Logic in Computer Science
Chapter 15

Antonina Kolokolova

February 7, 2014

15.1 Well-ordering principle and induction

In this section we will look at one of the main tools for proving statements in mathematics, that of mathematical induction. We will start with a related principle called well-ordering principle, and proceed to the standard induction, and then some variations.

Well-ordering theorem: Every set can be well-ordered (that is, $\forall x \exists y (y \leq x)$. In particular, for natural numbers this translates into the following statement (well-ordering principle): let S contain one or more integers all of which are greater than some fixed integer. Then S has a least element. Restating: every non-empty set of positive integers contains a smallest element.

Remember that natural numbers in set theory are defined in such a way that this principle holds (using axiom of choice).

Here is an example of applying well-ordering principle.

Example 1. Show that every amount of change $n \geq 8$ can be paid with only 3c and 5c coins.
Proof: Suppose, for the sake of contradiction, that there are some values of $n \geq 8$ such that it is not possible to pay n with 3c and 5c coins. Take the set of all such values. Since all of them are natural numbers, there is, by well-ordering principle, a minimal element in this set; let's call it k. Now, consider number $k-3$. There are two possibilities. First, it can be that $k-3 < 8$. Since $k \geq 8$ the only choices for k are $8, 9$ and 10. But $8 = 3+5$, $9 = 3*3$ and $10 = 5*2$, so in all these cases k is representable by a sum of 3s and 5s. So it should be that $k-3 \geq 8$. But then, $k-3$ is not representable as a sum of 3s and 5s either (otherwise if $k-3 = 3i+5j$, then $k = 3(i+1)+5j$.) But this contradicts the fact that k was the *smallest* such element, given to us by the well-ordering principle. Therefore, every $n \geq 8$ is representable as a sum of 3s and 5s.

15.2 Induction

The statement of mathematical induction is a contrapositive to the well-ordering principle:

Definition 1. *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) $P(a)$ is true. (called **base case**)*

*2) For all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true. (called **induction step**).*

Then the statement

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

is true.

Alternatively, the axiom of induction can be written as follows:

$$\text{for all predicates } P, (P(0) \wedge \forall k(P(k) \to P(k+1))) \to \forall n P(n)$$

Structure of a proof by induction:

1) **Predicate** State which $P(n)$ you are proving as a function of n.

2) **Base case:** Prove $P(a)$.

3) **Induction hypothesis:** State "Assume $P(k)$ holds" explicitly.

4) **Induction step:** Show how $P(k) \to P(k+1)$. That is, assuming $P(k)$ derive $P(k+1)$.

15.3 Examples of induction

In this lecture, we will see several examples of using induction to prove various statements.

Example 2. Show that for all $n \geq 0$, $0 + 1 + \cdots + n = n(n+1)/2$. This is a classical example of application of math. induction.
Proof: Predicate: $P(n) = 0 + 1 + \cdots + n = n(n+1)/2$.
Base case: $n = 0$, then $0 = 0 \cdot (1/2)$. Let's also check $n = 1$: $0 + 1 = 1 = 1 \cdot (1+1)/2$
Induction hypothesis: Assume that for some $k \geq 0$ $0 + 1 + \cdots + k = k(k+1)/2$.
Induction step: Show that $P(k) \to P(k+1)$. Take $0 + 1 + \cdots + k + (k+1) = (0 + 1 + \cdots + k) + (k+1)$. By induction hypothesis, the sum in the first parentheses is $k(k+1)/2$. Now,

$k(k+1)/2 + (k+1) = \frac{k(k+1)+2(k+1)}{2} = (k+2)(k+1)/2 = (k+1)(k+2)/2$, which is exactly the right hand side of $P(k+1)$.
Therefore, by induction, $\forall n \geq 0$, $0 + 1 + \cdots + n = n(n+1)/2$.

Note that in this case, the calculations would be slightly simpler if we would state the induction hypothesis and induction step as "Assume $P(k-1)$, prove $P(k)$". This is a valid argument, and is often used, as long as $k-1$ satisfies the restriction on n (in this case, $k - 1 \geq 0$).

