Review

- Satisfiability Modulo Theories
- Theory Solvers
- Combining Decision Procedures
- Abstract DPLL Modulo Theories
- Example Application: Translation Validation
Outline

• Number Theory

• Natural Numbers with Successor

• Natural Numbers with Successor and Less-Than

• Presburger Arithmetic

Source: Enderton, 3.0 - 3.2.
Number Theory

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

The parameters are $0, S, <, +, \times, E$.

Let $\mathcal{N}$ be the intended model of this language:

- $\text{dom}\mathcal{N} = \mathbb{N}$, the natural numbers.
- $0^\mathcal{N} = 0$,
- $S^\mathcal{N} = \text{the successor function}: S(n) = n + 1$.
- $<^\mathcal{N} = \text{the less-than relation on } \mathbb{N}$.
- $\times^\mathcal{N} = \text{multiplication on } \mathbb{N}$.
- $E^\mathcal{N} = \text{exponentiation on } \mathbb{N}$.

Number theory is the set of all sentences in this language which are true in $\mathcal{N}$. We denote this theory $\text{Th}\mathcal{N}$. 
Reducts of Number Theory

Besides considering the model \( N \), we also consider the following models which are restrictions of \( N \) to sublanguages:

- \( N_S = (N; 0, S) \)
- \( N_L = (N; 0, S, <) \)
- \( N_A = (N; 0, S, <, +) \)
- \( N_M = (N; 0, S, <, +, \times) \)

We consider the following questions for each model:

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

We will use infix notation: $x < y$ instead of $< xy$ etc.

For each natural number $k$, we denote the associated term by $S^k 0$.

This term is called the *numeral* for $k$. 
Natural Numbers with Successor

We begin with the simplest reduct:

\[ N_S = (\mathbb{N}; 0, S). \]

Consider the theory \( Th\mathbb{N}_S \). What are some of its sentences?
Natural Numbers with Successor

We begin with the simplest reduct:

\[ N_S = (N; 0, S). \]

Consider the theory \( Th N_S \). What are some of its sentences?

- S1. \( \forall x \, Sx \neq 0 \).
- S2. \( \forall x \, \forall y \, (Sx = S\, y \rightarrow x = y) \).
- S3. \( \forall y \, (y \neq 0 \rightarrow \exists x \, y = S\, x) \).
- S4.1 \( \forall x \, S\, x \neq x \).
- S4.2 \( \forall x \, SS\, x \neq x \).
- ... 
- S4.\, n \( \forall x \, S^n\, x \neq x \).

Let \( A_S \) be the above set of sentences (including S4.\, n for each \( n \)).
Natural Numbers with Successor

Now, consider the set $A_S$.

What does an arbitrary model $M$ of $A_S$ look like?
Natural Numbers with Successor

Now, consider the set $\mathbb{A}_S$.

What does an arbitrary model $\mathcal{M}$ of $\mathbb{A}_S$ look like?

$\mathcal{M}$ must contain the *standard* points:

$$0^\mathcal{M} \rightarrow S^\mathcal{M}(0^\mathcal{M}) \rightarrow S^\mathcal{M}(S^\mathcal{M}(0^\mathcal{M})) \rightarrow \ldots$$
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:

$$0^M \rightarrow S^M(0^M) \rightarrow S^M(S^M(0^M)) \rightarrow \ldots$$

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

$$0^M \rightarrow S^M(0^M) \rightarrow S^M(S^M(0^M)) \rightarrow \ldots$$

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

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

$$\ldots \circ \rightarrow \circ \rightarrow a \rightarrow S^M(a) \rightarrow S^M(S^M(a)) \rightarrow \ldots$$
Now, consider the set $A_S$.

