Discrete Mathematics

1. Logic

Artificial Intelligence & Computer Vision Lab
School of Computer Science and Engineering
Seoul National University

Logic

A formal system for describing knowledge and implementing reasoning on knowledge.

Logic consists of

1. A language describing knowledge (states of affairs) where its syntax describes how to make sentences and its semantics states how to interpret sentences
2. A set of rules for deducing the entailments of a set of sentences.

1-1. Propositional Logic

Propositional Logic

- *Propositional logic* treats simple sentences as atomic entities and constructs more complex sentences from simpler sentences using *Boolean connectives.*

Propositions and Proposition Variables

- *Definition*:
  1. A *proposition* is an assertion, a declarative sentence with a definite meaning, having a truth value that's either true (T) or false (F) (never both, neither, or somewhere in between).
  2. A *proposition variable* such as *P, Q, R,…,* denotes an arbitrary proposition with an unspecified truth value.

- Note the difference between a proposition and a proposition variable.

Examples:

- "It is raining." (In a given situation.)
- "Seoul is the capital of South Korea."
- "1 + 2 = 3"

<u>But, the following are NOT propositions:</u>

- "Who's there?" (interrogative, question)
- "La la la la la." (meaningless interjection)
- "Just do it!" (imperative, command)
- "Yeah, I sorta dunno, whatever..." (vague)
- "1 + 2" (expression with a non-true/false value)

Operators / Connectives

1. *Operator* or *connective* combines one or more *operand* expressions into a larger expression (*e.g.*, “+” in numeric expressions).
2. *Unary* operators take 1 operand (*e.g.*, −3).
3. *binary* operators take 2 operands (*e.g.*, 3 × 4).
4. *Propositional* or *Boolean* operators operate on propositions or truth values instead of on numbers.

Some Popular Boolean Operators

Formal Name	Nickname	Arity	Symbol
Negation operator	NOT	Unary	$\neg$
Conjunction operator	AND	Binary	$\wedge$
Disjunction operator	OR	Binary	$\vee$
Exclusive-OR operator	XOR	Binary	$\oplus$
Implication operator	IMPLIES	Binary	$\rightarrow$
Biconditional operator	IFF	Binary	$\leftrightarrow$

Negation Operator

The unary *negation operator* "¬" (*NOT*) transforms a prop. into its logical *negation*.

E.g. If P = "I have brown hair."

then $\neg P$ = "I do not have brown hair."

Truth table for NOT:

P	$\neg P$
T	F
F	T

Operand column

Result column

Conjunction Operator

The binary *conjunction operator* "$\wedge$" (*AND*) combines two propositions to form their logical *conjunction*.

Example:

If P = "I will have salad for lunch." and Q = "I will have steak for dinner.", then $P \wedge Q$ = "I will have salad for lunch and I will have steak for dinner."

—

Conjunction Truth Table

- Note that a conjunction $P_1 \wedge P_2 \wedge \ldots \wedge P_n$ of n propositions will have 2^n rows in its truth table.

P	Q	$P \wedge Q$
F	F	F
F	T	F
T	F	F
T	T	T

- Also: ¬ and ∧ operations together are sufficient to express *any* Boolean truth table!

Disjunction Operator

The binary *disjunction operator* "$\vee$" (*OR*) combines two propositions to form their logical *disjunction*.

P="My car has a bad engine."

Q="My car has a bad carburetor."

$P \vee Q$="Either my car has a bad engine, or my car has a bad carburetor."

Disjunction Truth Table

P	Q	$P \vee Q$
F	F	F
F	T	T
T	F	T
T	T	T

- Note that $P \vee Q$ means that P is true, or Q is true, or both are true!
- So, this operation is also called *inclusive or*, because it includes the possibility that both P and Q are true.
- "$\neg$" and "$\vee$" together are also universal.

Nested Propositional Expressions

- Use parentheses to *group sub-expressions*:
  "I just saw my old friend, and either he's *g*rown or I've shrunk." = $P \wedge (Q \vee R)$
  - $(P \wedge Q) \vee R$ would mean something different
  - $P \wedge Q \vee R$ would be ambiguous

- By convention, "$\neg$" takes *precedence* over both "$\wedge$" and "$\vee$".
  - $\neg R \wedge P$ means $(\neg R) \wedge P$, not $\neg (R \wedge P)$

Example

Let P="It rained last night",
Q="The sprinklers came on last night,"
R="The lawn was wet this morning."

Translate each of the following into English:

$\neg P$ = "It didn't rain last night."

$R \wedge \neg P$ = "The lawn was wet this morning, and it didn't rain last night."

$\neg R \vee P \vee Q$ = "Either the lawn wasn't wet this morning, or it rained last night, or the sprinklers came on last night."

Exclusive-Or Operator

The binary *exclusive-or operator* "⊕" (*XOR*) combines two propositions to form their logical "exclusive or".

P = "I will earn an A in this course,"

Q = "I will drop this course,"

P ⊕ *Q* = "I will either earn an A for this course,
or I will drop it (but not both!)"

Exclusive-Or Truth Table

- Note that $P \oplus Q$ means that P is true, or Q is true, but not both!
- This operation is called *exclusive or*, because it excludes the possibility that both P and Q are true.

P	Q	$P \oplus Q$
F	F	F
F	T	T
T	F	T
T	T	F

Implication Operator

antecedent consequent

The *implication* $P \rightarrow Q$ states that P implies Q.

i.e., If P is true, then Q is true; but if P is not true, then Q could be either true or false.

Example:

Let P = "You study hard."

Q = "You will get a good grade."

$P \rightarrow Q$ = "If you study hard, then you will get a good grade." (else, it could go either way)

Implication Truth Table

- $P \rightarrow Q$ is false only when P is true but Q is not true.
- $P \rightarrow Q$ does not say that P causes Q!
- $P \rightarrow Q$ does not require that P or Q are ever true!
- Example: "(1=0) $\rightarrow$ pigs can fly" is TRUE!

P	Q	$P \rightarrow Q$
F	F	T
F	T	T
T	F	F
T	T	T

Examples

- "If this lecture ends, then the sun will rise tomorrow."
  True or *False*?
- "If Tuesday is a day of the week, then I am a penguin."
  True or *False*?
- "If 1+1=6, then Bush is president."
  True or *False*?
- "If the moon is made of green cheese, then I am richer than Bill Gates." *True* or *False*?

