**CMCS 15300-1 — Foundations of Software**
**Midterm Examination Solutions**
**October 27, 2006**

**Question 1** Absorbtion Law (10 points)
Show that for any sets $A$ and $B$, $A \cap (A \cup B) = A$.

**Solution**: We show that each side of the equation is a subset of the other.

(1) $A \subseteq A \cap (A \cup B)$. For any element $x \in A$ we have $x \in A \lor x \in B$ and hence $x \in A \cup B$. It follows that $x \in A \land x \in A \cup B$, so $x \in A \cap (A \cup B)$.

(1) $A \cap (A \cup B) \subseteq A$. Suppose $x \in A \cap (A \cup B)$. Then $x \in A \land x \in A \cup B$, so $x \in A$.

**Question 2** Well-ordered sets (10 points)
A *well-ordered* set is a poset $\langle A, \leq \rangle$ such that the ordering $\leq$ is total and well-founded. Show that every nonempty subset of a well-ordered set A has a least element (which must be unique).

**Solution**: We know that because $\langle A, \leq \rangle$ is well-founded, every nonempty subset of A has a minimal element. We just need to show that if the order is total, a minimal element is also a least element. Suppose $X \subseteq A$ is nonempty, and $a \in X$ is minimal. For any $x \in X$, we know, because the order is total, that $x < a$, $x = a$, or $a < x$. The first case cannot happen because we have assumed that $a$ is minimal in $X$, so either $x = a$ or $a < x$, i.e. $a \leq x$. Since this is true of any $x \in X$, we have shown that $a$ is the least element of X. (The uniqueness of least elements is a simple consequence of the definition.)

**Question 3** Countable image (15 points)
Suppose $f : \mathbb{N} \to B$ is a surjective function. Show that $B$ is countable. (You can assume $B \neq \emptyset$.)

**Alternative Bonus version** (15 + 5 points)
Show that if $f : A \to B$ is surjective, then there exists an injection $g : B \to A$. Assume A and B are nonempty.

**Solution**: We start with the first version, assuming $f$ is a surjective function from $\mathbb{N}$ to a set $B$. Since $f$ is surjective, for each $b \in B$, the inverse image $X_b = f^{-1}(\{b\})$ is nonempty, and it is a subset of $\mathbb{N}$. Since $\mathbb{N}$ is well-ordered by the usual ordering, each inverse image sets $X_b$ has a least element, which we can denote by $\min(X_b)$. Therefore the function $g : B \to \mathbb{N}$ given by

$$g(b) = \min(X_b)$$

is well-defined for all $b \in B$. The fact that $g$ is an injection (is one-to-one) follows from the fact that for two distince elements $b_1 \neq b_2$ in $B$, the inverse image sets $f^{-1}(\{b_1\})$ and $f^{-1}(\{b_2\})$ must be disjoint because f is a function (i.e. a single-valued relation). An element $n$ in $X_{b_1} \cap X_{b_2}$ would have to be mapped to both $b_1$ and $b_2$ by the function f, which is impossible.

Since we have defined an injection $g : B \to \mathbb{N}$, it follows that $B \preceq \mathbb{N}$, which means that $B$ is countable, but not necessarily infinite.

For the Bonus version, we reason in the same way that $\{X_b \mid b \in B\}$, where $X_b = f^{-1}(\{b\})$, is a family of nonempty subsets of $A$ indexed by $B$. [Note that if $f$ is a total function, this family is the partition of $A$ associated with the kernel equivalence relation of $f$. If $f$ is partial, then it is a partition of the (strict) domain of $f$.]

The Axiom of Choice then says that the generalized product of this family,

$$\Pi_{b \in B} X_b$$

is nonempty. We can then take $g : B \to A$ to be any element of this generalized product. Such a $g$ will be injective because for any $b \in B$, $g(b) \in X_b$, and for two distinct elements $b_1, b_2 \in B$, the sets $X_{b_1}$ and $X_{b_2}$ are disjoint.

**Question 4** Monotonic function (10 points)
Suppose $A = \{a, b\}$ is a two element alphabet ordered by $a < b$, and let $\langle A^*, \leq_L \rangle$ be the poset of finite strings over $A$ with the lexicographic ordering on strings. The length function $\text{len} : A^* \to \mathbb{N}$ returns the length of a string. Is the len function monotonic with respect to the lexicographic order on strings and the normal ordering on $\mathbb{N}$? If so, prove it, and if not, give a counterexample.

**Solution**: We are given that the symbols in the alphabet $A$ are ordered by $a < b$. It follows that in the lexicographic ordering on $A^*$, the string $ab$ precedes the string $b$, i.e. $ab <_L b$. But $\text{len}(ab) = 2 > 1 = \text{len}(b)$, so len is not monotonic.

