HW 7 **Prof. Caldwell**
Due: 18 September 2008 **COSC 3015**

1

Problem 1.1. Read chapter 3 of Bird.

Problem 1.2. Do exercises 3.2.1 [1] and 3.2.4 (for finite natural numbers) using the principle of mathematical induction given on page 63. Hint for 3.2.4: Choose arbitrary $m, n \in Nat$ and do induction on p.

2 Induction Examples from Class

In class we gave the following definitions.

```
date Nat = Zero | Succ  Nat   deriving (Eq,Ord,Show)

(+) :: Nat -> Nat -> Nat
m + Zero = m
m + (Succ  n) = Succ  (m + n)
```

We can prove properties of our addition function, verifying that it really behaves like the addition we know an love, by using mathematical induction.

Lemma 2.1. $\forall m : Nat.\ \ Zero + m = m$
Proof: By induction on m. The property P is given as:

$$P(m) \stackrel{\text{def}}{=} Zero + m = m$$

Case$[P(Zero)]$ We must show $Zero + Zero = Zero$, which holds by the definition of $+$ so the base case holds.

Case$[P(Succ\ k)]$ Assume $P(k)$ and show $P(Succ\ k)$.

$$\begin{array}{rl} P(k): & Zero + k = k \\ P(Succ\ k): & Zero + (Succ\ k) = (Succ\ k) \end{array}$$

Starting on the left side of the equality $P(Succ\ k)$:

$$Zero + (Succ\ k) \stackrel{\langle\langle \text{def. of } (+)\rangle\rangle}{=} Succ\ (Zero + k) \stackrel{\langle\langle P(k)\rangle\rangle}{=} Succ\ k$$

□

[1] *i.e.* prove $\forall m : Nat.\ Succ\ Zero \times m = m$

Lemma 2.2. $\forall n : Nat.\ \forall k : Nat.\ Succ\, k + n = k + Succ\, n$
Proof: By induction on n. Then

$$P(n) \stackrel{\text{def}}{=} \forall k : Nat.\ Succ\, k + n = k + Succ\, n$$

Case$[P(Zero)]$ We must show $\forall k : Nat.\ Succ\, k + Zero = k + Succ\, Zero$. Choose arbitrary k and show $Succ\, k + Zero = k + Succ\, Zero$. But, consider the following sequences of equalities:

$$\begin{array}{l}
Succ\, k + Zero \stackrel{\langle\langle \text{def. of } (+)\rangle\rangle}{=} Succ\, k \\
k + Succ\, Zero \stackrel{\langle\langle \text{def. of } (+)\rangle\rangle}{=} Succ\, (k + Zero) \stackrel{\langle\langle \text{def. of } (+)\rangle\rangle}{=} Succ\, k
\end{array}$$

so the base case holds.
Case$[P(Succ\, m)]$ Assume $P(m)$ and show $P(Succ\, m)$.

$$\begin{array}{rl}
P(m): & \forall k : Nat.\ Succ\, k + m = k + Succ\, m \\
P(Succ\, m): & \forall k : Nat.\ Succ\, k + Succ\, m = k + Succ\, (Succ\, m)
\end{array}$$

Notice that in the second equation, substituting $Succ\, m$ for n in the term $Succ\, n$ on the right side gives $Succ\, (Succ\, m)$, this could would be an easy place to make an error. To prove $p(Succ\, m)$ holds, choose arbitrary $k \in Nat$ and show $Succ\, k + Succ\, m = k + Succ\, (Succ\, m)$ Consider the following sequences of equalities:

$$\begin{array}{l}
Succ\, k + Succ\, m \stackrel{\langle\langle \text{def. of } (+)\rangle\rangle}{=} Succ\, (Succ\, k + m) \stackrel{\langle\langle P(m)\rangle\rangle}{=} Succ\, (k + Succ\, m) \\
k + Succ\, (Succ\, m) \stackrel{\langle\langle \text{def. of } (+)\rangle\rangle}{=} Succ\, (k + Succ\, m)
\end{array}$$

$\square$

Now, we prove the commutativity of addition:

Theorem 2.1. $\forall n : Nat.\ \forall m : Nat.\ m + n = n + m$
Proof: By induction on m. Then

$$P(n) \stackrel{\text{def}}{=} \forall m : Nat.\ m + n = n + m$$

Case$[P(Zero)]$ We must show $\forall m : Nat.\ m + Zero = Zero + m$. Choose arbitrary m and notice that by definition of $(+)$ $m + Zero = m$ and by Lemma 2.1 $Zero + m = m$. Thus, the base case holds.
Case$[P(Succ\, m)]$ Assume $P(m)$ and show $P(Succ\, m)$.

$$\begin{array}{rl}
P(k): & \forall m : Nat.\ m + k = k + m \\
P(Succ\, k): & \forall m : Nat.\ m + Succ\, k = Succ\, k + m
\end{array}$$

To show $P(Succ\, k)$ choose arbitrary m and show $m + Succ\, k = Succ\, k + m$.

$$\begin{array}{l}
m + Succ\, k \\
\stackrel{\langle\langle \text{def. of } (+)\rangle\rangle}{=} Succ\, (m + k) \\
\stackrel{\langle\langle P(k)\rangle\rangle}{=} Succ\, (k + m) \\
\stackrel{\langle\langle \text{def. of } (+)[backwards]\rangle\rangle}{=} k + Succ\, m \\
\stackrel{\langle\langle (Lemma\ 2.1)\rangle\rangle}{=} Succ\, k + m
\end{array}$$

Note: In the second to last step, we use the equality $k + Succ\, m \stackrel{\langle\langle \text{def. of } (+)\rangle\rangle}{=} Succ\, (k + m)$ in the right to left direction. This can be seen as a step in which we *fold up* the definition of $(+)$.
$\square$