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

$M$ must contain the *standard* points:

$$0^M \rightarrow S^M(0^M) \rightarrow S^M(S^M(0^M)) \rightarrow \cdots$$

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

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

$$\cdots \circ \rightarrow \circ \rightarrow a \rightarrow S^M(a) \rightarrow S^M(S^M(a)) \rightarrow \cdots$$

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

Theorem

If $M$ and $M'$ are models of $A_S$ having the same number of $\mathbb{Z}$-chains, then they are isomorphic.

Proof

Clearly, there is an isomorphism between the standard parts of $M$ and $M'$. Since they have the same number of $\mathbb{Z}$-chains, we can extend this isomorphism to map each $\mathbb{Z}$-chain of $M$ to a $\mathbb{Z}$-chain of $M'$.

Recall that a theory $T$ is $\lambda$-categorical iff all models of $T$ having cardinality $\lambda$ are isomorphic.

Theorem

$Cn A_S$ is $\lambda$-categorical for any uncountable cardinal $\lambda$.

Proof

Since the standard part of a model of $A_S$ only contributes a countably infinite number of elements, a model of $A_S$ of cardinality $\lambda$ must have $\lambda$ different $\mathbb{Z}$-chains. By the above theorem, any two such models are isomorphic.
Natural Numbers with Successor

Theorem

\( Cn A_S \) is a complete theory.

Proof

Recall the Los-Vaught test:

Let \( T \) be a theory in a countable language such that

\- \( T \) is \( \lambda \)-categorical for some infinite cardinal \( \lambda \).
\- All models of \( T \) are infinite.

Then \( T \) is complete.

By the previous theorem, \( Cn A_S \) is \( \lambda \)-categorical for any uncountable cardinal \( \lambda \). Furthermore, \( Cn A_S \) has no finite models. Therefore \( Cn A_S \) is complete. \( \square \)
Natural Numbers with Successor

Corollary

\[ CnA_S = ThN_S. \]

Proof

We know that \( CnA_S \subseteq ThN_S \). The first theory is complete, and the second is satisfiable. Therefore, the theories must be equal. (Why?)

Corollary

\( ThN_S \) is decidable.

Proof

Any complete and axiomatizable theory is decidable. \( A_S \) is a decidable set of axioms for this theory.
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 $T$ admits elimination of quantifiers iff for every formula $\phi$ there is a quantifier-free formula $\psi$ such that

$$T \models (\phi \leftrightarrow \psi).$$

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

**Theorem**

Assume that for every formula $\phi$ of the form $\exists x (\alpha_0 \land \ldots \land \alpha_n)$, where each $\alpha_i$ is a literal, there is a quantifier-free formula $\psi$ such that $T \models (\phi \leftrightarrow \psi)$. Then $T$ admits elimination of quantifiers.
Quantifier Elimination

Proof

The proof is by induction on formulas. Clearly, every atomic formula is equivalent to a quantifier-free formula (itself). Suppose that $\alpha$ and $\beta$ are formulas with quantifier-free equivalents $\alpha'$ and $\beta'$.

The propositional connective cases are trivial: $T \models \neg \alpha \iff \neg \alpha'$, $T \models (\alpha \land \beta) \iff (\alpha' \land \beta')$, etc.

For the quantifier cases, we can rewrite $\forall x. \alpha$ as $\neg \exists x. \neg \alpha$, so it is sufficient to consider $\exists x. \alpha$. By induction hypothesis, this is equivalent to $\exists x. \alpha'$, where $\alpha'$ is quantifier-free. But now, we can convert $\alpha'$ to DNF and distribute the existential quantifier over the disjunction to get $(\exists x. \gamma_0) \lor (\exists x. \gamma_1) \lor \cdots \lor (\exists x. \gamma_n)$, where each $\gamma_i$ is a conjunction of literals. But then, by assumption, we can find an equivalent quantifier-free formula for each $\exists x. \gamma_i$, resulting in an equivalent quantifier-free formula for $\exists x. \alpha$. \qed
Elimination of Quantifiers

Theorem

$Th \bar{N}_S$ admits elimination of quantifiers.

