CSE 20 Discussion: Week 6

Quantified statements and proof strategies

Review (Week 4): conditional statements

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

- The only way to make $p \to q$ false is to have p true and q false. The **hypothesis** is p; the **conclusion** is q.
- **Converse** $q \to p$, **inverse** $\neg p \to \neg q$, **contrapositive** $\neg q \to \neg p$. Only the contrapositive is logically equivalent to $p \to q$.
- Useful equivalences: $p \to q \equiv \neg p \vee q \qquad \neg(p \to q) \equiv p \wedge \neg q$.
- In English, $p \to q$ may be read "if p, then q", "p is sufficient for q", "q is necessary for p", or "p only if q".

Review (Week 4): predicates and quantifiers

- A **predicate** is a function from a given set (domain) to $\{T, F\}$. For a predicate on a product domain we write, e.g., $L(\ (s, n)\ )$.
- $\forall x \in U\ P(x)$: "$P(x)$ for all values of x in the domain U".
  $\exists x \in U\ P(x)$: "there exists an element x in U such that $P(x)$".
- A **counterexample** of $\forall x P(x)$ is an element where $P(x) = F$; a **witness** of $\exists x P(x)$ is an element where $P(x) = T$.
- **De Morgan's laws for quantifiers**: $\neg\forall x P(x) \equiv \exists x\,(\neg P(x))$
  $\neg\exists x Q(x) \equiv \forall x\,(\neg Q(x))$.
  Applied repeatedly, they move a negation past each quantifier, switching $\forall$ and $\exists$.
- **Order matters** for alternating quantifiers.
  $\forall s \in S\ \exists n \in \mathbb{N}\ (basecount(\ (s, \mathtt{U})\ ) = n)$ is true (each strand may have its own n), while $\exists n \in \mathbb{N}\ \forall s \in S\ (basecount(\ (s, \mathtt{U})\ ) = n)$ is false (a single n must work for every strand).

Review (Week 5): evidence for quantified statements

	to show it is **true**	to show it is **false**
$\forall x\, P(x)$	universal generalization (or, on a finite domain, check every element: **exhaustion**)	a **counterexample**
$\exists x\, P(x)$	a **witness**	show $\forall x\, \neg P(x)$

Proof by universal generalization: To prove that $\forall x\, P(x)$ is true, we can take an arbitrary element e from the domain of quantification and show that $P(e)$ is true, without making any assumptions about e other than that it comes from the domain. An **arbitrary** element of a set or domain is a fixed but unknown element from that set.

- Examples, however many, never prove a universal statement over an infinite domain.
- When a witness is needed inside a universal statement ($\forall x\, \exists y$), the witness may depend on the arbitrary element.

Review (Week 5): proof strategies

- **Direct proof** of $p \to q$: assume p is true and use that assumption to show q is true.
- **Contrapositive proof** of $p \to q$: assume q is false and use that assumption to show p is also false.
- **Disjunction** $p \vee q$: rewrite it as $\neg p \to q$ and use a direct or contrapositive proof.
- **Proof by cases**: if $p_1 \vee p_2$ is true, $p_1 \to q$ is true, and $p_2 \to q$ is true, then q is true. The cases must cover every possibility.
- **Conjunction** $p \wedge q$: prove p (subgoal 1) and prove q (subgoal 2). To show $p \wedge q$ is false, it is enough to prove $\neg p$ (or $\neg q$).

Proof template: Consider . . . , an **arbitrary** . . . . **Assume** . . . , we **want to show** that . . . . Which is what was needed, so the proof is complete □. *or, in other words:* Let . . . be an **arbitrary** . . . . **Assume** . . . , **WTS** that . . . **QED**.

Review (Week 5): sets

- $A = B$ means $\forall x\,(x \in A \leftrightarrow x \in B)$; $A \subseteq B$ means $\forall x\,(x \in A \rightarrow x \in B)$; $A \subsetneq B$ means $(A \subseteq B) \wedge (A \neq B)$.
- To show $A \subseteq B$: let e be an arbitrary element, assume $e \in A$, and show $e \in B$.
- To show $A = B$: prove the two subgoals $A \subseteq B$ and $B \subseteq A$.
- To show $A \neq B$: show $\exists x\,(x \in A \oplus x \in B)$, i.e. find an element in exactly one of the sets.
- $A \cup B = \{x \mid x \in A \vee x \in B\}$, $A \cap B = \{x \mid x \in A \wedge x \in B\}$, $A - B = \{x \mid x \in A \wedge x \notin B\}$.
- $\mathcal{P}(U) = \{X \mid X \subseteq U\}$. Note the difference between $\in$ and $\subseteq$: $X \in \mathcal{P}(U)$ exactly when $X \subseteq U$.

Review (Week 5): numbers

- **Facts**: (1) $+$ and $\cdot$ are commutative and associative; (2) the product of two positive numbers is positive, of two negative numbers is positive, and of a positive and a negative number is negative; (3) sums, products, and differences of integers are integers; (4) no integer lies strictly between x and $x+1$; (5) for positive integers x, y: $xy \geq x$ and $xy \geq y$.
- For integers a, b with a nonzero, a **divides** b means there is an integer c such that $b = ac$. We write $F(\ (a,b)\ )$ or $a \mid b$; the domain is $\mathbb{Z}^{\neq 0} \times \mathbb{Z}$.
- n is **even** means $n = 2a$ for some integer a; n is **odd** means $n = 2a+1$ for some integer a.
- An integer p greater than 1 is **prime** means the only positive factors of p are 1 and p.

