Solution Set 5

Discrete Structures

23[rd] day of March of the year of our Lord 2026

1. We will show $(\forall x \in \mathbb{N})\Big(\forall y\big(y \in x \implies \forall z(z \in y \implies z \in x)\big)\Big)$.

   Proof. We proceed by *weak induction*.

   Basis Step:
   Let y be a set, and suppose $y \in 0$, which means $y \in \varnothing$ by definition. Recall that $y \notin \varnothing$ because $\forall w(w \notin \varnothing)$. Therefore, we conclude $\forall z\big(z \in y \implies z \in 0\big)$ as desired by applying the *principle of explosion*.

   Inductive Step:
   Let $k \in \mathbb{N}$, and assume $\forall y\big(y \in k \implies \forall z(z \in y \implies z \in k)\big)$.[1] Now, let y be a set and suppose that $y \in \mathfrak{suc}(k)$, so that $y \in k \cup \{k\}$ by definition. This implies that $y \in k$ or $y \in \{k\}$, so we will take two cases.[2]

   Case 1:
   Suppose that $y \in k$. Let z be a set such that $z \in y$, and observe $z \in k$ by the *inductive hypothesis*. This implies $z \in k \vee z \in \{k\}$, showing us $z \in k \cup \{k\}$, from which we can conclude $z \in \mathfrak{suc}(k)$ by definition.

   Case 2:
   Suppose $y \in \{k\}$, so that $y = k$. Let z be a set and assume $z \in y$. Then, we have that $z \in k$ because $y = k$.[3] From this, we can see $z \in k \vee z \in \{k\}$, so that $z \in k \cup \{k\}$, implying that $z \in \mathfrak{suc}(k)$ by definition.

   Thus, we have $\forall z\big(z \in y \implies z \in \mathfrak{suc}(k)\big)$ as desired.

   Therefore, we can conclude $(\forall x \in \mathbb{N})\Big(\forall y\big(y \in x \implies \forall z(z \in y \implies z \in x)\big)\Big)$.

   QED

[1] *inductive hypothesis*

[2] In either case, we now want $\forall z\big(z \in y \implies z \in \mathfrak{suc}(k)\big)$ to be shown.

[3] By the *axiom of extensionality*.

2. We will work up to a proof that addition on $\mathbb{N}$ is commutative.

   a. We will show $(\forall x, y \in \mathbb{N})\big(\mathfrak{suc}(x + y) = \mathfrak{suc}(x) + y\big)$.

   Proof. Let $x \in \mathbb{N}$.
   We will prove $(\forall y \in \mathbb{N})\big(\mathfrak{suc}(x + y) = \mathfrak{suc}(x) + y\big)$ by *weak induction*.

   Basis Step:
   Observe $\mathfrak{suc}(x + 0) = \mathfrak{suc}(x) = \mathfrak{suc}(x) + 0$ by the definition of addition.

   Inductive Step:
   Let $k \in \mathbb{N}$, and assume that $\mathfrak{suc}(x + k) = \mathfrak{suc}(x) + k$.[4] Observe the following.

$$\begin{aligned}
\mathfrak{suc}\big(x + \mathfrak{suc}(k)\big) &= \mathfrak{suc}\big(\mathfrak{suc}(x + k)\big) && \text{by definition of addition} \\
&= \mathfrak{suc}\big(\mathfrak{suc}(x) + k\big) && \text{by the \textit{inductive hypothesis}} \\
&= \mathfrak{suc}(x) + \mathfrak{suc}(k) && \text{by definition of addition}
\end{aligned}$$

   Thus, we have $\mathfrak{suc}\big(x + \mathfrak{suc}(k)\big) = \mathfrak{suc}(x) + \mathfrak{suc}(k)$ as desired.

   Therefore, we can conclude $(\forall y \in \mathbb{N})\big(\mathfrak{suc}(x + y) = \mathfrak{suc}(x) + y\big)$.

   QED

[4] *inductive hypothesis*

b. We will show $(\forall x, y \in \mathbb{N})(x + y = y + x)$.

Proof. Let $x \in \mathbb{N}$. We will prove $(\forall y \in \mathbb{N})(x + y = y + x)$ by *weak induction.*

Basis Step:
Observe that $x + 0 = x$ by the definition of addition. Further, $x = 0 + x$ because $(\forall z \in \mathbb{N})(z = 0 + z)$. Thus, $x + 0 = 0 + x$.

Inductive Step:
Let $k \in \mathbb{N}$, and assume that $x + k = k + x$.[5] Now, observe the following.

[5]*inductive hypothesis*

$$\begin{aligned} x + \mathfrak{suc}(k) &= \mathfrak{suc}(x + k) && \text{by definition of addition} \\ &= \mathfrak{suc}(k + x) && \text{by the } \textit{inductive hypothesis} \\ &= \mathfrak{suc}(k) + x && \text{by } \textit{problem 2.a.} \end{aligned}$$

Thus, we have that $x + \mathfrak{suc}(k) = \mathfrak{suc}(k) + x$ as needed.

