CSE 390Z: Mathematics for Computation Workshop

Week 3 Workshop Problems Solutions

Conceptual Review

(a) Inference Rules:

Introduce ∨:	$\frac{A}{\therefore\ A\vee B,\ B\vee A}$	Eliminate ∨:	$\frac{A\vee B\ ;\ \neg A}{\therefore\ B}$
Introduce ∧:	$\frac{A\ ;\ B}{\therefore\ A\wedge B}$	Eliminate ∧:	$\frac{A\wedge B}{\therefore\ A\ ,\ B}$
Direct Proof:	$\frac{A\Rightarrow B}{\therefore\ A\rightarrow B}$	Modus Ponens:	$\frac{A\ ;\ A\rightarrow B}{\therefore\ B}$
Intro ∃:	$\frac{P(c) \text{ for some } c}{\therefore\ \exists x P(x)}$	Eliminate ∃:	$\frac{\exists x P(x)}{\therefore\ P(c) \text{ for a fresh } c}$
Intro ∀:	$\frac{P(a);\ a \text{ is arbitrary}}{\therefore\ \forall x P(x)}$	Eliminate ∀:	$\frac{\forall x P(x)}{\therefore\ P(a);\ a \text{ is arbitrary}}$

(b) Given $A \wedge B$, prove $A \vee B$

Solution:

1. $A \wedge B$ (Given)
2. A (Elim ∧: 1.)
3. $A \vee B$ (Intro ∨: 2.)

Given $P \rightarrow R$, $R \rightarrow S$, prove $P \rightarrow S$.

1. $P \rightarrow R$ (Given)
2. $R \rightarrow S$ (Given)
   3.1 P (Assumption)
   3.2 R (Modus Ponens: 3.1, 1)
   3.3 S (Modus Ponens: 3.2, 2)
3. $P \rightarrow S$ (Direct Proof Rule; 3.1-3.3)

(c) How do you prove a "for all" statement in an English proof? E.g. prove $\forall x P(x)$. How do you prove a "there exists" statement? E.g. prove $\exists x P(x)$.

Solution:

To prove "for all", we show that for any **arbitrary** a in the domain, $P(a)$ holds. To prove "there exists", we show that for some specific a in the domain, $P(a)$ holds.

(d) What's the definition of "a divides b"?

Solution:

$a \mid b \leftrightarrow \exists k \in \mathbb{Z}\ (b = ka)$

1. Translations with Integers

Translate the following English sentences to predicate logic. The domain is integers, and you may use $=$, $\neq$, and $>$ as predicates. Assume the predicates Prime, Composite, and Even have been defined appropriately.
Note: Composite numbers are ones that have at least 2 factors (the opposite of prime).

(a) 2 is prime.

Solution:

Prime(2)

(b) Every **positive** integer is prime or composite, but not both.

Solution:

$\forall x\ ((x > 0) \rightarrow (\text{Prime}(x) \oplus \text{Composite}(x)))$

OR

$\forall x\ ((x > 0) \rightarrow [(\text{Prime}(x) \land \neg\text{Composite}(x)) \lor (\neg\text{Prime}(x) \land \text{Composite}(x))])$

(c) There is **exactly one** even prime.

Solution:

$\exists x((\text{Even}(x) \land \text{Prime}(x) \land \forall y[(\text{Even}(y) \land \text{Prime}(y)) \rightarrow (y = x)])$

OR

$\exists x((\text{Even}(x) \land \text{Prime}(x) \land \forall y[(y \neq x) \rightarrow \neg(\text{Even}(y) \land \text{Prime}(y))])$

(d) 2 is the only even prime.

Solution:

$\forall x\ ((x = 2) \leftrightarrow \text{Prime}(x) \land \text{Even}(x))$

(e) Some, but not all, composite integers are even.

Solution:

$\exists x(\text{Composite}(x) \land \text{Even}(x)) \land \neg\forall x(\text{Composite}(x) \rightarrow \text{Even}(x))$

OR

$\exists x(\text{Composite}(x) \land \text{Even}(x)) \land \exists x(\text{Composite}(x) \land \neg\text{Even}(x))$

2. Formal Proofs: Modus Ponens

(a) Prove that given $p \rightarrow q$, $\neg s \rightarrow \neg q$, and p, we can conclude s.

