1 XOR

Note 1

The truth table of XOR (denoted by $\oplus$) is as follows.

A	B	$A \oplus B$
F	F	F
F	T	T
T	F	T
T	T	F

(a) Express XOR using only $(\wedge, \vee, \neg)$ and parentheses.

(b) Does $(A \oplus B)$ imply $(A \vee B)$? Explain briefly.

(c) Does $(A \vee B)$ imply $(A \oplus B)$? Explain briefly.

Solution:

(a) These are all correct:

- $A \oplus B = (A \wedge \neg B) \vee (\neg A \wedge B)$
  Notice that there are only two instances when $A \oplus B$ is true: (1) when A is true and B is false, or (2) when B is true and A is false. The clause $(A \wedge \neg B)$ is only true when (1) is, and the clause $(\neg A \wedge B)$ is only true when (2) is.
- $A \oplus B = (A \vee B) \wedge (\neg A \vee \neg B)$
  Another way to think about XOR is that exactly one of A and B needs to be true. This also means exactly one of $\neg A$ and $\neg B$ needs to be true. The clause $(A \vee B)$ tells us *at least* one of A and B needs to be true. In order to ensure that one of A or B is also false, we need the clause $(\neg A \vee \neg B)$ to be satisfied as well.
- $A \oplus B = (A \vee B) \wedge \neg(A \wedge B)$
  This is the same as the previous, with De Morgan's law applied to equate $(\neg A \vee \neg B)$ to $\neg(A \wedge B)$.

(b) Yes. $(A \oplus B) \implies (A \wedge \neg B) \vee (\neg A \wedge B) \implies (A \vee B)$. When $(A \oplus B)$ is true, at least one of A or B is true, which makes $(A \vee B)$ true as well.

(c) No. When A and B are both true, then $(A \vee B)$ is true, but $(A \oplus B)$ is false.

2 Proof Practice

Note 2

(a) Prove that $\forall n \in \mathbb{N}$, if n is odd, then n^2+1 is even. (Recall that n is odd if $n = 2k+1$ for some natural number k.)

(b) Prove that $\forall x, y \in \mathbb{R}$, $\min(x,y) = (x+y-|x-y|)/2$. (Recall, that the definition of absolute value for a real number z, is

$$|z| = \begin{cases} z, & z \geq 0 \\ -z, & z < 0 \end{cases}$$

(c) Suppose $A \subseteq B$. Prove $\mathscr{P}(A) \subseteq \mathscr{P}(B)$. (Recall that $A' \in \mathscr{P}(A)$ if and only if $A' \subseteq A$.)

Solution:

(a) We will use a direct proof. Suppose n is odd. By the definition of odd numbers, we have $n = 2k+1$ for some natural number k. This means that we have

$$\begin{aligned} n^2+1 &= (2k+1)^2+1 \\ &= 4k^2+4k+2 \\ &= 2(2k^2+2k+1) \end{aligned}$$

Since $2k^2+2k+1$ is a natural number, by the definition of even numbers, n^2+1 is even.

(b) We will use a proof by cases. Again, the definition of the absolute value function for real number z is

$$|z| = \begin{cases} z, & z \geq 0 \\ -z, & z < 0 \end{cases}$$

Case 1: $x < y$. This means $|x-y| = y-x$. Substituting this into the formula on the right hand side, we get

$$\frac{x+y-y+x}{2} = x = \min(x,y).$$

Case 2: $x \geq y$. This means $|x-y| = x-y$. Substituting this into the formula on the right hand side, we get

$$\frac{x+y-x+y}{2} = y = \min(x,y).$$

(c) Suppose $A' \in \mathscr{P}(A)$; this means that $A' \subseteq A$ (by the definition of the power set).

Let $x \in A'$. Then, since $A' \subseteq A$, $x \in A$. Since $A \subseteq B$, $x \in B$. We have shown $(\forall x \in A')(x \in B)$, so $A' \subseteq B$.

Since the previous argument works for any $A' \subseteq A$, we have proven $(\forall A' \in \mathscr{P}(A))(A' \subseteq B)$. So, $(\forall A' \in \mathscr{P}(A))(A' \in \mathscr{P}(B))$ Thus, we conclude $\mathscr{P}(A) \subseteq \mathscr{P}(B)$ as desired.

3 Numbers of Friends

Note 2

Prove that if there are $n \geq 2$ people at a party, then at least 2 of them have the same number of friends at the party. Assume that friendships are always reciprocated: that is, if Alice is friends with Bob, then Bob is also friends with Alice.

