Example Application: Translation Validation

Combining Decision Procedures
Source: Enderton, 3.0 - 3.2.

- Presburger Arithmetic
- Natural Numbers with Successor and Less-Than
- Natural Numbers with Successor
- Number Theory
Number Theory

With a general understanding of first-order languages and theories, we now focus on a specific language, the language of number theory.

Number theory is the set of all sentences in this language which are true in $\mathbb{N}$.

We denote this theory $Th(N)$. Let $N$ be the intended model of this language: the set of natural numbers.

The parameters are $0, S, +, \cdot, \geq$.

The parameters are $0, S, +, \cdot, \geq$.
Reducts of Number Theory

Besides considering the model $\mathcal{N}$, we also consider the following reducts which are restrictions to sublanguages:

- $\mathcal{N}_S = (\mathbb{N}; 0; S)$
- $\mathcal{N}_L = (\mathbb{N}; 0; S; <)$
- $\mathcal{N}_A = (\mathbb{N}; 0; S; <; +)$
- $\mathcal{N}_M = (\mathbb{N}; 0; S; <; +; \cdot)$

We consider the following questions for each model:

- What do the nonstandard models of the theory look like?
- What subsets of $\mathbb{N}$ are definable in the model?
- Is it finitely axiomatizable?
- If so, how can the theory be axiomatized?
- Is the theory of this model decidable?

We consider the following sentences for each model:

1. $$(\times, +, \cdot, S, 0, \mathcal{N}) = \mathcal{N}$$
2. $$(+, \cdot, S, 0, \mathcal{N}) = \mathcal{V}_N$$
3. $$(S, 0, \mathcal{N}) = \mathcal{T}_N$$
4. $$(S, 0, \mathcal{N}) = \mathcal{S}_N$$

Besides considering the model $\mathcal{N}$, we also consider the reducts which are restrictions to sublanguages.
This term is called the \textit{numeral} for \( k \).

For each natural number \( k \), we denote the associated term by \( S^k_0 \).

We will use infix notation: \( x \ y \) instead of \( x y \) etc.

\textbf{Notation}
Consider the theory $Th_{SN}^S$. What are some of its sentences?

1. $S_{\mathbb{N}}'$
2. $(S \cdot 0, S_{\mathbb{N}})$
3. $(S \cdot x = y, y \neq 0)$
4. $S_{\mathbb{N}}'(x, S_{\mathbb{N}}')$

Let $A$ be the above set of sentences (including $S_{\mathbb{N}}'$ for each $n$).
Let $\mathcal{A}^S$ be the above set of sentences (including $S4.1$ for each $n$).

\[
\begin{align*}
S4.1 & \quad x \neq x \cdot \\
S4.2 & \quad x \neq x \cdot \\
S4.3 & \quad (xS = \bar{h} x \cdot [x \cdot 0 \neq \bar{h}]) \cdot [x \cdot A \cdot x]
\end{align*}
\]

Consider the theory $Th_N$. What are some of its sentences?

\[
(S^N \cdot 0) = \mathcal{S}_N
\]

We begin with the simplest reduct:

**Natural Numbers with Successor**
Now consider the set $A^S$. What does an arbitrary model of $A^S$ look like?

Such an element must be part of a $Z$-chain:

Thus, a model of $A^S$ contains the standard points and $0$ or more $Z$-chains.
Natural Numbers with Successor

Now, consider the set $A_S$.

What does an arbitrary model of $A_S$ look like?

Now, consider the set $A_S$.

\[ \cdots \leftarrow (a_0)_S \leftarrow (a_0)_S \leftarrow (a_0)_S \leftarrow a_0 \]

must contain the standard points:

\[ \mathbb{N} \]
Natural Numbers with Successor

Now consider the set $A_S$.

What does an arbitrary model of $A_S$ look like?

Consider the set $S_A$.

Can contain an element $a$ which is not among the standard points?

\[ \ldots \leftarrow ( (N 0)_N S)_N S \leftarrow (N 0)_N S \leftarrow N 0 \]

Thus, a model of $A_S$ contains the standard points and $0$ or more $S_A$-chains.
Natural Numbers with Successor

Now, consider the set $A_S$. What does an arbitrary model $M$ of $A_S$ look like?

$M$ must contain the standard points: $\mathbb{Z}$.

Can $M$ contain an element $a$ which is not among the standard points?

\[ \cdots \leftarrow ((a)_M S)_M S \leftarrow (a)_M S \leftarrow a \leftarrow \circ \leftarrow \circ \cdots \]

Such an element must be part of a $\mathbb{Z}$-chain:

What does an arbitrary model of $A_M$ look like?

