Problem Set 4 Solutions

Problem One: Cartesian Products and Cardinalities (20 Points)

i. Using the function f defined above, prove that if A, B, C, and D are sets where $|A| = |C|$ and $|B| = |D|$, then we have $|A \times B| = |C \times D|$. Specifically, prove that f is a bijection between $A \times B$ and $C \times D$.

Proof: Since $|A| = |C|$ and $|B| = |D|$, there must be bijections $g : A \to C$ and $h : B \to D$. Now, define the function $f : A \times B \to C \times D$ as $f(a, b) = (g(a), h(b))$. We will prove f is a bijection, from which we can conclude $|A \times B| = |C \times D|$.

To show that f is injective, consider any $(a_1, b_1) \in A \times B$ and $(a_2, b_2) \in A \times B$ where we have $f(a_1, b_1) = f(a_2, b_2)$. We will prove that $(a_1, b_1) = (a_2, b_2)$. Since $f(a_1, b_1) = f(a_2, b_2)$, we see that $(g(a_1), h(b_1)) = (g(a_2), h(b_2))$. Since two ordered pairs are equal iff their components are equal, this means $g(a_1) = g(a_2)$ and $h(b_1) = h(b_2)$. Since g and h are bijections, they are injective, so from $g(a_1) = g(a_2)$ we get that $a_1 = a_2$ and from $h(b_1) = h(b_2)$ we get $b_1 = b_2$. Thus $(a_1, b_1) = (a_2, b_2)$, as required.

To show that f is surjective, consider any $(c, d) \in C \times D$. We will prove that there is some ordered pair $(a, b) \in A \times B$ such that $f(a, b) = (c, d)$. To see this, note that since g and h are bijections, they are surjective. Therefore, there is some $a \in A$ such that $g(a) = c$ and some $b \in B$ such that $h(b) = d$. Therefore, $f(a, b) = (g(a), h(b)) = (c, d)$, as required. ■

ii. Using your result from (i) and the above definition, prove $|\mathbb{N}^k| = |\mathbb{N}|$ for all nonzero $k \in \mathbb{N}$.

Proof: By induction. Let $P(k)$ be "$|\mathbb{N}^k| = |\mathbb{N}|$." We'll prove $P(k)$ holds for all natural numbers $n \geq 1$.

As our base case, we prove $P(1)$, that $|\mathbb{N}^1| = |\mathbb{N}|$. Since by definition $\mathbb{N}^1 = \mathbb{N}$, this statement holds. For the inductive step, assume that for some $k \geq 1$ that $P(k)$ holds and $|\mathbb{N}^k| = |\mathbb{N}|$. We'll prove $P(k+1)$, that $|\mathbb{N}^{k+1}| = |\mathbb{N}|$. To see this, note that

$$|\mathbb{N}^{k+1}| = |\mathbb{N} \times \mathbb{N}^k| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$$

Thus $|\mathbb{N}^{k+1}| = |\mathbb{N}|$, so $P(k + 1)$ holds, completing the induction. ■

Why we asked this question: Part (i) of this question was designed to ensure that you have written at least one proof involving injectivity and surjectivity. We wanted to make sure that you had seen those definitions in action by working with them yourself.

Part (ii) of this problem was here to show you that even though we have formal definitions of cardinality in terms of bijections, that doesn't mean you have to use that definition all the time. All of the reasoning in the problem is layered on top of the theorems we know about cardinality (transitivity and the result from part (i), for example). We also wanted to give you another chance to write a proof by induction.

Problem Two: Simplifying Cantor's Theorem? (8 Points)

The problem with the proof is that it just shows that one particular function isn't a bijection from S to $\wp(S)$. For this proof to show that $|S| \neq |\wp(S)|$, it would have to show that *no* function is a bijection from S to $\wp(S)$, rather than just finding one function that doesn't work.

Why we asked this question: It's very natural to ask why this proof doesn't work – before putting it on the problem set, we typically got at least a few students a quarter who asked this – and the answer calls back down to the definition of cardinality. Additionally, we found that this question helps many students avoid making this sort of mistake when writing diagonalization proofs.

