Discrete Structures for Computing

CSCE 222

Sandeep Kumar

Many slides based on [Lee19], [Rog21], [GK22]

About me

- Teaching at A&M for one and a half years now.
- Prior to coming here, spent time in both academia and industry.
- Taught CSCE 111/222/313 in the last three semesters.
- Unfortunately, I've acquired a bit of a bad rap!

  > *I have taken two of the previously rated "hardest professors" at this university (via 3rd party polls) and gotten A's in both classes; they both pale in comparison to [CSCE 222]...*

- My exams and homeworks can [sometimes] appear to be tough, but
  - They get calibrated each time I teach.
  - You can control my pace in class by asking questions.
- I'm expecting the class to be a symbiotic learning experience.

Chapter 00—Administrivia

Administrivia

- Text book—*Discrete Mathematics and its Applications* 8^{th} ed., by Kenneth Rosen.
- $\approx$ Bi-weekly homeworks worth 40%.
  - Typeset in LaTeX, converted to PDF.
  - Some homeworks may be programming assignments.
  - Maybe extra credit in homeworks—beyond the classroom.
- Two midterms $\approx$ 30%, and a final $\approx$ 30%.
  - The final exam can make a difference between an **A** and a **B**.
  - Attending classes will be very useful!
- Don't want the class to become *too* abstract.
- Attendance **not** compulsory.
  - But I'll take attendance and report it if the university asks for it.
  - I may take pictures of the class to verify attendance.
- Keep a dated copy (mail *Sent* folder) of relevant communication.
- Lecture slides finalized sometime *after* the lecture.

Administrivia...

- Prefer Slack or Discord for discussion?
- Please complete "day one tasks" on Canvas.
  - Fill out the Google form to *introduce yourself*.
  - Mark your attendance for today.

Rough Schedule

Week	Topic	Reading
1-3	Propositional & Predicate Calculus	Sect 1.1–1.8
4-5	Sets, Functions, Denumerability	Sect 2.1–2.6
6	Algorithms and their Complexity	Chapter 3
7-8	Elementary Number Theory	Chapter 4
9-10	Induction and Recursion	Chapter 5
11	Counting	Sect 6.1–6.4
12	Relations	Chapter 9
13-15	Models of Computation	Chapter 13

Why Study Discrete Math?

- To acquire the essentials to understand the mathematical language used in computer science.
- Develop algorithmic thinking—specify *algorithms*, analyze the memory and time required by the execution of the algorithm, and verify that the algorithm produces the correct answer.
- Applications and Modeling—appreciate and understand the wide range of applications of the topics covered in discrete mathematics, and build the ability to develop new models in various domains.
  - https://schnekli-tamu.uc.r.appspot.com/sudoku.

Announcements for 2/14

- Don't sweat the quiz 1 marks.
  - A test is just one sample from a distribution.
  - I will curve your cumulative score before assigning a letter grade.
  - $A \geq 90$ is only an approximation.
- You should get another homework this week.
- Mid-term on thursday 2/23. Will include everything we cover in class upto 2/21.

Chapter 01

Propositional Logic

Chapter 1

Chapter Summary

- Propositional Logic
  - The Language of Propositions
  - Applications
  - Logical Equivalences
- Predicate Logic
  - The Language of Quantifiers
  - Logical Equivalences
  - Nested Quantifiers
- Proofs
  - Rules of Inference
  - Proof Methods
  - Proof Strategy

Propositional Logic Summary

- The Language of Propositions
  - Connectives
  - Truth Values
  - Truth Tables
- Applications
  - Translating English Sentences
  - System Specifications
  - Logic Puzzles
  - Logic Circuits
- Logical Equivalences
  - Important Equivalences
  - Showing Equivalence
  - Satisfiability

Section 1.1 Summary

- Propositions
- Connectives
  - Negation
  - Conjunction
  - Disjunction
  - Implication; contrapositive, inverse, converse
  - Biconditional
- Truth Tables

Propositions

A *proposition* is a declarative sentence that is either true or false.

Examples of propositions:

- The Moon is made of green cheese.
- Trenton is the capital of New Jersey.
- Toronto is the capital of Canada.
- $1 + 0 = 1$
- $0 + 0 = 2$

Examples that are not propositions.

- Sit down!
- What time is it?
- $x + 1 = 2$
- $x + y = z$

Propositional Logic

Constructing Propositions

- Propositional Variables: $p, q, r, s, \ldots$
  - A variable that represents propositions is called a propositional variable.
  - Propositional variables in logic play the same role as numerical variables in arithmetic.
- The proposition that is always true is denoted by **T** and the proposition that is always false is denoted by **F**.
- Compound Propositions; constructed from logical connectives and other propositions.
  - Negation $\neg$
  - Conjunction $\wedge$
  - Disjunction $\vee$
  - Implication $\rightarrow$
  - Biconditional $\leftrightarrow$

Compound Propositions: Negation

The *negation* of a proposition p is denoted by $\neg p$ and has this truth table:

p	$\neg p$
T	F
F	T

Example: If p denotes "The earth is round", then

- $\neg p$ denotes "It is not the case that the earth is round"
- Or more simply, "The earth is not round."

Conjunction

The conjunction of propositions p and q is denoted by $p \wedge q$ and has this truth table.

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

Example: If

- p denotes "I am at home" and,
- q denotes "It is raining", then
- $p \wedge q$ denotes "I am at home *and* it is raining."

Disjunction

The disjunction of propositions p and q is denoted by $p \vee q$ and has this truth table.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Example:

- p denotes "I am at home" and,
- q denotes "It is raining", then,
- $p \vee q$ denotes "I am at home *or* it is raining."

The Connective *or* in English

In English, "or" has two distinct meanings.

- "Inclusive Or"—In the sentence "Students who have taken CS202 or Math120 may take this class," we assume that students need to have taken one of the prerequisites, but may have taken both. This is the meaning of disjunction. For $p \vee q$ to be true, either one or both of p and q must be true.
- "Exclusive Or"—When reading the sentence "Soup or salad comes with this entrée," we do not expect to be able to get both soup and salad. This is the meaning of Exclusive Or (Xor). In $p \oplus q$, one of p and q must be true, but not both. The truth table for $\oplus$ is.

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Implication

If p and q are propositions, then $p \rightarrow q$ is a *conditional statement* or *implication* which is read as "*if p, then q*" and has this truth table.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Example:

- p denotes "I am at home" and,
- q denotes "It is raining", then,
- $p \rightarrow q$ denotes "If I am at home then it is raining."

In $p \rightarrow q$, p is the hypothesis (antecedent or premise) and q is the conclusion (or consequence).

Understanding Implication

In $p \rightarrow q$ there does not need to be any connection between the antecedent or the consequent. The "meaning" of $p \rightarrow q$ depends only on the truth values of p and q.

These implications are perfectly fine, but would not be used in ordinary English.

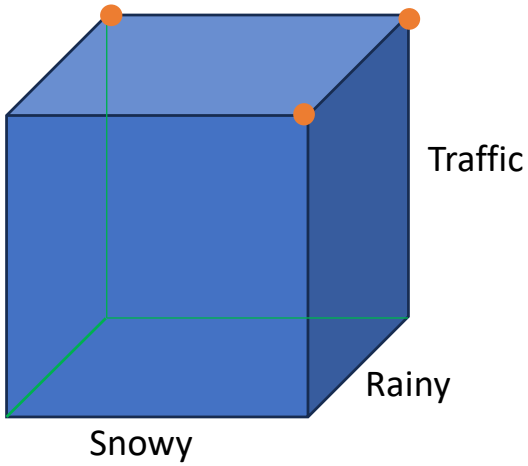
- "If the moon is made of green cheese, then I have more money than Bill Gates."
- "If the moon is made of green cheese, then I'm on welfare."
- "If $1 + 1 = 3$, then your grandma wears combat boots."

Understanding Implication. . .

One way to view the logical conditional is to think of an obligation or contract.

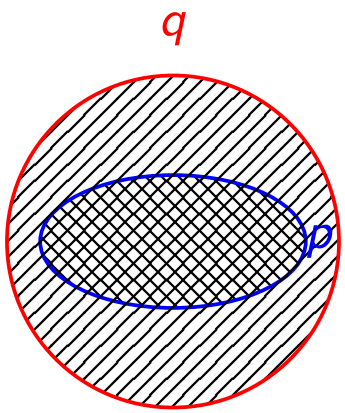
- "*If* I am elected, *then* I will lower taxes."
- "*If* you get 100% on the final, *then* you will get an A."

