# Introduction to the theory of computation
# week 2

31st May 2005

For most of this course we're interested in integers, denoted $\mathbf{Z}$, and in particular the non-negative integers (or natural numbers), denoted $\mathbf{N}$. In computer science we start count upwards from 0, (try counting on the fingers of one hand from 0 to 4, in front of a mirror) which will strike a jarring note if you are used to a calculus convention where the natural numbers start from 1.[1]

Integers and natural numbers have certain properties that we assume without proof in this course (for example, they are clSosed under multiplication and addition). Three properties of the natural numbers (principle of well-ordering, principle of mathematical induction, principle of complete induction) are so self-evident (you might even say "natural") that we don't prove them, we assume them without proof. Indeed, you CAN'T prove them from anything more basic, since they are part of the basic properties that we can't conceive of the natural numbers lacking.

## Principle of well-ordering

This principle claims that every non-empty subset of the natural numbers has a smallest element, an element that is no bigger than any other. This is something special about the natural numbers, since it is NOT true that every non-empty subset of the real numbers, integers, rational numbers, complex numbers, etcetera, has a smallest element.

This would be a simple fact to prove if we only considered finite subsets.[2] What makes it powerful is that it is also true for infinite subsets.

### Why do we believe well-ordering?

As mentioned before, this is an axiom so we don't prove it. If you're like the majority this axiom seems so obvious that you can't imagine NOT believing it. If you are spectacularly skeptical, you can either (a) look up the properties that mathematicians define the natural numbers as having, note that well-ordering (or something equivalent, see below) is one of those properties, and conclude that the natural numbers have well-ordering by definition, or (b) decide, pragmatically, that in CSC236 we behave as though the natural numbers have well-ordering, and conform in order to get along with your TAs and instructor.

### How do we use well-ordering?

The course notes (page 19) demonstrate an approach to using well-ordering. In that case, in order to show that some set $\mathbf{N} - P$ is empty, we assume it is non-empty and derive a contradiction by focusing on its smallest member.

Assignment 1, question 4a asks you to use the principle of well-ordering in a slightly different different sense, since the set of potential $q$'s and $r$'s is not empty.

We will use well-ordering to show that in any round-robin domino tournament with cycles there is a 3-cycle. What do the words mean?

1. A round-robin domino tournament among $n$ players means that each player plays each other player exactly once, and there are no draws (each player experiences either a win or a loss in each game).

2. If there are $k$ players $p_1, \ldots p_k$ whose tournament record consists of, for all $1 \leq i < k$, $p_i$ beats $p_{i+1}$ and $p_k$ beats $p_1$, we call this a $k$-cycle.

CLAIM: In any round-robin domino tournament, if there is a cycle then there is a 3-cycle.

ROUGH WORK: Is it possible to have a 1-cycle or 2-cycle? What is the connection between the possible lengths of cycles and the principle of well-ordering? How does PWO allow us to focus on the shortest cycle length? Draw some pictures of small tournaments to get some feeling about what possibilities there are.

SAMPLE SOLUTION: [3]

## Principle of simple induction

This principle claims both that if a set $P$ contains the starting value 0, and if whenever $P$ contains a natural number $i$ it also contains its next-biggest neighbour, $i + 1$, then $P$ contains all the natural numbers.

If $P$ is the set of all elements with a certain property $P$, if you can show that $P$ contains all the natural numbers, you have shown that all natural numbers have property $P$. This simple idea gets to be very powerful.

### Why do we believe in simple induction?

There are various convincing illustrations of why we believe that simple induction is true. In the Course Notes (page 18) the author shows that if some set $P$ contains 0, and if for every $i \in P$ it is true that $(i + 1) \in P$, then all the natural numbers up to 3 are in $P$. To the majority it seems obvious that we can "turn the crank" in the manner described on page 18 enough times to show that any natural number is in $P$, but a really stubborn skeptic will ask for details (and infinitely many natural numbers mean there are infinitely many details, or cranks to turn).

Here's another illustration. Stack up an infinite row of dominoes. If you show you can knock over the zeroth domino, and if you can show that every falling domino knocks over its next-higher-indexed neighbour, then it "seems reasonable" that by knocking over the zeroeth domino you will knock them all over. Now you substitute "membership in a set" for "domino falling," this is the principle of simple induction. But skeptics don't accept "seems reasonable," and will insist on a step-by-step justification that domino number 3,856,497 falls over. That could take you a long time, and the annoying skeptic will insist that you still must NOW show that domino 3,856,498 will fall over. And so on.

In all these justifications of simple induction you can hear the sound of hand-waving, or mental "..." being inserted — exactly the sort of hacks we use induction in order avoid. But, we believe induction because it seems so self-evident that we can't imagine not believing it (or, as above, we could make it part of the definition of natural numbers).

