1 Lecture 9 (2/17/2011)

Key Terms: *Proofs with quantifiers*

1.1 Quantified propositions

If $P(x)$ is an open sentence with universe U, then $\forall x \ P(x)$ is a proposition. How do we decide whether $\forall x \ P(x)$ is true or false?

If U is a small set we can simply check $P(u)$ for each $u \in U$.

Example 1 *Let $U = \{-1, 0, 1\}$ and let $P(x)$ be the sentence $\boxed{x^3 = x}$; then we simply check that $0^3 = 0, 1^3 = 1, (-1)^3 = -1$ and conlcude that $\forall x \ P(x)$ is true.*

If U is a large set then it is impractical to check for each $u \in U$. If U is an infinite set, then it is impossible to check every $u \in U$.

Remark 2 *Note that to prove that $\forall x \ P(x)$ is false, it suffices to produce a single element u such that $P(u)$ is false. But we can never prove that $\forall x \ P(x)$ is true by checking elements in an infinite universe.*

Some of the most famous math problems involve the infinite universe $U = \mathbb{N}$.

Example 3 *(Fermat's last theorem) If x, y, z, n are natural numbers, and if $n > 2$ then $x^n + y^n \neq z^n$.*

Remark 4 *Symbolically, $\forall x \forall y \forall z \forall n \ [(n > 2) \Rightarrow (x^n + y^n \neq z^n)]$; $U = \mathbb{N}$*

Remark 5 *This is a really hard problem, which remained unsolved for 350 years until Andrew Wiles solved it in the 1990's.*

1.2 Proofs of quantified propositions

If we cannot check all possible cases in U, how can we show that the proposition $\forall x \ P(x)$ is true? The main idea is to use a "proof with a variable".

Suppose we knew that some other open sentence $Q(x)$ was true for all x in U, e.g. by citation from some previously established result. Also suppose we could prove that $Q(x) \Rightarrow P(x)$ for each x in U, e.g. by following the usual HTM rules. Then we could use Modus Ponens to deduce that $P(x)$ is true for each x in U.

The structure of such a proof is similar to the kind of proofs that we have been dealing with before, except that these proofs involve one or more variables, whose presence is usually signaled by a "Let" statement. For example we might write the above proof as follows.

Theorem 6 *For all x in U, $P(x)$ is true.*

Proof. Let x be an arbitrary element of U
Then $Q(x)$ is true. (Citation)
$\boxed{\ldots \text{ then } Q(x) \Rightarrow P(x) \text{ is true.}}$
Therefore $P(x)$ is true. (Modus Ponens.) ■

Remark 7 *The boxed part of the proof has to be "universal" i.e. such that it works for every element in the universe.*

1.3 Proofs in number sets

The strategy desribed in the previous section works well remarkably well for universes consisting of number sets such as $\mathbb{N}$ and $\mathbb{R}$, which have a lot of *structure*. This structure is described as properties/axioms in the text (see the material on pages xiv-xvii, and also the order properties listed on page 321). These properties take the form $\forall x\ Q(x)$ or $\forall x \forall y\ R(x, y)$ etc; for example $\forall x \forall y$ $(x + y = y + x)$.

When trying to prove a quantified proposition such as $\forall x\ P(x)$ in a universe, we are allowed to cite the relevant properties of the universe. In particular most of the usual arithmetic operations etc. are justified by these properties.

We now give an example of such a proof, after recalling a definition from page xv of the text.

Definition 8 *If a and d are natural numbers, we say that d divides a if and only if there exists a natural number k such that $a = dk$.*

Theorem 9 *If a, b, d are natural numbers and d divides both a and b, then d divides $ax + by$ for any natural numbers x, y.*

Remark 10 *This theorem can be written symbolically as follows:*

$$\forall a \forall b \forall d \forall x \forall y \left[(d \textit{ divides } a) \wedge (d \textit{ divides } b) \Rightarrow (d \textit{ divides } ax + by)\right];\ U = \mathbb{N}$$

Proof.

1. Let a, b, d, x, y be natural numbers.

2. By hypothesis d divides a and d divides b.

3. By definition there exist natural numbers k, l such that $a = dk$ and $b = dl$.

4. Therefore
$$ax + by = dkx + dly = d(kx + ly)$$

5. By definition $[ax + by = d(kx + ly)] \Rightarrow [d \text{ divides } ax + by]$

6. Therefore d divides $ax + by$.

■

Let us examine the structure of this proof.
Statement 1 is a "Let" statement" signalling the presence of certain variables.
Statement 2 is a hypothesis statement.
Statement 3 is equivalent to statement 2, and introduces more variables.
We use *different* letters k, l because these variables need not be equal.
Statement 4 is an arithmetic result that follows from the properties of $\mathbb{N}$.
Statement 5 is a tautology.
Statement 6 is a Modus Ponens statement.

Note especially how crucially the "definition" is used in this proof. It produces the variables k, l and it is also responsible for the tautology in Step 5. After some practice with writing proofs, we we will skip the analogs of Statement 5, and go straight to Statement 6.

1.4 Exercises

All of the following exercises deal with the universe $U = \mathbb{N}$.

1. Prove that the following proposition is *false*:

$$\forall n \left(n^2 + n + 41 \text{ is a prime number}\right)$$

   [Hint: Small numbers will work, you need to think big!]

2. Prove that if a divides b, then a^n divides b^n for all n.

3. Prove that 2 divides $k(k+1)$ for all k.

4. Prove if 2 divides $m-1$ then 8 divides m^2-1.
   [Hint: Use problem 3.]