CSC240 Winter 2024 Homework Assignment 2

due January 25, 2024

My name and student number: Haoyun (Bill) Xi 1009992019
The list of people with whom I discussed this homework assignment:
Tianchu Li
Julia Zhong Guo

1. Let $\mathcal{S}$ denote the set consisting of all 16 binary connectives. For each binary connective $\star \in \mathcal{S}$, define the following propositional formulas:

   $A^\star$ = "((P OR Q) XOR T) IMPLIES ($P \star Q$)"
   $B^\star$ = "(P OR Q) IMPLIES (($P \star Q$) XOR T)"
   $C^\star$ = "((P OR Q) XOR P) IMPLIES ((P OR Q) XOR ($P \star Q$))"
   $D^\star$ = "((P OR Q) XOR Q) IMPLIES ((P OR Q) XOR ($P \star Q$))"

   (a) For how many binary connectives $\star \in \mathcal{S}$ is the formula $A^\star$ a tautology?
   Justify your answer without using a truth table.
   Answer:
   There are 8 binary connectives total which would make the formula A^* a tautology. A^* is not a tautology when there exist a truth-value assignment for P and Q such the formula will be False. Since the main connective is an implication, A^* will be false only when premise ((P OR Q) XOR T) is True while the conclusion ($P \star Q$) is true.
   More specifically, the premise is true only when (P OR Q) is False (by definition of XOR). This means only when P and Q are false, there is a potential for A^* to be false. As long as we let $P \star Q$ be True when the premise of implication A^* is true (that is, when P and Q are both false), the formula will be a tautology. Under the other three truth-value assignment for P and Q, it doesn't matter if $P \star Q$ returns true or false. This result in $2^3 = 8$ possibilities.
   Therefore, there are 8 binary connectives to make A^* a tautology.

   (b) For how many binary connectives $\star \in \mathcal{S}$ is the formula $B^\star$ a tautology?
   Justify your answer without using a truth table.
   Answer:
   There are 2 binary connectives total which would make the formula B^* a tautology. We will be using the same approach as stated in part (a). That is, consider the truth-value assignment when the premise is True, and find conditions for the output of $\star$ operator to make the conclusion True as well (to avoid non-tautology). When one of P or Q is true, the premise is true. Also, the conclusion is true when $P \star Q$ is False (so False XOR True returns True). So, the $\star$ operator is fixed to be False under three truth-value assignment, and is free (by free, we meant returning True or False under this assignment will not affect B^* is a tautology) only when P is False and Q is False. That is in total 2 possibilities.

   (c) For how many binary connectives $\star \in \mathcal{S}$ is the formula $C^\star$ a tautology?
   Justify your answer without using a truth table.
   Answer:

There are 8 binary connectives total which would make the formula C^* a tautology. Observe that when P is true, the premise is (T XOR T) which is False. When P is false but Q is false too, the premise (F XOR F) is False too. The only case when the premise is true is when P is false and Q is true. Now consider the conclusion under this truth-value assignment. To make (T XOR $(P \star Q)$) to be true, we simply need to ensure $(P \star Q)$ is false when P is false and Q is true. Under other three truth-value assignment, the premise is false so the formula C^* results a vacuum truth, independent of what $P \star Q$ is. Therefore, in total $2^3 = 8$ possibilities.

(d) For how many binary connectives $\star \in \mathcal{S}$ is at least one of $A^\star$, $B^\star$, $C^\star$, or $D^\star$ a tautology? Justify your answer without using a truth table.
Answer:
There are 14 binary connectives to make at least one of A^*, B^*, C^*, and D^* a tautology. We should first review the conditions of $P \star Q$ that would make A^*, B^*, and C^* not a tautology.
We explained in the previous parts that
(1) when $F \star F$ is true, A^* is a tautology. This suggests when $F \star F$ is false, A^* is not a tautology.
(2) When $T \star F = F \star T = T \star T = F$, B^* is a tautology. Otherwise, B^* is not a tautology.
(3) If and only if $F \star T = F$, C^* is a tautology.
Using the same reasoning presented in part (c) on part (d), we can conclude that (4) D^* is a tautology if and only if $T \star F = F$.
So if an operator $\star$ is to make non of A^*, B^*, C^*, and D^* a tautology, it needs satisfy the three property:
1. $F \star F = F$ [suggested by (1)]
2. $F \star T = T$ [suggested by (3)]
3. $T \star F = T$ [suggested by (4)]
If 1, 2, 3 are satisfied, we can see that (2) is satisfied too. So the three conditions above are necessary and sufficient to make non of the formulas tautology. It only left two choices ($T \star T$ can be either true or false).
Subtracting the above two, the rest 14 binary connectives can make at least one of A^*, B^*, C^*, and D^* a tautology.

