

CDM

Predicate Logic, II

Klaus Sutner
Carnegie Mellon University
www.cs.cmu.edu/~sutner

Battleplan

- First Order Theories
- Deduction and Completeness
- Compactness and Arithmetic
- Incompleteness
- (Un-)Decidability

First Order Theories

First Order Logic

So far we have referred to our new logic as "predicate logic". Alternatively, this system is often known as *first order logic (FOL)*: first order since we can only quantify over individuals but not over sets of individuals, functions, relations, and so on.

Needless to say, there are also systems of second order logic and, more generally, higher order logic. We will not get involved with these but we will use the terminology.

FOL and Theories

Again, why is FOL all that interesting?

It is a matter of experience that FOL is just expressive enough to pin down the properties of most objects that arise in mathematics and computer science. On the other hand, one can handle proofs in FOL rather well (see below).

To pin down a particular domain of discourse in FOL one chooses an appropriate language (i.e., one selects function and relation symbols) and then constructs a collection of formulae Γ , the axioms, in this language that pin down the desired properties of the intended functions and relations.

The hope is that the models of the axioms are precisely the structures one is interested in. In algebra this approach is hugely successful, but in more complicated theories such as arithmetic problems arise.

Semantic Consequence

Definition 1. Given a set Γ of sentences and a sentence φ we say that φ is a **semantic consequence** of Γ if any structure \mathcal{A} that satisfies all formulae in Γ also satisfies φ .

Notation:

$$\Gamma \models \varphi$$

For example, for a ground term t

$$\begin{aligned} \varphi(t) &\models \exists x \varphi(x) \\ \varphi, \varphi \rightarrow \psi &\models \psi \end{aligned}$$

The insistence on sentences (formulae without free variables) should be taken with a grain of salt: if there are free variables as in $\varphi(x_1, \dots, x_n)$ we often tacitly replace the formula by its universal closure.

Theories

Definition 2. A set Δ of sentences is a **theory** if for every sentence φ we have $\Delta \models \varphi$ implies $\varphi \in \Delta$.

So a theory is large, it contains all the statements that follow semantically from it.

As a matter of fact, a theory is always an infinite set of formulae, albeit for silly reasons: with every sentence φ a theory also contains $\varphi \wedge \varphi$.

As an example, consider

$$\Delta = \text{all true statements of arithmetic}$$

in the language $\mathcal{L}(+, *, 0, 1; <)$. Note that Δ is indeed closed under semantic consequence: whatever follows from a true statement is still a true statement.

Structures and Theories

The last example suggests that one can obtain theories from a structure, or a class of structures.

Definition 3. Given a class \mathcal{C} of structures we define the theory of \mathcal{C} to be the collection of sentences valid in all the structures in \mathcal{C} :

$$\text{Th}(\mathcal{C}) = \{ \varphi \mid \text{for all } \mathcal{A} \in \mathcal{C} : \mathcal{A} \models \varphi \}$$

Note that $\text{Th}(\mathcal{C})$ is indeed a theory. If there is only one structure \mathcal{A} in the class we write $\text{Th}(\mathcal{A})$.

For example, $\text{Th}(\mathcal{N})$ is the theory of arithmetic.

$\text{Th}(\text{Group})$ is the theory of groups and so on.

Axioms

By contrast, a set Γ of axioms is usually small, it does not contain most of its consequences.

Ideally, Γ should be

- Finite (finitely axiomatizable), or have a simple, regular structure;
- Independent: no axiom follows from the others.

At the least a set of axioms should be decidable; obviously, axioms that are not recognizable as such are not terribly interesting.

A good example for a simple but infinite collection of axioms are the induction axioms in Peano arithmetic. For any formula $\varphi(x)$ with one free variable as indicated we have an axiom

$$\varphi(0) \wedge \forall x (\varphi(x) \rightarrow \varphi(x+1)) \rightarrow \forall x \varphi(x)$$

Designing Axioms

Where do the axioms come from?

We have a particular structure (such as the natural numbers), or a collection of structures \mathcal{C} (such as the collection of all groups), and we want to find a set of axioms Γ such that

$$\text{Mod}(\Gamma) = \mathcal{C}.$$

For example, for groups it is not too hard to find the appropriate axioms – though it took quite some time to develop the axiomatic method itself. For example, the first serious attempt at axiomatizing the natural numbers dates back to 1888 (R. Dedekind).

Again, note that the challenge is to find simple axioms, otherwise we could cheat non-constructively and set $\Gamma = \text{Th}(\mathcal{C})$.

Axioms to Theories

So suppose we have some axiom system Γ , presumably not a theory.

Then Γ determines a theory, namely the set of sentences valid in all models of Γ :

$$\text{Th}(\Gamma) = \{ \varphi \mid \mathcal{A} \models \Gamma \text{ implies } \mathcal{A} \models \varphi \}$$

Proposition 1. $\text{Th}(\Gamma)$ is indeed a theory.

