3 Omniscience Principles

3.1 Introducing the omniscience principles

In **HAS** and $\mathbf{HA}_\omega$ we now have formal languages where we can talk about mathematical statements that constructive mathematicians might be interested in. In this section we will see some important examples known as *omniscience principles*. These are used by constructive mathematicians to provide prototypical examples of nonconstructive statements. They are often used to illustrate to classical mathematicians the kind of statement that is not allowed when working constructively. They are also a useful tool for showing that something is not provable constructively: if we can use a statement φ to prove an omniscience principle, then φ must also be non constructive. However, for this argument to really work, we first need to show that the omniscience principles are not provable in the formal theories we are working in. By having a range of different principles, we can classify mathematical statements by "how non constructive" they are. This is one of the key ideas of a field known as *constructive reverse mathematics*.

Each omniscience principle has a universal quantifier ranging over all *binary sequences*, that is, functions from $\mathbb{N}$ to 2. When we are working in $\mathbf{HA}_\omega$ we implement this by viewing $\forall f \in 2^{\mathbb{N}}\ \varphi$ as notational shorthand for $\forall f^{N \to N}\ ((\forall n\, fn = 0 \vee fn = 1) \to \varphi)$. We first consider the strongest omniscience principle, the limited principle of omniscience.

Definition 3.1. The *limited principle of omniscience* (**LPO**) is the following statement:

$$\forall f \in 2^{\mathbb{N}}\ (\forall n\, f(n) = 0) \vee (\exists n\, f(n) = 1)$$

We first observe that **LPO** is easily provable in classical mathematics:

Proposition 3.2. *The law of excluded middle implies* **LPO**.

Proof. Let f be any binary sequence. By the law of excluded middle we know $\exists n\, f(n) = 1$ is either true or false. If it is true, then we are done. Suppose then that it is false. We need to show $\forall n\, f(n) = 0$. For each natural number n, we know that $f(n) = 0$ or $f(n) = 1$ (exercise!). However, if we had $f(n) = 1$, this would contradict $\neg(\exists n\, f(n) = 1)$. Hence we must have $f(n) = 0$. But we can now deduce $\forall n\, f(n) = 0$, as we needed. $\square$

The intuition for why **LPO** is not constructively acceptable is that in order to know whether the sequence f contains a 1, we need to look at the entire sequence at once. We cannot tell whether or not there exists n such that $f(n) = 1$ by only looking at a finite portion of the sequence, whether that is the first five values, the first one million values, or first Graham's number values or higher. If we ever find a number n such that $f(n) = 1$, then we know for sure that $\exists n\, f(n) = 1$, but if $f(n) = 0$ for every value of n we have checked so far, then we have no way of knowing whether this will continue to be the case forever, or if we will find an n with $f(n) = 1$ sometime in the future.

We can also motivate the idea by thinking about physical measurements. As we improve our equipment and carry out more experiments we can know physical quantities with greater and greater precision, but we will never reach absolute precision. For example, if we are given two platinum bars, we will eventually find out if they have different lengths, but if they have the same length we will never know for sure. Hence, there is no way in general to decide which of the two cases we are in.

Finally, we can understand this idea through *computability.* Given a computer program that outputs the numbers 0 and 1, we have no way to decide, in general whether it will output 0 forever, or whether it will eventually output 1 given enough time on an ideal computer. We will later make this last intuition precise using realizability.

The remaining omniscience principles are the weak limited principle of omniscience, the lesser limited principle of omniscience and Markov's principle.

Definition 3.3. The *weak limited principle of omniscience* (**WLPO**) is the following statement.

$$\forall f \in 2^{\mathbb{N}}\ (\forall n\, f(n) = 0)\ \vee\ \neg(\forall n\, f(n) = 0)$$

Definition 3.4. *Markov's principle* (**MP**) is the following statement.

$$\forall f \in 2^{\mathbb{N}}\ \neg(\forall n\, f(n) = 0) \rightarrow \exists n\, f(n) = 1$$

Markov's principle is not always included as an omniscience principle, and many constructive mathematicians view it as a perfectly reasonable axiom to use in constructive proofs. For example, it is viewed as acceptable according to the philosophy of recursive or "Russian" constructive mathematics. The idea is that existential quantifiers need to be justified by computable functions. In the case of Markov's principle, we imagine the binary sequence as a computer program outputting a sequence of 0's and 1's as it is given different inputs. If it is false that the program will always output 0, then we can write a program to find a number n such that the program outputs 1 given input n - we simply keep running the original program on higher and higher input values until it returns 1, and then return the input value where this happened.

Note however that Markov's principle is exactly what we need to get from **WLPO** to **LPO**. More precisely, we have the following proposition.

Proposition 3.5. **LPO** *is equivalent to the conjunction of* **WLPO** *and* **MP**.