Now, consider the set $A_S$. 

**Natural Numbers with Successor**
Thus, a model of $S \forall$ contains the standard points and $\mathbb{Z}$-chains.

$$\cdots \leftarrow ((\forall)_{\mathbb{W}} S)_{\mathbb{W}} S \leftarrow (\forall)_{\mathbb{W}} S \leftarrow a \leftarrow 0 \leftarrow 0 \cdots$$

Such an element must be part of a $\mathbb{Z}$-chain.

Can contain an element $a$ which is not among the standard points?

$$\cdots \leftarrow ((\forall 0)_{\mathbb{W}} S)_{\mathbb{W}} S \leftarrow (\forall 0)_{\mathbb{W}} S \leftarrow \mathbb{W} 0$$

must contain the standard points.

What does an arbitrary model of $\mathbb{W}$ look like?

Now, consider the set $S \forall$.

---

Natural Numbers with Successor
Theorem

If \( M \) and \( M_0 \) are models of \( S \) having the same number of \( Z \)-chains, then they are isomorphic.

Proof

Clearly, there is an isomorphism between the standard parts of \( M \) and \( M_0 \). Since they have the same number of \( Z \)-chains, we can extend this isomorphism to map each \( Z \)-chain of \( M \) to a \( Z \)-chain of \( M_0 \). Therefore, \( M \) and \( M_0 \) are isomorphic.

Theorem

\( Cn \) is \( \lambda \)-categorical for any uncountable cardinal \( \lambda \).

Proof

Recall that a theory is \( \lambda \)-categorical if all models of cardinality \( \lambda \) are isomorphic. Since the standard part of a model of \( S \) only contributes a countably infinite number of elements, a model of \( S \) of cardinality \( \lambda \) must have a different number of elements, so a model of \( S \) of cardinality \( \lambda \) cannot have the same number of \( Z \)-chains. Therefore, any two such models are isomorphic.
Furthermore, \( CN_{AS} \) has no finite models. Therefore \( CN_{AS} \) is complete.

By the previous theorem, \( CN_{AS} \) is \( \kappa \)-categorical for any uncountable cardinal \( \kappa \).

Then \( \mathcal{L} \) is complete.

All models of \( \mathcal{L} \) are infinite.

Let \( \mathcal{L} \) be a theory in a countable language such that

Recall the Los-Vaught test:

**Proof**

\( CN_{AS} \) is a complete theory.

**Theorem**

**Natural Numbers with Successor**
Any complete and axiomatizable theory is decidable. \( \forall S \in \mathbb{A} \) is a decidable set of axioms for this theory.

**Proof**

\( \text{Th}_{\mathbb{N}} S \) is decidable.

**Corollary**

We know that \( \text{cn} \subseteq \text{Th}_{\mathbb{N}} S \). The first theory is complete, and the second is satisfiable. Therefore, the theories must be equal. (Why?)

\( \text{cn} \subseteq \text{Th}_{\mathbb{N}} S \).

**Proof**

\( \text{cn} \subseteq \text{Th}_{\mathbb{N}} S \).

**Corollary**

\( \text{cn} \subseteq \text{Th}_{\mathbb{N}} S \).

Natural Numbers with Successor
Elimination of Quantifiers

Once one knows that a theory is decidable, the next question is how to find an effective procedure for deciding it.

A common technique for providing decision procedures is the method of elimination of quantifiers.

A theory \( L \) admits elimination of quantifiers if for every quantifier-free formula \( \phi \) there is a quantifier formula \( \phi \) such that

\[
(\phi \leftrightarrow \phi) \models L
\]

Theorem

The following theorem reduces the quantifier elimination problem to a particular special case.

Assume that for every formula of the form

\[
\forall x (\exists a \exists \cdots \exists x \forall \exists \cdot \cdot \cdot \forall x (x \in L \phi)
\]

where each \( i \) is a literal, there is a quantifier-free formula such that

Then

\( L \) admits elimination of quantifiers.

A theory \( L \) admits elimination of quantifiers if for every formula \( \phi \) there is a quantifier-free formula such that

\( \phi \leftrightarrow \phi \) models \( L \).

A theory \( L \) admits elimination of quantifiers if for every formula \( \phi \) there is a quantifier-free formula such that

\( \phi \leftrightarrow \phi \) models \( L \).

Once one knows that a theory is decidable, the next question is how to find an effective procedure for deciding it.

