MT5867 Logic and Set Theory (Part 2)

Nik Ruškuc

March 13, 2023

Contents

Chapter 1.
Zermelo–Fraenkel Axiomatic Set Theory

1. The Axioms, Part 1

In this chapter we introduce an first order theory which is widely accepted as an accurate formal interpretation of naive set theory.

The first order language we will be working with is as simple as they get: just one binary relation, written as $\in$. We write $x \in y$ (instead of $(x, y) \in \in$!), and say x *is a member of* y, or x *is in* y, or y *contains* x. In addition, of course, we will have the equality relation.

The axioms are of several different types. Some are single axioms and are easy to state; we list these first. Others are actually infinite collections of axioms, and we treat them in the next section. Finally, thereis the axiom of choice, which requires a fair bit of preparation to state, and we leave it for a separate section.

Axiom 1: Extension. If two sets have the same members, they are equal:

$$(\forall x)(\forall y)((\forall z)(z \in x \Leftrightarrow z \in y) \Rightarrow x = y).$$

Axiom 2: Empty Set. There exists a set $\emptyset$ with no elements:

$$(\exists x)(\forall y)(y \notin x).$$

Strictly speaking, $\emptyset$ is our 'private' abbreviation for the set whose existence is guaranteed by the axiom (and which is unique by the Axiom of Extension). Every time this symbol occurs in the formula, it needs to be replaced by its definition. For instance, the formula $\emptyset \in z$ is an abbreviation for

$$(\forall y)(y \notin x) \Rightarrow x \in z.$$

Analogous conventions will hold for all the sets whose existence is asserted by the subsequent axioms, and thereafter.

Axiom 3: Pairs. For any sets x, y, there is a set $\{x, y\}$ whose elements are precisely x and y:

$$(\forall x)(\forall y)(\exists z)(\forall t)(t \in z \Leftrightarrow (t = x \vee t = y)).$$

There is no assumption that x and y are distinct here. When $x = y$ we write just $\{x\}$.

Axiom 4: Union. For any set x, there is a set $\bigcup x$ whose elements are precisely members of members of x:

$$(\forall x)(\exists y)(\forall z)(z \in y \Leftrightarrow (\exists t)(t \in x \wedge z \in t)).$$

Axiom 5: Power Set. For any sets x, there is a set $\mathcal{P}x$ whose elements are precisely the subsets of x:

$$(\forall x)(\exists y)(\forall z)(z \in y \Leftrightarrow (\forall t)(t \in z \Rightarrow t \in x)).$$

If we introduce an abbreviation $z \subseteq x$ to mean $(\forall t)(t \in z \Rightarrow t \in x)$ the axiom simplifies to

$$(\forall x)(\exists y)(\forall z)(z \in y \Leftrightarrow z \subseteq x).$$

Axiom 6: Infinity. There exists a set which contains $\emptyset$, and for each of its elements y it also contains its 'successor' $y \cup \{y\}$:

$$(\exists x)(\emptyset \in x \wedge (\forall y)(y \in x \Rightarrow y \cup \{y\} \in x)).$$

We cannot say that such a set should be unique by the Extension Axiom, as x may contain further elements.

Axiom 7: Selection. Let $\phi = \phi(x, p_1, \ldots, p_n)$ be a first order formula with free variables $x, p_1, \ldots, p_n$, and let y be a set. Then, for any fixed $p_1, \ldots, p_n$, there exists a set which consists precisely of all $x \in y$ such that the formula $\phi(x, p_1, \ldots, p_n)$ holds:

$$(\forall p_1) \ldots (\forall p_n)(\forall y)(\exists z)(\forall x)(x \in z \Leftrightarrow x \in y \wedge \phi(x, p_1, \ldots, p_n)).$$

Unlike the previous axioms, this is not a single formula, but an infinite collection (schema) of formulas. The variables $p_1, \ldots, p_n$ can be regarded as parameters. The simplest instance of this axiom is when $\phi = \phi(x)$ has no parameters:

$$(\forall y)(\exists z)(\forall x)(x \in z \Leftrightarrow x \in y \wedge \phi(x)).$$

This says that for any set y and formula $\phi(x)$ the collection of all members $x \in y$ which satisfy ϕ is a set. We will write $\{x \in y \,:\, \phi(x)\}$ for this set.

As an example of the use of the Axiom of Selection, let $\phi(x, p)$ be the formula $x \in p$; the axiom now reads

$$(\forall p)(\forall y)(\exists z)(\forall x)(x \in z \Leftrightarrow x \in y \wedge x \in p).$$

This the intersection of p and y. Let us denote this set as $p \cap y$.