Solution:

1. $p \to q$ (Given)
2. $\neg s \to \neg q$ (Given)
3. p (Given)
4. q (Modus Ponens; 1,3)
5. $q \to s$ (Contrapositive; 2)
6. s (Modus Ponens; 5,4)

(b) Prove that given $\neg(p \lor q) \to s$, $\neg p$, and $\neg s$, we can conclude q.

Solution:

1. $\neg(p \lor q) \to s$ (Given)
2. $\neg p$ (Given)
3. $\neg s$ (Given)
4. $\neg s \to \neg\neg(p \lor q)$ (Contrapositive; 1)
5. $\neg s \to (p \lor q)$ (Double Negation; 4)
6. $p \lor q$ (Modus Ponens; 3,5)
7. q (Elim $\lor$; 6,2)

3. Formal Proofs: Direct Proof Rule

(a) Prove that given $p \to q$, we can conclude $(p \land r) \to q$

Solution:

1. $p \to q$ (Given)
   2.1 $p \land r$ (Assumption)
   2.2 p (Elim $\land$; 2.1)
   2.3 q (Modus Ponens; 2.2, 1.)
2. $(p \land r) \to q$ (Direct proof rule; 2.1-2.3)

(b) Prove that given $p \lor q$, $q \to r$, and $r \to s$, we can conclude $\neg p \to s$.

Solution:

1. $p \lor q$ (Given)
2. $q \to r$ (Given)
3. $r \to s$ (Given)
   4.1 $\neg p$ (Assumption)
   4.2 q (Elim $\lor$; 1, 4.1)
   4.3 r (Modus Ponens; 4.2, 2)
   4.4 s (Modus Ponens; 4.3, 3)
4. $\neg p \to s$ (Direct proof rule; 4.1-4.4)

4. Predicate Logic Formal Proof

(a) Prove that $\forall x P(x) \rightarrow \exists x P(x)$. You may assume that the domain is nonempty.

Solution:

1.1. $\forall x P(x)$ (Assumption)

1.2. $P(a)$ (Elim $\forall$: 1.1)

1.3. $\exists x P(x)$ (Intro $\exists$: 1.2)

1. $\forall x P(x) \rightarrow \exists x P(x)$ (Direct Proof Rule, from 1.1-1.3)

(b) Given $\forall x(T(x) \rightarrow M(x))$ and $\exists x(T(x))$, prove that $\exists x(M(x))$.

Solution:

1. $\forall x(T(x) \rightarrow M(x))$ (Given)
2. $\exists x(T(x))$ (Given)
   Let r be the object that satisfies $T(r)$
3. $T(r)$ ($\exists$ elimination, from 2)
4. $T(r) \rightarrow M(r)$ ($\forall$ elimination, from 1)
5. $M(r)$ (Modus ponens, from 3 and 4)
6. $\exists x(M(x))$ ($\exists$ introduction, from 5)

(c) Given $\forall x(P(x) \rightarrow Q(x))$, prove that $(\exists x P(x)) \rightarrow (\exists y Q(y))$.

Solution:

1. $\forall x(P(x) \rightarrow Q(x))$ (Given)

2.1. $\exists x(P(x))$ (Assumption)

Let r be the object that satisfies $P(r)$

2.2. $P(r)$ ($\exists$ elimination, from 2.1)

2.3. $P(r) \rightarrow Q(r)$ ($\forall$ elimination, from 1)

2.4. $Q(r)$ (Modus Ponens, from 2.2 and 2.3)

2.5. $\exists y(Q(y))$ ($\exists$ introduction, from 2.4)

2. $(\exists x P(x)) \rightarrow (\exists y Q(y))$ (Direct Proof Rule, from 2.1-2.5)

5. A Rational Conclusion

Note: This problem will walk you through the steps of an English proof. If you feel comfortable writing the proof already, feel free to jump directly to part (h).

Let the predicate Rational(x) be defined as $\exists a \exists b(\text{Integer}(a) \wedge \text{Integer}(b) \wedge b \neq 0 \wedge x = \frac{a}{b})$. Prove the following claim:

$$\forall x \forall y(\text{Rational}(x) \wedge \text{Rational}(y) \wedge (y \neq 0) \rightarrow \text{Rational}(\frac{x}{y}))$$

(a) Translate the claim to English.

