# Logic and Computability Assignment 2

**Name:** Nate Stemen (20906566)
**Email:** `nate@stemen.email`
**Due:** Jan 28, 2022 11:59PM
**Course:** PMATH 632

**Problem 1: Truth functions**

(a) Prove DeMorgan's law:

$$\dot\wedge(x, y) = \dot\neg(\dot\vee(\dot\neg(x), \dot\neg(y)))$$

for all $x, y \in \{\mathsf{T}, \mathsf{F}\}$.

(b) Show that one can similarly express $\dot\rightarrow(x, y)$ and $\dot\leftrightarrow(x, y)$ in terms of the functions $\dot\neg$ and $\dot\vee$.

(c) Express contraposition as a statement about $\dot\rightarrow$ and $\dot\neg$ and $\dot\leftrightarrow$.

**Solution.** (a) DeMorgan's law can be seen by building up the right hand side of the equality from it's components.

| $x$ | $y$ | $\dot\neg(x)$ | $\dot\neg(y)$ | $\dot\vee(\dot\neg(x), \dot\neg(y))$ | $\dot\neg(\dot\vee(\dot\neg(x), \dot\neg(y)))$ | $\dot\wedge(x, y)$ |
|---|---|---|---|---|---|---|
| T | T | F | F | F | T | T |
| T | F | F | T | T | F | F |
| F | T | T | F | T | F | F |
| F | F | T | T | T | F | F |

(b) We give the following two characterizations by truth tables for implication and the biconditional.

| $x$ | $y$ | $\dot\neg(x)$ | $\dot\vee(\dot\neg(x), y)$ | $\dot\rightarrow(x, y)$ |
|---|---|---|---|---|
| T | T | F | T | T |
| T | F | F | F | F |
| F | T | T | T | T |
| F | F | T | T | T |

| $x$ | $y$ | $\dot\wedge(x, y)$ | $\dot\wedge(\dot\neg(x), \dot\neg(y))$ | $\dot\vee(\dot\wedge(x, y), \dot\wedge(\dot\neg(x), \dot\neg(y)))$ | $\dot\leftrightarrow(x, y)$ |
|---|---|---|---|---|---|
| T | T | T | F | T | T |
| T | F | F | F | F | F |
| F | T | F | F | F | F |
| F | F | F | T | T | T |

Now since we must use only negation and disjunction we can use DeMorgan's law to write the following.

$$\begin{aligned}
\dot\leftrightarrow(x, y) &= \dot\vee(\dot\wedge(x, y), \dot\wedge(\dot\neg(x), \dot\neg(y))) \\
&= \dot\vee(\dot\neg(\dot\vee(\dot\neg(x), \dot\neg(y))), \dot\neg(\dot\vee(\dot\neg(\dot\neg(x)), \dot\neg(\dot\neg(y))))) \\
&= \dot\vee(\dot\neg(\dot\vee(\dot\neg(x), \dot\neg(y))), \dot\neg(\dot\vee(x, y)))
\end{aligned}$$

Where we've used the contentious[1] idea that negation is an involution.

[1] Okay, maybe not that contentious, but some people don't like it, right?

(c) When attempting to prove $p \implies q$ we can sometimes try and prove $\neg q \implies \neg p$. This can be encoded into the following tautology using $\dot{\leftrightarrow}$, $\dot{\neg}$, and $\dot{\rightarrow}$.

$$\dot{\leftrightarrow}(\dot{\rightarrow}(x,y), \dot{\rightarrow}(\dot{\neg}(y), \dot{\neg}(x)))$$

To see this is indeed a tautology we can use our expressions above to simplify.

$$\begin{aligned}&\dot{\leftrightarrow}(\dot{\rightarrow}(x,y), \dot{\rightarrow}(\dot{\neg}(y), \dot{\neg}(x)))\\ &\qquad = \dot{\vee}(\dot{\neg}(\dot{\vee}(\dot{\neg}(\dot{\vee}(\dot{\neg}(x),y)), \dot{\neg}(\dot{\vee}(y,\dot{\neg}(x))))), \dot{\neg}(\dot{\vee}(\dot{\vee}(\dot{\neg}(x),y), \dot{\vee}(y,\dot{\neg}(x)))))\end{aligned}$$