If the politician is elected and does **not** lower taxes, then the voters can say that he or she has broken the campaign pledge (false implication). Something similar holds for the professor. This corresponds to the case where p is true and q is false.



$Rainy \vee Snowy \rightarrow Traffic?$

Different Ways of Expressing p $\rightarrow$ q



- **if** p, **then** q
- **if** p, q
- q **unless** $\neg p$
  - q is true unless p is false.
  - we can't say anything about q when p is false.
- q **if** p
- q **whenever** p
- q **follows from** p
- p **implies** q
- p **only if** q
- q **when** p
- p **is sufficient for** q
- q **is necessary for** p

a necessary condition for p **is** q, **a sufficient condition for** q is p

Converse, Contrapositive, and Inverse

From $p \to q$ we can form new conditional statements.

- $q \to p$ is the **converse** of $p \to q$
- $\neg q \to \neg p$ is the **contrapositive** of $p \to q$
- $\neg p \to \neg q$ is the **inverse** of $p \to q$

Example: Find the converse, inverse, and contrapositive of "It raining is a sufficient condition for my not going to town."

Let p be *it's raining*, and q be *going to town*.

- **converse**:
  - If I do not go to town, then it is raining.
- **inverse**:
  - If it is not raining, then I will go to town.
- **contrapositive**:
  - If I go to town, then it is not raining.

Biconditional

If p and q are propositions, then we can form the *biconditional* proposition $p \leftrightarrow q$, read as "p *if and only if* q." The biconditional $p \leftrightarrow q$ denotes the proposition with this truth table:

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

Example:

- p denotes "I am at home" and,
- q denotes "It is raining", then,
- $p \leftrightarrow q$ denotes "I am at home if and only if it is raining."

Expressing the Biconditional

Some alternative ways "p if and only if q" is expressed in English:

- p **is necessary and sufficient** for q
- **if** p **then** q, **and conversely**
- p **iff** q

Truth Tables For Compound Propositions

Construction of a truth table:

Rows

- Need a row for every possible combination of values for the atomic propositions.

Columns

- Need a column for the compound proposition (usually at far right)
- Need a column for the truth value of each expression that occurs in the compound proposition as it is built up.
  - This includes the atomic propositions

Example Truth Table

Construct a truth table for $p \vee q \rightarrow \neg r$

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

See https://schnekli-tamu.uc.r.appspot.com/logic.

Equivalent Propositions

Two propositions are equivalent if they always have the same truth value.

Example: Show using a truth table that the conditional $(p \rightarrow q)$ is equivalent to the contrapositive $(\neg q \rightarrow \neg p)$.

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

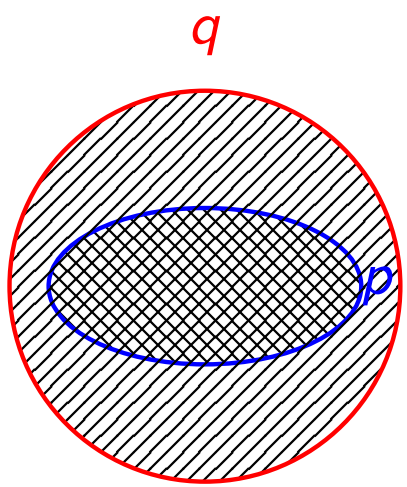
Logical Equivalence

- Intuitively, two sentences are equivalent if they say the same thing.
- I.e., they are *true* in exactly the same "worlds".
- More formally, we say that ϕ is logically equivalent to ψ iff
  - every truth assignment that satisfies ϕ satisfies ψ, and,
  - every truth assignment that satisfies ψ satisfies ϕ.
- $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$.
- $(p \wedge q) \not\equiv (p \vee q)$.
- Logically equivalence $\rightarrow$ substitutability.
  - If $\phi \equiv \psi$, then we can substitute ϕ for ψ in any propositional logic sentence and the result will be logically equivalent to the original sentence.
  - Not true for all logics, for e.g., intuitionistic logic.

Using a Truth Table to Show Non-Equivalence

Example: Show using truth tables that neither the converse nor inverse of an implication are equivalent to the implication.

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



Logical Entailment

We say that a sentence ϕ logically entails a sentence ψ (written $\phi \models \psi$) iff every truth assignment that satisfies ϕ also satisfies ψ.

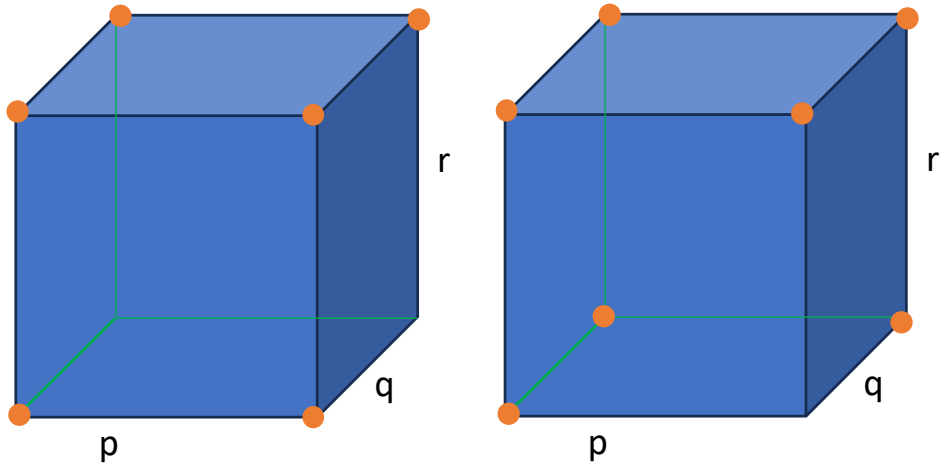
- Does $p \models (p \wedge q)$?
- Logical entailment is not the same as logical equivalence.
- Basically, *implication* in all possible "worlds".

p	q	p	$p \wedge q$
f	f	f	f
f	t	f	f
t	f	t	f
t	t	t	t

Use the Truth Table Method to answer the following.

- $\{p \rightarrow q \vee r\} \models (p \rightarrow r)$?
  - F. Consider $p = T, q = T, r = F$, which makes the LHS T but the RHS F.
- $\{p \rightarrow r\} \models (p \rightarrow q \vee r)$?
  - T.
- $\{q \rightarrow r\} \models (p \rightarrow q \vee r)$?
  - F. Consider $q = F, r = F, p = T$.

Logical Entailment. . .



- Cube 1: $q = 1$ is the back wall. Where is the implication false?
  - On the back wall where $r = 0$.
- Cube 2: $p = 1$ on the right wall of the cube. $q \vee r$ is false when both $q = 0$ and $r = 0$.

Problem

- How many rows are there in a truth table with n propositional variables?
- 2^n.
  - 40 folds of a paper $1mm$ thick generates a thickness of 1 million km. That's more than the distance from the earth to the moon.

$$1\text{mm} \times 2^{40} \approx 1M\text{km} > 382,240\text{km}$$

  - At 1 million evaluations per second, a 40 variable expression requires 12 days to run through the entire truth table.

$$2^{40}/10^6/3600/24 \approx 12 \text{ days}$$

How many propositional expressions on n variables?

- How many rows in truth table?
- How many functions?

Precedence of Logical Operators

Operator	*Precedence*
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

- $p \vee q \rightarrow \neg r$ is equivalent to $(p \vee q) \rightarrow \neg r$.
- If the intended meaning is $p \vee (q \rightarrow \neg r)$, then parentheses must be used.

Applications of Propositional Logic: Summary

- Translating English to Propositional Logic
- System Specifications
- Boolean Searching
- Logic Puzzles
- Logic Circuits
- AI Diagnosis Method

Translating English Sentences

Steps to convert an English sentence to a statement in propositional logic.

- Identify atomic propositions and represent using propositional variables.
- Determine appropriate logical connectives.

"If I go to Harry's or to the country, I will not go shopping."

- p: I go to Harry's
- q: I go to the country.
- r: I will go shopping.

- If p or q then not r.
- $(p \vee q) \rightarrow \neg r$.

Example

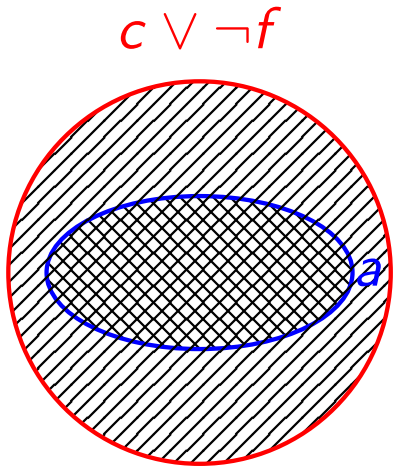
Problem: Translate the following sentence into propositional logic:

"You can access the Internet from campus only if you are a computer science major or you are not a freshman."