English Phrases Meaning $P \rightarrow Q$

- "*P* implies *Q*"
- "if *P*, then *Q*"
- "if *P*, *Q*"
- "when *P*, *Q*"
- "whenever *P*, *Q*"
- "*Q* if *P*"
- "*Q* when *P*"
- "*Q* whenever *P*"
- "*P* only if *Q*"
- "*P* is sufficient for *Q*"
- "*Q* is necessary for *P*"
- "*Q* follows from *P*"
- "*Q* is implied by *P*"

Converse, Inverse, Contrapositive

Some terminology, for an implication $P \rightarrow Q$:

- Its *converse* is: $Q \rightarrow P$.
- Its *inverse* is: $\neg P \rightarrow \neg Q$.
- Its *contrapositive*: $\neg Q \rightarrow \neg P$.
- One of these three has the *same meaning* (same truth table) as $P \rightarrow Q$. Can you figure out which?

How do we know for sure?

Proving the equivalence of $P \rightarrow Q$ and its contra positive using truth tables:

P	Q	$\neg Q$	$\neg P$	$P \rightarrow Q$	$\neg Q \rightarrow \neg P$
F	F	T	T	T	T
F	T	F	T	T	T
T	F	T	F	F	F
T	T	F	F	T	T

Biconditional operator

The *biconditional* $P \leftrightarrow Q$ states that P is true *if and only if (iff)* Q is true.

P= "You can take the flight."

P= "You buy a ticket"

$P \leftrightarrow Q$ = "You can take the flight if and only if you buy a ticket."

Biconditional Truth Table

- $P \leftrightarrow Q$ means that P and Q have the same truth value.
- Note this truth table is the exact opposite of $\oplus$'s!
  - $P \leftrightarrow Q$ means $\neg(P \oplus Q)$
- $P \leftrightarrow Q$ does not imply P and Q are true, or cause each other.

P	Q	$P \leftrightarrow Q$
F	F	T
F	T	F
T	F	F
T	T	T

Boolean Operations Summary

- We have seen 1 unary operator (out of the 4 possible) and 5 binary operators (out of the 16 possible). Their truth tables are below.

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \oplus Q$	$P \rightarrow Q$	$P \leftrightarrow Q$
F	F	T	F	F	F	T	T
F	T	T	F	T	T	T	F
T	F	F	F	T	T	F	F
T	T	F	T	T	F	T	T

Well-formed Formula (wff) for Propositional Logic

- *Definition*:
  1. Any proposition variable is a wff.
  2. For any wff P, $\neg P$ is a wff.
  3. If P and Q are wffs, then $(P \wedge Q)$, $(P \vee Q)$, $(P \rightarrow Q)$ and $(P \leftrightarrow Q)$ are wffs.
  4. A finite string of symbols is a wff only when it is constructed by steps 1, 2, and 3.

Examples

- By definition of a wff,
  - wff: $\neg(P \wedge Q)$, $(P \rightarrow (P \vee Q))$, $(\neg P \wedge Q)$, $(((P \rightarrow Q) \wedge (Q \rightarrow R)) \leftrightarrow (P \rightarrow R))$,
  - not wff: $(P \rightarrow Q) \rightarrow (\wedge Q)$, $(P \rightarrow Q$,

Tautology

- *Definition*:

  A well-formed formula (wff) is a *tautology* if for every truth value assignment to the variables appearing in the formula, the formula has the value of true.

- Example: $(P \vee \neg P)$

Substitution Instance

- *Definition*:

  A wff *A* is a substitution instance of another formula *B* if *A* is formed from *B* by substituting formulas for variables in *B* under condition that the same formula is substituted for the same variable each time that variable is occurred.

- *Theorem*:

  A substitution instance of a tautology is a tautology

Contradiction

- *Definition*:

  A wff is a *contradiction* if for every truth value assignment to the variables in the formula, the formula has the value of false.

- Example: $(P \wedge \neg P)$

Valid Consequence

- *Definition*:

  A (well-formed) formula *B* is a *valid consequence* of a formula *A*, denoted by $A \models B$, if for all truth assignments to variables appearing in *A* and *B*, the formula *B* has the value of true whenever the formula *A* has the value of true.

- *Definition*:

  A formula *B* is a *valid consequence* of a formula $A_1, \ldots, A_n$ ($A_1, \ldots, A_n \models B$) if for all truth value assignments to the variables appearing in $A_1, \ldots, A_n$ and *B*, the formula *B* has the value of true whenever the formula $A_1, \ldots, A_n$ have the value of true.

- *Theorem*:

  $A \vdash B$ *if and only if* $\vdash (A \rightarrow B)$

- *Theorem*:

  $A_1, \ldots, A_n \vdash B$ *if and only if* $(A_1 \wedge \ldots \wedge A_n) \vdash B$

- *Theorem*:

  $A_1, \ldots, A_n \vdash B$ *if and only if*

  $(A_1 \wedge \ldots \wedge A_{n\text{-}1}) \vdash (A_n \rightarrow B)$

Logical Equivalence

- *Definition*:

  Two wffs, *A* and *B*, are logically equivalent

  if and only if *A* and *B* have the same truth values for every truth value assignment to all variables contained in *A* and *B*.

- *Theorem*:

  If a formula A is equivalent to a formula B, then $\vdash A \leftrightarrow B$.

- *Theorem*:

  If a formula D is obtained from a formula A by replacing a part of A, say C, which is itself a formula, by another formula B such that $C \Leftrightarrow B$, then $A \Leftrightarrow D$

Proving Equivalence via Truth Tables

- Example: Prove that $P \vee Q \Leftrightarrow \neg(\neg P \wedge \neg Q)$.