Axiom 8: Foundation. Any non-empty set has a member disjoint from it.

$$(\forall x)(x \neq \emptyset \Rightarrow (\exists y)(y \in x \wedge x \cap y = \emptyset)).$$

We will see that this axiom reflects Zermelo's idea of 'constructing' sets in stages, and 'guarding against' including 'intruders' such as the set of all sets.

2. Axioms, Part 2: Functions

Our next axiom, Replacement Axiom, intuitively asserts that the image of a set under a function will again be a set. The functions in question will be those defined by a formula. Such a formula would have two free variables, say $\phi = \phi(x, y)$, and would need to satisfy the property that for every x there exists at most one y such that $\phi(x, y)$ holds. (Thus we are in fact talking about *partial* functions.) Again, as in the Axiom of Selection, we will also allow additional parameters in ϕ. This time, to reduce clutter, we will write $\overline{p}$ for $(p_1, \ldots, p_n)$.

Axiom 9: Replacement. For a first order formula $\phi = \phi(x, y, \overline{p})$ with free variables x, y and $\overline{p} = (p_1, \ldots, p_n)$, if ϕ is function-like, then the set of all images of elements of a set z under this function is a set:

$$\begin{aligned}(\forall \overline{p})((\forall x)(\forall y_1)(\forall y_2)\big[\big(\phi(x, y_1, \overline{p}) \wedge \phi(x, y_2, \overline{p}) \Rightarrow y_1 = y_1\big) \\ \Rightarrow (\forall z)(\exists u)(\forall y)\big(y \in u \Leftrightarrow (\exists x)(x \in z \wedge \phi(x, y, \overline{p}))\big)\big].\end{aligned}$$

Our final axiom is the Axiom of Choice. In order to write this axiom down in the first order language, we need to do quite some work.

The Axiom of Pairs guarantees the existence of a set $\{x, y\}$for any sets x, y. We can use this three times, to establish the existence of the set of the form

$\{\{x\},\{x,y\}\}$. Such a set is called *ordered pair*, and denoted by (x,y). It can be seen by using the Axiom of Extension that

$$(x,y)=(z,t)\Rightarrow x=z\wedge y=t$$

is a consequence of the axioms. The formula

$$\mathsf{OP}(z):(\exists x)(\exists y)(z=(x,y))$$

is the first order expression saying that z is an ordered pair.

Functions are then defined as certain sets of ordered pairs:

$$\begin{aligned}\mathsf{Fn}(f):(\forall u)(u\in f\Rightarrow(\exists x)(\exists y)(u=(x,y)))\\ \wedge(\forall x)(\forall y_1)(\forall y_2)(((x,y_1)\in f\wedge(x,y_2)\in f)\Rightarrow y_1=y_2).\end{aligned}$$

Now, suppose that f is a function. The formula $\phi(x,y):(\exists z)(x=(y,z))$ satisfies the conditions of the Replacement Axiom. Indeed if $\phi(x,y_1)$ and $\phi(x,y_2)$ hold that means that there exist z_1,z_2 such that $x=(y_1,z_1)$ and $x=(y_2,z_2)$. But then $(y_1,z_1)=(y_2,z_2)$ and hence $y_1=y_2$. Applying the Replacement Axiom with this formula and the set f yields the existence of a set consisting of all elements y such that $(y,z)\in f$ for some z. This is called the *domain* of f and is denoted by $\mathsf{dom}(f)$. Likewise, the collection of all y such that $(x,y)\in f$ is also a set, called the *image* and denoted $\mathsf{im}(f)$.

Axiom 10: Choice. For any function f defined on a set I, and having the property that $f(i)$ is a non-empty set for all $i\in I$ there is a function g defined on I with the property that $g(i)\in f(i)$ for all $i\in I$:

$$\begin{aligned}(\forall f)\big[\mathsf{Fn}(f)\wedge(\forall u)(\forall v)((u,v)\in f\Rightarrow v\neq\emptyset)\Rightarrow\\ \Rightarrow(\exists g)(\mathsf{Fn}(g)\wedge\mathsf{dom}(g)=\mathsf{dom}(f)\wedge\\ \wedge(\forall u)(\forall v)(\forall w)((u,v)\in g\wedge(u,w)\in f\Rightarrow v\in w))\big].\end{aligned}$$

Pretty complicated! But at least it is a single formula:-)

3. Axioms: Commentary

1. These are the axioms of the Zermelo-Fraenkel axiomatic set theory. The theory defined by the first nine will be denoted by ZF; when the Axiom of Choice is included as well, we denote the theory by ZFC.

2. The axioms are not independent. For example, the Empty Set Axiom can actually be derived from the Selection Axiom. Taking $\phi(x)$ to be any false formula (e.g. $x \neq x$) we obtain

$$(\forall y)(\exists z)(\forall x)(x \notin z).$$

The set z is the empty set!

