the remainder on dividing \( p \) by \( p_i \).

Justification

Suppose we have a sign matrix for \( Q \). We can infer the sign of \( p(x_i) \) for each point \( x_i \) that is a zero of one of the polynomials in \( \{p_0, \ldots, p_n\} \) as follows.

Suppose \( p_k(x_i) = 0 \). Since \( q_k \) is the remainder of \( p \) after division by \( p_k \), we have \( p(x) = s_k(x)p_k(x) + q_k(x) \) for some \( s_k(x) \).

Now, since \( p_k(x_i) = 0 \), it follows that \( p(x_i) = q_k(x_i) \), so we can derive the sign of \( p \) at \( x_i \) from that of the corresponding \( q_k \).
Real Algebra

So far, we have a sign matrix for \( \{p_0, p_1, \ldots, p_n, q_0, q_1, \ldots, q_n\} \) and we also know the correct sign for \( p \) at every zero of any \( p_i \).

Now, we can remove the columns of the matrix corresponding to the \( q_i \)'s and the rows corresponding to points which are not zeros of any \( p_i \).

In the resulting matrix, any two adjacent rows which are both intervals must be identical (why?) and can thus be combined.

Now we have a “sign matrix” for \( \{p, p_0, p_1, \ldots, p_n\} \) which is correct except that:

1. We do not know the value of \( p \) on the intervals (only at the points), and
2. It is possible that there are zeros of \( p \) that are not represented by rows of the matrix. Notice that because \( p_0 \) is the derivative of \( p \), there can be at most one zero of \( p \) in any interval.

We can address these issues as follows. For each pair \((x_i, x_{i+1})\) of consecutive points in the matrix, consider the sign of \( p(x_i) \) and \( p(x_{i+1}) \), both of which are correctly given by the matrix.

If they have the same sign, then there cannot be a zero of \( p \) between \( x_i \) and \( x_{i+1} \), and the sign on the interval is the same as the sign at the two points.
Real Algebra

If the signs of \( p(x_i) \) and \( p(x_{i+1}) \) are different, then there must be a zero of \( p \) between the two points. In this case, we add a new point \( y \) between \( x_i \) and \( x_{i+1} \).

This effectively replaces the row labeled by \( (x_i, x_{i+1}) \) with three rows labeled by \( (x_i, y) \), \( y \), and \( (y, x_{i+1}) \).

In all columns besides the column for \( p \), the entries in these new rows will have the same value as they did for the interval \( (x_i, x_{i+1}) \).

For \( p \)'s column, the value at \( y \) is 0, the value for the interval \( (x_i, y) \) is the same as the value at \( x_i \), and the value for the interval \( (y, x_{i+1}) \) is the same as the value at \( x_{i+1} \).

We can process the external intervals, \( (-\infty, x_1) \) and \( (x_m, +\infty) \) by temporarily introducing “points” at \( -\infty \) and \( +\infty \) representing the limit of \( p \) as \( x \) becomes arbitrarily small or large.

The signs of the limit values are easily determined as follows:

- \( p(-\infty) \) will have the same sign as the leading coefficient of \( p \) if \( p \) is of even degree and the opposite sign if \( p \) is of odd degree.

- \( p(+\infty) \) has the same sign as the leading coefficient of \( p \).
Real Algebra

Equivalently, $p(-\infty)$ has the opposite sign as $p'$ on the interval $(-\infty, x_1)$ and $p(+\infty)$ has the same sign as $p'$ on the interval $(x_m, +\infty)$.

After determining the values of $p(-\infty)$ and $p(+\infty)$, we can process the external intervals $(-\infty, x_1)$ and $(x_m, +\infty)$ in the same way we handled the other intervals.

Finally, we can throw away the column for $p'$ and eliminate any rows associated with points that not zeros of any remaining polynomial (including the temporary rows for $+\infty$ and $-\infty$), condensing the enclosing interval rows as before.

We are left with a complete and correct sign matrix for $P = \{p, p_1, \ldots, p_n\}$. □

We can apply this procedure recursively. The base case is determining the sign matrix for a set of constant polynomials which is trivial.