P	Q	$P \vee Q$	$\neg P$	$\neg Q$	$\neg P \wedge \neg Q$	$\neg(\neg P \wedge \neg Q)$
F	F	F	T	T	T	F
F	T	T	T	F	F	T
T	F	T	F	T	F	T
T	T	T	F	F	F	T

Equivalence Theorems

- *Identity*: $P \wedge \mathrm{T} \Leftrightarrow P$ $P \vee \mathrm{F} \Leftrightarrow P$
- *Domination*: $P \vee \mathrm{T} \Leftrightarrow \mathrm{T}$ $P \wedge \mathrm{F} \Leftrightarrow \mathrm{F}$
- *Idempotent*: $P \vee P \Leftrightarrow P$ $P \wedge P \Leftrightarrow P$
- *Double negation:* $\neg\neg P \Leftrightarrow P$
- *Commutative*: $P \vee Q \Leftrightarrow Q \vee P$ $P \wedge Q \Leftrightarrow Q \wedge P$
- *Associative*: $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$
  $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$

- *Distributive*: $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$
  $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$

- *De Morgan's*:
  $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
  $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$

- *Trivial tautology/contradiction*:
  $P \vee \neg P \Leftrightarrow \mathrm{T}$ $P \wedge \neg P \Leftrightarrow \mathrm{F}$

Defining Operators via Equivalences

Using equivalences, we can *define* operators in terms of other operators.

- Exclusive or: $P \oplus Q \Leftrightarrow (P \vee Q) \wedge \neg(P \wedge Q)$
  $P \oplus Q \Leftrightarrow (P \wedge \neg Q) \vee (Q \wedge \neg P)$
- Implies: $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
- Biconditional: $P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$
  $P \leftrightarrow Q \Leftrightarrow \neg(P \oplus Q)$

Examples

Let P and Q be the proposition variables denoting

P: It is below freezing.

Q: It is snowing.

Write the following propositions using variables, P and Q, and logical connectives.

a) It is below freezing and snowing. $P \wedge Q$

b) It is below freezing but not snowing. $P \wedge \neg Q$

c) It is not below freezing and it is not snowing. $\neg P \wedge \neg Q$

d) It is either snowing or below freezing (or both). $P \vee Q$

e) If it is below freezing, it is also snowing. $P \rightarrow Q$

f) It is either below freezing or it is snowing, but it is not snowing if it is below freezing. $(P \vee Q) \wedge (P \rightarrow \neg Q)$

g) That it is below freezing is necessary and sufficient for it to be snowing $P \leftrightarrow Q$

1-2. Predicate Logic

(First-order) Predicate Logic

- *Predicate logic* represents a sentence in terms of objects and predicates on objects (i.e., properties of objects or relationships between objects), as well as Boolean connectives and quantifiers.

- In *propositional logic* every expression is a sentence, which represents a fact. *First-order predicate logic* has sentences, but it also has *terms*, which represent objects. *Constant symbols*, *variables*, and *function symbols* are used to build *terms*, and *quantifiers* and *predicate symbols* are used to build sentences.

Syntax and Semantics

- Constant symbols: *A, B, John,…*
- Variables: *x, y, z, …*
- Predicate symbols: *ROUND, BROTHER,…* where a predicate symbol refers to a particular relation in the model. For example, the *BROTHER* symbol referring to the relation of brotherhood is a binary predicate symbol having two objects.
- Function symbols: *father, color,…* where a function symbol maps its objects into some object.

where predicate and function symbols are often given by mnemonic strings.

Terms

- A *term* is a logical expression that refers to an object, which is defined as follows:
- *Definition:*

  1. Constant symbols and variables are *terms*.
  2. If *x* is a *term* and *h* is a function symbol, *h(x)* is a term.
  3. A finite string is a term only when it is constructed by steps 1 and 2.

- Examples:

  x, *John*, *color(x)*, *father(John)*, *mother(father(John))*

Functions and Predicates

- Arguments of functions and predicates are given by *terms*.

- Examples:

father(John), mother(Sue), father(mother(Sue)),

MARRIED(John, Sue), FEMALE(x), MEMBER(Sue,y)

PARENT(mother(Sue), Tom)

Universe of Discourse (U.D.)

- *Definition*:

  The collection of values that a variable *x* can take is called *x*'s *universe of discourse*.

Quantifiers

- *Definition:*
  1. *Quantifiers* provide a notation that allows us to *quantify* (count) *how many* objects in the universe of discourse satisfy a given predicate.
  2. "$\forall$" is the FOR ALL or *universal* quantifier.
     $\forall x\ P(x)$ means for all x in the u.d., P holds.
  3. "$\exists$" is the EXISTS or *existential* quantifier.
     $\exists x\ P(x)$ means there exists an x in the u.d. (that is, 1 or more) such that $P(x)$ is true.

Universal Quantifier ∀

- Example:
  Let the u.d. of x be parking spaces at SNU.
  Let $F(x)$ be the *predicate* "x is full."
  Then the *universal quantification of* $F(x)$, $\forall x\, F(x)$,
  is the *proposition:*
  1. "All parking spaces at SNU are full."
  2. "Every parking space at SNU is full."
  3. "For each parking space at SNU, that space is full."

Existential Quantifier ∃

- Example:
  Let the u.d. of x be parking spaces at SNU.
  Let $F(x)$ be the *predicate* "x is full."
  Then the *existential quantification of* $F(x)$, $\exists x\, F(x)$, is the *proposition*:
  1. "Some parking space at SNU is full."
  2. "There is a parking space at SNU that is full."
  3. "At least one parking space at SNU is full."

Free and Bound Variables

- *Definition*:
  1. An expression like $P(x)$ is said to have a *free variable* x (meaning, x is undefined).
  2. A quantifier (either $\forall$ or $\exists$) *operates* on an expression having one or more free variables, and *binds* one or more of those variables, to produce an expression having one or more *bound variables*.

Examples

1. $P(x,y)$ has 2 free variables, x and y.
2. $\forall x\ P(x,y)$ has 1 free variable y, and one bound variable x.
3. $\forall x\ \forall y\ P(x,y)$ has zero free variables, which represents a proposition.

Nesting of Quantifiers

Example:

Let the u.d. of x and y be people.

Let $L(x,y)$="x likes y"

(A predicate with 2 free variables).

Then $\exists y\ L(x,y)$ = "There is someone whom x likes."

(A predicate with 1 free variable, x)

Then $\forall x\ \exists y\ L(x,y)$ = "Every one has someone whom they like."