Let a, c, and f represent respectively "You can access the internet from campus," "You are a computer science major," and "You are a freshman."

$a \rightarrow (c \vee \neg f)$. Why isn't it $(c \vee \neg f) \rightarrow a$?

That is a sufficiency condition for $(c \vee \neg f)$, meaning that if $(c \vee \neg f)$ then we can deduce a. But a may be false even when $(c \vee \neg f)$.



"You can only get a scholarship if you're a college student."

System Specifications

System and Software engineers take requirements in English and express them in a precise specification language based on logic.

Example: Express in propositional logic: "The automated reply cannot be sent when the file system is full."

Solution: One possibility:

- Let $p =$ "The automated reply can be sent", and
- Let $q =$ "The file system is full."

$$q \rightarrow \neg p$$

Consistent System Specifications

Definition: A list of propositions is *consistent* if it is possible to assign truth values to the proposition variables so that each proposition is true. I.e., their conjunction is *satisfiable*.

Are these specifications consistent?

- "The diagnostic message is stored in the buffer or it is retransmitted."
- "The diagnostic message is not stored in the buffer."
- "If the diagnostic message is stored in the buffer, then it is retransmitted."

Solution: Let

- $p =$ "The diagnostic message is stored in the buffer."
- $q =$ "The diagnostic message is retransmitted."

The specification can be written as: $p \vee q$, $\neg p$, $p \rightarrow q$. When p is false and q is true all three statements are true. **So the specification is consistent**.

- What if "The diagnostic message is not retransmitted" is added.
- Solution: Now we are adding $\neg q$ and there is no satisfying assignment. **So the specification is not consistent**.

Putting it together

Propositions:

P_1—Person 1 rides the bus.
P_2—Person 2 rides the bus.
...
P_n—Person n rides the bus.

But we can't have either of the following happen:

- That either P_1 or P_2 ride the bus and P_3 or P_4 ride the bus.
- P_2 or P_3 ride the bus and either P_4 rides the bus or P_5 doesn't.

Represent it in propositional form:

$$\neg(((P_1 \vee P_2) \wedge (P_3 \vee P_4)) \vee ((P_2 \vee P_3) \wedge (P_4 \vee \neg P_5)))$$

- Can P_3 ride the bus?
- Can P_3 and P_4 ride the bus together?

Logic Puzzles

An island has two kinds of inhabitants, *knights*, who always tell the truth, and *knaves*, who always lie.

You go to the island and meet A and B.

- A says "B is a knight."
- B says "The two of us are of opposite types."

What are the types of A and B? Let

- p refer to "A is a knight". Then, $\neg p$ represents that "A is a knave".
- q refer to "B is a knight". Then, $\neg q$ represents that "B is a knave".

Then,

- If A is a knight, then p is true. Since knights tell the truth, q must also be true. Then $(p \wedge \neg q) \vee (\neg p \wedge q)$ would have to be true, but it is not. So, A is not a knight and therefore $\neg p$ must be true.
- If A is a knave, then B must not be a knight since knaves always lie. So, then both $\neg p$ and $\neg q$ hold since both are knaves. I.e., the expression

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

has a satisfying assignment.

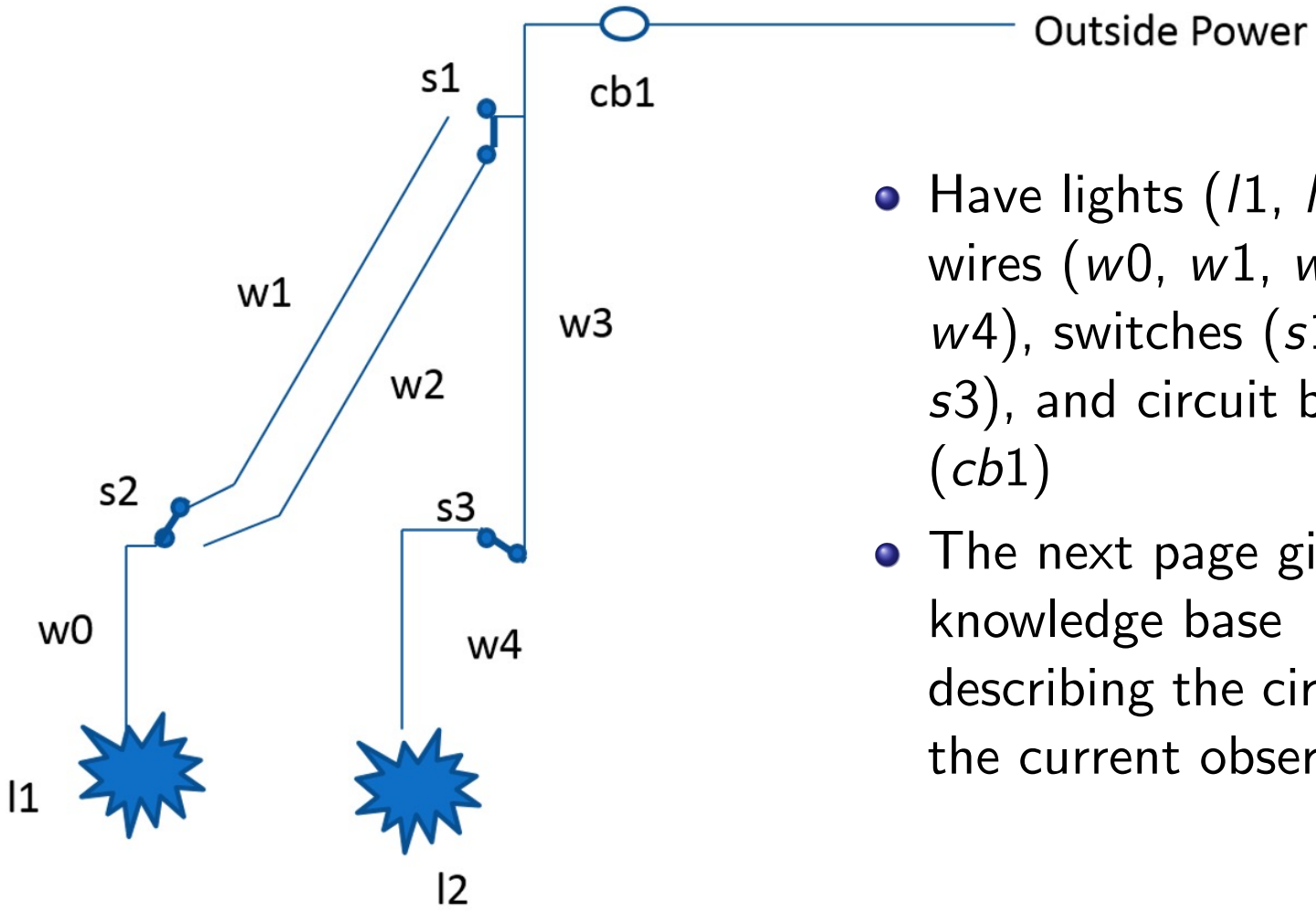
Diagnosis of Faults in an Electrical System

AI Example (from *Artificial Intelligence: Foundations of Computational Agents* by David Poole and Alan Mackworth, 2010)

Need to represent in propositional logic the features of a piece of machinery or circuitry that are required for the operation to produce observable features. This is called the **Knowledge Base (KB)**.

We also have observations representing the features that the system is exhibiting now.

Electrical System Diagram



- Have lights ($l1$, $l2$), wires ($w0$, $w1$, $w2$, $w3$, $w4$), switches ($s1$, $s2$, $s3$), and circuit breakers ($cb1$)
- The next page gives the knowledge base describing the circuit and the current observations.

Representing the Electrical System in Propositional Logic

We need to represent our common-sense understanding of how the electrical system works in propositional logic.
For example: "If *l*1 is a light and if *l*1 is receiving current, then *l*1 is lit.

$$\text{light\_l1} \wedge \text{live\_l1} \wedge \text{ok\_l1} \rightarrow \text{lit\_l1}$$

Also: "If $w1$ has current, and switch $s2$ is in the up position, and $s2$ is not broken, then $w0$ has current."

$$\text{live\_w1} \wedge \text{up\_s2} \wedge \text{ok\_s2} \rightarrow \text{live\_w0}$$

This task of representing a piece of our common-sense world in logic is a common one in logic-based AI.

