CSL105: Discrete Mathematical Structures
I semester 2008-09
Last updated: September 15, 2008

Tutorial sheet: **Induction Principles**

---

1. Prove the following using one of the principles of mathematical induction.

   (a) The unique prime factorization theorem for positive integers greater than 1.

   (b) The binomial theorem.

   (c) Prove that
   $$1(1!) + 2(2!) + 3(3!) + \cdots + n(n!) = (n+1)! - 1$$

   Find the fallacy in the proof of the following theorem. Rectify it and again prove it using one of the principles of mathematical induction.
   Theorem.
   $$\frac{1}{1\times 2} + \frac{1}{2\times 3} + \cdots + \frac{1}{(m-1)m} = \frac{3}{2} - \frac{1}{m}$$

   Proof: For $n = 1$ the LHS is $1/2$ and so is RHS. Assume the theorem is true for $n \geq 1$. We then prove the induction step.
   $$\begin{aligned} LHS &= \frac{1}{1\times 2} + \frac{1}{2\times 3} + \frac{1}{(n-1)n} + \cdots + \frac{1}{n\times(n+1)} \\ &= \frac{3}{2} - \frac{1}{n} + \frac{1}{n(n+1)} \\ &= \frac{3}{2} - \frac{1}{n} + \frac{1}{n} - \frac{1}{(n+1)} \\ &= \frac{3}{2} - \frac{1}{n(n+1)} \end{aligned}$$

   which was required to be proved.

3. Let A be any set with a reflexive and transitive binary relation $\leq$ defined on it. That is to say, $\leq \subseteq A \times A$ satisfies the following conditions.

   (a) For every $a \in A$, $a \leq a$.

   (b) For all $a, b, c \in A$, $a \leq b$ and $b \leq c$ implies $a \leq c$. Then show by induction that $\leq; R = \leq^n; R$ for all $n \geq 1$ for any binary relation $R \subseteq A \times A$.

4. Let Σ be any finite set and let A be the set defined inductively from $B = \{\varepsilon\}$ and $K = \{.\}$ by the rules $\varepsilon \in A$, and for all $u, v \in A$, $uv \in A$. Let ε denote the empty string and satisfies the identitites $u.\varepsilon = \varepsilon.u = u$ for all $u \in \Sigma^*$.

   (a) Prove that $A = \Sigma^*$.

   (b) Give examples of strings in A that may be constructed in more than one way. A is said to be *ambiguously* generated if there is such an element of A.

   (c) A is said to be *unambiguously generated* if every $a \in A$ is either in B or there is a unique constructor $f \in K$ and unique elements $a_1, \ldots, a_{\alpha(f)} \in A$ such that $a = f(a_1, \ldots, a_{\alpha(f)})$
   Give a different definition of the set Σ^* which allows every non-empty string to be constructed uniquely from unique components.

5. Let $A \subseteq U$ be unambiguously generated from B and K. Prove that A is a well-founded set. What is the ordering on A?

6. Let A be any set. Then the set $BT(A)$ of A-labelled binary trees is the subset of $U = (A \cup \{\emptyset, (,), ,\})^*$ inductively defined by the basis set $\{\emptyset\}$ and the single constructor $bt : A \times U \times U \to U$ such that $bt(a, l, r) = (a, l, r)$.

   (a) Define by structural induction, the functions $h, \#, l : BT(A) \to \mathbb{N}$ which respectively yield the height, the number of nodes and the number of leaves in any member of $BT(A)$.

(b) Prove by the *Principle of Structural Induction* that for any $t \in BT(A)$, $\#(t) \leq 2^{h(t)} - 1$ and $l(t) \leq 2^{h(t)-1}$

(c) Let $BT_\infty(A) = \bigcup_{n \in \mathbb{N}} BT_n$ where $BT_0(A) = \{\emptyset\}$ and $BT_{k+1}(A) = BT_k \cup \{(a, l, r) \mid a \in A, l, r \in BT_k\}$. Prove that $BT(A) = BT_\infty(A)$.

7. Let $A \subseteq U$ be inductively defined by a basis set $B \neq \emptyset$ and a constructor set $K \neq \emptyset$. Let $\mathcal{X}$ be the set of all sets $X \subseteq U$ such that $B \subseteq X$ and for every constructor $\kappa \in K$, for all $x_1, \ldots, x_{\alpha(\kappa)} \in X$, $\kappa(x_1, \ldots, x_{\alpha(\kappa)}) \in X$. Prove that $A = \bigcap_{X \in \mathcal{X}} X$

8. Let $A \subseteq U$ be inductively defined by a basis B and a constructor set K. Further let $A_\infty = \bigcup_{n \in \mathbb{N}} A_n$ where $A_0 = B$ and $A_{k+1} = A_k \cup \{f(a_1, \ldots, a_{\alpha(f)}) \mid f \in K, a_1, \ldots a_{\alpha(f)} \in A_k\}$. Prove that $A = A_\infty$.

9. Let A be any alphabet and let A^* be the set of all strings of characters from A. A *language* over A is any subset of A^*. The set $\mathcal{Q}$ of *rational languages* over A is defined inductively as follows:

Basis $\emptyset \in \mathcal{Q}$ and for every $a \in A$, $\{a\} \in \mathcal{Q}$,

Induction Steps . If $L, M \in \mathcal{Q}$ then $L \cup M$, $L.M$ and L^* also belong to $\mathcal{Q}$, where $L.M = \{u.v \mid u \in L, v \in M\}$ and $L^* = \{\varepsilon\} \cup L.L^*$.

(a) For any language L define $L^R = \{w^R | w \in L\}$, i.e. L^R is the language obtained from L by reversing every string in L. Prove that if $L \in \mathcal{Q}$ then $L^R \in \mathcal{Q}$.

(b) Let $Pref(L) = \{u \in A^* \mid \exists v \in A^* : uv \in L\}$ be the set of prefixes of strings in L. Prove that if $L \in \mathcal{Q}$ then $Pref(L) \in \mathcal{Q}$.