Part 1: Quantified statements

Q1. Order of quantifiers

Recall the predicate L with domain $S \times \mathbb{Z}^+$, where $L(\ (s, n)\ )$ means $rnalen(s) = n$.

(a) Is $\forall n \in \mathbb{Z}^+\ \exists s \in S\ L(\ (s, n)\ )$ true or false? Prove your answer.

(b) Write the negation of $\exists n \in \mathbb{Z}^+\ \forall s \in S\ L(\ (s, n)\ )$ so that the negation is applied only to L. Decide which of the statement and its negation is true, and prove it.

▸ Definitions

Q1. Order of quantifiers

Recall the predicate L with domain $S \times \mathbb{Z}^+$, where $L(\ (s, n)\ )$ means $rnalen(s) = n$.

(a) Is $\forall n \in \mathbb{Z}^+\ \exists s \in S\ L(\ (s, n)\ )$ true or false? Prove your answer.

True. Towards universal generalization, let n be an arbitrary positive integer. WTS $\exists s \in S\ L(\ (s, n)\ )$. Consider the strand $s = \texttt{AA} \cdots \texttt{A}$ consisting of n copies of `A`. It is in S: $\texttt{A} \in S$ by the basis step, and each of the $n - 1$ applications of the recursive step appends one more `A`. By the basis step of $rnalen$, $rnalen(\texttt{A}) = 1$, and each application of the recursive step adds 1, so $rnalen(s) = n$. Thus s is a witness. QED

(b) Write the negation of $\exists n \in \mathbb{Z}^+\ \forall s \in S\ L(\ (s, n)\ )$ so that the negation is applied only to L. Decide which of the statement and its negation is true, and prove it.

Q1. Order of quantifiers

Recall the predicate L with domain $S \times \mathbb{Z}^+$, where $L(\ (s, n)\ )$ means $rnalen(s) = n$.

(a) Is $\forall n \in \mathbb{Z}^+\ \exists s \in S\ L(\ (s, n)\ )$ true or false? Prove your answer.

True. Towards universal generalization, let n be an arbitrary positive integer. WTS $\exists s \in S\ L(\ (s, n)\ )$. Consider the strand $s = \texttt{AA} \cdots \texttt{A}$ consisting of n copies of A. It is in S: $\texttt{A} \in S$ by the basis step, and each of the $n - 1$ applications of the recursive step appends one more A. By the basis step of $rnalen$, $rnalen(\texttt{A}) = 1$, and each application of the recursive step adds 1, so $rnalen(s) = n$. Thus s is a witness. QED

(b) Write the negation of $\exists n \in \mathbb{Z}^+\ \forall s \in S\ L(\ (s, n)\ )$ so that the negation is applied only to L. Decide which of the statement and its negation is true, and prove it.

$$\neg\exists n \in \mathbb{Z}^+\ \forall s \in S\ L(\ (s, n)\ ) \equiv \forall n \in \mathbb{Z}^+\ \neg\forall s \in S\ L(\ (s, n)\ )$$

$$\equiv \boxed{\forall n \in \mathbb{Z}^+\ \exists s \in S\ \neg L(\ (s, n)\ )}$$

The negation is true, so the original statement is false. Let n be an arbitrary positive integer; WTS some strand does not have length n. Case $n = 1$: the witness AA works, since $rnalen(\texttt{AA}) = 1 + rnalen(\texttt{A}) = 2 \neq 1$. Case $n \neq 1$: the witness A works, since $rnalen(\texttt{A}) = 1 \neq n$. QED

▸ Definitions

Q1. Order of quantifiers

(c) Express symbolically: "There are at least two different RNA strands that have the same number of `A`s." Is the statement true?

▸ Definitions

Q1. Order of quantifiers

(c) Express symbolically: "There are at least two different RNA strands that have the same number of As." Is the statement true?

$$\exists s_1 \in S\ \exists s_2 \in S\ \big(\neg(s_1 = s_2) \wedge basecount(\ (s_1, \mathtt{A})\ ) = basecount(\ (s_2, \mathtt{A})\ )\big)$$

True. Consider the witness $s_1 = \mathtt{C}$, $s_2 = \mathtt{G}$. These are different strands, and by the basis step of $basecount$, $basecount(\ (\mathtt{C}, \mathtt{A})\ ) = 0 = basecount(\ (\mathtt{G}, \mathtt{A})\ )$.

The conjunct $\neg(s_1 = s_2)$ is essential: without it, choosing $s_1 = s_2$ would make the statement true for a trivial reason.

▸ Definitions

Part 2: Proofs about sets

Q2. Membership versus subset; the empty set

For each statement, write it symbolically, decide whether it is true or false, and give the evidence: a witness, a counterexample, or a proof by universal generalization.

(a) For some set Y, $\emptyset \in Y$.

(b) For every set Y, $\emptyset \in Y$.

(c) The empty set is a subset of every set.

(d) The empty set is a proper subset of every set.

▸ Definitions

Q2. Membership versus subset; the empty set

For each statement, write it symbolically, decide whether it is true or false, and give the evidence: a witness, a counterexample, or a proof by universal generalization.

(a) For some set Y, $\emptyset \in Y$.