Therefore, we can conclude $(\forall y \in \mathbb{N})(x + y = y + x)$.

QED

3. We will show $(\forall x, y \in \mathbb{N})\big(x < y \Rightarrow (\exists n \in \mathbb{N})(x + n = y)\big)$.

Proof. Let $x \in \mathbb{N}$.
We will show $(\forall y \in \mathbb{N})\big(x < y \Rightarrow (\exists n \in \mathbb{N})(x + n = y)\big)$ by *weak induction.*

Basis Step:
Suppose that $x < 0$, so that $x < \varnothing$, which implies $x \in \varnothing$ by definition. Recall that $x \notin \varnothing$ because $(\forall w \in \varnothing)(w \notin \varnothing)$. We then deduce $(\exists n \in \mathbb{N})(x + n = 0)$ by the *principle of explosion.*

Inductive Step:
Let $k \in \mathbb{N}$, and suppose that $x < k \Rightarrow (\exists n \in \mathbb{N})(x + n = y)$.[6] Now, assume that $x < \mathfrak{suc}(k)$ and observe the implications that follow from this assumption.

[6]*inductive hypothesis*

$$\begin{aligned} x < \mathfrak{suc}(k) &\Rightarrow x \in \mathfrak{suc}(k) && \text{by definition of } < \text{ on } \mathbb{N} \\ &\Rightarrow x \in k \cup \{k\} && \text{by definition of } \mathfrak{suc}(\square) \\ &\Rightarrow (x \in k) \vee \big(x \in \{k\}\big) && \text{by definition of } \cup \\ &\Rightarrow (x \in k) \vee (x = k) && \text{by definition of set roster notation} \\ &\Rightarrow (x < k) \vee (x = k) && \text{by definition of } < \text{ on } \mathbb{N} \end{aligned}$$

We can now take two cases.

Case 1:
Suppose $x < k$. Then, we can apply the *inductive hypothesis* to see that there exists $m \in \mathbb{N}$ such that $x + m = k$. We can now sit back and watch.

$$\begin{aligned} x + m = k &\Rightarrow \mathfrak{suc}(x + m) = \mathfrak{suc}(k) \\ &\Rightarrow (x + m) + 1 = \mathfrak{suc}(k) && \text{since } (\forall w \in \mathbb{N})\big(\mathfrak{suc}(w) = w + 1\big) \\ &\Rightarrow x + (m + 1) = \mathfrak{suc}(k) && \text{by associativity of addition} \end{aligned}$$

Since $m \in \mathbb{N}$, we know that $m + 1 \in \mathbb{N}$. Thus, $(\exists n \in \mathbb{N})\big(x + n = \mathfrak{suc}(k)\big)$.

Case 2:
Suppose $x = k$, so that $x + 1 = k + 1$. Recalling that $\mathfrak{suc}(k) = k + 1$, it should then be clear that $x + 1 = \mathfrak{suc}(k)$. If we then notice that $1 \in \mathbb{N}$, we obtain $(\exists n \in \mathbb{N})\big(x + n = \mathfrak{suc}(k)\big)$ as we had hoped.

In either case, we have $(\exists n \in \mathbb{N})\big(x + n = \mathfrak{suc}(k)\big)$.

Therefore, we can conclude that $(\forall y \in \mathbb{N})\big(x < y \Rightarrow (\exists n \in \mathbb{N})(x + n = y)\big)$.

QED

4. We will prove $(\forall x, y, z \in \mathbb{N})\big(x \cdot (y + z) = (x \cdot y) + (x \cdot z)\big)$.

Proof. Let $x \in \mathbb{N}$ and $y \in \mathbb{N}$.
We will show that $(\forall z \in \mathbb{N})\big(x \cdot (y + z) = (x \cdot y) + (x \cdot z)\big)$ by *weak induction.*

Basis Step:
Observe the following.

$$\begin{aligned} x \cdot (y + 0) &= x \cdot y && \text{by definition of addition} \\ &= (x \cdot y) + 0 && \text{by definition of addition} \\ &= (x \cdot y) + (x \cdot 0) && \text{by definition of multiplication} \end{aligned}$$

Inductive Step:
Let $k \in \mathbb{N}$, and assume $x \cdot (y + k) = (x \cdot y) + (x \cdot k)$.[7] We can now observe.

[7] *inductive hypothesis*

$$\begin{aligned} x \cdot \big(y + \mathfrak{suc}(k)\big) &= x \cdot \mathfrak{suc}(y + k) && \text{by definition of addition} \\ &= \big(x \cdot (y + k)\big) + x && \text{by definition of multiplication} \\ &= \big((x \cdot y) + (x \cdot k)\big) + x && \text{by the \textit{inductive hypothesis}} \\ &= (x \cdot y) + \big((x \cdot k) + x\big) && \text{by associativity of addition} \\ &= (x \cdot y) + \big(x \cdot \mathfrak{suc}(k)\big) && \text{by definition of multiplication} \end{aligned}$$

Thus, we have that $x \cdot \big(y + \mathfrak{suc}(k)\big) = (x \cdot y) + \big(x \cdot \mathfrak{suc}(k)\big)$ as required.

