Lecture 3: Natural Numbers and Induction

In the previous lecture, we talked about inference rules, and we used schematic variables A, B, C to serve as placeholders for real formulas. The rules we presented were actually not rules, they were rule schemas with holes, that must be plugged with mathematical formulas before they can be used. We also mentioned, that there are formulas, that are not composed from other formulas using connectives. We call these formulas *atomic*. An atomic formula is usually of the form $p(a_1...a_n)$. We call p a *predicate symbol*, and the a_i are arguments, that range over numbers. Examples of such atomic formulas include even(10), or prime(15) (which should not be derivable).

Let's start working with the natural numbers $\mathbb{N}$ and the the whole numbers $\mathbb{Z}$ that may be negative, zero, or positive. The positive numbers are those defined to be greater than 0, for example $1, 2, 3, 4, \ldots$. More formally, we write $\mathrm{pos}(1), \mathrm{pos}(2), \mathrm{pos}(3), \ldots$ for the property that $1, 2, 3$ are positive numbers. Negative numbers are not positive $\neg\mathrm{pos}(-1), \neg\mathrm{pos}(-2), \neg pos(-3), \ldots$. Similarly, we can define the property when a number is negative. $\mathrm{neg}(-2)$ true and is $\neg\mathrm{neg}(2)$ true. neg and pos are predicate symbols.

Recall from last lecture, that in classical mathematics, we are allowed to use an axiom, the law of the excluded middle $A \vee \neg A$. By this law, we know that for every number n, we either have $\mathrm{pos}(n) \vee \neg\mathrm{pos}(n)$. Notice what we have just done. Instead of writing a concrete number, we wrote n, a variable that ranges over numbers. This is something we often (always) do when we do mathematics, we abstract from the specific to the general case. It is – so to speak – our daily bread. We will be introducing two new connectives to our logic one for expressing that something is true for all numbers, and the other that there exists at least a number that makes a statement true. The former, we call *univeral quantifier* $\forall$, the later and *existential quantifier* $\exists$. Examples of fromulas that include quantifier include $\forall n \in \mathbb{Z}.\mathrm{pos}(n) \vee \neg\mathrm{pos}(n)$ or $\exists n \in \mathbb{Z}.\neg\mathrm{pos}(n) \wedge \neg\mathrm{neg}(n)$.

Quantifiers are logical connectives, but what makes the special is first that the talk about something else but logical truth, namely numbers, lists, and trees (as we will see later) and the like. We call these things *terms*. Second, they talk about infinite sets. There are infinitely many numbers, there are even uncountably many reals, but only countably many rational numbers, and countably many lists about natural numbers. etc.

This is why quantification is a very powerful construct. We will discuss two ways of using them in proofs. The first way allows us to prove properties about terms, without analyzing their structure. We give four rules, an introuction and elimination rule for the universal quantifier, and an introduction and elimination rule for the existential quanifier, just as we have done last week for all the propositional connectives.

$$\frac{A(u)\ \mathsf{true}}{\forall x \in \mathbb{N}.A(x)\ \mathsf{true}}\,\forall\mathrm{I}^u \qquad \frac{\forall x \in \mathbb{N}.A(x)\ \mathsf{true}}{A(n)\ \mathsf{true}}\,\forall\mathrm{E}$$

We could also generalize this scheme further. Since we never analyze the

structure of our terms by the virtue of these rules, we can let the quantifier range over variables of different sorts of variables. For example, instead of $\mathbb{N}$ we could use the domain of whole numbers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, lists, or trees. We will do this a little later, and when we do it, a bit more informally. The idea remains the same. Next up the rules for the existential quantifier.

$$\frac{A(n)\ \mathsf{true}}{\exists x \in \mathbb{N}.A(x)\ \mathsf{true}}\ \exists\mathrm{I} \qquad \frac{\exists x \in \mathbb{N}.A(x)\ \mathsf{true} \qquad \begin{array}{c}\overline{A(e)\ \mathsf{true}}\ u \\ \vdots \\ C\ \mathsf{true}\end{array}}{C\ \mathsf{true}}\ \exists\mathrm{E}^{e,u}$$

Before we start doing real mathematics now, I would like to tell you a little bit about arithmetic. True, we have learned and internalized lots of the mathematical facts over the years, during school and university life, but now we must make more precise what we actually do know. We add these facts as axioms. Mathematics is precise science. The following set of axioms is neither complete nor does it try to be complete. There are very well-known and well-studied axiomatizations, for example Heyting arithmetic, but we don't care about them here.

