COMP 3803 - Assignment 1 Solutions

January 30, 2015

1. **Q:** Prove that the sum of n real numbers if rational if all of them are rational. Is the converse true? Prove or disprove that the product of n real numbers is rational (resp. irrational) if all of them are rational (resp. irrational).

   A: We will prove the first part by induction. Of course, the base case is trivial: the sum of a single rational number is clearly rational. Then, suppose that the sum of n rational numbers is always rational. Given $n+1$ rational numbers $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_{n+1}}{b_{n+1}}$, their sum is:

   $$\frac{a_1}{b_1} + \frac{a_2}{b_2} + \ldots + \frac{a_n}{b_n} + \frac{a_{n+1}}{b_{n+1}}$$

   By the induction hypothesis, the sum of the first n of these numbers is some rational number $\frac{p}{q}$, so the above expression is:

   $$= \frac{p}{q} + \frac{a_{n+1}}{b_{n+1}} = \frac{pb_{n+1} + qa_{n+1}}{qb_{n+1}}$$

   which is rational. So by induction, the sum of n rational numbers is rational.

   The converse is not necessarily true, *i.e.* if a number is rational, it is not necessarily only a sum of rational numbers, *e.g.* $0 = -\sqrt{2} + \sqrt{2}$.

   Finally, a product of rational numbers is clearly rational (by multiplying all numerators together and all denominators together), but a product of irrational numbers need not be irrational. Indeed, $\sqrt{2} * \sqrt{2} = 2$. □

2. **Q:** Prove that if n is a positive integer, then n is odd if and only if $5n + 6$ is odd.

A: First, suppose that n is an odd positive integer, so $n = 2k + 1$ for some integer $k \geq 0$. Then:

$$5n + 6 = 5(2k + 1) + 6 = 10k + 11 = 2(5k + 5) + 1$$

So $5n + 6$ has the form $2\ell + 1$ for some integer ℓ – in other words, $5n + 6$ is odd.

Conversely, suppose that $5n + 6$ is odd, so $5n + 6 = 2k + 1$ for some integer $k \geq 0$. Then:

$$5n + 6 = 2k + 1 \Rightarrow 5n = 2k - 5 \Rightarrow n = \frac{2k}{5} - 1$$

Since n is known to be an integer, then $5|2k$, so $5|k$, and $\frac{k}{5} = \ell$ is an integer, whereby $n = 2\ell - 1$ is odd. $\square$

3. **Q:** Show by induction that $n^5 - n$ is divisible by 5 for all $n \geq 0$.

   A: For the base case, $n = 0$, $0^5 - 0 = 0$ is divisible by 5.

   Suppose $n^5 - n$ is divisible by 5 for some $n \geq 0$ – in other words, $n^5 - n = 5k$ for some integer k. Then:

$$\begin{aligned}(n+1)^5 - (n+1) &= (n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1) - (n+1) \\ &= (n^5 - n) + 5(n^4 + 2n^3 + 2n^2 + n) \\ &= 5k + 5(n^4 + 2n^3 + 2n^2 + n)\end{aligned}$$

   which is clearly divisible by 5. Thus, by induction, $n^5 - n$ is divisible by 5 for all $n \geq 0$. $\square$

4. **Q:** Show by induction that $n^3 - n$ is divisible by 3 for all $n \geq 0$.

   A: The solution is identical to that of the previous problem. For the base case, $n = 0$, $0^3 - 0 = 0$ is divisible by 3.

   Suppose $n^3 - n$ is divisible by 3 for some $n \geq 0$ – in other words, $n^3 - n = 3k$ for some integer k. Then:

$$\begin{aligned}(n+1)^3 - (n+1) &= (n^3 + 3n^2 + 3n + 1) - (n+1) \\ &= (n^3 - n) + 3(n^2 + n) \\ &= 3k + 3(n^2 + n)\end{aligned}$$

which is clearly divisible by 3. Thus, by induction, $n^3 - n$ is divisible by 3 for all $n \geq 0$. $\square$

