CSC165H1: Problem Set 1 Sample Solutions

Due October 2 before 4 p.m.

Note: solutions are incomplete, and meant to be used as guidelines only. We encourage you to ask follow-up questions on the course forum or during office hours.

1. [6 marks] Truth tables and formulas. Consider the following formula:

\[-r \Rightarrow (\neg p \Rightarrow q)\]

(a) [2 marks] Write the truth table for the formula. (No need to show your calculations).

\[
\begin{array}{ccc|c}
p & q & r & \neg r \Rightarrow (\neg p \Rightarrow q) \\
T & T & T & T \\
T & T & F & T \\
T & F & T & T \\
T & F & F & T \\
F & T & T & T \\
F & T & F & T \\
F & F & T & T \\
F & F & F & F \\
\end{array}
\]

(b) [2 marks] Write a logically equivalent formula that doesn’t use \(\Rightarrow\) or \(\Leftrightarrow\), in other words it uses only \(\land, \lor, \neg\). Show how you derived the result.

\[
\begin{align*}
\neg r \Rightarrow (\neg p \Rightarrow q) & \equiv r \lor (\neg p \Rightarrow q) & \text{# material implication} \\
& \equiv r \lor (p \lor q) & \text{# material implication again} \\
& \equiv r \lor p \lor q & \text{# \lor is associative}
\end{align*}
\]

(c) [2 marks] Write formula that is logically equivalent to the converse of the given formula, and that doesn’t use \(\Rightarrow\) or \(\Leftrightarrow\), in other words it uses only \(\land, \lor, \neg\). Show how you derived the result.

\[
\begin{align*}
(\neg p \Rightarrow q) \Rightarrow \neg r & \equiv \neg(\neg p \Rightarrow q) \lor \neg r & \text{# material implication} \\
& \equiv (\neg p \land \neg q) \lor \neg r & \text{# De Morgan’s}
\end{align*}
\]

2. [6 marks] One-to-one and onto

Use the following definitions in the questions below.
Onto($f$): $\forall n \in \mathbb{N}, \exists m \in \mathbb{N}, f(m) = n$, for $f : \mathbb{N} \to \mathbb{N}$.

OneToOne($f$): $\forall m, n \in \mathbb{N}, m \neq n \Rightarrow f(m) \neq f(n)$, for $f : \mathbb{N} \to \mathbb{N}$.

(a) [1 mark] Suppose $\neg$Onto($g$). Write this in predicate logic without using the predicate name Onto.

Solution
I simply negate the definition of Onto($g$):

$$\exists n \in \mathbb{N}, \forall m \in \mathbb{N}, g(m) \neq n$$

(b) [1 mark] Suppose $\neg$OneToOne($h$). Write this in predicate logic without using the predicate name OneToOne.

Solution
Again, I negate the definition of OneToOne($h$):

$$\exists m, n \in \mathbb{N}, m \neq n \land h(m) = h(n)$$

(c) [1 mark] Give an example of a function $f : \mathbb{N} \to \mathbb{N}$ where Onto($f$) and OneToOne($f$).

Solution
This function always sends different inputs to different outputs (themselves!), and any element of the codomain is output from itself in the domain:

$$f(n) = n$$

(d) [1 mark] Give an example of a function $f : \mathbb{N} \to \mathbb{N}$ where $\neg$Onto($f$) and OneToOne($f$).

Solution
Every input produces output twice itself, so different inputs get sent to different outputs, but there are no inputs that produce any odd natural number as output:

$$f(n) = 2n$$

(e) [1 mark] Give an example of a function $f : \mathbb{N} \to \mathbb{N}$ where Onto($f$) and $\neg$OneToOne($f$).

Solution
Inputs 0 and 1 both produce output 0, and for every output $n$ there is corresponding input $2n$:

$$f(n) = \lfloor n/2 \rfloor$$

(f) [1 mark] Give an example of a function $f : \mathbb{N} \to \mathbb{N}$ where $\neg$Onto($f$) and $\neg$OneToOne($f$).

Solution
Inputs 0 and 1 both produce output 5, and there is no input that produces output 6:

$$f(n) = 5$$

3. [7 marks] modular arithmetic

(a) [2 marks] Prove Example 2.19(1) from the course notes.
(b) [2 marks] Prove Example 2.19(3) from the course notes.