Example 3. Recall the following question: show that every amount of change ≥ 8 can be paid with only 3c and 5c coins. This time we will prove this using induction
Let $P(n) : \exists i, j \geq 0\ n = 3i + 5j$
Base case: Let $n = 8$. Then $n = 3 + 5$, $i = j = 1$. For this method of solving the problem, it is also convenient to have a base case $n = 9 = 3 \cdot 3$, $i = 3$, $j = 0$.
Induction hypothesis: Assume that $\exists i, j \geq 0\ k = 3i + 5j$. This assumption gives us the i and j which we will be using in the induction step.
Induction step: We want to show that $\exists i', j' \geq 0$ such that $k + 1 = 3i' + 5j'$. Look at i and j given to us by induction hypothesis, that is, i and j such that $k = 3i + 5j$. Consider the following two cases.
Case 1: $j > 0$. That is, at least one 5c coin was used to make k. Then we can replace this 5c coin with two 3c coins to get $k + 1$. That is, $i' = i + 2$ and $j' = j' - 1$, so $k + 1 = 3i' + 5j' = 3(i + 2) + 5(j - 1)$.
Case 2: $j = 0$. Suppose that there was no 5c coin used to make up k, that is, $k = 3i$ for some i. Since $k \geq 8$, $i \geq 3$. Now, to make $k + 1$ we can take three 3c coins out of i used to make up k and replace them by two 5c coins. That is, $i' = i - 3$ and $j' = 2$. Since $i \geq 3$, $i' \geq 0$, and $k + 1 = 3i' + 5j'$. This completes the proof.

Note how here we actively used the values i and j, existence of which was given to us by the induction hypothesis, to build our new i and j existence of which we were proving in the induction step. This is one reason why it is good to write out the induction hypothesis: to see the values that are available to be used in the induction step.

Example 4. Here is an example of proving an unequality by induction: $n^2 \leq 2^n$ for $n > 3$. You have seen this already in the assignment: this unequality says that for large enough numbers the size of a powerset 2^A is always larger than the size of a Cartesian product of a set with itself $A \times A$. Another way of looking at this unequality is from the algorithmic point of view: it says that for large enough input size n, an algorithm that runs in time $O(n^2)$ always runs faster than an algorithm that runs in time $O(2^n)$ and is not in $O(n^2)$.

We will prove this unequality by induction.
Predicate $P(n) :\ n^2 \leq 2^n$.
Base case: $P(4) : 4^2 = 16 \leq 2^4$
Induction hypothesis: assume that for $k > 3$, $k^2 \leq 2^k$.
Induction step: Assuming $P(k)$, prove that $(k+1)^2 \leq 2^{k+1}$.
First, $(k+1)^2 = k^2 + 2k + 1$ and $2^{k+1} = 2 \cdot 2^k = 2^k + 2^k$. By induction hypothesis,

$k^2 + 2k + 1 \leq 2^k + 2k + 1$. It remains to show that $2k + 1 \leq 2^k$, where this is the second "copy" of 2^k in $2^k + 2^k$ expression. We could prove this by doing another induction proof, but in this case it can be done easier. Notice that it is sufficient to show that $2k + 1 \leq k^2$, because then by induction hypothesis we will get $2k + 1 \leq k^2 \leq 2^k$. To see that $2k + 1 \leq k^2$, divide both sides of the unequality by k. Since k is positive, this preserves the unequality, resulting in $2 + 1/k \leq k$. But we do know that $k > 3$, so $2 + 1/k < 3 < k$. Therefore, $2k + 1 \leq k^2 \leq 2^k$, and so $k^2 + (2k + 1) \leq 2^k + 2^k$, completing the proof.

15.4 All horses are white

Puzzle 1. What is wrong with the following induction proof of: "All horses are white"?

1) Let $P(n)$ be: any n horses are white.
2) Base case: 0 horses are white.
3) Ind. hyp.: if any set of k horses are white, then any set of $k + 1$ horses are white.

Let the proof of the induction step be as follows. Take a set of $k + 1$ horses. Remove one horse; by induction hypothesis, all remaining horses are white. Now, put that horse back in and remove another horse. The remaining horses are again white by induction hypothesis, and so is the horse we took out the first time. Therefore, these $k + 1$ horses are white, and as it was an arbitrary set of $k + 1$ horses, induction step holds.

