CS 153	**Foundations of Software**	**Homework Solution 4**
Fall 2006		**Due Oct 27, 2006**

1. [5] Suppose $\langle B, \leq_B \rangle$ is a poset and $f : A \to B$ is a total function. Give two ways of a defining partial order on the domain A such that f is monotonic, and say under what circumstances (if any) these two definitions will coincide. [What I am looking for is the "natural" way of inducing an ordering on A such that f is monotonic, and a "trivial" way of defining an order such that f is monotonic.]

We can define a partial order on A in the following ways:

(a) We can define a partial order on A in terms of the partial order on B. B has a weak partial order, in the standard way, we define a strict partial order on B, $<_B$ by excluding the identity relation on B, denoted by I_B: $<_B = \leq_B - I_B$. Then, we define a strict partial order on A by

$$a <_A b \text{ iff } f(a) <_B f(b)$$

Now we have to show that $\langle A, <_A \rangle$ is a partial order, i.e. that $\langle A, <_A \rangle$ is irreflexive, transitive, and asymmetric.

(i) Irreflexive

aNTS: $\forall a \in A. a \not<_A a$

Proof: Let $a \in A$. Then $f(a) \not< f(a)$, which implies $a \not< a$.

(ii) Transitive

By the definition of $<_A$, $a_1 <_A a_2$ and $a_2 <_A a_3 \Rightarrow f(a_1) <_B f(a_2)$ and $f(a_2) <_B f(a_3)$. By transitivity of $<_B$ this implies that $f(a_1) <_B f(a_3)$. Therefore, by definition of $<_A$, $a_1 <_A a_3$.

(iii) Asymmetric

Assume for contradiction, $a_1 <_A a_2$ and $a_2 <_A a_1$. Then by transitivity, $a_1 <_A a_1$ which contradicts the fact that $<_A$ is irreflexive.

By our definition, $a_1 <_A a_2 \Rightarrow f(a_1) <_B f(a_2)$, so f is monotonic.

(b) Consider the identity relation on A: $I_A(a,b) \Leftrightarrow a = b$

Since f is a function and thus single valued, $I_A(a,b) \Leftrightarrow f(a) = f(b)$, and hence $f(a) \leq_B f(b)$, so f is monotonic with respect to I_A. We just need to show that I_A is a partial order. First note that the identity relation on any set is certainly an equivalence relation (in fact the notion of an equivalence relation generalizes the properties of the identity relation). So I_A is reflexive and transitive (and symmetric). To show that I_A is also antisymmetric, assume that $I_A(a,b)$ and $I_A(b,a)$. Then $a = b$ simply by the definition of I_A. Hence I_A is a partial order.

2. Exercise 4.4.2 (b) (p. 267) [5]

Prove by induction that $5 + 7 + 9 + 11 + ... + (2n+3) = \sum_{k=1}^{n}(2k+3) = n^2 + 4n$

Proof by ordinary mathematical induction on n.

Base case: n=1

$(2n+3) = 5 = n^2 + 4n$

Inductive case: Consider $1 < n$, so $n = m+1$ for some m.
Induction Hypothesis: Assume the statement holds for m, i.e. $\sum_{k=1}^{m}(2k+3) = m^2 + 4m$.

Then

$$\begin{aligned}
\sum_{k=1}^{n}(2k+3) &= \sum_{k=1}^{m}(2k+3) + (2n+3) \\
&= m^2 + 4m + (2n+3) \quad \text{(by IH)} \\
&= m^2 + 4m + (2(m+1)+3) \\
&= m^2 + 4m + 2m + 2 + 3 \\
&= (m^2 + 2m + 1) + 4(m+1) \\
&= (m+1)^2 + 4(m+1) \\
&= n^2 + 4n
\end{aligned}$$

3. Exercise 4.4.8 (p. 268) [10]

Let A be a finite set, $|A| = n$. Show that $|\mathscr{P}(A)| = 2^n$.

Proof by ordinary mathematical induction on n.