We can see an example in real.ml.
Real Algebra

Multivariate polynomials

As with the complex numbers, we can use essentially the same procedure for multivariate polynomials.

The only complication is that when dividing polynomials, we have to use pseudo-division to get:

\[ a^k s(x) = q(x)p(x) + r(x). \]

The result is that instead of inferring the sign of \( s(x) \) directly from \( r(x) \), we must also know the sign of \( a \).

In addition, we must know the sign of the coefficients of the current polynomial which may involve other variables.

Thus, the extension to the multivariate case requires a number of additional case-splits to fix the signs of the coefficients.

We will look at a few more examples in \textit{real.ml}. 
Combining Decision Procedures

Often, verification conditions are expressed in a language which mixes several theories.

A natural question is whether one can use decision procedures for individual theories to construct a decision procedure for the union theory.

More precisely, suppose that $\Sigma_1, \ldots, \Sigma_n$ are $n$ signatures, and for $i = 1, \ldots, n$, let $T_i$ be a $\Sigma_i$-theory.

Then, let $Sat_i$ be a decision procedure for deciding the $T_i$-satisfiability of $\Sigma_i$-formulas.

How can we use these to construct a decision procedure for the $T$-satisfiability of $\Sigma$-formulas, where $T = Cn \cup T_i$ and $\Sigma = \bigcup \Sigma_i$. 
The Nelson-Oppen Method

A very general method for combining decision procedures is the *Nelson-Oppen* method.

This method is applicable when

1. The signatures $\Sigma_i$ are disjoint.

2. The theories $T_i$ are stably-infinite.
   
   A $\Sigma$-theory $T$ is *stably-infinite* if every $T$-satisfiable quantifier-free $\Sigma$-formula is satisfiable in an infinite model.

3. The formulas to be tested for satisfiability are quantifier-free.

In practice, only the third requirement is a significant restriction.

We may also restrict our attention to conjunctions of literals.

This is because any quantifier-free formula can be put into disjunctive normal form. It then suffices to check the satisfiability of each conjunction.
The Nelson-Oppen Method

Before explaining the procedure in detail, we need the following definitions.

1. For \( i = 1, \ldots, n \), a member of \( \Sigma_i \) is an \( i \)-symbol.

2. A \( \Sigma \)-term \( t \) is an \( i \)-term if it is a variable, a constant \( i \)-symbol, or the application of a functional \( i \)-symbol.

3. An \( i \)-predicate is an application of a predicate \( i \)-symbol.

4. An atomic \( i \)-formula is an \( i \)-predicate or an equation whose left hand side is an \( i \)-term (for equations whose left-hand-sides are variables, we arbitrarily choose a theory \( T_i \) to associate with each variable).

5. An \( i \)-literal is an atomic \( i \)-formula or the negation of an atomic \( i \)-formula.

6. An occurrence of a term \( t \) in either a term or a formula is \( i \)-alien if \( t \) is a \( j \)-term with \( i \neq j \) and all of its super-terms (if any) are \( i \)-terms.

7. An \( i \)-term or \( i \)-literal is pure if it contains only \( i \)-symbols.
The Nelson-Oppen Method

Now we can explain step one of the Nelson-Oppen method:

1. **Conversion to Separate Form**

Given a conjunction of literals, \( \phi \), we desire to convert it into a *separate form*: a \( T \)-equisatisfiable conjunction of literals \( \phi_1 \land \phi_2 \land \ldots \land \phi_n \), where each \( \phi_i \) is a \( \Sigma_i \)-formula.

The following algorithm accomplishes this.

1. Let \( \psi \) be some \( i \)-literal in \( \phi \).

2. If \( \psi \) is a pure \( i \)-literal, for some \( i \), remove \( \psi \) from \( \phi \) and add \( \psi \) to \( \phi_i \); if \( \phi \) is empty then stop; otherwise goto step 1.

3. Let \( t \) be an \( i \)-alien term in \( \psi \). Replace \( t \) in \( \phi \) with a new variable \( z \) associated with theory \( T_i \), and add \( z = t \) to \( \phi \). Goto step 1.
The Nelson-Oppen Method

It is easy to see that $\phi$ is $T$-satisfiable iff $\phi_1 \land \ldots \land \phi_n$ is $T$-satisfiable.

