20:38 8/29/2012

Chapter 1

Logic and Proofs

coursenotes by Prof. J. L. Gross for Rosen 7th Edition

1.1 PROPOSITIONAL LOGIC

Mathematics is used to predict empirical reality, and is therefore the foundation of engineering. Logic gives precise meaning to mathematical statements.

PROPOSITIONS

DEF: A ***proposition*** is a statement that is either true (T) or false (F), but not both.

Example 1.1.1:

- $1 + 1 = 2$. (T)
- $2 + 2 = 5$. (F)

Example 1.1.2: A fact-based declaration is a proposition, even if no one knows whether it is true.

- 11213 is prime.
- 1 is prime.
- There exists an odd perfect number.

Example 1.1.3: Logical analysis of rhetoric begins with the modeling of fact-based natural language declarations by propositions.

- Portland is the capital of Oregon.
- Columbia University was founded in 1754 by Romulus and Remus.
- If 2+2 = 5, then you are the pope.
  (a conditional fact-based declaration).

Example 1.1.4: A statement cannot be true or false unless it is declarative. This excludes commands and questions.

- Go directly to jail.
- What time is it?

Example 1.1.5: Declarations about semantic tokens of non-constant value are NOT propositions.

- x + 2 = 5.

TRUTH TABLES

DEF: The ***boolean domain*** is the set $\{T, F\}$. Either of its elements is called a ***boolean value***. An n-tuple $(p_1, \ldots, p_n)$ of boolean values is called a ***boolean n-tuple***.

DEF: An ***truth table*** for an operator g on n-tuples specifies the value $g(x_1, x_2, \ldots, x_n)$ as T or F for every boolean n-tuple $(x_1, x_2, \ldots, x_n)$.

DEF: The following truth table defines the operator (on 1-tuples) called ***negation***:

p	¬p
T	F
F	T

In other words, the negation of a proposition has the opposite truth value from the proposition itself.

DEF: A ***propositional operator*** is a rule defined by a truth table.

DEF: An operator is ***monadic*** if it has only one argument. It is ***dyadic*** if it has two arguments.

Example 1.1.6: Thus, negation is a monadic operator.

Example 1.1.7: The negation operator can be used to model the following constructions:

- It is **not** sunny.
- $2 + 2 \neq 5$.

DEF: The following truth table defines the dyadic propositional operator called ***conjunction***:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Example 1.1.8: The word "and" is modeled by conjunction:

- It is sunny **and** I am going to the beach.

Proposition 1.1.1. *The total number of propositional operators on n arguments is 2^{2^n}.*

Pf: The number of boolean n-tuples is 2^n. Thus, the number of rows in a truth table for a propositional operator on n arguments is 2^n. The truth value (in the right hand column) of each boolean n-tuple has two possibilities. ♢

Corollary 1.1.2. *There are* $4 = 2^2$ *monadic propositional operators.*

Corollary 1.1.3. *There are* $16 = 2^{2^2}$ *dyadic propositional operators.*

Example 1.1.9: There are only four monadic propositional operators: Identity, Negation, Constant-True, and Constant-False.

DEF: The following truth table defines the dyadic propositional operator called ***disjunction***:

p	q	p ∨ q
T	T	T
T	F	T
F	T	T
F	F	F

The disjunction is true if either (or both) of its component clauses is true.

Example 1.1.10: Disjunction models "or":

- It is rainy **or** Sweetums goes to the beach.

This sentence is TRUE if Sweetums goes to the beach in the rain. It is false only if Sweetums does not go to the beach on a non-rainy day.

DEF: ***Exclusive or*** is true if one and only one of its component clauses is true:

p	q	p ⊕ q
T	T	F
T	F	T
F	T	T
F	F	F

Exclusive or is GOOD for modeling binary addition. It is BAD for modeling "or" in English.

Example 1.1.11: When taking a Discrete Math exam, students should know everything that is in the assigned readings from the Rosen text **or** that was taught in class.

CONDITIONAL OPERATOR

DEF: This truth table defines the dyadic operator called the ***conditional*** a.k.a ***"implies"***:

p	q	p → q
T	T	T
T	F	F
F	T	T
F	F	T

In the form $p \to q$, the proposition to the left of the conditional operator (in this case, p) is called the ***antecedent***, and the proposition to the right (in this case, q) is called the ***consequent***.

