Discrete Mathematics

The Foundations:
Logic & Proofs

Prof. Steven Evans

1.5: Nested Quantifiers

Nested Quantifiers

Example

Translate into English the statement

$$\forall x \forall y ((x > 0) \land (y < 0) \rightarrow (xy < 0)).$$

The order of quantifiers

Statement	When is it true?
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ is true for every pair x, y.
$\forall x \exists y P(x, y)$	For every x there is a y for which $P(x, y)$ is true.
$\exists x \forall y P(x, y)$	There is an x for which $P(x, y)$ is true for every y.
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	There is a pair x, y for which $P(x, y)$ is true.

The order of quantifiers

Statement	When is it false?
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	There is a pair x, y for which $P(x, y)$ is false.
$\forall x \exists y P(x, y)$	There is an x such that $P(x, y)$ is false for every y.
$\exists x \forall y P(x, y)$	For every x there is a y for which $P(x, y)$ is false.
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	$P(x, y)$ is false for every pair x, y.

Negating nested quantifiers

Example

Use quantifiers and predicates to express the fact that $\lim_{x \to a} f(x)$ does not exist where $f(x)$ is a real-valued function of a real variable x and a belongs to the domain of f.

1.6: Rules of Inference

Arguments

Definition

An *argument* is a sequence of propositions. All but the final proposition are called *premises*, and the final proposition is called the *conclusion*. An argument is *valid* if the truth of all its premises implies that the conclusion is true.

Arguments

Definition

An *argument* is a sequence of propositions. All but the final proposition are called *premises*, and the final proposition is called the *conclusion*. An argument is *valid* if the truth of all its premises implies that the conclusion is true.

Definition

An *argument form* is a sequence of compound propositions involving propositional variables. An argument form is *valid* if the conclusion is true no matter which propositions are substituted for the variables.

Rules of inference

Notation

Another way to write $(p \wedge q) \rightarrow r$ is the *inference tree*

$$\frac{p \qquad q}{\therefore r}.$$

Rules of inference

Notation

Another way to write $(p \wedge q) \rightarrow r$ is the *inference tree*

$$\frac{p \qquad q}{\therefore r}.$$

Rule of Inference	Name
$\dfrac{p \qquad p \rightarrow q}{\therefore q}$	Modus ponens
$\dfrac{\neg q \qquad p \rightarrow q}{\therefore \neg p}$	Modus tollens
$\dfrac{p \rightarrow q \qquad q \rightarrow r}{\therefore p \rightarrow r}$	Hypothetical syllogism

Rules of inference

Rule of Inference	Name
$\dfrac{p \vee q \qquad \neg p}{\therefore q}$	Disjunctive syllogism
$\dfrac{p}{\therefore p \vee q}$	Addition
$\dfrac{p \wedge q}{\therefore p}$	Simplification
$\dfrac{p \qquad q}{\therefore p \wedge q}$	Conjunction
$\dfrac{p \vee q \qquad \neg p \vee r}{\therefore q \vee r}$	Resolution

Rules of inference

Example

Show that the premises $(p \wedge q) \vee r$ and $r \rightarrow s$ imply $p \vee s$.

Rules of inference

Example

Show that the premises $(p \wedge q) \vee r$ and $r \rightarrow s$ imply $p \vee s$.

$$\frac{\overline{p \wedge q \vee r}}{}$$

Rules of inference

Example

Show that the premises $(p \wedge q) \vee r$ and $r \rightarrow s$ imply $p \vee s$.

$$\frac{\overline{p \wedge q \vee r}}{\neg\neg(p \wedge q) \vee r}$$

Rules of inference

Example

Show that the premises $(p \wedge q) \vee r$ and $r \rightarrow s$ imply $p \vee s$.

$$p \wedge q \vee r$$

$$\neg\neg(p \wedge q) \vee r$$

$$(\neg(p \wedge q)) \rightarrow r$$

Rules of inference

Example

Show that the premises $(p \wedge q) \vee r$ and $r \rightarrow s$ imply $p \vee s$.

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{p \wedge q \vee r}}{\neg\neg(p \wedge q) \vee r}}{(\neg(p \wedge q)) \rightarrow r} \qquad \cfrac{}{r \rightarrow s}}{(\neg(p \wedge q)) \rightarrow s}\ \text{Hypo. Syllog.}}{\cfrac{}{}}$$

Rules of inference

Example

Show that the premises $(p \land q) \lor r$ and $r \to s$ imply $p \lor s$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{p \land q \lor r}}{\neg\neg(p \land q) \lor r}}{(\neg(p \land q)) \to r} \qquad \dfrac{}{r \to s}}{(\neg(p \land q)) \to s}\ \text{Hypo. Syllog.}}{\neg\neg(p \land q) \lor s}}{\quad}$$