Furthermore, because each $\phi_i$ is a $\Sigma_i$-formula, we can run $Sat_i$ on each $\phi_i$.

Clearly, if $Sat_i$ reports that any $\phi_i$ is unsatisfiable, then $\phi$ is unsatisfiable.

But the converse is not true in general.

We need a way for the decision procedures to communicate with each other about shared variables.

First a definition: If $S$ is a set of terms and $\sim$ is an equivalence relation on $S$, then the arrangement of $S$ induced by $\sim$ is $Ar_\sim = \{ x = y \mid x \sim y \} \cup \{ x \neq y \mid x \not\sim y \}$.
The Nelson-Oppen Method

Suppose that $T_1$ and $T_2$ are theories with disjoint signatures $\Sigma_1$ and $\Sigma_2$ respectively. Let $T = Cn \bigcup T_i$ and $\Sigma = \bigcup \Sigma_i$. Given a $\Sigma$-formula $\phi$ and decision procedures $Sat_1$ and $Sat_2$ for $T_1$ and $T_2$ respectively, we wish to determine if $\phi$ is $T$-satisfiable. The non-deterministic Nelson-Oppen algorithm for this is as follows:

1. Convert $\phi$ to its separate form $\phi_1 \land \phi_2$.

2. Let $\Lambda$ be the set of variables shared between $\phi_1$ and $\phi_2$. Guess an equivalence relation $\sim$ on $\Lambda$.

3. Run $Sat_1$ on $\phi_1 \cup Ar_\sim$.

4. Run $Sat_2$ on $\phi_2 \cup Ar_\sim$.

If there exists an equivalence relation $\sim$ such that both $Sat_1$ and $Sat_2$ succeed, then we claim that $\phi$ is $T$-satisfiable.

If no such equivalence relation exists, then we claim that $\phi$ is $t$-unsatisfiable.

The generalization to more than two theories is straightforward.
Example

Consider the combination of the theory $T_Z$ with the theory $T_\varepsilon$ of equality.

Let $\phi = 1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$.

Is this satisfiable?
Example

Consider the combination of the theory $T_Z$ with the theory $T_E$ of equality.

Let $\phi = 1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$.

Is this satisfiable? **No.**
Example

Consider the combination of the theory $T_Z$ with the theory $T_E$ of equality.

Let $\phi = 1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$.

Is this satisfiable? **No.**

To determine this using the above algorithm, we first convert $\phi$ to a separate form:

\[
\begin{align*}
\phi_Z &= 1 \leq x \land x \leq 2 \land y = 1 \land z = 2 \\
\phi_E &= f(x) \neq f(y) \land f(x) \neq f(z)
\end{align*}
\]

Now, the shared variables are $\{x, y, z\}$. There are 5 possible arrangements based on equivalence classes of $x$, $y$, and $z$:

1. $\{x = y, x = z, y = z\}$
2. $\{x = y, x \neq z, y \neq z\}$
3. $\{x \neq y, x = z, y \neq z\}$
4. $\{x \neq y, x \neq z, y = z\}$
5. $\{x \neq y, x \neq z, y \neq z\}$
Example

Consider the combination of the theory $T_Z$ with the theory $T_E$ of equality.

Let $\phi = 1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$.

Is this satisfiable? No.

To determine this using the above algorithm, we first convert $\phi$ to a separate form:

$$\phi_Z = 1 \leq x \land x \leq 2 \land y = 1 \land z = 2$$
$$\phi_E = f(x) \neq f(y) \land f(x) \neq f(z)$$

Now, the shared variables are $\{x, y, z\}$. There are 5 possible arrangements based on equivalence classes of $x, y, z$:

1. $\{x = y, x = z, y = z\}$: inconsistent with $\phi_E$.
2. $\{x = y, x \neq z, y \neq z\}$
3. $\{x \neq y, x = z, y \neq z\}$
4. $\{x \neq y, x \neq z, y = z\}$
5. $\{x \neq y, x \neq z, y \neq z\}$
Example

Consider the combination of the theory $T_Z$ with the theory $T_\mathcal{E}$ of equality.

Let $\phi = 1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$.

Is this satisfiable? No.

