Section 04: Propositions and Proofs

1. Formal Spoofs

For each of the following proofs, determine why the proof is incorrect. Then, consider whether the conclusion of the proof is true or not. If it is true, state how the proof could be fixed. If it is false, give a counterexample.

(a) Show that $\exists z\ \forall x\ P(x, z)$ follows from $\forall x\ \exists y\ P(x, y)$.

1.	$\forall x\ \exists y\ P(x, y)$	[Given]
2.	$\forall x\ P(x, c)$	[$\exists$ Elim: 1, c special]
3.	$\exists z\ \forall x P(x, z)$	[$\exists$ Intro: 2]

Solution:

The mistake is on line 2 where an inference rule is used on a subexpression. When we apply something like the $\exists$ Elim rule, the $\exists$ must be at the start of the expression and outside all other parts of the statement.

The conclusion is false, it's basically saying we can interchange the order of $\forall$ and $\exists$ quantifiers. Let the domain of discourse be integers and define $P(x, y)$ to be $x < y$. Then the hypothesis is true: for every integer, there is a larger integer. However, the conclusion is false: there is no integer that is larger than every other integer. Hence, there can be no correct proof that the conclusion follows from the hypothesis.

(b) Show that $\exists z\ (P(z) \wedge Q(z))$ follows from $\forall x\ P(x)$ and $\exists y\ Q(y)$.

1.	$\forall x\ P(x)$	[Given]
2.	$\exists y\ Q(y)$	[Given]
3.	Let z be arbitrary	
4.	$P(z)$	[$\forall$ Elim: 1]
5.	$Q(z)$	[$\exists$ Elim: 2, let z be the object that satisfies $Q(z)$]
6.	$P(z) \wedge Q(z)$	[$\wedge$ Intro: 4, 5]
7.	$\exists z\ P(z) \wedge Q(z)$	[$\exists$ Intro: 6]

Solution:

The mistake is on line 5. The $\exists$ Elim rule must create a new variable rather than applying some property to an existing variable.

The conclusion is true in this case. Instead of declaring z to be arbitrary and then applying $\exists$ Elim to make it specific, we can instead just apply the $\exists$ Elim rule directly to create z. To do this, we would remove lines 3 and 5 and define z by applying $\exists$ Elim to line 2. Note, it's important that we define z before applying line 4.

2. Prime Checking

You wrote the following code, `isPrime(int n)` which you are confident returns `true` if and only if n is prime (we assume its input is always positive).

```
public boolean isPrime(int n) {
    int potentialDiv = 2;
    while (potentialDiv < n) {
```

```
        if (n % potenttialDiv == 0)
            return false;
        potentialDiv++;
    }
    return true;
}
```

Your friend suggests replacing `potentialDiv < n` with `potentialDiv <= Math.sqrt(n)`. In this problem, you'll argue the change is ok. That is, your method still produces the correct result if n is a positive integer.

We will use "nontrivial divisor" to mean a factor that isn't 1 or the number itself. Formally, a positive integer k being a "nontrivial divisor" of n means that $k|n$, $k \neq 1$ and $k \neq n$. Claim: when a positive integer n has a nontrivial divisor, it has a nontrivial divisor at most $\sqrt{n}$.

(a) Let's try to break down the claim and understand it through examples. Show an example (a specific n and k) of a nontrivial divisor, of a divisor that is not nontrivial, and of a number with only trivial divisors. **Solution:**

Some examples of "trivial" divisors: (1 of 15), (3 of 3)
Some examples of nontrivial divisors: (3 of 15), (9 of 81)
A number with only trivial divisor is just a prime number: it has no factors.

(b) Prove the claim. Hint: you may want to divide into two cases!

Solution:

Let k be a nontrivial divisor of n. Since k is a divisor, $n = kc$ for some integer c. Observe that c is also nontrivial, since if c were 1 or n then k would have to be n or 1.

We now have two cases:

Case 1: $k \leq \sqrt{n}$
If $k \leq \sqrt{n}$, then we're done because k is the desired nontrivial divisor.

Case 2: $k > \sqrt{n}$
If $k > \sqrt{n}$, then multiplying both sides by c we get $ck > c\sqrt{n}$. But $ck = n$ so $n > c\sqrt{n}$. Finally, dividing both sides by $\sqrt{n}$ gives $\sqrt{n} > c$, so c is the desired nontrivial factor.

In both cases we find a nontrivial divisor at most $\sqrt{n}$, as required.

