HW6 Proofs, Numbers, and Cardinality

CSE20F21

Sample Solutions

Assigned questions

1. Recall the definition of the set of linked lists from class, and some associated functions.

$$\begin{array}{ll} \text{Basis Step:} & [] \in L \\ \text{Recursive Step:} & \text{If } l \in L \text{ and } n \in \mathbb{N}\text{, then } (n, l) \in L \end{array}$$

The length function $length : L \to \mathbb{N}$ is defined by

$$\begin{array}{llll} \text{Basis Step:} & & length(\ []\ ) & = 0 \\ \text{Recursive Step:} & \text{If } l \in L \text{ and } n \in \mathbb{N}\text{, then} & length(\ (n, l)\ ) & = 1 + length(l) \end{array}$$

The function $prepend : L \times \mathbb{N} \to L$ is defined by

$$prepend(\ (l, n)\ ) = (n, l)$$

The function $append : L \times \mathbb{N} \to L$ is defined by

$$\begin{array}{llll} \text{Basis Step:} & \text{If } m \in \mathbb{N} \text{ then} & append(\ ([], m)\ ) & = (m, []) \\ \text{Recursive Step:} & \text{If } l \in L \text{ and } n \in \mathbb{N} \text{ and } m \in \mathbb{N}\text{, then} & append(\ (\ (n, l), m\ )\ ) & = (n, append(\ (l, m)\ )\ ) \end{array}$$

(a) (*Graded for fair effort completeness*[1]) Fill in the blanks in the following proof of the statement

$$\forall l \in L\ \forall m \in \mathbb{N}\ (\ length(prepend(\ (l, m)\ )) = length(append(\ (l, m)\ ))\ )$$

Proof: We proceed by structural induction on L.

Basis step: We need to show that

$$\forall m \in \mathbb{N}\ (\ length(prepend(\ ([], m)\ )) = length(append(\ ([], m)\ ))\ )$$

[1] Graded for fair effort completeness means you will get full credit so long as your submission demonstrates honest effort to answer the question. You will not be penalized for incorrect answers.

Towards universal generalization, let m be an arbitrary natural number. Calculating:

$$LHS = \underline{\mathit{length}(\mathit{prepend}(\ ([], m)\ )) \overset{\text{def of } \mathit{prepend}}{=} \mathit{length}(\ (m, [])\ ) \overset{\text{def of } \mathit{length}}{=} 1 + \mathit{length}([]) \overset{\text{def of } \mathit{length}}{=} 1 + 0 = 1}$$

$$RHS = \underline{\mathit{length}(\mathit{append}(\ ([], m)\ )) \overset{\text{def of } \mathit{append}}{=} \mathit{length}(\ (m, [])\ ) \overset{\text{def of } \mathit{length}}{=} 1 + \mathit{length}([]) \overset{\text{def of } \mathit{length}}{=} 1 + 0 = 1}$$

Since $LHS = RHS$, the basis step is complete.

Recursive step: Consider an arbitrary: $l' \in L$, $n \in \mathbb{N}$, and we assume as the **induction hypothesis** that:

$$\underline{\forall m \in \mathbb{N}\ (\ \mathit{length}(\mathit{prepend}(\ (l', m)\ )) = \mathit{length}(\mathit{append}(\ (l', m)\ ))\ )}$$

Our goal is to show that

$$\forall m \in \mathbb{N}\ (\ \mathit{length}(\mathit{prepend}(\ (\ (n, l')\ , m)\ )) = \mathit{length}(\mathit{append}(\ (\ (n, l'), m)\ ))\ )$$

is also true. Let m be an arbitrary natural number. Calculating:

$$\begin{aligned}
LHS &= \mathit{length}(\mathit{prepend}(\ ((n, l'), m)\ )) \\
&\overset{\text{def of } \mathit{prepend}}{=} \mathit{length}(\ (m, (n, l'))\ ) \\
&\overset{\text{def of } \mathit{length}}{=} 1 + \mathit{length}(\ (n, l')\ ) \\
&\overset{\text{def of } \mathit{length}}{=} 1 + 1 + \mathit{length}(l') \\
RHS &= \mathit{length}(\mathit{append}(\ (\ (n, l'), m)\ ))\ ) \\
&\overset{\text{def of } \mathit{append}}{=} \mathit{length}(\ (n, \mathit{append}(\ (l', m)\ )\ ) \\
&\overset{\text{def of } \mathit{length}}{=} 1 + \mathit{length}(\ \mathit{append}(\ (l', m)\ )\ ) \\
&\overset{\text{IH}}{=} 1 + \mathit{length}(\ \mathit{prepend}(\ (l', m)\ )\ ) \\
&\overset{\text{def of } \mathit{prepend}}{=} 1 + \mathit{length}(\ (m, l')\ ) \\
&\overset{\text{def of } \mathit{length}}{=} 1 + 1 + \mathit{length}(l')
\end{aligned}$$

Since $LHS = RHS$, the recursive step is complete.

(b) (*Graded for correctness*[2]) Disprove the statement

$$\forall l \in L\ \forall m \in \mathbb{N}\ (\ \mathit{prepend}(\ (l, m)\ ) = \mathit{append}(\ (l, m)\ )\ )$$

Solution: We will disprove this universal statement with a counterexample, namely a choice of $l \in L$ for which $\forall m \in \mathbb{N}\ (\ \mathit{prepend}(\ (l, m)\ ) = \mathit{append}(\ (l, m)\ )\ )$ is false.

[2] Graded for correctness means your solution will be evaluated not only on the correctness of your answers, but on your ability to present your ideas clearly and logically. You should explain how you arrived at your conclusions, using mathematically sound reasoning. Whether you use formal proof techniques or write a more informal argument for why something is true, your answers should always be well-supported. Your goal should be to convince the reader that your results and methods are sound.

Consider $l = (2, [])$ (a linked list by the recursive step in the recursive definition of L). To show that $\forall m \in \mathbb{N}$ (*prepend*(($(2, [])$, m)) = *append*(($(2, [])$, m))) is false, we consider the counterexample $m = 1$ (a natural number): By definition of *prepend*

$$\textit{prepend}(\ (\ (2,[])\ ,1)\ ) = (1,(2,[]))$$

whereas, by definition of *append*,

$$\textit{append}(\ (\ (2,[])\ ,1)\ ) = (2,\textit{append}(\ ([],1)\ )) = (2,(1,[]))$$

These two lists have different head nodes (2 vs. 1) so they are not equal, as required for a counterexample.

Notice: alternatively, we could present both counterexamples together, as $l = (2, [])$ and $m = 1$, and then proceed to show that $\textit{prepend}(\ (\ (2,[])\ ,1)\ ) \neq \textit{append}(\ (\ (2,[])\ ,1)\ )$.

(c) (*Graded for correctness*) Determine whether the statement

$$\exists l \in L\ \exists m \in \mathbb{N}\ (\ \textit{prepend}(\ (l,m)\ ) = \textit{append}(\ (l,m)\ )\ )$$

is true or false, and justify your conclusion using valid proof strategies.

Solution: This statement is true, as we can see from the witness $l = []$ and $m = 20$. Note that l is a linked list (because of the basis step in the definition) and m is a nonnegative integer. Calculating:

$$\textit{prepend}(\ ([],20)\ ) = (20,[])$$

and

$$\textit{append}(\ ([],20)\ ) = (20,[])$$

using the basis step in the recursive definition of *prepend* and *append*, and these values agree as required.

2. Recall the definition of the set of rational numbers,

$$Q = \left\{ \frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z} \text{ and } q \neq 0 \right\}$$

We define the set of **irrational** numbers $\overline{\mathbb{Q}} = \mathbb{R} - \mathbb{Q} = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$.

