JANUARY TERM 2013
FUN and GAMES WITH DISCRETE MATHEMATICS
Module #4 (Least-Number principle, induction and strong induction, total and partial ordering, recursion)

Author: Azalea Vo
Reviewer: Louis Li
Last modified: January 22, 2013

Reading from Meyer, Mathematics for Computer Science:

- Section 2.2 discusses the Least-Number Principle (also referred to as the Well Ordering Principle). In this section you’ll find a nice template for writing proofs using this principle. Proofs for the formula for the sum of nonnegative integers and prime factorization are in the following sections.

- The introduction of sections 6.1.2 and 6.2 discuss induction and strong induction, respectively. In sections 6.1.3 and 6.2.1 you will find proofs which correspond to the examples from chapter 2.

- Definitions 7.1.1, 7.1.2, 7.3.1, and 7.5.6 formally define partial and total orders and also introduce important terms. The examples in sections 7.1-7.5 should help with intuition for these relations.

- The introduction of chapter 11 describes the necessary components for defining a recursive data type. Section 11.3 illustrates how recursion and induction are related.

Warmups (try to do these before class):

- A candy store specializes in chocolate hippos and chocolate elephants. The chocolate hippos cost $3 and the chocolate elephants cost $8. Show that for any $n \geq 14$, there is a way to buy an assortment of chocolate hippos and elephants that costs exactly $n$.

- Are the following sets partially ordered? Totally ordered?
  - The negative integers, with the less than/greater than relation.
  - The power set of a nonempty set, with the relation of inclusion.
  - Words in the dictionary, with the alphabetical order relation.
Notes

1. **Least-Number Principle**
   - Every nonempty set of nonnegative integers has a smallest element.

   The Least-Number Principle is also called the Well-Ordering Principle. For any ordered set \( A \), \( A \) is said to be *well ordered* if for every \( B \subseteq A \), \( B \) has a smallest element. The natural numbers are a well ordered set. The integers are not a well ordered set.

2. **Induction and Strong Induction**
   Let \( P(x) \) be a predicate and \( m, n \) nonnegative integers.
   - Principle of Induction: If \( P(m) \) is true and \( P(n) \Rightarrow P(n+1) \) for all \( n \geq m \), then \( P(n) \) is true for all \( n \geq m \).
   - Principle of Strong Induction: If \( P(m) \) is true and \( P(m), P(m+1), \ldots, P(n) \) together \( \Rightarrow P(n+1) \) for all \( n \geq m \), then \( P(n) \) is true for all \( n \geq m \).

When writing a proof using induction it is necessary to include a statement of the proposition, proof of the base case, proof of the inductive step, and the conclusion. Be sure to think carefully about what is being inducted on, a step? a length? sides of tiles? In some problems it may be beneficial to break down by cases if the inductive step is more involved.

3. **Least-Number Principle and Induction**
   - The Least-Number principle and the principle of induction are equivalent.

A proof that relies on either principle can be reformulated using the other. However, in many cases it is evident which principle is easiest to reason about when writing a proof.

The equivalence of the two principles can be shown by deriving each one from the other. A sketch of this proof in both directions is provided here.

*From the Least-Number principle to the principle of induction*. Proof by contradiction. Let \( S \) be the subset of natural numbers for which a given property holds. We want to show that if \( 1 \in S \) (base case) and \( n \in S \Rightarrow n + 1 \in S \) (inductive step), then \( S = \mathbb{N} \). To do this we suppose \( \mathbb{N} \setminus S \) is nonempty. Using the base case and the inductive step, it can be shown that there is no smallest element of \( \mathbb{N} \setminus S \), which violates the Least-Number principle. This set must be empty, which is a contradiction, and \( S = \mathbb{N} \).
From the principle of strong induction to the Least-Number principle. Proof by contradiction and strong induction. Suppose that the Least-Number principle is false, then there is some $S$ which is a nonempty subset of the natural numbers that has no least element. We then use strong induction to arrive at the conclusion that either $S$ must contain a least element or is empty, which contradicts our assumptions.

4. Total and Partial Ordering

A binary relation $R$, on a set $A$ is specified by a collection of ordered pairs of elements of $A$, that is $R$ is subset of $A \times A$. For $x, y \in A$, the notation $xRy$ is equivalent to $(x, y) \in R$, which can be read as “$x$ is related to $y$ in relation $R$”. Similarly, a binary relation $R$, between two sets $A$ and $B$ is a subset of $A \times B$.

Total and partial orders are properties of sets with binary relations. The notation $\prec$ is used to show the partial ordering between elements. The concept of partial ordering is important in computer science for certain problems dealing with graphs and scheduling, for example ordering based on constraints in a problem, dealing with a sequence of events. For the following properties, consider a set $A$, $x, y \in A$ and a binary relation $R$.

- Partial orders are transitive relations.
  
  A weak partial order is both antisymmetric and reflexive. Antisymmetric means for all $x \neq y, (x, y) \in R \rightarrow (y, x) \notin R$, while reflexive means that for all $x, (x, x) \in R$. For example, the $\leq$ relation on the set $\mathbb{N}$ indicates the possibility of a less than or equal relation.
  
  A strict partial order is asymmetric, meaning $(x, y) \in R \rightarrow (y, x) \notin R$ for any $x, y$. We can see this does not allow for reflexivity. For example, the $<$ relation on the set $\mathbb{N}$ indicates a strict inequality.

- Two elements $x, y$ of a set $A$ are comparable with respect to a binary relation $R$ if and only if $(x, y) \in R$ or $(y, x) \in R$.
  
  A set is totally ordered if every pair of distinct elements in the set is comparable. A set with this property is called a chain. A set is an antichain if every pair of elements are incomparable.