Problem Three: Understanding Diagonalization (8 Points)

i. Suppose that $f(n) = n$. What is the diagonal number d in this case?

The diagonal number is 1.111... = $^{10}/_{9}$. Notice that $r[n] = 0$ for every n, either because

- $n = 0$ and the integer part of $f(0) = 0$ is 0, or because
- $n > 0$ and the nth decimal digit of $f(n)$ n is 0.

ii. Let d_0 be the value of d that you found in part (i). Give an example of a function $g : \mathbb{N} \to \mathbb{R}$ such that there is an $n \in \mathbb{N}$ where $g(n) = d_0$.

One extremely simple function is $f(n) = {}^{10}/_{9}$.

iii. What is the diagonal number for your function g that you defined in part (ii)?

Since every decimal digit of every number outputted by f is 1, the diagonal number is 0.

Problem Four: Uncomputable Functions (28 Points)

i. Define an injective function $g : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$.

One possible option is

$$g(n)(m) = n$$

In other words, the function $g(n)$ is a function that always produces the value n regardless of input.

ii. Prove the function you came up with in part (i) is an injection. You might want to use the fact that two functions $h_1 : \mathbb{N} \to \mathbb{N}$ and $h_2 : \mathbb{N} \to \mathbb{N}$ are equal iff $h_1(n) = h_2(n)$. Equivalently, this means that $h_1 \neq h_2$ iff there is some n where $h_1(n) \neq h_2(n)$.

Proof: We will prove that if $n_1 \neq n_2$, then we can find an x such that $f(n_1)(x) \neq f(n_2)(x)$. This means that if $n_1 \neq n_2$, we will have that $f(n_1) \neq f(n_2)$.

To see this, note that if $n_1 \neq n_2$, then $f(n_1)(0) = n_1$ and $f(n_2)(0) = n_2$, so $f(n_1)(0) \neq f(n_2)(0)$. Therefore, $f(n_1) \neq f(n_2)$, as required. Thus f is injective. ■

iii. Let $f : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ be an arbitrary function from $\mathbb{N}$ to $\mathbb{N}^{\mathbb{N}}$. Give a definition of a "diagonal function" $d : \mathbb{N} \to \mathbb{N}$ such that $f(n) \neq d$ for any $n \in \mathbb{N}$.

One possible function is this one:

$$d(n) = f(n)(n) + 1$$

In other words, the value of d, evaluated at n, is the nth value of the nth function plus one.

How would you come up with this? One option is to draw out a 2D table, where each row represents a function and each column the output of that function at a particular point. This diagonal function is then formed by taking the diagonal of the table and adding one to each entry, making d different from every function. Another way to think of this is to think of the nth "piece" of a function as the value of that function evaluated at n. Then the nth piece of d (that is, $d(n)$) is defined to be different from the nth piece of the nth function (that is, $f(n)(n)$).

iv. Using the diagonal function d you defined in part (iii), prove that $|\mathbb{N}| \neq |\mathbb{N}^{\mathbb{N}}|$. Make sure that you formally prove why your diagonal function has the property that $f(n) \neq d$ for any $n \in \mathbb{N}$.

Proof: Suppose for the sake of contradiction that $|\mathbb{N}| = |\mathbb{N}^{\mathbb{N}}|$. Then there must exist some bijection $f : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$. Define the function $d : \mathbb{N} \to \mathbb{N}$ as $d(n) = f(n)(n) + 1$.

Since f is a bijection, it is surjective, so there must be some $n \in \mathbb{N}$ such that $f(n) = d$. This means, in particular, that $f(n)(n) = d(n)$. However, $d(n) = f(n)(n) + 1$, so this means that $f(n)(n) = f(n)(n) + 1$, which is impossible.

We have reached a contradiction, so our assumption was wrong. Thus $|\mathbb{N}| \neq |\mathbb{N}^{\mathbb{N}}|$. ■

Why we asked this question: Diagonalization proofs are hard. They're perhaps the most sophisticated type of proof that we're going to do this quarter. Because they're so important in computability theory (as you'll see later on), we wanted to make sure that you have practice with diagonalization.

