

**Lecture 15: Formal systems (syntax); Induction.**

**Read:** Chapter 8, Sections 1 and 4. (179-183, 192-198)

**Attention: Induction is a mind-bender, more than it seems at first!**

**Section 8.1. The syntactic side of formal systems.**

In Section 8.1, we look in greater detail at the syntactic side of formal systems, particularly at recursive definitions, which we introduced in Chapter 1 as a means of specifying sets. [Section 8.2, which we will skip, looks at axiomatic systems in greater detail as purely formal systems, looking at them from a perspective very much as “grammars”, and Section 8.3, which we will also skip, looks at a particular class of axiom systems, “Semi-Thue systems”, also from a grammar-like perspective.]

Section 8.4., which we will pay close attention to, introduces Peano’s axioms for arithmetic, and the closely related notion of the *Principle of Mathematical Induction*, and the corresponding notion of *proof by induction* or *inductive proof*.

Then in the following two sections we will look at parts of 8.5 in a study of model theory, the semantic side of formal systems.

**8.1.1. Recursive definitions.**

Consider the set  $M$  of all even-length mirror-image strings on  $\{a,b\}$ . An even-length mirror-image string is a string that can be divided into two halves, with the right half a mirror-image reversal of the left half (a “palindrome”). Examples:  $abba$ ,  $babbab$ ,  $aaaa$ ,  $bbabbabb$ . Non-examples:  $babb$ ,  $aaab$ ,  $bab$ .

Recursive definition of  $M$ :

- (8-1) 1.  $aa \in M \ \& \ bb \in M$   
 2.  $(\forall x)(x \in M \rightarrow (axa \in M \ \& \ bxb \in M))$   
 3. *Nothing is in  $M$  except by virtue of rules 1 and 2.*

(Line 1 is called the *base* of the recursion, line 2 the *recursion step*, and line 3 is an obligatory *restriction* that is often omitted, but always understood to be included.)

The recursive step of a recursive definition looks a lot like a “circular definition”, as in the “definition” of *subset* in (8-2).

- (8-2) For any sets  $A$  and  $B$ ,  $A$  is a subset of  $B$  iff every subset of  $A$  is a subset of  $B$ .

The “definition” in (8-2) is no good; it contains a vicious circle. But (8-1) is a perfectly good recursive definition. What makes the difference? The presence of the base, and the possibility of applying the recursive step repeatedly, one iteration at a time.

The derivation of a string  $abaaba \in M$  can be presented in a form virtually identical to the form of a proof.

- (8-3) 1.  $aa \in M \ \& \ bb \in M$  Ax. 1  
 2.  $(\forall x)(x \in M \rightarrow (axa \in M \ \& \ bxb \in M))$  Ax. 2  
 3.  $aa \in M$  1, Simp.  
 4.  $aa \in M \rightarrow (aaaa \in M \ \& \ baab \in M)$  2, U.I.  
 5.  $aaaa \in M \ \& \ baab \in M$  3,4, M.P.  
 6.  $baab \in M$  5, Simp.  
 7.  $baab \in M \rightarrow (abaaba \in M \ \& \ bbaabb \in M)$  2, U.I.  
 8.  $abaaba \in M \ \& \ bbaabb \in M$  6,7, M.P.

And we could keep going. Deriving longer strings just requires longer proofs with more of the same sorts of steps.

We can similarly give a recursive definition of the wffs of statement logic. (See pp 182-183.) If we want to have the possibility of arbitrarily many basic statements,  $p, q, r, p', q', r', p'', q'',$  etc., then we have to start with a recursive definition of atomic statement, and then use that in giving a recursive definition of the set of all wffs.

**8.4. Peano’s axioms and Proof by Induction.**

In this section we will look at an axiomatic approach to the natural numbers. “Peano’s axioms” for the natural numbers, actually due to Dedekind, are one of the most well-known axiomatic systems in the history of mathematics. And they also give rise to the important *Principle of Mathematical Induction* and the related technique of *proof by induction*. (We’ll return to the semantic or model-theoretic side of Peano’s axioms in section 8.5.7.)

In the axiomatic approach to natural numbers, the aim is to set forth some essential properties of the natural numbers from which all their other properties are derivable as theorems, just as in Euclid’s axiomatization of plane geometry.

We start with three primitive (undefined) notions: two primitive predicates and one primitive constant. (i) 1-place predicate ‘is a natural number’, which we will symbolize by  $Nx$ ; (ii) a 2-place predicate ‘is a (the) successor of’: we write  $Sxy$  for ‘ $x$  is successor of  $y$ ’; (iii) the constant 0.