## Using simple induction

Suppose $P(n), n \in \mathbf{N}$, is some predicate of the natural numbers: a statement that is either true or false, depending on which value $n$ takes. Suppose on a case-by-case basis you can show that $P(n)$ is true for all the values of $n$ you manage to verify. One way to show that $P(n)$ is true for each $n \in \mathbf{N}$ is to turn this into a question about sets. If $P = \{x : P(x) \text{ is true}\}$ (I don't specify the universe containing $P$, since it could be $\mathbf{N}, \mathbf{R}, \mathbf{C}$, or any other feasible set), then we want to show that $\mathbf{N} \subseteq P$. This becomes a problem in simple induction.

1. Showing that $0 \in P$ means showing that $P(0)$ is true. This is called the BASE CASE (aka BASIS).

2. For each $n \in \mathbf{N}$, showing that if $n \in P$ then $(n+1) \in P$ means showing that if $P(n)$ is true, then $P(n+1)$ is true. This is called the INDUCTION STEP. The antecedent, $P(n)$ in the implication $P(n) \Rightarrow P(n+1)$ is called the INDUCTION HYPOTHESIS.

After successfully completing these two steps, you can conclude, by induction, that $\mathbf{N} \subseteq P$, which means that $P(n)$ is true for all $n \in \mathbf{N}$. Since we've already carried out this exercise once, we don't need to refer to the set $P$ in our everyday work on induction, and simply carry out the parts of steps 1 and 2 that refer to predicate $P$.

Step 1 is often pretty straightforward (it can only be true or false). It is usually harder to show that for any $n \in \mathbf{N}$, $P(n) \Rightarrow P(n+1)$. Finding out why this implication holds is what makes induction an art. Here's an example

P(N): For all natural numbers $n$, $12^n - 1$ is an integer multiple of 11.

ROUGH WORK: What is the definition of being a multiple of 11, and how do we write this algebraically? How can we write $12^{n+1}$ in terms of $12^n$? Write down (symbolically) what $P(n)$ means, and then try to manipulate this to derive $P(n+1)$.

SAMPLE SOLUTION: [4]

The proof just given is constructive — it tells you how to construct the mystery integer $k$ so that $12^n - 1 = 11k$. You could write a recursive program to do just that (see web page), and the structure of the recursive program would mimic the structure of the proof.

## Principle of complete induction

This principle asserts that if a set $P$ has the property that it contains natural number $n$ whenever it contains all the natural numbers less than $n$, then P contains all natural numbers.

Complete induction seems economical in one sense: we don't need to specify that $P$ must contain 0, since EVERY set (including the empty set) contains all the natural numbers less than 0 (read and re-read that part, if necessary)! On the other hand, complete induction seems a bit uneconomical in another sense: we can only be certain that $n$ is in $P$ if every natural number preceding $n$ is in $P$, not just $n$'s immediate predecessor. We use complete induction to show that if $P$ is the set of elements having some property $P$, and if whenever all the natural numbers less than $n$ are in $P$, then $n$ is also in $P$, then all natural numbers have property $P$.

### Why do we believe in complete induction?

The illustrations you have seen for simple induction can all be translated into illustrations of complete induction. If a set $P$ satisfies the hypothesis of complete induction (for any natural number $n$, if all the natural numbers preceding $n$ are in $P$, then $n$ is also in $P$), then certainly 0 is in $P$ (all the natural numbers preceding 0, an empty set of natural numbers, is in $P$). Once you're satisfied that 0 is in $P$, then you have to allow 1 to be in $P$ (since 0 is), and then 2 (since 0 and 1 are), and so on.

Of course, the stubborn skeptic may raise the same objection to complete induction as to induction. But the skeptic's objection doesn't stop most of us, because it seems self-evident that we can keep admitting natural numbers into $P$ by repeating the steps above.

## Using complete induction

Start with a predicate of the natural numbers $P(n)$. Proving that $P(n)$ is true for each $n \in \mathbf{N}$ can be done by showing that the corresponding set, $P$ (the set of all elements for which $P$ is true) contains $\mathbf{N}$. Here's the recipe

1. Show that for for a natural number $n$, if every natural number less than $n$ is a member of $P$, then so is $n$. This is equivalent to showing that if $P(k)$ is true for every natural number $k$ less than $n$, then so is $P(n)$.

You can always break up step 1 into more steps. Since there are no natural numbers less than 0, you can certainly establish as a base case, that $P(0)$ is true. You can then treat natural numbers greater than 0 separately, and show that if $n > 0$ and if $P(k)$ is true for every $0 \leq k < n$, then $P(n)$ is also true. Here's an example about trees (see the definitions on trees and binary trees on pages 32, 33, and 34 of the Course Notes).