Definition 4. A theory T is **axiomatizable** if there is a decidable set Γ of sentences such that $T = \text{Th}(\Gamma)$.

A theory T is **finitely axiomatizable** if there is a finite set Γ of sentences such that $T = \text{Th}(\Gamma)$.

Example: Groups

Groups are a standard example of an elementary class of structures. We use the language

$$\mathcal{L}(*, e) \text{ of signature } (2, 0)$$

The axioms for groups are (recall our convention about free variables being universally quantified):

$$\begin{aligned} x * (y * z) &\approx (x * y) * z \\ x * e &\approx x \wedge e * x \approx x \\ \exists y (x * y &\approx e \wedge y * x \approx e) \end{aligned}$$

Hence group theory is finitely axiomatizable (or, equivalently, the class of all groups is elementary).

Example: Fields

Rings and fields form an elementary class.

Here are axioms for fields in the language $\mathcal{L}(+, *, -, ^{-1}, 0, 1)$ of type $(2, 2, 1, 1, 0, 0)$.

$$\begin{array}{ll} x + (y + z) \approx (x + y) + z & x * (y * z) \approx (x * y) * z \\ x + y \approx y + x & x * y \approx y * x \\ x + 0 \approx x & x * 1 \approx x \\ x + (-x) \approx 0 & x \neq 0 \rightarrow x * x^{-1} \approx 1 \\ x * (y + z) \approx x * y + x * z & 0 \neq 1 \end{array}$$

Exercise 1. What would these axioms look like using the language $\mathcal{L}(+, *)$ of type $(2, 2)$?

Characteristic

Write \underline{n} for the ground term $\underbrace{1 + 1 + \dots + 1}_n, n \geq 1$.

Consider the sentences $\chi_n = \underline{n} \approx 0, n \geq 2$.

Adding a single axiom χ_n, n prime, to the field axioms produces axioms for fields of characteristic n .

Adding all axioms $\neg\chi$ produces axioms for fields of characteristic 0.

Exercise 2. What happens if we adjoin an axiom χ_n for n composite?

Exercise 3. How can one axiomatize the theory of algebraically closed fields?

Example: Boolean Algebras

Boolean algebras are also an elementary class.

Here the language is $\mathcal{L}(\sqcup, \sqcap, ', 0, 1)$ of signature $(2, 2, 1, 0, 0)$.

$$\begin{array}{ll} x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z & x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z \\ x \sqcup y = y \sqcup x & x \sqcap y = y \sqcap x \\ x \sqcup 0 = x & x \sqcap 1 = x \\ x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z) & x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z) \\ x \sqcup x' = 1 & x \sqcap x' = 0 \end{array}$$

Exercise 4. What would these axioms look like we adopted as primitive notion a partial order $x \leq y \iff x \sqcap y = x$?

Example: Linear Orders

Yet another elementary class.

Here the language is $\mathcal{L}(<)$ of signature (2) . For a strict total order we need transitivity, trichotomy and anti-symmetry.

$$\begin{array}{l} x < y \wedge y < z \rightarrow x < z \\ x < y \vee x \approx y \vee y < x \\ x < y \rightarrow \neg y < x \end{array}$$

To get a dense order we add

$$x < y \rightarrow \exists z (x < z < y)$$

Completeness

Completeness of a Theory

Since axiom systems are typically small the problem arises whether they contain enough information to really pin down the objects under discussion. Ideally we would like the axioms to settle all possible questions (at least questions that can be phrased in the particular language we have chosen).

Definition 5. A set of sentences Γ is **complete** if for every sentence φ of the language we have either $\Gamma \models \varphi$ or $\Gamma \models \neg\varphi$.

In other words, Γ contains enough information to determine truth of any possible assertion. A cheap example for a complete theory is $\text{Th}(\mathcal{C})$.

Completeness is a rather strong property; for example, Γ has to pin down statements about cardinality. Most standard axiom systems are indeed incomplete.

Example 1. The theory of algebraically closed fields of characteristic 0 is complete, as is the theory of real closed fields.

Elementary Equivalence

Another way of thinking about completeness is to consider the models, they are all very similar in the following sense:

Definition 6. Two structures \mathcal{A} and \mathcal{B} are **elementarily equivalent** if $\text{Th}(\mathcal{A}) = \text{Th}(\mathcal{B})$.

As always, we assume that the structures have the same signature.

Thus, as long as we restrict ourselves to the limitations of FOL we cannot distinguish between the two structures. But note that this notion is much weaker than the existence of an isomorphism between the structures.

Proposition 2. Γ is complete if, and only if, any two models of Γ are elementarily equivalent.

Axioms versus Models

As the examples show, most axiom systems have many different models: there are many choices for a structure $\mathcal{A} \models \Gamma$. Rarely are all models elementarily equivalent, much less isomorphic.

For some applications such as the axiomatization of arithmetic or the real numbers this is a problem: we would like the axioms to pin down the structure completely (up to isomorphism). We do not want several versions of the reals or the integers lying around.