2. Let U denote a set and let $P : U \times U \to \{\mathrm{T}, \mathrm{F}\}$ denote a binary predicate. Consider the following predicate logic formulas:

$$A_1 = \text{“}\forall u \in U.\forall v \in U.([\forall w \in U.(P(w,u) \text{ IFF } P(w,v)))] \text{ IMPLIES}(u = v))\text{”}$$
$$A_2 = \text{“}\exists u \in U.\forall v \in U.(\mathrm{NOT}(P(v,u)))\text{”}$$
$$A_3 = \text{“}\forall u \in U.\exists v \in U.\forall w \in U.(P(w,v) \text{ IFF } [\exists x \in U.(P(w,x) \text{ AND } P(x,u))])\text{”}$$
$$A_4 = \text{“}\forall u \in U.\forall v \in U.\exists w \in U.\forall x \in U.[P(x,w) \text{ IFF } ((x = u) \text{ OR } (x = v))]\text{”}$$

(a) Consider the interpretation where $U = \mathbb{N}$ and $P(u,v)$ is T if and only if $u < v$.
Which of A_1, A_2, A_3, and A_4 are true under this interpretation? Justify your answer.
Answer:
A_1, A_2, A_3 are true under this interpretation.

To see why A_1 is true, consider arbitrary $u, v \in \mathbb{N}$. Assume $[\forall w \in U.(P(w,u) \text{ IFF } P(w,v))]$. If one of u, w is 0. Without the loss of generality, assume $u = 0$, we can pick If we take $w = 1$. $u < w$, so $v \leq w = 1$, which means $w = v = 0$. When non of them are 0, pick $w = u + 1$. Since NOT $(P(w,u))$, we know NOT$(P(w,v))$, or $v \leq w + 1$. If we pick $w = u - 1$, since $P(w,u)$, we know $u - 1 < v$. This suggests $u = v$.

To see why A_2 is true, we pick $u = 0 \in \mathbb{N}$ and consider an arbitrary $v \in \mathbb{N}$.There's no smaller element of natural number than 0, so clearly, $v \geq 0$. This means NOT $(P(v,u))$.

To see why A_3 is true, we first pick $u \in \mathbb{N}$ be an arbitrary element. If $u = 0$, we pick $v = 0$ too. Let $w \in \mathbb{N}$. $P(w,v)$ is clearly false as 0 is the smallest element in $\mathbb{N}$. There is also no other $x \in \mathbb{N}$ to satisfy $P(x,0)$. If $u \neq 0$, we pick $v = u - 1$. The rest of the sentence is saying for all natural numbers w, $w < u - 1$ is equivalent to saying there exist a natural number x between w and u (this is what $P(w,x)$ AND $P(x,u)$ means). This is of cause true, as v is itself the number between w and u (given $w < u - 1$).

To see why A_4 is NOT true, we consider the following counterexample, which will prove the negation to be true. The negation of A_4 is $\exists u \in U.\exists v \in U.\forall w \in U.\exists x \in U.\text{NOT}[P(x,w) \text{ IFF } ((x = u) \text{ OR } (x = v))]$. Pick $u = v = 10$. Let $w \in \mathbb{N}$. If $w = 0$, we pick $x = 10 = u$. This way, $((x = u) \text{ OR } (x = v))$ is true. However, $P(10,0)$ is not true. If $w \neq 0$, we pick $x = 0 \in \mathbb{N}$. So $P(0,w)$ is always true. However, since none of u, v are 0, $((x = u) \text{ OR } (x = v))$ is false. This counterexample shows the negation of A_4 is true under this interpretation.

(b) Consider the interpretation where $U = \mathbb{N}$ and for $u, v \in \mathbb{N}$, predicate $P(u,v)$ is true if and only if the u^{th} least significant digit in the binary expansion of v is 1.
Which of A_1, A_2, A_3, and A_4 are true under this interpretation? Justify your answer.