Claim: Let $P(n)$ be "If a full binary tree has $n \geq 1$ nodes, then $n$ is odd." Then $\forall n \in \mathbf{N}, P(n)$.

Rough work: What is the definition of a tree, binary tree, full binary tree? Since $P(n)$ is an implication, what can we say about the case $n = 0$? What about $n = 1$? When $n > 1$, what connection is there between the structure of a full binary tree and $P(\{0, \ldots, n-1\})$?

Sample solution: [5]

Notice that the assumption that $P(k)$ is true for every positive natural number $k$ less than $n$ wasn't used in the case where $n = 1$. We could have treated $n = 1$ as a separate base case.

## Bases other than 0

Suppose you want to prove that some predicate is true for almost all natural numbers. If the claim is true starting from natural number $n'$, but perhaps not true for every natural number $0, 1, \ldots, n' - 1$, then you can set up induction to show that $P(n)$ is true for every $n \geq n'$, as follows. To convince yourself that this is equivalent to starting with the base case 0, you can mentally create a related predicate $S(n) = P(n + n')$.

1. Show that $P(n')$ is true (equivalent to showing that $S(0)$ is true).
2. Show that, for any $n \geq n'$, $P(n)$ implies $P(n + 1)$ (equivalent to showing that $S(n) \Rightarrow S(n + 1)$ for any $n \in \mathbf{N}$).

Now, conclude that $P(n)$ is true for all $n \geq n'$ (equivalent to concluding that $S(n)$ is true for all $n \in \mathbf{N}$).

Claim: There exists an integer $n_0$ such that for any integer $n \geq n_0$, postage worth $n$ cents can be made up using 3 and 5-cent stamps.

Rough work: There's two parts to this. For the existence part we need to find an integer $n_0$ that works (it needn't be minimal). The we prove the claim for all $n \geq n_0$ by either simple induction or complete induction. Notice that 3 and 5 cent stamps can make postage for any multiple of 3, any multiple of 5, and multiples of 3 plus 5, and so on. Also notice that if we can form the correct postage for $n$, we can form the postage for $n + 3$ and $n + 5$. Work this as an exercise.

## Equivalence

This material was not covered during lecture, but you should be familiar with it.

It may seem a bit troubling that these three principles have to be accepted as axioms, and you might reasonably worry that the number of axioms necessary for the natural numbers will have to increase every time we find a useful and self-evident principle. However, it turns out that if you accept just one of the three principles (take your pick) as self-evident, then you can use it to prove the other two. The course notes (pages 19 and 20) sets up a cycle of implications so that each of these implies the other two:

$$\begin{aligned} \text{well ordering} &\Rightarrow \text{simple induction} \\ \text{simple induction} &\Rightarrow \text{complete induction} \\ \text{complete induction} &\Rightarrow \text{well ordering.} \end{aligned}$$

Since implication is transitive, any principle that appears on th e left-hand side implies the other two (WO⇒SI and SI⇒CI means WO⇒CI). Here's how to build the cycle.[6]

# Notes

[1] To see how natural counting from zero can be, see *Anno's counting book*, Anno Mitsumasa, Harper-Collins 1977. The hyper-observant among you will remark that, if I really practiced what I preached, these footnotes would begin at footnote 0.

[2] Just iterate through until you find the minimum.

[3] Assume $T$ is a tournament with a cycle. For the sake of contradiction, assume that $T$ has no 3-cycle. The set $L$ of cycle lengths in $T$ is non-empty (since we have assumed that $T$ has a cycle), so by the principle of well-ordering it has a shortest cycle length $k > 3$, corresponding to some cycle $p_1, p_2, p_3, \ldots, p_k$. Consider the result of the game between $p_1$ and $p_3$. If $p_3$ won there would be a 3-cycle $p_1, p_2, p_3, p_1$, contradicting our assumption that there are no 3-cycles. If $p_3$ lost, then there is a $(k-1)$-cycle $p_1, p_3, \ldots p_k$, contradicting our assumption that the shortest cycle length is $k$. Thus the assumption that the shortest cycle length is greater than 3 leads to a contradiction, and is false. QED.

[4] Basis: $P(0)$ states that $12^0 - 1 = 0$ is an integer multiple of 11, which is certainly true, since $0 = 0 \times 11 + 0$, and 0 is certainly an integer. So $P(0)$ is true.