Proof

Consider a formula $\exists x (\alpha_0 \land \ldots \land \alpha_l)$, where each $\alpha_i$ is a literal.

Note that the only possible terms in the language are $S^k u$ where $u$ is either 0 or a variable. Each $\alpha_i$ must be an equation or disequation between two such terms.

If $x$ does not appear in some $\alpha_i$, we can move $\alpha_i$ outside the quantifier. The remaining literals have the form $S^m x = S^n u$ or $S^m x \neq S^n u$ where $u$ is 0 or a variable.

If $u$ 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, after making the above simplifications, all remaining literals are disequations, then the formula is true. (Why?)
Elimination of Quantifiers

Proof (cont.)

We have $\exists x (\alpha_0 \land \ldots \land \alpha_l)$, where each $\alpha_i$ is of the form $S^m x = S^n u$ or $S^m x \neq S^n u$, where $u$ is 0 or a variable other than $x$. We also know there is at least one equation.

Suppose $\alpha_i$ is an equation $S^m x = t$. We replace $\alpha_i$ by $t \neq 0 \land \ldots \land t \neq S^{m-1}0$ (since $x$ cannot be negative) and then in each other $\alpha_j$, we replace $S^k x = u$ by $S^k t = S^m u$.

After processing each literal containing $x$, the new formula does not contain $x$, so the quantifier can be eliminated. □
Natural Numbers with Successor

We can now give a decision procedure for $Cn\, A_S$. Suppose we are given a sentence $\sigma$. Using quantifier elimination, we can find a quantifier-free sentence $\tau$ such that $A_S \models (\sigma \leftrightarrow \tau)$.

Note that $\tau$ is a sentence because quantifier elimination does not introduce any free variables, so if we start with a sentence, we will finish with a sentence.

An atomic sentence must be of the form $S^{k_0}0 = S^{l_0}0$ and each such sentence can be evaluated to true or false using $A_S$. Thus any Boolean combination of such sentences can also be evaluated to true or false.

This also provides an alternative proof that $Cn\, A_S$ is complete, since given any sentence $\sigma$ we can compute its quantifier-free equivalent $\tau$ which must be either true or false.

Finally, we can use quantifier-elimination to show that a subset of $\mathcal{N}$ is definable in $\mathcal{N}_S$ iff either it is finite or its complement is finite. (Why?)
Natural Numbers with Successor

Example

\[ \forall x \forall y (x \neq y \rightarrow (x \neq 0 \lor y \neq 0)) \in Cn A_S \]
Natural Numbers with Successor

Example

\[ \forall x \forall y (x \neq y \rightarrow (x \neq 0 \lor y \neq 0)) \in CnA_S \]

iff

\[ \neg \exists x \exists y \neg(x \neq y \rightarrow (x \neq 0 \lor y \neq 0)) \in CnA_S \]
Natural Numbers with Successor

Example

\[ \forall x \forall y (x \neq y \to (x \neq 0 \lor y \neq 0)) \in Cn A_S \]

iff

\[ \neg \exists x \exists y \neg (x \neq y \to (x \neq 0 \lor y \neq 0)) \in Cn A_S \]

iff

\[ \neg \exists x \exists y (x \neq y \land x = 0 \land y = 0) \in Cn A_S \]
Natural Numbers with Successor

Example

$$\forall x \forall y (x \neq y \rightarrow (x \neq 0 \lor y \neq 0)) \in \mathcal{Cn}A_S$$

iff

$$\neg \exists x \exists y \neg (x \neq y \rightarrow (x \neq 0 \lor y \neq 0)) \in \mathcal{Cn}A_S$$

iff

$$\neg \exists x \exists y (x \neq y \land x = 0 \land y = 0) \in \mathcal{Cn}A_S$$

iff

$$\neg \exists x (x \neq 0 \land x = 0) \in \mathcal{Cn}A_S$$
Natural Numbers with Successor