Alternate solution (proof by contradiction): Let k be a nontrivial divisor of n. Since k is a divisor, $n = kc$ for some integer c. Observe that c is also nontrivial, since if c were 1 or n then k would have to be n or 1.

Suppose, for contradiction, that $k > \sqrt{n}$ and $c > \sqrt{n}$. Then $kc > \sqrt{n}\sqrt{n} = n$. But by assumption we have $kc = n$, so this is a contradiction. It follows that either k or c is at most $\sqrt{n}$ meaning that n has a nontrivial divisor at most $\sqrt{n}$.

(c) Informally explain why the fact about integers proved in (b) lets you change the code safely.

Solution:

The new code makes a subset of "checks" that the old code makes, thus the only concern would be that a non-prime number we found in the later checks would "slip through" without the extra checks. However, if a number has any nontrivial divisor, it will have one that is $\leq \sqrt{n}$, so even if we exit the loop early after $\sqrt{n}$ instead of n checks, our method is still guaranteed to always work.

3. How Many Elements?

For each of these, how many elements are in the set? If the set has infinitely many elements, say ∞.

(a) $A = \{1, 2, 3, 2\}$

Solution:

3

(b) $B = \{\{\}, \{\{\}\}, \{\{\}, \{\}\}, \{\{\}, \{\}, \{\}\}, \dots\}$

Solution:

$$\begin{aligned} B &= \{\{\}, \{\{\}\}, \{\{\}, \{\}\}, \{\{\}, \{\}, \{\}\}, \dots\} \\ &= \{\{\}, \{\{\}\}, \{\{\}\}, \{\{\}\}, \dots\} \\ &= \{\varnothing, \{\varnothing\}\} \end{aligned}$$

So, there are two elements in B.

(c) $C = A \times (B \cup \{7\})$

Solution:

$C = \{1, 2, 3\} \times \{\varnothing, \{\varnothing\}, 7\} = \{(a, b) \mid a \in \{1, 2, 3\}, b \in \{\varnothing, \{\varnothing\}, 7\}\}$. It follows that there are $3 \times 3 = 9$ elements in C.

(d) $D = \varnothing$

Solution:

0.

(e) $E = \{\varnothing\}$

Solution:

1.

(f) $F = \mathcal{P}(\{\varnothing\})$

Solution:

$2^1 = 2$. The elements are $F = \{\varnothing, \{\varnothing\}\}$.

4. Set = Set

Prove the following set identities.

(a) Let the universal set be $\mathcal{U}$. Prove $A \cap \overline{B} \subseteq A \backslash B$ for any sets A, B.

Solution:

Suppose $A \cap \overline{B}$ is nonempty (if it is empty, the proof is done; we need this line in order to assert that there is an element x in the next sentence). Let x be an arbitrary element in $A \cap \overline{B}$.

$$\begin{aligned} x \in A \cap \overline{B} \quad &\text{implies that} \quad x \in A \wedge x \in \overline{B} && \text{[Definition of } \cap\text{]} \\ &\text{which implies that} \quad x \in A \wedge x \notin B && \text{[Definition of } \overline{B}\text{]} \\ &\text{which implies that} \quad x \in A \setminus B && \text{[Definition of } \setminus\text{]} \end{aligned}$$

The above logic shows that $x \in A \cap \overline{B} \rightarrow x \in A \setminus B$. So by the definition of subset, we have $A \cap \overline{B} \subseteq A \setminus B$.

Solution:

Observe that the following equalities hold.

$$\begin{aligned} A \cap \overline{B} &= \{x : x \in A \wedge x \in \overline{B}\} && \text{[Definition of } \cap\text{]} \\ &= \{x : x \in A \wedge x \notin B\} && \text{[Definition of } \overline{B}\text{]} \\ &= \{x : x \in A \setminus B\} && \text{[Definition of } \setminus\text{]} \\ &= A \setminus B && \text{[Definition of set comprehension]} \end{aligned}$$

Thus, the two sets $A \cap \overline{B}$ and $A \setminus B$ are in fact equal, so each is a subset of the other.

Solution:

Let x be arbitrary.

$$\begin{aligned} x \in A \cap \overline{B} \quad &\rightarrow \quad x \in A \wedge x \in \overline{B} && \text{[Definition of } \cap\text{]} \\ &\rightarrow \quad x \in A \wedge x \notin B && \text{[Definition of } \overline{B}\text{]} \\ &\rightarrow \quad x \in A \setminus B && \text{[Definition of } \setminus\text{]} \end{aligned}$$

Thus, since $x \in A \cap \overline{B} \rightarrow x \in A \setminus B$, it follows that $A \cap \overline{B} \subseteq A \setminus B$, by definition of subset.