The conditional operator is best understood as a CONTRACT.

Example 1.1.12: The assertion "If the Yankees win the World Series, then they give Lou Gehrig a $1,000 bonus" is of the form $p \to q$:

p: Yankees win World Series

q: Yankees give Gehrig a $1,000 bonus.

What circumstance would allow Gehrig to win a breach-of-contract suit against the Yankees?

Example 1.1.13: Conditional propositions.

- If $2 + 2 = 4$, then Albany is the capital of NY.
- If $2 + 2 = 4$, then Peapack is the capital of NJ.
- If $2 + 2 = 5$, then there is a state with only one neighbor.
- If $2 + 2 = 5$, then you* are the pope.

DISAMBIGUATION: ***Premises*** and ***conclusions*** are parts of logical arguments. We disambiguate them from "antecedent" and "consequent".

- "Hypothesis" is already an overloaded term.

DEF: The following truth table defined the dyadic operator called the ***biconditional***:

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

* N.B. Technically, "you" is a variable.

COMPOUND PROPOSITIONAL FORMS

DEF: A ***propositional variable*** is a variable such as p, q, r (possibly subscripted, e.g. p_j) over the boolean domain.

DEF: An ***atomic propositional form*** is either a boolean constant or a propositional variable.

DEF: A ***compound propositional form*** is derived from atomic propositional forms by application of propositional operators. Monadic operators are evaluated first, and otherwise, precedence is indicated by parentheses.

DISAMBIGUATION: A "proposition" is an instance of a propositional form. Careful terminological distinction is temporary.

Example 1.1.14: Some compound propositional forms on two variables: $p \vee q$, $p \wedge q$, $p \oplus q$, $p \rightarrow q$, $p \leftrightarrow q$, $(p \vee \neg q) \rightarrow q$.

Example 1.1.15: If you don't repay the Friendly Loan Company, then you will get a call from the Unfriendly Collection Agency.

$$\neg p \rightarrow q.$$

Any compound propositional form can be evaluated by a truth table

Example 1.1.16: $(p \vee \neg q) \rightarrow q$

p	q	$\neg$q	p $\vee \neg$q	(p $\vee \neg$q) $\rightarrow$ q
T	T			
T	F			
F	T			
F	F			

Example 1.1.17: From Quiz 1 in Fall 1994: Analyze $(p \wedge \neg(r \rightarrow \neg q))$ with a truth table.

SOLUTION

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

Example 1.1.18: §1.1 Exer 60: solve a crime.
Alice: Carlos did it. Carlos: Diana did it.
Diana: Carlos is lying. John: I didn't do it.

Oracle: Only one of them is telling the truth.
Problem: Who did it?

METHOD 1: modified truth table. Find the row in which only one statement is true.

perpetrator	Alice: "C"	Carlos: "D"	Diana: "¬D"	John: "¬J"
Alice	F	F	T	T
Carlos	T	F	T	T
Diana	F	T	F	T
John	F	F	T	F

METHOD 2: sequential analysis.
(1) If Alice is telling the truth, then so is John. Thus, Alice is lying, which implies that Carlos did not do it.
(2) Similarly, if Carlos is telling the truth, then so is John. Thus, Carlos is lying, which implies that Diana did not do it.
(3) By (2), Diana must be telling the truth.
(4) By (3), John is lying. Thus, John did it.

1.3 LOGICAL EQUIVALENCES

Logical equivalences occur in mathematical proofs. They are also useful in simplifying loop-exit conditions in computer programs.

DEF: Two propositional forms on the same variables are ***(logically) equivalent*** if they have the same result column in their truth tables.
NOTATION: $F \Leftrightarrow G$.

DISAMBIGUATION: The biconditional $\leftrightarrow$ is an operator. Logical equivalence $\Leftrightarrow$ is a relation on propositions.

Example 1.3.1: $\neg p \vee q \Leftrightarrow p \rightarrow q$

p	q	$\neg$p	$\neg$p $\vee$ q	p $\rightarrow$ q
T	T			
T	F			
F	T			
F	F			

CONTRAPOSITIVE, etc.