Elimination of Quantifiers
The proof is by induction on formulas. Clearly, every atomic formula is equivalent to a quantifier-free formula (issuer). Suppose that \( \varphi \) and \( \psi \) are formulas with quantifier-free equivalents \( \varphi' \) and \( \psi' \), respectively.

\[
\varphi \leftrightarrow \psi \models L
\]

\( \text{Propositional connective cases are trivial.} \)

The proof is by induction on formulas. Clearly, every atomic formula is equivalent to a quantifier-free formula (issuer). Suppose that \( \varphi \) and \( \psi \) are formulas with quantifier-free equivalents \( \varphi' \) and \( \psi' \), respectively.

\[
\varphi \leftrightarrow \psi \models L
\]

The propositional connective cases are trivial. Clearly, every atomic formula is equivalent to a quantifier-free formula (issuer). Suppose that \( \varphi \) and \( \psi \) are formulas with quantifier-free equivalents \( \varphi' \) and \( \psi' \), respectively.

\[
\varphi \leftrightarrow \psi \models L
\]

The propositional connective cases are trivial. Clearly, every atomic formula is equivalent to a quantifier-free formula (issuer). Suppose that \( \varphi \) and \( \psi \) are formulas with quantifier-free equivalents \( \varphi' \) and \( \psi' \), respectively.

\[
\varphi \leftrightarrow \psi \models L
\]
Elimination of Quantifiers

Theorem

$\mathcal{N}$ admits elimination of quantifiers.

Proof

Consider a formula $\forall x \left( \lor \cdots \lor 0 \right)$, where each $\alpha_i$ is a literal.

If $\alpha_i$ is $x$, then the equation is true if $m = n$ and false otherwise. We can use $0 = 0$ to represent true, and $0 \neq 0$ to represent false.

If $\alpha_i$ is $x$, then the equation is true if $m = n$ and false otherwise. We can use $0 = 0$ to represent true, and $0 \neq 0$ to represent false.

If $x$ does not appear in some $\alpha_i$, we can move $\alpha_i$ outside the quantifier. The remaining literals have the form $n_u S = x_u S$ or $n_u S \neq x_u S$, where $u$ is either $0$ or a variable. Each $\alpha_i$ must be an equation or disjunction between two such terms.

Note that the only possible terms in the language are $n_u S$, where $n$ is either $0$ or a variable.

Consider a formula $\forall x \left( \lor \cdots \lor 0 \right)$, where each $\alpha_i$ is a literal.

If the formula is true, then $S\mathcal{N}$ admits elimination of quantifiers.
We have
\[ n_{uw}S = \forall \exists y \exists S \text{ by } n = x_{\exists y \exists S} \]
and each \( i \) is of the form \( S_{m \exists x} = S_{n \exists u} \) or \( S_{m \exists x} \neq S_{n \exists u} \) where \( u \) is \( 0 \) or a variable other than \( x \).

We also know that each \( \forall \) is of the form \( \forall (x) \) where each \( \forall \) is \( 0 \) or a variable other than \( x \).

We have
\[ n_{uw}S = x_{uw}S \]

After processing each literal containing \( x \), the new formula does not contain \( x \), so the quantifier can be eliminated.

Suppose \( \forall x \) is an equation.

Let \( u \neq 0 \), \( u \neq t \), \( u \neq S_{m \exists x} \), \( u \neq S_{n \exists u} \)

Therefore, the new formula does not contain \( x \), so the quantifier can be eliminated.

Prove (cont.)
Finally, we can use quantifier-elimination to show that a subset of $\mathbb{N}$ is definable true or false.

This also provides an alternative proof that $C_n$ is complete, since given any sentence we can compute its quantifier-free equivalent $\overline{S}$ which must be either true or false.

An atomic sentence must be of the form $S \lor \neg S$. Thus any Boolean combination of such sentences can also be evaluated to true or false.

Free variables, so if we start with a sentence, we will finish with a sentence. Note that $T$ is a sentence because quantifier elimination does not introduce any such that $T \iff \alpha \iff S \lor \neg S$.

