CS280, Spring 2001 **Handout 13**
February 19, 2001

1. Reading: K. Rosen *Discrete Mathematics and Its Applications*, 3.2

2. The main message of this lecture:

> **Imaging that you are facing a ladder. If**
> **1) you can reach the first rung, and**
> **2) once you can get to a rung, you can always climb to the next one up, then**
> **3) you can reach any rung.**
> **(This is the essence of reasoning by induction).**

Let us analyze this reasoning mathematically. Let $R(n)$ denote *you can reach the nth rung*; in general $R(n)$ is called the **induction proposition** (which, as you see, depends on n). Then the assumptions and conclusion above can be represented as

1) $R(1)$ (this condition is called the **base** or the **basis step** of induction)
2) $\forall n(R(n) \to R(n+1))$ (this condition is called the **induction step**)
3) $\forall n R(n)$ (this is the conclusion)

Note that every detail in (1) and (2) is important for asserting (3). If the base (1) is false then what use could we make of knowing (2)? Since we cannot reach even the first rung the assertion (3) is false. Suppose (1) holds, but (2) holds not for all n (for example, does not hold only for $n = 3$). Then we know $R(1)$, $R(1) \to R(2)$, $R(2) \to R(3)$, and we also know that $R(3) \to R(4)$ is false, since (2) fails for $n = 3$. Then $R(1), R(2), R(3)$ and not $R(4)$, i.e. you cannot reach the fourth rung of the ladder, and (3) is false.

A common kinder-garden fallacy: instead of the induction step (2) to check

$2'$) $\forall n R(n) \to \forall n R(n+1)$.

From the logical point of view ($2'$) is *always true* (and therefore does not substitute the real induction step). Indeed, ($2'$) claims that if $R(n)$ holds for all n (i.e. $R(1), R(2), R(3), \ldots$), then $R(n)$ holds for all $n+1$ (i.e. $R(1+1), R(2+1), R(3+1), \ldots$, i.e. $R(2), R(3), R(4), \ldots$).

Proving the induction step. The base $R(1)$ has a very simple logical structure, whereas the induction step $\forall n(R(n) \to R(n+1))$ is a delicate logically compound statement. Its principal (outermost) logical symbol is the universal quantifier $\forall n$. A common method of proving universal statements $\forall n A(n)$ is by the universal generalization (cf. lecture 12):

- establish $A(n)$ *for an arbitrary* n, i.e. without assuming any specific properties of n and then conclude $\forall n A(n)$.

Here $A(n) = R(n) \to R(n+1)$ which we have to establish "for an arbitrary n". The usual reasoning here:

- assume $R(n)$ (called the **induction hypothesis**) and try to deduce $R(n+1)$.

This is a position where the most difficulties in grasping the induction method are concentrated. A "naive" question: why assuming $R(n)$ for an *arbitrary* n is any different from assuming $R(n)$ *for all* n (which, as we are already aware is a felony called *circular reasoning* when one assumes the statement being proved)? Use the formal logical analysis: $R(n)$ is a statement *with a free variable* n, i.e. a priori $R(n)$ may be true or false depending on n. While proving an implication $R(n) \to R(n+1)$ we do not claim that $R(n)$ is true. We are trying to say that *if* $R(n)$ *is true* then so does $R(n+1)$.

Example 13.1. Prove that $n^3 - n$ is divisible by 3 for all n. By an induction on $n \geq 0$.

Proposition: $R(n)$ is $3|(n^3 - n)$

Base: $R(1)$. Indeed, $3|(1^3 - 1) = 0$.

Induction hypothesis: Assume $R(n)$: $n^3 - n$ is divisible by 3.

Step: Consider $(n+1)^3 - (n+1) = (n^3 + 3n^2 + 3n + 1) - (n+1) = n^3 + 3n^2 + 3n - n = (n^3 - n) + 3(n^2 + n)$. The latter is divisible by 3 as a sum of two terms $n^3 - n$ (which is divisible by 3 by the induction hypothesis) and $3(n^2 + n)$ (which is divisible by 3 by its appearance). Therefore, $R(n+1)$. Thus we have established $R(n) \to R(n+1)$ for an arbitrary integer n. By the universal generalization, $\forall n(R(n) \to R(n+1))$, and the inductions step is proved.

There is nothing magic in beginning an induction with $n = 1$. We can begin with $n = 0$ or with any integer k. The base of induction will then be $R(k)$, the induction step should prove that $R(n) \to R(n+1)$ for all $n \geq k$, and the theorem will clam that $R(n)$ holds for all $n \geq k$.

Example 13.2. Prove that the powerset of an n-element set has 2^n elements. By an induction on $n \geq 0$.

Proposition: $R(n)$ is "any n-element set X has the 2^n-element powerset".

Base: $R(0)$ here is "if $|X| = 0$ then $|P(X)| = 2^0 = 1$". It holds since $|X| = 0$ yields $X = \emptyset$ yields $P(X) = \{\emptyset\}$ thus $|P(X)| = |\{\emptyset\}| = 1$.

Induction hypothesis: Assume $R(n)$, i.e. that any n-element set Y has the 2^n-element powerset". **Step.** We have to show that if a set X has $n+1$ element then $P(X)$ has 2^{n+1} elements. Since $|X| > 0$ the set X is not empty, i.e. there is $a \in X$. The set $Y = X - \{a\}$ then has exactly n elements and, by the induction hypothesis, has exactly 2^n subsets. There are two sorts of subsets $Z \subseteq X$.

1. $Z \subseteq Y$ (equivalently, $a \notin Z$). The total number of such Zs is 2^n.

2. $Z \not\subseteq Y$ (equivalently, $a \in Z$). The total number of such Zs equals to the number of subsets of the first sort. Moreover, $f(Z) = Z \cup \{a\}$ is a one-to-one correspondence between sorts 1 and 2. Indeed, f is one-to-one: if $Z_1 \neq Z_2$ then $Z_1 \cup \{a\} \neq Z_1 \cup \{a\}$ (the condition $a \notin Z_i$ is important!). Furthermore, f is onto: any Z of sort 2 contains a and thus is $Z' \cup \{a\} = f(Z')$ for some Z' of sort 1. We have just established that there are 2^n subsets of X of sort 1 and 2^n subsets of X of sort 2, which gives the total number of subsets in X equal to $2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$.

The inductive step may be even more sophisticated, for example

$2'')$ $\forall n[R(1) \wedge R(2) \wedge \ldots \wedge R(n) \to R(n+1)]$.

Example 13.3. Every integer $n > 1$ is a product of primes.

Proposition: $R(n)$ is "n is a product of primes".

Base: $n = 2$ is itself a prime.

Induction hypothesis: $R(2) \wedge R(3) \wedge \ldots \wedge R(n)$.

Step. Consider $n+1$. If $n+1$ is prime, we are done with $R(n+1)$. Otherwise $n+1 = q \cdot r$, where both $1 < q, r < (n+1)$. By the induction hypothesis, both $R(q)$ and $R(r)$ hold, therefore both q, r are products of primes, so is $q \cdot r = (n+1)$.

Homework assignments. (due Friday 02/23).

13A:Rosen3.2-2; 13B:Rosen3.2-14; 13C:Rosen3.2-20; 13D:Rosen3.2-48