DEF: The ***contrapositive*** of a proposition of the form $p \to q$ is the proposition of the form

$$\neg q \to \neg p$$

Proposition 1.3.1. *The contrapositive of $p \to q$ is logically equivalent to $p \to q$.*

Pf:

p	q	¬q	¬p	p → q	¬q → ¬p
T	T	F	F	T	T
T	F	T	F	F	F
F	T	F	T	T	T
F	F	T	T	T	T

Example 1.3.2:

- conditional $p \to q$: If it is sunny, then you can find me at the beach.
- contrapositive $\neg q \to \neg p$: If you can't find me at the beach, then it is not sunny.

DEF: The ***converse*** of a proposition of the form $p \to q$ is the proposition of the form

$$q \to p$$

DEF: The ***inverse*** of a proposition of the form $p \to q$ is the proposition of the form

$$\neg p \to \neg q$$

Example 1.3.3:

- conditional $p \to q$: If it is sunny, then you can find me at the beach.
- converse $q \to p$: If you can find me at the beach, then it is sunny.
- inverse $\neg p \to \neg q$: If it is not sunny, then you can't find me at the beach.

Proposition 1.3.2. *The converse and the inverse are equivalent to each other, but not to the original conditional.*

Pf: Left to the reader. ♢

CATEGORIES of PROPOSITIONAL FORMS

DEF: A ***tautology*** is a propositional form that is always true, no matter what truth values are assigned to its variables.

DEF: A ***self-contradiction*** is a propositional form that is always false, no matter what truth values are assigned to its variables.

DEF: A ***contingency*** is a propositional form that is neither a tautology nor a contradiction.

DISAMBIGUATION: The word "contradiction" means two propositions with opposite truth values. See §1.5, §1.6.

Prop 1.3.3. *A propositional form is a tautology iff it is equivalent to the constant T.*

Pf: This is simply a rephrasing. ♢

Proposition 1.3.4. *A propositional form is a self-contradiction iff it is equivalent to the constant F.*

Pf: This is a rephrasing. ♢

LAWS of LOGIC

Various logical equivalences and tautologies have earned the honorific appelation ***law***.

DEF: ***Double Negation Law:*** $\neg\neg p \Leftrightarrow p$.

p	¬p	¬(¬p)
T	F	T
F	T	F

DEF: ***Law of the Excluded Middle:*** $p \vee \neg p$.

p	¬p	p ∨ (¬p)
T	F	T
F	T	T

AVOIDING BOREDOM

First Law of Good Pedagogy: Boredom does not help anyone to learn.

Example 1.3.4: Table 5 of §1.2 (de Morgan, associativity, etc.) is excellent for self-study, but not for exhaustive classroom presentation.

1.4 PREDICATES & QUANTIFIERS

DEF: Informally, a ***predicate*** is a statement about a (possibly empty) collection of variables over various domains. Its truth value depends on the values of the variables in their respective domains.

DEF: Formally, a ***predicate*** is a function from the cartesian product of the domains of the variables to the boolean set $\{T, F\}$.

Example 1.4.1: $x + 2 = 5$.

Example 1.4.2: $4x - 3y > 2x$.

DEF: The ***universal quantification (over x)*** of a predicate $P(x)$ is the predicate $(\forall x)[P(x)]$.

Example 1.4.3: $(\forall x)[x + 2 = 5]$.

Example 1.4.4: $(\forall x)[4x - 3y > 2x]$.

DEF: The ***existential quantification (over x)*** of a predicate $P(x)$ is the predicate $(\exists x)[P(x)]$.

Example 1.4.5: $(\exists x)[x + 2 = 5]$.

Example 1.4.6: $(\exists x)[4x - 3y > 2x]$.

Remark: Observe that the result of quantifying a predicate is still a predicate. Moreover, when propositional operators are applied to predicates, the results are predicates.

VARYING THE DOMAIN

Example 1.4.7: $(\forall x)[x^2 = 1]$ is FALSE over the integers, but TRUE over the domain $\{-1, 1\}$.

Example 1.4.8: $(\exists x)[x^2 = -9]$ is FALSE over the integers, but TRUE over the domain of complex numbers.