We can now give a decision procedure for $C_n$. Suppose we are given a sentence $\alpha$. Using quantifier elimination, we can find a quantifier-free sentence $\overline{\alpha}$. Using quantifier-elimination, we can show that $\overline{\alpha}$ is definable.
Example

Natural Numbers with Successor
\[ \forall x \exists y \left( x \neq y \land (x \neq 0 \lor y \neq 0) \right) \]
$\forall h \in (0 = h \lor 0 = x \lor h \neq x) \land h \in x \land \bot$

$\forall h \in ((0 \neq h \land 0 \neq x) \leftrightarrow h \neq x) \land h \in x \land \bot$

$\forall h \in ((0 \neq h \land 0 \neq x) \leftrightarrow h \neq x) \land h \land x \land A$

Example

Natural Numbers with Successor
Natural Numbers with Successor

Example
Natural Numbers with Successor

Example

$\forall y \neg (y \not\equiv x)$

iff

$\exists x \forall y (x \not\equiv y \lor y \equiv 0) \in \text{CnAs}$

iff

$\exists (x \not\equiv y \lor y \equiv 0) \in \text{CnAs}$

iff

$\exists x \forall y (x \not\equiv y \lor y \equiv 0) \in \text{CnAs}$

iff

$\exists x (x \not\equiv 0 \land x = 0) \in \text{CnAs}$

iff

$\exists (0 \not\equiv 0) \in \text{CnAs}$
\[\forall n \in \mathbb{N} \exists 0 = 0\]
\[\forall n \in \mathbb{N} \exists (0 \neq 0)\]
\[\forall n \in \mathbb{N} \exists (0 = x \lor 0 \neq x) x \in \mathbb{N}\]
\[\forall n \in \mathbb{N} \exists (0 = \overline{n} \lor 0 = x \lor \overline{n} \neq x) \overline{n} \in x \in \mathbb{N}\]
\[\forall n \in \mathbb{N} \exists ((0 \neq \overline{n} \land 0 \neq x) \iff \overline{n} \neq x) \overline{n} \land x \land \overline{A} \land x \land A\]
Natural Numbers with Successor and Less-Than

The ordering relation

\[ m < n \]

is not definable in \( \mathbb{N} \).

Thus, suppose we add the less-than symbol, \(<\>, to our language, and consider

\[ S \mathbb{N} \]

the standard model of first-order arithmetic.

We will show that \( T \mathbb{N} \) is decidable and admits elimination of quantifiers.

Our goal is to show that

\[ \forall x \exists y (x < y) \iff \exists z (z = x) \]

is not definable in \( \mathbb{N} \).

The ordering relation

\[ \{ u > w \mid \langle u, w \rangle \} \]

is not definable in \( \mathbb{N} \).
Our goal is to show that \( \text{Th}^L_N \in \text{Th}^L \).

\[(z > x \leftrightarrow z > \bar{n} \leftrightarrow \bar{n} > x) \in L_5 \bullet \]
\[(x \neq \bar{n} \leftrightarrow \bar{n} > x) \in L_4 \bullet \]
\[(x > \bar{n} \land \bar{n} = x \land \bar{n} > x) \in L_3 \bullet \]
\[0 \neq x \bar{n} \in L_2 \bullet \]
\[(\bar{n} > x \leftrightarrow \bar{n} > x) \in L_1 \bullet \]
\[(x S = \bar{n} x \in \bar{0} \neq \bar{n}) \in S_3 \bullet \]

Consider the following set \( A^L \) of sentences:

However, unlike \( \text{Th}^S_N \), it is not finitely axiomatizable.

We will show that \( \text{Th}^L_N \) is decidable and admits elimination of quantifiers.

The standard model \( (\text{Th}^L_N, S^L_N) = \text{Th}_N \).

Thus, we add the less-than symbol \( \text{<} \) to our language, and consider

\[\text{The ordering relation } \{ u > w | \langle u', w \rangle \text{is not definiible in } N \}.\]
Thus, a model of $\forall A W$ consists of a standard part plus 0 or more $\mathbb{Z}$-chains. In $\forall A W$, a model $M$ of $\forall A$ consists of a standard part plus 0 or more $\mathbb{Z}$-chains. In $\forall A W$, $S^4$ follows from (1), (2), and $L_5$.

$S^3$ is already in $\forall A T$. $S^1$ follows from $L_5$ and (1). $S^2$ follows from (4), $L_3$, and (2).

Recall the definition of $\forall A$:

$S^1$. $x \neq x S x \supset \forall A W$.

$S^2$. $(x S = \neg \exists x \in \mathbb{E} \iff 0 \neq \neg \exists x \in \mathbb{E} ) \neg \forall A W$.

$S^3$. $(\neg \forall A W \iff S x = x S) \forall A x \iff \forall A W$.

$S^4$. $0 \neq x S x \supset \forall A W$.

We first show that $\forall A S \subset \forall A T$.

Natural Numbers with Successor and Less-Than
The theory $\mathcal{A}L$ admits elimination of quantifiers.