(A predicate with 0 free variables)

Well-formed Formula (wff) for Predicate Logic

- *Definition*:

  A wff for (the first-order) predicate logic

  1. Every predicate formula is a wff.
  2. If P is a wff, $\neg P$ is a wff.
  3. Two wffs parenthesized and connected by $\wedge$, $\vee$, $\leftrightarrow$, $\rightarrow$ form a wff.
  4. If P is a wff and x is a variable then $(\forall x)P$ and $(\exists x)P$ are wff*s*.
  5. A finite string of symbols is a wff only when it is constructed by steps 1-4.

Examples

Let $R(x,y)$="x relies upon y". Express the following in unambiguous English:

1. $\forall x \exists y\ R(x,y)$ = Everyone has *someone* to rely on.
2. $\exists y \forall x\ R(x,y)$ = There's a poor overburdened soul whom *everyone* relies upon (including himself)!
3. $\exists x \forall y\ R(x,y)$ = There's some needy person who relies upon *everybody* (including himself).
4. $\forall y \exists x\ R(x,y)$ = Everyone has *someone* who relies upon them.
5. $\forall x \forall y\ R(x,y)$ = *Everyone* relies upon *everybody*. (including themselves)!

Natural language is ambiguous!

- "Everybody likes somebody."
  - For everybody, there is somebody he likes.
    - $\forall x \exists y\ Likes(x,y)$ [Probably more likely.]
  - There is somebody (a popular person) whom everyone likes.
    - $\exists y \forall x\ Likes(x,y)$
- "For everybody, there is somebody who likes him."
  - Same problem: $\forall y \exists x\ Likes(x,y)$, $\exists x \forall y\ Likes(x,y)$
  - Depends on context, emphasis.

More to Know About Binding

- $\forall x\ \exists x\ P(x)$ - x is not a free variable in $\exists x\ P(x)$, therefore the $\forall x$ binding isn't used.

- $(\forall x\ P(x)) \wedge Q(x)$ - The variable x is outside of the *scope* of the $\forall x$ quantifier, and is therefore free. Not a proposition!

- $(\forall x\ P(x)) \wedge (\exists x\ Q(x))$ – This is legal, because there are 2 different x's!

Quantifier Equivalence Laws

- Definitions of quantifiers: If u.d.=$a,b,c,\ldots$
  $\forall x\, P(x) \Leftrightarrow P(a) \wedge P(b) \wedge P(c) \wedge \ldots$
  $\exists x\, P(x) \Leftrightarrow P(a) \vee P(b) \vee P(c) \vee \ldots$

- From those, we can prove the laws:
  $\forall x\, P(x) \Leftrightarrow \neg(\exists x\, \neg P(x))$
  $\exists x\, P(x) \Leftrightarrow \neg(\forall x\, \neg P(x))$

More Equivalence Laws

- $\forall x\ \forall y\ P(x,y) \Leftrightarrow \forall y\ \forall x\ P(x,y)$
  $\exists x\ \exists y\ P(x,y) \Leftrightarrow \exists y\ \exists x\ P(x,y)$

- $\forall x\ (P(x) \wedge Q(x)) \Leftrightarrow (\forall x\ P(x)) \wedge (\forall x\ Q(x))$
  $\exists x\ (P(x) \vee Q(x)) \Leftrightarrow (\exists x\ P(x)) \vee (\exists x\ Q(x))$

Defining New Quantifiers

- *Definition*:

  $\exists!x\, P(x)$ is defined to mean "$P(x)$ is true of *exactly one* x in the universe of discourse."

- Note that $\exists!x\, P(x) \Leftrightarrow \exists x \left(P(x) \wedge \neg\exists y \left(P(y) \wedge \neg\, EQ(y,x)\right)\right)$
  "There is an x such that $P(x)$ holds and there is no y such that $P(y)$ and y is not equal to x."

Conversion of wff into Proposition

- The well-formed formula with variables becomes the proposition when all the variables are bound and the quantifiers are removed with appropriate value assignment to the variables.

Higher-order Logic

- First-order logic gets its name from the fact that one can quantify over objects (the first-order entities that actually exist in the world) but not over relations or functions on those objects. Higher-order logic allows us to quantify over relations and functions as well as over objects. For example, in higher-order logic we can say that two objects are equal if and only if all properties applied to them are equivalent. Or we could say that two functions are equal if and only if they have the same value for all arguments:

  1. $(\forall x)(\forall y)\ (x=y) \leftrightarrow (\forall P)(P(x)\leftrightarrow P(y))$
  2. $(\forall f)(\forall g)\ \ (f=g)\ \ \leftrightarrow (\forall x)(f(x)=g(x))$

Logic for Monotonic Reasoning and Nonmonotonic Reasoning

- A logic is monotonic if, when some new sentences are added to the knowledge base, all the sentences entailed by the original knowledge base are still entailed by the new larger knowledge base. Otherwise, it is nonmonotonic.

Examples

Let $L(x, y)$ be the statement "*x loves y*," where the universe of discourse for both x and y consists of all people in the world. Use quantifiers to express each of these statements.

a) Everybody loves Jerry. $(\forall x)\, L(x, Jerry)$

b) Everybody loves somebody. $(\forall x)(\exists y)\, L(x,y)$

c) There is somebody whom everybody loves. $(\exists y)\, (\forall x)\, L(x,y)$

d) Nobody loves everybody. $\neg\, (\exists\, x)(\forall y)\, L(x,y)$

e) There is somebody whom Lydia does not love. $(\exists x) \neg\, L(Lydia,x)$

f) There is somebody whom no one loves. $(\exists x)(\forall y)\, \neg L(y,x)$

g) There is exactly one person whom everybody loves. $(\exists! x)(\forall y) L(y,x)$

h) There are exactly two people whom Lynn loves.

$(\exists x)\, (\exists y)\, ((x \neq y) \wedge L(Lynn,x) \wedge L(\text{Lynn},y) \wedge (\forall z)\, (\, L(\text{Lynn},z) \rightarrow (z=x) \vee (z=y)\,)\,)$

i) Everyone loves himself or herself $(\forall x)\, L(x,x)$

j) There is someone who loves no one besides himself or herself.