CLASSROOM EXERCISE

Consider these two condition statements.

1. $(\forall x)[P(x)] \rightarrow (\exists x)[P(x)]$.

Over the domain of people, this would mean "If something is good for everybody, then it's good for somebody.".

2. $(\exists x)[P(x)] \rightarrow (\forall x)[P(x)]$.

Over the domain of people, this could mean "What's good for me is good for everybody.".

Try to think of a general property of a domain under which statement (1) is necessarily FALSE.

Try to think of a general property of a domain under which statement (2) is necessarily TRUE.

Hint: These general properties are based solely on the number of elements in the domain.

SCOPE of QUANTIFIERS

DEF: The ***scope*** of a quantifier is the clause to which it applies.

Example 1.4.9: Let x range over the integers.

$$P(x) : x > 2 \qquad Q(x) : x < 2$$

Compare these two non-equivalent propositions:

A. $(\exists x)[P(x) \wedge Q(x)]$

B. $(\exists x)[P(x)] \wedge (\exists x)[Q(x)]$

A is FALSE, but B is TRUE.

DEF: An ***unbound variable*** in a predicate is a variable not within the scope of any quantifier.

Example 1.4.10: x is an unbound variable.

$$x + 4 > 2$$

Example 1.4.11: x is an unbound variable.

$$(\forall y)[2x + 3y = 7]$$

Remark: A predicate with no unbound variables is a proposition.

NEGATION with QUANTIFIERS

p: There exists some input data for which this program will crash.

$\neg p$: No matter what input data you supply to this program, it will not crash.

Rule 1: $\neg(\exists x)[P(x)] \Leftrightarrow (\forall x)[\neg P(x)]$

Rule 2: $\neg(\forall x)[P(x)] \Leftrightarrow (\exists x)[\neg P(x)]$

CLASSROOM EXERCISE

On a New Jersey Transit commuter run, the conductor announces:

> At the next stop, all doors will not be open.

Express this in symbolic logic.
Explain what his words mean.
What words accurately express what he probably intended?

1.5 NESTED QUANTIFIERS

Example 1.5.1: Every sophomore owns a computer or has a friend in the junior class who owns a computer.

Domains S and J are the sets of sophomores and juniors. Predicates $C(u)$ and $F(v, w)$ mean that u owns a computer and that w is a friend of v.

$$(\forall x \in S)\big[C(x) \vee (\exists y \in J)[F(x, y) \wedge C(y)]\big].$$

DISAMBIGUATION: Specify the domain when not evident from context. Use brackets to identify scope of quantifiers.

The text calls this a ***quantifier with restricted domain***. The text uses slightly different notation.

The **important issue** is that the notation should be self-explanatory to anyone familiar with the underlying concept.

TRANSPOSING QUANTIFIERS

Be careful about transposing different kinds of quantifiers.

- $(\forall x)(\exists y)[x^2 \leq y]$ is true.
- $(\exists y)(\forall x)[x^2 \leq y]$ is false.

However, you can safely transpose two quantifiers of the same kind.

RECALL NEGATION with QUANTIFIERS

p: There exists some input data for which this program will crash.

$\neg p$: No matter what input data you supply to this program, it will not crash.

Rule 1: $\neg(\exists x)[P(x)] \Leftrightarrow (\forall x)[\neg P(x)]$

Rule 2: $\neg(\forall x)[P(x)] \Leftrightarrow (\exists x)[\neg P(x)]$

CLASSROOM EXERCISE

Write the negation of this statement

$$(\forall x)(\exists y)[x^2 \leq y]$$

so that no negation ($\neg$) appears to the left of a quantifier.

$\neg(\forall x)(\exists y)[x^2 \leq y] =$

OPTIONAL CLASSROOM EXERCISE

An exercise about varying the subdomain from within the set of all people.

B(x,y) : y is the brother of x (predicate)

Specify a subdomain — maximal, if possible — in which each of the following assertions is TRUE.

1. $(\forall x)(\forall y)[B(x,y) \rightarrow B(y,x)]$.

For any two persons Bill(x) and George(y),
if George(y) is a brother of Bill(x),
then Bill(x) is the brother of George(y).

2. $(\exists x)(\forall y)[B(x,y) \rightarrow B(y,x)]$.