Answer:
A_1, A_2, A_3, and A_4 are all true under this interpretation.

To see why A_1 is true, we consider arbitrary $u, v \in \mathbb{N}$. Assume $[\forall w \in U.(P(w,u) \text{ IFF } P(w,v))]$. Under this interpretation, it means that for every digit w, the u^{th} least significant digit in the binary expansion of u is 1 if and only if the same digit is 1 for v too. Since digit in binary expansion can either be 1 or 0, this predicate actually means that every digit of u, v are equal. So clearly, $u = v$.

To see why A_2 is true, we pick $u = 0 \in \mathbb{N}$. Since every digits in the binary expansion of 0 must be 0, therefore, $\forall v \in \mathbb{N}.(\text{NOT}(P(v,0)))$.

To see why A_3 is true, we can consider an arbitrary $u \in \mathbb{N}$. Let's also translate what does it mean by $\forall w \in U.(P(w,v) \text{ IFF } [\exists x \in U.(P(w,x) \text{ AND } P(x,u))])$. It is saying that the w^{th} digit of v (we will from now on abbreviate "the w^{th} least significant digit in the binary expansion of v" simply as above) is 1 if and only if there is an x where (1) the x^{th} digit of u is 1 and (2) the w^{th} digit of x is 1. Notice that if u is 0, we can simply pick $v = 0 \in \mathbb{N}$. This is because all x will fail $P(x, u)$. So $P(w, 0)$ is consistently false with $\exists x$... for any $w \in \mathbb{N}$. When $u \neq 0$, we can also come up with a systematic method to construct v. Let $I \subseteq \mathbb{N}$ denotes the indices where u is 1. $I \neq \emptyset$ and is finite because $u \neq 0$ and $u \in \mathbb{N}$. Each $i \in I$ is a potential candidate for x (satisfying $P(i, u)$). We loop through all $i \in I$, and consider the binary expansion of i too. We let $K_i \in \mathbb{N}$ denotes the indices where $k \in K_i$ IFF $P(k, i)$. This is also a finite set as i is finite (specifically, because of the nature of binary expansion, $i \leq \lceil \log_2 u \rceil$ and $k \leq \lceil \log_2 i \rceil$). For each i and each $k \in K_i$, it satisfy $P(k, i)$ and $P(i, u)$. So by finding all possible values of k, we found all possible value of w that $\exists x \in U.(P(w, x)$ AND $P(x, u))$. As long as we initialize an infinite sequence of 0s, and set the k^{th} digit to be 1 (for all possible $k \in K_i, i \in I$), it suffices the propety of v. A concrete illustration is provided at the bottom of this document.

To see why A_4 is true, we consider arbitrary $u, v \in U$. The rest of the sentence is saying that there is a natural number w such that, the x^{th} digit in the binary expansion of w is 1, if x is u and v, and only if so too. If $u = v$, we simply pick $w = 2^u$. So the only digit $=1$ is the u^{th} least significant digit. Otherwise, we pick $w = 2^u + 2^v$. This also satisfy the property where the x^{th} least significant digit is 1 if and only if $(x = u)$ or $(x = v)$.

(c) Is A_4 logically implied by the formula A_1 AND A_2 AND A_3? Justify your answer.

Answer:
A_4 is not logically implied by the formula A_1 AND A_2 AND A_3. We have seen in part (a) that under the interpretation where $U = \mathbb{N}$ and $P(u, v)$ is T if and only if $u < v$, A_1, A_2, A_3 are true but not A_4. A counterexample exists means that the implication is not logically valid.

(d) Is A_2 logically implied by the formula "A_1 AND A_3 AND A_4"? Justify your answer.

Answer:
A_2 is not logically implied by the formula A_1 AND A_3 AND A_4. We can construct an interpretation where the latter 3 formulas are true but not A_2.
Consider the slightly modified interpretation for part (b): take $U = \mathbb{Z}^+$, and for $u, v \in \mathbb{Z}^+$, the predicate $P(u, v)$ is true if and only if the $(u-1)^{\text{th}}$ least significant digit in the binary expansion of v is 1. In plain English, we are removing 0 from our universe, and start from 1 when counting least significant digits of the binary expansions.