But otherwise this ambiguity is actually a considerable advantage of the axiomatic method: the axioms describe a whole class of models. For example, we have seen how to axiomatize groups with just three natural axioms.

In a sense, FOL is much better for the second approach; it tends to fail when it comes to pinning things down.

Derivations and Proofs

Derivations

To really get mileage out of FOL, though, we need a better grip on $\text{Th}(\Gamma)$: we need to be able to find the consequences φ of Γ directly, without complete knowledge of all the models.

We would like to argue solely from the axioms themselves, without any reference to the (possibly complicated) assortment of models.

For example, we know informally how to derive the assertion

$$\forall x, y ((x * y)^{-1} = y^{-1} * x^{-1})$$

directly from the group axioms, using some basic equational reasoning and "obvious" rules for quantification.

How do we formalize these rules?

How do we construct proofs in FOL?

Syntactic Consequence

We need to come up with a notion of proof or derivation in FOL that allows us to draw inferences from a set of given formulae. The goal is to develop a notion of *provability*

$$\Gamma \vdash \varphi$$

analogous to provability in propositional logic. There are many different ways of doing this, for the sake of brevity let us only indicate how the natural deduction system from the lecture on propositional logic can be expanded to FOL.

Needless to say, we can retain the propositional rules, they are still sound in the new context.

Natural Deduction and FOL

To extend natural deduction to FOL we need to add rules for quantifiers. Intuitively, that's not too hard.

$$\frac{\phi(t)}{\exists x \phi(x)} (\exists e) \qquad \frac{\exists x \phi(x)}{\phi(c)} (\exists i)$$

$$\frac{\phi(c)}{\forall x \phi(x)} (\forall i) \qquad \frac{\forall x \phi(x)}{\phi(t)} (\forall e)$$

where x is a variable, c a constant, and t a term.

Alas, while these rules are correct in spirit, as stated they are not sound.

Counterexample

Suppose we adopt the quantifier rules from above. Then we can perform a derivation along the following lines.

$\forall x \exists y (x < y)$	premise
$\exists y (c < y)$	$(\forall e)$
$(c < d)$	$(\exists e)$
$\forall x (x < d)$	$(\forall i)$
$\exists y \forall x (x < y)$	$(\exists i)$

Disaster! This is exactly the wrong direction of the valid implication $\exists x \forall y \varphi(x, y) \rightarrow \forall y \exists x \varphi(x, y)$. The problem is that the "constant" d really depends on c .

Counterexample, contd.

To address this and similar problems, one has to add some technical conditions to the quantifier rules that rule out the derivation from above.

For $(\forall i)$ we insist that c is "fresh": it must not occur in any undischarged assumptions in the derivation of $\varphi(c)$ nor in the conclusion $\forall x \varphi(x)$ itself.

For $(\exists e)$ again we insist on a fresh constant c :

$$\frac{\exists x \phi(x) \quad \begin{array}{c} [\phi(c)] \\ \vdots \\ \chi \end{array}}{\chi} (\exists e)$$

For $(\forall e)$ and $(\exists i)$ we insist that term t is substitutable for x in φ : no variable in t becomes bound as a result of the replacement process.

Syntactic Consequence

We won't belabour the details, though they are extremely important when one tries to actually implement a deduction system in FOL. What we need here is the ability to derive consequences from a given collection of formulae, in a purely syntactic fashion.

Definition 7. The set of all provable theorems of a collection of sentences in FOL is called its (syntactic) theory or its set of consequences.

Notation:

$$\text{Cn}(\Gamma) = \{ \varphi \mid \Gamma \vdash \varphi \}$$

For example, the standard claims about

Proofs versus Truth

As with propositional logic the central problem is that we need

- Soundness: $\Gamma \vdash \varphi \Rightarrow \Gamma \models \varphi$, and
- Completeness: $\Gamma \models \varphi \Rightarrow \Gamma \vdash \varphi$.

at the same time.

Note that two worlds interact here: proofs are merely syntactic objects (data structures) whereas truth and semantic consequence depend on actual structures. There can be very many such structures and they are possibly infinite, so it is difficult to get a clear understanding of what they look like.

As a consequence, it is far from clear that there even exists a set of non-logical axioms, which, together with the logical axioms and the rules of inference, would achieve this goal.

Proofs in FOL

The first proof of completeness is due to Gödel.



Theorem 1. Completeness Theorem, Gödel 1930

There is a formal system for FOL that is sound and complete.

Deduction Theorem

As far as implications are concerned, FOL behaves just like propositional logic.

Theorem 2. Let Γ, φ, ψ be sentences. Then $\Gamma, \varphi \vdash \psi$ if, and only if, $\Gamma \vdash \varphi \rightarrow \psi$.

But note the condition on sentences here, free variables cause problems. For example, $P(x) \vdash P(y)$ but $\vdash P(x) \rightarrow P(y)$ is false.

So if there is a proof $\Gamma \vdash \varphi$ between sentences, then

$$\vdash \psi_1 \wedge \psi_2 \dots \wedge \psi_n \rightarrow \varphi$$

for some ψ_i in Γ .