$\exists Y\,(\emptyset \in Y)$. True. Witness: $Y = \{\emptyset\}$, whose only element is $\emptyset$.

(b) For every set Y, $\emptyset \in Y$.

(c) The empty set is a subset of every set.

(d) The empty set is a proper subset of every set.

▸ Definitions

Q2. Membership versus subset; the empty set

For each statement, write it symbolically, decide whether it is true or false, and give the evidence: a witness, a counterexample, or a proof by universal generalization.

(a) For some set Y, $\emptyset \in Y$.

$\exists Y\,(\emptyset \in Y)$. True. Witness: $Y = \{\emptyset\}$, whose only element is $\emptyset$.

(b) For every set Y, $\emptyset \in Y$.

$\forall Y\,(\emptyset \in Y)$. False. Counterexample: $Y = \mathbb{Z}$. Every element of $\mathbb{Z}$ is an integer, and $\emptyset$ is not an integer, so $\emptyset \notin \mathbb{Z}$.

(c) The empty set is a subset of every set.

(d) The empty set is a proper subset of every set.

Q2. Membership versus subset; the empty set

For each statement, write it symbolically, decide whether it is true or false, and give the evidence: a witness, a counterexample, or a proof by universal generalization.

(a) For some set Y, $\emptyset \in Y$.

$\exists Y\,(\emptyset \in Y)$. True. Witness: $Y = \{\emptyset\}$, whose only element is $\emptyset$.

(b) For every set Y, $\emptyset \in Y$.

$\forall Y\,(\emptyset \in Y)$. False. Counterexample: $Y = \mathbb{Z}$. Every element of $\mathbb{Z}$ is an integer, and $\emptyset$ is not an integer, so $\emptyset \notin \mathbb{Z}$.

(c) The empty set is a subset of every set.

$\forall X\,(\emptyset \subseteq X)$, i.e. $\forall X\ \forall x\,(x \in \emptyset \to x \in X)$. True. Let X be an arbitrary set and x an arbitrary element. The hypothesis $x \in \emptyset$ is false, because $\emptyset$ has no elements, so the conditional $x \in \emptyset \to x \in X$ is true. QED

(d) The empty set is a proper subset of every set.

Q2. Membership versus subset; the empty set

For each statement, write it symbolically, decide whether it is true or false, and give the evidence: a witness, a counterexample, or a proof by universal generalization.

(a) For some set Y, $\emptyset \in Y$.

$\exists Y\,(\emptyset \in Y)$. True. Witness: $Y = \{\emptyset\}$, whose only element is $\emptyset$.

(b) For every set Y, $\emptyset \in Y$.

$\forall Y\,(\emptyset \in Y)$. False. Counterexample: $Y = \mathbb{Z}$. Every element of $\mathbb{Z}$ is an integer, and $\emptyset$ is not an integer, so $\emptyset \notin \mathbb{Z}$.

(c) The empty set is a subset of every set.

$\forall X\,(\emptyset \subseteq X)$, i.e. $\forall X\ \forall x\,(x \in \emptyset \to x \in X)$. True. Let X be an arbitrary set and x an arbitrary element. The hypothesis $x \in \emptyset$ is false, because $\emptyset$ has no elements, so the conditional $x \in \emptyset \to x \in X$ is true. QED

(d) The empty set is a proper subset of every set.

$\forall X\,(\emptyset \subseteq X \wedge \emptyset \neq X)$. False. Counterexample: $X = \emptyset$. Then $\emptyset \neq X$ is false, so the conjunction is false.

▸ Definitions

Q3. Subsets and power sets - Unpacking defintions

Let $W = \mathcal{P}(\{1, 2, 3, 4, 5\})$. **Prove** or **disprove**:
$\forall A \in W \ \forall B \in W \ \big(A \subseteq B \to \mathcal{P}(A) \subseteq \mathcal{P}(B)\big)$

(a) Let $A, B \in W$ be arbitrary and assume $A \subseteq B$. Using the definitions of $\subseteq$ and $\mathcal{P}$, rewrite the statement you need to show until it is expressed in terms of membership ($\in$) only.

(b) Prove or disprove the statement.

Q3. Subsets and power sets - Unpacking defintions

Let $W = \mathcal{P}(\{1, 2, 3, 4, 5\})$. **Prove** or **disprove**:
$\forall A \in W \; \forall B \in W \; \big(A \subseteq B \to \mathcal{P}(A) \subseteq \mathcal{P}(B)\big)$

(a) Let $A, B \in W$ be arbitrary and assume $A \subseteq B$. Using the definitions of $\subseteq$ and $\mathcal{P}$, rewrite the statement you need to show until it is expressed in terms of membership ($\in$) only.

WTS $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, i.e. $\forall X \, \big(X \in \mathcal{P}(A) \to X \in \mathcal{P}(B)\big)$, i.e. $\forall X \, (X \subseteq A \to X \subseteq B)$, i.e. $\boxed{\forall X \, \big(\forall y \, (y \in X \to y \in A) \to \forall x \, (x \in X \to x \in B)\big)}$.

(b) Prove or disprove the statement.

Q3. Subsets and power sets - Unpacking defintions

Let $W = \mathcal{P}(\{1, 2, 3, 4, 5\})$. **Prove** or **disprove**:
$\forall A \in W \; \forall B \in W \; \big(A \subseteq B \to \mathcal{P}(A) \subseteq \mathcal{P}(B)\big)$

(a) Let $A, B \in W$ be arbitrary and assume $A \subseteq B$. Using the definitions of $\subseteq$ and $\mathcal{P}$, rewrite the statement you need to show until it is expressed in terms of membership ($\in$) only.