3. Also, the Replacement Axiom implies the Selection Axiom. Consider a formula $\phi(x)$ with a single free variable (ignoring parameters for simplicity), and let b be a set. Consider the formula $\psi(x, y) : x = y \wedge \phi(x)$. This formula satisfies the assumption of the Replacement Axiom, and we get the existence of the set

$$\{y : x \in b \wedge \psi(x, y)\} = \{y : x \in b \wedge x = y \wedge \phi(x)\} = \{x \in b \ : \ \phi(x)\}.$$

4. The Foundation Axiom implies the following formula:

$$(\forall x)(x \notin x).$$

No set is an element of itself! Indeed, for any x, we have that $\{x\}$ is a set. It is non-empty, so it has an element y such that $y \cap \{x\} = \emptyset$. But $y = x$, and so $x \notin x$.

Now consider the true formula

$$(\exists x)(\forall y)(y \in x) \Rightarrow (\exists x)(x \in x).$$

Take the contrapositive:

$$\neg(\exists x)(x \in x) \Rightarrow \neg(\exists x)(\forall y)(y \in x).$$

Use MP to obtain

$$\neg(\exists x)(\forall y)(y \in x).$$

There exists no set that contains all sets!

The Foundation Axiom also implies that there is no infinite sequence of the form $\cdots \in x_3 \in x_2 \in x_1$. Although as expressed, this is not a first order sentence, it can actually be formulated as one. But we will not do any of this here.

However, this does not mean that it is 'forbidden to speak' of all sets. The entire ZFC does precisely that: it is a theory of all sets. For instance, the

obviously correct formula $(\forall x)(\emptyset \subseteq x)$ is a true formula about all sets. The point is simply that there is no set which contains all sets as elements.

5. It might seem tempting to replace the Selection Axiom by a more powerful, simpler formula, which asserts that the collection of all objects satisfying a first order formula is a set:

$$(\exists z)(\forall x)(x \in z \Leftrightarrow \phi(x)).$$

This would be ill-advised: taking $\phi(x)$ to be $x = x$ or any other tautology would yield

$$(\exists z)(\forall x)(x \in z),$$

the set of all sets!

4. Development

From here, the development of the ZFC system proceeds by establishing that the cornerstones of naive set theory all have expressions within the ZFC. We have seen the beginnings of this in Section 2. This includes:

- Standard set-theoretic constructions: intersection, difference, complement.
- The algebraic laws involving the set operations, e.g. associativity of $\cup$ and $\cap$, or the distributivity of $\cap$ over $\cup$ (or vice versa).
- Operations and properties of mappings: composition, surjections, injections, bijections, etc.
- Relations and their properties: reflexivity, symmetry, asymmetry, transitivity, equivalence relations, order relations, total orders, well-orders.
- Ordinals: to be an ordinal is a first order property within ZFC.
- Cardinals.
- Ordinal and Cardinal arithmetic, etc. etc.
- Number systems: The set of natural numbers $\mathbb{N}_0$ is the smallest infinite ordinal. It is also the smallest set guaranteed by the Infinity Axiom.

- Peano arrithmetic on $\mathbb{N}_0$: arrithmetic operations, ordering $\leq$, divisibility, etc.
- Number systems $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Developing all this systematically would take a course in its own right, so we will leave it at this point.

Let us briefly discuss models of set theory. The first question, of course, is whether ZFC is consistent (i.e. whether it has a model). In a sense, this question almost does not make sense stated just like that. Obviously, if ZFC is inconsistent we may be able to show that by simply stumbling on a proof of a contradiction. But, if this is not the case, and we would like to prove its consistency, within which mathematical framework (i.e. axiomatic system) would we do that? What is certainly the case is that the consistency of ZFC cannot be proved within ZFC itself – such results will be discussed later in the course.

So, it is therefore reasonable to work under the assumption that ZFC is consistent – if it isn't, our intuition about the nature of sets has decived us (for over 100 years!), and we have been building castles in the sand. So it must have a model. But our 'intuitive sets' *will not* be such a model: a model consists of a *set* and and interpretation. But the collection of all sets is not a set!

Still, if ZFC is consistent it *does* have a model. This model would be an (intuitive) set U with a binary relation which will interpret $\in$. This turns U into a digraph! Models of set theory are certain digraphs! The elements of U correspond to sets; and arrow $u \to v$ corresponds to $u \in v$. But what about U itself – is it not the set of all sets? Well, yes and now, depending on where you stand: The intuitive set U is indeed the collection of all ZFC sets; but it itself is not a ZFC set.

