CSE 311: Foundations of Computing I

Section 4: English Proofs and Sets Solutions

1. Formal Spoofs

For each of 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]

(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 mistakes are as follows:

(a) Line 2: inference rule used on a subexpression.

(b) Line 5: must use a new variable with $\exists$ Elim

Next, we consider whether the statements are actually true:

(a) **False**. Let the domain of discourse be the 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 integer that is larger than every other integer (no largest integer). Hence, there can be no correct proof that the conclusion follows from the hypothesis.

(b) **True**. Remove line 3 declaring z to be arbitrary. Instead, define z by applying $\exists$ Elim to line 2. Finally, move line 4 after line 5. (We need z to already exist in order to apply $\forall$ Elim, so we need to do this after the $\exists$ Elim on line for, which actually defines z.)

2. Game, Set, Match

Let A, B, and C be arbitrary sets. Consider the claim that $A \setminus B \subseteq A \cup C$.

(a) Write a formal proof of the claim.

Solution:

1.	Let x be an arbitrary object.	
2.1.	$x \in A \setminus B$	Assumption
2.2.	$(x \in A) \wedge \neg(x \in B)$	Def of “$\setminus$”: 2.1
2.3.	$x \in A$	Elim $\wedge$: 2.2
2.4.	$(x \in A) \vee (x \in C)$	Intro $\vee$: 2.3
2.5.	$x \in A \cup C$	Def of $\cup$: 2.4
2.	$(x \in A \setminus B) \to (x \in A \cup C)$	Direct Proof
3.	$\forall x\,((x \in A \setminus B) \to (x \in A \cup C))$	Intro $\forall$: 1, 2
4.	$A \setminus B \subseteq A \cup C$	Def of $\subseteq$: 3

(b) Translate your formal proof to an English proof.

Solution:

Let x be an arbitrary object. Suppose that $x \in A \setminus B$. By definition, this means that $x \in A$ and $x \notin B$. Since $x \in A$, we have $x \in A \cup C$ by the definition of $\cup$. Since x was arbitrary, this shows $A \setminus B \subseteq A \cup C$.

3. Ghosts and Skeletons

Let A and B be sets and P and Q be predicates. For each of the claims below, write the *skeleton* of an English proof of the claim. It will not be possible to complete the proof with just the information given, but you should be able to see the basic shape of the proof.

(a) $A = B$

Solution:

Let x be arbitrary.

Suppose that $x \in A$. **....** Thus, $x \in B$.

Now, suppose that $x \in B$. **....** Thus, $x \in A$.

We have shown that $x \in A$ iff $x \in B$. Since x was arbitrary, the sets are equal by definition.

(b) No element of A satisfies P.

Solution:

Let x be arbitrary.

Suppose that $x \in A$. **....** Thus, $P(x)$ is false.

Since x was arbitrary, this shows that no element of A satisfies P.

[Note: we have actually proven $\forall x\, \neg P(x)$, whereas the claim best translates as $\neg \exists x\, P(x)$. However, the two are equivalent by De Morgan's law, and that is a simple enough step that the reader should see it.]

(c) Any object that satisfies P but not Q is in the set B.

Solution:

Let x be arbitrary.

Suppose that x satisfies P but not Q. **....** Thus, $x \in B$.

Since x was arbitrary, this shows that anything satisfying P but not Q is in B.

(d) B is not a subset of A.

Solution:

[We need to show $\neg \forall x\, ((x \in B) \to (x \in A))$, but that is equivalent to $\exists x\, ((x \in B) \land (x \notin A))$.]

Let $x = \ldots.$ Since ..., we can see that $x \in B$. On the other hand, since ..., we can see that $x \notin A$. Thus, x is a counterexample to the claim that B is a subset of A.

4. Primality Checking

When checking if a number n is prime by brute force, it is only necessary to check possible factors up to $\sqrt{n}$.

Specifically, we can show the following. Let n, a, and b be positive integers. Here is a proof that, if $n = ab$, then either a or b is at most $\sqrt{n}$.

1.1.	$n = ab$	Assumption
1.2.1	$\neg(a \leq \sqrt{n} \vee b \leq \sqrt{n})$	Assumption
1.2.2	$(a > \sqrt{n}) \wedge (b > \sqrt{n})$	De Morgan: 1.2.1
1.2.3	$a > \sqrt{n}$	Elim $\wedge$: 1.2.2
1.2.4	$b > \sqrt{n}$	Elim $\wedge$: 1.2.2
1.2.5	$ab > \sqrt{n}\sqrt{n} = n$	Prop of "$>$": 1.2.3, 1.2.4 Algebra
1.2.6	$(ab = n) \wedge (ab > n)$	Intro $\wedge$: 1.1, 1.2.5
1.2.7	F	Prop of "$>$", 1.2.6
1.2.	$\neg(a \leq \sqrt{n} \vee b \leq \sqrt{n}) \rightarrow$ F	Direct Proof
1.3.	$\neg\neg(a \leq \sqrt{n} \vee b \leq \sqrt{n}) \vee$ F	Law of Implication: 1.2
1.4.	$\neg\neg(a \leq \sqrt{n} \vee b \leq \sqrt{n})$	Identity: 1.3
1.5.	$a \leq \sqrt{n} \vee b \leq \sqrt{n}$	Double Negation: 1.4
1.	$(n = ab) \rightarrow (a \leq \sqrt{n} \vee b \leq \sqrt{n})$	Direct Proof

Translate this formal proof to an English proof. (Hint: notice which of the proof strategies is being used in part of this proof. Our proof strategies each have special, often shorter, English translations.)

Solution:

Suppose that $n = ab$. Suppose for a contradiction that $a, b > \sqrt{n}$. It follows that $ab > \sqrt{n}\sqrt{n} = n$. We cannot have both $ab = n$ and $ab > n$, so this is a contradiction. It follows that a or b is at most $\sqrt{n}$.