WTS $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, i.e. $\forall X \, \big(X \in \mathcal{P}(A) \to X \in \mathcal{P}(B)\big)$, i.e. $\forall X \, (X \subseteq A \to X \subseteq B)$, i.e. $\boxed{\forall X \, \big(\forall y \, (y \in X \to y \in A) \to \forall x \, (x \in X \to x \in B)\big)}$.

(b) Prove or disprove the statement.

$\boxed{\text{True.}}$ Let $A, B \in W$ be arbitrary. Towards a direct proof, assume $A \subseteq B$; WTS $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Let X be arbitrary and assume $X \in \mathcal{P}(A)$, i.e. $X \subseteq A$; WTS $X \in \mathcal{P}(B)$, i.e. $X \subseteq B$. Let x be arbitrary and assume $x \in X$. Since $X \subseteq A$, $x \in A$; since $A \subseteq B$, $x \in B$. Hence $X \subseteq B$, so $X \in \mathcal{P}(B)$. QED

Q3. Subsets and power sets - Unpacking defintions

(c) The domain W is finite. Could the statement be proved by exhaustion? Why is universal generalization preferable?

Q3. Subsets and power sets - Unpacking defintions

(c) The domain W is finite. Could the statement be proved by exhaustion? Why is universal generalization preferable?

Yes in principle: W has $2^5 = 32$ elements, so there are $32 \cdot 32 = 1024$ pairs (A, B) to check. Universal generalization handles all of them in one argument, and the same argument works for any sets, finite or not.

Q4. Direct and contrapositive proof strategies

Let $W = \mathcal{P}(\{1, 2, 3, 4, 5\})$. **Prove** or **disprove**:
$\forall A \in W \ \forall B \in W \ \big(\mathcal{P}(A) = \mathcal{P}(B) \to A = B\big)$

(a) Write the converse and the contrapositive of the conditional $\mathcal{P}(A) = \mathcal{P}(B) \to A = B$. Then express the conditional in English using "only if".

(b) After universal generalization, what do we assume and what do we need to show in a direct proof? In a proof by contrapositive? Write $A \neq B$ using a quantifier.

Q4. Direct and contrapositive proof strategies

Let $W = \mathcal{P}(\{1, 2, 3, 4, 5\})$. **Prove** or **disprove**:
$\forall A \in W \ \forall B \in W \ \big(\mathcal{P}(A) = \mathcal{P}(B) \to A = B\big)$

(a) Write the converse and the contrapositive of the conditional $\mathcal{P}(A) = \mathcal{P}(B) \to A = B$. Then express the conditional in English using "only if".

Converse: $A = B \to \mathcal{P}(A) = \mathcal{P}(B)$. Contrapositive: $A \neq B \to \mathcal{P}(A) \neq \mathcal{P}(B)$.
"$\mathcal{P}(A) = \mathcal{P}(B)$ only if $A = B$."

(b) After universal generalization, what do we assume and what do we need to show in a direct proof? In a proof by contrapositive? Write $A \neq B$ using a quantifier.

Q4. Direct and contrapositive proof strategies

Let $W = \mathcal{P}(\{1, 2, 3, 4, 5\})$. **Prove** or **disprove**:
$\forall A \in W \; \forall B \in W \; \big(\mathcal{P}(A) = \mathcal{P}(B) \to A = B\big)$

(a) Write the converse and the contrapositive of the conditional $\mathcal{P}(A) = \mathcal{P}(B) \to A = B$. Then express the conditional in English using "only if".

Converse: $A = B \to \mathcal{P}(A) = \mathcal{P}(B)$. Contrapositive: $A \neq B \to \mathcal{P}(A) \neq \mathcal{P}(B)$.
"$\mathcal{P}(A) = \mathcal{P}(B)$ only if $A = B$."

(b) After universal generalization, what do we assume and what do we need to show in a direct proof? In a proof by contrapositive? Write $A \neq B$ using a quantifier.

Direct: assume $\mathcal{P}(A) = \mathcal{P}(B)$; WTS $A = B$.
Contrapositive: assume $A \neq B$, i.e. $\exists x \, (x \in A \oplus x \in B)$; WTS $\mathcal{P}(A) \neq \mathcal{P}(B)$.

▸ Definitions

Q4. Direct and contrapositive proof strategies

(c) Give a direct proof of the statement.

▸ Definitions

Q4. Direct and contrapositive proof strategies

(c) Give a direct proof of the statement.

True. Let $A, B \in W$ be arbitrary. Towards a direct proof, assume $\mathcal{P}(A) = \mathcal{P}(B)$. WTS $A = B$, which we prove as two subgoals.

Subgoal 1: $A \subseteq B$. Every element of A is an element of A, so $A \subseteq A$, and therefore $A \in \mathcal{P}(A)$ by the definition of power set. Since $\mathcal{P}(A) = \mathcal{P}(B)$, we get $A \in \mathcal{P}(B)$, which means $A \subseteq B$.

Subgoal 2: $B \subseteq A$. Similarly, $B \subseteq B$ gives $B \in \mathcal{P}(B) = \mathcal{P}(A)$, which means $B \subseteq A$.