Knowledge Base

- live_outside $\leftarrow$ *We have outside power.*
- light_l1
- light_l2 $\leftarrow$ *Both l1 and l2 are lights.*
- live_w0 $\rightarrow$ live_l1
- live_w1 $\wedge$ up_s2 $\wedge$ ok_s2 $\rightarrow$ live_w0
- live_w2 $\wedge$ down_s2 $\wedge$ ok_s2 $\rightarrow$ live_w0 $\leftarrow$ *If s2 is ok and s2 is in a down position and w2 has current, then w0 has current.*
- live_w3 $\wedge$ up_s1 $\wedge$ ok_s1 $\rightarrow$ live_w1
- live_w3 $\wedge$ down_s1 $\wedge$ ok_s1 $\rightarrow$ live_w2
- live_w4 $\rightarrow$ live_l2
- live_w3 $\wedge$ up_s3 $\wedge$ ok_s3 $\rightarrow$ live_w4
- live_outside $\wedge$ ok_cb1 $\rightarrow$ live_w3
- light_l1 $\wedge$ live_l1 $\wedge$ ok_l1 $\rightarrow$ lit_l1
- light_l2 $\wedge$ live_l2 $\wedge$ ok_l2 $\rightarrow$ lit_l2

Observations

Observations need to be added to the KB.

- Both Switches up
  - up_s1
  - up_s2
- Both lights are dark
  - $\neg$ lit_l1
  - $\neg$ lit_l2

Diagnosis

- We assume that the components are working ok, unless we are forced to assume otherwise. These atoms are called assumables.
- The assumables (ok_cb1, ok_s1, ok_s2, ok_s3, ok_l1, ok_l2) represent the assumption that we assume that the switches, lights, and circuit breakers are ok.
- If the system is working correctly (all assumables are true), the observations and the knowledge base are consistent (i.e., satisfiable).
- The augmented knowledge base is clearly not consistent if the assumables are all true. The switches are both up, but the lights are not lit. Some of the assumables must then be false. This is the basis for the method to diagnose possible faults in the system.
- A diagnosis is a minimal set of assumables which must be false to explain the observations of the system.

Diagnostic Results

See *Artificial Intelligence: Foundations of Computational Agents* (by David Poole and Alan Mackworth, 2010) for details on this problem and how the method of consistency based diagnosis can determine possible diagnoses for the electrical system.

The approach yields 7 possible faults in the system. At least one of these must hold:

- Circuit Breaker 1 is not ok.
- Both Switch 1 and Switch 2 are not ok.
- Both Switch 1 and Light 2 are not ok.
- Both Switch 2 and Switch 3 are not ok.
- Both Switch 2 and Light 2 are not ok.
- Both Light 1 and Switch 3 are not ok.
- Both Light 1 and Light 2 are not ok.

Section Summary

Tautologies, Contradictions, and Contingencies.

Logical Equivalence

- Important Logical Equivalences
- Showing Logical Equivalence

Normal Forms

- Disjunctive Normal Form
- Conjunctive Normal Form

Propositional Satisfiability

- Sudoku Example

Tautologies, Contradictions, and Contingencies

A *tautology* is a proposition which is always true.

- $p \vee \neg p$

A *contradiction* is a proposition which is always false.

- $p \wedge \neg p$

A *contingency* is a proposition which is neither a tautology nor a contradiction, such as p.

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	F	T	F
F	T	T	F

Logical Equivalence. . .Revisited

- Two compound propositions p and q are logically equivalent if $p \leftrightarrow q$ is a tautology.
- We write this as $p \leftrightarrow q$ or as $p \equiv q$ where p and q are compound propositions.
- Two compound propositions p and q are equivalent if and only if the columns in a truth table giving their truth values agree.
- The following truth table shows that $\neg p \vee q$ is equivalent to $p \rightarrow q$.

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

De Morgan's Laws

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

This truth table shows that De Morgan's Second Law holds.

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

Key Logical Equivalences

- Identity Laws: $p \wedge T \equiv p$, $p \vee F \equiv p$
- Domination Laws: $p \vee T \equiv T$, $p \wedge F \equiv F$
- Idempotent laws: $p \vee p \equiv p$, $p \wedge p \equiv p$
- Double Negation Law: $\neg(\neg p) \equiv p$
- Negation Laws: $p \vee \neg p \equiv T$, $p \wedge \neg p \equiv F$

Key Logical Equivalences...

Commutative Laws: $p \vee q \equiv q \vee p, \quad p \wedge q \equiv q \wedge p$

Associative Laws

- See https://en.wikipedia.org/wiki/Associative_property.
- Repeated application of the operation produces the same result regardless of how valid pairs of parentheses are inserted in the expression.
- $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- $(p \vee q) \vee r \equiv p \vee (q \vee r)$

Distributive Laws

- $(p \vee (q \wedge r)) \equiv (p \vee q) \wedge (p \vee r)$ $\qquad (p + q \cdot r) = (p + q) \cdot (p + r)$
- $(p \wedge (q \vee r)) \equiv (p \wedge q) \vee (p \wedge r)$ $\qquad p \cdot (q + r) = p \cdot q + p \cdot r$

Absorption Laws: $p \vee (p \wedge q) \equiv p, \quad p \wedge (p \vee q) \equiv p$

More Logical Equivalences

Conditional Statements

$p \to q \equiv \neg p \vee q$

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

$p \vee q \equiv \neg p \to q$

$p \wedge q \equiv \neg(p \to \neg q)$

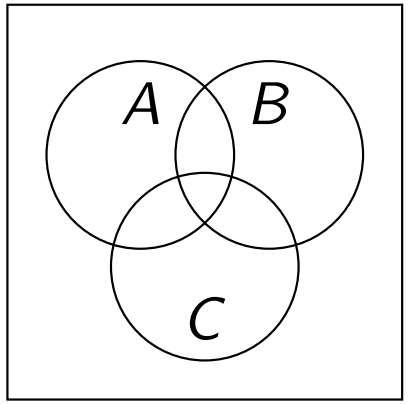
$\neg(p \to q) \equiv p \wedge \neg q$

$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$

$(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$

$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$

$(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$



Biconditional Statements

$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$

$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$

$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

Constructing New Logical Equivalences

We can show that two expressions are logically equivalent by developing a series of logically equivalent statements.

To prove that $A \equiv B$ we produce a series of equivalences beginning with A and ending with B.

$$A \equiv A_1$$

$$\vdots$$

$$A_n \equiv B$$

Keep in mind that whenever a proposition (represented by a propositional variable) occurs in the equivalences listed earlier, it may be replaced by an arbitrarily complex compound proposition.

Equivalence Proofs

Show that $\neg(p \vee (\neg p \wedge q))$ is logically equivalent to $\neg p \wedge \neg q$.

$\neg(p \vee (\neg p \wedge q))$	$\equiv \neg p \wedge \neg(\neg p \wedge q)$	by the second De Morgan law
	$\equiv \neg p \wedge [\neg(\neg p) \vee \neg q]$	by the first De Morgan law
	$\equiv \neg p \wedge (p \vee \neg q)$	by the double negation law
	$\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q)$	by the second distributive law
	$\equiv F \vee (\neg p \wedge \neg q)$	because $\neg p \wedge p \equiv F$
	$\equiv (\neg p \wedge \neg q) \vee F$	by the commutative law
	$\equiv (\neg p \wedge \neg q)$	for disjunction

Equivalence Proofs. . .

Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

$(p \wedge q) \rightarrow (p \vee q)$	$\equiv \neg(p \wedge q) \vee (p \vee q)$	by truth table for $\rightarrow$
	$\equiv (\neg p \vee \neg q) \vee (p \vee q)$	by the first De Morgan law
	$\equiv (\neg p \vee p) \vee (\neg q \vee q)$	by assoc and comm laws
	$\equiv T \vee T$	by truth tables
	$\equiv T$	by the domination law

Disjunctive Normal Form

A propositional formula is in *disjunctive normal form* if it consists of

- a disjunction of $(1, \ldots, n)$ disjuncts where,
- each disjunct consists of a conjunction of $(1, \ldots, m)$ atomic formulas or the negation of an atomic formula.
- Is $(p \wedge \neg q) \vee (\neg p \wedge q)$ in DNF?
  - Yes!
- What about $p \wedge (p \vee q)$?
  - No!

Disjunctive Normal Form is important for the circuit design methods discussed in Chapter 12.

Disjunctive Normal Form

Show that every compound proposition can be put in disjunctive normal form.

