Outline

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

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 $\mathbf{0}, \mathbf{S}, <, +, \times, \mathbf{E}$.

Let N be the intended model of this language:

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

Number theory is the set of all sentences in this language which are true in N. We denote this theory *Th* N.

Reducts of Number Theory

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

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

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 $\mathcal{N}$ 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 $\mathbf{S}^k\mathbf{0}$.

This term is called the *numeral* for k.

Natural Numbers with Successor

We begin with the simplest reduct:

$$N_S = (\mathcal{N}; 0, S).$$

Consider the theory *Th* N_S. What are some of its sentences?

Natural Numbers with Successor

We begin with the simplest reduct:

$$N_S = (\mathcal{N}; 0, S).$$

Consider the theory $Th\, N_S$. What are some of its sentences?

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

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?

M must contain the *standard* points:

$$\mathbf{0}^M \rightarrow \mathbf{S}^M(\mathbf{0}^M) \rightarrow \mathbf{S}^M(\mathbf{S}^M(\mathbf{0}^M)) \rightarrow \cdots$$

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

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

$$\cdots \circ \rightarrow \circ \rightarrow a \rightarrow \mathbf{S}^M(a) \rightarrow \mathbf{S}^M(\mathbf{S}^M(a)) \rightarrow \cdots$$

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 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 Z-chains, we can extend this isomorphism to map each Z-chain of M to a Z-chain of M'.

Recall that a theory T is *λ-categorical* iff all models of T having cardinality λ are isomorphic.

Theorem

Cn A_S is λ-categorical for any uncountable cardinal λ.

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 λ must have λ different 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 λ-categorical for some infinite cardinal λ.
- All models of T are infinite.

Then T is complete.

By the previous theorem, *Cn* A_S is λ-categorical for any uncountable cardinal λ. Furthermore, *Cn* A_S has no finite models. Therefore *Cn* A_S is complete.

Natural Numbers with Successor

Corollary

$Cn\, A_S = Th\, N_S$.

Proof

We know that $Cn\, A_S \subseteq Th\, N_S$. The first theory is complete, and the second is satisfiable. Therefore, the theories must be equal. (Why?)

Corollary

$Th\, N_S$ 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 ϕ there is a quantifier-free formula ψ 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 ϕ of the form $\exists\, x\, (\alpha_0 \wedge \ldots \wedge \alpha_n)$, where each α_i is a literal, there is a quantifier-free formula ψ 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 α and β are formulas with quantifier-free equivalents α' and β'.

The propositional connective cases are trivial: $T \models \neg\alpha \leftrightarrow \neg\alpha'$, $T \models (\alpha \wedge \beta) \leftrightarrow (\alpha' \wedge \beta')$, 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 α' is quantifier-free. But now, we can convert α' to DNF and distribute the existential quantifier over the disjunction to get $(\exists x.\ \gamma_0) \vee (\exists x.\ \gamma_1) \vee \cdots \vee (\exists x.\ \gamma_n)$, where each γ_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 $\exists x.\ \alpha$.

Elimination of Quantifiers

Theorem

$Th\, N_S$ admits elimination of quantifiers.

Proof

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

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

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

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

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

Proof (cont.)

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

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

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 $\mathit{Cn}\, A_S$. Suppose we are given a sentence σ. Using quantifier elimination, we can find a quantifier-free *sentence* τ such that $A_S \models (\sigma \leftrightarrow \tau)$.

Note that τ 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 $\mathbf{S}^k\mathbf{0} = \mathbf{S}^l\mathbf{0}$ 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 $\mathit{Cn}\, A_S$ is complete, since given any sentence σ we can compute its quantifier-free equivalent τ which must be either true or false.

