

CSC165H1 Winter 2018: Problem Set 1

By: Eric Koehli, Conor Vedova, Jacob Chmura

January 24, 2018

1 Propositional formulas

(a) $(p \Rightarrow q) \Rightarrow \neg q$.

(i) Truth table:

p	q	$(p \Rightarrow q)$	$\neg q$	$((p \Rightarrow q) \Rightarrow \neg q)$
T	T	T	F	F
T	F	F	T	T
F	T	T	F	F
F	F	T	T	T

(ii) Since:

p	q	$(p \Rightarrow q)$	$(\neg p \vee q)$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

From the truth table above, we can see that $(p \Rightarrow q)$ is logically equivalent to $(\neg p \vee q)$ since both are *false* only if p is *true* and q is *false*, but are *true* otherwise. We can therefore use this to change the structure of our original implication:

$$\begin{aligned}
 &(p \Rightarrow q) \Rightarrow \neg q \\
 &(\neg p \vee q) \Rightarrow \neg q \\
 &\neg(\neg p \vee q) \vee \neg q \\
 &(p \wedge \neg q) \vee \neg q
 \end{aligned}$$

(b) $(p \Rightarrow \neg r) \wedge (\neg p \Rightarrow q)$.

(i) Truth table:

p	q	r	$((p \Rightarrow \neg r) \wedge (\neg p \Rightarrow q))$
T	T	T	F
T	T	F	T
T	F	T	F
F	T	T	T
F	F	T	T
T	F	F	T
F	T	F	T
F	F	F	T

(ii) The strategy will be the same as problem (ii), which is to replace the implications with $(\neg p \wedge q)$. Each line is logically equivalent to the line above:

$$\begin{aligned}
 & (p \Rightarrow \neg r) \wedge (\neg p \Rightarrow q) \\
 & (\neg p \vee \neg r) \wedge (\neg(\neg p) \vee q) \\
 & (\neg p \vee \neg r) \wedge (p \vee q)
 \end{aligned}$$

2 Fixed points

- (a) “ f has a fixed point.”:
 $\exists x \in \mathbb{N}, f(x) = x$
- (b) “ f has a *least* fixed point.”:
 $\exists x \in \mathbb{N}, \forall y \in \mathbb{N}, ((f(x) = x) \wedge (f(y) = y) \wedge (x \neq y)) \Rightarrow x < y$
- (c) “ f has a *greatest* fixed point.”:
 $\exists x \in \mathbb{N}, \forall y \in \mathbb{N}, ((f(x) = x) \wedge (f(y) = y) \wedge (x \neq y)) \Rightarrow x > y$
- (d)
 - The fixed points of f are: $\{x \in \mathbb{N} \mid 0 \leq x \leq 6\}$
 - The *least* fixed point of f is 0.
 - The *greatest* fixed point of f is 6.

For all natural numbers less than seven, we have that a division by seven will always be zero, with the remainder equal to the divisor. Therefore we have that the input and output match. Since the remainders of the division must be strictly less than the dividend, any input larger or equal to seven cannot output itself.

3 Partial Orders

- (a) An example of a binary predicate R on \mathbb{N} that is a partial order, but that is not a total order, is the divides operator.

Let $R(x, y)$ be the statement: x divides y , denoted by $x \mid y$, (where $x, y \in \mathbb{N}$). Then this binary predicate R on \mathbb{N} is a partial order because it satisfies all three partial order conditions.

- Reflexive: All numbers divide themselves to get one.
- Transitive: Suppose $n_1 \mid n_2 \wedge n_2 \mid n_3$. Then it must follow that $n_1 \mid n_3$.

Proof:

Assume $n_1 \mid n_2$. Then by the definition of divisibility,

$$\exists k_1 \in \mathbb{Z}, k_1 \cdot n_1 = n_2.$$

Assume $n_2 \mid n_3$. Then by the definition of divisibility,

$$\exists k_2 \in \mathbb{Z}, k_2 \cdot n_2 = n_3 \implies \exists k_2 \in \mathbb{Z}, k_2 \cdot (k_1 \cdot n_1) = n_3 \implies \exists k_3 \in \mathbb{Z}, \text{ that is, } (k_2 \cdot k_1), \text{ such that } k_3 \cdot n_1 = n_3$$

Therefore transitivity holds.

- Anti-Symmetric: In the realm of natural numbers, divisibility is Anti-Symmetric:

Proof:

Assume $n_1 \mid n_2$. Then by the definition of divisibility,

$$\exists k_1 \in \mathbb{Z}, k_1 \cdot n_1 = n_2.$$

Assume $n_2 \mid n_1$. Then by the definition of divisibility,

$$\exists k_2 \in \mathbb{Z}, k_2 \cdot n_2 = n_1$$

Then it must follow that $(n_1 \cdot k_1) \cdot k_2 = n_1$, in which case either n_1 and $n_2 = 0$ or $k_1 \cdot k_2 = 1$ and we have that $n_1 = n_2$

Therefore Anti-Symmetric Property holds.

$R(x, y)$ does not satisfy the total order property: $\forall x, y \in \mathbb{N}, R(x, y) \vee R(y, x)$. For instance if we choose $x = 3$ and $y = 5$, then this property does not hold over \mathbb{N} .

- (b) In order for every element to be a maximal, we examine the definition, which tells us that d is a maximal if: $\forall d' \text{ in } D, d = d' \vee \neg R(d, d')$. Therefore, we can make every element of D a *maximal*, by defining a partial order such that, $a = b = c = d$.