To determine this using the above algorithm, we first convert $\phi$ to a separate form:

\[
\phi_Z = 1 \leq x \land x \leq 2 \land y = 1 \land z = 2 \\
\phi_\mathcal{E} = f(x) \neq f(y) \land f(x) \neq f(z)
\]

Now, the shared variables are $\{x, y, z\}$. There are 5 possible arrangements based on equivalence classes of $x$, $y$, and $z$:

1. $\{x = y, x = z, y = z\}$: inconsistent with $\phi_\mathcal{E}$.
2. $\{x = y, x \neq z, y \neq z\}$: inconsistent with $\phi_\mathcal{E}$.
3. $\{x \neq y, x = z, y \neq z\}$
4. $\{x \neq y, x \neq z, y = z\}$
5. $\{x \neq y, x \neq z, y \neq z\}$
Example

Consider the combination of the theory $T_Z$ with the theory $T_E$ of equality.

Let $\phi = 1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$.

Is this satisfiable? **No.**

To determine this using the above algorithm, we first convert $\phi$ to a separate form:

$$\phi_Z = 1 \leq x \land x \leq 2 \land y = 1 \land z = 2$$
$$\phi_E = f(x) \neq f(y) \land f(x) \neq f(z)$$

Now, the shared variables are $\{x, y, z\}$. There are 5 possible arrangements based on equivalence classes of $x$, $y$, and $z$:

1. $\{x = y, x = z, y = z\}$: inconsistent with $\phi_E$.
2. $\{x = y, x \neq z, y \neq z\}$: inconsistent with $\phi_E$.
3. $\{x \neq y, x = z, y \neq z\}$: inconsistent with $\phi_E$.
4. $\{x \neq y, x \neq z, y = z\}$
5. $\{x \neq y, x \neq z, y \neq z\}$
Example

Consider the combination of the theory $T_Z$ with the theory $T_E$ of equality.

Let $\phi = 1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$.

Is this satisfiable? **No.**

To determine this using the above algorithm, we first convert $\phi$ to a separate form:

$$
\phi_Z = 1 \leq x \land x \leq 2 \land y = 1 \land z = 2 \\
\phi_E = f(x) \neq f(y) \land f(x) \neq f(z)
$$

Now, the shared variables are $\{x, y, z\}$. There are 5 possible arrangements based on equivalence classes of $x$, $y$, and $z$:

1. $\{x = y, x = z, y = z\}$: inconsistent with $\phi_E$.
2. $\{x = y, x \neq z, y \neq z\}$: inconsistent with $\phi_E$.
3. $\{x \neq y, x = z, y \neq z\}$: inconsistent with $\phi_E$.
4. $\{x \neq y, x \neq z, y = z\}$: inconsistent with $\phi_Z$.
5. $\{x \neq y, x \neq z, y \neq z\}$
Example

Consider the combination of the theory $T_Z$ with the theory $T_\mathcal{E}$ of equality.

Let $\phi = 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$.

Is this satisfiable? No.

To determine this using the above algorithm, we first convert $\phi$ to a separate form:

$$\phi_Z = 1 \leq x \wedge x \leq 2 \wedge y = 1 \wedge z = 2$$
$$\phi_\mathcal{E} = f(x) \neq f(y) \wedge f(x) \neq f(z)$$

Now, the shared variables are $\{x, y, z\}$. There are 5 possible arrangements based on equivalence classes of $x, y,$ and $z$:

1. $\{x = y, x = z, y = z\}$: inconsistent with $\phi_\mathcal{E}$.
2. $\{x = y, x \neq z, y \neq z\}$: inconsistent with $\phi_\mathcal{E}$.
3. $\{x \neq y, x = z, y \neq z\}$: inconsistent with $\phi_\mathcal{E}$.
4. $\{x \neq y, x \neq z, y = z\}$: inconsistent with $\phi_Z$.
5. $\{x \neq y, x \neq z, y \neq z\}$: inconsistent with $\phi_Z$. 

21-g
Example

Consider the combination of the theory $T_Z$ with the theory $T_E$ of equality.

Let $\phi = 1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$.