(a) (*Translation graded for fair effort completeness; Witness graded for correctness*) Translate the statement to English and then give a witness that could be used to prove the statement

$$\exists x \in \mathbb{Q}\ \forall y \in \overline{\mathbb{Q}}\ (x \cdot y \in \mathbb{Q})$$

You do not need to justify your answer. However, if you include clear explanations, we may be able to give partial credit for an answer with some imprecision.

Solution: A translation would be "There is a rational number whose product with any irrational number is rational." A witness that can be used to prove this statement is 0, a rational number because $0 = \frac{0}{1}$, and for any irrational y, $0 \cdot y = 0$, which is rational.

(b) (*Translation graded for fair effort completeness; Witness graded for correctness*) Translate the statement to English and then give a counterexample that could be used to disprove the statement

$$\forall x \in \overline{\mathbb{Q}} \ (x > 0 \ \to \ x \geq 1)$$

You do not need to justify your answer. However, if you include clear explanations, we may be able to give partial credit for an answer with some imprecision.

Solution: A translation would be "Every positive irrational number is greater than or equal to 1". A counterexample to this statement is $x = \frac{1}{\sqrt{2}}$. This number is irrational (we can prove this by contradiction: assume $\frac{1}{\sqrt{2}}$ is rational and there are integers p, q such that $\frac{1}{\sqrt{2}} = \frac{p}{q}$. Notice that neither p not q is zero because q is in the denominator and since $\frac{1}{\sqrt{2}}$ is nonzero. Thus, we can take the reciprocal $\frac{q}{p}$ and get a rational number. But, the reciprocal of $\frac{1}{\sqrt{2}}$ is $\sqrt{2}$ so we have that $\sqrt{2}$ is rational, contradicting our proof from class that it is irrational. Thus, the proof by contradiction is complete and we have proved that $\frac{1}{\sqrt{2}}$ is irrational.). Moreover, $0 < \frac{1}{\sqrt{2}} < 1$ because $1 < \sqrt{2}$. Thus, the statement $\frac{1}{\sqrt{2}} > 0 \ \to \ \frac{1}{\sqrt{2}} \geq 1$ evaluates to $T \to F = F$, as required for this to be a valid counterexample to the universal claim.

(c) (*Translation graded for fair effort completeness; Witness graded for correctness*) Translate the statement to English and then give a witness that could be used to prove the statement

$$\exists (x, y, z) \in \overline{\mathbb{Q}} \times \mathbb{Q} \times \mathbb{Q} \ (y \neq z \land x^y = z)$$

You do not need to justify your answer. However, if you include clear explanations, we may be able to give partial credit for an answer with some imprecision.

Solution: A translation would be "Some irrational number raised to a rational power gives a rational output, and this output is different from the exponent in the power". A witness to this statement is $x = \sqrt{\sqrt{2}} = \sqrt[4]{2} = 2^{\frac{1}{4}}$, $y = 4$, $z = 2$. The number x is irrational (again, we can prove by contradiction that if it were rational, so would $\sqrt{2}$ be) while y, z are distinct integers so are rational. Moreover,

$$x^y = \left(2^{\frac{1}{4}}\right)^4 = 2 = z$$

as required.

(d) (*Graded for fair effort completeness*[3]) Fill in the blanks in the following argument.

Claimed statement: $\exists x \in \overline{\mathbb{Q}} \ \exists y \in \overline{\mathbb{Q}} \ \exists z \in \mathbb{Q} \ (x^y = z)$.

> **Proof**: We need to give a witness to prove this existential claim. We proceed in a proof by cases, since the disjunction **(i)**$\underline{(\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}) \lor (\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q})}$ is true.
>
> - **Case 1**: We need to show that
>
> $$(\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}) \to \exists x \in \overline{\mathbb{Q}} \ \exists y \in \overline{\mathbb{Q}} \ \exists z \in \mathbb{Q} \ (x^y = z)$$

[3] Fair effort completeness for this question means either attempting to correctly answer each part or to write a sentence or two on where you get stuck in your attempt to correctly answer the question.