In past quarters, we didn't subdivide these tasks and we found that students didn't build a rigorous intuition for diagonalization. By subdividing this task into multiple smaller tasks, we hoped that you would understand what specifically goes into each step and how the overall proof is derived from the construction of smaller objects.

Problem Five: Propositional Equivalences (12 Points)

i. $p \to q$ and $\neg q \to \neg p$

These are equivalent.

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

p	q	$\neg q$	$\to$	$\neg p$
F	F	T	T	T
F	T	F	T	T
T	F	T	F	F
T	T	F	T	F

ii. $\neg(p \to q)$ and $p \to \neg q$

These are **not** equivalent. If p is false, then $\neg(p \to q)$ evaluates to false (because $p \to q$ evaluates to true), but $p \to \neg q$ evaluates to true.

iii. $\neg(p \leftrightarrow q)$ and $p \leftrightarrow \neg q$

These are equivalent.

p	q	$\neg$	$(p \leftrightarrow q)$
F	F	F	T
F	T	T	F
T	F	T	F
T	T	F	T

p	q	$p \leftrightarrow$	$\neg q$
F	F	F	T
F	T	T	F
T	F	T	T
T	T	F	F

iv. $p \lor q$ and $\neg p \to q$

These are equivalent.

p	q	$p \lor q$
F	F	F
F	T	T
T	F	T
T	T	T

p	q	$\neg p$	$\to q$
F	F	T	F
F	T	T	T
T	F	F	T
T	T	F	T

Why we asked this question: Parts (i), (iii), and (iv) are important equivalences. (i) justifies proof by contradiction, (iii) is useful when negating biconditionals, and (iv) is the equivalence you used in Problem Set Three to show that a graph or its negation must be connected. Part (ii) is an *extremely common* misconception. To make sure that you understand that these two statements are not the same, we wanted to let you explore whether or not they were equal so that you would eventually discover how they differ from one another.

Problem Six: First-Order Negations (16 points)

i. $\exists S. (Set(S) \land \forall x. x \notin S)$

$$\neg\exists S. (Set(S) \land \forall x. x \notin S)$$
$$\forall S. \neg(Set(S) \land \forall x. x \notin S)$$
$$\forall S. (Set(S) \to \neg\forall x. x \notin S)$$
$$\forall S. (Set(S) \to \exists x. \neg(x \notin S))$$
$$\forall S. (Set(S) \to \exists x. x \in S)$$

Note: the original statement here is "the empty set exists." The negation says "every set contains at least one element."

ii. $\forall p. \forall q. (p \in \mathbb{N} \land q \in \mathbb{N} \land q \neq 0 \to q \times q \times 2 \neq p \times p)$

$$\neg\forall p. \forall q. (p \in \mathbb{N} \land q \in \mathbb{N} \land q \neq 0 \to q \times q \times 2 \neq p \times p)$$
$$\exists p. \neg\forall q. (p \in \mathbb{N} \land q \in \mathbb{N} \land q \neq 0 \to q \times q \times 2 \neq p \times p)$$
$$\exists p. \exists q. \neg(p \in \mathbb{N} \land q \in \mathbb{N} \land q \neq 0 \to q \times q \times 2 \neq p \times p)$$
$$\exists p. \exists q. (p \in \mathbb{N} \land q \in \mathbb{N} \land q \neq 0 \land \neg(q \times q \times 2 \neq p \times p))$$
$$\exists p. \exists q. (p \in \mathbb{N} \land q \in \mathbb{N} \land q \neq 0 \land q \times q \times 2 = p \times p)$$

The original statement here is "the square root of two is irrational." (Do you see why?) The negation of this statement is "the square root of two is rational."

