INTRODUCTION TO PROOFS

Week 11 Tutorial Solutions

Note: comments in square brackets [such as this comment] are not necessary for a complete solution.

1. (a) Let P, Q represent propositions (meaning statements that are either true or false, but not both simultaneously). Use a truth table to show that $\neg(P \implies Q)$ is equivalent to $P \wedge \neg Q$.

   (b) Recall that we found that an equivalent definition of $f : X \to Y$ being injective is:

   $$\forall x_1, x_2 \in X,\ (f(x_1) = f(x_2) \implies x_1 = x_2).$$

   Negate this statement, meaning find a statement that is logically equivalent to

   $$\neg[\forall x_1, x_2 \in X,\ (f(x_1) = f(x_2) \implies x_1 = x_2)].$$

   Write your answer without using the symbol $\neg$.

   Solutions:

   (a) Consider the following truth table.

P	Q	$\neg Q$	$P \implies Q$	$\neg(P \implies Q)$	$P \wedge \neg Q$
T	T	F	T	F	F
T	F	T	F	T	T
F	T	F	T	F	F
F	F	T	T	F	F

   So for any truth values of P, Q, R, the truth values of $\neg(P \implies Q)$ and of $P \wedge \neg Q$ are the same, proving (b).

   (b) We have

$$\begin{aligned}
&\neg[\forall x_1, x_2 \in X,\ (f(x_1) = f(x_2) \implies x_1 = x_2)] \\
&\quad\iff [\exists x_1, x_2 \in X,\ \neg(f(x_1) = f(x_2) \implies x_1 = x_2)] \\
&\quad\iff [\exists x_1, x_2 \in X, (f(x_1) = f(x_2) \wedge x_1 \neq x_2)].
\end{aligned}$$

2. Define a map $f : \mathbb{Z}_+ \to \mathbb{Z}_+$ that is surjective but not injective, and demonstrate that this map is surjective but not injective.

   Solution:

   [There are many correct answers. One option is as follows:] Define $f : \mathbb{Z}_+ \to \mathbb{Z}_+$ by $f(1) = 1$, and for $x \in \mathbb{Z}_+$ with $x > 1$, $f(x) = x - 1$.

   To see that f is surjective, take [arbitrary] $y \in \mathbb{Z}_+$. Then $y+1 > 1$ and $f(y + 1) = (y + 1) - 1 = y$. Hence f is surjective.

   To see that f is not injective, note that $1, 2 \in \mathbb{Z}_+$ with $f(1) = f(2) \wedge 1 \neq 2$. So by part (b) of question 1, f is not injective.

3. Suppose A is a finite set with $|A| = n$ for some $n \in \mathbb{Z}$ with $n \geq 0$. Recall that $\mathcal{P}(A)$ denotes the poser set of A, meaning that

   $$\mathcal{P}(A) = \{C :\ C \subseteq A\ \}.$$

Use induction to show that $|\mathcal{P}(A)| = 2^n$. (Suggestion: For the induction step, suppose A is a nonempty set, and fix an element $u \in A$. Let $B = A \setminus \{u\}$. Argue that there is a bijection between $\{C : C \subseteq B\}$ and $\{D : D \subseteq A, u \in D\}$. Then show that this means that $\mathcal{P}(A) = 2\mathcal{P}(B)$, and use your induction hypothesis to conclude that $|\mathcal{P}(A)| = 2^{k+1}$ where $|A| = k + 1$.)

Solution: We argue by induction on n.

[Base case.] Suppose $|A| = 0$; so $A = \emptyset$ and $\mathcal{P}(A) = \{\emptyset\}$. Hence $|\mathcal{P}(A)| = 1 = 2^0$.

[Induction step.] Suppose that $k \in \mathbb{Z}$ with $k \geq 0$ and for a set B with $|B| = k$, $\mathcal{P}(B) = 2^k$. Suppose A is a set with $|A| = k+1$. Since $|A| \geq 1$ and hence $A \neq \emptyset$, we can choose $u \in A$; we fix this choice of u. Let $B = A \setminus \{u\}$. So $|B| = k$. Let

$$X = \{C : C \subseteq B\},\ Y = \{D : D \subseteq A,\ u \in D\}.$$

Define $f : X \to Y$ by $f(C) = C \cup \{u\}$. We claim that f is bijective. To see that f is surjective, choose $D \in Y$. Thus $D \subseteq A$ and $u \in D$. Let $C = D \setminus \{u\}$. Thus $C \subseteq A \setminus \{u\} = B$, and $D = C \cup \{u\} = f(C)$. Hence f is surjective. To see f is injective, suppose $C_1, C_2 \in X$ with $C_1 \neq C_2$. Thus $C_1, C_2 \subseteq B$, and either there is an element $b \in C_1$ with $b \notin C_2$, or there is an element $b \in C_2$ with $b \notin C_1$; without loss of generality, suppose $b \in C_1$ with $b \notin C_2$. Then $b \in f(C_1)$, and $b \notin f(C_2)$, so $f(C_1) \neq f(C_2)$. Hence f is injective. Therefore f is bijective, so $|X| = |Y|$. We also have $X \cup Y = \mathcal{P}(A)$ [since every subset of A either contains u, and hence is in Y, or does not contain u, and hence is in X]. Also, $X \cap Y = \emptyset$, since all the elements of X do not contain u, and all the elements of Y do contain u. [So $\{X, Y\}$ is a partition of $\mathcal{P}(A)$.] Hence $|\mathcal{P}(A)| = |X| + |Y| = 2|X|$ [as $|X| = |Y|$]. Also, $X = \mathcal{P}(B)$, so $|X| = |\mathcal{P}(B)|$. Thus $|\mathcal{P}(A)| = 2|\mathcal{P}(B)|$. Since $|B| = k$, the induction hypothesis tells us that $|\mathcal{P}(B)| = 2^k$, so $|\mathcal{P}(A)| = 2 \cdot 2^k = 2^{k+1}$.

So by the principle of mathematical induction, $|\mathcal{P}(A)| = 2^n$ for any finite set $|A|$ with $|A| = n$.