Proof. There is a short proof in intuitionistic natural deduction that $\exists n\, f(n) = 1$ implies $\neg(\forall n\, f(n) = 0)$. From this it is clear that **LPO** implies **WLPO**. Similarly, given Markov's principle, we also have the converse statement, that $\neg(\forall n\, f(n) = 0)$ implies $\exists n\, f(n) = 1$, and so we also have that **WLPO** and **MP** together imply **LPO**.

We just need to check that **LPO** implies **MP**, but this is again straightforward: if $\exists n\, f(n) = 1$, then we are done, and if $\forall n\, f(n) = 0$, we can apply ex falso together with the assumption $\neg(\forall n\, f(n) = 0)$ to deduce $\exists n\, f(n) = 1$. $\square$

Definition 3.6. The *lesser limited principle of omniscience* (**LLPO**) is the following statement.

$$\forall f \in 2^{\mathbb{N}}\, \forall n, m\, ((f(n) = 1 \wedge f(m) = 1) \to n = m) \longrightarrow$$
$$(\forall n\, f(2n) = 0) \vee (\forall n\, f(2n+1) = 0)$$

Most people find lesser limited principle of omniscience to be the least intuitive of the omniscience principles. To explain it a bit more, the clause $\forall n, m\, ((f(n) = 1 \wedge f(m) = 1) \to n = m)$ says that f has "at most one 1." That is, $f(n)$ is equal to 0 for almost all n. It could be equal to 0 for all n, for example. However, we also allow for the possibility that $f(n)$ is equal to 1 for some n. In this case we know that $f(m)$ is equal to 0 whenever $m \neq n$. The statement $\forall n\, f(2n) = 0$ is telling us that if $f(n) = 1$, then n must be odd. Similarly, $\forall n\, f(2n+1) = 0$ tells us that if $f(n) = 1$, then n must be even. So **LLPO** is telling us that even if we don't know whether there is an n such that $f(n) = 1$, we can say either "if there is such an n it is odd" or "if there is such an n it is even."

Proposition 3.7. *The weak limited principle of omniscience implies the lesser limited principle of omniscience.*

Proof. Let f be a binary sequence with at most one 1. We apply **WLPO** to the sequence f' defined by $f'(n) := f(2n)$. If we have $\forall n\, f'(n) = 0$, then we are done, since $f(2n) = 0$ for all n.

Now suppose that we have $\neg(\forall n\, f'(n) = 0)$. We will show that for all n, we have $f(2n+1) = 0$. First recall that we know for each n that either $f(2n+1) = 0$ or $f(2n+1) = 1$. If we had $f(2n+1) = 1$, then it would imply that $f(2m) = 0$ for all numbers m, since we have $2m \neq 2n + 1$ for all m. However, this would contradict $\neg(\forall n\, f'(n) = 0)$. Hence we have $f(2n+1) = 0$, and since this applies for all numbers n, we are done. $\square$

Although **LLPO** is usually seen as not acceptable in constructive mathematics, in settings where we do not have countable choice it can be surprisingly harmless. A kind of realizability called *Lifschitz realizability* can be used to show that **LLPO** is consistent with *Church's thesis* (an anti classical axiom that says "all functions $\mathbb{N} \to \mathbb{N}$ are computable").

3.2 Review of the standard ordering on natural numbers

In order to help formalise some ideas we briefly review the standard ordering on natural numbers.

Definition 3.8. We write $x < y$ as shorthand for the formula $\exists z\, y = x + Sz$

The following standard properties of $<$ can be proved in **HA**. However, for this course we will omit the proofs.

Proposition 3.9. *The binary relation $x < y$ has the following properties.*

1. $\neg(x < x)$ *(irreflexivity)*

2. $x < y \wedge y < z \rightarrow x < z$ *(transitivity)*

3. $x < y \vee y < x \vee x = y$ *(trichotomy)*

4. $\neg(x < 0)$

5. $x < Sy \leftrightarrow (x = y \vee x < y)$

We also review some more standard notation. First of all, we write $x \leq y$ to mean $\exists z\, y = x + z$. This also satisfies a list of properties that we will assume without proof (but can be proved in **HA**).

Proposition 3.10. *The binary relation $x \leq y$ has the following properties.*

1. $x \leq x$ *(reflexivity)*

2. $x \leq y \wedge y \leq z \rightarrow x \leq z$ *(transitivity)*

3. $x \leq y \wedge y \leq x \rightarrow x = y$ *(anti-symmetry)*

4. $x \leq y \vee y \leq x$ *(linearity)*

5. $x \leq y \leftrightarrow x = y \vee x < y$

We will sometimes use the notational convention of "bounded quantifiers." Namely, we do the following:

1. We write $\forall x < y\, \varphi$ to mean $\forall x\, (x < y \rightarrow \varphi)$.

2. We write $\exists x < y\, \varphi$ to mean $\exists x\, (x < y \wedge \varphi)$

3. We write $\forall x \leq y\, \varphi$ to mean $\forall x\, (x \leq y \rightarrow \varphi)$.

4. We write $\exists x \leq y\, \varphi$ to mean $\exists x\, (x \leq y \wedge \varphi)$

Definition 3.11. Suppose we are given a formula $\varphi(x)$. We say n is the *least* number satisfying φ if the following holds:

$$\varphi(n) \wedge \forall x\, (\varphi(x) \rightarrow n \leq x)$$

Note that by the propositions above (in particular trichotomy), this is equivalent to the following:

$$\varphi(n) \wedge \forall x < n\, \neg\varphi(x)$$

We justify saying *the* least number by the fact that if n and m both have this property, then $m \leq n$ and $n \leq m$, and so $m = n$.

3.3 An explicit version of LPO and the axiom of unique choice

For each omniscience principle, we can also define an "explicit" version where we have a function that "witnesses" the truth of the omniscience principle.

For example, for **LPO**, we define this as follows.

Definition 3.12. The *explicit limited principle of omniscience* states that there is a function $F : 2^{\mathbb{N}} \to (2 \times \mathbb{N})$ with the following property. For every binary sequence f, exactly one of the following two conditions applies:

1. $\mathbf{p}_0\, F(f) \;=\; 0$ and $\forall n\, f(n) = 0$
2. $\mathbf{p}_0\, F(f) \;=\; 0$ and $f(\mathbf{p}_1\, F(f)) = 1$

Since we don't have a sort for 2 in $\mathbf{HA}_\omega$, we note that we can alternatively define F on *all* functions $\mathbb{N} \to \mathbb{N}$ and ignore those that are not binary sequences. Namely, we can formalise explicit **LPO** in $\mathbf{HA}_\omega$ as the following statement:

$$\exists F^{N \to N, N \times N}\, \forall f^{N \to N}\, (\forall n\, fn = 0 \;\vee\; fn = 1) \;\to\; (\mathbf{p}_0(Ff) = 0 \wedge \forall n\, fn = 0) \vee (\mathbf{p}_0(Ff) = 1 \wedge f(\mathbf{p}_1(Ff)) = 1)$$

We can easily see that explicit **LPO** implies **LPO**. For the converse we sometimes (if working in $\mathbf{HA}_\omega$, for example) need an additional axiom, the axiom of unique choice.

We first introduce some notation.

Definition 3.13. We write $\exists! x\, \varphi(x)$ as notation for the following statement.

$$\exists x\, (\varphi(x) \;\wedge\; \forall y\, \varphi(y) \to x = y)$$

We say "there exists a *unique* x satisfying φ."

Definition 3.14. Given sorts σ and τ *axiom of unique choice*, $\mathbf{AC}_!^{\sigma,\tau}$ is the following statement for each formula φ.

$$\forall x^\sigma\, \exists! y^\tau\, \varphi(x, y) \;\to\; \exists f^{\sigma \to \tau}\, \forall x^\sigma\, \varphi(x, fx)$$

Theorem 3.15. *Assuming* **LPO** *and the axiom of unique choice, we can prove explicit* **LPO***.*

Proof. We will just give an informal proof in constructive mathematics. Exercise: Think about how you would formalise this in $\mathbf{HA}_\omega$.

We are going to construct $F : (\mathbb{N} \to 2) \to (2 \times \mathbb{N})$ using unique choice.

We define $\varphi(f, x)$ to be following statement: Either $\mathbf{p}_0 x = 0$, $\mathbf{p}_1 x = 0$, and $\forall n\, f(n) = 0$ or $\mathbf{p}_0 x = 1$ and $\mathbf{p}_1 x$ is the least number n such that $f(n) = 1$.

We first check existence of x. By **LPO**, we know that either $\forall n\, f(n) = 0$ or $\exists n\, f(n) = 1$. In the former case we can take $x = \mathbf{p}00$. In the latter case, we can in fact deduce there is a *least* n such that $f(n) = 1$ (exercise!), and then take x to be $\mathbf{p}1n$.

We now need to check uniqueness. Suppose we have x and y such that $\varphi(f, x)$ and $\varphi(f, y)$ are both true. Note that we cannot have both $\forall n\, f(n) = 0$ and $\exists n\, f(n) = 1$ since these would contradict each other. It follows that $\mathbf{p}_0 x = \mathbf{p}_0 y$. To show the $\mathbf{p}_1 x = \mathbf{p}_1 y$, we split into the two cases $\forall n\, f(n) = 0$ and $\exists n\, f(n) = 1$. In the former case we have $\mathbf{p}_1 x = 0 = \mathbf{p}_1 y$. In the latter case we recall that the least number satisfying any condition is unique, and so we also have $\mathbf{p}_1 x = \mathbf{p}_1 y$ in that case, as we needed. $\square$