# Section 04: Solutions

## 1. Formal Proof (Direct Proof Rule)

Show that $\neg t \to s$ follows from $t \vee q$, $q \to r$ and $r \to s$ with a formal proof. Then, translate your proof to English.

**Solution:**

**Formal proof:**

| | | | |
|---|---|---|---|
| 1. | $t \vee q$ | | [Given] |
| 2. | $q \to r$ | | [Given] |
| 3. | $r \to s$ | | [Given] |
| | 4.1. | $\neg t$ | [Assumption] |
| | 4.2. | $q$ | [Elim of $\vee$: 1, 4.1] |
| | 4.3. | $r$ | [MP of 4.2, 2] |
| | 4.4. | $s$ | [MP 4.3, 3] |
| 4. | $\neg t \to s$ | | [Direct Proof Rule] |

**English proof:**
Suppose $\neg t$. Since we are given that $t$ holds or $q$ holds, we know that $q$ holds. Given this, and that we know $q$ implies $r$, we know $r$ holds. We also know $r$ implies $s$, so $s$ must hold.

## 2. Formal Proof

Show that $\neg p$ follows from $\neg(\neg r \vee t)$, $\neg q \vee \neg s$ and $(p \to q) \wedge (r \to s)$ with a formal proof. Then, translate your proof to English. **Solution:**

**Formal proof:**

| | | |
|---|---|---|
| 1. | $\neg(\neg r \vee t)$ | [Given] |
| 2. | $\neg q \vee \neg s$ | [Given] |
| 3. | $(p \to q) \wedge (r \to s)$ | [Given] |
| 4. | $\neg\neg r \wedge \neg t$ | [DeMorgan's Law: 1] |
| 5. | $\neg\neg r$ | [Elim of $\wedge$: 4] |
| 6. | $r$ | [Double Negation: 5] |
| 7. | $r \to s$ | [Elim of $\wedge$: 3] |
| 8. | $s$ | [MP, 6,7] |
| 9. | $\neg\neg s$ | [Double Negation: 8] |
| 10. | $\neg s \vee \neg q$ | [Commutative: 2] |
| 11. | $\neg q$ | [Elim of $\vee$: 10, 9] |
| 12. | $p \to q$ | [Elim of $\wedge$: 3] |
| 13. | $\neg q \to \neg p$ | [Contrapositive: 12] |
| 14. | $\neg p$ | [MP: 11,13] |

**English proof:**
We are given that neither $\neg r$ nor $t$ is true, which tells us that, $r$ (and $\neg t$) must hold. We know that $r$ implies $s$, so $s$ must also hold. Since we know that $\neg s$ holds or $\neg q$ holds, and $s$ holds, it must be that $\neg q$ holds. We

were also given that $p$ implies $q$, so taking the contrapositive, we know that $\neg q$ implies $\neg p$. Since we know $\neg q$, we can conclude that $\neg p$ holds.

## 3. Spoof and Goofs

For each claim, translate the English proof into a formal proof and say whether it is a **spoof** (the claim is true but the proof is wrong) or a **goof** (the claim is false). Then, if it is a spoof, point out the errors in the proof and explain how to correct them, and if it is a goof, point out the first error and show that the claim is false by giving a counterexample.

(a) Show that $r$ follows from $\neg p$ and $p \leftrightarrow r$.

*Spoof:* Since we are given that $p \leftrightarrow r$, we know $p \rightarrow r$. We are also given that $\neg p$ holds, so it must be the case that $\neg p \vee (p \vee r)$ holds. This claim is equivalent to $(p \wedge \neg p) \rightarrow r$. Since this last claim starts by assuming both $p$ and $\neg p$, we can infer that this holds with just $\neg p$, giving us $\neg p \rightarrow r$. Since we were given that $\neg p$ holds, we get that $r$ holds.

**Solution:**

| | | |
|---|---|---|
| 1. | $p \leftrightarrow r$ | Given |
| 2. | $(p \rightarrow r) \wedge (r \rightarrow p)$ | Defn Biconditional: 1 |
| 3. | $p \rightarrow r$ | Elim $\wedge$: 2 |
| 4. | $\neg p$ | Given |
| 5. | $\neg p \vee (p \vee r)$ | Intro $\vee$: 4 |
| 6. | $(\neg p \vee p) \vee r$ | Associativity: 5 |
| 7. | $(\neg\neg\neg p \vee \neg\neg p) \vee r$ | Double Negation: 6 |
| 8. | $\neg(\neg\neg p \wedge \neg p) \vee r$ | De Morgan's: 7 |
| 9. | $\neg(p \wedge \neg p) \vee r$ | Double Negation: 8 |
| 10. | $(p \wedge \neg p) \rightarrow r$ | Law of Implication: 9 |
| 11. | $\neg p \rightarrow r$ | Elim $\wedge$: 10 |
| 12. | $r$ | Modus Ponens: 4, 11 |

This is a goof. On line 10, Elim $\wedge$ is applied to a subexpression, which is not valid. The conclusion of the proof is false, which we can see by considering the following counterexample. If $p \equiv F$ and $r \equiv F$, then $\neg p \equiv T$ and $p \leftrightarrow r \equiv F \leftrightarrow F$ is true (i.e. the givens are true), but $r$, the conclusion, is false.