Consistency

Could it ever happen that some set of axioms Γ has no models at all?

Sure, let $\Gamma = \{\perp\}$ or $\Gamma = \{c \neq c\}$.

Of course, no one would use these as axioms. But, it might happen that \perp is provable from an ill-chosen set of axioms: there will be no models, but that may not at all be obvious from the axioms.

Definition 8. Γ is **inconsistent** if $\Gamma \vdash \perp$, and **consistent** otherwise.

Hence, an inconsistent set of axioms has no models; the properties we were trying to pin down contradict each other.

No Other Problems

Surprisingly, this is the only thing that can go wrong.

Theorem 3. Every consistent set of axioms has a model.

Proof.

Without going into details, the idea of a proof by L. Henkin is to

- add many constants c to the language, and
- extend Γ to a certain complete set T of sentences.

The constants are used to make sure that $\exists x \varphi(x) \in T$ implies $\varphi(c) \in T$ for some c .

Then we can construct a term model for Γ : the collection of all terms, modulo equality provable in T , turns out to be a model of Γ .

□

Enforcing Completeness

The fact that consistency is the only requirement for the existence of a complete extension of an axiom system is really a separate theorem by Tarski.

Theorem 4. *Tarski*

Every consistent set of sentences T can be extended to a complete set of sentences $T' \supseteq T$.

Of course, T' might be very complicated. For example, we might lose decidability.

Exercise 5. What might a complete extension of the theory of fields look like? Note that it has to settle on a value for 0^{-1} .

Completeness of FOL

Theorem 5. $\Gamma \models \varphi$ implies that $\Gamma \vdash \varphi$.

Proof.

Suppose otherwise. Then $\Gamma, \neg\varphi$ must be consistent by the Deduction Theorem.

But then $\Gamma, \neg\varphi$ has a model, contradicting our assumption.

□

So semantic and syntactic consequence are the same:

$$\text{Th}(\Gamma) = \text{Cn}(\Gamma)$$

Compactness

Compactness

Another crucial property of first order theories is based on the following simple observation: any single derivation in FOL uses only finitely many formulae. One can certainly imagine stronger systems where a single proof involves infinitely many formulae, but in FOL this is not the case.

Hence, Γ inconsistent means that there is a finite subset Γ_0 of Γ that is already inconsistent. By completeness we get the following surprising consequence:

Theorem 6. *Compactness Theorem*

Γ has a model if, and only if, every finite subset Γ_0 of Γ has a model.

This is positively wild, because infinitely many axioms can be used to construct weird conditions, when every finite subset is perfectly harmless.

Application: Finite Structures

Lemma 1. *The class of all finite structures (of some signature) is not definable in FOL.*

For assume that Γ is some axiom system that characterizes finite structures. Hence Γ has arbitrarily large finite models. But then Γ must have an infinite model.

To see this, add new constants $c_i, i \in \mathbb{N}$, to the language and add new axioms

$$c_i \neq c_j \quad \text{for } i < j$$

to Γ to obtain an extension Γ' . Every finite subset of Γ' has a model; by compactness Γ' has a model which must be infinite by choice of the additional axioms.

Exercise 6. *Use a similar argument to show that there is an infinite field of characteristic 2. By contrast, give an algebraic construction of such a field.*

Application: Infinite Structures

Lemma 2. *The class of all infinite structures (of some signature) is not elementary.*

For otherwise the class of finite structures would also be elementary.

But note that the class of infinite structures is FO definable: we need infinitely many sentences of the form "there are at least n elements".

$$\text{EX}_{\geq n} = \exists x_1, \dots, x_n (x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge \dots \wedge x_{n-1} \neq x_n)$$

Exercise 7. *Fill in the details in the proofs above.*

More Exercises

Exercise 8. *Write down axioms for fields.*

Exercise 9. *Write down axioms for finite fields, for infinite fields and for fields of characteristic p (both for $p = 0$ and p prime).*

Exercise 10. *How would you axiomatize vector spaces where one has to deal with a field and the actual vector space at the same time?*

Exercise 11. *Axiomatize the real numbers as best as you can: use field axioms and add Write down axioms for finite fields, for infinite fields and for fields of characteristic p (both for $p = 0$ and p prime).*

Repeat for complex numbers (of course, without the order relation).

Exercise 12. *Try to write down axioms for a stack of elements of some ground type. Repeat for queues, lists and trees.*

Peano Arithmetic (PA)

Here is an example of a hugely important axiom system due to G. Peano in 1889 that describes the salient properties of the structure of natural numbers $\mathcal{N} = \langle \mathbb{N}; +, \cdot, S, 0, 1, < \rangle$, signature $(2, 2, 1, 0, 2)$, with the usual arithmetic operations and order. Actually, R. Dedekind, Gauss' last student, developed the same system a year before Peano but never published.