Induction step: I want to prove that $P(n) \Rightarrow P(n+1)$. One way to prove this implication is by direct proof: assume $P(n)$ and derive $P(n+1)$. So I assume that $12^n - 1$ is an integer multiple of 11, that is $12^n - 1 = 11k$, for some integer $k$. This can be equivalently re-written as $12^n = 11k + 1$, so $12^{n+1} = 12 \times 12^n = 12(11k+1)$, or $12^{n+1} = 11(12k+1) + 1$. Re-write this as $12^{n+1} - 1 = 11(12k+1)$, and you have shown that $12^{n+1} - 1$ is a multiple of 11, since $12k + 1$ is an integer (integers are closed under multiplication and addition), so $P(n+1)$ is true. Thus $P(n) \Rightarrow P(n+1)$.

Conclude that $P(n)$, $12^n - 1$ is an integer multiple of 11, is true for every natural number $n$. QED.

[5] Proof (complete induction): Suppose a complete binary tree has $n \geq 1$ nodes, and assume that $P(k)$ holds for every positive natural number less than $n$. We'll show that this assumption implies $P(n)$. If $n = 1$, then we're done, since 1 is obviously odd independently of any facts about binary trees. If $n > 1$, then there are more nodes than the root node, so (by the definition of full binary tree) the root has exactly two children, a left and right one. You can verify that each of these children is the root of a full binary subtree with $n_L$, and $n_R$ nodes respectively. Since the subtrees have fewer than $n$ nodes, but at least 1 node each, the inductive hypothesis says that $n_L$ and $n_R$ are odd. Counting the root plus all the nodes in the its subtrees yields $n_L + n_R + 1$ nodes in all, an odd number, so $P(n)$ is true.

Conclude that $P(n)$ is true for every positive natural number $n$. QED.

[6] well-ordering $\Rightarrow$ simple induction:

Proof (contrapositive): Assume that the principle of well ordering is true, and use this to prove the contrapositive of the principle of simple induction: for any set $A$ if $\mathbf{N} \not\subset A$ then $A$ doesn't satisfy the antecedent of the principle of simple induction ($0 \in A$, and for each $n \in \mathbf{N}$, $n \in A \Rightarrow n + 1 \in A$).
Suppose $\mathbf{N} \not\subseteq A$. Then the set of natural numbers that don't belong to $A$ (call these $\overline{A} = \mathbf{N} - A$) is non-empty, and hence has a smallest member $i$. If $i = 0$, then $0 \notin A$ and $A$ doesn't satisfy the antecedent of simple induction. If $i > 0$, then $i - 1$ is a natural number belonging to $A$, and $A$ doesn't satisfy the antecedent of simple induction, since $i - 1 \in A$ doesn't imply $i \in A$. In either case, the antecedent of simple induction doesn't hold, which proves the contrapositive of the principle of simple induction. QED.

SIMPLE INDUCTION $\Rightarrow$ COMPLETE INDUCTION:

PROOF (DIRECT): Assume that the principle of simple induction holds, and let $A$ be a set that satisfies the antecedent of complete induction (for any $n \in \mathbf{N}$, if every natural number less than $n$ is in $A$, then so is $n$). You now need to show that $A$ contains $\mathbf{N}$. First construct the largest initial segment of $\mathbf{N}$ contained in $A$: $B = \{\text{n} \in \mathbf{N} : \text{every natural number less than or equal to } n \text{ is in } A\}$. Since $B$ is a subset of $A$, if you can show that $B$ contains $\mathbf{N}$, then so does $A$.
Since $A$ contains $n \in \mathbf{N}$ if it contains every natural number that is less than $n$, $A$ contains 0, so $0 \in B$ also. If $n$ is a natural number and $n \in B$, then every natural number less than $n+1$ is an element of $A$, so (by the hypothesis of complete induction) $n+1$ is in $A$, which means (by the definition of $B$), $n+1 \in B$. By the principle of simple induction, $\mathbf{N} \subseteq B \subseteq A$. Thus simple induction implies complete induction. QED.

COMPLETE INDUCTION $\Rightarrow$ WELL-ORDERING:

PROOF (CONTRAPOSITIVE): Suppose $A$ is a subset of the natural numbers with no smallest element, and assume that the principle of complete induction is true. You can prove that $A$ is empty, or (equivalently) that $\mathbf{N} - A$ is a superset of the natural numbers, which is the contrapositive of the well-ordering principle.
Let $\overline{A} = \mathbf{N} - A$. For each natural number $n$, if every natural number less than $n$ is in $\overline{A}$, then so is $n$, since otherwise $n$ would be the smallest element of $A$, which has no smallest member. This is the antecedent of the principle of complete induction, so $\mathbf{N} \subseteq \overline{A}$. But $\mathbf{N} \subseteq \overline{A} = \mathbf{N} - A$ means that $A$ is empty. QED.