- Construct the truth table for the proposition.
- Then an equivalent proposition is the disjunction with n disjuncts where n is the number of rows for which the formula evaluates to T.
- Each disjunct has m conjuncts where m is the number of distinct propositional variables.
- Each conjunct includes the positive form of the propositional variable if the variable is assigned T in that row and the negated form if the variable is assigned F in that row.
- This proposition is in disjunctive normal from.

Disjunctive Normal Form

Find the Disjunctive Normal Form (DNF) of

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

This proposition is true when r is false, or when both p and q are false.

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

p	**q**	**r**	Val
F	F	F	T
T	F	F	T
F	T	F	T
T	T	F	T
F	F	T	T
T	F	T	F
F	T	T	F
T	T	T	F

Conjunctive Normal Form

A compound proposition is in *Conjunctive Normal Form* (CNF) if it is a conjunction of disjunctions.

- Every proposition can be put in an equivalent CNF.
- Conjunctive Normal Form (CNF) can be obtained by eliminating implications, moving negation inwards and using the distributive and associative laws.
- Important in *resolution* theorem proving used in AI.
- A compound proposition can be put in conjunctive normal form through repeated application of the logical equivalences covered earlier.
  - See StackOverflow.
  - For e.g., $(a + b \cdot c) \equiv (a + b) \cdot (a + c)$.

Conjunctive Normal Form

Put the following into CNF:

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

- Eliminate implication signs:

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

- Move negation inwards; eliminate double negation:

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

- Convert to CNF using associative/distributive laws[1]

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

[1] $a \cdot b + c = (a + c) \cdot (b + c)$.

Conjunctive Normal Form...

Find the Conjunctive Normal Form (CNF) of

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

p	q	r	v
F	F	F	T
T	F	F	T
F	T	F	T
T	T	F	T
F	F	T	T
T	F	T	F
F	T	T	F
T	T	T	F

1. What if we could write a DNF expression of the rows that evaluate **F**?
2. Then what...?

Propositional Satisfiability

A compound proposition is *satisfiable* if there is an assignment of truth values to its variables that makes it true. When no such assignments exist, the compound proposition is *unsatisfiable*.

A compound proposition is unsatisfiable *iff* its negation is a tautology.

- $p \wedge \neg p$ is unsatisfiable, but its negation $\neg p \vee p$ is a tautology.

Questions on Propositional Satisfiability

Determine the satisfiability of the following compound propositions:

- $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$
  - Satisfiable. Let $p = T, q = T, r = T$.
- $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$
  - Satisfiable. Let $p = T, q = F$
- $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$
  - Not satisfiable. Check each possible assignment of truth values to the propositional variables and none will make the proposition true.
  - Let $p = T$. Then we get
    $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$
  - Let $p = F$. Then we get
    $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$

Notation

$\vee_{j=1}^{n} p_j$ is used for $p_1 \vee p_2 \vee \ldots \vee p_n$

$\wedge_{j=1}^{n} p_j$ is used for $p_1 \wedge p_2 \wedge \ldots \wedge p_n$

Sudoku

A **Sudoku puzzle** is represented by a 9×9 grid made up of nine 3×3 subgrids, known as **blocks**. Some of the 81 cells of the puzzle are assigned one of the numbers $1, 2, \ldots, 9$.

The puzzle is solved by assigning numbers to each blank cell so that every row, column and block contains each of the nine possible numbers.

	2	9				4		
			5			1		
	4							
				4	2			
6							7	
5								
7			3					5
	1			9				
							6	

Encoding as a Satisfiability Problem

- Let $p(i, j, n)$ denote the proposition that is true when the number n is in the cell in the ith row and the jth column.
- There are $9 \times 9 \times 9 = 729$ such propositions.
- In the sample puzzle $p(5, 1, 6)$ is true, but $p(5, j, 6)$ is false for $j = 2, 3, \ldots 9$.

Encoding as a Satisfiability Problem I

- For each cell with a given value, assert $p(i, j, n)$, when the cell in row i and column j has the given value.
- Assert that every row contains every number.

$$\bigwedge_{i=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{j=1}^{9} p(i, j, n)$$

- Assert that every column contains every number.

$$\bigwedge_{j=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{i=1}^{9} p(i, j, n)$$

Encoding as a Satisfiability Problem II

- Assert that each of the 3×3 blocks contain every number.

  for each $n \in \{1, \ldots, 9\}$:

$$\bigwedge_{r=0}^{2} \bigwedge_{s=0}^{2} \bigvee_{i=1}^{3} \bigvee_{j=1}^{3} p(3r + i, 3s + j, n)$$

- Assert that no cell contains more than one number. Take the conjunction over all values of $n, n', i,$ and j, where each variable ranges from 1 to 9 and $n \neq n'$, of

$$p(i, j, n) \rightarrow \neg p(i, j, n')$$

Solving Satisfiability Problems

To solve a Sudoku puzzle, we need to find an assignment of truth values to the 729 variables of the form $p(i, j, n)$ that makes the conjunction of the assertions true. Those variables that are assigned T yield a solution to the puzzle.

A truth table can always be used to determine the satisfiability of a compound proposition. But this is too complex even for modern computers for large problems.

There has been much work on developing efficient methods for solving satisfiability problems as many practical problems can be translated into satisfiability problems.

Summary

Predicate Logic (First-Order Logic (FOL), Predicate Calculus)

- The Language of Quantifiers
- Logical Equivalences
- Nested Quantifiers
- Translation from Predicate Logic to English
- Translation from English to Predicate Logic

Section Summary

- Predicates
- Variables
- Quantifiers
  - Universal Quantifier
  - Existential Quantifier
- Negating Quantifiers
  - De Morgan's Laws for Quantifiers
- Translating English to Logic
- Logic Programming?

Propositional Logic Not Enough

- If we have:
- "All men are mortal."
- "Socrates is a man."

Does it follow that "Socrates is mortal?"

Can't be represented in propositional logic. Need a language that talks about objects, their properties, and their relations.

Later we'll see how to draw inferences.

Introducing Predicate Logic

Predicate logic uses the following new features:

- Variables: x, y, z
- Predicates: $P(x), M(x)$
- Quantifiers

Propositional functions are a generalization of propositions.

- They contain variables and a predicate, e.g., $P(x)$
- Variables can be replaced by elements from their *domain*.

Propositional Functions

Propositional functions become propositions, and have truth values when

- their variables are each replaced by a value from their *domain*, or
- when the variables are *bound* by a quantifier (as we will see later).

The statement $P(x)$ is said to be the value of the propositional function P at x.

For e.g., let $P(x)$ denote "$x > 0$" and the domain be the integers. Then:

- P(-3) is false.
- P(0) is false.
- P(3) is true.
- Often the domain is denoted by U. So in this example U is the integers.

Examples of Propositional Functions

Let "$x + y = z$" be denoted by $R(x, y, z)$ and U (for all three variables) be the integers. Find these truth values:

- $R(2, -1, 5)$. Solution: F.
- $R(3, 4, 7)$. Solution: T.
- $R(x, 3, z)$. Solution: Not a Proposition.

Now let "$x - y = z$" be denoted by $Q(x, y, z)$, with U as the integers. Find these truth values:

- $Q(2, -1, 3)$. Solution: T.
- $Q(3, 4, 7)$. Solution: F.
- $Q(x, 3, z)$. Solution: Not a Proposition.

Compound Expressions

Connectives from propositional logic carry over to predicate logic.

If $P(x)$ denotes "$x > 0$" find these truth values:

- $P(3) \vee P(-1)$ Solution: T
- $P(3) \wedge P(-1)$ Solution: F
- $P(3) \rightarrow P(-1)$ Solution: F
- $P(3) \rightarrow \neg P(-1)$ Solution: T

Expressions with variables are not propositions and therefore do not have truth values. For example,

- $P(3) \wedge P(y)$
- $P(x) \rightarrow P(y)$

When used with quantifiers (to be introduced next), these expressions (propositional functions) become propositions.

Quantifiers

We need *quantifiers* to express the meaning of English words including all and some:

- "All men are Mortal."
- "Some cats do not have fur."

The two most important quantifiers are:

- Universal Quantifier, "For all," symbol: $\forall$
- Existential Quantifier, "There exists," symbol: $\exists$

We write as in $\forall x\, P(x)$ and $\exists x\, P(x)$.

- $\forall x\, P(x)$ asserts $P(x)$ is true for every x in the domain.
- $\exists x\, P(x)$ asserts $P(x)$ is true for some x in the domain.