Base case: n=0. Then $A = \emptyset$, so $\mathscr{P}(A) = \{\{\emptyset\}\}$ and $|\mathscr{P}(A)| = 1 = 2^0$

Inductive case: Assume $n > 1, n = m+1$ and $|A| = n$

Induction Hypothesis: For any set B, such that $|B| = m$, $|\mathscr{P}(B)| = 2^M$.

NTS: $|\mathscr{P}(A)| = 2^n$

Since $n > 1$ and $|A| = n$, we know that A is not empty. So let x be any element of A and define $B = A - \{x\}$. Then $|B| = n - 1 = m$, and by the induction hypothesis, $|\mathscr{P}(B)| = 2^m$.

Next we define a function $f : \mathscr{P}(B) \to \mathscr{P}(A)$ by $f(X) = X \cup \{x\}$. We claim that (a) f is injective, (b) $\mathscr{P}(A) = \mathscr{P}(B) \cup f(\mathscr{P}(B))$, and (c) $\mathscr{P}(B) \cap f(\mathscr{P}(B)) = \emptyset$.

(a) Let $X_1, X_2 \in \mathscr{P}(B)$ and assume that $f(X_1) = f(X_2)$. Then $X_1 \cup \{x\} = X_2 \cup \{x\}$ by the definition of f. Since x is not a member of either X_1 or X_2, this implies that $X_1 = X_2$, so f must be injective.

(b) For any $Y \in \mathscr{P}(A)$, either $x \in Y$ so that $Y = f(Y - \{x\})$ and hence $y \in f(\mathscr{P}(B))$, or $x \notin Y$, in which case $Y \in \mathscr{P}(B)$. Thus any element of $\mathscr{P}(A)$ is in $f(\mathscr{P}(B))$ or $\mathscr{P}(B)$, or $\mathscr{P}(A) = \mathscr{P}(B) \cup f(\mathscr{P}(B))$.

(c) Suppose $Z \in \mathscr{P}(B) \cap f(\mathscr{P}(B))$. Then $Z \in \mathscr{P}(B)$, implying $x \notin Z$, and $Z \in f(\mathscr{P}(B))$, implying $Z = Y \cup \{x\}$ for some $Y \in \mathscr{P}(B)$, which in turn implies $x \in Z$. Since this is impossible, we conclude there is no such Z, and hence $\mathscr{P}(B) \cap f(\mathscr{P}(B)) = \emptyset$.

Now property (a) implies that $|f(\mathscr{P}(B))| = |\mathscr{P}(B)| = m$, while (b) and (c) imply that $|\mathscr{P}(A)| = |f(\mathscr{P}(B))| + |\mathscr{P}(B)|$. Thus $|\mathscr{P}(A)| = 2m = n$.

4. Exercise 4.4.19 (b) (p. 270) [10]

Show: `isMember(a,removeAll(b,L))=isMember(a,L)`, given $\texttt{a} \neq \texttt{b}$.

First, we will introduce some notation. We will denote the empty list by the constant `nil`. Every nonempty list can be written as `L = cons(h,m)`, where `h` is the head of the list and `M` is the tail of the list.

The proof is by induction on the length of L.

Base case: `L = nil`, so $\texttt{len}(\texttt{L}) = 0$. Then

```
isMember(a,L) = isMember(a,nil) = false and
removeAll(b,L) = removeAll(b,nil) = nil implying
isMember(a,removeAll(b,L)) = isMember(a,nil) = false
```

So `isMember(a,removeAll(b,L)) = false = isMember(a,L).`

Inductive case: `L = cons(h,M)`, so $\texttt{len}(\texttt{L}) > 0$ and $\texttt{len}(\texttt{M}) = \texttt{len}(\texttt{M}) - 1$.

Induction Hypothesis: Assume the proposition holds for all lists K such that $\texttt{len}(\texttt{K}) < n$. [Note: Actually, we can prove this by *structural induction*, were we only assume the property holds for `M`, the tail of `L`.]

