Solution Set 7

Discrete Structures

17^{th} day of April of the year of our Lord 2026

1. a. We will prove $\forall X \forall Y(X \subseteq Y \;\Rightarrow\; |X| \leqslant |Y|)$.

   Proof. Let X and Y be sets and assume $X \subseteq Y$. Consider the function $f : X \to Y$ given by $f(x) := x$ for each $x \in X$. We will prove this function is injective.

   Let $a, b \in X$ and suppose $f(a) = f(b)$. Then, since $f(a) = a$ and $f(b) = b$ by the definition of f, we have that $a = b$. Thus, f is injective, implying $|X| \leqslant |Y|$.

   QED

   b. We will prove that every injection between nonempty sets is monomorphic.

   Proof. Let X and Y be sets such that $X \neq \varnothing$ and $Y \neq \varnothing$, and let $f : X \to Y$ be an arbitrary injection. Since $X \neq \varnothing$, we know there exists some $x_0 \in X$. Consider now the function $g : Y \to X$ defined, for each $y \in Y$, as follows.

   $$g(y) := \begin{cases} x & \text{if } x \in X \text{ such that } f(x) = y \\ x_0 & \text{if } (\forall x \in X)(f(x) \neq y) \end{cases}$$

   We know that g is a function because the fact that f is injective guarantees that every element of Y has *at most* one preimage.[1] We will now show $g \circ f = \mathtt{id}_X$.

   [1]This addresses *uniqueness* of the output of g; *existence* is guaranteed by the structure of the definition, since the two cases are mutually exclusive and exhaustive.

   Let $x \in X$. Notice that there exists $y \in Y$ such that $f(x) = y$ because f is a function. The definition of g then implies $g(y) = x$. This permits the following observation.

   $$(g \circ f)(x) = g(f(x)) = g(y) = x$$

   Since we can see that $g \circ f$ and $\mathtt{id}_X$ have the same domain, same codomain, and $(g \circ f)(x) = \mathtt{id}_X(x)$ for every $x \in X$, we conclude that $g \circ f = \mathtt{id}_X$.

   QED

2. a. We will prove $\forall A \forall B \forall C((|A| \leqslant |B| \wedge |B| \leqslant |C|) \;\Rightarrow\; |A| \leqslant |C|)$.

   Proof. Let A, B, and C be sets such that $|A| \leqslant |B|$ and $|B| \leqslant |C|$. This means there exist two injective functions $\alpha : A \hookrightarrow B$ and $\beta : B \hookrightarrow C$ by definition. We will now prove that $\beta \circ \alpha : A \to C$ is an injection.

   Let $x_1, x_2 \in A$ and suppose $(\beta \circ \alpha)(x_1) = (\beta \circ \alpha)(x_2)$. We now must observe.

   $$\begin{aligned} (\beta \circ \alpha)(x_1) = (\beta \circ \alpha)(x_2) \quad &\Rightarrow \quad \beta(\alpha(x_1)) = \beta(\alpha(x_2)) && \text{by definition} \\ &\Rightarrow \quad \alpha(x_1) = \alpha(x_2) && \text{because } \beta \text{ is injective} \\ &\Rightarrow \quad x_1 = x_2 && \text{because } \alpha \text{ is injective} \end{aligned}$$

   Therefore, $x_1 = x_2$, demonstrating that $\beta \circ \alpha$ is injective, meaning $|A| \leqslant |C|$.

   QED

   b. We will prove $\forall A \forall B \forall C((|A| \geqslant |B| \wedge |B| \geqslant |C|) \;\Rightarrow\; |A| \geqslant |C|)$.

   Proof. Let A, B, and C be sets such that $|A| \geqslant |B|$ and $|B| \geqslant |C|$. This means there exist two surjective functions $\alpha : A \twoheadrightarrow B$ and $\beta : B \twoheadrightarrow C$ by definition. We will now prove that $\beta \circ \alpha : A \to C$ is a surjection.