Following the definition of natural numbers, the next most important definition is that of the equality between two numbers. Equality is a predicate symbol, if one likes, that takes two arguments $= (x, y)$ for which we usually write $x = y$. The first axiom states that all numbers are equal to themselves. We also say that equality is *reflexive*.

$$\frac{}{\forall x \in \mathbb{N}.x = x}\ \mathrm{refl}$$

The second one states that the equality between numbers is also *transitive*.

$$\frac{}{\forall x \in \mathbb{N}.\forall y \in \mathbb{N}.\forall z \in \mathbb{N}.x = y \wedge y = z \to x = z}\ \mathrm{trans}$$

The third axiom says that that the equality relation is also *symmetric*.

$$\frac{}{\forall x \in \mathbb{N}.\forall y \in N.x = y \to y = x}\ \mathrm{sym}$$

There are a few more axioms that we need, for example,[1]

$$\frac{}{\forall x \in \mathbb{N}.\neg(x = x + 1)}\ \mathrm{eq}_1$$

Similarly to equality, there are differnent axioms defining inequality, strictly less then, for example $<$.

$$\frac{}{\forall x \in N.\neg(x + 1 < x)}\ \mathrm{lt}_1$$

[1] [*more probably be added later ..*]

It might be good to point out at this point that there is no best way to specifiy those axioms.[2].

Let's try to define the even numbers. Recall from high school that a number is even if it is divisble by 2. When we define even(n), we basically stipulate the existence of an axiom that is

$$\frac{}{\text{even}(n) \leftrightarrow \exists n' \in \mathbb{N}.n = 2n' \ \mathsf{true}} \text{ def-even}$$

Mathematically, we would simply write,

Definition 15 (Even numbers) even(n) *if and only if* $\exists n' \in \mathbb{N}.n = 2n'$.

and similarly, we define the odd numbers as

$$\frac{}{\text{odd}(n) \leftrightarrow \exists n' \in \mathbb{N}.n = 2n' + 1 \ \mathsf{true}} \text{ def-odd}$$

Definition 16 (Odd numbers) odd(n) *if and only if* $\exists n' \in \mathbb{N}.n = 2n' + 1$.

Time for a little theorem? The sum of two odd numbers is even:

Theorem 17 *Let x be odd and y be odd, then $x + y$ is even.*

Proof:

odd(x)	by assumption
$\exists x' \in \mathbb{N}.x = 2x' + 1$	by axiom def-odd
odd(y)	by assumption
$\exists y' \in \mathbb{N}.y = 2y' + 1$	by axiom def-odd
Choose $z' = x' + y' + 1$	
$x + y = 2x' + 1 + 2y' + 1 = 2(x' + y' + 1) = 2z'$	by equational reasoning
$\exists z' \in \mathbb{N}.x + y = 2z'$	by $\exists$I
even($x + y$)	by axiom def-even

□

Exercise 1 Write out the proof as a formal derivation in our logic using only the rules that we have discussed so far. Recall that $A \leftrightarrow B$ is just an abbreviation for $A \to B \wedge B \to A$.

The next theorem states that the square of an odd number is odd again. The proof is again a little bit more informal, but perhaps more readable.

Theorem 18 *If x is odd then x^2 is odd.*

Proof:

[2] [*could bring an exmaple here, if really necessary*]

x is odd	by assumption
there exists a k, s.t. $x = 2k + 1$	by definition
$x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$	by equation reasoning
Choose $z' = (2k^2 + 2k)$	
$\exists z'.x^2 = 2z' + 1$	by $\exists$I
x^2 is odd	by definition of def-odd

□

Theorem 19 (Euclid) *There is no largest number.* $\neg(\exists m \in I\!N.\forall x \in I\!N.x < m)$.

Proof:

Assume $\exists m \in I\!N.\forall x \in I\!N.x < m$	called u
Let p be an arbitrary but fixed formula	
$\forall x \in I\!N.x < m$	by $\exists E^m$
$m + 1 < m$	by $\forall$E choosing $m + 1$ for x
$\neg(m + 1 < m)$	by axiom lt_1
p	by $\neg$E
$\neg(\exists m \in I\!N.\forall x \in I\!N.x < m)$	by $\neg$I discharing p and q

□

Since Kindergarten, we all know the natural numbers and how to generate them. We start with 0 as a natural number, if n is a natural number then $n+1$ is also a natural number. It is pretty easy to see, that any number can we written as a large sum:

$$n = 0 + \underbrace{1 + \ldots + 1}_{n \text{ times}}$$

We say that the numbers are inductively defined, by two constructors, 0 and +1.