Is this satisfiable? **No.**

To determine this using the above algorithm, we first convert $\phi$ to a separate form:

$\phi_Z = 1 \leq x \land x \leq 2 \land y = 1 \land z = 2$

$\phi_E = f(x) \neq f(y) \land f(x) \neq f(z)$

Now, the shared variables are $\{x, y, z\}$. There are 5 possible arrangements based on equivalence classes of $x, y, \text{ and } z$:

1. $\{x = y, x = z, y = z\}$: inconsistent with $\phi_E$.
2. $\{x = y, x \neq z, y \neq z\}$: inconsistent with $\phi_E$.
3. $\{x \neq y, x = z, y \neq z\}$: inconsistent with $\phi_E$.
4. $\{x \neq y, x \neq z, y = z\}$: inconsistent with $\phi_Z$.
5. $\{x \neq y, x \neq z, y \neq z\}$: inconsistent with $\phi_Z$.

We will look at this same example in *combining.ml*. 
Correctness of Nelson-Oppen

We define an *interpretation* of a signature $\Sigma$ to be a model of $\Sigma$ together with a variable assignment.

Two interpretations $A$ and $B$ are *isomorphic* if there exists an isomorphism $h$ of the model of $A$ into the model of $B$ and $h(x^A) = x^B$ for each variable $x$ (where $x^A$ signifies the value assigned to $x$ by the variable assignment of $A$).

We furthermore define $A^{\Sigma,V}$ to be the restriction of $A$ to the symbols in $\Sigma$ and the variables in $V$.

**Theorem**

Let $\Sigma_1$ and $\Sigma_2$ be signatures, and for $i = 1, 2$, let $\phi_i$ be a set of $\Sigma_i$-formulas, and $V_i$ the set of variables appearing in $\phi_i$. Then $\phi_1 \cup \phi_2$ is satisfiable iff there exists a $\Sigma_1$-interpretation $A$ satisfying $\phi_1$ and a $\Sigma_2$-interpretation $B$ satisfying $\phi_2$ such that:

$$A^{\Sigma_1 \cap \Sigma_2, V_1 \cap V_2} \text{ is isomorphic to } B^{\Sigma_1 \cap \Sigma_2, V_1 \cap V_2}.$$
Correctness of Nelson-Oppen

Proof

Let $\Sigma = \Sigma_1 \cap \Sigma_2$ and $V = V_1 \cap V_2$.

Suppose $\phi_1 \cup \phi_2$ is satisfiable. Let $M$ be an interpretation satisfying $\phi_1 \cup \phi_2$. If we let $A = M^{\Sigma_1;V_1}$ and $B = M^{\Sigma_2;V_2}$, then clearly

- $A \models \phi_1$
- $B \models \phi_2$
- $A^{\Sigma;V}$ is isomorphic to $B^{\Sigma;V}$

On the other hand, suppose that we have $A$ and $B$ satisfying the three conditions listed above. Let $h$ be an isomorphism from $A^{\Sigma;V}$ to $B^{\Sigma;V}$.

We define an interpretation $M$ as follows:

- $\text{dom}(M) = \text{dom}(A)$
- For each variable or constant $u$, $u^M = \begin{cases} u^A & \text{if } u \in (\Sigma_1^C \cup V_1) \\ h^{-1}(u^B) & \text{otherwise} \end{cases}$
Correctness of Nelson-Oppen

- For function symbols of arity $n$,
  $$f^M(a_1, \ldots, a_n) = \begin{cases} f^A(a_1, \ldots, a_n) & \text{if } f \in \Sigma_1^F \\ h^{-1}(f^B(h(a_1), \ldots, h(a_n))) & \text{otherwise} \end{cases}$$

- For predicate symbols of arity $n$,
  $$(a_1, \ldots, a_n) \in P^M \iff (a_1, \ldots, a_n) \in P^A \text{ if } P \in \Sigma_1^P$$
  $$(a_1, \ldots, a_n) \in P^M \iff (h(a_1), \ldots, h(a_n)) \in P^B \text{ otherwise}$$

By construction, $M_{\Sigma_1, V_1}$ is isomorphic to $A$. In addition, it is easy to verify that $h$ is an isomorphism of $M_{\Sigma_2, V_2}$ to $B$.