**Proof**

Again, consider a formula $\exists x \bigwedge_{i \leq d} \phi_i$ where each $\phi_i$ is an atomic formula.

By distributing over $\land$ (note there is a typo in the book), we obtain formulas of the form $\bigwedge_{i \leq 0} \phi_i$.

First, we can eliminate negation. We replace $t_1 > t_2$ by $t_2 > t_1$. We replace $t_u S > n$ and $t_u S = n$.

There are now two possible cases for atomic formulas:

1. Variable.
2. Before, the only possible terms in the language are either 0 or $n$.

Again, consider a formula $\bigwedge_{i \leq 0} \phi_i$ where each $\phi_i$ is a literal. As before, if $x$ does not appear in some $\phi_i$, we can move it outside the quantifier.

Also, if some $\phi_i$ is an equation $S_k u = S_m t$, we can proceed as in the proof for $\mathcal{N}$. We can proceed as in the proof for $\mathcal{N}$.
Proof (continued)

The remaining literals must have the form $x\text{ }^*\text{ }S < y$ or $y\text{ }^*\text{ }S > x$. Notice that if $n$ is a variable, then the formula can be replaced with $x\text{ }^*\text{ }S > n\text{ }^*\text{ }S$ or $n\text{ }^*\text{ }S > x\text{ }^*\text{ }S$. The formula is true or false. We can rewrite the formula as:

$$\cdot\cdot\cdot n > 0\text{ }^*\text{ }S \bigvee \bigwedge \left( \bigvee \text{ }^*\text{ }S > i + \text{ }^*\text{ }S \bigvee \right)$$

Otherwise, we form

$$\cdot\cdot\cdot n > 0\text{ }^*\text{ }S \bigvee$$

empty, we can replace the formula by

If the second conjunction is empty, the formula is true. If the first conjunction is empty, we can replace the formula by

$$\cdot\cdot\cdot n > x\text{ }^*\text{ }S \bigvee \bigwedge \left( \bigvee \text{ }^*\text{ }S > i \bigvee \right)$$

$x \in \mathbb{N}$
Natural Numbers with Successor and Less-Than

Corollary

\[ C_n A \setminus \{ \leq \} \text{ is complete.} \]

Proof

As before, given a sentence \( \varphi \), we can find a quantifier-free sentence \( \varphi' \) which we can then evaluate to true or false. We have \( \forall \mathbb{N} \subset \forall \mathbb{N}^L \), and \( \forall \mathbb{N} \) is complete, and \( \forall \mathbb{N}^L \) is satisfiable.

Corollary

\[ \forall \mathbb{N} = \forall \mathbb{N}^L \]

Proof

\[ \forall \mathbb{N} \subseteq \forall \mathbb{N}^L \]

Corollary

\[ \forall \mathbb{N} \text{ is complete.} \]

Corollary

\[ \forall \mathbb{N} \text{ is decidable.} \]

Proof

\[ \forall \mathbb{N} \text{ is decidable and axiomatizable. Also, quantifier elimination gives an explicit decision procedure.} \]

Corollary

\[ \forall \mathbb{N} \text{ is complete and axiomatizable.} \]
A subset of $\mathbb{N}$ is definable in $\mathbb{N}$ if it is either finite or has finite complement.

Proof

The addition relation $\{d = u + w | \langle d, u, w \rangle \}$ is not definable in $\mathbb{N}$.

Exercise.

Proof

If we could define addition, we could define the set of even natural numbers:

$$h = x + x \quad x \in \mathbb{N}$$

But this set is neither finite nor has finite complement.

Corollary

A subset of $\mathbb{N}$ is definable in $\mathbb{N}$ if and only if it is either finite or has finite complement.

Corollary

Natural Numbers with Successor and Less-Than
Now, suppose we add the addition symbol, $\mathbf{+}$, to our language, and consider the standard model $\mathbb{N} = \langle \mathbb{N}; 0, S, + \rangle$. We state the following result without proof.

Theorem

Presburger arithmetic is decidable.

Corollary

A set of natural numbers is periodic if and only if it is eventually periodic.

Theorem

A set of natural numbers is definable in $\mathbb{N}$ if and only if it is eventually periodic.

Theorem

The multiplication relation $d = u \times m \lor \mathbb{N} \ni d \langle d', u, m \rangle$ is not definable in $\mathbb{N}^\mathbb{A}$.

Corollary

Presburger arithmetic is decidable.

We state the following result without proof.

Standard model $\langle \mathbb{N}; 0, S, + \rangle = \forall \mathbb{N}$.