Solution

translation: Example 2.19(3) states:
\[ \forall a, b, c, d, n \in \mathbb{Z}, n \neq 0 \Rightarrow (a \equiv c \mod n \land b \equiv d \mod n \Rightarrow ab \equiv cd \mod n) \]

discussion: Unpacking the definition of congruence modulo \( n \) and using linear combination worked so well last time that I will try it again. Since I need to end up with an \( ab \) term, I multiply \((a - c)\) by \( b \), but then I need to multiply \((b - d)\) by something to undo the damage... Multiplying by \( c \) seems to work!

header: Let \( a, b, c, d, n \in \mathbb{Z} \). Assume \( n \neq 0 \) and \( a \equiv c \mod n \) and \( b \equiv d \mod n \), in other words \( n \mid (a - c) \) and \( n \mid (b - d) \). WTS \( n \mid ((a + b) - (c + d)) \).

body:
\[ n \mid (a - c) \land n \mid (b - d) \Rightarrow n \mid (1 \cdot (a - c) + 1 \cdot (b - d)) \]

# by divisibility of linear combinations, proved in lecture
\[ n \mid ((a + b) - (c + d)) \]

(c) [3 marks] Use Example 2.19(3) to find the units digit of \( 257^{256} \). Use Example 2.19(3) to prove your result — we will not accept the argument that you used a calculator or programming language to compute this with brute force.

Solution

translation:
\[ 257^{256} \equiv 1 \mod 10 \]
description: The translation says, in other words, \( \exists k \in \mathbb{Z}, 257^{256} = 10k + 1 \), or the units digit of \( 257^{256} \) is 1. I show by repeatedly multiplying pairs of numbers equivalent to each other modulo 10.

I will use a small lemma in the process:[^2]

claim: \[ \forall a, b, c, n \in \mathbb{Z}, n \neq 0 \Rightarrow (a \equiv b \mod n \land b \equiv c \mod n \Rightarrow a \equiv c \mod n) \]

header: Let \( a, b, c, n \in \mathbb{Z} \). Assume \( n \neq 0 \land a \equiv b \mod n \land b \equiv c \mod n \). WTS \( a \equiv c \mod n \).

body:

\[ n \mid (a - b) \land n \mid (b - c) \quad \text{# definition of congruence} \]
\[ n \mid 1 \cdot (a - b) + 1 \cdot (b - c) \quad \text{# by divisibility of linear combinations} \]
\[ n \mid (a - c) \]
\[ a \equiv c \mod n \quad \text{# definition of congruence} \]

main header: WTS \( 257^{256} \equiv 1 \mod 10 \).

main body:

\[
\begin{align*}
257 & \equiv 7 \mod 10 \quad \text{# since } 10 \mid 257 - 7 \\
257^2 & \equiv 7^2 \mod 10 \quad \text{# by 2.19(3)} \\
7^2 & \equiv 9 \mod 10 \quad \text{# since } 10 \mid 49 - 9 \\
257^2 & \equiv 9 \mod 10 \quad \text{# by lemma} \\
257^4 & \equiv 9^2 \mod 10 \quad \text{# by 2.19(3)} \\
9^2 & \equiv 1 \mod 10 \quad \text{# since } 10 \mid 81 - 1 \\
257^4 & \equiv 1 \mod 10 \quad \text{# by lemma} \\
257^8 & \equiv 1^2 \mod 10 \quad \text{# by 2.19(3)} \\
257^{16} & \equiv 1^4 \mod 10 \quad \text{# by 2.19(3)} \\
257^{32} & \equiv 1^8 \mod 10 \quad \text{# by 2.19(3)} \\
257^{64} & \equiv 1^{16} \mod 10 \quad \text{# by 2.19(3)} \\
257^{128} & \equiv 1^{32} \mod 10 \quad \text{# by 2.19(3)} \\
257^{256} & \equiv 1^{64} \mod 10 \quad \text{# by 2.19(3)} \\
257^{256} & \equiv 1 \mod 10 \quad \text{# } 1^{64} = 1 \quad \blacksquare
\end{align*}
\]

[^2]: Fairly obvious, so we won’t require this for full marks.

4. [7 marks] remainders

(a) [1 mark] Prove:

\[ \exists x \in [0, 34], x \equiv 3 \mod 5 \land x \equiv 5 \mod 7 \]

Solution
discussion: I can just check the 35 integers 0, ..., 34 and find one that works.

header: Let \( x = 33 \). WTS \( x \equiv 3 \mod 5 \land x \equiv 5 \mod 7 \).

body:

\[
5 \mid (33 - 3) \quad \land \quad 7 \mid (33 - 5)
\]

\[
33 \equiv 3 \mod 5 \land 33 \equiv 5 \mod 7 \quad \# \text{ definition of congruence}
\]

\[
x \equiv 3 \mod 5 \land x \equiv 5 \mod 7 \quad \blacksquare
\]

(b) [1 mark] Prove:

\[
\exists m_1, m_2 \in \mathbb{Z}, (m_1 \times 7) + (m_2 \times 11) = 1
\]

... by finding suitable values for \( m_1 \) and \( m_2 \).