Now define $A := \dot{\vee}(\dot{\neg}(x), y) = \dot{\vee}(y, \dot{\neg}(x))$ where the last equality holds by the symmetry of or. We now have

$$\begin{aligned}\dot{\leftrightarrow}(\dot{\rightarrow}(x,y), \dot{\rightarrow}(\dot{\neg}(y), \dot{\neg}(x))) &= \dot{\vee}(\dot{\neg}(\dot{\vee}(\dot{\neg}(A), \dot{\neg}(A))), \dot{\neg}(\dot{\vee}(A,A)))\\ &= \dot{\vee}(\dot{\neg}(\dot{\neg}(A)), \dot{\neg}(A))\\ &= \dot{\vee}(A, \dot{\neg}(A)).\end{aligned}$$

We've now reached the infamous law of excluded middle which we take to be true, always. Thus we have a tautology, and hence proof by contraposition is a valid proof (if you take LEM).

**Problem 2**

Let $S$ be the first-order alphabet $\{R_1, R_2, f\}$ in which $R_1$ and $R_2$ are unary relation symbols and $f$ is a binary function symbol. Suppose $\mathcal{A} = (A, \mathfrak{a})$ is an $S$-structure and that $\mathcal{J} = (\mathcal{A}, \beta)$ is an $S$-interpretation and $\mathbf{\Phi}$ is the set of formulas $\{\phi_1, \phi_2, \phi_3, \phi_4\}$ with

$$\begin{aligned}
\phi_1 &= \exists v_0 \exists v_1((R_1 v_0 \wedge R_1 v_1) \wedge \neg v_0 \equiv v_1) \\
\phi_2 &= \exists v_0 \exists v_1((R_2 v_0 \wedge R_2 v_1) \wedge \neg v_0 \equiv v_1) \\
\phi_3 &= \forall v_0 \exists v_1 \exists v_2((R_1 v_1 \wedge R_2 v_2) \wedge f v_1 v_2 \equiv v_0) \\
\phi_4 &= \forall v_1 \forall v_2 \forall v_3 \forall v_4(((((R_1 v_1 \wedge R_1 v_2) \wedge R_2 v_3) \wedge R_2 v_4) \wedge f v_1 v_3 \equiv f v_2 v_4) \\
&\qquad \to (v_1 \equiv v_2 \wedge v_3 \equiv v_4)).
\end{aligned}$$

(a) Show that if $\mathcal{J} \models \mathbf{\Phi}$ and $|A|$ is finite then $|A|$ is a composite number (i.e., not prime and not 1).

(b) Show that if $|A| < \infty$ is composite then there is an $S$-interpretation $\mathcal{J}$ with universe $A$ such that $\mathcal{J} \models \mathbf{\Phi}$.

**Solution.** (a) We first interpret each equation $\phi_i$ given we know $|A|$ is finite.

$$\phi_1 = \exists v_0, v_1 \in A \quad R_1^A v_0 \text{ and } R_1^A v_1 \text{ and } v_1 \neq v_0$$

Thus $\phi_1$ is telling us there are *at least* two distinct elements that satisfy the relation $R_1^A$. Put differently, since $R_1^A \subseteq A$, we know $|R_1^A| \geq 2$. Similarly for $\phi_2$ we have

$$\phi_2 = \exists v_0, v_1 \in A \quad R_2^A v_0 \text{ and } R_2^A v_1 \text{ and } v_1 \neq v_0$$

where again this is telling us that $|R_2^A| \geq 2$, or that there are at least two elements that satisfy $R_2^A$. Moving on for $\phi_3$ we have

$$\phi_3 = \forall v_0 \in A \quad \exists v_1, v_2 \in A \quad R_1^A v_2 \text{ and } R_2^A v_2 \text{ and } f^A(v_1, v_2) = v_0.$$