(b) Prove that $(A \cap B) \times C \subseteq A \times (C \cup D)$ for any sets A, B, C, D.

Solution:

Let x be an arbitrary element of $(A \cap B) \times C$. Then, by definition of Cartesian product, x must be of the form (y, z) where $y \in A \cap B$ and $z \in C$. Since $y \in A \cap B$ by definition of $\cap$, $y \in A$ and $y \in B$; in particular, all we care about is that $y \in A$. Since $z \in C$, by definition of $\cup$, we also have $z \in C \cup D$. Therefore since $y \in A$ and $z \in C \cup D$, by definition of Cartesian product we have $x = (y, z) \in A \times (C \cup D)$.

Since x was an arbitrary element of $(A \cap B) \times C$ we have proved that $(A \cap B) \times C \subseteq A \times (C \cup D)$ as required.

5. Modular Arithmetic

(a) Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Solution:

Suppose that $a \mid b$ and $b \mid a$, where a, b are integers. By the definition of divides, we have $a \neq 0$, $b \neq 0$ and

$b = ka, a = jb$ for some integers k, j. Combining these equations, we see that $a = j(ka)$.

Then, dividing both sides by a, we get $1 = jk$. So, $\frac{1}{j} = k$. Note that j and k are integers, which is only possible if $j, k \in \{1, -1\}$. It follows that $b = -a$ or $b = a$.

(b) Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

Solution:

Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$. By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$. By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$. Combining the two equations, we see that $a - b = (knj) = n(kj)$. By definition of congruence, we have $a \equiv b \pmod{n}$, as required.

6. Trickier Set Theory

Note, this problem requires a little more thinking. The solution will cover both the answer as well as the intuition used to arrive at it.

Show that for any set X and any set A such that $A \in \mathcal{P}(X)$, there exists a set $B \in \mathcal{P}(X)$ such that $A \cap B = \emptyset$ and $A \cup B = X$.

Solution:

This solution might look long, but most of it is explaining the intuition. The proof itself is fairly short!

We start by letting X and A be arbitrary sets and assume that $A \in \mathcal{P}(X)$. Now we think about our goal. We want to show there is some set B with the given properties. The way to do this is usually to construct B somehow, but there's nothing in the problem that tells us where B might come from!

When you get stuck like this, try to use all the information given in the problem to deduce as many things as we can. First we might notice that $A \in \mathcal{P}(X)$ means that $A \subseteq X$ and $B \in \mathcal{B}$ means $B \subseteq X$. So given some subset of X, we must construct some other subset.

Next, we consider what we know about B. The property that $A \cap B = \emptyset$ means that B and A share no elements in common. That is, B consists only of elements in X that are not in A. The property that $A \cup B = X$ is a little tricker. We might think of A as some collection of objects from X, $A \cup B$ throws in all the elements of B, and once we do that we have all the elements of X. In order for this to happen, we know B must contain all the elements of X that weren't in A.

At this point we've deduced that B contains only elements in X that are not in A, but also that it must contain all the elements of X that are not in A. This says that B is exactly the elements of X that are not in A. Does this sound familiar? It's exactly the set difference $X \setminus A$.

Now we can write out the proof. Let X be an arbitrary set and let A be an arbitrary element of $\mathcal{P}(X)$. Let $B = X \setminus A$. For any $x \in X \setminus A$, by definition we have $x \in X$ which shows that $B \subseteq X$ and by definition $B \in \mathcal{P}(X)$.

To show that $A \cap B = \emptyset$, we must show that there are no elements that are both in A and B. If x is in $X \setminus A$, then by definition x is not in A, so there's no element that can be in both. Thus, $A \cap B = \emptyset$. To prove $A \cup B = X$, we first suppose $x \in A \cup B$ which by definition means $x \in A$ or $x \in B$. If $x \in A$ then since $A \subseteq X$ we have $x \in A$. If $x \in B$ then $x \in X \setminus A$ which by definition means that $x \in X$. In either case $x \in X$. In the other direction suppose $x \in X$. We again consider two cases. If $x \in A$ then there's nothing to show because then $x \in A \cup B$ automatically. If $x \notin A$ then since x is an element of X not in A, by definition we have $x \in X \setminus A$ which is equal to B, so in this case we also have $x \in A \cup B$. In either case $x \in A \cup B$. Since we've shown $x \in A \cup B$ if and only if $x \in X$, we've shown $A \cup B = X$, which completes the proof.