Problem §1 Choose any three problems from 1.2(a-i) as a warmup. Then complete Exercise 1.3.

- 1.2: Use truth tables to prove:
  - 1.2.a: $P \iff \neg(\neg P)$.
  - 1.2.c: $(P \Rightarrow Q) \iff (\neg Q \Rightarrow \neg P)$.
  - 1.2.d: $(P \Rightarrow Q) \iff (\neg P) \vee Q$.
- 1.3: Let P and Q be statements.
  (a) Prove that
  $$P \veebar \neg P$$
  is true, and explain why this justifies the Law of the Excluded Middle (which states that exactly one of P and $\neg P$ is true).
  (b) Prove that
  $$(\neg Q \Rightarrow \neg P) \Rightarrow (P \Rightarrow Q)$$
  is true, and explain why this justifies the method of Proof by Contradiction (which states that in order to prove that P is true, it suffices to show that $\neg P$ is false).

Solution:

1.2.a

P	$\neg P$	$\neg(\neg P)$
T	F	T
F	T	F

•

1.2.c

P	Q	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

•

1.2.d

P	Q	$\neg P$	$P \Rightarrow Q$	$\neg P \vee Q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

•

1.3.a

P	$\neg P$	$P \veebar \neg P$
T	F	T
F	T	T

- Since the statement is true regardless of P, $P \veebar \neg P$ is true. This also justifies the Law of the Excluded Middle, as an XOR statement is true only when one, but not both, of the statements are true; hence only one of P and $\neg P$ may be true at once in order for $P \veebar \neg P$ to be true.

1.3.b

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$	$(\neg Q \Rightarrow \neg P) \Rightarrow (P \Rightarrow Q)$
T	T	F	F	T	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

- Since the statement is true regardless of P or Q, $(\neg Q \Rightarrow \neg P) \Rightarrow (P \Rightarrow Q)$ is true. This also justifies Proof by Contradiction: if $\neg P$ is false, then P is necessarily true in order for the above statement to be true as well (alternatively, from the Law of the Excluded Middle, $\neg P$ being false necessarily implies that P is true).

Problem §2 Complete Exercise 1.7: *Prove each of the following formulas:*

(a) $S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$

(b) $S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$

(c) Suppose $S, T \subset U$. Then

$$(S \cup T)^c = S^c \cap T^c \text{ and } (S \cap T)^c = S^c \cup T^c.$$

(d) $S \Delta T = (S \cup T) \setminus (S \cap T) = (S \setminus T) \cup (T \setminus S)$

Solution:

(a) *Proof.* Let $e \in S \cap (T \cup U)$. Then e is in S, and e must also be in T or U. Equivalently, e is in S and T, or e is in S and U. Thus, $e \in (S \cap T) \cup (S \cap U)$, and so $S \cap (T \cup U) \subset (S \cap T) \cup (S \cap U)$.
Conversely, let $e \in (S \cap T) \cup (S \cap U)$. Then e is in S and T, or e is in S and U. Equivalently, e must be in S; additionally, e must be in T or U. Thus, $e \in S \cap (T \cup U)$, and so $(S \cap T) \cup (S \cap U) \subset S \cap (T \cup U)$.
Since both are subsets of each other, $S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$. ☐

(b) *Proof.* Let $e \in S \cup (T \cap U)$. Then e is in S, or e is in both T and U. Equivalently, e is in S or T, and e must be in S or U. Thus, $e \in (S \cup T) \cap (S \cup U)$, and so $S \cup (T \cap U) \subset (S \cup T) \cap (S \cup U)$.
Conversely, let $e \in (S \cup T) \cap (S \cup U)$. Then e is in S or T, and e is in S or U. If e is not in S, then e must be in T and U. If e is not in T and not in U, then e must be in S. From this, we gather that e is in S, or e is in T and U. Thus, $e \in S \cup (T \cap U)$, and so $(S \cup T) \cap (S \cup U) \subset S \cup (T \cap U)$.
Since both are subsets of each other, $S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$. ☐

(c) *Proof.* Let $e \in (S \cup T)^c$. Then $e \in U$, and $e \notin (S \cup T)$. Equivalently, e is not in S and e is not in T. Then e must be in U and not in S, and e must be in U and not in T. Thus, $e \in S^c \cap T^c$, and so $(S \cup T)^c \subset S^c \cap T^c$.
Conversely, let $e \in S^c \cap T^c$. Then e is in U and e is not in S, and e is in U and e is not in T. Equivalently, e is in U, and e is not in either T or S; or, since T and S are subsets of U, e is in the

complement of T or S. Thus, $e \in (S \cup T)^c$, and so $S^c \cap T^c \subset (S \cup T)^c$.
Since both subsets are equal, $(S \cup T)^c = S^c \cap T^c$.