Case 1: `h = a`, so `L = cons(a,M).`

```
isMember(a,L)
  = isMember(a,cons(a,M))
  = true
isMember(a,removeAll(b,L))
  = isMember(a,removeAll(b,cons(a,M)))
  = isMember(a,cons(a,removeAll(b,M)))  since a ≠ b
  = true
```

So, `isMember(a,removeAll(b,L)) = true = isMember(a,L).`

Case 2: `h = b`, so `L=cons(b,M).`

```
isMember(a,L)
  = isMember(a,cons(b,M))
  = isMember(a,M) since a≠b
isMember(a,removeAll(b,L))
  = isMember(a,removeAll(b,cons(b,M)))
  = isMember(a,removeAll(b,M)))
  = isMember(a,M) by the IH
```

So, `isMember(a,removeAll(b,L)) = isMember(a,M) = isMember(a,L).`

Case 3: `L=cons(h,M)` where `h≠b` and `h≠a`.

```
isMember(a,L)
  = isMember(a,cons(h,M))
  = isMember(a,M) since a≠h
isMember(a,removeAll(b,L))
  = isMember(a,removeAll(b,cons(h,M)))
  = isMember(a,cons(h,removeAll(b,M)))  since b≠h
  = isMember(a,removeAll(b,M))  since a≠h
  = isMember(a,M) by the IH
```

So, `isMember(a,removeAll(b,L)) = isMember(a,M) = isMember(a,L).`

4. [20] (Generalized product). Let I be a nonempty set, which we will call an *index* set. A family of sets indexed by I, which we write as $\{X_i \mid i \in I\}$ is just a function $F : I \to \mathscr{P}(U)$, where the set

U is some universe such that each $X_i = F(i) \subseteq U$. For example, if $\langle A, \leq \rangle$ is a poset, we can define the family of initial segments of A by letting $I = A$ and $X_i = s(i)$, where $s(i) = \{x \in A \mid x < i\}$. Note that $X_i = \emptyset$ if i is minimal in A. [What can we use as the universe U in this example?]

Now assume that the elements in a family $\{X_i \mid i \in I\}$ are all nonempty, i.e. $X_i \neq \emptyset$ for each $i \in I$. The generalized product of this family is the set

$$\Pi_{i \in I} X_i = \{f : I \to \cup_{i \in I} X_i \mid \forall i \in I. f(i) \in X_i\}$$

Note that the function space $A \to B$ of total functions from A to B is the same as the generalized product $\Pi_{a \in A} X_a$ where $X_a = B$ for all $a \in A$.

(a). Let $I = \{0, 1\}$ and define the family $\{X_i \mid i \in I\}$ by $X_0 = A$ and $X_1 = B$. Define a function $g : A \times B \to \Pi_{i \in I} X_i$ so that g is a bijection and $\mathit{fst}(p) = (g(p))(0)$ and $\mathit{snd}(p) = (g(p))(1)$ for any $p \in A \times B$. [Here *fst* and *snd* are the first and second projections on ordered pairs, such that $\mathit{fst}(a, b) = a$ and $\mathit{snd}(a, b) = b$.]

Solution:

We will define g as follows:

$$g(a, b) = f_{a,b} : I \to \cup_{i \in I} X_i \quad \text{where } f_{a,b}(0) = a,\ f_{a,b}(1) = b$$

(i) we can verify by inspection that all $f_{a,b}$ satisfy the condition that $\forall i \in I,\ f(i) \in X_i$.

(ii) g is injective:

Assume $(a, b), (c, d) \in A \times B$ and $(a, b) \neq (c, d)$. Then either $a \neq c$, in which case $f_(a, b)(0) = a \neq b = f_(c, d)(0)$, or $b \neq d$, in which case $f_(a, b)(1) = b \neq d = f_(c, d)(1)$. In either case, $f_(a, b) \neq f_(c, d)$.

(iii) g is surjective:

Let $f \in \Pi_{i \in I} X_i$. We claim that $g(f(0), f(1)) = f$.

