Discrete Math Problem Set 7

Will Krzastek

March 28th, 2024

1. Let X be a set. Show that $(\forall Y \in \mathbb{P}(X))(|Y| \leq |X|)$.
   Proof. Let X, Y be sets. Assume $Y \in \mathbb{P}(X)$. Because $\mathbb{P}(X)$ is the set of all subsets of X, and $Y \in \mathbb{P}(X)$, we then know $Y \subseteq X$. By the definition of a subset, we know $\forall b(b \in Y \Rightarrow b \in X)$.
   Recall that $|Y| \leq |X| \Leftrightarrow \exists f(f : Y \hookrightarrow X)$ by the definition of *equinumerosity*.
   Consider an f where $f : Y \to X$. Also, let $a, b \in Y$.
   Now let f be defined as $f(a) = a$. Because $Y \subseteq X$, we know $\forall a(a \in Y \Rightarrow a \in X)$.
   Recall that the definition of injectivity is $\exists f(f(a) = f(b) \Rightarrow a = b)$. To prove f is injective, assume $f(a) = f(b)$. Then by the definition of f, we know that $f(a) = a$ and $f(b) = b$. So, we have $f(a) = a$ and $f(b) = b$ by the definition of f.
   Since $f(a) = f(b)$, we know $a = b$.
   So, by the definition of *injectivity*, we know that f is injective.
   So, $|Y| \leq |X|$ by the definition of injectivity.

   ■

2. Show that $\forall X \forall Y(|X| \leq |Y| \Rightarrow \exists Z(Z \subseteq Y \land |X| = |Z|))$.
   Proof. Let X, Y, Z be sets. Assume $|X| \leq |Y|$. By definition, this means that $\exists f(f : X \hookrightarrow Y)$, which means there exists an injective function f from X to Y.
   Now, let $Z := \{f(a) \mid a \in X\}$. Because Y is the codomain of f, Z only contains elements of Y, so $Z \subseteq Y$.
   Now, let $g : X \to Z$ be the function $g(a) := f(a)$ where $a \in X$.
   Now, we want to show that $|X| = |Z|$, so we want to show that g is a bijection.
   To do so, we will independently show that g is both an injection and a surjection.
   First, we will show g is injective. Recall the definition of injectivity: $(\forall a, b \in X)(g(a) = g(b) \Rightarrow a = b)$. Assume $g(a) = g(b)$. By the definition of g, we then know that $f(a) = f(b)$. So, we have $a = b$ because f is injective. So, g is injective.
   Now, we want to show that g is surjective. Let h be an element of Z. Recall the definition of surjectivity: $(\forall h \in Z)(\exists x \in X)(g(x) = h)$. $h = f(a)$ where $a \in X$. Thus, $g(a) = f(a)$ because we know this is true $\forall h \in Z$. So, $g(a) = h$

by definition. Thus, g is surjective.

Because g is injective *and* surjective, g is by definition bijective. Thus, we obtain $|X| = |Z|$ by definition. Therefore, $|X| \leq |Y| \Rightarrow \exists Z(Z \subseteq Y \wedge |X| = |Z|)$.

$\blacksquare$

3. Let X, Y, Z be sets and consider $f : X \to Y$ and $g : Y \to Z$. We define the *composition* of f with g to be the function $g \circ f : X \to Z$ given by $(g \circ f)(x) := g(f(x))$ for all $x \in X$.

   (a) Show that, if f and g are both injections, then $g \circ f$ is injective.

   Proof. Let X, Y, Z be sets. Let $f : X \to Y$ and $g : Y \to Z$. Recall $(\forall x \in X)(g \circ f(x) := g(f(x)))$. Also recall the definition of injectivity: $(\forall a, b \in X)(g(f(a)) = g(f(b)) \Rightarrow a = b)$. Assume f and g are both injections. Also assume $g(f(a)) = g(f(b))$.

   Because g is injective, we know $f(a) = f(b)$.