$(\exists x)\, (\forall y)\, L(x,y) \leftrightarrow \text{x=y})$

Exercise

1. Let P, Q, and r be the proposition variables such that

   P : You have the flu.

   Q : You miss the final examination

   R : You pass the course

Express each of the following formulas as an English sentence.

(a) $(P \rightarrow \neg R) \vee (Q \rightarrow \neg R)$

(b) $(P \wedge Q) \vee (\neg Q \wedge R)$

2. Let P, Q, and R be the proposition variables such that

P : You get an A on the final exam.

Q : You do every exercise in this book

R : You get an A in this class

Write the following propositions using P, Q, R, and logical connectives.

(a) You get an A on the final, but you don't do every exercise in this book; nevertheless, you get an A in this class.

(b) Getting an A on the final and doing every exercise in this book is sufficient for getting an A in this class.

3. Assume the domain of all people.

Let $J(x)$ stand for "x is a junior", $S(x)$ stand for "x is a senior", and $L(x, y)$ stand for "x likes y". Translate the following into well-formed formulas:

(a) All people like some juniors.

(b) Some people like all juniors.

(c) Only seniors like juniors.

4. Let $B(x)$ stand for "x is a boy", $G(x)$ stand for "x is a girl", and $T(x,y)$ stand for "x is taller than y". Complete the well-formed formula representing the given statement by filling out ? part.

(a) Only girls are taller than boys: $(?)(\forall y)((? \wedge T(x,y)) \rightarrow ?)$

(b) Some girls are taller than boys: $(\exists x)(?)(G(x) \wedge (? \rightarrow ?))$

(c) Girls are taller than boys only: $(?)(\forall y)((G(x) \wedge ?) \rightarrow ?)$

(d) Some girls are not taller than any boy: $(\exists x)(?)(G(x) \wedge (? \rightarrow ?))$

(e) No girl is taller than any boy: $(?)(\forall y)((B(y) \wedge ?) \rightarrow ?)$

1-3. Proofs and Inference Rules

Proof Terminology

- *Theorem*

  A statement that has been proven to be true.

- *Axioms*, *postulates*, *hypotheses*, *premises*

  Assumptions (often unproven) defining the structures about which we are reasoning.

- *Lemma*

  A minor theorem used as a stepping-stone to proving a major theorem.

- *Corollary*

  A minor theorem proved as an easy consequence of a major theorem.
- *Theory*

  The set of all theorems that can be proven from a given set of axioms.
- *Rules of inference*

  Patterns of deriving conclusions from hypotheses: *Sound* and *Complete*.

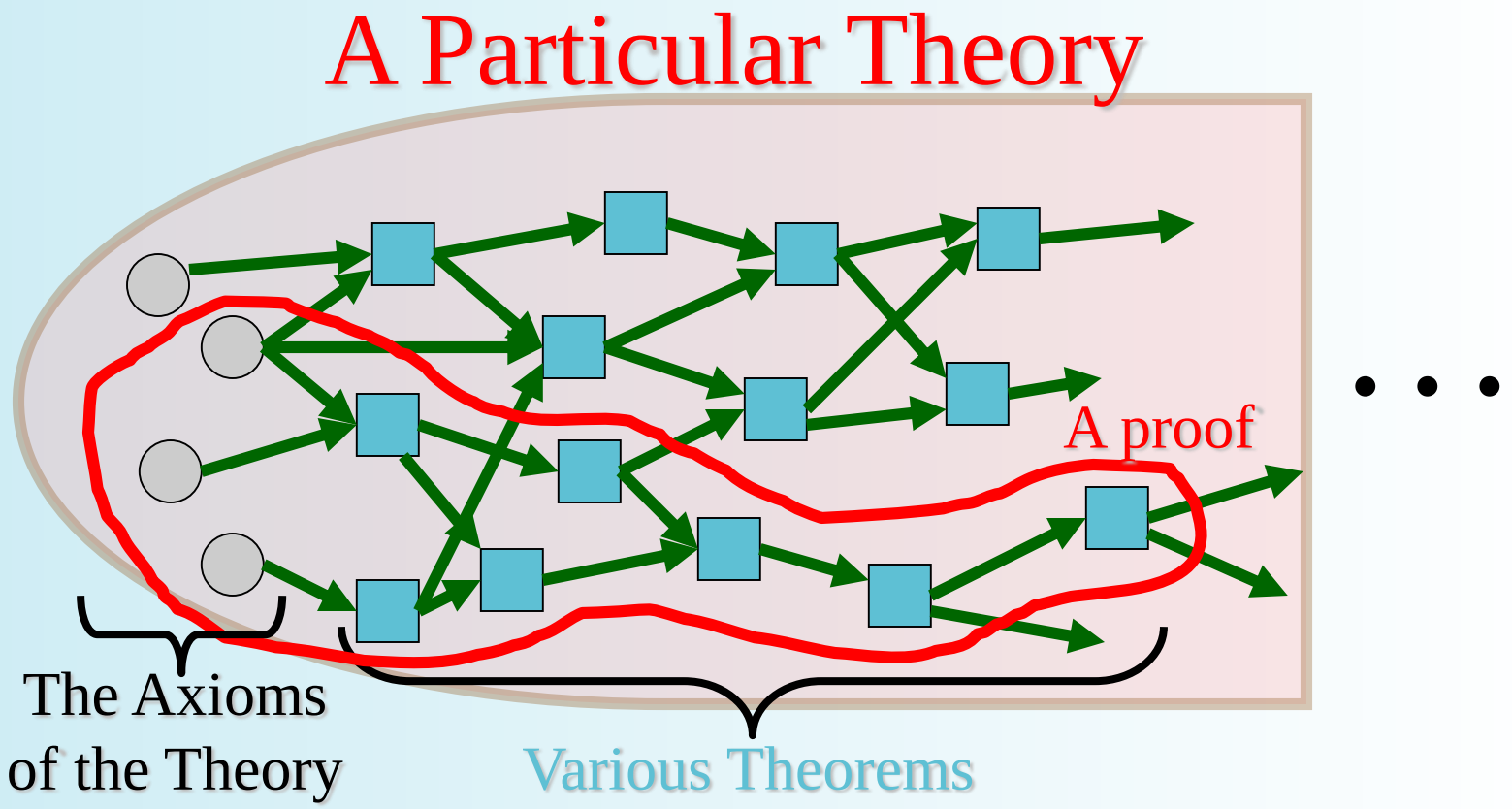
Depending on Inference Rules

- Deduction: $A \rightarrow B,\ A \Rightarrow B$
- Induction:

$$x \rightarrow B,\ y \rightarrow B,\ \ x,y \in A \Rightarrow \forall z \in A,\ \ z \rightarrow B$$

- Abduction: $A \rightarrow B,\ B \Rightarrow A$

Graphical Visualization



Inference Rules: General Form

- *Inference Rule*:

  Pattern establishing that if we know that a set of *antecedent* statements of certain forms are all true, then a certain related *consequent* statement is true (valid arguments).