**Solution**

discussion: I experiment with multiples of 7 and 11 to find a pair that are within 1 of each other: 
21 and 22 will do!

header: Let \( m_1 = -3 \) and let \( m_2 = 2 \). WTS \( m_17 + m_211 = 1 \).

body:

\[
m_17 + m_211 = (-3)7 + (2)11 = -21 + 22 = 1 \quad \blacksquare
\]

(c) [2 marks] Assume that \( m_1, m_2 \) are integers such that \((m_1 \times 7) + (m_2 \times 11) = 1\). Prove:

\[
\forall a_1, a_2 \in \mathbb{Z}, (a_2 \times m_1 \times 7) + (a_1 \times m_2 \times 11) \equiv a_2 \mod 11
\]

**Solution**

translation:

\[
\forall m_1, m_2 \in \mathbb{Z}, m_17 + m_211 = 1 \Rightarrow \forall a_1, a_2 \in \mathbb{Z}, a_2m_17 + a_1m_211 \equiv a_2 \mod 11
\]

discussion: Since the first term has a factor \( m_17 \), I will try to add and then subtract \( m_211 \), based on the assumed linear combination, to see if I can isolate \( a_2 \).

header: Let \( m_1, m_2 \in \mathbb{Z} \). Assume \( m_17 + m_211 = 1 \). Let \( a_1, a_2 \in \mathbb{Z} \). WTS \( a_2m_17 + a_1m_211 \equiv a_2 \mod 11 \).
(d) [3 marks] Prove that if $p_1, p_2$ are any two distinct primes and $a_1, a_2$ are any two integers, then there is some integer $x$ such that $x \equiv a_1 \mod p_1$ and $x \equiv a_2 \mod p_2$. Hint: Note that $\gcd(p_1, p_2) = 1$, read the material on $\gcd$ in the course notes, and read the previous part of this question.

**Solution**

**translation:**

$$\forall p_1, p_2, a_1, a_2 \in \mathbb{Z}, \text{Prime}(p_1) \land \text{Prime}(p_2) \land p_1 \neq p_2 \Rightarrow \exists x \in \mathbb{Z}, x \equiv a_1 \mod p_1 \land x \equiv a_2 \mod p_2$$

**discussion:** The structure is identical to the previous question if I substitute $p_1$ for 7 and $p_2$ for 11. I also know that, since $\gcd(p_1, p_2) = 1$ there are integers $m_1$ and $m_2$ so that $m_1 p_1 + m_2 p_2 = 1$.

**header:** Let $p_1, p_2, a_1, a_2 \in \mathbb{Z}$. Assume $\text{Prime}(p_1) \land \text{Prime}(p_2) \land p_1 \neq p_2$. WTS:

$$\exists x \in \mathbb{Z}, x \equiv a_1 \mod p_1 \land x \equiv a_2 \mod p_2$$

**body:**

$$\begin{align*}
p_1 &> 1 \land p_2 > 1 & \# \text{definition of } \text{Prime}(p_1), \text{Prime}(p_2) \\
p_1 \mid p_2 \land p_2 \mid p_1 & \land p_1 \neq p_2 \land p_1 \neq p_2 & \# \text{only possible divisor left} \\
\gcd(p_1, p_2) & = 1 & \# \text{definition of } \text{Prime}(p_1), \text{Prime}(p_2) \\
\exists m_1, m_2 \in \mathbb{Z}, m_1 p_1 + m_2 p_2 & = 1 & \# \text{Course Notes, p. 56}
\end{align*}$$

Let $x = a_2 m_1 p_1 + a_1 m_2 p_2$

$$\begin{align*}
x - a_2 & = a_2 (m_1 p_1 + m_2 p_2 - m_2 p_2) + a_1 m_2 p_2 - a_2 \\
& = a_2 - a_2 m_2 p_2 + a_1 m_2 p_2 - a_2 & \# m_1 p_1 + m_2 p_2 = 1 \\
x - a_2 & = (a_1 - a_2) m_2 p_2 \\
p_2 \mid x - a_2 & \# \text{there's a factor of } p_2 \\
x & \equiv a_2 \mod p_2 & \# \text{definition of congruence}
\end{align*}$$

$$x \equiv a_1 \mod p_1 \# \text{swap roles of } a_1, p_1 \text{ with } a_2, p_2 \text{ in algebra above}$$