There is a person who is a brother to each of his brothers.

3. $(\forall x)(\exists y)[B(x,y) \rightarrow B(y,x)]$.

Every person has a brother to whom that person is also a brother.

4. $(\exists x)(\exists y)[B(x,y) \rightarrow B(y,x)]$.

There exist two persons, Bill (x) and George (y), such that if George is Bill's brother, then Bill is George's brother.

1.6 RULES OF INFERENCE

Some forms of argument ("valid") never lead from correct statements to an incorrect conclusion. But some other forms of argument ("fallacies") can lead from true statements to an incorrect conclusion.

DEF: An ***axiom*** is a statement that is given as true, or in the case of a mathematical system, is used to specify the system.

DEF: A ***mathematical argument*** is a list of statements. Its last statement is called the ***conclusion***.

DEF: A ***logical rule of inference*** is a method that depends on logic alone for deriving a new statement from a set of other statements.

DEF: A ***mathematical rule of inference*** is a method for deriving a new statement that may depend on inferential rules of a mathematical system as well as on logic.

VALID ARGUMENTS

DEF: A ***logical argument*** consists of a list of (possibly compound) propositions called premises and a single proposition called the conclusion.

Example 1.6.1: A Logical Argument

If I dance all night, then I get tired.

I danced all night.

Therefore I got tired.

Logical representation of underlying variables:

p: I dance all night. q: I get tired.

Logical analysis of argument:

$p \to q$	premise 1
p	premise 2
q	conclusion

DEF: A form of logical argument is ***valid*** if whenever every premise is true, the conclusion is also true. A form of argument that is not valid is called a ***fallacy***.

We shall see why the argument above is valid.

This form of argument is called ***modus ponens***.

$p \to q$	premise 1
p	premise 2
q	conclusion

Operational Method of Validation

Step 1. Form a truth table in which the premises are columns, and the conclusion is the last column.

Step 2. Star every row in which all the premises are true.

Step 3. Declare the argument to be valid if every starred row has a T in its last column (the conclusion column).

p	q	p → q	p	q	*
T	T	T	T	T	*
T	F	F	T	F	
F	T	T	F	T	
F	F	T	F	F	

Having once verified modus ponens with truth tables, we need never question its validity again.

FALLACIES

Example 1.6.2: A Fallacy

If I dance all night, then I get tired.

I got tired.

Therefore I danced all night.

Logical form of argument:

$p \to q$	premise 1
q	premise 2
p	conclusion

Now for the validity check.

p	q	p → q	q	p	*
T	T	T	T	T	*
T	F	F	F	T	
F	T	T	T	F	*
F	F	T	F	F	

Row 3 indicates it is possible that even when all the premises are true, the conclusion can be false. Thus, this form of argument is a fallacy.

NOTORIOUS FALLACIES

In the ***fallacy of affirming the consequent***, one affirms the consequent of a conditional and concludes that the antecedent is true.

$$[(p \to q) \wedge q] \to p$$

Example 1.6.2 affirms the consequent.

In the ***fallacy of denying the antecedent***, one denies the antecedent of a conditional and concludes that the consequent is false.

$$[(p \to q) \wedge \neg p] \to \neg q$$

Example 1.6.3: Denying the Antecedent

She says:

Even if you were the last man on earth,

I would not marry you.

He thinks:

But I am not the last man on earth,

and that implies that she will marry me.

I'll keep on trying.

VALIDITY and TRUTH

(1) The conclusion of a valid argument might be false, if one or more of the premises is not true.

(2) The conclusion of a fallacy might be true.

(3) If the premises are correct, and if the argument is valid, then the conclusion is correct.

LOGICAL RULES of INFERENCE

TERMINOLOGY NOTE: A ***rule of inference*** is defined to be any valid argument. Typically, however, it is only called a ***valid argument*** unless it is frequently applied.

All of the following rules of inference can be confirmed with truth tables.

Modus Ponens.

$p \to q$	premise 1
p	premise 2
q	conclusion

Modus Tollens.

$p \to q$	premise 1
$\neg q$	premise 2
$\neg p$	conclusion

Addition.

p	premise 1
$p \vee q$	conclusion

Simplification.