- *antecedent 1*
  antecedent 2 ...
  ∴ *consequent*

  "∴" means "therefore"

Inference Rules: Implications

- Each logical inference rule corresponds to an implication that is a *tautology*.

- *antecedent 1*
  antecedent 2 ...

  $\therefore$ *consequent*

  Inference rule

- Corresponding tautology:

  $((ante.\ 1) \wedge (ante.\ 2) \wedge \ldots) \Rightarrow consequent$

Implication Tautologies

I_1 $P \wedge Q \Rightarrow P$

I_2 $P \wedge Q \Rightarrow Q$

I_3 $P \Rightarrow P \vee Q$

I_4 $Q \Rightarrow P \vee Q$

I_5 $\neg P \Rightarrow P \rightarrow Q$

I_6 $Q \Rightarrow P \rightarrow Q$

I_7 $\neg(P \rightarrow Q) \Rightarrow P$

I_8 $\neg(P \rightarrow Q) \Rightarrow \neg Q$

I_9 $P, Q \Rightarrow P \wedge Q$

I_{10} $\neg P, P \vee Q \Rightarrow Q$

I_{11} $P, P \rightarrow Q \Rightarrow Q$

I_{12} $\neg Q, P \rightarrow Q \Rightarrow \neg P$

I_{13} $P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$

I_{14} $P \vee Q, P \rightarrow R, Q \rightarrow R \Rightarrow R$

I_{15} $(\forall x)A(x) \vee (\forall x)B(x)$
$\Rightarrow (\forall x)(A(x) \vee B(x))$

I_{16} $(\exists x)(A(x) \wedge B(x))$
$\Rightarrow (\exists x)A(x) \wedge (\exists x)B(x)$

Biconditional Tautologies: Equivalences

E_1 $\neg\neg P \Leftrightarrow P$

E_2 $P \wedge Q \Leftrightarrow Q \wedge P$

E_3 $P \vee Q \Leftrightarrow Q \vee P$

E_4 $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$

E_5 $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$

E_6 $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$

E_7 $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$

E_8 $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$

E_9 $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$

E_{10} $P \vee P \Leftrightarrow P$

E_{11} $P \wedge P \Leftrightarrow P$

E_{12} $R \vee (P \wedge \neg P) \Leftrightarrow R$

E_{13} $R \wedge (P \vee \neg P) \Leftrightarrow R$

E_{14} $R \vee (P \vee \neg P) \Leftrightarrow T$

E_{15} $R \wedge (P \wedge \neg P) \Leftrightarrow F$

E_{16} $P \rightarrow Q \Leftrightarrow \neg P \vee Q$

E_{17} $\neg(P \rightarrow Q) \Leftrightarrow P \wedge \neg Q$

E_{18} $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$

E_{19} $P \rightarrow (Q \rightarrow R) \Leftrightarrow (P \wedge Q) \rightarrow R$

E_{20} $\neg(P \leftrightarrow Q) \Leftrightarrow (P \leftrightarrow \neg Q)$

E_{21} $(P \leftrightarrow Q) \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$

E_{22} $(P \leftrightarrow Q) \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$

E_{23} $(\exists x)(A(x) \vee B(x)) \Leftrightarrow (\exists x)A(x) \vee (\exists x)B(x)$

E_{24} $(\forall x)(A(x) \wedge B(x)) \Leftrightarrow (\forall x)A(x) \wedge (\forall x)B(x)$

E_{25} $\neg(\exists x)A(x) \Leftrightarrow (\forall x)\neg A(x)$

E_{26} $\neg(\forall x)A(x) \Leftrightarrow (\exists x)\neg A(x)$

E_{27} $(\forall x)(A \vee B(x)) \Leftrightarrow A \vee (\forall x)B(x)$

E_{28} $(\exists x)(A \wedge B(x)) \Leftrightarrow A \wedge (\exists x)B(x)$

E_{29} $(\forall x)A(x) \rightarrow B \Leftrightarrow (\exists x)(A(x) \rightarrow B)$

E_{30} $(\exists x)A(x) \rightarrow B \Leftrightarrow (\forall x)(A(x) \rightarrow B)$

E_{31} $A \rightarrow (\forall x)B(x) \Leftrightarrow (\forall x)(A \rightarrow B(x))$

E_{32} $A \rightarrow (\exists x)B(x) \Leftrightarrow (\exists x)(A \rightarrow B(x))$

E_{33} $(\exists x)(A(x) \rightarrow B(x)) \Leftrightarrow (\forall x)A(x) \rightarrow \exists x B(x))$

Formal Proofs

- *Definition*:
  1. A formal proof of a conclusion C, given premises P_1, $P_2, \ldots, P_n$ consists of a sequence of *steps*, each of which applies some inference rule to premises or to previously-proven statements (as antecedents) to yield a new true statement (the consequent).
  2. Inference Rules
     - Rule ***P*** : premise
     - Rule ***T*** : tautology
     - Rule ***CP*** : conditional premise

- Note that a proof demonstrates that *if* the premises are true, *then* the conclusion is true.

Examples:

1. Suppose we have the following premises:
   (1) It is not sunny and it is cold.
   (2) We will swim only if it is sunny.
   (3) If we do not swim, then we will canoe.
   (4) If we canoe, then we will be home early.

Given these premises, prove using inference rules the theorem, “We will be home early”.