**Question 5** Well-founded induction (25 points)
The Ackermann function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is defined by

$$\begin{aligned} f(x,y) \quad = \quad & \text{if } x = 0 \text{ then } y+1 \\ & \text{else if } y = 0 \text{ then } f(x-1, 1) \\ & \text{else } f(x-1, f(x, y-1)) \end{aligned}$$

Prove that $f$ terminates for all $(x, y) \in \mathbb{N} \times \mathbb{N}$ by defining an appropriate well-founded ordering on $\mathbb{N} \times \mathbb{N}$ and using well-founded induction.

**Solution**: Take $\mathbb{N} \times \mathbb{N}$ to be ordered by the standard lexicographic ordering:

$$(x_1, y_1) \leq_l (x_2, y_2) \text{ iff } x_1 < x_2 \ \lor \ (x_1 = x_2 \ \land \ y_1 \leq y_2)$$

We prove that the Ackermann function terminates for all arguments $(x, y) \in \mathbb{N} \times \mathbb{N}$ by well-founded induction over this ordering.

**Base case**: As the base case, we will take $x = 0$, rather than just the minimal (actually *least*) element $(0, 0)$ under the lexicographic ordering, since this condition matches the first clause of the conditional expression defining the function. When $x = 0$, we have $f(x, y) = f(0, y) = y + 1$ by the first line of the definition, so $f(x, y)$ terminates.

**Induction case**: Assume that $x > 0$, and that the followiing induction hypothesis holds:

$$\textbf{IH} : \ \forall x', y' \in \mathbb{N}. \, (x', y') \leq_l (x, y) \Rightarrow \ f(x', y') \text{ terminates}$$

There are two cases to consider, depending on whether $y = 0$ or $y > 0$.

$y = 0$: In this case, the definition of $f$ tells us that

$$f(x, y) = f(x, 0) = f(x-1, 1)$$

But $(x-1, 1) \leq_l (x, y)$, so by the IH $f(x-1, 1)$ terminates, and hence $f(x, y)$ terminates.

$y > 0$: In this case the third clause of the definition of $f$ applies, so we have

$$f(x, y) = f(x-1, f(x, y-1))$$

We have $(x,y-1) \leq_l (x,y)$ so the induction hypothesis tells us that the nested recursive call $f(x,y-1)$ terminates. Let $k = f(x,y-1)$. Now we also have $(x-1,k) \leq_l (x,y)$, so the inductive hypothesis tells us that $f(x-1,k) = f(x-1, f(x,y-1))$ also terminates. Hence $f(x,y)$ terminates, and we are done.

**Question 6** Lattices (30 points)
A poset $\langle A, \leq \rangle$ is a *lattice* if for every pair of elements $x,y \in A$ (not necessarily distinct), the glb (greatest lower bound) and lub (least upper bound) of the set $\{x,y\}$ exist. We use the notation $x \wedge y$ for glb($\{x,y\}$), and $x \vee y$ for lub($\{x,y\}$). These operations are called the *meet* and *join* operations, respectively.

(a) (5 points) Show that $\langle \mathbb{N}, \leq \rangle$, where $\leq$ is the usual ordering, is a lattice, and give direct definitions of the $\wedge$ and $\vee$ operations in terms of familiar operations on numbers.

**Solution**: $\langle \mathbb{N}, \leq \rangle$ is totally ordered, so given any numbers $n$ and $m$, we will have $n \leq m$ or $m \leq n$. The greatest lower bound of $n$ and $m$ will be the lessor of the two numbers, i.e. $min(x,y)$, while the least upper bound will be the greater of the two, i.e. $max(x,y)$. Hence we have

$$\begin{aligned} x \wedge y &= min(x,y) \\ x \vee y &= max(x,y) \end{aligned}$$

(b) (5 points) Show that for any nonempty set $A$, the poset $\langle \mathscr{P}(A), \subseteq \rangle$ is a lattice, and define the meet and join operations in terms of set operations.

**Solution**: For any sets $X,Y \subseteq A$, the union $X \cup Y$ is clearly an upper bound of $X$ and $Y$ in the subset ordering. Suppose $Z$ is another upper bound, so $X \subseteq Z$ and $Y \subseteq Z$. Then $X \cup Y \subseteq Z$. Thus $X \cup Y$ is the least upper bound of $X$ and $Y$, or $X \vee Y = X \cup Y$.

On the other hand, we have $X \cap Y \subseteq X$ and $X \cap Y \subseteq Y$, so $X \cap Y$ is a lower bound of $X$ and $Y$. And for any other lower bound $Z$ such that $Z \subseteq X$ and $Z \subseteq Y$, we have $Z \subseteq X \cap Y$. Thus $X \wedge Y = X \cap Y$.

(c) (5 points) Consider the poset of partial functions from $\mathbb{N}$ to $\mathbb{N}$ (denoted $\mathbb{N} \rightarrow_p \mathbb{N}$) under the extension ordering on partial functions (i.e. $f \leq g$ if $f \subseteq g$ as relations). Show that this poset is not a lattice.