More confusingly still: any model of ZFC will not be finite – this is a consequence of several axioms, e.g. Infinity, or Power Set (repeatedly). Therefore Löwenheim–Skolem Theorem gives us:

Theorem 4.1. *ZFC has a countable model.*

This seems counter-intuitive: ZFC certainly guarantees existence of uncountable sets (such as $\mathcal{P}\mathbb{N}_0$). How can you fit an uncountable set into a countable model? The issue here is what uncountability will mean in the

model U. It need not mean uncountably many elements of a set. Instead, it will mean the existence of a set (a vertex u in U), such that if n is the vertext correponding to the natural numbers $\mathbb{N}_0$, there is no vertex f in U which represents a bijective mapping with the domain n and image r.

We said that you can re-create real numbers with ZFC. So, in our model U, there will be a vertex r interpreting this set, and it will have at most countably many other sets as elements. Is this really so in odds with our intuitive perception of $\mathbb{R}$? We say $\mathbb{R}$ has uncountably many elements. But, in thinking about $\mathbb{R}$ (and proving theorems about it) we have only ever encountered finitely many specific numbers, or, if accept infinite algorithmic constructions as existence, then countably many of them.

You may think that this rather undermines ZFC as a theory – that is a valid point of view. But, consider: anything you prove in ZFC you can prove in U as well. So why are we 'unhappy' with U? Perhaps we will discover a statement in U that is not a consequence of ZFC (in fact, such statements must exist – to be discussed later). But if you find such a statement, and it seems at odds with our intuition about sets, we can add its negation to ZFC, and the whole game would start again.

Finally, a few words about sets vs. classes. We have seen that there is no set containing all sets. But there is a *formula* which describes all sets – any tautology would do. Thus, given a model $\mathcal{U}$ of ZF, and a formula $\phi(u_1, \ldots, u_n, x)$ with parameters from $\mathcal{U}$ and one free variable x, we can take $\phi(u_1, \ldots, u_n, x)$ to stand for the 'class' of all sets satisfying the formula. Within the model, this would be a set (in its intuitive sense) of elements of $\mathcal{U}$ such that there is no set (in the formal sense of ZF) which consists precisely of those sets. Every formal set u is a class: the formula $x \in u$ describes precisely its elements. Proper classes are classes that are not sets. One can talk about the intersection and union of two classes C_1 and C_2, say defined by formulas ϕ and ψ: the former is defined by the formula $\phi \wedge \psi$, the latter by $\phi \vee \psi$. But one cannot form the power-set of a class C defined by ϕ: this would involve taking a disjunction of all the formulas ψ such that $\psi \Rightarrow \phi$ is a theorem of ZFC.

Chapter 2.
Peano Arithmetic

5. The Axioms

In the previous chapter we have seen what an attempt to formalise set theory into a first order theory would look like. It was clear even from the limited development we undertook that things become very complicated very quickly, and that there are serious obstacles in principle to e.g. discussing consistency of the theory. One might wonder whether such problems would disappear if one adopted a more limited task, and attempted to axiomatise a more basic part of mathematics. In that regard, the basic arithmetic of natural numbers seems a perfect candidate.

Our language will consist of

- one constant symbol 0, interpreted as the natural number 0;
- one unary operation s, interpreted as the successor operation $x \mapsto x + 1$;
- two binary operations $+$ and $\cdot$ interpreted as addition and multiplication on natural numbers.

Our theory will be a theory with equality; the axioms of first order logic, as well as those of equality, will be taken as read.

The special axioms, involving $0, s, +, \cdot$ are:

(PA1) $(\forall x)(0 \neq s(x))$

(PA2) $(\forall x)(\forall y)(s(x) = s(y) \Rightarrow x = y)$

(PA3) $(\forall x)(x + 0 = x)$

(PA4) $(\forall x)(\forall y)(x + s(y) = s(x + y))$

(PA5) $(\forall x)(x \cdot 0 = 0)$

(PA6) $(\forall x)(\forall y)(x \cdot s(y) = x \cdot y + x)$

(PA7) $\big[\phi(0) \ \wedge \ (\forall x)(\phi(x) \Rightarrow \phi(s(x)))\big] \Rightarrow (\forall x)(\phi(x))$.

Unlike the axioms of set theory, these axioms should be immediately acceptable to everyone, as reflecting some very basic properties of arithmetic, and only brief commentary is needed here:

- The first two axioms are about s: they assert that 0 is not the successor of any number, and that s is injective.
- Axioms (PA3), (PA4) combined can be viewed as an inductive definition of addition.
- Likewise Axioms (PA5), (PA6) combined can be viewed as an inductive definition of multiplication.
- Finally Axiom (PA7) is an expression of the principle of induction in first order language. In it ϕ stands for any formula with a free variable x.
- Perhaps one point worth noting is that (PA7) is indexed by first order formulas, while the 'intuitive' principle of induction talks about arbitrary subsets of $\mathbb{N}_0$. This should be non-controversial: in this theory we are *precisely* trying to establish the arithemtic without resorting to set theory.