$p \wedge q$	premise 1
p	conclusion

Disjunctive Syllogism.

$p \vee q$	premise 1
$\neg p$	premise 2
q	conclusion

Hypothetical Syllogism.

$p \to q$	premise 1
$q \to r$	premise 2
$p \to r$	conclusion

1.7 INTRODUCTION TO PROOFS

This section of the Rosen test discusses the connection between the formal methods of proof described in §1.6 and the informal proofs that are given most of the time in textbooks and classroom presentations. Nearly all proofs in archival mathematical research journals are informal.

TWO FAMOUS PROBLEMS

Fermat's Last Thm: For $n > 2$, the equation

$$a^n + b^n = c^n$$

has no solutions for non-zero integers a, b, c.
Status: Proved by Andrew Wiles.

Goldbach Conjecture: Every even number $2n$ larger than 4 is the sum of two odd primes.
Status: Open.

Example: $98 = 19 + 79$

MATHEMATICAL PROOFS (DIRECT)

DEF: A ***direct proof*** is a mathematical argument that uses rules of inference to derive the conclusion from the premises.

Example 1.7.1: Alt Proof of Disj Syllogism: by a chain of inferences.

$p \vee q$	**premise 1**
$\neg\neg p \vee q$	double negation law
$\neg p \to q$	$\neg A \vee B \Leftrightarrow A \to B$ (use $A = \neg p$)
$\neg p$	**premise 2**
q	**conclusion** by modus ponens

Example 1.7.2: a theorem
The sum of two even numbers x and y is even.

Pf: (1) There exist integers m and n such that $x = 2m$ and $y = 2n$ (by def of "even").

(2) Then $x + y = 2m + 2n$ (by substitution).

$= 2(m + n)$ (by left distrib)

which is even, by the defn of evenness. $\diamondsuit$

MATHEMATICAL PROOFS (INDIRECT)

DEF: An ***indirect proof*** uses rules of inference on the negation of the conclusion and on some of the premises to derive the negation of a premise. This result is called a ***contradiction***.

Example 1.7.3: a theorem
If x^2 is odd, then so is x.

Pf: Assume that x is even (neg of concl).

Say $x = 2n$ (defn of even).

Then $x^2 = (2n)^2$ (substitution)

$= 2n \cdot 2n$ (defn of exponentiation)

$= 2 \cdot 2n^2$ (commutativity of mult.)

which is an even number (defn of even)

which contradicts the premise that x^2 is odd. $\diamondsuit$

TERMINOLOGY

DEF: A ***mathematical proof*** is a list of statements in which every statement is one of the following:

(1) an axiom

(2) derived from previous statements by a rule of inference

(3) a previously derived *theorem*

Its last statement is called a ***theorem.***

TERMINOLOGY: There is a hierarchy of terminology that gives opinions about the importance of derived truths:

(1) A ***proposition*** is a theorem of lesser generality or of lesser importance.

(2) A ***lemma*** is a theorem whose importance is mainly as a key step in something deemed to be of greater significance.

(3) A ***corollary*** is a consequence of a theorem, usually one whose proof is much easier than that of the theorem itself.

1.8 PROOF STRATEGY

FORWARD AND BACKWARD REASONING

Example 1.8.1: Backward Reasoning

Let $a, b > 0$, with $a \neq b$. Then $\dfrac{(a+b)}{2} > \sqrt{ab}$.

Pf: Conclusion is true if $a + b > 2\sqrt{ab}$,
which is true if $(a+b)^2 > 4ab$,
which is true if $a^2 + 2ab + b^2 > 4ab$,
which is true if $a^2 - 2ab + b^2 > 0$,
which is true if $(a-b)^2 > 0$, which is true. ♢

Example 1.8.2: Forward Reasoning
Let $n \in \mathcal{N}$, such that n is not divisible by 2 or 3.
Then $n^2 - 1$ is divisible by 24.