The system defines addition, multiplication and order in terms of the *successor function*

$$S(x) = x + 1$$

Peano's Axioms

successor

$$S(x) \neq 0 \quad S(x) \approx S(y) \rightarrow x \approx y$$

addition

$$x + 0 \approx x \quad x + S(y) \approx S(x + y)$$

multiplication

$$x \cdot 0 \approx 0 \quad x \cdot S(y) \approx (x \cdot y) + x$$

order

$$\neg(x < 0) \quad x < S(y) \leftrightarrow x \approx y \vee x < y$$

Computational Aspects

The Peano axioms are about 100 years old. Surprisingly, they are almost like programs.

More precisely, the axioms provide primitive recursive definitions of plus, times and less-than in terms of the atomic successor function succ.

```
int add( int x, int y ) {
    if( y == 0 ) return x;
    return succ( x, pred(y) );
}

bool mult( int x, int y ) {
    if( y == 0 ) return 0;
    return add( mult( x, pred(y) ), x );
}
```

Here pred(y) stands for the predecessor $y - 1$.

Induction

Arithmetic operations alone are not enough, we are missing one essential feature of the natural numbers: induction. To capture induction we add the *Induction Axiom*:

$$\varphi(0) \wedge \forall x (\varphi(x) \rightarrow \varphi(S(x))) \rightarrow \forall x \varphi(x)$$

Strictly speaking, this is not an axiom but an axiom schema: we get one axiom for each choice of φ .

At any rate, (PA) is a very succinct representation of the essential features of arithmetic.

Basic Number Theory

When someone says "prove that every number is divisible by a prime", they really mean: "prove in (PA) that every number is divisible by a prime".

OK, this is a white lie: a great many mathematicians and even more computer scientists are blissfully unaware of (PA).

But the point is that even if one is not interested in formal derivations, Peano arithmetic still provides a natural framework for reasoning about the natural numbers.

There are more powerful systems such as set theory or type theory which allow us to prove more complicated facts, but when dealing with the natural numbers (PA) is almost always all you need.

A Sample Proof

Lemma 3. (PA) proves that $\forall x (0 + x \approx x)$

Proof.

Consider the formula $\varphi(x) \equiv (0 + x \approx x)$.

Then $\varphi(0)$ is the first addition axiom (more precisely, replace x by 0 there).

Now assume $\varphi(x)$. Then by the second addition axiom

$$0 + S(x) \approx S(0 + x) \approx S(x)$$

Hence we have shown $\varphi(0) \wedge \forall x (\varphi(x) \rightarrow \varphi(S(x)))$.

By the Induction Axiom and modus ponens we get $\forall x \varphi(x)$. □

More

The important point in all of these exercises is to argue from the axioms, not any intuitive understanding of the structure.

Exercise 13. Prove the following assertions in (PA).

$$\forall x, y, z (x + (y + z) \approx (x + y) + z)$$

$$\forall x, y (x + y \approx y + x)$$

Conclude that $\langle \mathbb{N}; +, 0 \rangle$ is a commutative monoid.

Exercise 14. Define the GCD and describe the Euclidean algorithm in (PA).

Exercise 15. Prove that there are infinitely many primes in (PA).

Who Cares???

One could argue that some 50+ years ago, no one cared except some mathematicians and logicians.

Some were even rather proud of their work being totally impractical (G. H. Hardy, "A Mathematician's Apology", CUP 1948).

As recent history shows, Hardy totally underestimated the impact of apparently obscure branches of mathematics (in his defense: the role of computers was not clear when he wrote the book).

Modern cryptography is unthinkable without number theory, group theory, finite field theory. Graphics without projective geometry is a sad affair. The notion of efficient algorithm is derived from recursion theory (classical theory of computation). Verification of IEEE protocols uses formal logic.

And so on.

Axiomatizing Arithmetic

One would hope that the Peano axioms allow one to derive all true statements of arithmetic.

But note that there is a little problem here: the true statements of arithmetic are the theory of a single structure:

$$\text{Th}(\mathcal{N}) = \{ \varphi \mid \mathcal{N} \models \varphi \}$$

But all we get from our notion of provability is the statements that hold in all models of (PA).

That would be fine if \mathcal{N} were the only such model (up to isomorphism or even elementary equivalence). Unfortunately, there are others as we shall see shortly.

A Weird Model for (PA)

If we think of (PA) as pinning down axiomatically the properties of the natural numbers, here is some very bad news: \mathcal{N} is not the only model of (PA).

To see this, introduce a new constant c and add the following new axioms to (PA):

$$0 < c, S(0) < c, S^2(0) < c, \dots, S^n(0) < c, \dots$$

Call the new set of axioms (PA^∞) .

Claim 1. (PA^∞) has a model.

Proof. To see this, exploit compactness. Any finite subset Γ of (PA^∞) contains only finitely many of the new axioms. So there is a largest n such that $S^n(0) < c \in \Gamma$.

