18 The Theory $\mathcal{Q}$

18.1 Finite axiomatization

Axioms – what changes? We drop the induction axioms and add instead the very basic axiom, which says that any non-zero number must be a successor: $x{\neq}0 \Rightarrow \exists y.S\,y = x$

1. $S\,x{\neq}0$
2. $S\,x = S\,y \Rightarrow x = y$
3. $x + 0 = x$
4. $x + S\,y = S(x + y)$
5. $x * 0 = 0$
6. $x * S\,y = x * y + x$
7. $x{\neq}0 \Rightarrow \exists y.S\,y = x$

This theory is obviously consistent with our view of the natural numbers, because the *Standard-Interpretation* works out fine. It has the advantage of having only finitely many axioms, and we will show that it is very strong, as far as expressiveness is concerned.

18.2 Properties:

Q: Did we lose expressiveness?

Can we still represent all recursive functions?
Recall that an n-ary function f can be *represented* in a theory $\mathcal{T}$ if there is an n+1–ary predicate F such that for all $\bar{x}, y$
$f(\bar{x}) = y$ implies $F(\underline{\underline{\bar{x}}}, \underline{\underline{y}})$ is valid and $f(\bar{x}){\neq}y$ implies $\neg F(\underline{\underline{\bar{x}}}, \underline{\underline{y}})$ is valid.
I showed you on thursday how to express 0, S, +, *, projection, composition, and minimization in Peano arithmetic. We can use the same representations in $\mathcal{Q}$

- S, +, *, 0 can obviously be represented
- *Projection* $p_i^n(x_1, ..x_n) := x_i$

  $p_i^n(x_1, ..x_n) = y$ iff $y = x_i$ is valid
- *Composition* h(x) := f(g(x): f,g represented by F and G

  h(x) = y iff $\exists z.G(x, z) \wedge F(z, y)$ valid
- *Minimization*: g(x) := μ_y[f(x,y)=0]: f(x,y)=t represented by $F(x, y, t)$

  g(x) = z iff $(\forall y)(y{\leq}z \Rightarrow \exists t.[F(x, y, t) \wedge t = 0 \Leftrightarrow y = z])$

  This is the unrestricted loop or search

I have also shown that primitive recursion can be simulated with minimization and the other operations, so we can in fact represent all computable functions in the theory $\mathcal{Q}$. Now the question is, can we prove the respective validities if we only have the theory $\mathcal{Q}$ without induction? In fact, we can: recall, for instance, that the predecessor validity proofs needed only Axioms 1 and 2. I used an inductive proof to show that I can prove validity from the axioms. I gave you an inductive method how to apply them for each particular representation of a function value – but I did not use the induction *axiom*. So induction is only required on the meta-level but not on the level of the theory we're talking about.
Now you can prove the same facts not just about the predecessor but also about all other constructs. We do NOT need the induction *axiom* to prove the validity of a formula that represents a function value. So the theory $\mathcal{Q}$ is in fact sufficient.

Q: We can express the same functions but can we prove the same laws?

NO, here is an example of a law that does NOT hold anymore in $\mathcal{Q}$.

> The law $(\forall x)(S\,x{\neq}x)$ is not valid in $\mathcal{Q}$.
>
> This is strange, because it is a basic law of the natural numbers. So how do we prove that it is not valid in $\mathcal{Q}$? It is certainly satisfiable, because the standard interpretation of the natural numbers satisfies it. But there must be an interpretation of the axioms of $\mathcal{Q}$ in which this law does not hold.
>
> So how do we find such an interpretation?
>
> The easiest way is to extend the universe beyond the natural numbers and to define S, +, * on this extension in a way that violates $(\forall x)(S\,x{\neq}x)$, that is for some x in this extension $S\,x$ must be equal to x.
>
> So let us pick an element ω that is not a natural number. We don't need to give an intuition for this element, but we could imagine that ω could be infinity, that is the limit of applying the successor function to 0. Note that there is no term that represents ω but it must be included in our evaluation whenever we talk about a quantified formula.
>
> Now let us interpret the symbols of $\mathcal{Q}$.
>
> 0 obviously remains to be zero, and S, $+$, and * are interpreted on the natural numbers as usual.
>
> Now how do we interpret these functions when ω is involved.
>
> We define $S\,\omega = \omega$, so we already have an interpretation that violates the law $(\forall x)(S\,x{\neq}x)$.
>
> We define $x + \omega = \omega = \omega + x$ for all x.
>
> We define $0 * \omega = 0 = \omega * 0$ and $x * \omega = \omega = \omega * x$ for all other x.
>
> Note that we are talking about the interpretation of the symbols S, $+$, and * and not about the symbols themselves, although I use the same notation.
>
> Now let us check the seven laws. We only have to investigate the cases that involve ω because the others haven't changed.