Example

∀ 𝑥 ∀ 𝑦 (𝑥 ≠ 𝑦 → (𝑥 ≠ 0 ∨ 𝑦 ≠ 0)) ∈ Cn AS

iff

¬∃ 𝑥 ∃ 𝑦 ¬(𝑥 ≠ 𝑦 → (𝑥 ≠ 0 ∨ 𝑦 ≠ 0)) ∈ Cn AS

iff

¬∃ 𝑥 ∃ 𝑦 (𝑥 ≠ 𝑦 ∧ 𝑥 = 0 ∧ 𝑦 = 0) ∈ Cn AS

iff

¬∃ 𝑥 (𝑥 ≠ 0 ∧ 𝑥 = 0) ∈ Cn AS

iff

¬(0 ≠ 0) ∈ Cn AS
Natural Numbers with Successor

Example

\[ \forall x \forall y (x \neq y \rightarrow (x \neq 0 \lor y \neq 0)) \in Cn A_S \]

iff

\[ \neg \exists x \exists y \neg (x \neq y \rightarrow (x \neq 0 \lor y \neq 0)) \in Cn A_S \]

iff

\[ \neg \exists x \exists y (x \neq y \land x = 0 \land y = 0) \in Cn A_S \]

iff

\[ \neg \exists x (x \neq 0 \land x = 0) \in Cn A_S \]

iff

\[ \neg (0 \neq 0) \in Cn A_S \]

iff

\[ 0 = 0 \in Cn A_S \]
The ordering relation \( \{ \langle m, n \rangle \mid m < n \} \) is not definable in \( N_S \).

Thus, suppose we add the less-than symbol, \(<\), to our language, and consider the standard model \( N_L = (\mathbb{N}; 0, S, <) \).

We will show that \( Th N_L \) is decidable and admits elimination of quantifiers. However, unlike \( Th N_S \), it is finitely axiomatizable.
Natural Numbers with Successor and Less-Than

The ordering relation \{⟨m, n⟩ | m < n\} is *not* definable in \(N_S\).

Thus, suppose we add the less-than symbol, \(<\), to our language, and consider the standard model \(N_L = (\mathbb{N}; 0, S, <)\).

We will show that \(Th_{N_L}\) is decidable and admits elimination of quantifiers. However, unlike \(Th_{N_S}\), it is finitely axiomatizable.

Consider the following set \(A_L\) of sentences:

- **S3.** \(∀y (y \neq 0 \rightarrow ∃x y = Sx)\)
- **L1.** \(∀x ∀y (x < S y ↔ x ≤ y)\)
- **L2.** \(∀x x ≠ 0\)
- **L3.** \(∀x ∀y (x < y \lor x = y \lor y < x)\)
- **L4.** \(∀x ∀y (x < y \rightarrow y < x)\)
- **L5.** \(∀x ∀y ∀z (x < y \rightarrow y < z \rightarrow x < z)\)

Our goal is to show that \(Cn_{A_L} = Th_{N_L}\).
Natural Numbers with Successor and Less-Than

We first show that $A_S \subseteq Cn A_L$.

1. $A_L \vdash \forall x \ x < Sx$ (by L1).
2. $A_L \vdash \forall x \ x \not< x$ (by L4).
3. $A_L \vdash \forall x \forall y \ (x \not< y \iff y \leq x)$ (by L3, L4, (2)).
4. $A_L \vdash \forall x \forall y \ (x < y \iff Sx < Sy)$ (by L1, (3)).

Recall the definition of $A_S$:

- S1. $\forall x \ Sx \not= 0$.
- S2. $\forall x \forall y \ (Sx =Sy \rightarrow x = y)$.
- S3. $\forall y \ (y \not= 0 \rightarrow \exists x \ y = Sx)$.
- S4. $n \forall x \ S^n x \not= x$.

S3 is already in $A_L$. S1 follows from L2 and (1). S2 follows from (4), L3, and (2). S4. $n$ follows from (1), (2), and L5.