   Because f is injective, we then know $a = b$.

   So, if g and f are injections, $g \circ f$ is injective.

   $\blacksquare$

   (b) Show that, if f and g are both surjections, then $g \circ f$ is surjective.

   Proof. Let X, Y, Z be sets. Let $f : X \to Y$ and $g : Y \to Z$. Recall the definition of surjectivity: $(\forall a \in A)(\exists b \in B)(f(b) = a)$.

   Assume g and f are both surjections.

   Because f is surjective, $(\forall y \in Y)(\exists x \in X)(f(x) = y)$.

   Because g is surjective, $(\forall z \in Z)(\exists y \in Y)(g(y) = z)$.

   Thus, $g(f(x)) = g(y) = z$ for arbitrary values of y and z.

   So, if g and f are surjections, then $g \circ f$ is a surjection.

   $\blacksquare$

   (c) Show that, if f and g are both bijections, then $g \circ f$ is bijective.

   Proof. Let X, Y, Z be sets. Let $f : X \to Y$ and $g : Y \to Z$. Recall the definition of bijectivity is possessing sujrectivity and injectivity.

   Assume g and f are bijections.

   So, g and f are both injective and surjective by definition.

   In *3(a)*, we proved $g \circ f$ is injective when g and f are injective.

   In *3(b)*, we proved $g \circ f$ is surjective when g and f are surjective.

   Because $g \circ f$ is injective *and* surjective when g and f are bijections, $g \circ f$ is bijective.

   $\blacksquare$

4. For this problem, let X and Y be nonempty sets and let $f : X \to Y$.

(a) If f is injective, show there exists $g : Y \to X$ where $g \circ f = id_X$.

Proof. Let X, Y be sets. Let $f : X \to Y$. Assume f is injective. We want to show $(\exists g : Y \to X)(g \circ f = id_X)$. Because X is nonempty, an arbitrary element $x \in X$ exists. Remember $id_X := g(f(x)) = x$.

Because f is injective, we know $f(x) = y$ for some distinct $y \in Y$, where x is the only input mapped to y. Now, consider $g(y) := x$ where y is the same y as the output of $f(x)$. Here, we see that $g(f(x)) = g(y) = x$. When $f(x) = y$, this would mean that $g(f(x)) = g(y) =$ x. Therefore, $g \circ f = x$, which means that $(\exists g : Y \to X)(g \circ f = id_X)$.

■

(b) If f is surjective, show there exists $g : Y \to X$ where $f \circ g = id_Y$.

Proof. Let X, Y be sets. Let $f : X \to Y$. Assume f is surjective. We want to show $(\exists g : Y \to X)(f \circ g = id_Y)$. Because Y is nonempty, an arbitrary $y \in Y$ exists. Remember $id_Y := f(g(x)) = y$.

Because f is surjective, we know that $f(x) = y$ for some $x \in X$. Now, consider $g(y) := x$ where x is the same x that is input into f. This means that $f(g(y)) = f(x) = y$. Therefore, $f \circ g = y$, which means that $(\exists g : Y \to X)(f \circ g = id_Y)$.

■

(c) If f is a bijection, then show there exists a function $g : Y \to X$ such that $g \circ f = id_X$ and $f \circ g = id_Y$.

Proof. Let X, Y be sets. Let $f : X \to Y$. Assume f is a bijection. By definition, this means that f is both surjective and injective.

In *4(a)*, we proved that when f is an injection, there exists a function $g : Y \to X$ where $g \circ f = id_X$ and we defined this function as $g := x$.

In *4(b)*, we proved that when f is a surjection, there exists a function $g : Y \to X$ where $f \circ g = id_Y$ and we defined this function as $g := x$.

Therefore, when f is injective and surjective, the function $g := x$ exists where $g \circ f = id_X$ and $f \circ g = id_Y$.