The resulting first order theory is called *Peano Arithmetic* (PA). In what follows we will establish a (long!) sequence of theorems in this theory, which will eventually lead us to Gödel's Theorems. In doing so, we will accept several conventions:

- In formal proofs we will use the axioms, and indeed theorems, of the first order logic, including those of equality, without special reference; we will just write FOL instead.
- When there is no danger of ambiguity, we will write $\vdash$ for $\vdash_{\text{PA}}$.

- We know that for any formula ϕ and $(\forall x)\phi$ are equivalent, provided x has no bound occurences in ϕ. In particular, we will tend to write our formulas without the universal quantifiers at the beginning. For instance, we would write (and use) (PA2) as

$$s(x) = s(y) \Rightarrow x = y.$$

- We also know that $(\forall x)(\phi(x)) \Rightarrow \phi(t)$ is a valid formula for any term t which is free for substitution in ϕ. Thus, for example, from (PA2) we can deduce $s(t_1) = s(t_2) \Rightarrow t_1 = t_2$ for any terms t_1, t_2. This will be used throughout with further discussion.

- From (PA7) and (MP) we obtain

$$\phi(0),\ \phi(x) \Rightarrow \phi(s(x)) \vdash \phi(x).$$

  Thus, in what follows, when we are proving a theorem ϕ it will come in two parts: one establishing $\phi(0)$, and the other establishing $\phi(x) \Rightarrow \phi(s(x))$.

6. Building up basic arithmetic

We now start on the long journey of exhibiting consequences of our theory, which comprise the basic facts of arithmetic: properties of basic operations, ordering, and divisibility. There will be a large number of these results. We are going to give proofs only to a small sample; some will be done as tutorial exercises; and all the remaining ones are good resources for practice.

(PT8) $\vdash 0 + x = x$.

Denoting this formula by ϕ, we see that $\phi(0)$ is $0 + 0 = 0$, which follows from (PA3). Next we show $\phi(x) \vdash \phi(s(x))$:

1.	$0 + x = x$	hypothesis
2.	$s(0 + x) = s(x)$	1, FOL
3.	$0 + s(x) = s(0 + x)$	(PA4)
4.	$0 + s(x) = s(x)$	3, 2, FOL

We conclude that $\vdash 0 + x = x$ using (PA7).

(PT9) $\vdash s(x) + y = s(x + y)$.

The proof is by induction on y; so denote this formula by $\phi(y)$. The formula $\phi(0)$ is $s(x) + y = s(x + y)$ which follows from (PA3) and FOL. For $\phi(y) \vdash \phi(s(y))$ we have:

1.	$s(x) + y = s(x + y)$	hypothesis
2.	$s(s(x) + y) = s(s(x + y))$	FOL
3.	$s(x) + s(y) = s(x + s(y))$	(PA4)

(PT10) $\vdash x + y = y + x$.

Induction on y. The first part is $x + 0 = 0 + x$ which follows from (PA3), (PT8) and FOL. The second part is $x + y = y + x \vdash x + s(y) = s(y) + x$, which follows from hypothesis, (PA4), (PT9) and FOL.

(PT11) $\vdash (x + y) + z = x + (y + z)$.

(PT12) $\vdash 0x = 0$.

(PT13) $\vdash s(x)y = xy + y$.

(PT14) $\vdash xy = yx$.

(PT15) $\vdash x(y + z) = xy + xz$.

(PT16) $\vdash (x + y)z = xz + yz$.

(PT17) $\vdash (xy)z = x(yz)$.

(PT18) $\vdash x + z = y + z \Rightarrow x = y$.

In what follows we denote the terms 0, $s(0)$, $s(s(0))$ etc. by $\overline{0}$, $\overline{1}$, $\overline{2}$ etc. Thus for every natural number n we have a term $\overline{n}$.

(PT19) $\vdash x + \overline{1} = s(x)$.

(PT20) $\vdash x\overline{1} = x$.

(PT21) $\vdash x\overline{2} = x + x$.

(PT22) $\vdash x + y = 0 \Rightarrow (x = 0 \wedge y = 0)$.

Denote this formula by $\phi(y)$. Then $\phi(0)$ follows from (PA3). Next, note that $x + s(y) = 0$ is false, because $x + s(y) = s(x + y) \neq 0$ by (PA4), (PA1). It now follows that $x + s(y) \Rightarrow (x = 0 \wedge s(y) = 0)$ is true (tautology), and hence $\vdash \phi(y) \Rightarrow \phi(s(y))$ (another tautology).