But then we can simply interpret c as $n + 1$ in the standard model \mathcal{N} , done. \square

Non-Standard Models

So let \mathcal{A} be a model of (PA^∞) . Since \mathcal{A} is in particular a model of (PA) we have a full copy of \mathcal{N} inside \mathcal{A} : there are distinct elements for $0, S(0), S(S(0))$ and so forth.

But, this structure also contains an "infinitely large" element $c^{\mathcal{A}}$: since c is a constant in the language it is interpreted by some element of \mathcal{A} , and it follows from the extra axioms that

$$\mathcal{A} \models S^n(0) < c$$

for all $n \geq 0$.

Of course, $c^{\mathcal{A}}$ is not infinitely large from the perspective of \mathcal{A} , it's just a "natural number" there. As are $c^{\mathcal{A}} + 1, c^{\mathcal{A}} + c^{\mathcal{A}}, (c^{\mathcal{A}})^2$ and so on.

Complicated Diagrams

Note that the atomic diagram $\text{diag}(\mathfrak{N})$ of the natural numbers is very simple (atomic, we are not making any claims about the complete diagram).

A typical formula in the atomic diagram is $2 + 3 \approx 5$ or $\neg 3 < 2$.

Certainly $\text{diag}(\mathfrak{N})$, given some reasonable encoding, is decidable, even primitive recursive (at a very low level of the hierarchy).

Theorem 7. *Tennenbaum, 1960*

No non-standard model \mathcal{A} of (PA) is computable: the atomic diagram of \mathcal{A} is always undecidable.

Note that we are dealing with the atomic diagram here, not quantified sentences. The problem comes from prime divisors of integers in the model:

$$\{ n \in \mathbb{N} \mid \mathcal{A} \models p_n \text{ divides } a \}$$

If a here is non-standard, these sets can be very complicated.

Non-Standard Analysis

Non-standard models of Peano arithmetic may seem like a mere curiosity, vaguely interesting but essentially useless, in particular in view of Tennenbaum's theorem.

A. Robinson realized in 1960, though, that this type of unintended model is the perfect framework for analysis: one can construct strange models of the reals that contain infinitesimal elements.

As a consequence, there is no need for limits in such a model.

In essence, differentiation is just a quotient operation $\frac{f(x+h) - f(x)}{h}$ and integrals are just sums.

The drawback is, of course, that someone trying to learn or apply calculus this way must already have a solid background in logic – perhaps unsurprisingly, non-standard analysis never really took off.

True Arithmetic

True arithmetic (TA) is defined as the theory of \mathcal{N} .

Of course, $\text{Cn}(\text{PA}) \subseteq (\text{TA})$ but because of non-standard models we are nowhere near equality: (PA) only proves theorems that are valid in all models.

$$\forall \mathcal{A} \in \text{Mod}(\text{PA}) \mathcal{A} \models \varphi \text{ implies } (\text{PA}) \vdash \varphi$$

This is most emphatically NOT the same as

$$\varphi \in (\text{TA}) \text{ implies } (\text{PA}) \vdash \varphi$$

There are statements of arithmetic that hold in \mathcal{N} but not in non-standard models.

Exercises

Exercise 16. Show that if Γ has arbitrarily large finite models then Γ must have an infinite model.

Conclude that there are infinite fields of characteristic $p > 0$.

Exercise 17. Show that every partial order can be embedded into a total order.

Exercise 18. Show that there is no FO set of axioms Γ that characterizes finiteness in the sense that $c\mathcal{A} \models \Gamma$ if, and only if, $c\mathcal{A}$ is infinite.

Incompleteness

Gödel Incompleteness

So how about (PA)? Is (PA) complete, and if not can we augment it a bit to obtain a complete theory?

Sadly, Kurt Gödel showed in 1931 that this is impossible: there are lots of facts about the natural numbers that cannot be proven in (PA), nor in any other reasonable axiom system for arithmetic (e.g., $\text{Th}(\mathcal{N})$ is not a good choice).

Theorem 8. *Suppose (PA) is consistent. There is a sentence of arithmetic such that (PA) neither proves nor refutes this sentence.*

But of course \mathcal{N} must be a model of this sentence φ or its negation $\neg\varphi$, it's just that (PA) is not strong enough to determine which.

One might still hope that such sentences are horribly complicated, but in fact a single universal quantifier suffices.

Gödel Incompleteness, II

Gödel's second Incompleteness Theorem pins down one such sentence explicitly.

Theorem 9. *If (PA) is consistent then its consistency cannot be proven in (PA).*

This does not mean that we cannot prove (PA) to be consistent, we just cannot do it inside of the system (transfinite induction to ε_0 suffices, though, or you can just believe that \mathcal{N} is a model).

Still, the missing theorems tend to be a bit weird, they don't seem to matter much in "real life", that is, in applications of number theory.

Note the hedge here, in 1975 Paris and Harrington showed how to construct statements of finite combinatorics that are true but not provable in (PA).

Programs and (PA)

How does this relate to computer science?

Suppose P is a program in some standard programming language that computes a numerical function $\hat{P} : \mathbb{N} \rightarrow \mathbb{N}$.