The quantifiers are said to bind the variable x in these expressions.

Universal Quantifier

$\forall x\, P(x)$ is read as "For all x, $P(x)$" or "For every x, $P(x)$"

Examples:

- If $P(x)$ denotes $x > 0$ and U is the integers, then $\forall x\, P(x)$ is false.
- If $P(x)$ denotes $x > 0$ and U is the positive integers, then $\forall x\, P(x)$ is true.
- If $P(x)$ denotes x is even and U is the integers, then $\forall x\, P(x)$ is false.

Existential Quantifier

$\exists x\, P(x)$ is read as "For some x, $P(x)$", or as "There is an x such that $P(x)$," or "For at least one x, $P(x)$."

Examples:

- If $P(x)$ denotes $x > 0$ and U is the integers, then $\exists x\, P(x)$ is true. It is also true if U is the positive integers.
- If $P(x)$ denotes $x < 0$ and U is the positive integers, then $\exists x\, P(x)$ is false.
- If $P(x)$ denotes x is even and U is the integers, then $\exists x\, P(x)$ is true.

Thinking about Quantifiers

When the domain of discourse is finite, we can think of quantification as looping through the elements of the domain.

To evaluate $\forall x\, P(x)$ loop through all x in the domain.

- If at every step $P(x)$ is true, then $\forall x\, P(x)$ is true.
- If at a step $P(x)$ is false, then $\forall x\, P(x)$ is false and the loop terminates.

To evaluate $\exists x\, P(x)$ loop through all x in the domain.

- If at some step, $P(x)$ is true, then $\exists x\, P(x)$ is true and the loop terminates.
- If the loop ends without finding an x for which $P(x)$ is true, then $\exists x\, P(x)$ is false.

Even if the domains are infinite, we can still think of the quantifiers this fashion, but the loops will not terminate in some cases.

Properties of Quantifiers

The truth value of $\exists x\, P(x)$ and $\forall x\, P(x)$ depend on both the propositional function $P(x)$ and on the domain U.

Examples:

- If U is the positive integers and $P(x)$ is the statement $x < 2$, then $\exists x\, P(x)$ is true, but $\forall x\, P(x)$ is false.
- If U is the negative integers and $P(x)$ is the statement $x < 2$, then both $\exists x\, P(x)$ and $\forall x\, P(x)$ are true.
- If U consists of $3, 4, 5$, and $P(x)$ is the statement $x > 2$, then both $\exists x\, P(x)$ and $\forall x\, P(x)$ are true.
- But if $P(x)$ is the statement $x < 2$, then both $\exists x\, P(x)$ and $\forall x\, P(x)$ are false.

Precedence of Quantifiers

The quantifiers $\forall$ and $\exists$ have higher precedence than all the logical operators.

- For example, $\forall x\, P(x) \vee Q(x)$ means $[\forall x\, P(x)] \vee Q(x)$
- $\forall x\, (P(x) \vee Q(x))$ means something different.

Unfortunately, often people write

$$\forall x\, P(x) \vee Q(x)$$

when they mean $\forall x\, (P(x) \vee Q(x))$.

Translating from English to Logic

Translate the following sentence into predicate logic: "Every student in this class has taken a course in Java."

- First decide on the domain U.
- If U is all students in this class, define a propositional function $J(x)$ denoting "x has taken a course in Java," and translate as

$$\forall x\, J(x)$$

- But if U is all people, also define a propositional function $S(x)$ denoting "x is a student in this class," and translate as

$$\forall x\, (S(x) \rightarrow J(x))$$

- $\forall x\, (S(x) \wedge J(x))$ is not correct. What does it mean?

Translating from English to Logic...

Translate the following sentence into predicate logic: "Some student in this class has taken a course in Java."

- First decide on the domain U.
- If U is all students in this class, translate as

$$\exists x\, J(x)$$

- But if U is all people, then translate as

$$\exists x\, (S(x) \wedge J(x))$$

$\exists x\, (S(x) \rightarrow J(x))$ is not correct. What does it mean?

Returning to the Socrates Example

Introduce the propositional functions $Man(x)$ denoting "x is a man" and $Mortal(x)$ denoting "x is mortal." Specify the domain as all people.

The two premises are:

- $\forall x\,(Man(x) \rightarrow Mortal(x))$
- $Man(Socrates)$

The conclusion is:

- $Mortal(Socrates)$

Later we will show how to prove that the conclusion follows from the premises.

Equivalences in Predicate Logic ✗

Statements involving predicates and quantifiers are *logically equivalent* if and only if they have the same truth value:

- for every predicate substituted into these statements and
- for every domain of discourse used for the variables in the expressions.

The notation $S \equiv T$ indicates that S and T are logically equivalent.

For example: $\forall x \neg\neg S(x) \equiv \forall x\, S(x)$

Quantifiers as Conjunctions and Disjunctions

If the domain is finite,

- a universally quantified proposition is equivalent to a conjunction of propositions without quantifiers, and
- an existentially quantified proposition is equivalent to a disjunction of propositions without quantifiers.

If U consists of the integers 1, 2, and 3:

$$\forall x\, P(x) \equiv P(1) \wedge P(2) \wedge P(3)$$
$$\exists x\, P(x) \equiv P(1) \vee P(2) \vee P(3)$$

Even if the domains are infinite, you can still think of the quantifiers in this fashion, but the equivalent expressions without quantifiers will be infinitely long.

Negating Quantified Expressions

Consider for example $\forall x\, J(x)$.

- "Every student in your class has taken a course in Java."
- Here $J(x)$ is "x has taken a course in Java" and the domain is students in your class.

Negating the original statement gives

- "It is not the case that every student in your class has taken Java."

This implies that

- "There is a student in your class who has not taken Java."

Symbolically, $\neg \forall x\, J(x) \equiv \exists x \neg J(x)$.

Negating Quantified Expressions...

Now consider $\exists x\, J(x)$.

- "There is a student in this class who has taken a course in Java."
- Where $J(x)$ is "x has taken a course in Java."

Negating the original statement gives

- "It is not the case that there is a student in this class who has taken Java."

This implies that

- "Every student in this class has not taken Java".

Symbolically, $\neg\, \exists x\, J(x) \equiv \forall x \neg\, J(x)$.

De Morgan's Laws for Quantifiers

The rules for negating quantifiers are:

Negation	Equivalent	When Is negation True?	When False?
$\neg\exists x\, P(x)$	$\forall x\, \neg P(x)$	For every x, $P(x)$ is false.	There is x for which $P(x)$ is true.
$\neg\forall x\, P(x)$	$\exists x\, \neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x.

The reasoning in the table shows that:

$$\neg\forall x\, P(x) \equiv \exists x\, \neg P(x)$$
$$\neg\exists x\, P(x) \equiv \forall x\, \neg P(x)$$

Translation from English to Logic

- "Some student in this class has visited Mexico."

  Let $M(x)$ denote "x has visited Mexico," and $S(x)$ denote "x is a student in this class," and U be all people.

  $$\exists x\,(S(x) \wedge M(x))$$

- "Every student in this class has visited Canada or Mexico." Add $C(x)$ denoting "x has visited Canada."

  $$\forall x\,[S(x) \rightarrow (M(x) \vee C(x))]$$

Some Fun with Translating from English into Logical Expressions ✗

- $U =$ fleegles, snurds, thingamabobs
- $F(x)$: x is a fleegle
- $S(x)$: x is a snurd
- $T(x)$: x is a thingamabob

Translate "Everything is a fleegle."

$$\forall x\, F(x)$$

Some Fun with Translating from English into Logical Expressions... ✗

"Nothing is a snurd."

$$\neg\exists x\, S(x)$$

Or,

$$\forall x\, \neg S(x)$$

Some Fun with Translating from English into Logical Expressions... ✗

"All fleegles are snurds."

$$\forall x\,(F(x) \rightarrow S(x))$$

Some Fun with Translating from English into Logical Expressions... ✗

"Some fleegles are thingamabobs."

$$\exists x\,(F(x) \wedge T(x))$$

Some Fun with Translating from English into Logical Expressions... ✗

"No snurd is a thingamabob."

$$\neg\exists x\,(S(x) \wedge T(x))$$

Or,

$$\forall x\,(S(x) \rightarrow \neg T(x))$$

Why not

$$\neg\exists x\,(S(x) \rightarrow T(x))$$

If you consider $S(x) \wedge T(x)$ vs. $S(x) \rightarrow T(x)$, there are many "worlds" in which they yield different truth values for choices of S & T. They are not equivalent. In particular, if $S(x) \not\rightarrow T(x)$ then $S(x) \wedge T(x)$ is *false* everywhere, but $S(x) \rightarrow T(x)$ is *true* when $\neg S(x)$.

