**TheoryPrep** **(Due: 6/21/20)**

# Assignment #3: Functions and Cardinality

*Name:* Student name(s)

We've taken some problems from the course texts. Some problems are marked as (Challenge) or (Additional Problems). Do the rest first, and if you have time, return to these problems. It's **much more important** to have a rigorous understanding of the core problems and how to prove them than to simply finish all the additional problems.

**Problem 1: Do Our Definitions Make Sense**

Learning goal: As discussed in the videos, whenever you see a definition that's supposed to capture an intuitive idea like "size", you should make sure the definitions have the properties you would expect. In this section you will prove some of these properties. Hint: you'll mostly be applying the definitions of surjectivity and injectivity.

**(a)** If $|A| \leq |B|$ and $|B| \leq |C|$, then we'd expect $|A| \leq |C|$ (this is called transitivity). According to our definitions, this means we need to prove that if there exist surjections $f : B \to A$ and $g : C \to B$ then there must be a surjection from $C \to A$.

**Solution:**
Let $f, g$ be surjections as defined in the problem. I claim $f \circ g$ is a surjection from $C$ to $A$. Fix arbitrary element $c \in C$, and since $g$ is surjective $\exists b \in B$ such that $g(c) = b$. Since $f$ is surjective, $\exists a \in A$ such that $f(b) = a$, so $f \circ g(c) = a$.

**(b)** If $|A| = |B|$ and $|B| = |C|$, then we'd expect $|A| = |C|$ (this is again the transitivity property). According to our definitions, this means we should prove, if there exists a bijection $f : B \to A$ and a bijection $g : C \to B$, then there exists a bijection from $C$ to $A$.

**Solution:**
Let $f, g$ be bijections as specified in the problem. I claim $f \circ g : C \to A$ is a bijection. We proved above it is a surjection so we only need to prove it is an injection. Fix arbitrary $c \neq c' \in C$. We know that $g(c) \neq g(c')$ since $g$ is injective, and since $f$ is injective, we have $f(g(c)) \neq f(g(c'))$. This implies our claim.

**(c)** If two sets have the same cardinality, we'd expect be able to write either $|A| = |B|$ or $|B| = |A|$ (this is called the symmetric property–it's not true for $<$ for example). Thus, we want to prove that there exists a bijection $f : A \to B$ if and only if there exists a bijection from $g : B \to A$.

**Solution:**
Let $f : A \to B$ a bijection. Now define the function $g$ as follows. First recall that we know that $\forall b \in B \exists a \in A.f(a) = b$. In particular, since $f$ is injective, we know there exists a unique $a$ such that $f(a) = b$. Let $g$ send each $b$ to that $a$. I claim this is a bijection. It is surjective because $\forall a' \in A$, $f(a') = b'$ for some $b' \in B$, so by definition $g(b') = a'$ (recall that $g$ sends $b'$ to its unique preimage). It is injective because if $c \neq c' \in B$ then $g(c) \neq g(c')$ since $g(c) = g(c') = d \Rightarrow f(d) = c, c'$ and it is not possible

for a function to map an input to two different outputs.

The other direction follows identically. We use a bijection $B \to A$ to construct a bijection $A \to B$.

**(d)** In the videos we discussed how an surjection from $A \to B$ defines $|A| \geq |B|$ and an injection from $A \to B$ intuitively corresponds to $|A| \leq |B|$. In explaining why these definitions were consistent, we used the fact that a surjection $f : A \to B$ exists if and only if an injection $g : B \to A$ exists (you can assume the axiom of choice if you want–you don't need to worry about it though if you feel all the assumptions in your proof are fine). Prove this fact.

**Solution:**
($\Rightarrow$) Let $f : A \to B$ be surjective. I will define an injection $g : B \to A$ as follows. For any $b \in B$, since $f$ is surjective, there exists some $a \in A$ such that $f(a) = b$ (the axiom of choice says since there may be multiple elements in the preimage of $\{b\}$ we can pick one–if students don't bring this up, I don't think you should either since it's not relevant to the course). Thus, let $g$ map $b$ to this $a$. This is an injection because fix arbitrary $b \neq b' \in B$. $g(b) = g(b') = a'$ implies that there is some $a'$ such that $f(a') = b \neq b' = f(a')$, a contradiction (ie $f$ cannot map the same element to two different elements).

($\Leftarrow$) Let $g : B \to A$ be an injection. Pick an arbitrary $b' \in B$ and define $f : A \to B$ as follows

$$f(a) = \begin{cases} b & \exists b \in B . g(b) = a \\ b' & \text{else} \end{cases} \tag{0.1}$$

Note that in the first case, there can be only one $b \in B$ such that $g(b) = a$ because $g$ is injective. We now prove $f$ surjective. For any $b \in B$, $g(b) = a$ (note here we are assuming $g$ is total as we said we would in general in the videos) and by definition $f(a) = b$.