(Hint: The Pigeonhole Principle states that if n items are placed in m containers, where $n > m$, at least one container must contain more than one item. You may use this without proof.)

Solution:

We will prove this by contradiction. Suppose the contrary that everyone has a different number of friends at the party. Since the number of friends that each person can have ranges from 0 to $n-1$, we conclude that for every $i \in \{0, 1, \ldots, n-1\}$, there is exactly one person who has exactly i friends at the party. In particular, there is one person who has $n-1$ friends (i.e., friends with everyone), is friends with a person who has 0 friends (i.e., friends with no one). This is a contradiction since friendship is mutual.

Here, we used the pigeonhole principle because assuming for contradiction that everyone has a different number of friends gives rise to n possible containers. Each container denotes the number of friends that a person has, so the containers can be labelled $0, 1, ..., n-1$. The objects assigned to these containers are the people at the party. However, containers 0, $n-1$ or both must be empty since these two containers cannot be occupied at the same time. This means that we are assigning n people to at most $n-1$ containers, and by the pigeonhole principle, at least one of the $n-1$ containers has to have two or more objects i.e. at least two people have to have the same number of friends.

4 Preserving Set Operations

Note 0
Note 2

For a function f, define the image of a set X to be the set $f(X) = \{y \mid y = f(x) \text{ for some } x \in X\}$. Define the inverse image or preimage of a set Y to be the set $f^{-1}(Y) = \{x \mid f(x) \in Y\}$. Prove the following statements, in which A and B are sets.

Recall: For sets X and Y, $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$. To prove that $X \subseteq Y$, it is sufficient to show that $(\forall x)\ ((x \in X) \implies (x \in Y))$.

(a) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

(b) $f(A \cup B) = f(A) \cup f(B)$.

Solution:

In order to prove equality $A = B$, we need to prove that A is a subset of B, $A \subseteq B$ and that B is a subset of A, $B \subseteq A$. To prove that LHS is a subset of RHS we need to prove that if an element is a member of LHS then it is also an element of the RHS.

(a) Suppose $x \in f^{-1}(A \cup B)$ which means that $f(x) \in A \cup B$. Then either $f(x) \in A$, in which case $x \in$

$f^{-1}(A)$, or $f(x) \in B$, in which case $x \in f^{-1}(B)$, so in either case we have $x \in f^{-1}(A) \cup f^{-1}(B)$. This proves that $f^{-1}(A \cup B) \subseteq f^{-1}(A) \cup f^{-1}(B)$.

Now, suppose that $x \in f^{-1}(A) \cup f^{-1}(B)$. Suppose, without loss of generality, that $x \in f^{-1}(A)$. Then $f(x) \in A$, so $f(x) \in A \cup B$, so $x \in f^{-1}(A \cup B)$. The argument for $x \in f^{-1}(B)$ is the same. Hence, $f^{-1}(A) \cup f^{-1}(B) \subseteq f^{-1}(A \cup B)$.

(b) Suppose that $x \in A \cup B$. Then either $x \in A$, in which case $f(x) \in f(A)$, or $x \in B$, in which case $f(x) \in f(B)$. In either case, $f(x) \in f(A) \cup f(B)$, so $f(A \cup B) \subseteq f(A) \cup f(B)$.

Now, suppose that $y \in f(A) \cup f(B)$. Then either $y \in f(A)$ or $y \in f(B)$. In the first case, there is an element $x \in A$ with $f(x) = y$; in the second case, there is an element $x \in B$ with $f(x) = y$. In either case, there is an element $x \in A \cup B$ with $f(x) = y$, which means that $y \in f(A \cup B)$. So $f(A) \cup f(B) \subseteq f(A \cup B)$.

A common pitfall for this question is to start with an element $y \in f(A \cup B)$, and to take $f^{-1}(y) \in A \cup B$. The issue here is that $f^{-1}(y)$ is not necessarily a single element; it can be a set of elements, so the more precise statement is $f^{-1}(\{y\}) \subseteq A \cup B$. Here, we can't necessarily conclude that either $f^{-1}(\{y\}) \subseteq A$ or $f^{-1}(\{y\}) \subseteq B$, since $f^{-1}(\{y\})$ could contain some elements in A and some elements in B. This would require more careful consideration; it's easier in this case to work with an element $x \in A \cup B$.

The purpose of this problem is to gain familiarity to naming things precisely. In particular, we named an element in the LHS (or the pre-image of the LHS) and then argued about whether that element or its image was in the right hand side. By explicitly naming an element generically where it could be *any* element in the set, we could argue about its membership in a set and or its image or preimage. With these different concepts floating around it is helpful to be clear in the argument.