Remark. Just some extra information if you are curious! You don't need to know anything about this, but you may find it interesting.
The previous two questions hint at a pattern: is it true that $n^k - n$ is divisible by k for every $k \geq 2$ and $n \geq 0$? We can easily verify that this is not always the case: indeed, $2^4 - 2 = 14$ which is not divisible by 4.
However, if p is prime, then $n^p - n$ is always divisible by p. We only need a basic algebraic fact to prove this – the so-called "freshman's dream" – that if p is prime, then for any integers x and y:

$$(x + y)^p \equiv x^p + y^p \pmod p$$

Now, to show that $n^p - n$ is divisible by p, we proceed by induction as before. The base case is trivial, so we assume the induction hypothesis, and by the "freshman's dream":

$$(n + 1)^p - (n + 1) \equiv n^p + 1^p - n - 1 = n^p - n \pmod p$$

Since we've assumed that $n^p - n \equiv 0 \pmod p$, then we are done by induction. This result is known as *Fermat's little theorem*, and its more general form is seen in *Euler's theorem*.

5. **Q:** We had shown in class that the set of real numbers in the interval $[0, 1]$ is uncountable. What can you then say about the cardinality of the set of real numbers in the interval $[0.5, 0.6]$? If it is countable, why is it? If it is uncountable, present the arguments in the same way we did the proof for the interval $[0, 1]$. Given what was taught in class, could you have come up with an easier proof?

   A: You are asked to present a similar argument to the one shown in class: such an argument is called a *diagonalisation*, or a *diagonal argument*.

   We proceed by contradiction. Suppose $[0.5, 0.6]$ is countable. Then, we can exhaustively enumerate its elements in a sequence $s_1, s_2, \ldots$.

We represent each s_i in decimal as follows:

$$\begin{aligned} s_1 &= 0.5s_{11}s_{12}s_{13}\dots \\ s_2 &= 0.5s_{21}s_{22}s_{23}\dots \\ s_3 &= 0.5s_{31}s_{32}s_{33}\dots \\ &\vdots \end{aligned}$$

Then, I claim that there exists an element $t \in [0.5, 0.6]$ which is never listed in the above sequence. Indeed, let:

$$t = 0.5t_1t_2t_3\dots$$

where $t_1 \neq s_{11}$, $t_2 \neq s_{22}$, $\dots$, and in general, t_n is chosen so that $t_n \neq s_{nn}$. It is a fact that t is never listed: suppose $t = s_n$ for some n. Then $t_1 = s_{n1}$, $t_2 = s_{n2}$, $\dots$, $t_n = s_{nn}$, but t was chosen precisely so that $t_n \neq s_{nn}$.

So, in conclusion, if $[0.5, 0.6]$ were countable, we could exhaustively enumerate its elements, but this enumeration allows us to construct a number in $[0.5, 0.6]$ which could not possibly be listed in the enumeration. Thus, by contradiction, $[0.5, 0.6]$ must be uncountable. □

Remark. There is a simpler proof: define the function f as follows:

$$\begin{aligned} f : [0,1] &\to [0.5, 0.6] \\ x &\mapsto 0.1 * x + 0.5 \end{aligned}$$

f is a bijection, so $[0,1]$ is uncountable if and only if $[0.5, 0.6]$ is uncountable.

6. **Q:** Let **A** be the set of all even natural numbers, and **B** be the set of natural numbers divisible by 3. Prove that the set of fractions $\frac{a}{b}$ where $a \in \mathbf{A}$ and $b \in \mathbf{B}$ is countable.

   A: We will say $\mathbf{C} = \{\frac{a}{b} : a \in \mathbf{A}, b \in \mathbf{B}\}$. The task is to show that **C** is countable.

   Clearly **A** and **B** are countable as subsets of the natural numbers, which by definition is a countable set. Thus, $\mathbf{A} \times \mathbf{B}$ is also countable. Each pair $(a, b) \in \mathbf{A} \times \mathbf{B}$ exhaustively maps to an element $\frac{a}{b} \in \mathbf{C}$, so **C** is countable. Formally, here we have constructed a surjection (or *surjective* mapping, also sometimes called an *onto* mapping), $\mathbf{A} \times \mathbf{B} \to \mathbf{C}$. □

Remark. Again, a simple observation makes this a proof exceedingly easy. Note that $\mathbf{C}$ is a subset of the rationals, which is a countable set, so $\mathbf{C}$ must be countable.