Therefore, all horses are white.

What is the trick here? The problem is that the induction step relies on some assumption about k that is not quite valid. More precisely, it needs a different base case. The problem occurs when the proof says "Now, put that horse back in and remove another horse". But then we need to guarantee that there is "another horse" in the set. It would be true if $k \geq 1$. However, for our base case we chose $k \geq 0$. Thus, the proof does not go through without the base case of $k = 1$ (which, as our common sense tells us, is not true: there are some horses out there that are not white).

This is just an example of caveats to watch out for when doing induction proofs: make sure there are no assumptions about k that could not be handled by the base case.

15.5 Variants of induction

You have seen already the Well-Ordering Principle, which can be considered an (equivalent) variant of induction. In this lecture we will look at another (also equivalent, although looking

more powerful) variant of induction, called *strong* (or sometimes *complete*) induction. Here, instead of assuming that $P(i)$ holds for just one preceding element i, we assume that it holds for all elements from the base case up to (but not including) k, and then proceed with this stronger assumption to proving $P(k)$. We will prove the equivalence of the three principles later.

Definition 2 (Strong induction)**.** *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.

Example 5. Here is another way of solving the 3c and 5c coins problem, this time using strong induction. Recall that the goal is to prove that $\forall n \geq 8, \exists i, j \geq 0\ n = 3i + 5j$.
Proof: Let $P(n)$ be $\exists i, j \geq 0\ n = 3i + 5j$, as before.
`Base case:` This time, there are three base cases, $n = 8 = 3 \cdot 1 + 5 \cdot 1$, $n = 9 = 3 \cdot 3 + 5 \cdot 0$, and $n = 10 = 3 \cdot 0 + 5 \cdot 2$.
`Induction hypothesis` Assume that $\forall m, 8 \leq m < k$, $\exists i, j \geq 0 m = 3i + 5j$.
`Induction step.` As in the proof with well-ordering, consider $k - 3$. If $k - 3 \geq 8$, then there are i, j such that $k - 3 = 3i + 5j$ and so $k = 3(i + 1) + 5j$. Otherwise, k must be one of the three base cases $8, 9$ or 10, for which we know the corresponding i and j.

In this example, we made use of two things: first, strong induction allowed us to talk about the value of $k - 3$ as opposed to just $k - 1$. Second, we explicitly used base cases.

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 6 (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 $c_r = d_r$, $c_{r-1} = d_{r-1}$, $\ldots$, $c_{i+1} = d_{i+1}$. 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.

□

15.6 Equivalences of well-ordering, induction and complete induction.

Theorem 2. *Well-ordering principle, (weak) induction and strong induction are all equivalent to each other.*

Here is a very brief (and technical) outline of the main structure of the proof of the equivalences. The structure of the proof is circular: first we show that well-ordering implies induction, then that induction implies strong induction, and finally strong induction implies well-ordering, completing the cycle of implications.

Proof. 1) Well-ordering implies induction.
Assume well-ordering holds. Let $0 \in A$ and let $\forall i \in \mathbb{N}$, if $i \in A$ then $i + 1 \in A$. Need to show $\mathbb{N} \subset A$. The rest is by contradiction. Look at $\bar{A} = \mathbb{N} - A$. If $\mathbb{N} \not\subseteq A$, then $\bar{A}$ is nonempty. By well-ordering, $\bar{A}$ has a minimal element j. That element is > 0, since $0 \in A$. Then $j - 1$ is a natural number. But then $(j - 1) + 1$ must be in A. Contradiction.

2) Induction implies complete induction.
Prove by induction the following property: $P'(n) = \forall i < n P(i)$.

3) Complete induction implies well-ordering.
Let A be a subset of $\mathbb{N}$ with no minimal element. Show that A is empty. For any $i \in \mathbb{N}$, any number less than i is not in A. Then $i \notin A$ either (it would be the minimal element of A then). Look at the complement of A, $\bar{A}$. By complete induction, if any natural number less than i is in $\bar{A}$, then i is also in $\bar{A}$. But then every natural number is in $\bar{A}$. So A is empty.

□