Now, let $e \in (S \cap T)^c$. Then $e \in U$, and $e \notin (S \cap T)$. Equivalently, e is in U, and e is not in both S and T (but could be in S, or in T). Then e must be in U and not in S (and thus possibly in T without its overlap with S), or e must be in U and not in T (and thus possibly in S without its overlap with T). Thus, $e \in S^c \cup T^c$, and so $(S \cap T)^c \subset S^c \cup T^c$.
Conversely, let $e \in S^c \cup T^c$. Then e is in U and not in S, or e is in U and not in T. Equivalently, e is in U, and e is not in both S and T (but could be in just S or just T for the same reasons listed above); since S and T are subsets of U, e is in the complement of S and T. Thus, $e \in (S \cap T)^c$, and so $S^c \cup T^c \subset (S \cap T)^c$.
Since both are subsets of each other, $(S \cap T)^c = S^c \cup T^c$. □

(d) *Proof.* Let $e \in (S \cup T) \setminus (S \cap T)$. Then e is in either S or T, but cannot be in both S and T. Equivalently, the set e is in cannot have any "overlap" between sets S and T. So, e is either in $S \setminus T$ (S without any potential overlap with T) or $T \setminus S$ (T without any potential overlap with S). Thus, $e \in (S \setminus T) \cup (T \setminus S)$, and so $(S \cup T) \setminus (S \cap T) \subset (S \setminus T) \cup (T \setminus S)$.
Conversely, let $e \in (S \setminus T) \cup (T \setminus S)$. Then e is in S but not T, or e is in T but not S. From the first part of each statement, we get that e must be in S or T; and from the second part of each statement we get that e cannot be in the overlap between S and T. Thus, we get the statement $e \in (S \cup T) \setminus (S \cap T)$, and so $(S \setminus T) \cup (T \setminus S) \subset (S \cup T) \setminus (S \cap T)$.
Since both are subsets of each other, $(S \cup T) \setminus (S \cap T) = (S \setminus T) \cup (T \setminus S)$. □

From these problems, we observe that sets and logical statements are quite similar. A set is analogous to a logical statement, and the operators union and intersection resemble the logical "or" and "and" respectively (specifically, given sets S, T, $e \in S \cup T$ is equivalent to $e \in S \vee e \in T$, and $e \in S \cap T$ is equivalent to $e \in S \wedge e \in T$). Given a well defined complement of S, the complement S^c is analogous to the logical "not" (just as only one of P and $\neg P$ may be true, only one of $e \in S^c$ and $e \in S$ may be true). The symmetric difference is analogous to the "xor" operator in the sense that an element e being in $S \Delta T$ meaning e is in S or T, but not both, is similar in structure to notion that $P \veebar Q$ means that in order to be true, either P or Q could be true, but not both.

Problem §3 Complete Exercise 1.16:

- Let S, T be finite sets with $|S| = |T|$, and let $f : S \to T$ be a function from S to T. Prove the following are equivalent:
  - f is injective.
  - f is surjective.
  - f is bijective.

and Exercise 1.17:

- Give an example of a function $f : \mathbb{N} \to \mathbb{N}$ that is injective, but not surjective.
- Give an example of a function $f : \mathbb{N} \to \mathbb{N}$ that is surjective, but not injective.

Solution:

- (1.16)

Proof. Let $n = |S| = |T|$. We start by showing f injective implies f surjective. Let f be an injective function, and suppose that f is not surjective. Then $\exists t \in T$ such that $\forall s \in S, f(s) \neq t$; and so $|\operatorname{im} S| < n$. By the definition of a function, every $s \in S$ is mapped to some element $f(s) \in T$; and since $|S| = n$ and $|\operatorname{im} S| < n$, at least one $e \in \operatorname{im} S$ is mapped to by at least two distinct elements $s, s' \in S$ (analogously, imagine each $e \in \operatorname{im} S$ represents a "hole", and each $s \in S$ a pigeon; since there are at most $n-1$ holes, and n pigeons, by the PHP, at least one hole must have at least two distinct pigeons).

But this implies that $e = f(s) = f(s'), s \neq s'$, a contradiction to injectivity. Thus, if f is injective, then f is surjective as well.

Now, we show that f surjective implies f injective. Let f be a surjective function, and suppose that f is not injective. Then $\exists s, s' \in S$ such that $f(s) = f(s'), s \neq s'$. By definition of a function, each $s \in S$ is mapped to one and only one $f(s) \in \operatorname{im} S$. But since f is not injective, at least one $f(s) \in \operatorname{im} S$ is mapped to by at least two distinct $s, s' \in S$, which implies that $|\operatorname{im} S| < n$ (equivalently, at least one $t \in T$ is not mapped to by any $s \in S$), a contradiction to surjectivity. Thus, if f is surjective, then f is injective as well.
Since f injective implies f surjective, and f surjective implies f injective, if f is either injective or surjective, it is bijective as well; and trivially, f bijective implies both injective and surjective. Thus the three statements are equivalent. $\square$

- (1.17)
  - Let
    $$\begin{aligned} f : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto f(n) = n + 1. \end{aligned}$$
    f is injective, as no two $n_1, n_2 \in \mathbb{N}$ share a $succ(n)$ unless $n_1 = n_2$ (equivalently, $n_1 + 1 = n_2 + 1$ implies $n_1 = n_2$). f is also not surjective, as $1 \notin \operatorname{im} f$.
  - Let
    $$\begin{aligned} f : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto f(n) = \left\lceil \frac{n}{2} \right\rceil. \end{aligned}$$
    f is surjective, as for any $k \in \mathbb{N}$, take $n = 2k \in \mathbb{N}$; then we get $f(n) = \left\lceil \frac{2k}{2} \right\rceil = k$. On the other hand, f is not injective. Let $n_1, n_2 \in \mathbb{N}, n_1 = 1, n_2 = 2$. Then $f(n_1) = f(n_2) = 1$, but $n_1 \neq n_2$.