## Problem 2: Problems about Functions

Learning goal: This section has a number of problems about functions that require a diversity of techniques. Working on them will develop your proof skills and understanding of the mathematical concepts around functions.

**(a)** Give an example of a function $f : \mathbb{R} \to \mathbb{R}$ that is injective but not bijective. Prove that it is injective but not surjective.

**Solution:**
Let $f(x) = e^x$. This is not surjective since it cannot output $-1$, for example. It is injective because (using the contrapositive) $e^x = e^{x'} \Rightarrow \log(e^x) = \log(e^{x'}) \to x = x'$.

**(b)** Let $f : A \to B$ and $g : B \to C$ for some sets $A, B, C$. Prove that if $g \circ f$ is a bijection, then $f$ is an injection and $g$ is a surjection.

**Solution:**
First we prove $g$ is a surjection. Suppose towards a contradiction that it is not, so $\exists c \in C$ that is not in the image of $g(B)$. We see therefore that $c$ is not in the image of $g \circ f(A)$, so this contradicts that $g \circ f$ is a bijection.

Now we prove that $f$ is an injection. Again, suppose towards a contradiction that $f$ is not an injection, so $\exists a, a' \in A$ such that $f(a) = f(a')$. This implies that $g \circ f(a) = g \circ f(a')$, contradicting that $g \circ f$ is bijective.

**(c)** Let $f : A \to B$ and $g : B \to C$ for some sets $A, B, C$. Prove or disprove: If $g \circ f$ is a bijection, then $g$ is an injection or $f$ is a surjection.

**Solution:**
We provide a counterexample.

Let $A = \mathbb{R}^{\geq 0}$ be the set of non-negative real numbers, let $B = \mathbb{R}$, and let $C = \mathbb{R}^{\geq 0}$. Now if we let $f(a) = \sqrt{a}$ and $g(b) = b^2$ then we have $g(f(a)) = (\sqrt{a})^2 = a$. So we have $g \circ f$ is a bijection since it is an identity mapping from $\mathbb{R}^{\geq 0}$ to $\mathbb{R}^{\geq 0}$.

But $g$ is not an injection since $g(-b) = g(b)$ for all $b$ and $f$ is not a surjection since it cannot produce any negative numbers.

**(d)** Let $f : D \to D$ be a function where $D$ is nonempty. Indicate which of the below conditions are logically equivalent to $f$ being injective ($g$ is a function mapping $D \to D$). You do not need to prove the equivalence, but you should justify it to yourself.

1. $\forall x, y \in D. x = y$ or $f(x) \neq f(y)$
2. $\forall x, y \in D. x = y \Rightarrow f(x) = f(y)$
3. $\forall x, y \in D. x \neq y \Rightarrow f(x) \neq f(y)$
4. $\forall x, y \in D. f(x) = f(y) \Rightarrow x = y$
5. $\neg(\exists x, y \in D. x \neq y$ and $f(x) = f(y))$
6. $\neg(\exists x \in D \forall y \in D. f(x) = f(y))$
7. $\exists g \forall x \in D. f(g(x)) = x$
8. $\exists g \forall x \in D. g(f(x)) = x$

**Solution:**

1. True
2. False
3. True
4. True
5. True
6. False
7. False
8. True

**Problem 3: Longer Proofs**

Learning Goal: These proofs require multiple different techniques and steps which will help you understand how to do and clearly write up multi-step proofs.

**(a)** We first introduce a couple of definitions. Let $\{0, 1\}^*$ be the set of all finite length binary strings (so things like $0, 110, 110101011$). Let $F = \{f : \mathbb{N} \to \{0,1\}^*\}$ be the set of all functions mapping the natural numbers to finite binary strings ($\{0,1\}^*$ is the set of all finite length binary strings).

We might be interested in knowing which of these sets (if either) is larger. Intuitively, it seems like $F$ should be much larger, but as we know, comparing infinite cardinalities is not as easy as that. Prove that $F$ is indeed larger, or in other words that there exists no surjection from $\{0,1\}^* \to F$.

**Solution:**
First we prove that we can enumerate out the elements of $\{0,1\}^*$ (ie that they are countable). We can simply list them out in order of increasing length, and amongst string of the same length use their value in binary as the tiebreaker. We list them out below

$$0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100... \tag{0.2}$$

By definition, this is what it means for them to be countable. The important property here that we need is that we can list out the finite length binary strings in some way (the convenience of the definition of countability here demonstrates its strength). Let $N : \mathbb{N} \to \{0,1\}^*$ be the function that maps each natural number to a finite binary string according to the above order (we will use this later). We now prove that there does not exist a surjection from $\{0,1\}^* \to F$. Fix an arbitrary map $g : \{0,1\}^* \to F$. To prove it is not a surjection, we will find a function $f \in F$ that is not in the image of $g$. We proceed by diagonalization argument.

