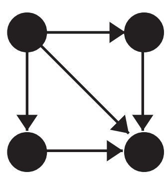
Harvey Mudd College
Computer Science 80
Logic for Computer Science
Spring Semester 1999

Assignment #1 – Mathematical Preliminaries
Sample Solution

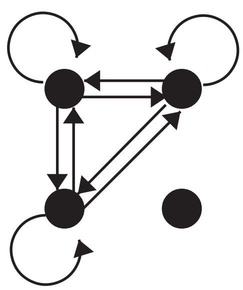
1. Using the directed graph representation used in class, provide examples of relations on a set of four objects that are:

   (There are many examples of each of these. Here is just one for each:)

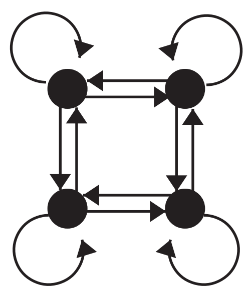
   (a) transitive, not reflexive, not symmetric



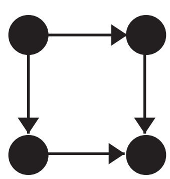
(b)transitive, symmetric, not reflexive



(c) symmetric, reflexive, not transitive



(d) anti-transitive, anti-symmetric, anti-reflexive



2. Define a *non-trivial chain* in a binary relation R as a sequence $(a_1, \ldots, a_n)$ for some $n \geq 2$ such that the a_i are distinct, and $(a_i, a_{i+1}) \in R$ for $i \in [n-1]$. A chain is a *non-trivial cycle* if (a_n, a_1) is also an element of R.

   Prove that a relation is a partial order iff it is reflexive and transitive and has no non-trivial cycles.

•••

Proof: We prove each direction separately:

($\Rightarrow$) Suppose R is a partial order. Then by definition R is reflexive and transitive, so all we need to show is that R has no non-trivial cycles. Suppose, to the contrary, that $(a_1, \ldots, a_n)$ is a non-trivial cycle in R.

Claim: $(a_1, a_i) \in R$ for all $1 \leq i \leq n$.

By induction:

Base case ($i = 1$). $(a_1, a_i) = (a_1, a_1)$, which is in R since R is reflexive.

Induction step ($i \to i+1$). Suppose $(a_1, a_j) \in R$ for all $1 \leq j \leq i$. Then since $(a_1, a_i) \in R$ by that assumption, and $(a_i, a_{i+1}) \in R$ as part of the non-trivial cycle, then, since R is transitive, $(a_1, a_{i+1}) \in R$.

Therefore, we know $(a_1, a_n) \in R$. Further, we know $(a_n, a_1) \in R$ by the definition of non-trivial cycle. Finally, $a_1 \neq a_n$ since the a_i are distinct. Together, these facts contradict the anti-symmetry of R. Therefore it is not possible for R to have non-trivial cycles.

($\Leftarrow$) Suppose R is reflexive and transitive and has no non-trivial cycles.

Claim: R is anti-symmetric.

Suppose, to the contrary, that there exist $a, b \in R$ such that $(a, b) \in R$, $(b, a) \in R$, and $a \neq b$. Then, letting a_1 be a and a_2 be b, we see that (a_1, a_2) forms a (really small) non-trivial cycle. Therefore no such a and b exist, so R is anti-symmetric.

Since we already know that R is reflexive and transitive, it must be a partial order.

3. Given two binary relations, R between A and B, and S between B and C, their *composition*, denoted by $R \circ S$, is a relation between A and C defined by the set of ordered pairs $\{(a, c) | \text{there is a } b \in B \text{ such that } (a, b) \in R \text{ and } (b, c) \in S\}$.

   (a) Let $R = \{(a, b), (a, c), (c, d), (a, a), (b, a)\}$. What is the value of $R \circ R$?

   •••

   $$R \circ R = \{(a, a), (a, b), (a, c), (a, d), (b, a), (b, b), (b, c)\}$$

   (There is a convenient way of composing binary relations by multiplying matrices of 0s and 1s. See if you can discover it.)

   (b) Prove that, given any relation R on a set A, R is transitive iff $R \circ R$ is a subset of R.

   •••

   Proof: Again, we prove each direction separately:

   ($\Rightarrow$) Suppose R is transitive. Given any $(a, c) \in R \circ R$, we need to show $(a, c) \in R$. Now since $(a, c) \in R \circ R$, there must exist a $b \in A$ such that $(a, b) \in R$ and $(b, c) \in R$. Then $(a, c) \in R$ since R is transitive.

   ($\Leftarrow$) Suppose $R \circ R \subseteq R$. Given $(a, b) \in R$ and $(b, c) \in R$, we need to show that $(a, c) \in R$. But by the definition of $R \circ R$, we must have $(a, c) \in R \circ R \subseteq R$, so $(a, c) \in R$.