Pf: Since n is not divisible by 2 or 3,
it follows that $n = 6k + 1$ or $6k + 5$.
Case 1. $(6k+1)^2 - 1 \equiv 36k^2 + 12k \bmod 24$
$\equiv 12k^2 + 12k \equiv 0 \bmod 24$, since 2 divides $k^2 + k$.
Case 2. $(6k+5)^2 - 1 \equiv 36k^2 + 60k + 24 \bmod 24$
$\equiv 12k^2 + 12k \equiv 0 \bmod 24$, as above. ♢

MATHEMATICAL PROOFS (by CASES)

DEF: A ***proof by cases*** uses the following rule of inference:

$p \to r$	premise 1
$q \to r$	premise 2
$p \vee q$	premise 3
r	conclusion

Example 1.8.3: a theorem
Let x be any integer. Then $x^2 + x$ is even.

Pf: setup for proof-by-cases inference
$p : x$ is even; $q : x$ is odd; $r : x^2 + x$ is even.

Verify premise 1. If x is even, then $x = 2n$, for some integer n. Hence,

$$x^2 + x = (2n)^2 + 2n = 4n^2 + 2n$$

which is even.

Verify premise 2. If x is odd, then $x = 2n + 1$, for some n. Hence,

$$\begin{aligned} x^2 + x &= (2n+1)^2 + (2n+1) \\ &= (4n^2 + 4n + 1) + (2n + 1) \\ &= 4n^2 + 6n + 2 \end{aligned}$$

which is even.

Verify premise 3: An arbitrary integer is either even or odd. ♢

PROVING QUANTIFIED ASSERTIONS

(1) To prove $(\forall x)[P(x)]$
Let x be an arbitrary (unrestricted) member of the universal set of context, and show $P(x)$ is true.

Example: Show that $x^2 + x$ is even, for all x.

(2) To prove $(\exists x)[P(x)]$
Exhibit any member of the universe for which $P(x)$ is true. One example suffices.

Example: Show that 729 is a power of 3, that is, $(\exists n)[3^n = 729]$.

(3) To prove $\neg(\forall x)[P(x)]$
Exhibit any member of the universe for which $P(x)$ is false. One counterexample suffices.

Example: Show that 323 is not prime.

(4) To prove $\neg(\exists x)[P(x)]$
Let x be an arbitrary (unrestricted) member of the universal set of context and show $P(x)$ is false.

Example: Show that $\sqrt{2}$ is irrational, that is,

$$\neg(\exists p, q)\left[\sqrt{2} = \frac{p}{q}\right]$$

1.9 LOGIC SUPPLEMENT

PROPOSITIONS

Example 1.9.1: Opinions are NOT propositions.

- Millard Fillmore was our greatest President.

Example 1.9.2: Ambiguities of meaning often obscure whether or not a sentence is a proposition.

- Who's on first. (comedy routine)
- Smith was guilty.

Propositional interpretations:

(1) Smith actually committed the offense.

(2) Smith was convicted.

Nonpropositional interpretation:

(3) an opinion about moral culpability:

"A person who sincerely believes in something simply is not guilty." (This redefines guilt to mean insincerity. Exercise: define sincerity.)

TIME OUT to discuss OBSCENITY

You will *not* be tested on the following material.

DEF: An ***obscenity*** is a word or phrase that has been proscribed from ***polite conversation***.

Example 1.9.3: Two four-letter obscenities:

- Ain't is an English-language obscenity.
- GOTO is a programming obscenity.
- Pronouncing GOTO as two words is a further obscenity.

Remark: Some words have both a polite meaning and an obscene meaning. (Exercise: list 20 such words.) Sometimes one subculture regards a meaning as an obscenity, while another thinks it perfectly polite usage.

Example 1.9.4: Saying only "Columbia" to refer to any educational institution other than the real Columbia is obscene. The right people use phrases such as "Columbia College in Who-KnowsWhere" that acknowledges the primary meaning of "Columbia".

CONCLUSION: Saying only "or" to refer to *exclusive-or* is regarded as obscene in the technological subculture. The right way to express exclusive-or is to say "X or Y but not both", because *inclusive-or* is the primary meaning.

TERMINOLOGY NOTE: If a phrase is ambiguous or has some other easily described fault, then we just specify the fault. The epithet "obscenity" is reserved for usage we don't like but can't say why not.

DISAMBIGUATION: ***Implication*** is a relation on statements, and not an operator. It's okay to say "p implies q" for $p \to q$, but not to write it.