This formula tells us that $f^A : A \times A \to A$ when restricted to $R_1^A \times R_2^A$ is a surjection onto $A$. That is $f^A|_{R_1^A \times R_2^A}$ is a surjection. Lastly we have

$$\phi_4 = \forall v_1, v_2, v_3, v_4 \in A \quad v_1, v_2 \in R_1^A \text{ and } v_3, v_4 \in R_2^A \text{ and } f^A(v_1, v_3) = f^A(v_2, v_4) \\ \text{imply } v_1 = v_2 \text{ and } v_3 = v_4.$$

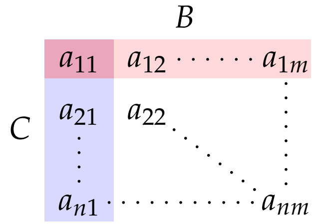
This is exactly the condition for $f^A|_{R_1^A \times R_2^A}$ being injective. This fact, together with the previous one implies $f^A$ is a bijection, and hence the domain and range have the same cardinality: $|R_1^A \times R_2^A| = |A|$. A basic property about the cardinality of finite sites $B$ and $C$ is $|B \times C| = |B| \cdot |C|$.[2] We then have $|A| = |R_1^A| \cdot |R_2^A|$ and hence a composite number.

[2]Maybe this holds for larger cardinals too, but I'm not familiar enough to say.

(b) Now take $|A| = n \cdot m$ with $n, m \in \mathbb{N}$ such that $n, m \neq 1$. Arrange the elements of $A$ in a grid as follows (in arbitrary order) and give each element a name based on it's grid position.

$$\begin{matrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & & \vdots \\ \vdots & & \ddots & \vdots \\ a_{n1} & \cdots & \cdots & a_{nm} \end{matrix}$$

Then form the following two (intersecting) subsets of $A$.




These can be written $B = \{a_{1j} \in A : 1 \leq j \leq m\}$, and $C = \{a_{i1} \in A : 1 \leq i \leq n\}$. Since $n, m > 1$ each one of these subsets must have more than one element in each. That is $|B| > 1$ and $|C| > 1$. We can then take $B$ and $C$ to be relations on $A$ and hence $\phi_1$ and $\phi_2$ are automatically satisfied with $R_1^A = B$ and $R_2^A = C$. Next we define $f^A : B \times C \to A$ as

$$f(b, c) = f(a_{1j}, a_{i1}) := a_{ij}.$$

This is clearly a bijection from $B \times C$ to $A$, and hence $\phi_3$ and $\phi_4$ are also satisfied. Hence we have constructed an $\{R_1, R_2, f\}$-structure where $\mathcal{J} \models \mathbf{\Phi}$.

**Problem 3**

In the following questions, let $S_{\mathrm{gr}} = (1, \cdot, i)$ and we only consider $S_{\mathrm{gr}}$-interpretations $\mathcal{J} = (A, \mathfrak{a}, \beta)$ in which $A$ is a group, $1^A$ is the identity of $A$, $\cdot^A$ is multiplication, and $i^A$ is the inverse map. For the following formulas $\phi$ give an informal statement of what the formula is saying and say whether $\mathcal{J} \models \phi$ for every such interpretation $\mathcal{J}$, for at least one such interpretation but not every such interpretation, or for no such interpretations.

(a) $\forall v_0 \forall v_1 \forall v_2 \cdot \cdot v_0 v_1 v_2 \equiv \cdot v_0 \cdot v_1 v_2$

(b) $\forall v_0 \forall v_1 \cdot \cdot v_0 v_1 v_1 \equiv \cdot \cdot v_1 v_0 v_1$

(c) $\exists v_0 ((\neg v_0 \equiv 1) \wedge \cdot v_0 v_0 \equiv 1)$

(d) $\exists v_0 \forall v_1 v_2 \equiv \cdot v_0 v_1$

(e) $\exists v_0 \exists v_1 v_2 \equiv \cdot v_0 v_1$

(f) $\exists v_0 \exists v_1 (\neg v_0 \equiv v_1 \vee \forall v_3 v_3 \equiv 1)$