Hence $A = B$. QED

▸ Definitions

Q5. Counterexamples

Let $W = \mathcal{P}(\{1, 2, 3, 4, 5\})$. **Prove** or **disprove**:
$\forall A \in W\ \forall B \in W\ \forall C \in W\ \big(A \cup B = A \cup C \to B = C\big)$

(a) List the conditions that a counterexample must satisfy. Then give a counterexample and verify that it satisfies each condition.

(b) Suppose $A \cup B = A \cup C$. Explain why every element that belongs to exactly one of B and C must belong to A.

▸ Definitions

Q5. Counterexamples

Let $W = \mathcal{P}(\{1,2,3,4,5\})$. **Prove** or **disprove**:
$\forall A \in W\ \forall B \in W\ \forall C \in W\ \big(A \cup B = A \cup C \to B = C\big)$

(a) List the conditions that a counterexample must satisfy. Then give a counterexample and verify that it satisfies each condition.

A counterexample is a choice of A, B, C with (1) $A, B, C \in W$, i.e. each is a subset of $\{1,2,3,4,5\}$; (2) $A \cup B = A \cup C$; (3) $B \neq C$.

The statement is false. Take $A = \{1\}$, $B = \{1\}$, $C = \emptyset$. Each is a subset of $\{1,2,3,4,5\}$; $A \cup B = \{1\} = A \cup C$; and $1 \in B$ but $1 \notin C$, so $B \neq C$.

(b) Suppose $A \cup B = A \cup C$. Explain why every element that belongs to exactly one of B and C must belong to A.

Q5. Counterexamples

Let $W = \mathcal{P}(\{1,2,3,4,5\})$. **Prove** or **disprove**:
$\forall A \in W\ \forall B \in W\ \forall C \in W\ \big(A \cup B = A \cup C \to B = C\big)$

(a) List the conditions that a counterexample must satisfy. Then give a counterexample and verify that it satisfies each condition.

A counterexample is a choice of A, B, C with (1) $A, B, C \in W$, i.e. each is a subset of $\{1,2,3,4,5\}$; (2) $A \cup B = A \cup C$; (3) $B \neq C$.

The statement is false. Take $A = \{1\}$, $B = \{1\}$, $C = \emptyset$. Each is a subset of $\{1,2,3,4,5\}$; $A \cup B = \{1\} = A \cup C$; and $1 \in B$ but $1 \notin C$, so $B \neq C$.

(b) Suppose $A \cup B = A \cup C$. Explain why every element that belongs to exactly one of B and C must belong to A.

Suppose $x \in B$ and $x \notin C$ (the other case is symmetric). Then $x \in A \cup B = A \cup C$. Since $x \notin C$, the definition of union gives $x \in A$.

▸ Definitions

Q5. Counterexamples

(c) Prove:

$$\forall A \in W\ \forall B \in W\ \forall C \in W\ \big((A \cup B = A \cup C \wedge A \cap B = A \cap C) \rightarrow B = C\big)$$

▸ Definitions

Q5. Counterexamples

(c) Prove:

$$\forall A \in W\ \forall B \in W\ \forall C \in W\ \big((A \cup B = A \cup C \wedge A \cap B = A \cap C) \to B = C\big)$$

Let $A, B, C \in W$ be arbitrary. Towards a direct proof, assume $A \cup B = A \cup C$ and $A \cap B = A \cap C$. WTS $B = C$, which we prove as two subgoals.

Subgoal 1: $B \subseteq C$. Let x be arbitrary and assume $x \in B$; WTS $x \in C$. We work by cases.

- Case 1: $x \in A$. Then $x \in A \cap B = A \cap C$, so $x \in C$.
- Case 2: $x \notin A$. Then $x \in A \cup B = A \cup C$; since $x \notin A$, we get $x \in C$.

Subgoal 2: $C \subseteq B$. The same argument with the roles of B and C exchanged.

Hence $B = C$. QED

▸ Definitions

Part 3: Proofs about numbers

Q6. Divisibility

Recall that $F(\ (a,b)\ )$ means "a divides b", i.e. $\exists c \in \mathbb{Z}\ (b = ac)$, with domain $\mathbb{Z}^{\neq 0} \times \mathbb{Z}$.
For each statement, write it symbolically, then prove or disprove it.

(a) Every positive factor of an integer is less than or equal to it.

▸ Definitions

Q6. Divisibility

Recall that $F(\ (a,b)\ )$ means "a divides b", i.e. $\exists c \in \mathbb{Z}\ (b = ac)$, with domain $\mathbb{Z}^{\neq 0} \times \mathbb{Z}$.
For each statement, write it symbolically, then prove or disprove it.

(a) Every positive factor of an integer is less than or equal to it.

$\forall b \in \mathbb{Z}\ \forall a \in \mathbb{Z}^+\ \big(F(\ (a,b)\ ) \to a \leq b\big)$. False.

Counterexample: $a = 1$, $b = 0$. Here $1 \in \mathbb{Z}^+$ and $0 \in \mathbb{Z}$; $F(\ (1,0)\ )$ is true with $c = 0$, since $0 = 1 \cdot 0$; but $1 \leq 0$ is false. (Another counterexample: $a = 2$, $b = -6$.)

▸ Definitions

Q6. Divisibility

(b) Every factor of a positive integer is less than or equal to it.

▸ Definitions

Q6. Divisibility

(b) Every factor of a positive integer is less than or equal to it.