Let $c \in C$. Since β is a surjection, we know there exists $b \in B$ such that $\beta(b) = c$. Now, since α is surjective, we also know there is some $a \in A$ such that $\alpha(a) = b$. We can now observe the sequence of equalities below, all following by definition.

$$(\beta \circ \alpha)(a) = \beta(\alpha(a)) = \beta(b) = c$$

Since we found element of A—namely a—such that $(\beta \circ \alpha)(a) = c$, and since c was an arbitrary element of C, we now know $\beta \circ \alpha$ is surjective. Thus, we conclude that $|A| \geqslant |C|$ by definition.

QED

c. We will prove $\forall A \forall B \forall C((|A| = |B| \wedge |B| = |C|) \implies |A| = |C|)$.

Proof. Let A, B, and C be sets such that $|A| = |B|$ and $|B| = |C|$. This means there exist two bijective functions $\alpha : A \to B$ and $\beta : B \to C$ by definition. In particular, this means α and β are both injective and both surjective.

In 2.a., we proved that the composition of two injections is injective, so $\beta \circ \alpha$ is an injection. Similarly, in 2.b., we proved that the composition of two surjections is surjective, implying $\beta \circ \alpha$ is surjective. This means that $\beta \circ \alpha$ is a bijection, allowing us to conclude $|A| = |C|$ by definition.

QED

3. We will prove $|A \cup B| = |A| + |B|$ for any pair of disjoint finite sets A and B.

Proof. Let A and B be finite sets such that $A \cap B = \varnothing$. Since A and B are finite, there exist $n_A, n_B \in \mathbb{N}$ such that $|A| = |n_A|$ and $|B| = |n_B|$. This, in turn, implies there exist functions $f_A : A \to n_A$ and $f_B : B \to n_B$ such that f_A and f_B are both bijections. Consider the function $g : A \cup B \to n_A + n_B$ given below for all $x \in A \cup B$.

$$g(x) := \begin{cases} f_A(x) & \text{if } x \in A \\ f_B(x) + n_A & \text{if } x \in B \end{cases}$$

The fact that $A \cap B = \varnothing$ ensures that g is well-defined. We will prove g is bijective.

Injectivity:
Let $x_1, x_2 \in A \cup B$ and suppose $g(x_1) = g(x_2)$. We take two cases.

Case 1:
Suppose $x_1 \in A$, so $0 \leqslant g(x_1) = f_A(x_1) = g(x_2) < n_A$. Towards a contradiction, assume $x_2 \notin A$. Since $x_2 \in A \cup B$ and $A \cap B = \varnothing$, we have $x_2 \in B$. However, the definition of g then implies $g(x_2) = f_B(x_2) + n_A \geqslant n_A$, which contradicts our earlier assumption that $g(x_2) < n_A$. $\lightning$ Therefore, $x_2 \in A$. We then know that $f_A(x_1) = g(x_1) = g(x_2) = f_A(x_2)$. Since f_A is injective, we conclude with the observation that $x_1 = x_2$.

Case 2:
Suppose $x_1 \notin A$, so that $x_1 \in B$ due to the fact that $A \cap B = \varnothing$. This implies $n_A \leqslant g(x_1) = f_B(x_1) = g(x_2) < n_A + n_B$. Towards a contradiction, assume $x_2 \notin B$, so that $x_2 \in A$. From this, $g(x_2) = f_A(x_2) < n_A$, contradicting our earlier assumption that $n_A \leqslant g(x_2)$. $\lightning$ Therefore, $x_2 \in B$. We then know that $f_B(x_1) + n_A = g(x_1) = g(x_2) = f_B(x_2)$, so that $f_B(x_1) = f_B(x_2)$. Since f_B is injective, this implies $x_1 = x_2$ as desired.

Therefore, g is injective.

Surjectivity:
Let $y \in n_A + n_B$. We take two cases based on which *"half"* of $n_A + n_B$ contains y.