The induction principle differs significantly from the introduction rule above. It is designed to analyze the structure of a term.

Let's consider the situation that we need to show something for all numbers: $\forall n \in I\!N.P(n)$. Since the rule for universal quantification introduction does not allow us to inspect the structure of a general n, theorems of that kind are not always directly provable. Very often the proof only goes through when we look at the structure of n.

Since we know that all numbers are constructed from these two constructors, we could try to prove P for every concreate instantiation of n such as

$$P(0), P(1), P(2), P(3), \ldots$$

It is pretty clear that this would take forever, and therefore not result in a proof. This is not ideal. Here is another idea. We should try to justify $P(n+1)$ based

on the knowledge that $P(n)$ holds. This means we have to prove two cases, first the base case,

$$P(0)$$

and secondly the step case

$$\forall n \in \mathbb{N}.P(n) \to P(n+1)$$

If we provide a proof of these two cases, then we have conducted a proof by induction on the structure of that natural number n. In the case that we cannot prove the second case directly (using our rules from last lecture + the standard unification introduction and elimination rules), we might have to do a second nested induction on n again.

Once these two cases are proved, we can apply the theorems and convince ourselves that, if we only had infinite amounts of time, we could convince ourselves that $P(n)$ is true for any $n \in \mathbb{N}$.

$P(0)$	from the first case
$P(0) \to P(1)$	form the second case with $n = 0$
$P(1)$	by $\to$ E
$P(1) \to P(2)$	form the second case with $n = 1$
$P(2)$	by $\to$ E
$\ldots$	

All we have to believe is that this argument scales to the infinite. What could go wrong? Nothing, but we have to admit, this proof constructions is somewhat less intuitive then the other. We must believe that everything works out ok in the infinite. It is not justified/justifiable in any other way then what I just showed you. Note, that very few mathematicans distrust this prinicple.

This completes the technical part of this lecture. The cool thing is that using the principle of induction, we can actually prove quite intersting things, about numbers. Here is one, a theorem that is named after Carl Friedrich Gauss "the little Gauss". When he was eight years old, Gauss's class was asked to add all numbers between 1 and 100. Gauss answered immediately 5050. The teacher asked him how he did it: Add the first number and the last, $1+100 = 101$. Then you add $2 + 99 = 101$, then $3 + 98 = 101$, etc. until you come to $50 + 51 = 101$. Hence you have $50 \times 101 = 550$.

Let's generalize it a little bit. What happenes if we do not only want to add up the first 100 numbers, but the first n numbers? We introduce some notation, which will make it much easier for us to formulate the theorem. We write

$$\sum_{i=0}^{n} i$$

as an abbreviation for $0 + 1 + 2 \ldots n$.

Theorem 20

$$\forall n \in \mathbb{N}. \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

Proof: How do we prove it? Of course by induction over n. We must consider two case.

Case 1

$\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2}$ by equational reasoning

Case 2

Let n be arbitray but fixed
Assume $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ called u
$\sum_{i=0}^{n+1} i$
$= \sum_{i=0}^{n} i + (n+1)$ by the definition of $\sum$
$= \frac{n(n+1)}{2} + (n+1)$ be replacing equals for equals
$= (\frac{n}{2} + 1)(n+1)$ by pulling out the $(n+1)$
$= (\frac{n+2}{2})(n+1)$
$= (\frac{(n+1)+1}{2})(n+1)$
$= \frac{((n+1)+1)(n+1)}{2}$
$= \frac{(n+1)((n+1)+1)}{2}$

$\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \to \sum_{i=0}^{(n+1)} i = \frac{(n+1)((n+1)+1)}{2}$ by $\to$ I discharging u

$\forall n \in I\!N . \sum_{i=0}^{n} i = \frac{n(n+1)}{2} \to \sum_{i=0}^{(n+1)} i = \frac{(n+1)((n+1)+1)}{2}$
by $\forall$I discharging n

$\forall n \in I\!N . \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ by the principle of induction

□