iii. $\forall x \in \mathbb{R}. \forall y \in \mathbb{R}. (x < y \to \exists q \in \mathbb{Q}. (x < q \land q < y))$

$$\neg\forall x. (x \in \mathbb{R} \to \forall y. (y \in \mathbb{R} \to (x < y \to \exists q. (q \in \mathbb{Q} \land x < q \land q < y))))$$
$$\exists x. \neg(x \in \mathbb{R} \to \forall y. (y \in \mathbb{R} \to (x < y \to \exists q. (q \in \mathbb{Q} \land x < q \land q < y))))$$
$$\exists x. (x \in \mathbb{R} \land \neg\forall y. (y \in \mathbb{R} \to (x < y \to \exists q. (q \in \mathbb{Q} \land x < q \land q < y))))$$
$$\exists x. (x \in \mathbb{R} \land \exists y. \neg(y \in \mathbb{R} \to (x < y \to \exists q. (q \in \mathbb{Q} \land x < q \land q < y))))$$
$$\exists x. (x \in \mathbb{R} \land \exists y. (y \in \mathbb{R} \land \neg(x < y \to \exists q. (q \in \mathbb{Q} \land x < q \land q < y))))$$
$$\exists x. (x \in \mathbb{R} \land \exists y. (y \in \mathbb{R} \land (x < y \land \neg\exists q. (q \in \mathbb{Q} \land x < q \land q < y))))$$
$$\exists x. (x \in \mathbb{R} \land \exists y. (y \in \mathbb{R} \land (x < y \land \forall q. \neg(q \in \mathbb{Q} \land x < q \land q < y))))$$
$$\exists x. (x \in \mathbb{R} \land \exists y. (y \in \mathbb{R} \land (x < y \land \forall q. (q \in \mathbb{Q} \land x < q \to \neg(q < y)))))$$
$$\exists x. (x \in \mathbb{R} \land \exists y. (y \in \mathbb{R} \land (x < y \land \forall q. (q \in \mathbb{Q} \land x < q \to q \geq y))))$$

This statement says "there is a rational number in-between every two real numbers," which is true but utterly baffling when you realize that $|\mathbb{R}| > |\mathbb{Q}|$. The negation is "there are two real numbers with no rational number between them."

(continued on the next page...)

iv. $(\forall x. \forall y. \forall z. (R(x, y) \land R(y, z) \to R(x, z))) \to (\forall x. \forall y. \forall z. (R(y, x) \land R(z, y) \to R(z, x)))$

$\neg(\forall x. \forall y. \forall z. (R(x, y) \land R(y, z) \to R(x, z))) \to (\forall x. \forall y. \forall z. (R(y, x) \land R(z, y) \to R(z, x)))$

$(\forall x. \forall y. \forall z. (R(x, y) \land R(y, z) \to R(x, z))) \land \neg(\forall x. \forall y. \forall z. (R(y, x) \land R(z, y) \to R(z, x)))$

$(\forall x. \forall y. \forall z. (R(x, y) \land R(y, z) \to R(x, z))) \land (\exists x. \neg\forall y. \forall z. (R(y, x) \land R(z, y) \to R(z, x)))$

$(\forall x. \forall y. \forall z. (R(x, y) \land R(y, z) \to R(x, z))) \land (\exists x. \exists y. \neg\forall z. (R(y, x) \land R(z, y) \to R(z, x)))$

$(\forall x. \forall y. \forall z. (R(x, y) \land R(y, z) \to R(x, z))) \land (\exists x. \exists y. \exists z. \neg(R(y, x) \land R(z, y) \to R(z, x)))$

$(\forall x. \forall y. \forall z. (R(x, y) \land R(y, z) \to R(x, z))) \land (\exists x. \exists y. \exists z. (R(y, x) \land R(z, y) \land \neg R(z, x)))$

This statement says "if R is transitive, then the inverse relation R^{-1} is transitive." The inverse relation of a relation R is the relation R^{-1} such that $xR^{-1}y$ iff yRx. For example, the inverse relation of $<$ is $>$. The negation says "R is transitive and R^{-1} is not transitive."

Problem Seven: Translating into Logic (28 points)

i. Given the predicate

Natural(x), which states that x is an natural number;

the function

Product(x, y), which yields the product of x and y;

and the constants 1 and 137, write a statement in first-order logic that says "137 is prime."