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

*Spoof:* We are given that, for every x, there is some y such that P(x, y) holds. Thus, there must be some object c such that for every x, P(x, c) holds. This shows that there exists an object z such that, for every x, P(x, z) holds.

**Solution:**

| | | |
|---|---|---|
| 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 |

This is a goof. 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.

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

*Spoof:* Let z be arbitrary. Since we were given that for every x, P(x) holds, P(z) must hold. Since we were given that there is a y such that Q(y) holds, Q(z) must also hold. From the previous facts, we know that there is some object z such that P(z) and Q(z) hold.

**Solution:**

| | | |
|---|---|---|
| 1. | $\forall x\ P(x)$ | Given |
| 2. | $\exists y\ Q(y)$ | Given |
| 3. | Let $z$ be arbitrary | |
| 4. | $P(z)$ | Elim $\forall$: 1 |
| 5. | $Q(z)$ | Elim $\exists$: 2 ($z$ special) |
| 6. | $P(z) \wedge Q(z)$ | Intro $\wedge$: 4, 5 |
| 7. | $\exists z\ P(z) \wedge Q(z)$ | Intro $\exists$: 6 |

This is a spoof. 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.

## 4. Predicate Logic Formal Proof

Given $\forall x\, T(x) \to M(x)$, we wish to prove $(\exists x\, T(x)) \to (\exists y\, M(y))$.

The following formal proof does this, but it is missing explanations for each line. Fill in the blanks with inference rules or equivalences to apply (as well as the line numbers) to complete the proof. Then, translate the proof to English.

1. $\forall x\, T(x) \to M(x)$ (_____)
   - 2.1. $\exists x\, T(x)$ (_____)
   - 2.2. $T(c)$ (_____)
   - 2.3. $T(c) \to M(c)$ (_____)
   - 2.4. $M(c)$ (_____)
   - 2.5. $\exists y\, M(y)$ (_____)
2. $(\exists x\, T(x)) \to (\exists y\, M(y))$ (_____)

**Solution:**

1. $\forall x\, T(x) \to M(x)$ Given

| | |
|---|---|
| 2.1. $\exists x.\, T(x)$ | Assumption |
| 2.2. $T(c)$ | Elim $\exists$: 2.1 (c) |
| 2.3. $T(c) \to M(c)$ | Elim $\forall$: 1 |
| 2.4. $M(c)$ | Modus Ponens: 2.2, 2.3 |
| 2.5. $\exists y\, M(y)$ | Intro $\exists$: 2.4 |

2. $(\exists x\, T(x)) \to (\exists y\, M(y))$ Direct Proof: 2.1-2.5

**English proof:**
Suppose that there exists an object $c$ such that $T(c)$. Since we are given that for any object $x$ in the domain, $T(x)$ implies $M(x)$, we know that this must also be true for $c$. So, we can conclude $M(c)$. This shows that there exists an object $y$ (=c) such that $M(y)$.

# 5. A Formal Proof in Predicate Logic

Prove $\exists x\ (P(x) \vee R(x))$ from $\forall x\ (P(x) \vee Q(x))$ and $\forall y\ (\neg Q(y) \vee R(y))$ using a formal proof. Then, translate your proof to English.
Assume that "a" is the name of a well-known constant in this domain (for e.g., $\pi$ in the domain of real numbers).

**Solution:**

**Formal proof:**

| | | | |
|---|---|---|---|
| 1. | $\forall x\ (P(x) \vee Q(x))$ | | Given |
| 2. | $\forall y\ (\neg Q(y) \vee R(y))$ | | Given |
| 3. | $P(a) \vee Q(a)$ | | Elim $\forall$: 1 |
| 4. | $\neg\neg P(a) \vee Q(a)$ | | Double Negation: 3 |
| 5. | $\neg P(a) \to Q(a)$ | | Law of Implication: 4 |
| 6. | $\neg Q(a) \vee R(a)$ | | Elim $\forall$: 2 |
| 7. | $Q(a) \to R(a)$ | | Law of Implication: 6 |
| | 8.1. $\neg P(a)$ | Assumption | |
| | 8.2. $Q(a)$ | Modus Ponens: 8.1, 7 | |
| | 8.3. $R(a)$ | Modus Ponens: 8.2, 5 | |
| 8. | $\neg P(a) \to R(a)$ | | Direct Proof |
| 9. | $\neg\neg P(a) \vee R(a)$ | | Law of Implication: 8 |
| 10. | $P(a) \vee R(a)$ | | Double Negation: 9 |
| 11. | $\exists x\ (P(x) \vee R(x))$ | | Intro $\exists$: 10 |

**English proof:** Since we are given that everything (in the domain) is either a $P$ or a $Q$, we know that $a$ must be a $P$ or a $Q$. This is equivalent to the claim that, if $a$ is not a $P$, then it is a $Q$. Similarly, we are given that everything is either not a $Q$ or is an $R$. This is equivalent to the claim that if $a$ is a Q, then it is an $R$.

Now, suppose that $a$ is not a P. From our first equivalence above, this means $a$ must be a $Q$. Then, from our second equivalence, $a$ must be an $R$.

The result of the prior paragraph (if $a$ is not a $P$, then it is an $R$) is equivalent to the claim that $a$ is either a $P$ or an $R$. This proves that there is some element that is either a P or an R.

# 6. 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.