$\forall b \in \mathbb{Z}^+ \; \forall a \in \mathbb{Z}^{\neq 0} \; \big(F(\;(a,b)\;) \rightarrow a \leq b\big)$. True.

Let b be an arbitrary positive integer and a an arbitrary nonzero integer. Towards a direct proof, assume $F(\;(a,b)\;)$: there is an integer c with $b = ac$. WTS $a \leq b$. Since $a \neq 0$, there are two cases.

- Case 1: $a < 0$. Then $a < 0 < b$.
- Case 2: $a > 0$. Then $c \neq 0$, since otherwise $b = 0$; and c is not negative, since by Fact 2 the product of a positive and a negative number is negative, while $b > 0$. So c is a positive integer, and Fact 5 gives $b = ac \geq a$.

In both cases $a \leq b$. QED

Q7. Consecutive primes (in-class examples)

Let $Pr(p)$ mean "p is prime". Consider the statement: "There are three consecutive positive integers that are prime."

(a) Write symbolically what must be shown to prove that this statement is false, with the negation applied only to Pr.

(b) A proof lets e be an arbitrary positive integer and considers two cases. Case 1 (e even) shows that $e + 2$ is not prime. A student writes Case 2 as follows: *"Assume e is odd. Then $e + 1$ is even, so 2 is a factor of $e + 1$, and therefore $e + 1$ is not prime."* Identify the flaw and repair the argument.

Q7. Consecutive primes (in-class examples)

Let $Pr(p)$ mean "p is prime". Consider the statement: "There are three consecutive positive integers that are prime."

(a) Write symbolically what must be shown to prove that this statement is false, with the negation applied only to Pr.

The statement is $\exists p \in \mathbb{Z}^+ \ \big(Pr(p) \wedge Pr(p+1) \wedge Pr(p+2)\big)$. Its negation is

$$\boxed{\forall p \in \mathbb{Z}^+ \ \big(\neg Pr(p) \vee \neg Pr(p+1) \vee \neg Pr(p+2)\big)}$$

(b) A proof lets e be an arbitrary positive integer and considers two cases. Case 1 (e even) shows that $e+2$ is not prime. A student writes Case 2 as follows: *"Assume e is odd. Then $e+1$ is even, so 2 is a factor of $e+1$, and therefore $e+1$ is not prime."* Identify the flaw and repair the argument.

Q7. Consecutive primes (in-class examples)

Let $Pr(p)$ mean "p is prime". Consider the statement: "There are three consecutive positive integers that are prime."

(a) Write symbolically what must be shown to prove that this statement is false, with the negation applied only to Pr.

The statement is $\exists p \in \mathbb{Z}^+ \ \big(Pr(p) \wedge Pr(p+1) \wedge Pr(p+2)\big)$. Its negation is

$$\boxed{\forall p \in \mathbb{Z}^+ \ \big(\neg Pr(p) \vee \neg Pr(p+1) \vee \neg Pr(p+2)\big)}$$

(b) A proof lets e be an arbitrary positive integer and considers two cases. Case 1 (e even) shows that $e+2$ is not prime. A student writes Case 2 as follows: *"Assume e is odd. Then $e+1$ is even, so 2 is a factor of $e+1$, and therefore $e+1$ is not prime."* Identify the flaw and repair the argument.

Flaw: a factor of 2 shows $e+1$ is not prime only if $2 \neq e+1$. For $e = 1$, $e+1 = 2$, which is prime.

Repair, by two subcases:

- $e = 1$: then e is not prime, because a prime is greater than 1.
- $e \geq 3$: write $e = 2k+1$ with $k \in \mathbb{Z}$; then $e+1 = 2(k+1)$, so 2 is a positive factor of $e+1$, and $e+1 \geq 4$, so $2 \neq e+1$. Hence $e+1$ is not prime.

In each subcase the disjunction holds.

▸ Definitions

Q7. Consecutive primes (in-class examples)

(c) Is the statement "There are three consecutive odd positive integers that are prime" true? Write it symbolically and give the evidence.

▸ Definitions

Q7. Consecutive primes (in-class examples)

(c) Is the statement "There are three consecutive odd positive integers that are prime" true? Write it symbolically and give the evidence.

$\exists p \in \mathbb{Z}^+ \ \big(p \text{ is odd} \wedge Pr(p) \wedge Pr(p+2) \wedge Pr(p+4)\big)$. **True.**

Witness: $p = 3$. It is a positive integer, and $3 = 2 \cdot 1 + 1$ is odd. The numbers 3, 5, 7 are each greater than 1, and none is divisible by any integer strictly between 1 and itself, so the only positive factors of each are 1 and the number itself: all three are prime.