The axioms:

P1. N0 (0 is a natural number)

P2.  $(\forall x)(Nx \rightarrow (\exists y)(Ny \ \& \ Sx \ \& \ (\forall z)(Szx \rightarrow z = y)))$  (Every natural number has a unique successor.)

P3.  $\sim(\exists x)(Nx \ \& \ S0x)$  (0 is not the successor of any number.)

P4.  $(\forall x)(\forall y)(\forall z)(\forall w)((Nx \ \& \ Ny \ \& \ Szx \ \& \ Swy \ \& \ z=w) \rightarrow x = y)$  (No two distinct natural numbers have the same successor.)

P5. If  $Q$  is a property which has properties (i) and (ii) below,

(i)  $Q0$  (zero has  $Q$ ), and

(ii)  $(\forall x)(\forall y)((Nx \ \& \ Qx \ \& \ Ny \ \& \ Syx) \rightarrow Qy)$  (if a natural number has  $Q$  then its successor has  $Q$ , i.e.  $Q$  is a 'hereditary' property)

then  $(\forall x)(Nx \rightarrow Qx)$  (every natural number has  $Q$ )

The fifth Peano postulate is very important; it introduces the notion of mathematical induction. It is not expressed in our familiar first-order predicate logic, because it involves quantification over a second-order property  $Q$ . Intuitively, it is an axiom that says that the natural numbers are subject to the "domino effect": Whenever you find a property that holds of ("knocks down") zero, and such that when it holds of ("knocks down") any number it must hold of its successor, you can conclude that it holds of ("knocks down") all numbers.

The first four axioms guarantee the existence of an infinite chain of numbers. The fifth one makes sure that there is no more than the one infinite chain guaranteed by the first four.

The *intended model*: 0, 1, 2, 3, ...

(Other models: we will see some in section 8.5.7.)

A simpler form of P5, suppressing  $N$  (assuming that our domain of quantification is just the natural numbers) and writing  $Succ(x)$  for the number which is successor of  $x$  (which is legitimate given that the first four axioms guarantee that the successor relation is actually a function):

For any predicate  $Q$ , if the two statements in 1 and 2 are both true of  $Q$ :

1.  $Q0$
2.  $(\forall x)(Qx \rightarrow Q(Succ(x)))$

then the following statement is also true of  $Q$ :

3.  $(\forall x)Qx$

The axiom P5 is actually the principle of mathematical induction. P5 as an axiom states that the principle of mathematical induction is valid on the natural numbers. It provides a rule of inference that can be applied to statements about the natural numbers. Any proof that uses this rule of inference is called a *proof by induction* or an *inductive proof*.

**The general form of a proof by induction:**

**First establish  $Q(0)$ .**

**Then establish (usually via conditional proof plus U.G.) the truth of the needed second premise, i.e. the truth of the statement  $(\forall x)(Q(x) \rightarrow Q(x+1))$ .**

**Then you are entitled to conclude ("by Mathematical Induction"):  $(\forall x)Q(x)$ .**

Where the hard work comes in: First, in figuring out what the relevant property  $Q$  should be, and second, in proving  $(\forall x)(Q(x) \rightarrow Q(x+1))$ .

Because the proof of  $(\forall x)(Q(x) \rightarrow Q(x+1))$  usually requires U.G. (Universal Generalization), you have to be really sure that you are considering "an arbitrary number", and proving that for *any number  $x$  at all*, if  $Q$  holds of  $x$ , then it must hold of  $x + 1$ . This takes getting used to.

Example: Prove for all  $n$  that  $0 + 1 + \dots + (n-1) + n = \frac{n(n+1)}{2}$

Steps: First identify the property  $Q$ .

$$Q(k) \text{ is: } 0 + 1 + \dots + (k-1) + k = \frac{k(k+1)}{2}$$

Then step 1: Prove  $Q(0)$

Then step 2: Prove that for all  $k$ ,  $Q(k)$  implies  $Q(k+1)$ . Do it by conditional proof. So start by assuming that  $Q(k)$  holds for some *arbitrary natural number  $k$*  and prove that  $Q$  must then hold of  $k+1$ . Then by the rule of Conditional Proof followed by U.G., you can conclude, as desired, that  $(\forall k)(Q(k) \rightarrow Q(k+1))$ .

THEN you can conclude, by Mathematical Induction, that

$$(\forall n) (0 + 1 + \dots + (n-1) + n = \frac{n(n+1)}{2})$$

**More examples in the text and in the homeworks and in the review exercises. It is entirely natural for this not to make sense at first. But try hard, and redo and/or do more exercises until you get it straight.**