Case 1:
Suppose $0 \leqslant y < n_A$. Then, $y \in n_A$, so we know there exists some $x \in A$ such that $f_A(x) = y$ by the fact that f_A is surjective. We can then simply verify that $x \in A \cup B$ and $g(x) = f_A(x) = y$ by definition of g.

Case 2:
Suppose $n_A \leqslant y < n_A + n_B$. We then know $0 \leqslant y - n_A < n_B$, from which we can derive that there exists $x \in B$ such that $f_B(x) = y - n_A$ from the fact that f_B is surjective. We then have $g(x) = f_{B(x)} + n_A = (y - n_A) + n_A = y$.

Therefore, g must be surjective.

From this analysis, we can clearly see that g is a bijection. We therefore conclude that $|A \cup B| = |n_A + n_B|$ as was requested of us.

QED

4. We will prove $(\forall n \in \mathbb{N})(\forall X(|X| = |n| \Rightarrow |\mathbb{P}(X)| = |2^n|))$.

Proof. We perform weak induction on the cardinality of the finite set in question.

Basis Step:
Let X be a set such that $|X| = |0|$, so that there exists a bijection $\varphi : X \to \varnothing$ by definition. The fact that φ is a function implies $\forall x(x \in X \Rightarrow \varphi(x) \in \varnothing)$, showing us that X must be empty.[2] Recalling $\mathbb{P}(X) = \mathbb{P}(\varnothing) = \{\varnothing\} = \{0\} = 1$, we conclude $|\mathbb{P}(X)| = |1| = 1 = 2^0$ since every set is in bijection with itself.[3]

Inductive Step:
Let $k \in \mathbb{N}$ and suppose $\forall X\big(|X| = |k| \Rightarrow |\mathbb{P}(X)| = |2^k|\big)$.[4]
Now, let X be a set and assume $|X| = |k+1| = k+1$. Since $k \in \mathbb{N}$, we know that $k \geqslant 0$, implying $k + 1 \geqslant 1$, which tells X is nonempty.[5] Therefore, there exists some $\hat{x} \in X$, and we can observe that $|X \setminus \{\hat{x}\}| = |X| - 1 = (k+1) - 1 = k$. By the *inductive hypothesis*, we then know $|\mathbb{P}(X \setminus \{\hat{x}\})| = |2^k|$, which means there exists a bijection $\rho : \mathbb{P}(X \setminus \{\hat{x}\}) \to \left\{z \in \mathbb{N} \,\middle|\, z < 2^k\right\}$ by definition. We now construct a new function $\lambda : \mathbb{P}(X) \to \left\{z \in \mathbb{N} \,\middle|\, z < 2^{k+1}\right\}$ as follows. For any $W \subseteq X$,

$$\lambda(W) := \begin{cases} \rho(W) & \text{if } \hat{x} \notin W \\ \rho(W \setminus \{\hat{x}\}) + 2^k & \text{if } \hat{x} \in W \end{cases}$$

Let's prove λ is a bijection.

Injectivity:
Let $A, B \in \mathbb{P}(X)$ and assume $\lambda(A) = \lambda(B)$. We take two cases.

Case 1:
Suppose $\hat{x} \notin A$. Then, $\lambda(A) = \rho(A)$, so $0 \leqslant \lambda(A) = \lambda(B) < 2^k$. Towards a contradiction, suppose $\hat{x} \in B$; by definition, this would imply $\lambda(B) = \rho(B \setminus \{\hat{x}\}) + 2^k \geqslant 2^k$, contradicting our earlier observation. ↯
Thus, $\hat{x} \notin B$, so that $\rho(A) = \lambda(A) = \lambda(B) = \rho(B)$. Since ρ was injective, we conclude that $A = B$.

[2] Otherwise, we would have an element $x \in X$ such that $\varphi(x) \in \varnothing$, contradicting the fact that $\forall z(z \notin \varnothing)$.