Proof: Let $a = f(0) \in X_0$ and $b = f(1) \in X_1$, and let $f' = g(a, b)$. Then $f'(0) = a = f(0)$ and $f'(1) = b = f(1)$, so $f' = f$.

Therefore f is a bijection.

(iv) Furthermore, we see that the condition stated in the problem holds:

$$g(a, b)(0) = f_{a,b}(0) = a = fst(a, b)$$

and

$$g(a, b)(1) = f_{a,b}(1) = b = \mathit{snd}(a, b)$$

(b). Now assume that each X_i is a (nonempty) well-founded poset with ordering $\leq_i$, and define the pointwise ordering of $\Pi_{i \in I} X_i$ by

$$f \leq_p g \quad \Leftrightarrow \quad \forall i \in I. f(i) \leq_i g(i)$$

Give two examples of such pointwise ordered families where the ordering is well-founded and non-well-founded, respectively.

Example 1:

We use the generalized product $\Pi_{i\in I} X_i$ from part (a), where $I = \{0,1\}$ and $X_0 = A$ and $X_1 = B$. We assume A and B to have well-founded partial orders $\leq_0$ and $\leq_1$, respectively. Two functions $f, f' \in \Pi_{i\in I} X_i$ are ordered by $f \leq f' \Leftrightarrow f(0) \leq_0 f'(0)$ and $f(1) \leq 1 f'(1)$.

In part (a) we saw that there is a bijection g between the cartesian product $A \times B$ and $\Pi_{i\in I} X_i$. g is also an order isomorphism if we consider $A \times B$ to be ordered by the weak pointwise ordering:

$$(a,b) \leq (c,d) \Leftrightarrow a \leq_0 c \ \wedge \ b \leq_1 c$$

So if we can show that $A \times B$ is well-founded under this ordering, it will follow that $\Pi_{i\in I} X_i$ will be well-founded under its corresponding ordering.

Now let C be a non-empty subset of $A \times B$. Since A is well-founded, there is an $a_0 \in A$ which is a minimal element of $\{a \in A \,|\, \exists b.\, (a,b) \in C\} = fst(C)$. Let $Y = \{b \in B | (a_0, b) \in C\}$. Since B is also well-founded, $\exists b_0 \in Y$ such that b_0 is the minimal element of Y.

Claim: (a_0, b_0) is minimal in C.

Proof: Suppose that $(x,y) < (a_0,b_0)$ for some $(x,y) \in C$. Then either $x <_0 a_0$, contradicting the minimality of a_0 in $fst(C)$, or $x = a_0$ and $y <_1 b_0$, contradicting the minimality of b_0 in Y. Thus no such (x,y) can exist, and (a_0,b_0) is minimal.

Therefore, it will follow by the fact that g preserves the orderings that $f_0 = g(a_0,b_0)$ is the minimal element in $g(C)$. Note that any $Z \subseteq \Pi_{i\in I} X_i$ will be equal to $g(C)$ for some $C \subseteq A \times B$, namely, $C = g^{-1}(Z)$.

Example 2:

Now consider $X_i = \mathbb{N}$ and $I = \mathbb{N}$. Here $\Pi_{i\in\mathbb{N}} \mathbb{N}$ is the same as the function space $\mathbb{N} \to \mathbb{N}$.

We define an infinite descending chain $\{g_i\}_{i\in\mathbb{N}}$ as follows:

Let $g_j(i) = 0$ if $i < j$ and $g_j(i) = 1$ if $i \geq j$.

Then for every j,

$$\begin{array}{lllll} g_j(k) & = & g_{j+1}(k) & = & 0 \quad \text{for } k = 1, \ldots, j-1 \\ g_j(k) & = & g_{j+1}(k) & = & 1 \quad \text{for } k \geq j+1 \end{array}$$

but $g_{j+1}(j) = 0 < 1 = g_j(j)$, so $g_{j+1} < g_j$ in the pointwise partial order.

Thus, there is an infinite descending chain and the pointwise order on this generalized product is not well-founded.