**Solution**: Let $f = \{(0,0)\}$ (the partial function that maps 0 to 0 and is undefined for $x \neq 0$), and let $g = \{(0,1)\}$. Then there is no single valued function that extends both $f$ and $g$, so $f$ and $g$ have no common upper bound, and hence $f \vee g$ is undefined. Therefore $\mathbb{N} \rightarrow_p \mathbb{N}$ is not a lattice under the subset (i.e. function extension) ordering.

For any lattice, the meet and join operations satisfy the following algebraic laws.

| | | |
|---|---|---|
| $x \wedge y = y \wedge x$ | $x \vee y = y \vee x$ | (Commutative) |
| $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ | $x \vee (y \vee z) = (x \vee (y \vee z)$ | (Associative) |
| $x \wedge (x \vee y) = x$ | $x \vee (x \wedge y) = x$ | (Absorption) |

(d) (15 points) Prove the first absorption law holds in any lattice.

**Solution**: Since $x \wedge (x \vee y)$ is the glb of $x$ and $x \vee y$, it is in particular a lower bound of $x$, so $x \wedge (x \vee y) \leq x$. Similarly, $x \leq x \vee y$, and $x \leq x$ by reflexivity, so $x$ is a lower bound of $\{x, x \vee y\}$, and so x must be less than or equal to the glb of $\{x, x \vee y\}$, or $x \leq \{x, x \vee y\}$. By antisymmetry, we have the desired equality.

**Bonus** (15 points). A structure $\langle L, \wedge, \vee \rangle$ consisting of a set $L$ and two binary operations $\wedge$ and $\vee$ on $L$ that satisfy the commutative, associative, and absorption laws given above can also be called a lattice. Show that for such a structure, an ordering $\leq$ can be defined on $L$ in terms of the meet and join operations such that meet is the glb and join is the lub.

**Solution**: We defined an ordering $\leq$ on $L$ by $x \leq y$ iff $x = x \wedge y$ (it will turn out that this is equivalent to defining $x \leq y$ when $x \vee y = y$). We need to show (a) that this is a partial ordering (i.e. it satisfies the reflexivity, antisymmetry, and transitivity laws), and (b) that under this ordering $x \wedge y$ is the glb of $\{x, y\}$ and $x \vee y$ is the lub of $\{x, y\}$.

(a). $\leq$ is a partial order.

*Reflexivity*: $x = x \wedge (x \vee (x \wedge x))$ by the first absorption law, with $y$ replaced by $(x \wedge x)$. Then by the second absorption law, the right hand argument $(x \vee (x \wedge x))$ is equal to $x$. Thus $x = x \wedge x$, and hence $x \leq x$.

> An operation like $\wedge$ that satifies the equation $x = x \wedge x$ is said to be *idempotent*. A similar proof shows that $\vee$ is also an idempotent operation.

*Antisymmetry*: Assume $x \leq y$ and $y \leq x$. Then $x = x \wedge y$ and $y = y \wedge x$ by the definition of $\leq$. But then it follows that $x = y$ by the commutativity of $\wedge$.

*Transitivity*: Assume $x \leq y$ (so $x = x \wedge y$) and $y \leq z$ (so $y = y \wedge z$). Then we have

$$\begin{aligned} x &= x \wedge y && \text{(since } x \leq y\text{)} \\ &= x \wedge (y \wedge z) && \text{(since } y \leq z\text{)} \\ &= (x \wedge y) \wedge z && \text{(associativity of } \wedge\text{)} \\ &= x \wedge z && \text{(since } x \leq y\text{)} \end{aligned}$$

So we have $x \leq z$ as required.

(b). $x \wedge y$ is glb of $\{x, y\}$.
We start by showing that $x \wedge y \leq x$.

$$\begin{aligned} (x \wedge y) \wedge x &= (x \wedge x) \wedge y && \text{(associativity and communtativity)} \\ &= x \wedge y && \text{(idempotence of } \wedge\text{)} \end{aligned}$$

Hence $x \wedge y \leq x$. Similarly we have $x \wedge y \leq y$. So $x \wedge y$ is a lower bound. Suppose $z$ is another lower bound, implying that $z = z \wedge x$ and $z = z \wedge y$. Then $z \wedge (x \wedge y) = (z \wedge x) \wedge y = z \wedge y = z$, so $z \leq x \wedge y$. Hence $x \wedge y$ is the glb.

A "dual" proof shows that that $x \vee y$ is the lub of $\{x, y\}$, provided that we prove the following lemma.

**Lemma**: $x = x \wedge y \;\Leftrightarrow\; y = x \vee y$
**Proof**: [$\Rightarrow$]: Assume $x = x \wedge y$. Then $x \vee y = (x \wedge y) \vee y = y \vee (y \wedge x) = y$, the first equality following by commutativity, and the second by the second absorption law. Therefore $y = x \vee y$.

[$\Leftarrow$]: Assume $y = x \vee y$. Then $x \wedge y = x \wedge (x \vee y) = x$, so $x = x \wedge y$.