(PT23) $\vdash x \neq 0 \Rightarrow (xy = 0 \Rightarrow y = 0)$.

(PT24) $\vdash x + y = 1 \Rightarrow (x = 0 \wedge y = \overline{1}) \vee (x = \overline{1} \wedge y = 0)$.

(PT25) $\vdash xy = \overline{1} \Rightarrow x = \overline{1} \wedge y = \overline{1}$.

(PT26) $\vdash x \neq 0 \Rightarrow (\exists y)(x = s(y))$.

(PT27) $\vdash z \neq 0 \Rightarrow (xz = yz \Rightarrow x = y)$.

(PT28) $\vdash (x \neq 0 \wedge x \neq \overline{1} \Rightarrow (\exists y)(x = s(s(y)))$.

In the next three theorems we want to prove some properties that hold for all terms $\overline{n}$. This is done by induction on n. It is important to note that this is not an application of (PA7), but induction in our 'intuitive'/'naive' natural numbers, as parts of ordinary language.

(PT29) For any natural numbers $m \neq n$ we have $\vdash \overline{m} \neq \overline{n}$.

We prove the contrapositive, i.e. that $\vdash \overline{m} = \overline{n}$ implies $m = n$, and appeal to an appropriate tautology. The proof is by 'meta-induction' on n. For $n = 0$, the assumption $\vdash \overline{m} = 0$ implies $m = 0$ by (PA1). Suppose $n > 0$. Again, we cannot have $m = 0$. So our assumption reads $s(\overline{m-1}) = s(\overline{n-1})$. By induction $m - 1 = n - 1$, and hence $m = n$.

(PT30) For any natural numbers m, n we have $\vdash \overline{m} + \overline{n} = \overline{m+n}$ and $\vdash \overline{m}\,\overline{n} = \overline{mn}$.

At this point we can record the following significant facts about the theory PA:

Theorem 6.1. *Every model of PA is infinite. PA has models of every infinite cardinality.*

Proof. By (PT29), in any interpretation of our theory, the terms $\overline{n}$ are all pairwise distinct. The second statement is an immediate application of the Löwenheim–Skolem Theorem. ■

The next step is to add the natural ordering to our theory. We will write

$$\begin{aligned} x < y \quad & \text{for } (\exists z)(z \neq 0 \wedge x + w = y) \\ x \leq y \quad & \text{for } x < y \vee x = y. \end{aligned}$$

We will also use $x > y$, $x \not< y$ etc. with obvious meanings.

There follows a long sequence of theorems of PA, establishing the properties of these formulas, and their relationship with the basic operations. We just list them here, in case we need to refer to them later on. They are certainly not worth memorising!

(PT31) $\vdash x \not< x$.

(PT32) $\vdash x < y \wedge y < z \Rightarrow x < z$.

(PT33) $\vdash x < y \Rightarrow y \not< x$.

(PT34) $\vdash x < y \Rightarrow x + z < y + z$.

(PT35) $\vdash x \leq x$.

(PT36) $\vdash x \leq y \wedge y \leq z \Rightarrow x \leq z$.

(PT37) $\vdash x \leq y \Rightarrow x + z \leq y + z$.

(PT38) $\vdash x \leq y \wedge y < z \Rightarrow x < z$.

(PT39) $\vdash 0 \leq x$.

(PT40) $\vdash 0 < s(x)$.

(PT41) $\vdash x < y \Leftrightarrow s(x) \leq y$.

(PT42) $\vdash x \leq y \Leftrightarrow x < s(y)$.

(PT43) $\vdash x < s(x)$.

(PT44) $\vdash \overline{n} < \overline{n+1}$ for all n.

(PT45) $\vdash x < y \Rightarrow x < y \vee y < x$.

(PT46) $\vdash x < y \vee x = y \vee x > y$.

(PT47) $\vdash x \leq y \vee y \leq x$.

(PT48) $\vdash x + y \geq x$.

(PT49) $\vdash y \neq 0 \Rightarrow x + y > x$.

(PT50) $\vdash y \neq 0 \Rightarrow xy \geq x$.

(PT51) $\vdash x \neq 0 \Rightarrow x > 0$.

(PT52) $\vdash x > 0 \wedge y > 0 \Rightarrow xy > 0$.

(PT53) $\vdash x \neq 0 \wedge y > 1 \Rightarrow xy > x$.

(PT54) $\vdash z \neq 0 \Rightarrow (x < y \Leftrightarrow xz < yz)$.