I define a partial order as follows:

$R(a, b) = R(b, a) = R(b, c) = R(c, b) = R(c, d) = R(d, c) = R(a, a) = R(b, b) = R(c, c) = R(d, d) = \text{True}$ and all other values are *False*.

Clearly such is reflexive since $R(a, a) = R(b, b) = R(c, c) = R(d, d) = \text{True}$ Also, since we have that whenever $R(d, d')$ is *True*, we say that $d \leq d'$;

- $a \leq b \wedge b \leq a \implies a = b$
- $b \leq c \wedge c \leq b \implies b = c$
- $c \leq d \wedge d \leq c \implies c = d$

The above is a direct result of the anti-symmetric property. Moreover, transitivity is evident since collectively, $a = b = c = d$

Lastly, such a partial order ensures a and b and c and d are all *maximal*, since all other elements in the set a, b, c, d satisfy the first condition on the left of the *or*. (*equality*)¹

- (c) We need $a \in D$ to be a *maximal* but **not** a *greatest element*. In other words, we need that none of b, c, d be larger than a but also that a is not greater than or equal to some element. The way to achieve this is to have elements that are not comparable to a .²

I define a partial order as follows:

$R(d, a) = R(d, b) = R(d, c) = R(d, d) = R(c, c) = R(b, b) = R(a, a) = \text{True}$ and all other values are *False*.

What this says is that:

- $d \leq a$
- $d \leq b$
- $d \leq c$

It does not follow from this that a is greater than or equal to every other element. In fact, a is not even comparable to every other element.

\therefore The definition of *greatest element* is not satisfied for a .

However, it *does* follow that *no other element is larger than a* , since by definition of $R(d, d')$, it follows from the partial order that $a \geq d$, and also, neither b nor c nor d can possibly be larger than a since that comparison cannot be made in the first place.

\therefore The definition of *maximal* is satisfied for a .

¹ d is a maximal if: $\forall d' \text{ in } D, d = d'$

²This requires a partial order. Had it have been asked with a total order, a *maximal* would have necessarily been a *greatest element*.

4 One-to-one functions

(a) There are $4^3 = 64$ functions from $\{1, 2, 3\} \rightarrow \{a, b, c, d\}$

- Every element in domain has 4 possible choices for an output. Therefore to get the total number of possible combinations, we must multiply: $4 \cdot 4 \cdot 4 = 4^3 = 64$.

(b) There are 24 one-to-one functions from $\{1, 2, 3\} \rightarrow \{a, b, c, d\}$

- One-to-one says that no two distinct inputs are mapped to the same output. This means that input (1) has 4 possible outputs, since none have been exhausted by a different input. Input(2) has only 3 possible outputs: all but the one chosen by input(1). By similar logic, input(3) has only 2 possible outputs. Together, there are $4 \cdot 3 \cdot 2 = 24$ one-to-one functions.

(c) There are 36 onto function from $\{1, 2, 3, 4\} \rightarrow \{a, b, c\}$

- Lets say $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c\}$. Then we know $|A| = 4 = n$ and $|B| = 3 = m$.

Lets first suppose $|A| = |B| = n$, then the first element from A could map to any particular element in B . The second element in A could map to any of the remaining $n - 1$ elements of B , and so on. Then the number of onto functions from A to B would equal $n!$.

Since $|A| > |B|$, we of course can't use the formula above to find the number of *onto functions* from A to B . We want to find the number of *onto functions* from A to B , where $n > m$. So the crux of the idea is this: if we can find all the partitions of A into groups of m , then each of those partitions describes an *onto function* from A to B , and we can simply multiply the number of partitions by $m!$. For example, the partitions of A into *six* groups of *three* include: $A = \{\{1, 2\}, 3, 4\} = \{\{1, 3\}, 2, 4\} = \{\{1, 4\}, 2, 3\} = \{1, \{2, 3\}, 4\} = \{1, \{2, 4\}, 3\} = \{1, 2, \{3, 4\}\}$. In the first partition, this says that elements 1 and 2 map to the same arbitrary element in B , 3 maps to an arbitrary element from the remaining $3 - 1$ elements, and similarly, 4 maps to last remining element in B , $3 - 2$. Since we can do this for each of the *six* functions above, we arrive at our answer of $6 \cdot 3! = 6 \cdot 3 \cdot 2 \cdot 1 = 36$.

(d) Function(R): $\forall x, \exists y_1, R(x, y_1) \wedge \forall y_2, R(x, y_2) \Rightarrow y_1 = y_2$, where $x \in \mathbb{N}, y_1 \in \mathbb{N}, y_2 \in \mathbb{N}$

(e) Onto(R): $\text{Function(R)} \wedge \forall y \in \mathbb{N}, \exists x \in \mathbb{N}, R(x, y)$

(f) One-to-one(R): $\text{Function(R)} \wedge \forall x_1, x_2, y \in \mathbb{N}, R(x_1, y) \wedge R(x_2, y) \Rightarrow x_1 = x_2$

(g) Inf(R): $\text{Function(R)} \wedge \forall x_1, y_1 \in \mathbb{N}, R(x_1, y_1), \exists x_2, y_2 \in \mathbb{N}, R(x_2, y_2) \wedge y_1 < y_2$

(h) All-but(R): \exists a set $D = \{x_1, x_2, \dots, x_c\}, \forall x_i \in D, \forall y \in \mathbb{N}, \neg R(x_i, y) \wedge \forall x_j \notin D, R(x_j, y) \wedge \exists m \in \mathbb{N}, c \leq m$