Proof:

Let us adopt the following abbreviations:

sunny = “It is sunny”; *cold* = “It is cold”;

swim = “We will swim”; *canoe* = “We will canoe”;

early = “We will be home early”.

Then, the premises can be represented by the following formulas:

$\neg sunny \wedge cold$, $swim \rightarrow sunny$, $\neg swim \rightarrow canoe$, $canoe \rightarrow early$.

Based on these formulas, the *proof* would be

Step	Inference Rule
(1) $\neg sunny \wedge cold$	***P***
(2) $\neg sunny$	***T***, (1) and $\boldsymbol{I_1}$
(3) $swim \rightarrow sunny$	***P***
(4) $\neg swim$	***T***, (2), (3) and $\boldsymbol{I_{12}}$
(5) $\neg swim \rightarrow canoe$	***P***
(6) *canoe*	***T***, (4), (5) and $\boldsymbol{I_{11}}$
(7) $canoe \rightarrow early$	***P***
(8) *early*	***T***, (6), (7), and $\boldsymbol{I_{11}}$

2. Show that ($R \rightarrow S$) can be derived from ($P \rightarrow (Q \rightarrow S)$), ($\neg R \vee P$), and Q. (Instead of deriving $R \rightarrow S$ directly, we shall include R as an additional premise and show S can be derive from there premises.)

Proof:

Step		Inference Rule
(1)	$\neg R \vee P$	***P***
(2)	R	***P*** (assumed premise)
(3)	P	***T***, (1), (2) and $\boldsymbol{I_{10}}$
(4)	$P \rightarrow (Q \rightarrow S)$	***P***
(5)	$Q \rightarrow S$	***T***, (3), (4) and $\boldsymbol{I_{11}}$
(6)	Q	***P***
(7)	S	***T***, (5), (6) and $\boldsymbol{I_{11}}$
(8)	$R \rightarrow S$	***CP***, (2), (7)

3. Show that $S \vee R$ can be derived from $(P \vee Q)$, $(P \rightarrow R)$ and $(Q \rightarrow S)$.

Proof:

Step		Inference Rule
(1)	$P \vee Q$	***P***
(2)	$\neg P \rightarrow Q$	***T,*** (1) , $\boldsymbol{E_1}$ and $\boldsymbol{E_{16}}$
(3)	$Q \rightarrow S$	***P***
(4)	$\neg P \rightarrow S$	***T,*** (2), (3), and $\boldsymbol{I_{13}}$
(5)	$\neg S \rightarrow P$	***T***, (4) , $\boldsymbol{E_{18}}$ and $\boldsymbol{E_1}$
(6)	$P \rightarrow R$	***P***
(7)	$\neg S \rightarrow R$	***T,*** (5), (6), and $\boldsymbol{I_{13}}$
(8)	$S \vee R$	***T***, (7), $\boldsymbol{E_{16}}$ and $\boldsymbol{E_1}$

Inference Rules for Quantifiers

- $\dfrac{\forall x\, P(x)}{\therefore P(o)}$ Universal Specification (***US***)
  (substitute *any* object o)
- $\dfrac{P(g)}{\therefore \forall x\, P(x)}$ (for *general* element g of u.d.)
  Universal Generalization (***UG***)
- $\dfrac{\exists x\, P(x)}{\therefore P(c)}$ Existential Specification (***ES***)
  (substitute *some* object c)
- $\dfrac{P(o)}{\therefore \exists x\, P(x)}$ (for some extant object o)
  Existential Generalization (***EG***)

Examples:

1. Show that

$(\forall x)\,(P(x) \rightarrow Q(x))\,,\,(\forall x)\,(Q(x) \rightarrow R(x)) \Rightarrow (\forall x)\,(P(x) \rightarrow R(x))$

Proof:

Step		Inference Rule
(1)	$(\forall x)\,(P(x) \rightarrow Q(x))$	***P***
(2)	$P(y) \rightarrow Q(y)$	***US***, (1)
(3)	$(\forall x)\,(Q(x) \rightarrow R(x))$	***P***
(4)	$Q(y) \rightarrow R(y)$	***US***, (3)
(5)	$P(y) \rightarrow R(y)$	***T***, (2), (4) and $\boldsymbol{I_{13}}$
(6)	$(\forall x)\,(P(x) \rightarrow R(x))$	***UG***, (5)

2. Show that from $(\exists x)\,(F(x) \wedge S(x)) \rightarrow (\forall y)\,(M(y) \rightarrow W(y))$ and $(\exists y)\,(M(y) \wedge \neg W(y))$, the conclusion $(\forall x)\,(F(x) \rightarrow \neg\, S(x))$ logically follows.

Proof:

Step		Inference Rule
(1)	$(\exists y)\,(M(y) \wedge \neg W(y))$	***P***
(2)	$M(z) \wedge \neg W(z)$	***ES***, (1)
(3)	$\neg\,(M(z) \rightarrow W(z))$	***T***, (2) and $\boldsymbol{E_{17}}$
(4)	$(\exists y) \neg\,(M(y) \rightarrow W(y))$	***EG***, (3)
(5)	$\neg(\forall y)(M(y) \rightarrow W(y))$	***T***, (4) and $\boldsymbol{E_{26}}$
(6)	$(\exists x)\,(F(x) \wedge S(x)) \rightarrow (\forall y)\,(M(y) \rightarrow W(y))$	***P***
(7)	$\neg(\exists x)\,(F(x) \wedge S(x))$	***T***, (5), (6) and $\boldsymbol{I_{12}}$
(8)	$(\forall x) \neg(F(x) \wedge S(x))$	***T***, (7) and $\boldsymbol{E_{25}}$
(9)	$\neg(F(x) \wedge S(x))$	***US***, (8)
(10)	$F(x) \rightarrow \neg\, S(x)$	***T***, (9), $\boldsymbol{E_8}$ and $\boldsymbol{E_{16}}$
(11)	$(\forall x)\,(F(x) \rightarrow \neg\, S(x))$	***UG***, (10)

Restriction

- ***UG*** applicable variable should not be free in any of the given premises
- ***UG*** should not be applied to the free variables after ***ES*** making some variable free in a prior step.