Assume towards a direct proof that **(ii)**$\underline{(\sqrt{2}^{\sqrt{2}} \in \mathbb{Q})}$. We choose the witnesses $x = \sqrt{2}$, $y = \sqrt{2}$, $z = \sqrt{2}^{\sqrt{2}}$. By the theorem we proved in class, $\sqrt{2} \notin \mathbb{Q}$. Since $x = y = \sqrt{2}$, $x \in \overline{\mathbb{Q}}$ and $y \in \overline{\mathbb{Q}}$. By the assumption of this direct proof, $z \in \mathbb{Q}$. Thus, the witnesses we picked are in the required domains. Moreover, by definition, $z = x^y$, as required. Thus, the existential claim is proved and we have completed the direct proof required for this case.

- **Case 2**: We need to show that

  $$(\sqrt{2}^{\sqrt{2}} \in \overline{\mathbb{Q}}) \to \exists x \in \overline{\mathbb{Q}}\ \exists y \in \overline{\mathbb{Q}}\ \exists z \in \mathbb{Q}\ (x^y = z)$$

  Assume towards a direct proof that $(\sqrt{2}^{\sqrt{2}} \in \overline{\mathbb{Q}})$. We choose the witnesses

  $$x = \textbf{(iii)}\underline{\sqrt{2}^{\sqrt{2}}},\ y = \textbf{(iv)}\underline{\sqrt{2}},\ z = \textbf{(v)}\underline{\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}}$$

  By the assumption of this direct proof, $x \in \overline{\mathbb{Q}}$. As we mentioned above, $\sqrt{2} \notin \mathbb{Q}$ so $y \in \overline{\mathbb{Q}}$. Picking $p = 2, q = 1$, we observe that $z = \frac{2}{1}$ and since **(vi)**$\underline{2 \in \mathbb{Z} \text{ and } 1 \in \mathbb{Z}^{\neq 0}}$, $z \in \mathbb{Q}$. Thus, the three witnesses we picked are in the required domains. Calculating:

  $$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2}\cdot\sqrt{2}} = \left(\sqrt{2}\right)^{2} = \sqrt{2} \cdot \sqrt{2} = 2$$

  which proves that **(vii)**$\underline{x^y = z}$, and hence x, y, z are the required witnesses. Thus, the existential claim is proved and we have completed the direct proof required for this case.

The proof by cases is now complete and the statement has been proved. QED

3. Recall that A **hex color** is a nonnegative integer, n, that has a base 16 fixed-width 6 expansion

   $$n = (r_1 r_2 g_1 g_2 b_1 b_2)_{16,6}$$

   where $(r_1 r_2)_{16,2}$ is the red component, $(g_1 g_2)_{16,2}$ is the green component, and $(b_1 b_2)_{16,2}$ is the blue component. For notational convenience, we define the set $C = \{x \in \mathbb{N} \mid x < 16^6\}$. This is the set of possible hex colors because these are all numbers that have hexadecimal fixed-width 6 expansions.

   (a) (*Graded for correctness*) Determine and briefly justify whether C is finite, countably infinite, or uncountable.

   Solution: This set is finite because it is a bounded collection of natural numbers: the natural numbers between 0 and $16^6 - 1$. Since the number of distinct element in this set is 16^6, a natural number, the set is finite.

   (b) Consider the function $red : C \to C$ given by $red(\ (r_1 r_2 g_1 g_2 b_1 b_2)_{16,6}\ ) = (r_1 r_2 0000)_{16,6}$.

i. (*Graded for correctness*) Determine whether *red* is one-to-one, and justify your conclusion using valid proof strategies.

Solution: This function is not one-to-one, as can be seen by the counterexample $a_1 = (FF0000)_{16,6}$, $a_2 = (FFFFFF)_{16,6}$. These are distinct elements of the domain because they are different from one another and they are each integers that have hexadecimal fixed-width 6 representations. However,

$$red(a_1) = red(\ (FF0000)_{16,6}\ ) = (FF0000)_{16,6}$$

and

$$red(a_2) = red(\ (FFFFFF)_{16,6}\ ) = (FF0000)_{16,6}$$

so these distinct domain elements are mapped to the same codomain element, a failure of injectivity.

ii. (*Graded for correctness*) Determine whether *red* is onto, and justify your conclusion using valid proof strategies.