Therefore, we can conclude that $(\forall z \in \mathbb{N})\big(x \cdot (y + z) = (x \cdot y) + (x \cdot z)\big)$.

QED

5. We will show that $(\forall n \in \mathbb{N})\big(1 + \sum_{i=0}^{n} 2^i = 2^{n+1}\big)$.

Proof. We proceed by *weak induction.*

Basis Step:
The sequence of equalities below must follow.

$$\begin{aligned} 1 + \sum_{i=0}^{0} 2^i &= 1 + 2^0 && \text{by definition of } \sum \\ &= 1 + 1 && \text{by definition of exponentiation} \end{aligned}$$

On the other hand, we can not refute the following sequence of equalities.

$$\begin{aligned}
2^{0+1} &= 2^1 && \text{because } (\forall w \in \mathbb{N})(0 + w = w) \\
&= 2^{\mathfrak{suc}(0)} && \text{by definition of 1} \\
&= 2^0 \cdot 2 && \text{by definition of exponentiation} \\
&= 1 \cdot 2 && \text{by definition of exponentiation} \\
&= 1 \cdot \mathfrak{suc}(1) && \text{by definition of 2} \\
&= (1 \cdot 1) + 1 && \text{by definition of multiplication} \\
&= \big(1 \cdot \mathfrak{suc}(0)\big) + 1 && \text{by definition of 1} \\
&= \big((1 \cdot 0) + 1\big) + 1 && \text{by definition of multiplication} \\
&= (0 + 1) + 1 && \text{by definition of multiplication} \\
&= 1 + 1 && \text{because } (\forall w \in \mathbb{N})(0 + w = w)
\end{aligned}$$

We hence realize that $1 + \sum_{i=0}^{0} 2^i = 1 + 1 = 2^{0+1}$.

Inductive Step:
Let $k \in \mathbb{N}$, and assume $1 + \sum_{i=0}^{k} 2^i = 2^{k+1}$.[8] Now, watch *this.*

[8] *inductive hypothesis*

$$\begin{aligned}
1 + \sum_{i=0}^{\mathfrak{suc}(k)} 2^i &= 1 + \left(\left(\sum_{i=0}^{k} 2^i \right) + 2^{\mathfrak{suc}(k)} \right) && \text{by definition of } \sum \\
&= \left(1 + \left(\sum_{i=0}^{k} 2^i \right) \right) + 2^{\mathfrak{suc}(k)} && \text{by associativity of addition} \\
&= 2^{k+1} + 2^{\mathfrak{suc}(k)} && \text{by the } \textit{inductive hypothesis} \\
&= 2^{\mathfrak{suc}(k)} + 2^{\mathfrak{suc}(k)} && \text{since } (\forall w \in \mathbb{N})\big(\mathfrak{suc}(w) = w + 1\big) \\
&= \big(2^k \cdot 2\big) + \big(2^k \cdot 2\big) && \text{by definition of exponentiation} \\
&= 2^k \cdot (2 + 2) && \text{by distributivity of } \cdot \text{ over } + \\
&= 2^k \cdot \big((0 + 2) + 2\big) && \text{because } (\forall w \in \mathbb{N})(0 + w = w) \\
&= 2^k \cdot \big(((2 \cdot 0) + 2) + 2\big) && \text{by definition of multiplication} \\
&= 2^k \cdot \big((2 \cdot \mathfrak{suc}(0)) + 2\big) && \text{by definition of multiplication} \\
&= 2^k \cdot \big((2 \cdot 1) + 2\big) && \text{by definition of 1} \\
&= 2^k \cdot \big(2 \cdot \mathfrak{suc}(1)\big) && \text{by definition of multiplication} \\
&= 2^k \cdot (2 \cdot 2) && \text{by definition of 2} \\
&= \big(2^k \cdot 2\big) \cdot 2 && \text{by associativity of multiplication} \\
&= 2^{\mathfrak{suc}(k)} \cdot 2 && \text{by definition of exponentiation} \\
&= 2^{\mathfrak{suc}(\mathfrak{suc}(k))} && \text{by definition of exponentiation} \\
&= 2^{\mathfrak{suc}(k)+1} && \text{since } (\forall w \in \mathbb{N})\big(\mathfrak{suc}(w) = w + 1\big)
\end{aligned}$$

We thus finally obtain the desired result that $1 + \sum_{i=0}^{\mathfrak{suc}(k)} = 2^{\mathfrak{suc}(k)+1}$.

Therefore, we can conclude that $(\forall n \in \mathbb{N})\Big(1 + \sum_{i=0}^{n} 2^i = 2^{n+1}\Big)$.

QED