Thus, a model $M$ of $A_L$ consists of a standard part plus 0 or more $\mathbb{Z}$-chains. In addition the elements are ordered by $<^M$. 

19
Theorem

The theory $Cn A_L$ admits elimination of quantifiers.

Proof

Again, consider a formula $\exists x (\beta_0 \land \ldots \land \beta_l)$, where each $\beta_i$ is a literal. As before, the only possible terms in the language are $S^k u$ where $u$ is either 0 or a variable.

There are now two possibilities for atomic formulas:

$$S^m u = S^n t \text{ and } S^m u < S^n t.$$ 

First, we can eliminate negation. We replace $t_1 \not< t_2$ by $t_2 \leq t_1$. We replace $t_1 \not= t_2$ by $t_1 < t_2 \lor t_2 < t_1$.

By distributing $\exists$ over $\lor$ (note there is a typo in the book), we obtain formulas of the form $\exists x (\alpha_0 \land \ldots \land \alpha_p)$, where each $\alpha_i$ is an atomic formula.

As before, if $x$ does not appear in some $\alpha_i$, we can move it outside the quantifier. Also, if some $\alpha_i$ is an equation $S^m x = t$, we can proceed as in the proof for $N_S$. 
Natural Numbers with Successor and Less-Than

Proof (continued)

The remaining literals must have the form $S^m x < S^n u$ or $S^m u < S^n x$ where $u$ is $0$ or a variable. Notice that if $u$ is $x$, then the formula can be replaced with true or false. We can rewrite the formula as

$$\exists x \left( \bigwedge_i t_i < S^{m_i} x \land \bigwedge_j S^{n_j} x < u_j \right).$$

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

$$\bigwedge_j S^{n_j} 0 < u_j.$$ 

Otherwise, we form

$$\left( \bigwedge_{i,j} S^{n_j+1} t_i < S^{m_i} u_j \land \right) \land \bigwedge_j S^{n_j} 0 < u_j.$$ 

$\square$
Natural Numbers with Successor and Less-Than

Corollary

$Cn\ A_L$ is complete.

Proof

As before, given a sentence $\sigma$, we can find a quantifier-free sentence $\tau$ which we can then evaluate to true or false.

Corollary

$Cn\ A_L = Th\ N_L$

Proof

We have $Cn\ A_L \subseteq Th\ N_L$, $Cn\ A_L$ is complete, and $Th\ N_L$ is satisfiable.

Corollary

$Th\ N_L$ is decidable.

Proof

$Th\ N_L$ is complete and axiomatizable. Also, quantifier elimination gives an explicit decision procedure.
Natural Numbers with Successor and Less-Than

Corollary

A subset of \( \mathcal{N} \) is definable in \( \mathcal{N}_L \) iff it is either finite or has finite complement.

Proof

Exercise. \( \square \)

Corollary

The addition relation \( \{ \langle m, n, p \rangle \mid m + n = p \} \) is not definable in \( \mathcal{N}_L \).

Proof

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

\[ \exists x \; x + x = y. \]

But this set is neither finite nor has finite complement. \( \square \)
Presburger Arithmetic

Now, suppose we add the addition symbol, $+$, to our language, and consider the standard model $N_A = (\mathbb{N}; 0, S, <, +)$.

We state the following results without proof.

**Theorem**

Presburger arithmetic is decidable.

A set $D$ of natural numbers is *periodic* if there exists some positive $p$ such that $n \in D$ iff $n + p \in D$. $D$ is *eventually periodic* iff there exists positive numbers $M$ and $p$ such that if $n > M$, then $n \in D$ iff $n + p \in D$.

**Theorem**

A set of natural numbers is definable in $N_A$ iff it is eventually periodic.

**Corollary**

The multiplication relation $\{\langle m, n, p \rangle \mid p \in \mathbb{N} \land m \times n = p \}$ is not definable in $N_A$. 