Appendix: Definitions from the lecture notes

Definitions for Q1

RNA strands: The set of RNA strands S is defined (recursively) by:
Basis Step: $\mathtt{A} \in S, \mathtt{C} \in S, \mathtt{U} \in S, \mathtt{G} \in S$
Recursive Step: If $s \in S$ and $b \in B$, then $sb \in S$
where sb is string concatenation.

rnalen: The function *rnalen* that computes the length of RNA strands in S is defined recursively by:

		$\mathit{rnalen} : S$	$\to \mathbb{Z}^+$
Basis Step:	If $b \in B$ then	$\mathit{rnalen}(b)$	$= 1$
Recursive Step:	If $s \in S$ and $b \in B$, then	$\mathit{rnalen}(sb)$	$= 1 + \mathit{rnalen}(s)$

◂ Back to Q1

Definitions for Q1

The predicate L: L with domain $S \times \mathbb{Z}^+$ is defined by, for $s \in S$ and $n \in \mathbb{Z}^+$,

$$L(\ (s,n)\ ) = \begin{cases} T & \text{if } rnalen(s) = n \\ F & \text{otherwise} \end{cases}$$

In other words, $L(\ (s,n)\ )$ means $rnalen(s) = n$

Quantification: The **universal quantification** of predicate $P(x)$ over domain U is the statement "$P(x)$ for all values of x in the domain U" and is written $\forall x P(x)$ or $\forall x \in U\ P(x)$. The **existential quantification** of predicate $P(x)$ over domain U is the statement "There exists an element x in the domain U such that $P(x)$" and is written $\exists x P(x)$ for $\exists x \in U\ P(x)$.

◂ Back to Q1

Definitions for Q1

Quantifier version of De Morgan's laws: $\neg\forall x P(x) \equiv \exists x\,(\neg P(x))$
$\neg\exists x Q(x) \equiv \forall x\,(\neg Q(x))$

Counterexample and witness: An element for which $P(x) = F$ is called a **counterexample** of $\forall x P(x)$. When there is a counterexample in the domain of predicate P, $\forall x P(x)$ is false. An element for which $P(x) = T$ is called a **witness** of $\exists x P(x)$. When there is a witness in the domain of predicate P, then $\exists x P(x)$ is true.

◂ Back to Q1

Definitions for Q2

Definitions: A **set** is an unordered collection of elements. When A and B are sets, $A = B$ (set equality) means $\forall x(x \in A \leftrightarrow x \in B)$. When A and B are sets, $A \subseteq B$ ("A is a **subset** of B") means $\forall x(x \in A \rightarrow x \in B)$. When A and B are sets, $A \subsetneq B$ ("A is a **proper subset** of B") means $(A \subseteq B) \wedge (A \neq B)$.

◀ Back to Q2

Definitions for Q2

Counterexample and witness: An element for which $P(x) = F$ is called a **counterexample** of $\forall x P(x)$. When there is a counterexample in the domain of predicate P, $\forall x P(x)$ is false. An element for which $P(x) = T$ is called a **witness** of $\exists x P(x)$. When there is a witness in the domain of predicate P, then $\exists x P(x)$ is true.

Proof by universal generalization: To prove that $\forall x\, P(x)$ is true, we can take an arbitrary element e from the domain of quantification and show that $P(e)$ is true, without making any assumptions about e other than that it comes from the domain. An **arbitrary** element of a set or domain is a fixed but unknown element from that set.

◂ Back to Q2

Definitions for Q3

Definitions: A **set** is an unordered collection of elements. When A and B are sets, $A = B$ (set equality) means $\forall x(x \in A \leftrightarrow x \in B)$. When A and B are sets, $A \subseteq B$ ("A is a **subset** of B") means $\forall x(x \in A \rightarrow x \in B)$. When A and B are sets, $A \subsetneq B$ ("A is a **proper subset** of B") means $(A \subseteq B) \wedge (A \neq B)$.

Power set: When U is a set, $\mathcal{P}(U) = \{X \mid X \subseteq U\}$

◀ Back to Q3

Definitions for Q3

Proof by universal generalization: To prove that $\forall x\, P(x)$ is true, we can take an arbitrary element e from the domain of quantification and show that $P(e)$ is true, without making any assumptions about e other than that it comes from the domain. An **arbitrary** element of a set or domain is a fixed but unknown element from that set.

Proof of conditional by direct proof: To prove that the conditional statement $p \to q$ is true, we can assume p is true and use that assumption to show q is true.

◀ Back to Q3

Definitions for Q4

Conditional: The only way to make the conditional statement $p \to q$ false is to have p true and q false. The **hypothesis** (**antecedent**) of $p \to q$ is p; the **conclusion** (**consequent**) of $p \to q$ is q.

The **converse** of $p \to q$ is $q \to p$. The **inverse** of $p \to q$ is $\neg p \to \neg q$. The **contrapositive** of $p \to q$ is $\neg q \to \neg p$.

Conditional $p \to q$ can be said in English as: if p, then q; p is sufficient for q; q when p; q whenever p; p implies q; q follows from p; q is necessary for p; p only if q.

◀ Back to Q4

Definitions for Q4

Definitions: A **set** is an unordered collection of elements. When A and B are sets, $A = B$ (set equality) means $\forall x(x \in A \leftrightarrow x \in B)$. When A and B are sets, $A \subseteq B$ ("A is a **subset** of B") means $\forall x(x \in A \rightarrow x \in B)$. When A and B are sets, $A \subsetneq B$ ("A is a **proper subset** of B") means $(A \subseteq B) \wedge (A \neq B)$.

Power set: When U is a set, $\mathcal{P}(U) = \{X \mid X \subseteq U\}$

◀ Back to Q4

Definitions for Q4

Proof of conditional by direct proof: To prove that the conditional statement $p \to q$ is true, we can assume p is true and use that assumption to show q is true.

Proof of conditional by contrapositive proof: To prove that the implication $p \to q$ is true, we can assume q is false and use that assumption to show p is also false.