■

5. *Euler's totient function* is the function: $\varphi_e : \mathbb{N} \to \mathbb{N}$ that counts how many positive integers are *coprime* with each $n \in \mathbb{N}$, defined below:

$$\varphi_e(n) := |\{z \in \mathbb{N} \mid 1 \leq z \leq n \wedge gcd(z, n) = 1\}|$$

(a) If $p, k, m \in \mathbb{N}_+$ are *positive* naturals with p prime and $m \leq p^k$, then prove that $\gcd(p^k, m) \neq 1 \Leftrightarrow p \mid m$.

Proof. Let $p, k, m \in \mathbb{N}_+$ and assume p is prime and $m \leq p^k$. We will prove this by cases.

Case 1: $\gcd(p^k, m) \neq 1 \Rightarrow p \mid m$.

Assume $\gcd(p^k, m) \neq 1$. This means that p^k and m share a common divisor. Recall that $p^k := p * p$ (k many times). Thus, p is the only prime factor of p^k because of the unique prime factorization of p^k and the FTA. Because they share a common divisor and p is the only prime divisor of p^k, p must divide m. Therefore, $p \mid m$.

Case 2: $p \mid m \Rightarrow gcd(p^k, m) \neq 1$.

Assume $p \mid m$. So, p is a divisor of m. Remember, p is the only prime divisor of p^k as shown in Case 1. As such p is a divisor of p^k and m, so $\gcd(p^k, m) \geq p$, and p is prime so $p > 1$. Therefore, $\gcd(p^k, m) \neq 1$.

Thus, both cases hold so $\gcd(p^k, m) \neq 1 \Leftrightarrow p \mid m$.

■

(b) If p is prime, then prove that $\varphi_e(p) = p - 1$.

Proof. Let $p \in \mathbb{N}_+$ and assume p is prime.

We then define $\varphi_e(p) := |\{z \in \mathbb{N} \mid 1 \leq z \leq p \wedge gcd(z, p) = 1\}|$.

We want to now show that $\varphi_e(p) = p - 1$.

The set of all numbers that satisfies $1 \leq z \leq p$ is $[p+1]$, but 0 is excluded, so its cardinality will be p. Because p is prime, the set of all numbers that satisfies $gcd(z, p) = 1$ while being less than or equal to p is every number strictly less than p. So, $\varphi_e(p)$ will be $[p]$, but we still must exclude 0. So, $\varphi_e(p) = |[p] - 1|$. A set with p elements has cardinality p, so we equivalently get $\varphi_e(p) = p - 1$.

■

(c) If p is prime and $k \in \mathbb{N}_+$, then prove that $\varphi_e(p^k) = p^k - p^{k-1}$.

Proof. Let $p, k \in \mathbb{N}_+$ and assume p is prime.

We then define $\varphi_e(p^k) := |\{z \in \mathbb{N} \mid 1 \leq z \leq p^k \wedge gcd(z, p^k) = 1\}|$.

We want to show that $\varphi_e(p^k) = p^k - p^{k-1}$.

The set of all numbers that satisfies $1 \leq z \leq p^k$ is $[p^k+1]$, but 0 is excluded, so its cardinality is p^k.

Because p is prime and p is the only prime divisor of p^k as we proved in $5(a)$, z cannot equal a multiple of p, or else they would share a common divisor and $\gcd(z, p^k) \neq 1$. So, the set of all numbers that satisfies $1 \leq z \leq p^k \wedge gcd(z, p^k) = 1$ is p^k minus the set of all multiples of p up to p^k. Let $M :=$ the set of all multiples of p up to p^k excluding p^k. We can find $|M|$ by looking at the number of elements of the original set (p^k), and dividing it by the difference between the first element (0) and p, which is just p. So, we see that $|M| = p^k/p$. By basic arithmetic, we know $p^k/p = p^{k-1}$. Thus, $|M| = p^{k-1}$. So, $\varphi_e(p^k) = p^k - |M|$, which is equal to $p^k - p^{k-1}$. Therefore, $\varphi_e(p^k) = p^k - p^{k-1}$.

$\blacksquare$