Solution:

If x is rational and $y \neq 0$ is rational, then $\frac{x}{y}$ is rational.

(b) State the givens and declare any arbitrary variables you need to use.
Hint: there are no givens in this problem.

Solution:

Let x and y be arbitrary.

(c) State the assumptions you're making.
Hint: assume everything on the left side of the implication.

Solution:

Suppose x and y are rational numbers and that $y \neq 0$.

(d) Unroll the predicate definitions from your assumptions.

Solution:

Since x and y are rational numbers, by definition there are integers a, b, n, m with $b, n \neq 0$ such that $x = \frac{a}{b}$ and $y = \frac{m}{n}$.

(e) Manipulate what you have towards your goal (might be easier to do the next step first).

Solution:

Then $\frac{x}{y} = \frac{a/b}{m/n} = \frac{a \cdot n}{b \cdot m}$. Let $p = a \cdot n$ and $q = bm$. Note that since $y \neq 0$, m cannot be 0, and since $b \neq 0$ then $q \neq 0$. Because a, b, m, n are integers, $a \cdot n$ and $b \cdot m$ are integers.

(f) Reroll into your predicate definitions.

Solution:

Since $\frac{x}{y} = \frac{p}{q}$, p, q are integers, and $q \neq 0$, $\frac{x}{y}$ is rational.

(g) State your final claim.

Solution:

Because x and y were arbitrary, for any rational numbers x and y with $y \neq 0$, $\frac{x}{y}$ is rational.

(h) Now take these proof parts and assemble them into one cohesive English proof.

Solution:

Let x and y be arbitrary rational numbers with $y \neq 0$. Since x and y are rational numbers, by definition there are integers a, b, n, m with $b, n \neq 0$ such that $x = \frac{a}{b}$ and $y = \frac{m}{n}$. Then $\frac{x}{y} = \frac{a/b}{m/n} = \frac{a \cdot n}{b \cdot m}$. Let $p = a \cdot n$ and $q = bm$. Note that since $y \neq 0$, m cannot be 0, and since $b \neq 0$ then $q \neq 0$. Because a, b, m, n are integers, $a \cdot n$ and $b \cdot m$ are integers. Since $\frac{x}{y} = \frac{p}{q}$, p, q are integers, and $q \neq 0$, $\frac{x}{y}$ is rational. Because x and y were arbitrary, for any rational numbers x and y with $y \neq 0$ $\frac{x}{y}$ is rational.

6. Oddly Even

(a) Write a formal proof to show: If n, m are odd, then $n + m$ is even.

Let the predicates Odd(x) and Even(x) be defined as follows where the domain of discourse is integers:

$$\text{Odd}(x) := \exists y\ (x = 2y + 1)$$
$$\text{Even}(x) := \exists y\ (x = 2y)$$

Solution:

1.	Let x be an arbitrary integer.	
2.	Let y be an arbitrary integer.	
3.1.	$\text{Odd}(x) \land \text{Odd}(y)$	[Assumption]
3.2.	$\text{Odd}(x)$	[Elim $\land$: 3.1]
3.3.	$\exists k\ (x = 2k + 1)$	[Definition of Odd, 3.2]
3.4.	$x = 2k + 1$	[Elim $\exists$: 3.3]
3.5.	$\text{Odd}(y)$	[Elim $\land$: 3.1]
3.6.	$\exists k\ (y = 2k + 1)$	[Definition of Odd, 3.5]
3.7.	$y = 2j + 1$	[Elim $\exists$: 3.7]
3.8.	$x + y = 2k + 1 + 2j + 1$	[Algebra: 3.4, 3.7]
3.9.	$x + y = 2(k + j + 1)$	[Algebra: 3.8]
3.10.	$\exists r\ (x + y = 2r)$	[Intro $\exists$: 3.9]
3.11.	$\text{Even}(x + y)$	[Definition of Even, 3.10]
3.	$\text{Odd}(x) \land \text{Odd}(y) \to \text{Even}(x + y)$	[Direct Proof Rule]
4.	$\forall m(\text{Odd}(x) \land \text{Odd}(m) \to \text{Even}(x + m))$	[Intro $\forall$: 2,3]
5.	$\forall n \forall m(\text{Odd}(n) \land \text{Odd}(m) \to \text{Even}(n + m))$	[Intro $\forall$: 1,4]

(b) Prove the same statement from part (a) using an English proof.