Write \underline{n} for the term $1 + 1 + \dots + 1$ that represents the natural number n in (PA). Then there is a formula $\phi(x, y)$ of arithmetic such that

- $\hat{P}(m) = n$ implies $(\text{PA}) \vdash \phi(\underline{m}, \underline{n})$.
- $(\text{PA}) \vdash \phi(x, y) \wedge \phi(x, z) \rightarrow y \approx z$.

But even though \hat{P} is total, (PA) may well not be powerful enough to prove it: in general

$$(\text{PA}) \not\vdash \forall x \exists y \phi(x, y).$$

(Un-)Decidability

The Entscheidungsproblem for a Theory

If we cannot prove all true statements of arithmetic, can we at least give a decision algorithm for them?

It is a direct consequence of the way proof systems are built that all formulae provable from a decidable set of axioms are semi-decidable: we can systematically enumerate all axioms and all proofs in the system based on these axioms – in principle, efficiency is not a consideration here.

Theorem 10. *Let Γ be decidable. Then $\text{Cn}(\Gamma)$ is semi-decidable.*

So for $\text{Cn}(\Gamma)$ to be decidable we only need a semi-algorithm for the non-theorems, the sentences that do not follow from Γ . Alas, there is no obvious general way to obtain such an algorithm. But sometimes it happens that the set of axioms is very rich and "knows" facts about non-theorems in the following sense:

$$\Gamma \not\vdash \varphi \quad \text{implies} \quad \Gamma \vdash \neg\varphi$$

Completeness and Decidability

Lemma 4. *Suppose T is a complete and axiomatizable theory. Then T is decidable.*

Proof. It suffices to show that the complement of T is semi-decidable. But $\varphi \notin T \iff \neg\varphi \in T$, done. \square

Unfortunately, completeness of a theory is not all that easy to check in general. Here is one valuable test.

Let's assume throughout that the language we are using is countable. A set of sentences Γ is κ -categorical for some cardinal $\kappa \geq \aleph_0$ if all models of Γ of size κ are isomorphic.

Theorem 11. *Los-Vaught Test*

Let T be a theory with no finite models. If T is κ -categorical for some cardinal $\kappa \geq \aleph_0$ then T is complete.

Algebraically Closed Fields

Let (ACF_0) be the theory of algebraically closed fields of characteristic 0.

Clearly, all models of (ACF_0) are infinite.

Suppose \mathcal{A} is a model of (ACF_0) of cardinality $\kappa = |\mathbb{R}|$. Then \mathcal{A} must be an extension field of \mathbb{Q} . The transcendence degree of \mathcal{A} is κ . But then it is easy to construct an isomorphism between any two such models.

Hence (ACF_0) is complete.

Exercise 19. *Fill in the details of the last argument.*

Exercise 20. *Show that the theory of atomless Boolean algebras is complete.*

Exercise 21. *Show that the theory of (\mathbb{N}, S) is complete.*

Arithmetic

Peano arithmetic is not complete and indeed undecidable.

Theorem 12. *K. Gödel 1931, J.B. Rosser, 1936*

Peano arithmetic is undecidable.

Two questions arise naturally:

- Is there a large subsystem of Peano arithmetic that is still decidable?
- Is there a small subsystem of Peano arithmetic that is still undecidable?

To avoid undecidability we have to remove multiplication. Presburger arithmetic uses the language $\mathcal{L}(+, -, 0, 1; <)$ of signature $(2, 2, 0, 0; 2)$ and axiomatizes these operations over the integers \mathbb{Z} .

Theorem 13. *M. Presburger, 1929*

Presburger arithmetic is decidable.

But note that the algorithm is not practical (triple exponential). In fact, even for quantifier-free formulae the problem is \mathbb{NP} -hard.

System Q

For the second question it turns out that indeed the full power of Peano arithmetic is not even needed for undecidability, the following rather weak fragment, called Q suffices:

successor

$$\begin{aligned} S(x) \neq 0 & & S(x) \approx S(y) \rightarrow x \approx y \\ x \neq 0 \rightarrow \exists y (x \approx S(y)) & & \end{aligned}$$

addition

$$x + 0 \approx x \qquad x + S(y) \approx S(x + y)$$

multiplication

$$x \cdot 0 \approx 0 \qquad x \cdot S(y) \approx (x \cdot y) + x$$

Algebra

Theorem 14. *The theory of Abelian groups is decidable. But the theory of general groups is undecidable.*

This result is rather remarkable since the axioms are nearly identical: only one commutativity axiom is needed to enforce decidability.

This decidability result reflects nicely the fact that Abelian groups are much less complicated than general groups.

In general, many familiar structures in algebra are undecidable: rings, commutative rings, integral domains, fields, fields of characteristic 0.

Boolean algebra, on the other hand, is decidable.

The Reals

For important structures \mathcal{A} such as the rationals and reals, the question arises whether $\text{Th}(\mathcal{A})$ is decidable (regardless of attempts at axiomatization).