7. **Q:** For arbitrary strings X and Y, show that $(XY)^R = Y^R \cdot X^R$, where, by notation, V^R is the string obtained by reversing the string V.

   A: If $X = x_1x_2\ldots x_i$, $Y = y_1y_2\ldots y_j$, then:

$$\begin{aligned}
X^R &= x_i x_{i-1} \ldots x_1 \\
Y^R &= y_j y_{j-1} \ldots y_1 \\
XY &= x_1 x_2 \ldots x_i y_1 y_2 \ldots y_j \\
(XY)^R &= y_j y_{j-1} \ldots y_1 x_i x_{i-1} \ldots x_1 \\
Y^R X^R &= y_j y_{j-1} \ldots y_1 x_i x_{i-1} \ldots x_1
\end{aligned}$$

   So $(XY)^R = Y^R X^R$. □

8. **Q:** For any language $\mathbf{A}$, let $\mathbf{A}^R$ be $\{X^R : X \in \mathbf{A}\}$. Then, for arbitrary languages $\mathbf{A}$ and $\mathbf{B}$, show that $(\mathbf{AB})^R = \mathbf{B}^R \cdot \mathbf{A}^R$, and that $(\mathbf{A} \cup \mathbf{B})^R = \mathbf{A}^R \cup \mathbf{B}^R$. Your arguments must be brief but accurate.

   A: For $(\mathbf{AB})^R$, by definition:

$$\begin{aligned}
(\mathbf{AB})^R &= \{X^R : X \in \mathbf{AB}\} = \{(XY)^R : X \in \mathbf{A}, Y \in \mathbf{B}\} \\
&= \{Y^R X^R : X \in \mathbf{A}, Y \in \mathbf{B}\} \\
&= \{Y^R : Y \in \mathbf{B}\} \cdot \{X^R : X \in \mathbf{A}\} = \mathbf{B}^R \mathbf{A}^R
\end{aligned}$$

   For $(\mathbf{A} \cup \mathbf{B})^R$, by definition:

$$\begin{aligned}
(\mathbf{A} \cup \mathbf{B})^R &= \{X^R : X \in \mathbf{A} \cup \mathbf{B}\} = \{X^R : X \in \mathbf{A} \text{ or } X \in \mathbf{B}\} \\
&= \{X^R : X \in \mathbf{A}\} \cup \{X^R : X \in \mathbf{B}\} = \mathbf{A}^R \cup \mathbf{B}^R
\end{aligned}$$

   □

9. **Q:** If the *languages* $\mathbf{A}$ and $\mathbf{B}$ are countably infinite and we use the notation of Question 8, what can you say about the size of the language obtained by concatenating $(\mathbf{AB})^R$ and $(\mathbf{A} \cup \mathbf{B})^R$. Is the size of the set $(\mathbf{AB})^R \cdot (\mathbf{A} \cup \mathbf{B})^R$ any larger or smaller than the size of the language obtained by concatenating $\mathbf{B}^R$ and $\mathbf{A}^R$?

A: We first show that if the language $\mathbf{A}$ is countable, then $\mathbf{A}^R$ is countable. Indeed, each string $X \in \mathbf{A}$ corresponds exactly to one string $X^R \in \mathbf{A}$, so $\mathbf{A}$ is countable if and only if $\mathbf{A}^R$ is countable. Moreover, if either one is countably infinite, then so is the other.

Recall also that the concatenation of countably infinite languages results in a countably infinite language.

So, from the previous problem, $(\mathbf{AB})^R$ is countably infinte since $\mathbf{AB}$ is countably infinite. Similarly, $(\mathbf{A} \cup \mathbf{B})^R$ is countably infinite since $\mathbf{A} \cup \mathbf{B}$ is countably infinite.

Since $\mathbf{A}$ and $\mathbf{B}$ are countably infinite, then by the above observations, $(\mathbf{AB})^R \cdot (\mathbf{A} \cup \mathbf{B})^R$ is countably infinite and $\mathbf{B}^R \cdot \mathbf{A}^R$ is countably infinite, so they are both of equal cardinality.. $\square$