CS 2742 (Logic in Computer Science) – Winter 2014
Lecture 21

Antonina Kolokolova

March 17, 2014

Recall that a proof by strong induction has the following form:

Let $P(n)$ be a property that is defined for integers n, and let a be a fixed integer. Suppose the following two statements are true:

1) **Base case**: for some $b \geq a$, $\forall a \leq c \leq b, P(c)$ is true.

2) **Induction step:** $(\forall i, b \leq i < kP(i)) \rightarrow P(k)$

Then the statement

$$\text{for all integers } n \geq a,\ P(n)$$

is true.

The following is a classical example of using strong induction. It shows how it is applicable in cases where we do not know beforehead which elements between the base case and k we need to use.

Example 1 (Divisibility by prime)**.** Show that for every natural number $n \geq 2$, n is divisible by a prime number.
Proof: Let $P(n)$ be a predicate $\exists p \in \mathbb{N}, 2 \leq p < n,\ p|n \wedge \forall q, q \not| p$. Here, the notation $q \not| p$ ("q does not divide p") means that there is no such integer r that $p = qr$.
`Base case:` 2 is a prime, so it is divisible by itself.
`Induction hypothesis:` Assume that for all numbers i, $2 \leq i < k$, i is divisible by a prime number p (that is, $\exists p \geq 2$ such that $p|i$).
`Induction step:` Look at a number k. If k is prime, done, since k is divisible by itself. If it is not, then by definition of a number being not prime $\exists a, b \geq 2$, $k = ab$. Take a to be our i from induction hypothesis. By induction hypothesis, there is a prime numbers $p \geq 2$ such that $p|a$ Since the division relation is transitive, $p|k$. Here, we don't even need to use the

induction hypothesis for b; we would if we were proving the Unique Factorization Theorem that says that any number can be represented as a product of powers of primes.

Here, we relied heavily on having the strong induction hypothesis, because a and b can be any numbers between 2 and $k/2$.

The following is a long example of a known theorem proved by induction (using both the usual and strong induction). Although we only did existence part in class, here I am including both parts, for completeness.

Theorem 1 (Existence and uniqueness of binary integer representation.)**.** *We all rely on the fact that any positive integer can be written as a binary string. But how do we convince ourselves that any integer can be written that way, and, moreover, every binary string (under some assumptions) encodes a unique integer? In this example we will show that there is a bijection between positive integers $n > 0$ and binary strings starting with 1.*

More precisely, we want to prove that $\forall n > 0$, $\exists r, c_r \dots c_0$ such that $c_r = 1$, $c_i \in \{0, 1\}$ for $0 \leq i < r$ and $n = \Sigma_{i=0}^{r} c_i 2^i = c_r 2^r + c_{r-1} 2^{r-1} + \dots + c_1 \cdot 2 + c_0$, and that such $r, c_r \dots c_0$ are unique.

Proof. We will start by proving the existence, and then prove the uniqueness separately.

Existence. The proof is by strong induction. We are working with the following predicate $P(n) : \exists r \in \mathbb{N}, c_r \dots c_0 \in \{0, 1\}\ c_r = 1 \wedge n = \Sigma_{i=0}^{r} c_i 2^i$.
`Base case:` $P(1)$: for $n = 1$, take $r = 0$ and $c_r = 1$. Then $1 = c_0 \cdot 2^0 = 1 \cdot 1 = 1$.
`Induction hypothesis`. Since this is a strong induction argument, the induction hypothesis is as follows: assume that $\forall m, 1 \leq m < k, \exists r \in \mathbb{N}, c_r \dots c_0 \in \{0, 1\}$ such that $c_r = 1$ and $m = c_r 2^r + \dots + c_1 \cdot 2 + c_0$.
`Induction step.` Now we will show that there exist $r', c'_{r'}, \dots, c'_0 \in \{0, 1\}$ with $c'_{r'} = 1$ and $k = \Sigma_{i=0}^{r'} c'_i 2^i$. The idea is to use the values of r and $c'_i s$ existence of which is given to us by the induction hypothesis, to explicitly construct the new r' and the new c'_i's (if we are able to construct it, it must exist).

Consider two cases. First, suppose that k is even. That is, there exists $m < k$ such that $k = 2m$. In that case, since m satisfies the conditions of the induction hypothesis, $k = 2(c_r 2^r + \dots + c_0) = \Sigma_{i=0}^{r} c_i 2^{i+1}$. It is easy to see that this formula gives us a binary representation of k with all coefficients shifted to the next power of 2, that is, $r' = r + 1$, $c'_{i+1} = c_i$ for all $i \leq r$ and $c'_0 = 0$. Thus, we have constructed $r', c'_{r'} \dots c_0$ which define a binary representation of number k.