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

Example

$$\forall\, x\, \forall\, y\, (x \neq y \rightarrow (x \neq \mathbf{0} \vee y \neq \mathbf{0})) \in \mathit{Cn}\, A_S$$

Natural Numbers with Successor

Example

$\forall\, x\, \forall\, y\, (x \neq y \rightarrow (x \neq \mathbf{0} \vee y \neq \mathbf{0})) \in \mathit{Cn}\, A_S$

iff

$\neg\exists\, x\, \exists\, y\, \neg(x \neq y \rightarrow (x \neq \mathbf{0} \vee y \neq \mathbf{0})) \in \mathit{Cn}\, A_S$

iff

$\neg\exists\, x\, \exists\, y\, (x \neq y \wedge x = \mathbf{0} \wedge y = \mathbf{0}) \in \mathit{Cn}\, A_S$

iff

$\neg\exists\, x\, (x \neq \mathbf{0} \wedge x = \mathbf{0}) \in \mathit{Cn}\, A_S$

iff

$\neg(\mathbf{0} \neq \mathbf{0}) \in \mathit{Cn}\, A_S$

iff

$\mathbf{0} = \mathbf{0} \in \mathit{Cn}\, A_S$

Natural Numbers with Successor and Less-Than

The ordering relation $\{\langle m, n\rangle \,|m < n\}$ is *not* definable in N_S.

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

We will show that $\mathit{Th}\, N_L$ is decidable and admits elimination of quantifiers. However, unlike $\mathit{Th}\, N_S$, it is finitely axiomatizable.

Consider the following set A_L of sentences:

- S3. $\forall y\,(y \neq \mathbf{0} \to \exists x\, y = \mathbf{S}x)$
- L1. $\forall x \forall y\,(x < \mathbf{S}y \leftrightarrow x \leq y)$
- L2. $\forall x\, x \not< \mathbf{0}$
- L3. $\forall x \forall y\,(x < y \vee x = y \vee y < x)$
- L4. $\forall x \forall y\,(x < y \to y \not< x)$
- L5. $\forall x \forall y \forall z\,(x < y \to y < z \to x < z)$

Our goal is to show that $\mathit{Cn}\, A_L = \mathit{Th}\, N_L$.

We first show that $A_S \subseteq \mathit{Cn}\, A_L$.

1. $A_L \vdash \forall x\, x < \mathbf{S}x$ (by L1).
2. $A_L \vdash \forall x\, x \not< x$ (by L4).
3. $A_L \vdash \forall x \forall y\,(x \not< y \leftrightarrow y \leq x)$ (by L3, L4, (2)).
4. $A_L \vdash \forall x \forall y\,(x < y \leftrightarrow \mathbf{S}x < \mathbf{S}y)$ (by L1, (3)).

Recall the definition of A_S:

- S1. $\forall x\, \mathbf{S}x \neq \mathbf{0}$.
- S2. $\forall x \forall y\,(\mathbf{S}x = \mathbf{S}y \to x = y)$.
- S3. $\forall y\,(y \neq \mathbf{0} \to \exists x\, y = \mathbf{S}x)$.
- S4.n $\forall x\, \mathbf{S}^n x \neq x$.

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 Z-chains. In addition the elements are ordered by $<^M$.

Theorem

The theory *Cn* A_L admits elimination of quantifiers.

Proof

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

There are now two possibilities for atomic formulas:

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

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

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

As before, If x does not appear in some α_i, we can move it outside the quantifier. Also, if some α_i is an equation $\mathbf{S}^m x = t$, we can proceed as in the proof for N_S.

Proof (continued)

The remaining literals must have the form $\mathbf{S}^m x < \mathbf{S}^n u$ or $\mathbf{S}^m u < \mathbf{S}^n x$ where u is $\mathbf{0}$ 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

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

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

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

Otherwise, we form

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

Corollary

$Cn\, A_L$ is complete.

Proof

As before, given a sentence σ, we can find a quantifier-free sentence τ 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.

Corollary

A subset of $\mathcal{N}$ is definable in N_L iff it is either finite or has finite complement.

Proof

Exercise.

Corollary

The addition relation $\{\langle m, n, p\rangle \,|m + n = p\}$ is not definable in 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.

Presburger Arithmetic

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

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 $\{\langle m, n, p\rangle \,|p \in \mathcal{N} \wedge m \times n = p\}$ is not definable in N_A.