(g) $\exists v_3 (\cdot v_3 v_2 \equiv 1 \wedge \neg v_3 \equiv i v_2)$

(h) $\forall v_0 ((\cdot v_0 v_0 \equiv 1 \wedge \cdot \cdot v_0 v_0 v_0 \equiv 1) \rightarrow v_0 \equiv 1)$

**Solution.** First, here is a summary of my solutions, with more details expounded in each part.

| Part | Holds for ___ interpretations |
|---|---|
| (a) | all |
| (b) | some |
| (c) | some |
| (d) | some |
| (e) | all |
| (f) | all |
| (g) | no |
| (h) | all |

(a) Written in infix notation this equation reads

$$\forall v_0, v_1, v_2 \in A \quad (v_0 \cdot v_1) \cdot v_2 = v_0 \cdot (v_1 \cdot v_2)$$

which clearly shows that the multiplication in the group is associative. This facts holds for every such interpretation $\mathcal{J}$ by the definition of group multiplication.

(b) Again, writing in infix notation we have

$$\forall v_0, v_1 \in A \quad (v_0 \cdot v_1) \cdot v_1 = (v_1 \cdot v_0) \cdot v_1$$

Multiplying on thr right by $v_1^{-1}$ we have $v_0 \cdot v_1 = v_1 \cdot v_0$ which is clearly only true in Abelian groups. The existence of non-Abelian groups (e.g. the permutation group) shows this formula holds in at least one such interpretation $\mathcal{J}$.

(c) In everyday math notation we might write

$$\exists v_0 \in A \quad v_0 \neq 1^A \text{ and } v_0^2 = 1^A.$$

This formula holds for at least one interpretation, but not necessarily all. To see this take the trivial group $G = (\{e\}, \cdot)$ where the only multiplication rule we have is

$e \cdot e = e$. Since $G$ is a group where this formula does not hold it cannot hold in all interpretations. That said the group $H = (\{1, -1\}, \cdot_{\mathbb{R}})$ is a group where this formula holds with $v_0 = -1$.

(d) Here we have

$$\exists v_0 \in A \ \forall v_1 \in A \quad v_2 = v_0 \cdot v_1.$$

This can be found to hold, for example, in the trivial group $G = (\{e\}, \cdot)$. We then have $v_0, v_1, v_2 = e$ and the equation reads $e = e \cdot e$ which clearly holds. That said this equation does not hold in all interpretations. To see this take the group $H = (\{1, -1\}, \cdot_{\mathbb{R}})$. Now take $v_2 = 1$ and the equation says either $1 = 1 \cdot -1 \wedge 1 = 1 \cdot 1$ *or* $1 = -1 \cdot -1 \wedge 1 = -1 \cdot 1$ which clearly neither hold.

(e) Here we have

$$\exists v_0, v_1 \in A \quad v_2 = v_0 \cdot v_1.$$

This can be found to hold in all interpretations by taking $v_0 = v_2$ and $v_1 = 1^A$.

(f)

$$\exists v_0, v_1 \in A \quad v_0 \neq v_1 \text{ or } \forall v_3 \in A \quad v_3 = 1^A$$

This formula says you either have

- two distinct elements in the group, or
- all elements in your group are the identity element.

And this holds for all interpretations $\mathcal{J}$.

(g) Here we use the notation $g^{-1}$ instead of $i^A(g)$ for familiarity.

$$\exists v_3 \in A \quad v_3 \cdot v_2 = 1^A \text{ and } v_3 \neq v_2^{-1}$$

This formula does not hold in any such interpretation $\mathcal{J}$ because of the uniqueness of (left and right) inverses in groups.

(h) Finally, in modern notation we have:

$$\forall v_0 \in A \quad v_0^2 = 1^A \text{ and } v_0^3 = 1^A \implies v_0 = 1^A.$$

This formula holds for all such interpretations $\mathcal{J}$ as follows. We can write $v_0^3 = v_0 \cdot v_0^2 = v_0 \cdot 1^A = v_0 = 1^A$. This manipulation does not use anything about a particular group and so this formula holds for all such interpretations $\mathcal{J}$.