Now suppose that k is odd, that is, for some $m < k$, $k = 2m + 1$. We obtain r' and $c'_{r'} \dots c'_1$ the same way as before, and in this case, $c'_0 = 1$ gives us the right answer.

This completes the proof of the induction step. Therefore, for any k there exists a binary representation. Our next step will be to show that such a representation is unique.

Uniqueness. Suppose, that there are two representations of the same number n, first with $r, c_r \dots c_0$ and the second with q terms instead of r and $d_q \dots d_0$ for the coefficients. To prove the uniqueness we will show that they must be the same, that is, $r = q$ and $\forall i \leq r, c_i = d_i$. To help us with the proof, we will need the following lemma.

Lemma 1. *For any n, $2^n > \Sigma_{i=0}^{n-1} 2^i$.*

Proof. For the intuition, think about $7 = 2^2 + 2^1 + 2^0 < 8 = 2^3$. We will show, using induction, that this is true for all powers of 2. In fact, this is true even when 2 is replaced by any natural number greater than 1.

We will prove this by induction (the usual weak induction this time). Here, $P(n) : 2^n > \Sigma_{i=0}^{n-1} 2^i$.
`Base case`: $P(1) : 2^1 = 2, \Sigma_{i=0}^{0} 2^i = 2^0 = 1, 2 > 1$
`Induction hypothesis`: Assume $P(k)$, that is, that $2^k > \Sigma_{i=0}^{k-1} 2^i$.
`Induction step:` Now show $P(k+1)$, that is, that $2^{k+1} > \Sigma_{i=0}^{k} 2^i$. This is simple: $2^{k+1} = 2^k + 2^k > 2^k + \Sigma_{i=1}^{k} 2^i = \Sigma_{i=1}^{k+1} 2^i$ The unequality is by induction hypothesis, the first equality is by the algebraic manipulations and the last by the definition of a Σ.
This completes the proof that $\forall n \geq 1, 2^n > \Sigma_{i=0}^{n-1} 2^i$. □

A corollary of this lemma is that for any $m < n$, $2^n > \Sigma_{i=1}^{m} 2^i$. The reason for that is that $\Sigma_{i=1}^{m} 2^i = \Sigma_{i=1}^{n-1} 2^i - \Sigma_{i=m+1}^{n-1} 2^i$. The second sum is a positive number if $m < n + 1$, and a 0 otherwise, therefore the difference is $\Sigma_{i=1}^{n-1} 2^i$. or even less, which is what we wanted to prove.

Now we come back to the proof of uniqueness of binary representation. Remember that we are trying to prove the equality of any two representations of the same number n, first with $r, c_r \dots c_0$ and the second with q terms instead of r and $d_q \dots d_0$ for the coefficients.

Suppose they are not the same. Then there are two cases: either $r \neq q$ or $r = q$. Consider the first case. Without loss of generality, let $r > q$. By our definition of binary representation, then $c_r = 1$. Therefore, $n \geq 2^r$ (the equality is achieved when all the other coefficients c_i are 0s.) Now, consider the number $\Sigma_{i=1}^{q} 2^i$. This number is greater than the number in the second representation (here, we set all d_i's to 1). Now, $n \leq \Sigma_{i=1}^{q} 2^i < 2^r \leq n$, where the middle unequality comes from the corollary of the lemma above. So we get $n < n$ which is a contradiction: nothing can be strictly less than itself.

Now, suppose that $r = q$, so $c_r = d_q = 1$. Now, consider the largest i where the coefficients differ, that is, $c_i \neq d_i$, but $c_r = d_r$, $c_{r-1} = d_{r-1}$, $\dots$, $c_{i+1} = d_{i+1}$. Suppose, without loss of generality, that $c_i = 1$, but $d_i = 0$. Now, consider only the part of the two representation starting with i^{th} coefficient: that is, subtract the common part $\Sigma_{j=i+1}^{r} c_j 2^j$ from both. We

assumed that $d_i = 0$; let $k < i$ be the largest such that $d_k = 1$. But now we are in the same case as for $r > q$, except our r is now i, and our q is now k so we know that these two sums must be different. Adding the same amount to two different numbers gives a different numbers, therefore, $(\Sigma_{j=i+1}^{r} c_j 2^j) + (\Sigma_{l=1}^{i} c_l 2^l) > (\Sigma_{j=i+1}^{r} c_j 2^j) + (\Sigma_{l=1}^{i} d_l 2^l)$ This completes the proof.

□