Solution: This function is not onto, as can be seen by the counterexample $b = (FFFFFF)_{16,6}$. This is an element of the codomain (because it is a valid hex color) but is not the image under *red* of *any* domain element because all images under *red* have 0s in the blue and green components, whereas b does not.

4. Consider the set of ratings in a 3-movie database $R = \{-1, 0, 1\} \times \{-1, 0, 1\} \times \{-1, 0, 1\}$ and the set of bases of RNA strands $B = \{\mathtt{A}, \mathtt{C}, \mathtt{U}, \mathtt{G}\}$.

(a) (*Graded for fair effort completeness*) Give a (well-defined) one-to-one function with domain R and codomain B or explain why there is no such function.

Solution: There is no such function because $|R| = 27$ (see earlier review quiz) and $|B| = 4$ and the existence of a one-to-one function with domain R and codomain B would imply that $27 \leq 4$, which is not true.

(b) (*Graded for fair effort completeness*) Give a (well-defined) one-to-one function with domain B and codomain R or explain why there is no such function.

Solution: Consider the function $f : B \to R$ given by $f(\mathtt{A}) = (1, 0, 1)$, $f(\mathtt{C}) = (0, 0, 0)$, $f(\mathtt{G}) = (1, -1, 0)$ and $f(\mathtt{U}) = (1, -1, 1)$. This is a well-defined function and it is one-to-one.

(c) (*Graded for fair effort completeness*) Give a (well-defined) onto function with domain R and codomain B or explain why there is no such function.

Solution: Consider the function $g : R \to B$ given by

$$g(\ (a_1, a_2, a_3)\ ) = \begin{cases} \mathtt{A} & \text{if } (a_1, a_2, a_3) = (1, 1, 1) \\ \mathtt{C} & \text{if } (a_1, a_2, a_3) = (1, 1, 0) \\ \mathtt{G} & \text{if } (a_1, a_2, a_3) = (1, 1, -1) \\ \mathtt{U} & \text{otherwise} \end{cases}$$

This is a well-defined function and it is onto.

(d) (*Graded for fair effort completeness*) Give a (well-defined) onto function with domain B and codomain R or explain why there is no such function.

Solution: There is no such function because $|R| = 27$ (see earlier review quiz) and $|B| = 4$ and the existence of an onto function with domain B and codomain R would imply that $4 \geq 27$, which is not true.

Sample calculation that can be used as reference for the detail expected in your answer when specifying functions and reasoning about their properties:

We give a (well-defined) function with domain R and codomain B that is neither one-to-one nor onto.

Define $g : R \to B$ by, for $(x_1, x_2, x_3) \in R$,

$$g(\ (x_1, x_2, x_3)\ ) = \begin{cases} \texttt{A} & \text{if } x_1 = 1 \\ \texttt{C} & \text{if } x_1 = 0 \\ \texttt{G} & \text{if } x_1 = -1 \end{cases}$$

This function is well-defined because each ratings 3-tuples is mapped to a unique base. However, this function is not one-to-one, as we can see from the counterexample: $a = (1, 1, 1)$, $b = (1, 0, 0)$. These are ratings 3-tuples (in the domain) which are distinct (they disagree about the second and third movies) but

$$g(a) = g(\ (1, 1, 1)\ ) = \texttt{A} = g(\ (1, 0, 0)\ ) = g(b)$$

because the two ratings agree on the first movie. Distinct domain elements getting mapped to the same codomain elements is a counterexample to injectivity.

The function g is also not onto, as we can see from the counterexample $\texttt{U}$. This is an element of the codomain which is not $f(x)$ for any x in the domain, as we can see from the piecewise definition of g, where in no case do we have the output value $\texttt{U}$.