Proof of conjunctions with subgoals: To show that $p \wedge q$ is true, we have two subgoals: subgoal (1) prove p is true; and, subgoal (2) prove q is true. To show that $p \wedge q$ is false, it's enough to prove that $\neg p$. To show that $p \wedge q$ is false, it's enough to prove that $\neg q$.

◂ Back to Q4

Definitions for Q5

Definitions: A **set** is an unordered collection of elements. When A and B are sets, $A = B$ (set equality) means $\forall x(x \in A \leftrightarrow x \in B)$. When A and B are sets, $A \subseteq B$ ("A is a **subset** of B") means $\forall x(x \in A \rightarrow x \in B)$. When A and B are sets, $A \subsetneq B$ ("A is a **proper subset** of B") means $(A \subseteq B) \wedge (A \neq B)$.

◂ Back to Q5

Definitions for Q5

Union: When A and B are sets, $A \cup B = \{x \mid x \in A \vee x \in B\}$.

Intersection: When A and B are sets, $A \cap B = \{x \mid x \in A \wedge x \in B\}$.

Set difference: When A and B are sets, $A - B = \{x \mid x \in A \wedge x \notin B\}$.

Disjoint sets: sets A and B are disjoint means $A \cap B = \emptyset$

Counterexample and witness: An element for which $P(x) = F$ is called a **counterexample** of $\forall x P(x)$. When there is a counterexample in the domain of predicate P, $\forall x P(x)$ is false. An element for which $P(x) = T$ is called a **witness** of $\exists x P(x)$. When there is a witness in the domain of predicate P, then $\exists x P(x)$ is true.

Back to Q5

Definitions for Q5

Proof by Cases: To prove q, we can work by cases by first describing all possible cases we might be in and then showing that each one guarantees q. Formally, if we know that $p_1 \vee p_2$ is true, and we can show that $(p_1 \rightarrow q)$ is true and we can show that $(p_2 \rightarrow q)$, then we can conclude q is true.

Proof of conjunctions with subgoals: To show that $p \wedge q$ is true, we have two subgoals: subgoal (1) prove p is true; and, subgoal (2) prove q is true. To show that $p \wedge q$ is false, it's enough to prove that $\neg p$. To show that $p \wedge q$ is false, it's enough to prove that $\neg q$.

◀ Back to Q5

Definitions for Q6

Definition: When a and b are integers and a is nonzero, a **divides** b means there is an integer c such that $b = ac$. Symbolically, $F(\ (a, b)\ ) = \exists c \in \mathbb{Z}\ (b = ac)$ and is a predicate over the domain $\mathbb{Z}^{\neq 0} \times \mathbb{Z}$. Other (synonymous) ways to say that $F(\ (a, b)\ )$ is true: a is a **factor** of b; a is a **divisor** of b; b is a **multiple** of a; $a|b$.

◂ Back to Q6

Definitions for Q6

Facts about numbers:

1. Addition and multiplication of real numbers are each commutative and associative.
2. The product of two positive numbers is positive, of two negative numbers is positive, and of a positive and a negative number is negative.
3. The sum of two integers, the product of two integers, and the difference between two integers are each integers.
4. For every integer x there is no integer strictly between x and $x+1$,
5. When x, y are positive integers, $xy \geq x$ and $xy \geq y$.

◀ Back to Q6

Definitions for Q6

Proof of conditional by direct proof: To prove that the conditional statement $p \to q$ is true, we can assume p is true and use that assumption to show q is true.

Proof by Cases: To prove q, we can work by cases by first describing all possible cases we might be in and then showing that each one guarantees q. Formally, if we know that $p_1 \vee p_2$ is true, and we can show that $(p_1 \to q)$ is true and we can show that $(p_2 \to q)$, then we can conclude q is true.

◂ Back to Q6

Definitions for Q7

Definition: An integer p greater than 1 is called **prime** means the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.

Definition: an integer n is **even** means that there is an integer a such that $n = 2a$; an integer n is **odd** means that there is an integer a such that $n = 2a + 1$. Equivalently, an integer n is **even** means $n \mod 2 = 0$; an integer n is **odd** means $n \mod 2 = 1$. Also, an integer is even if and only if it is not odd.

◂ Back to Q7

Definitions for Q7

Definition: When a and b are integers and a is nonzero, a **divides** b means there is an integer c such that $b = ac$. Symbolically, $F(\ (a, b)\ ) = \exists c \in \mathbb{Z}\ (b = ac)$ and is a predicate over the domain $\mathbb{Z}^{\neq 0} \times \mathbb{Z}$. Other (synonymous) ways to say that $F(\ (a, b)\ )$ is true: a is a **factor** of b; a is a **divisor** of b; b is a **multiple** of a; $a|b$.

◂ Back to Q7

Definitions for Q7

Quantifier version of De Morgan's laws: $\neg\forall x P(x) \equiv \exists x\,(\neg P(x))$
$\neg\exists x Q(x) \equiv \forall x\,(\neg Q(x))$

Proof of disjuction using equivalent conditional: To prove that the disjunction $p \vee q$ is true, we can rewrite it equivalently as $\neg p \to q$ and then use direct proof or contrapositive proof.

Proof by Cases: To prove q, we can work by cases by first describing all possible cases we might be in and then showing that each one guarantees q. Formally, if we know that $p_1 \vee p_2$ is true, and we can show that $(p_1 \to q)$ is true and we can show that $(p_2 \to q)$, then we can conclude q is true.

◂ Back to Q7