1. $S\,\omega \neq 0$
2. $S\,x = S\,\omega \Rightarrow S\,x = \omega \Rightarrow x = \omega$
   $S\,\omega = S\,y \Rightarrow \omega = S\,y \Rightarrow \omega = y$
   No successor of a natural number is ω
3. $\omega + 0 = \omega$ by definition
4. $\omega + S\,y = \omega = S(\omega) = S(\omega + y)$
   $x + S\,\omega = x + \omega = \omega = S(\omega) = S(x + \omega)$
5. $\omega * 0 = 0$ by definition
6. $\omega * S\,y = \omega = \omega * y + \omega)$ regardless of what y is
   $0 * S\,\omega = 0 = 0 + 0 = 0 * \omega + 0)$
   $x * S\,\omega = \omega = \omega + x = x * \omega + x)$ for all other x
7. $x \neq 0 \Rightarrow \exists y.S\,y = x$ this holds for ω as well because we defined $S\,\omega = \omega$.

So we have found an interpretation of $\mathcal{Q}$ that violates the law $(\forall x)(S\,x \neq x)$

So, although we can express everything we can't prove everything anymore.

HOMEWORK:

Show that the following laws are not valid in $\mathcal{Q}$

1. $(\forall x, y)\ (x + y = y + x)$
2. $(\forall x, y, z)\ (x + (y + z) = (x + y) + z)$
3. $(\forall x)\ (0 + x = x)$
4. $(\forall x, y)\ (x * y = y * x)$
5. $(\forall x)\ (0 * x = 0)$

Find an interpretation of $\mathcal{Q}$ that violates all these 5 laws.

Solution: Extend the universe beyond the natural numbers and define S, +, * on this extension in a way that violates the 5 laws but satisfies the 7 axioms of $\mathcal{Q}$. For this purpose we select two elements ω and ζ which are not natural numbers and define S, $+$, $*$ according to the following tables:

S	
ω	ω
ζ	ζ
$i \in \mathbb{N}$	$i + 1$

$+$	ω	ζ	$j \in \mathbb{N}$
ω	ζ	ω	ω
ζ	ζ	ω	ζ
$i \in \mathbb{N}$	ζ	ω	$i + j$

$*$	ω	ζ	0	$j \neq 0$
ω	ζ	ζ	0	ζ
ζ	ω	ω	0	ω
0	ω	ζ	0	0
$i \neq 0$	ω	ζ	0	$i * j$

It is easy to check that all 7 axioms of $\mathcal{Q}$ hold while all 5 laws are violated in this interpretation.

Q: What about decidability?

Obviously still undecidable because of the expressiveness (but see also BJ chapter 15). So to formulate it stronger:

> **Theorem**: No consistent extension of $\mathcal{Q}$ is decidable.

So if we look at **Arithmetic** – that is the theory that uses the formal language of arithmetic (at least +,*,=,S) and contains exactly the theorems that are true in the standard-interpretation of the natural numbers – then we know that all the axioms of $\mathcal{Q}$ as theorems, which means that Arithmetic is a consistent extension of $\mathcal{Q}$. Thus we know:

> **Theorem**: Arithmetic is not decidable

This is pretty bad but probably not surprising, since we know this result from Peano Arithmetic already. But it becomes even worse. What about axiom systems for arithmetic. Let me introduce a few notions

Q: What about finite axiomatizations?

We call a theory $\mathcal{T}$ *complete*, if for every closed formula X that can be formulated in the language of T either X or $\neg X$ is a theorem of $\mathcal{T}$.
$\mathcal{Q}$ is obviously not complete but Arithmetic is a complete extension of $\mathcal{Q}$.
We call a theory $\mathcal{T}$ *axiomatizable*, if there is a decidable subset S of the theorems of $\mathcal{T}$ whose logical consequences are exactly the theorems of $\mathcal{T}$. Not that we do not require the set of axioms to be finite. $\mathcal{Q}$ is obviously axiomatizable, because we defined it by a finite set of axioms. The axioms of Peano Arithmetic are not decidable (it is hard to figure out whether INSTANCES of an arbitrary formula describe a proper step case). So is Arithmetic axiomatizable or not?

> **Theorem**: every consistent, axiomatizable, and complete theory $\mathcal{T}$ is decidable.
> Let S be the set of axioms of $\mathcal{T}$. Since S is decidable, we can decide whether a given sequence of proof rule applications using the axioms of $\mathcal{T}$ is a valid proof. Thus it is possible to *enumerate* all the proofs in $\mathcal{T}$. Now let X be an arbitrary formula in $\mathcal{T}$. Since $\mathcal{T}$ is complete, the enumeration of the proofs in $\mathcal{T}$ will yield a proof of either X or $\neg X$ after finitely many steps. Thus we can decide whther X is valid or not.

The consequence?

> **Theorem**: every consistent, and complete extension of $\mathcal{Q}$ is not axiomatizable.
>
> Arithmetic is not axiomatizable.

In other words, there is no decidable axiom system for the Arithmetic as we know it, and there is definitely no way to find a finite axiomatization of Arithmetic. Every attempt to give a decidable axiomatization will bei either incomplete or inconsistent.
We have to live with that fact when we build formal systems for mathematics and program verification. If we want to be expressive enough, we have to tolerate undecidability and undecidable axiom schemata. If we want to decide an arithmetic property, we have to restrict ourselves to an incomplete subset.
In NuPRL, we aim at a hybrid solution: we formalize the full arithmetic using Peano arithmetic with induction schemata and many predefined operations, and we provide a decision procedure for the sub-theory of elementary arithmetic, which helps us to decide the most fundamental arithmetical statements.