In particular, denote $g(b) = f_b$, so $f_b : \mathbb{N} \to \{0,1\}^*$ is the map that we get from $g$ on binary bit $b$. Now define $f(n) = f_{N(n)}(n)|0$ (where by $|0$ we mean append a 0). We see that $f$ is not in the image of $g$ because for any $b \in \{0,1\}^*$, $g(b) = f_b$ disagrees with $f$ on the natural number $n$ such that $N(n) = b$ (which must exist since $N$ is a bijection), since $f(n) = f_{N(n)}(n)|0 = f_b(n)|0$.

**(b)** (Additional Problem) Let $E = \{ae^{bx} + c | a, b, c \in \mathbb{R}, a \neq 0, b \neq 0\}$ be the set of non-constant exponential functions and $L = \{ax + b | a, b \in \mathbb{R}, a \neq 0\}$ be the set of non-constant linear functions.

We inductively define $S$ to contain functions $f$ which satisfy any of the following 3 conditions:

1. $f \in E$
2. $f \in L$
3. $f = g \circ h$, where $g \in S$ and $h \in S$

That is, we start with all the linear and exponential functions in $S$ and then add any function we can get by composing them together.

Prove that if $f \in S$, then $f$ is injective.

**Solution:**
Last week we talked about how to generalize inductive proofs for inductively defined sets, made concrete with example problems about $\mathbb{Z}, \mathbb{Q}$. In this problem, we apply similar skills. We have an explicit, inductively constructed set, and we will prove that $\forall f \in S$ $f$ injective via induction. There are two base cases (corresponding to 1 and 2)

1. $f \in E$. In this case, if $f(x) = f(x')$ we have by definition

$$\begin{gathered} ae^{bx} + c = ae^{bx'} + c \\ \Downarrow \\ \log(e^{bx}) = \log(e^{bx'}) \\ \Downarrow \\ x = x' \end{gathered} \tag{0.3}$$

assuming that $a \neq 0$.

2. $f \in L$. Then if $f(x) = f(x')$ we have

$$\begin{gathered} ax + b = ax' + b \\ \Downarrow \\ x = x' \end{gathered} \tag{0.4}$$

again assuming that $a \neq 0$.

Now for the inductive step. Suppose that $g, h \in S$ and $g, h$ injective. Then $f = g \circ h$ is injective since the composition of injective functions injective. $\forall x \neq x'$ we have $g(h(x)) = g(h(x'))$ and $h(x) \neq h(x')$ since $h$ injective, so $g(h(x)) \neq g(h(x'))$ since $g$ injective.

Note importantly that this does not prove injectivity for infinite compositions of linear and exponential functions, because $S$ is defined by the application of a finite number of rules (arbitrarily large finite quantity, but nonetheless finite). This is similar to the reason that a proof inducting on the number of elements failed to prove the well-ordering principle on problem 1 of last week, except here, $S$ only contains finite compositions of linear and exponential functions.

**(c)** Let $\{1, 2, 3\}^\omega$ be the set of infinite strings of $1, 2$, and $3$ and $\{4, 5\}^\omega$ be the set of infinite strings of 4 and 5. Prove that a bijection exists between $\{4, 5\}^\omega$ and $\{1, 2, 3\}^\omega \times \{1, 2, 3\}^\omega$

**Solution:**
In order to prove a bijection exists, we prove that a surjection exists in both directions. First we prove a surjection $f : \{4, 5\}^\omega \to \{1, 2, 3\}^\omega \times \{1, 2, 3\}^\omega$. For any $a \in \{4, 5\}^\omega$, $f(a)$ splits up the string $a$ into groups of 2, so $a = a_0a_1a_1...$ where each $a_i$ is two numbers. Then it replaces each $a_i$ with $a'_i$ determined as follows: $a'_i = 1$ if $a_i = 44$, $a'_i = 2$ if $a_i = 45$, and $a'_i = 3$ if $a_i = 54, 55$. It then returns the strings $(a'_0a'_2a'_4..., a'_1a'_3a'_5...)$. I claim this is a surjection. Fix arbitrary $b, c \in \{1, 2, 3\}^\omega \times \{1, 2, 3\}^\omega$. We can write $b = b_0b_1b_2...$ for $b_i \in \{1, 2, 3\}$ and similarly $c = c_0c_1c_2....$ Now define $a_i$ as follows

$$a_i = \begin{cases} 44 & 2|i \text{ and } b_{\frac{i}{2}} = 1 \\ 45 & 2|i \text{ and } b_{\frac{i}{2}} = 2 \\ 55 & 2|i \text{ and } b_{\frac{i}{2}} = 3 \\ 44 & 2 \nmid i \text{ and } c_{\frac{i-1}{2}} = 1 \\ 45 & 2 \nmid i \text{ and } c_{\frac{i-1}{2}} = 2 \\ 55 & 2 \nmid i \text{ and } c_{\frac{i-1}{2}} = 3 \end{cases} \tag{0.5}$$