(PT55) $\vdash z \neq 0 \Rightarrow (x \leq y \Leftrightarrow xz \leq yz)$.

(PT56) $\vdash x \not< 0$.

(PT57) $\vdash x \leq y \wedge y \leq x \Rightarrow x = y$.

(PT58) $\vdash x = 0 \vee x = \overline{1} \vee \cdots \vee x = \overline{n} \Leftrightarrow x \leq \overline{n}$ for every natural number n.

From (PT44) and (PT36) we have $\overline{k} \leq \overline{n}$ for all $k \leq n$. It follows that

$$\vdash x = 0 \vee x = \overline{1} \vee \cdots \vee x = \overline{n} \Rightarrow x \leq \overline{n}.$$

We prove the converse implication by meta-induction on n. For $n = 0$, we have $\vdash x \leq 0 \Rightarrow x \leq 0$, as a consequence of (PT39), (PT57). Assume that for some n we have

$$\vdash x \leq \overline{n} \Rightarrow x = 0 \vee x = \overline{1} \vee \cdots \vee x = \overline{n}.$$

Take $x \leq \overline{n+1}$ as a hypothesis. By definition, this is $x < \overline{n+1} \vee x = \overline{n+1}$. Clearly $\vdash x = \overline{n+1} \Rightarrow x = 0 \vee x = \overline{1} \vee \cdots \vee x = \overline{n+1}$. Suppose $x < \overline{n+1}$. Then $x \leq \overline{n}$ by (PT42). By induction, we obtain $x = 0 \vee x = \overline{1} \vee x = \overline{n}$, which, in turn, implies $x = 0 \vee x = \overline{1} \vee x = \overline{n+1}$.

Next we introduce divisibility: $x \mid y$ stands for $(\exists z)(y = xz)$.

(PT59) $\vdash x \mid x$.

(PT60) $\vdash \overline{1} \mid x$.

(PT61) $\vdash x \mid 0$.

(PT62) $\vdash x \mid y \wedge y \mid z \Rightarrow x \mid z$.

(PT63) $\vdash y \neq 0 \wedge x \mid y \Rightarrow x \leq y$.

(PT64) $\vdash x \mid y \wedge y \mid x \Rightarrow x = y$.

(PT65) $\vdash x \mid y \Rightarrow x \mid (yz)$.

(PT66) $\vdash x \mid y \wedge x \mid z \Rightarrow x \mid (y + z)$.

And we finish this section with the statement of division with quotient and remainder.

(PT67) $\vdash y \neq 0 \Rightarrow (\exists u)(\exists v)\big[x = yu + v \wedge v < y \wedge (\forall u_1)(\forall v_1)((x = yu_1 + v_1 \wedge v_1 < y) \Rightarrow u = u_1 \wedge v = v_1)\big]$.

Giving a fully formal proof of this is quite tricky, but basically just because it is a complicated statement. The basic idea is to do induction on x. The case $x = 0$ follows from $0 = y0+0$ and $0 < y$, since $y \neq 0$ as hypothesis. The inductive step assumes that $x = yu + v$ with $v < y$. Then $s(x) = yu + s(v)$. If $s(v) < y$ we are done, and if $s(v) = y$ then $s(x) = ys(u) + 0$.

For uniqueness, assume that $x = yu+v \wedge v < y$ and also $x = yu_1+v_1 \wedge v_1 < y$. Now $u = u_1$, $u < u_1$ or $u_1 < u$ by (PT46). If $u = u_1$ then $v = v_1$ by (PT18). If $u < u_1$ then $u_1 = u + w$ for some $w \neq 0$. Then $yu + v = x = yu_1 + v_1 = y(u + w) + v_1 = yu + yw + v_1$. It follows that $v = yw + v_1$. Since $w \neq 0$ we have $yw \geq y$, and hence $v \geq y$, contradiction. Thus $u \not< u_1$, and an analogous argument shows $u_1 \not< u$.

7. Representable functions and relations

In the previous sections we have seen that the 'intuitive' natural numbers $\mathbb{N}$ can be 'seen' in the axiomatic theory PA, via the terms $\overline{n}$, $\mathbb{N}$. In this section we continue building this connection.

We are going to talk about functions and relations on the 'intuitive' natural numbers $\mathbb{N}$, and whether they can be 'seen' (we will say *represented*) in PA.

Definition 7.1. Let $R \subseteq \mathbb{N}^k$ be a k-ary relation. We say that R is *representable* in PA if there exists a formula $\phi(x_1, \ldots, x_k)$ with free variables $x_1, \ldots, x_k$ such that the following hold for all $n_1, \ldots, n_k \in \mathbb{N}$:

- if $(n_1, \ldots, n_k) \in R$ then $\vdash \phi(\overline{n}_1, \ldots, \overline{n}_k)$;
- if $(n_1, \ldots, n_k) \notin R$ then $\vdash \neg\phi(\overline{n}_1, \ldots, \overline{n}_k)$.