One possible solution is the following:

$$\forall p. \forall q. (Natural(p) \land Natural(q) \land Product(p, q) = 137 \to ((p = 1 \land q = 137) \lor (p = 137 \land q = 1)))$$

This statement says that if you can find a pair of natural numbers p and q whose product is 137, then either they are 1 and 137 or 137 and 1, respectively.

ii. Given the predicates

Morality(m), which states that m is a morality;
Practice(m), which states that m is practiced; and
Preach(m), which states that m is preached;

write a statement in first-order logic that says "there are exactly two kinds of moralities: one that is practiced but not preached, and one that is preached but not practiced" (paraphrased from a quote by Bertrand Russell.)

One possible solution is

$$\exists m_1. \exists m_2. (Morality(m_1) \land Morality(m_2) \land Practice(m_1) \land \neg Preach(m_1) \land Preach(m_2) \land \neg Practice(m_2) \land \forall m. (Morality(m) \to m = m_1 \lor m = m_2))$$

This says that there are two moralities m_1 and m_2, where m_1 is practiced and not preached and m_2 is preached and not practiced. It also says that any morality has to be either m_1 or m_2.

(continued...)

iii. Given the predicates

$x \in y$, which states that x is an element of y, and
Set(S), which states that S is a set,

write a statement in first-order logic that says "every set has a power set."

Let's walk through this one step-by-step. Recall that the power set of a set S is the set of all subsets of S. Initially, we can encode this as follows:

$$\forall S.\ (Set(S) \to \exists P.\ (P \text{ is the set of all subsets of } S))$$

This isn't legal first-order logic, but it expresses our basic idea. We will encode that every set has a power set by showing that for any sets S, there is some other object P that is its power set.

So how do we say that P is the set of all subsets of S? Well, we'd like to say that it's a set, which we can do by using the *Set* predicate. Furthermore, we need to say that the elements of P are *exactly* the subsets of S. We can try that as follows:

$$
\begin{array}{l}
\forall S.\ (Set(S) \to \\
\quad\quad \exists P.\ (Set(P) \land \\
\quad\quad\quad\quad \forall T.\ (T \in P \leftrightarrow (Set(T) \land T \subseteq S)) \\
\quad\quad) \\
)
\end{array}
$$

Note that we use a biconditional here. We want to say that every subset of S is contained in P, and that nothing else is. Unfortunately, we're not done here, because the $\subseteq$ predicate isn't part of our vocabulary. We can fix this by replacing $T \subseteq S$ with the definition of what it means to be a subset:

$$
\begin{array}{l}
\forall S.\ (Set(S) \to \\
\quad\quad \exists P.\ (Set(P) \land \\
\quad\quad\quad\quad \forall T.\ (T \in P \leftrightarrow \\
\quad\quad\quad\quad\quad\quad (Set(T) \land \\
\quad\quad\quad\quad\quad\quad \forall x \in T.\ x \in S.) \\
\quad\quad\quad\quad) \\
\quad\quad) \\
)
\end{array}
$$

If you ever need to translate something down into first-order logic, it never hurts to take this sort of step-by-step approach of constantly lowering the definition one step at a time.

(continued, again)

iv. Given the predicates

Lady(x), which states that x is a lady;
Glitters(x), which states that x glitters;
IsSureIsGold(x, y), which states that x is sure that y is gold;
Buying(x, y), which states that x buys y; and
StairwayToHeaven(x), which states that x is a Stairway to Heaven;

write a statement in first-order logic that says "There's a lady who's sure all that glitters is gold, and she's buying a Stairway to Heaven."

One possible solution is

$$
\begin{aligned}
&\exists L.\ (\\
&\qquad Lady(L) \land \\
&\qquad \forall x.\ (Glitters(x) \to IsSureIsGold(L, x)) \land \\
&\qquad \exists S.\ (StairwayToHeaven(s) \land Buying(L, S)) \\
&)
\end{aligned}
$$

Though I still have no idea what this means.