I claim that $f(a) = (b, c)$. By definition, $f$ uses the $a_i$ with $2|i$ to define $b_{\frac{i}{2}}$, and by definition, these $a_i$ give the right $b_i$ values. They similarly give the correct $c_{\frac{i-1}{2}}$ values by construction.

Now to prove that a surjection $g : \{1, 2, 3\}^\omega \times \{1, 2, 3\}^\omega \to \{4, 5\}^\omega$. For any $a, b \in \{1, 2, 3\}^\omega \times \{1, 2, 3\}^\omega$, consider only $a$. Replace each 1 or 2 in $a$ with a 4 and each 3 in $a$ with a 5. I claim $g$ is surjective. For any $c \in \{4, 5\}^\omega$, let $a'$ be the string created by replacing each 4 with a 1 and each 5 with a 3 in $c$, and $b'$ be an infinite string of 1s. By definition, $g(a', b') = c'$.

**(d)** (Challenge) Prove Schroder-Bernstein.

**Solution:**
This proof is very difficult and is meant for the extraordinary student who's completely finished the rest of the pset. Usually Schroeder-Bernstein is phrased in terms of injections, but assuming the axiom of choice (and therefore the result we prove in 1.d), the phrasing in the Math for CS in terms of surjections is the same. Below are two good explanations: first a more detailed proof and second a more concise AoPS explanation.

**Problem 4: Review**

Learning goal: It's important to keep skills fresh. We review material from the previous two weeks.

**(a)** (Additional Problem) Consider a modified version of football, where the teams can score either 4 or 7 points at a time. Find and prove the minimum point value $k$ such that a team can achieve any score any number of points greater than or equal to $k$.

**Solution:**
Let $P(j)$ be true if we can score $j$ points in this game.

With just scoring 4 points we can achieve the scores $4, 8, 12, 16, 20$. With just scoring 7 points we can achieve the scores $7, 14, 21$. With both of them we can achieve scores $11, 15, 18, 19$.

These lists show that we can achieve scores of $18, 19, 20, 21$. We have that $P(j) \implies P(j+4)$, as we can always score 4 more points. Together with the base cases $P(18), P(19), P(20), P(21)$, induction gives us that $P$ holds for $j \geq 18$. You can check that $P(17)$ fails to hold, so that $k = 18$.

**(b)** (Additional Problem) There are some interesting closure relationships between rationals and irrationals (here closure means that if you do an operation to elements of a set–like adding two elements or taking the square root of an element–you stay in the set). For example, we proved in a previous video if $n^2$ is irrational, then $n$ is also irrational. We might also note that if $a, b$ are rational, then so is $a + b$ or $ab$. In this problem we consider a more complex operation of exponentiation. Prove that both the rationals and the irrationals are not closed under exponentiation. This means, prove that there exists $a, b \in \mathbb{Q}$ such that $a^b \notin \mathbb{Q}$, and prove there exists $a, b \in \mathbb{R} - \mathbb{Q}$ ($\mathbb{R} - \mathbb{Q}$ is the irrationals) such that $a^b \notin \mathbb{R} - \mathbb{Q}$. As a hint, try using $\sqrt{2}^{\sqrt{2}}$. You may assume $\sqrt{2}$ is irrational.

**Solution:**
$\mathbb{Q}$ is not closed under exponentiation since $2^{\frac{1}{2}} = \sqrt{2}$ is irrational.

Now we will prove that the irrationals are not closed. We do this by cases. Suppose that $\sqrt{2}^{\sqrt{2}}$ is rational. Then we're done. Now suppose that it is irrational, then we take $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$, which is clearly rational since it is an integer, giving us the exponentiation of two irrationals to a rational.

**Problem 5: Logistics**

Purpose: This helps us make sure the course is going at the right speed!

**(a)** How long did you spend on the videos and readings this week?

**(b)** How long (including time in problem sessions) did you spend on this problem set?

**(c)** Do you have any feedback about the course in general (did the videos and readings sufficiently prepare you for the problem set)?