Under this interpretation, I'll explain why A_1, A_3, A_4 are still true despite the modification. It is clear that A_1 still express the meaning that "if for $u, v \in \mathbb{Z}^+$ every digit of the expansion is the same implies u, v are the same number". Since our universe and counting system both starts from 1, the arguments maintain to be true.

A_3 is true as well. Since $\mathbb{Z}^+ \subseteq \mathbb{N}$, we have shown that $\forall u \in \mathbb{Z}^+.\exists v \in \mathbb{N}.\forall w \in \mathbb{Z}^+.(P(w, v)$ IFF $[\exists x \in \mathbb{N}.(P(w, x)$ AND $P(x, u))])$. We will explain two things: (1) why changing the domain of x from $\mathbb{N}$ to $\mathbb{Z}^+$ means the same thing. (2) why changing the domain of v from $\mathbb{N}$ to $\mathbb{Z}^+$ does not affect the truth value given $u \neq 0$.

We will start with (1). We will use P_b, P_d to denote the interpretation predicate of P used in part (b), (d), respectively. Notice that all we are modifying is to shift the digit corresponding to index 1 right by 1 digit. So $P_d(i+1,n) = P_b(i,n)$ for all $i, n \in \mathbb{Z}^+$. So changing the $P_b(w,x)$ where $w = 0, 1, 2, ...$ to $P_d(w,x)$ where $w = 1, 2, ...$ does not affect the meaning. For the " ...AND $P_d(x,u)$" part, if we know there exists $x_b \in \mathbb{N}$ such that $P_b(x_b, u)$, we just need to pick $x_d = x_b + 1 \in \mathbb{Z}^+$ and $P_d(x_d, u)$ is true as well.

We will then explain (2). The idea here is that there exist $v \geq 1$ for any arbitrary $u \in \mathbb{Z}^+$. Since we are guaranteed $u \geq 1$, the set of indices where $P(i,u)$, $I \subseteq \mathbb{N}$, is also guaranteed to be non-empty (as non zero integer must has at least one 1 on their binary expansion). Moreover, for every $i \in I, i \geq 1$ by our modified definition. So the binary expansion of i must contain non-zero digits too. So there must exist at least 1 $k \geq 1$ and $P(k,i)$. Again, looping through all the possible $k \in K_i, i \in I$, and changing the k^{th} (counting from 1 as the rightmost digit) in our initialized infinite zero sequence to 1, the sequence will have non-zero entries ($v \geq 1$). Therefore, we obtained this $v \in \mathbb{Z}^+$ for u.

A_4 is still true for the same justification. If $u = v$, we simply pick $w = 2^{(u+1)}$. So the only digit =1 is the u^{th} (counting from 1 as the rightmost digit) least significant digit. Otherwise, we pick $w = 2^{(u+1)} + 2^{(v+1)}$.

We have shown that A_1, A_3, A_4 are true but not A_2. A counterexample exists means that the implication is not logically valid.

Extra: The word explanation for why A_3 is true in (2b) under the binary expansion context is very abstract. We here provide an concrete example to illustrate our algorithm.

Let $u = 13$, for example. The binary expansion is $u_{\text{base2}} = ...0001101$. $I = \{0, 2, 3\}$ are indices where the digit of u is 1. So our conclusion is that, to satisfy $\exists x \in U.(P(w,x) \text{ AND } P(x,u))$, x must be either $0, 2, 3$. Consider all $i \in I$.
(1) When $i = 0, i_{\text{base2}} = ...0000$. K_0 (indices where the digit of i is 1) is the empty set.
(2) When $i = 2, i_{\text{base2}} = ...0010$. $K_2 = \{1\}$.
(3) When $i = 3, i_{\text{base2}} = ...0011$. $K_3 = \{0, 1\}$.
This means that
from (2) and $1 \in K_2$: $w = 1, x = 2$, $P(w,x)$ AND $P(x,u)$ is true;
from (3) and $1 \in K_3$: $w = 1, x = 3$, $P(w,x)$ AND $P(x,u)$ is true;
from (3) and $0 \in K_3$: $w = 0, x = 3$, $P(w,x)$ AND $P(x,u)$ is true. So all possible w for the predicate true is $\{0, 1\}$. The v we construct will be:
$v_{\text{base2}} = ...00011$. Or alternatively, $v = 3 \in \mathbb{N}$ will work for $u = 13$.