Example 7.2. The full relation is represented by any tautology. The empty relation is represented by any contradiction. The equality relation on $\mathbb{N}$ is represented by the formula $x = y$; this follows from (PT29). The relation $<$ on $\mathbb{N}$ can be represented by the formula $x < y$ in PA, which stands for $(\exists z)(z \neq 0 \wedge x + z = y)$; this follows from (PT29), (PT30).

Definition 7.3. A function $f : \mathbb{N}^k \to \mathbb{N}$ is *representable* if there exists a formula $\phi(x_1, \ldots, x_k, y)$ with free variables $x_1, \ldots, x_k, y$ such that the following conditions hold for all $n_1, \ldots, n_k, m \in \mathbb{N}$:

(i) if $f(n_1, \ldots, n_k) = m$ then $\vdash \phi(\overline{n}_1, \ldots, \overline{n}_k, \overline{m})$;

(ii) $\vdash (\exists_1 y)\phi(x_1, \ldots, x_k, y)$.

Recall that $\exists_1$ stands for 'there exists one and only one', which can be expressed by a formula.

It turns out that it is sufficient for (ii) to hold only for $x_i = \overline{n}_i$:

Lemma 7.4. *In Definition 7.3 one can replace* (ii) *by*

(ii') $\vdash (\exists_1 y)\phi(\overline{n}_1, \ldots, \overline{n}_k, y)$

for all $n_1, \ldots, n_k \in \mathbb{N}$.

Proof. It is clear that (ii) implies (ii'). For the converse, the idea is set some arbitrary value for y for the cases where it is not unique, knowing that this will not happen for $x_i = \overline{n}_i$ because of (ii'). In other words, if a formula ϕ satisfies (i) and (ii'), then the formula

$$((\exists_1 y)\phi(x_1, \ldots, x_k, y) \wedge \phi(x_1, \ldots, x_k, y)) \vee (\neg(\exists_1 y)\phi(x_1, \ldots, x_k, y) \wedge y = 0).$$

■

Example 7.5. The zero function $Z : \mathbb{N} \to \mathbb{N}$, $Z(n) = 0$, is representable by $x = x \wedge y = 0$. The successor function $S : \mathbb{N} \to \mathbb{N}$, $S(n) = n + 1$, is representable by $y = s(x)$.

Proposition 7.6. (i) *A relation $R \subseteq \mathbb{N}^k$ is representable if and only if its characteristic function $C_R : \mathbb{N}^k \to \mathbb{N}$,*

$$C_R(n_1, \ldots, n_k) = \begin{cases} 1 & \text{if } (n_1, \ldots, n_k) \in R \\ 0 & \text{if } (n_1, \ldots, n_k) \notin R \end{cases}$$

is representable.

(ii) *A function $f : \mathbb{N}^k \to \mathbb{N}$ is representable if and only if its graph relation $R_f \subseteq \mathbb{N}^{k+1}$*

$$(n_1, \ldots, n_k, m) \in R_f \Leftrightarrow f(n_1, \ldots, n_k) = m$$

is representable.

Proof. For the direct part of (i), if R is represented by a formula $\phi(x_1, \ldots, x_k)$, then C_R is represented by the formula

$$(\phi(x_1, \ldots, x_k, y) \wedge y = 1) \vee (\neg\phi(x_1, \ldots, x_k, y) \wedge y = 0).$$

The converse of (i) and part (ii) are left as exercises. ■

Theorem 7.7. *Suppose we have functions $f : \mathbb{N}^k \to \mathbb{N}$ and $g_1, \ldots, g_k : \mathbb{N}^l \to \mathbb{N}$. Define a new function $h : \mathbb{N}^l \to \mathbb{N}$ by*

$$h(n_1, \ldots, n_l) = f(g(n_1, \ldots, n_l), \ldots, g_k(n_1, \ldots, n_l)).$$

If $f, g_1, \ldots, g_k$ are representable then so is h.

Proof. If $f, g_1, \ldots, g_k$ are represented by formulas $\phi, \psi_1, \ldots, \psi_k$, then h is represented by the formula $\pi(x_1, \ldots, x_l, y)$:

$$(\exists z_1) \ldots (\exists z_k)(\psi_1(x_1, \ldots, x_l, z_1) \wedge \cdots \wedge \psi_k(x_1, \ldots, x_l, z_k) \wedge \phi(z_1, \ldots, z_k, y)).$$

■