Rules of inference

Example

Show that the premises $(p \wedge q) \vee r$ and $r \rightarrow s$ imply $p \vee s$.

$$\dfrac{\dfrac{\dfrac{\text{Hypo. Syllog.}\;\dfrac{\dfrac{\dfrac{\dfrac{}{p \wedge q \vee r}}{\neg\neg(p \wedge q) \vee r}}{(\neg(p \wedge q)) \rightarrow r} \qquad \dfrac{}{r \rightarrow s}}{(\neg(p \wedge q)) \rightarrow s}}{\neg\neg(p \wedge q) \vee s}}{(p \wedge q) \vee s}}{}$$

Rules of inference

Example

Show that the premises $(p \land q) \lor r$ and $r \to s$ imply $p \lor s$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{p \land q \lor r}}{\neg\neg(p \land q) \lor r}}{(\neg(p \land q)) \to r} \qquad \dfrac{}{r \to s}}{(\neg(p \land q)) \to s}\ \text{Hypo. Syllog.}}{\neg\neg(p \land q) \lor s}}{(p \land q) \lor s}}{\therefore p \lor s}\ \text{Simp.}$$

Fallacies

The proposition $((p \to q) \wedge q) \to p$ is not a tautology. Making this mistake is called *affirming the conclusion*.

The proposition $((p \to q) \wedge \neg p) \to \neg q$ is not a tautology. Making this mistake is called *denying the hypothesis*.

Rules of inference for quantified statements

Rule of Inference	Name
$\dfrac{\forall P(x)}{\therefore P(c)}$	Universal instantiation
$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$	Universal generalization
$\dfrac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$	Existential instantiation
$\dfrac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$	Existential generalization

Combining rules of inference

Universal modus ponens

$$\frac{\forall x(P(x) \to Q(x)) \qquad P(a), \text{ where } a \text{ is a particular element}}{\therefore Q(a).}$$

Universal modus tollens

$$\frac{\forall x(P(x) \to Q(x)) \qquad \neg Q(a), \text{ where } a \text{ is a particular element}}{\therefore \neg P(a).}$$

1.7: Introduction to Proofs

Some terminology

- A *theorem* is a statement that can be shown to be true.

Some terminology

- A *theorem* is a statement that can be shown to be true.
- Oftentimes, theorem refers to an "important" statement. Less important theorems are sometimes called *propositions*.
- Less important theorems which are used crucially in the proofs of other theorems are called *lemmas* (or *lemmata*).
- A *corollary* is a theorem that can be established directly from a theorem that has been proved.

Some terminology

- A *theorem* is a statement that can be shown to be true.
- Oftentimes, theorem refers to an "important" statement. Less important theorems are sometimes called *propositions*.
- Less important theorems which are used crucially in the proofs of other theorems are called *lemmas* (or *lemmata*).
- A *corollary* is a theorem that can be established directly from a theorem that has been proved.
- A theorem is demonstrated to be true by a *proof*.
- Proofs include statements called *axioms* or *postulates*.

Direct proofs

Example

Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square.

(An integer a is a *perfect square* if there is an integer b with $a = b^2$.)

Proof by contraposition

Example

Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof by contradiction

Example

Give a proof by contradiction of the theorem "If $3n + 2$ is odd, then n is odd."

Proofs of equivalence

Example

Show that these statements about the integer n are equivalent:

1. n is even.
2. $n - 1$ is odd.
3. n^2 is even.

Counterexamples

Example

Show that the statement "Every positive integer is the sum of the squares of two integers" is false.

1.8: Proof Methods and Strategy

Exhaustive proof and proof by cases

Exhaustive proofs

Some theorems can be proved by examining a relatively small number of examples (e.g., considering a truth table). Such proofs are called *exhaustive proofs* or *proofs by exhaustion*, because these proofs proceed by exhausting all possibilities.

Exhaustive proof and proof by cases

Exhaustive proofs

Some theorems can be proved by examining a relatively small number of examples (e.g., considering a truth table). Such proofs are called *exhaustive proofs* or *proofs by exhaustion*, because these proofs proceed by exhausting all possibilities.

Important remark

A proof by cases must cover all possible cases that arise in a theorem. **It is not sufficient to check just one.**

“Without loss of generality”

Example

Show that if x and y are integers and both xy and $x + y$ are even, then x and y are both even.

Existence proofs

Example

Show that there exist irrational numbers x and y such that x^y are rational.

Proof strategy in action: forward and backward reasoning

Remark

Oftentimes, it is important to employ both *forward* and *backward reasoning*.

Example

Suppose that two people play a game taking turns removing one, two, or three stones at a time from a pile that begins with 15 stones. The person who removes the last stone wins the game. Show that the first play can win the game no matter what the second player does.

Proof strategy in action: tilings

Example

Can we tile the board obtained by deleting the upper right and lower left corner squares of a standard checkerboard, as pictured below?