5. Recursion

A recursive data type is specified by a two part definition consisting of a base case and a constructor case. The constructor case is a set of rules defining a new case based on a previous case or cases. In such a way, all other case can be constructed from the base case. This seems very similar to the structure of proofs using induction, and in fact, induction operates on these recursive data types.
Recursion in computer science usually refers to the use of a recursive function, whose implementation references itself. Divide-and-conquer is a common problem solving strategy using recursion, and it can used when a problem can be divided into sub-problems, solved, and then combined. Each sub-problem can again be divided until reaching the base (or terminating case) at which point the solutions are combined. When writing recursive code, induction can be used to prove statements about the results of the code execution.

For example, when using divide-and-conquer, consider the time taken to compute the solution. Suppose we have a problem of size $n$ that can be divided into a smaller sub-problems of size $\frac{n}{b}$. Then we can determine a function $T(n)$ which gives us the runtime of the problem of size $n$. We can write the following:

$$T(n) = \begin{cases} 
\Theta(1) & n \leq c \\
aT\left(\frac{n}{b}\right) + D(n) + C(n) & n > c 
\end{cases}$$

Here, $\Theta(1)$ refers to a constant time taken to evaluate our base case(s) where $n$ is less than or equal to some value $c$. We will return to asymptotics in the next module. $D(n)$ and $C(n)$ refer to the time needed to divide our problem of size $n$ and combine the solutions of the sub-problems, respectively. The $aT\left(\frac{n}{b}\right)$ term is the time needed for our sub-problems to be solved. As with the divide-and-conquer approach, the runtime is also describe using recursion. It is possible to find a closed-form solution for this relation which uses no recursion, and once this is found, a proof by induction is necessary to show equivalence.
Sample problems

1. Consider real numbers in the interval \([0,1]\) with respect to the relationship “\(<\)”. Is this partially ordered? Totally ordered? Well ordered?

2. Let \(S\) be the sequence \(a_1, a_2, a_3, \ldots\) where \(a_1 = 1, a_2 = 2, a_3 = 3\), and \(a_n = a_{n-1} + a_{n-2} + a_{n-3}\). Prove that \(a_n < 2^n\).
   
   (a) By induction

   (b) Using the Least-Number principle
3. Consider \( S = \{1, 2, 3, 4, 5, 6, 12, 15, 20, 60\} \) and the division relation: \( a \preceq b \) iff \( a|b \) (read as “a divides b”). Find a maximum length chain.

4. Define a sorted list \( L \) as a sequence of natural numbers \( a_1, a_2, a_3, \ldots, a_n \) where \( a_1 \leq a_2 \leq a_3 \leq \cdots \leq a_n \). Now consider a second definition of a sorted list:

- A sequence consisting of a single natural number \( a_1 \) is a sorted list.
- Given all \( a_i, b \in \mathbb{N} \), if a sequence \( a_1, a_2, a_3, \ldots, a_n \) is a sorted list and \( a_n \leq b \), then \( a_1, a_2, a_3, \ldots, a_n, b \) is also a sorted list.

Prove that these definitions are equivalent.
Small group exercises

1. Proofs using induction or the Least-Number principle

   (a) Let $A$ be a set with $n \geq 0$ elements. Prove that the power set of $A$ has $2^n$ elements.

   (b) Let $x$ and $y$ be distinct integers. Prove that for each $n \in \mathbb{N}$, $x - y$ divides $x^n - y^n$.

   *Hint:* $x^{n+1} - y^{n+1} = x(x^n - y^n + y^n) - y(y^n)$
2. Ordering

(a) Consider $\mathcal{P}\{1, 2, 3, \ldots, n\}$ and the subset relation, $\subset$. Is this a weak partial order? Strict partial order? Find a maximum length chain and explain why this is the maximum length.

(b) Consider each element of $\mathcal{P}\{0, 1\} \times \{0, 1\}$ as a binary relation on $\{0, 1\}$. Which of these relations are weak partial orders? Strict partial orders?

(c) Consider the set $\mathbb{N} \times \mathbb{N}$ and with the relation defined for all $a, b \in \mathbb{N}$:

$$(a, b) \prec (a + 1, b)$$
$$(a, b) \prec (a, b + 1)$$
$$(a, b) \prec (a + 1, b + 1)$$

This means that $(3,4)$ and $(4,3)$ are incomparable. Can you find a chain of length 6 with maximal element $(3, 2)$? In general, if given a maximal pair $(m, n)$ the maximum chain is of length at most $m + n + 1$. Briefly explain, but do not prove, why this is true.

(d) Consider the following list of chains. Can you find a total ordering so that these relations hold?

$$f \prec d \prec l \prec m$$
$$f \prec i \prec b \prec d \prec a \prec k$$
$$e \prec n \prec k \prec j \prec m \prec h$$
$$e \prec i \prec d \prec g \prec j \prec l \prec c$$
Homework problems.

1. The Fibonacci numbers are defined $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$. Prove in two ways, first by using strong induction then by using the Least-Number principle that for all $n \geq 2$:

$$F_n \geq \phi^{n-2}$$

where $\phi$ is the constant $\frac{1+\sqrt{5}}{2}$.

*Hint:* Verify that $\phi + 1 = \phi^2$.

2. Consider the natural numbers ordered by divisibility.

   (a) Is this set partially ordered? Totally ordered? Well ordered?

   (b) Prove that this set has both an infinite chain and an infinite antichain.

   (c) Consider the natural numbers $\leq 2^n$.

   Briefly explain why $1 \leq 2 \leq 4 \leq 8 \leq \cdots \leq 2^n$ is a maximum length chain.