$(\forall x)(\exists z)\, A(z,x)$

$\Rightarrow (\exists z)A(z,x)$ *by* ***US***

$\Rightarrow A(z,x)$ *by* ***ES***

$\Rightarrow (\forall x)A(z,x)$ *by* ***UG*** (not allowed!)

$\Rightarrow (\exists z)\,(\forall x)A(z,x)$ *by* ***EG*** contradiction!

Proof Methods for Implications

For proving implications $P \rightarrow Q$, we have:

- *Direct* proof: Assume P is true, and prove Q.
- *Indirect* proof: Assume $\neg Q$, and prove $\neg P$.
- *Vacuous* proof: Prove $\neg P$ by itself.
- *Trivial* proof: Prove Q by itself.
- Proof by cases:
  Show $P \rightarrow (A \vee B)$, and $(A \rightarrow Q)$ and $(B \rightarrow Q)$.

Example of Direct Proof

- *Definition*:

  An integer n is called *odd* iff $n=2k+1$ for some integer k; n is *even* iff $n=2k$ for some k.

- *Axiom*:

  Every integer is either odd or even.

- *Theorem*:

  (For all numbers n) If n is an odd integer, then n^2 is an odd integer.

  Proof:

  If n is odd, then $n = 2k+1$ for some integer k. Thus, $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Therefore n^2 is of the form $2j + 1$ (with j the integer $2k^2 + 2k$), thus n^2 is odd. □

Example of Indirect Proof

- *Theorem*: (For all integers n)
  If $3n+2$ is odd, then n is odd.

  Proof:

  Suppose that the conclusion is false, *i.e.*, that n is even. Then $n=2k$ for some integer k. Then $3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1)$. Thus $3n+2$ is even, because it equals $2j$ for integer $j = 3k+1$. So $3n+2$ is not odd. We have shown that $\neg(n \text{ is odd}) \rightarrow \neg(3n+2 \text{ is odd})$, thus its contra-positive $(3n+2 \text{ is odd}) \rightarrow (n \text{ is odd})$ is also true. □

Example of Vacuous Proof

- *Theorem*: If n is both odd and even, then $n^2 = n + n$.

  Proof:

  The statement "n is both odd and even" is necessarily false, since no number can be both odd and even. So, the theorem is vacuously true. □

Example of Trivial Proof

- *Theorem*: (For integers *n*) If *n* is the sum of two prime numbers, then either *n* is odd or *n* is even.

  Proof:

  Any integer *n* is either odd or even. So the conclusion of the implication is true regardless of the truth of the antecedent.

  Thus the implication is true trivially. □

Proof by Contradiction

1. A method for proving P.
2. Assume $\neg P$, and prove both Q and $\neg Q$ for some proposition Q.
3. Thus $\neg P \rightarrow (Q \wedge \neg Q)$
4. $(Q \wedge \neg Q)$ is a trivial contradiction, equal to F
5. Thus $\neg P \rightarrow$F, which is only true if $\neg P$=F
6. Thus P is true.

Proving Existentials

1. A proof of a statement of the form $\exists x\, P(x)$ is called an *existence proof*.
2. If the proof demonstrates how to actually find or construct a specific element a such that $P(a)$ is true, then it is a *constructive* proof.
3. Otherwise, it is *nonconstructive*.

Constructive Existence Proof

- *Theorem*:

  There exists a positive integer n that is the sum of two perfect cubes in two different ways:

  - equal to $j^3 + k^3$ and $l^3 + m^3$ where j, k, l, m are positive integers, and $\{j,k\} \neq \{l,m\}$

  Proof:

  Consider $n = 1729$, $j = 9$, $k = 10$, $l = 1$, $m = 12$. Now just check that the equalities hold.

Nonconstructive Existence Proof

- *Theorem*:

  There are infinitely many prime numbers.

  Proof:

  Any finite set of numbers must contain a maximal element, so we can prove the theorem if we can just show that there is *no* largest prime number.

  i.e., show that for any prime number, there is a larger number that is *also* prime.

  More generally: For *any* number, $\exists$ a larger prime.

  Formally: Show $\forall n \, \exists p \, ((p>n) \wedge (p \text{ is prime}))$.

Given $n>0$, prove there is a prime $p>n$.

Consider $x = n!+1$. Since $x>1$, we know

(x is prime)$\vee$(x is composite).

Case 1: x is prime.

Obviously $x>n$, so let $p=x$ and we're done.

Case 2: x has a prime factor p.

But if $p \leq n$, then $x \bmod p = 1$.

So $p>n$, and we're done.

Uniqueness Proof

- Some theorems assert the existence of a unique element with a particular property.

- To prove a statements of this type, we show following two parts.
  1. Existence: element x with a desired property exists
  2. Uniqueness: if $y \neq x$, then y does not have the desired property

Example of Uniqueness Proof

- *Theorem*:
  "Every integer has a unique additive inverse."

  Proof:

  If p is an integer, we find that $p+q=0$ where $p=-q$ and q is also an integer. Consequently, there exists an integer q such that $p+q=0$. (Existence)

  if r is an integer with $r \neq q$ such that $p+r=0$. then $p+q=p+r$. So We can show $q=r$, which contradicts our assumption $r \neq q$. Consequently, there is a unique integer q such that $p+q=0$. □

Exercise

1. Prove that the square of an even number is an even number using
   (a) A direct proof
   (b) An indirect proof
   (c) A proof by contradiction

2. Prove formally using inference rules that $R \wedge (P \vee Q)$ logically follows from $(P \vee Q)$, $(Q \rightarrow R)$, $(P \rightarrow M)$, and $\neg M$.

3. Prove that if n is a positive integer, then n is a even if and only if $7n+4$ is even.

4. Let P, Q, R and S be statement variables.

   Prove formally the following.

   (a) $\neg P \vee Q, \neg Q \vee R, R \rightarrow S \Rightarrow P \rightarrow S$

   (b) $\neg P \wedge (P \vee Q) \Rightarrow Q$

5. Show the following implication.

   (a) $(\forall x)(P(x) \vee Q(x)), (\forall x) \neg P(x) \Rightarrow (\exists x) Q(x)$

   (b) $\neg((\exists x) P(x) \wedge Q(a)) \Rightarrow (\exists x) P(x) \rightarrow \neg Q(a)$