Some Fun with Translating from English into Logical Expressions... ✗

"If any fleegle is a snurd then it is also a thingamabob."

$$\forall x\,[(F(x) \wedge S(x)) \rightarrow T(x)]$$

. . . . . .

Could it also be

$$\forall x\,[(F(x) \rightarrow S(x)) \rightarrow (F(x) \rightarrow T(x))]$$

This says that there is no x for which $F(x) \rightarrow S(x)$, but $F(x) \not\rightarrow T(x)$.

System Specification Example ✗

Predicate logic is used to specify properties that systems must satisfy. For example, translate into predicate logic:

- Every mail message larger than one megabyte will be compressed.
- If a user is active, at least one network link will be available.

Decide on predicates and domains (left implicit here) for the variables:

- Let $L(m, y)$ be "Mail message m is larger than y megabytes."
- Let $C(m)$ denote "Mail message m will be compressed."
- Let $A(u)$ represent "User u is active."
- Let $S(n, x)$ represent "Network link n is state x."

Now we have:

$$\forall m\,(L(m, 1) \rightarrow C(m))$$

$$\exists u\,A(u) \rightarrow \exists n\,S(n, \mathit{available})$$

Lewis Carroll Example ✗

The first two are called *premises* and the third is called the *conclusion*.

- "All lions are fierce."
- "Some lions do not drink coffee."
- "Some fierce creatures do not drink coffee."

Here is one way to translate these statements to predicate logic. Let $P(x)$, $Q(x)$, and $R(x)$ be the propositional functions "x is a lion," "x is fierce," and "x drinks coffee," respectively.

- $\forall x\,(P(x) \rightarrow Q(x))$
- $\exists x\,(P(x) \wedge \neg R(x))$
- $\exists x\,(Q(x) \wedge \neg R(x))$

Later we will see how to prove that the conclusion follows from the premises.

Some Predicate Calculus Definitions ✗

An assertion involving predicates and quantifiers is *valid* if it is true

- for all domains
- every propositional function substituted for the predicates in the assertion.

Example:

$$\forall x \neg S(x) \leftrightarrow \neg \exists x\, S(x)$$

An assertion involving predicates is *satisfiable* if it is true

- for some domains
- some propositional functions that can be substituted for the predicates in the assertion.

Otherwise, it is *unsatisfiable*. For example,

$\forall x(F(x) \leftrightarrow T(x))$ not valid but satisfiable

$\forall x(F(x) \wedge \neg F(x))$ unsatisfiable

Nested Quantifiers

Section Summary

- Nested Quantifiers
- Order of Quantifiers
- Translating from Nested Quantifiers into English
- Translating Mathematical Statements into Statements involving Nested Quantifiers.
- Translated English Sentences into Logical Expressions.
- Negating Nested Quantifiers.

Nested Quantifiers

Nested quantifiers are often necessary to express the meaning of sentences in English as well as important concepts in computer science and mathematics.

Example: "Every real number has an additive inverse" is

$$\forall x \, \exists y \, (x + y = 0)$$

where the domains of x and y are the real numbers.

We can also think of nested propositional functions. $\forall x \, \exists y \, (x + y = 0)$ can be viewed as

- $\forall x \, Q(x)$, where
- $Q(x)$ is $\exists y \, P(x, y)$, where
- $P(x, y)$ is $(x + y = 0)$.

Thinking of Nested Quantification ✗

Nested Loops

- To see if $\forall x \forall y\, P(x, y)$ is true, loop through the values of x:
  - At each step, loop through the values for y.
  - If for some pair of x and y, $P(x, y)$ is false, then $\forall x \forall y\, P(x, y)$ is false and both the outer and inner loop terminate.

  $\forall x \forall y\, P(x, y)$ is true if the outer loop ends after stepping through each x.
- To see if $\forall x \exists y\, P(x, y)$ is true, loop through the values of x:
  - At each step, loop through the values for y.
  - The inner loop ends when a pair x and y is found such that $P(x, y)$ is true.
  - If no y is found such that $P(x, y)$ is true the outer loop terminates as $\forall x \exists y\, P(x, y)$ has been shown to be false.

  $\forall x \exists y\, P(x, y)$ is true if the outer loop ends after stepping through each x.

If the domains of the variables are infinite, then this process cannot be carried out.

Order of Quantifiers

1. Let $P(x, y)$ be the statement "$x + y = y + x$."
   - Assume that U is the real numbers.
   - Then $\forall x \forall y\, P(x, y)$ and $\forall y \forall x\, P(x, y)$ have the same truth value.
2. Let $Q(x, y)$ be the statement "$x + y = 0$."
   - Assume that U is the real numbers.
   - Then $\forall x \exists y\, Q(x, y)$ is true, but $\exists y \forall x\, Q(x, y)$ is false.

Questions on Order of Quantifiers ✗

Let U be the real numbers, define

$$P(x, y) : x \cdot y = 0$$

What is the truth value of the following?

- $\forall x \forall y\, P(x, y)$. False.
- $\forall x \exists y\, P(x, y)$. True.
- $\exists x \forall y\, P(x, y)$. True.
- $\exists x \exists y\, P(x, y)$. True.

Questions on Order of Quantifiers ✗

Let U be the real numbers, define

$$P(x, y) : x/y = 1$$

What is the truth value of the following?

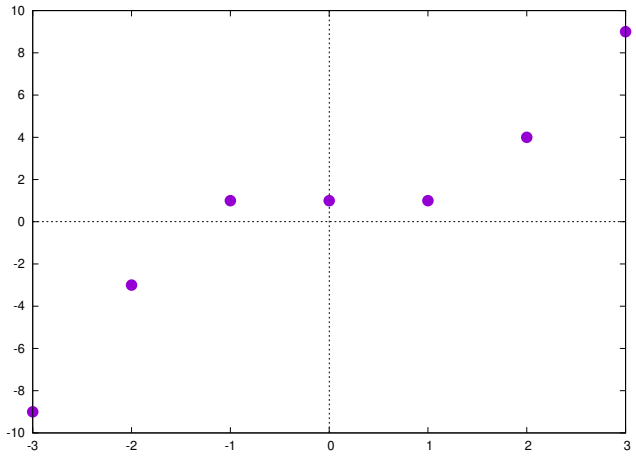
- $\forall x \forall y\, P(x, y)$. False.
- $\forall x \exists y\, P(x, y)$. False.
- $\exists x \forall y\, P(x, y)$. False.
- $\exists x \exists y\, P(x, y)$. True.

Quantifications of Two Variables

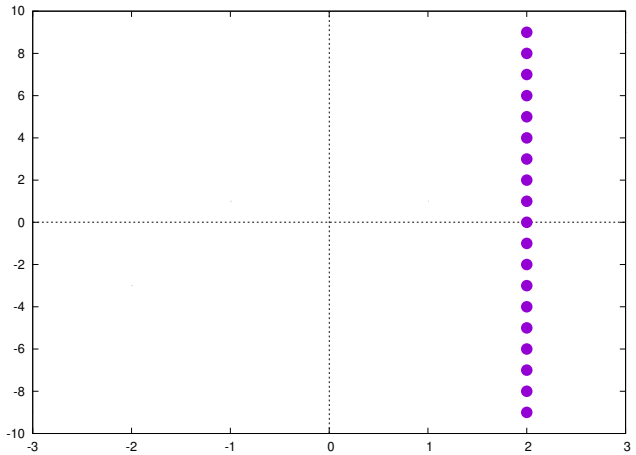
Statement	When True?	When False
$\forall x \forall y\, P(x, y)$ $\forall y \forall x\, P(x, y)$	$P(x, y)$ is true for every pair x, y.	There is a pair x, y for which $P(x, y)$ is false.
$\forall x \exists y\, P(x, y)$	For every x there is a y for which $P(x, y)$ is true.	There is an x such that $P(x,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

Quantifications of Two Variables...

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



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



Translating Nested Quantifiers into English

- Translate the statement

$$\forall x(C(x) \vee \exists y(C(y) \wedge F(x, y)))$$

where

- $C(x)$ is "x has a computer," and
- $F(x, y)$ is "x and y are friends,"

and the domain for both x and y consists of all students in your school.

Every student in your school has a computer or has a friend who has a computer.

- Translate the statement

$$\exists x \, \forall y \, \forall z \, ((F(x, y) \wedge F(x, z) \wedge (y \neq z)) \rightarrow \neg F(y, z))$$

There is a student none of whose friends are also friends with each other.