Theorem 15. *J. Robinson, 1948*

The theory of the rationals with addition and multiplication is undecidable.

This is in sharp contrast to a famous theorem by Tarski concerning the real numbers.

Theorem 16. *A. Tarski, 1948*

The theory of the reals with addition and multiplication is decidable.

As a consequence, basic geometry is decidable.

The theorem is proved by a very interesting technique that provides a direct decision algorithm: *quantifier elimination*.

Tarski's original method was highly inefficient, though (not bounded by a stack of exponentials).

Quantifier Elimination

Definition 9. A theory T admits **quantifier elimination** if for every formula φ there is a quantifier-free formula φ_0 such that $T \vdash \varphi \leftrightarrow \varphi_0$.

It actually suffices to show that one can eliminate existential quantifiers in a formula

$$\exists x (A_1 \wedge A_2 \wedge \dots \wedge A_n)$$

where all the A_i are literals (atomic formulae or negations thereof).

Note that on the face of it this may seem utterly hopeless: the existence of x may depend on the values of the free variables. It is not clear how to capture this dependence without quantifiers.

Exercise 22. Prove that full quantifier elimination follows from the weaker form.

Q-Elimination for the Successor Function

Consider the theory of the simple structure $\mathcal{N}_S = \langle \mathbb{N}, S, 0 \rangle$.

We can give an axiom system Γ for this theory as follows:

$$\begin{aligned} S(x) &\neq 0 \\ S(x) \approx S(y) &\rightarrow x \approx y \\ y \neq 0 &\rightarrow \exists x S(x) \approx y \\ S^n(x) &\neq x \quad \text{schema } n \geq 1 \end{aligned}$$

It is quite obvious that $\text{Cn}(\Gamma) \subseteq \text{Th}(\mathcal{N}_S)$ but because of non-standard models the obvious direction is far from obvious.

What does an arbitrary, non-standard model \mathcal{A} of Γ look like?

Intuitively, we must have

$$A = \mathbb{N} \cup \mathbb{Z} \cup \mathbb{Z} \cup \mathbb{Z} \dots$$

where the unions are meant to be disjoint: There is one copy of \mathbb{N} , the standard model, plus a number of copies of \mathbb{Z} .

Completeness of Γ

We can make this precise by showing that $\exists n \geq 0 (S^n(x) = y \vee S^n(y) = x)$ is an equivalence relation on A with the equivalence classes as indicated.

At any rate, the cardinality of A is $\aleph_0 + \aleph_0 \kappa$ where κ is the number of copies of \mathbb{Z} .

But then any two models of Γ with the same κ must be isomorphic. Hence by Los-Vaught $\text{Cn}(\Gamma) = \text{Th}(\mathcal{N}_S)$ is complete. So we have decidability.

To get a real algorithm we show that quantifier elimination holds. Consider

$$\exists x (A_1 \wedge A_2 \wedge \dots \wedge A_n)$$

We may safely assume that x occurs in each A_i . Now the positive atomic formulae must be of the form

$$S^n(x) \approx t.$$

If $t \approx S^m(x)$ the literal can easily be replaced by \perp or \top . So we only have to deal with $S^n(x) \approx S^m(y)$ and $S^n(x) \approx 0$.

Completeness, II

If all the literals are negative then we can replace the whole formula by \top .

So suppose $A_1 = S^n(x) \approx t$ is positive. But then we can replace A_1 by

$$t \neq 0 \wedge t \neq S(0) \wedge \dots \wedge t \neq S^{n-1}(0).$$

Any other literal $S^r(x) \approx z$ is replaced by $S^r(t) \approx S^m(z)$ (and likewise for negative ones).

But then none of the literals contains x any more, so we can drop the quantifier.

Note that if we apply our elimination process to a sentence we wind up with a quantifier-free sentence, which must be a Boolean combination of pieces $S^m(0) \approx S^n(0)$.

Exercise 23. Fill in all the details in the argument.

FOL is Undecidable

In fact, even if we disregard attempts to axiomatically describe some reasonable class of structures and only consider the logic itself we run into undecidability.

Theorem 17. First order logic is undecidable: it is undecidable whether a sentence in FOL is derivable from the empty set of axioms.

Theorem 18. Satisfiability in first order logic is undecidable: it is undecidable whether a sentence in FOL has a model.

One has to be a bit careful about having enough function and relation symbols around for these results to hold. E.g., one binary relation symbol suffices, as does one unary and one ternary function symbol.

The point is: for any underlying language that is strong enough to be useful provability and satisfiability are undecidable.

Automatic Verification

From the point of view of verification this is a disaster: one cannot hope in general to automatically check specifications that are written in FOL.

For some limited areas of discourse there are decision algorithms. For example, the theory of real numbers is decidable (quantifier elimination, a result by Tarski). As a result, certain aspects of geometry are decidable (though the algorithms are not particularly efficient).

To get around this problem one has to regroup and develop languages that are expressive enough to state correctness properties, but still weak enough to allow for decision algorithms.