It follows by the homomorphism theorem that $M$ satisfies $\phi_1 \cup \phi_2$.  

$\square$
Correctness of Nelson-Oppen

Theorem

Let $\Sigma_1$ and $\Sigma_2$ be signatures, with $\Sigma_1 \cap \Sigma_2 = \emptyset$, and for $i = 1, 2$, let $\phi_i$ be a set of $\Sigma_i$-formulas, and $V_i$ the set of variables appearing in $\phi_i$. As before, let $V = V_1 \cap V_2$. Then $\phi_1 \cup \phi_2$ is satisfiable iff there exists an interpretation $A$ satisfying $\phi_1$ and an interpretation $B$ satisfying $\phi_2$ such that:

1. $|A| = |B|$, and

2. $x^A = y^A$ iff $x^B = y^B$ for every pair of variables $x, y \in V$.

Proof

Clearly, if $\phi_1 \cup \phi_2$ is satisfiable in some interpretation $M$, then the only if direction holds by letting $A = M$ and $B = M$.

Consider the converse. Let $h : V^A \to V^B$ be defined as $h(x^A) = x^B$. This definition is well-formed by property 2 above.

In fact, $h$ is bijective. To show that $h$ is injective, let $h(a_1) = h(a_2)$. Then there exist variables $x, y \in V$ such that $a_1 = x^A$, $a_2 = y^A$, and $x^B = y^B$. By property 2, $x^A = y^A$, and therefore $a_1 = a_2$. 
Correctness of Nelson-Oppen

To show that $h$ is surjective, let $b \in V^B$. Then there exists a variable $x \in V^B$ such that $x^B = b$. But then $h(x^A) = b$.

Since $h$ is bijective, it follows that $|V^A| = |V^B|$, and since $|A| = |B|$, we also have that $|A - V^A| = |B - V^B|$. We can therefore extend $h$ to a bijective function $h'$ from $A$ to $B$.

By construction, $h'$ is an isomorphism of $A^V$ to $B^V$. Thus, by the previous theorem, we can obtain an interpretation satisfying $\phi_1 \cup \phi_2$. 

$\square$
Correctness of Nelson-Oppen

We can finally prove the correctness of the nondeterministic Nelson-Oppen method.

**Theorem**

Let $T_i$ be a stably-infinite $\Sigma_i$-theory, for $i = 1, 2$, and suppose that $\Sigma_1 \cap \Sigma_2 = \emptyset$. Also, let $\phi_i$ be a set of $\Sigma_i$ literals, $i = 1, 2$, and let $\Lambda$ be the set of variables appearing in both $\phi_1$ and $\phi_2$. Then $\phi_1 \cup \phi_2$ is $T_1 \cup T_2$-satisfiable iff there exists an equivalence relation $\sim$ on $\Lambda$ such that $\phi_i \cup Ar_\sim$ is $T_i$-satisfiable, $i = 1, 2$.

**Proof**

Suppose $M$ is an interpretation satisfying $\phi_1 \cup \phi_2$. We define an equivalence relation $x \sim y$ iff $x, y \in \Lambda$ and $x^M = y^M$. By construction, $M$ is a $T_i$-interpretation satisfying $\phi_i \cup Ar_\sim$, $i = 1, 2$. 


Correctness of Nelson-Oppen

Suppose on the other hand that there exists an equivalence relation $\sim$ of $\Lambda$ such that $\phi_i \cup Ar_\sim$ is $T_i$-satisfiable, $i = 1, 2$. Since $T_1$ is stably-infinite, there is an infinite interpretation $A$ satisfying $\phi_1 \cup Ar_\sim$. Similarly, there is an infinite interpretation $B$ satisfying $\phi_2 \cup Ar_\sim$.

But by LST, we can take the least upper bound of $|A|$ and $|B|$ and obtain interpretations of that cardinality.

Then we have $|A| = |B|$ and $x^A = y^A$ iff $x^B = y^B$ for every variable $x, y \in \Lambda$. We can thus apply the previous theorem and obtain the existence of a $(\Sigma_1 \cup \Sigma_2)$-interpretation satisfying $\phi_1 \cup \phi_2$. 

\[\Box\]