Solution:

Let n, m be arbitrary odd integers. Then by definition of odd, $n = 2k + 1$ for some integer k. Similarly by definition of odd, $m = 2j + 1$ for some integer j. Then $n + m = 2k + 1 + 2j + 1 = 2k + 2j + 2 = 2(k + j + 1)$. Then by definition, $n + m$ is even.

7. Divisibility Proof

Let the domain of discourse be integers. Consider the following claim:

$$\forall n \forall d \ ((d \mid n) \rightarrow (-d \mid n))$$

(a) Translate the claim into English.

Solution:

For integers n, d, if $d \mid n$, then $-d \mid n$.

(b) Write a formal proof to show that the claim holds.

Solution:

1. Let n be an arbitrary integer.
2. Let d be an arbitrary integer.
   - 3.1. $d \mid n$ (Assumption)
   - 3.2. $\exists k \ (n = kd)$ (Definition of divides, from 3.1)
   - 3.3. $n = jd$ (∃ elimination, from 3.2)
   - 3.4. $n = (-d)(-j)$ (Algebra, from 3.3)
   - 3.5. $\exists k \ (n = k(-d))$ (Intro ∃, from 3.4)
   - 3.6. $-d \mid n$ (Definition of divides, from 3.5)
3. $(d \mid n) \rightarrow (-d \mid n)$ (Direct Proof Rule, from 3.1-3.6)
4. $\forall d \ ((d \mid n) \rightarrow (-d \mid n))$ (Intro ∀, from 3)
5. $\forall n \forall d \ ((d \mid n) \rightarrow (-d \mid n))$ (Intro ∀, from 4)

(c) Translate your proof to English.

Solution:

Let d, n be arbitrary integers, and suppose $d|n$. By definition of divides, there exists some integer k such that $n = dk = 1 \cdot dk$. Note that $-1 \cdot -1 = 1$. Substituting, we see $n = (-1)(-1)dk$. Rearranging, we have $n = (-d)(-1 \cdot k)$. Since k is an integer, $-1 \cdot k$ is an integer because the integers are closed under multiplication. So, by definition of divides, $-d|n$. Since d and n were arbitrary, it follows that for any integers d and n, if $d|n$, then $-d|n$.

8. Challenge: Divides Proof

Write an English proof to prove that if k is an odd integer, then $4 \mid k^2 - 1$.

Solution:

Let k be an arbitrary odd integer. Then by definition of odd, $k = 2j + 1$ for some integer j. Then $k^2 - 1 = (2j+1)^2 - 1 = 4j^2 + 4j + 1 - 1 = 4j^2 + 4j = 4(j^2 + j)$. Then by definition of divides, $4 \mid k^2 - 1$.

9. Challenge: Formal Proof

Given $\forall x\ (P(x) \lor Q(x))$ and $\forall y\ (\neg Q(y) \lor R(y))$, prove $\exists x\ (P(x) \lor R(x))$. You may assume that the domain is not empty.

Solution:

1.	$\forall x\ (P(x) \lor Q(x))$	[Given]
2.	$\forall y\ (\neg Q(y) \lor R(y))$	[Given]
3.	$P(a) \lor Q(a)$	[Elim $\forall$: 1]
4.	$\neg Q(a) \lor R(a)$	[Elim $\forall$: 2]
5.	$Q(a) \to R(a)$	[Law of Implication: 4]
6.	$\neg\neg P(a) \lor Q(a)$	[Double Negation: 3]
7.	$\neg P(a) \to Q(a)$	[Law of Implication: 5]
	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.	$\neg\neg P(a) \lor R(a)$	[Law of Implication: 8]
10.	$P(a) \lor R(a)$	[Double Negation: 9]
11.	$\exists x\ (P(x) \lor R(x))$	[Intro $\exists$: 10]