4. Given a poset $(A, \leq)$, define the *lexicographic ordering*, $\ll$, on $A \times A$, induced by $\leq$, as follows:

   For all $x, y, x', y' \in A$, $(x, y) \ll (x', y')$ iff either:

   - $x = x'$ and $y = y'$, or
   - $x < x'$, or
   - $x = x'$ and $y < y'$

   Prove that if the poset $(A, \leq)$ is well-founded, then $(A \times A, \ll)$ is also well-founded. (You may assume [though you might want to confirm for yourself] that if $\leq$ is a partial order, then $\ll$ is indeed a partial order).

   • • •

   Proof: There are a couple of ways to do this. We will use the lemma that a poset is well-founded iff every non-empty subset of it has a minimal element. It is also possible to work from the definition of well-founded poset.

   Let $(A, \leq)$ be a well-founded poset. Then $(A \times A, \ll)$ is a poset (a fact which is annoying to prove, but not particularly difficult). If we can show that every non-empty subset of $A \times A$ has a minimal element, we will know that $(A \times A, \ll)$ is well-founded. With this in mind, let S be any non-empty subset of $A \times A$. We will try to find a minimal element of S.

   Letting $X = \{x \mid (x, y) \in S\}$, we know X is non-empty, and $X \subseteq A$. Then X must have a minimal element x_0. Similarly, letting $Y = \{y \mid (x_0, y) \in S\}$, we know Y is non-empty (why?), so Y has a minimal element y_0. Also, we can be sure $(x_0, y_0) \in S$ because of the way Y was defined. (If we had used $Y = \{y \mid (x, y) \in S\}$ instead, which might seem more obvious, this would not necessarily have been true.)

   Claim: (x_0, y_0) is a minimal element of S.

   Let $(a, b) \in S$, and suppose $(a, b) \ll (x_0, y_0)$. We need to show that $(a, b) = (x_0, y_0)$.

   By the definition of $\ll$, either

   - $a < x_0$, or
   - $a = x_0$ and $b < y_0$, or
   - $a = x_0$ and $b = y_0$

   But $a \in X$ and x_0 is a minimal element of X, so it can't be that $a < x_0$.

   If $a = x_0$, then $b \in Y$. But then since y_0 is a minimal element of Y, it can't be that $b < y_0$. So it's not true that $a = x_0$ and $b < y_0$.

   Since the other two cases have been eliminated, it must be that $a = x_0$ and $b = y_0$, which is just what we needed to show.

   Therefore, every non-empty subset S of $A \times A$ has a minimal element, so $(A \times A, \ll)$ is well-founded.

5. Ackerman's function on $\mathcal{N} \times \mathcal{N}$ is defined recursively in ML as:

```
fun A(x,y) = if x = 0
               then y+1
               else if y = 0
                      then A(x-1,1)
                      else A(x-1, A(x,y-1));
```

Assuming that such a recursive definition actually defines a partial function (this is non-trivial but is established in *recursive function theory*), prove by induction over the lexicographic ordering of $\mathcal{N} \times \mathcal{N}$ that Ackerman's function is in fact a total function on pairs of natural numbers.

• • •

Proof: We will use the shorthand $A(x, y) \downarrow$ to indicate that Ackermann's function is defined for the pair (x, y). Also, let $\ll_s$ be the strict order associated with $\ll$ (which will be convenient later).

Since $(\mathcal{N} \times \mathcal{N}, \ll)$ is well-founded by the last problem, we can use the principle of complete induction show that $A(x, y) \downarrow$ for all $(x, y) \in \mathcal{N} \times \mathcal{N}$. Because of the structure of PCI, it is not necessary to state and prove a base case (though there is no harm in doing so, of course). The truth of the base cases is a consequence of the form of the statement of PCI and the fact that the set is well-founded.

The proof proceeds as follows:

Let $(x, y) \in \mathcal{N} \times \mathcal{N}$, and suppose that $A(a, b) \downarrow$ for all $(a, b) \ll_s (x, y)$. We need to show that $A(x, y) \downarrow$.

By cases:

($x = 0$) In this case, $A(x, y) = y + 1$, so certainly $A(x, y) \downarrow$.

($x > 0$ and $y = 0$) Since $(x - 1, 1) \ll_s (x, y)$, we know $A(x - 1, 1) \downarrow$. Since $A(x, y) = A(x - 1, 1)$, we know that $A(x, y) \downarrow$.

($x > 0$ and $y > 0$) Since $(x, y - 1) \ll_s (x, y)$, we know $A(x, y - 1) \downarrow$. No matter what $A(x, y - 1)$ is, we know $(x - 1, A(x, y - 1)) \ll_s (x, y)$, so $A(x - 1, A(x, y - 1)) \downarrow$. Since $A(x, y) = A(x - 1, A(x, y - 1))$, we know that $A(x, y) \downarrow$.

In each case, $A(x, y) \downarrow$, which was what we needed to show.

Therefore, by the principle of complete induction, $A(x, y) \downarrow$ for every $(x, y) \in \mathcal{N} \times \mathcal{N}$.