[3] We proved $\forall x(|x| = |x|)$; the bijection in question is $\mathtt{id}_x$.

[4] *inductive hypothesis*

[5] If $X = \varnothing$, then $|X| = |\varnothing| = 0$, contradicting the fact that $|X| = k + 1 \geqslant 1$.

Case 2:
Suppose $\hat{x} \in A$. Then, $\lambda(A) = \rho(A \setminus \{\hat{x}\}) + 2^k$. Since $\rho(A \setminus \{\hat{x}\}) \in \mathbb{N}$, we can observe $2^k = 0 + 2^k \leqslant \rho(A \setminus \{\hat{x}\}) + 2^k = \lambda(A) = \lambda(B) < 2^{k+1}$. Towards a contradiction, supposing $\hat{x} \notin B$ implies $\lambda(B) = \rho(B) < 2^k$, which would contradict the observation we just made. $\lightning$ Thus, $\hat{x} \in B$. We therefore have $\rho(A \setminus \{\hat{x}\}) + 2^k = \lambda(A) = \lambda(B) = \rho(B \setminus \{\hat{x}\}) + 2^k$, from which we can derive $\rho(A \setminus \{\hat{x}\}) = \rho(B \setminus \{\hat{x}\})$. Since ρ is an injection, this tells us $A \setminus \{\hat{x}\} = B \setminus \{\hat{x}\}$, letting us conclude $A = B$.[6]

[6] This follows directly from the *axiom of extensionality* if we recall $\hat{x} \notin A$ and $\hat{x} \notin B$.

Surjectivity:
Let $n \in \left\{z \in \mathbb{N} \,\middle|\, z < 2^{k+1}\right\}$. We take two cases based on where n lies.

Case 1:
Suppose $0 \leqslant n < 2^k$. This puts n squarely within the codomain of ρ, which means there exists some $W \in \mathbb{P}(X \setminus \{\hat{x}\})$ such that $\rho(W) = n$ because of the fact that ρ is a surjection. Now, notice $W \subseteq X \setminus \{\hat{x}\}$ and $X \setminus \{\hat{x}\} \subseteq X$, so $W \subseteq X$, putting W in the domain of λ. Since $\hat{x} \notin W$, we can apply the definition of λ to reveal $\lambda(W) = \rho(W) = n$.

Case 2:
Suppose $2^k \leqslant n < 2^{k+1}$. Then, $0 \leqslant n - 2^k < 2^{k+1} - 2^k = 2^{k(2-1)} = 2^k$, demonstrating to us that $n - 2^k$ is in the codomain of ρ. Again, since ρ is a surjection, this means there exists some $W \in \mathbb{P}(X \setminus \hat{x})$ such that $\rho(W) = n - 2^k$. By the same observation as in the previous case, we know $W \subseteq X$, and $\hat{x} \in X$, so it should be clear that $W \cup \{\hat{x}\} \subseteq X$. If we recall that $(W \cup \{\hat{x}\}) \setminus \{\hat{x}\} = W$, we can then observe the following.

$$
\begin{aligned}
\lambda(W \cup \{\hat{x}\}) &= \rho(W \cup \{\hat{x}\} \setminus \{\hat{x}\}) + 2^k \\
&= \rho(W) + 2^k \\
&= \left(n - 2^k\right) + 2^k \\
&= n
\end{aligned}
$$

Therefore, we have that λ is a bijection between $\mathbb{P}(X)$ and $\left\{z \in \mathbb{N} \,\middle|\, z < 2^{k+1}\right\}$. We thus conclude that $|\mathbb{P}(X)| = \left|2^{k+1}\right|$ as desired.

By the graces of the theorem of *weak induction*, we can finally admire the conclusion that $(\forall n \in \mathbb{N})(\forall X(|X| = |n| \implies |\mathbb{P}(X)| = |2^n|))$

QED