Translating Mathematical Statements into Predicate Logic

✗

Translate "The sum of two positive integers is always positive" into a logical expression.

- Rewrite the statement to make the implied quantifiers and domains explicit:

  "For every two integers, if these integers are both positive, then the sum of these integers is positive."

- Introduce the variables x and y, and specify the domain, to obtain:

  "For all positive integers x and y, $x + y$ is positive."

- The result is:

$$\forall x \forall y \, [((x > 0) \wedge (y > 0)) \rightarrow (x + y > 0)]$$

  where the domain of both variables consists of all integers.

Translating English into Logical Expressions Example ✗

Use quantifiers to express the statement "There is a woman who has taken a flight on every airline in the world."

- Let $P(w, f)$ be "w has taken f" and $Q(f, a)$ be "f is a flight on a."
- The domain of w is all women, the domain of f is all flights, and the domain of a is all airlines.
- Then the statement can be expressed as:

$$\exists w \, \forall a \, \exists f \, (P(w, f) \wedge Q(f, a))$$

Calculus in Logic ✗

Use quantifiers to express the definition of the limit of a real-valued function $f(x)$ of a real variable x at a point a in its domain.

Recall the definition of the statement

$$\lim_{x \to a} f(x) = L$$

is "For every real number $\epsilon > 0$, there exists a real number $\delta > 0$ such that $|f(x) - L| < \epsilon$ whenever $0 < |x - a| < \delta$."

Using quantifiers:

$$\forall \epsilon \, \exists \delta \, \forall x \, (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon)$$

Where the domain for the variables ϵ and δ consists of all positive real numbers and the domain for x consists of all real numbers.

Questions on Translation from English ✗

Choose the obvious predicates and express in predicate logic.

- "Brothers are siblings." $\forall x \forall y (B(x, y) \rightarrow S(x, y))$
- "Siblinghood is symmetric." $\forall x \forall y (S(x, y) \rightarrow S(y, x))$
- "Everybody loves somebody." $\forall x \exists y L(x, y)$
- "There is someone who is loved by everyone." $\exists y \forall x L(x, y)$
- "There is someone who loves someone." $\exists x \exists y L(x, y)$
- "Everyone loves himself." $\forall x L(x, x)$

Negating Nested Quantifiers ✗

Recall the logical expression developed three slides back:

$$\exists w \, \forall a \, \exists f \, (P(w, f) \wedge Q(f, a))$$

Use quantifiers to express the statement that "There does not exist a woman who has taken a flight on every airline in the world."

$$\neg \exists w \, \forall a \, \exists f \, (P(w, f) \wedge Q(f, a))$$

Now use De Morgan's Laws to move the negation as far inwards as possible.

1. $\neg \exists w \, \forall a \, \exists f \, (P(w, f) \wedge Q(f, a))$
2. $\forall w \, \neg \forall a \, \exists f \, (P(w, f) \wedge Q(f, a))$ by De Morgan's for $\exists$
3. $\forall w \, \exists a \, \neg \exists f \, (P(w, f) \wedge Q(f, a))$ by De Morgan's for $\forall$
4. $\forall w \, \exists a \, \forall f \, \neg (P(w, f) \wedge Q(f, a))$ by De Morgan's for $\exists$
5. $\forall w \, \exists a \, \forall f \, (\neg P(w, f) \vee \neg Q(f, a))$ by De Morgan's for $\wedge$.

Negating Nested Quantifiers... ✗

Can you translate the result back into English?

"For every woman there is an airline such that for all flights, this woman has not taken that flight or that flight is not on this airline"

Some Questions about Quantifiers (optional)

Can you switch the order of quantifiers?

- Is this a valid equivalence? $\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y)$
  - Yes! The left and the right side will always have the same truth value. The order in which x and y are picked does not matter.
- Is this a valid equivalence? $\forall x \exists y P(x, y) \equiv \exists y \forall x P(x, y)$
  - No! The left and the right side may have different truth values for some propositional functions for P. Try "$x + y = 0$" for $P(x, y)$ with U being the integers. The order in which the values of x and y are picked does matter.

Some Questions about Quantifiers (optional)...

Can you distribute quantifiers over logical connectives?

- Is this a valid equivalence? $\forall x(P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$
  - Yes! The left and the right side will always have the same truth value no matter what propositional functions are denoted by $P(x)$ and $Q(x)$.
- Is this a valid equivalence? $\forall x\,(P(x) \rightarrow Q(x)) \equiv \forall x\,P(x) \rightarrow \forall x\,Q(x)$
  - No! The left and the right side may have different truth values. Pick
    - ★ "x is a fish" for $P(x)$, and
    - ★ "x has scales" for $Q(x)$

    with the domain of discourse being all animals.

    Then the left side is false, because there are some fish that do not have scales. But the right side is true since not all animals are fish.

Summary

- Valid Arguments and Rules of Inference
- Proof Methods
- Proof Strategies

Rules of Inference

Section Summary

- Valid Arguments
- Inference Rules for Propositional Logic
- Using Rules of Inference to Build Arguments
- Rules of Inference for Quantified Statements
- Building Arguments for Quantified Statements

Revisiting the Socrates Example

We have the two premises:

- "All men are mortal."
- "Socrates is a man."

And the conclusion: "Socrates is mortal."

How do we get the conclusion from the premises?

The Argument

We can express the premises (above the line) and the conclusion (below the line) in predicate logic as an argument:

$$\begin{array}{l} \forall x(\text{Man}(x) \rightarrow \text{Mortal}(x)) \\ \text{Man}(\text{Socrates}) \\ \hline \therefore \quad \text{Mortal (Socrates)} \end{array}$$

We will see shortly that this is a valid argument.

Valid Arguments

We will show how to construct valid arguments in two stages:

- first for propositional logic, and then
- for predicate logic.

The rules of inference are the essential building block in the construction of valid arguments.

- Propositional Logic: Inference Rules.
- Predicate Logic: Inference rules for propositional logic plus additional inference rules to handle variables and quantifiers.

Arguments in Propositional Logic

An *argument* in propositional logic is a sequence of propositions. All but the final proposition are called premises. The last statement is the conclusion.

The argument is valid if the premises imply the conclusion. An *argument form* is an argument that is valid no matter what propositions are substituted into its propositional variables.

If the premises are $p_1, p_2, \ldots, p_n$ and the conclusion is q then

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$$

is a tautology.

Inference rules are all argument simple argument forms that will be used to construct more complex argument forms.

Rules of Inference for Propositional Logic: Modus Ponens

$p \rightarrow q$ $\underline{p}$ $\therefore q$	Corresponding Tautology $(p \wedge (p \rightarrow q)) \rightarrow q$

- Let p be "It is snowing."
- Let q be "I will study discrete math."
- "If it is snowing, then I will study discrete math."
- "It is snowing."
- "Therefore, I will study discrete math."

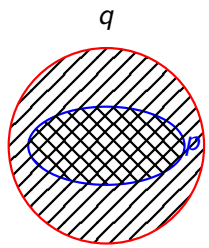
Modus Tollens

$$\begin{array}{l} p \rightarrow q \\ \underline{\neg q} \\ \therefore \neg p \end{array}$$

Corresponding Tautology

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

- Let p be "it is snowing."
- Let q be "I will study discrete math."
- "If it is snowing, then I will study discrete math."
- "I will not study discrete math."
- "Therefore, it is not snowing."



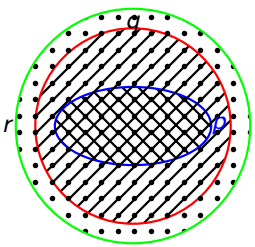
Hypothetical Syllogism

$$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array}$$

Corresponding Tautology

$$((p \to q) \wedge (q \to r)) \to (p \to r)$$

- Let p be "it snows."
- Let q be "I will study discrete math."
- Let r be "I will get an A."
- "If it snows, then I will study discrete math."
- "If I study discrete math, I will get an A."
- "Therefore, If it snows, I will get an A."



Disjunctive Syllogism

$$\begin{array}{l} p \vee q \\ \underline{\neg p} \\ \therefore q \end{array}$$

Corresponding Tautology

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

- Let p be "I will study discrete math."
- Let q be "I will study English literature."
- "I will study discrete math or I will study English literature."
- "I will not study discrete math."
- "Therefore, I will study English literature."

Addition

$\dfrac{p}{\therefore p \vee q}$	Corresponding Tautology $p \rightarrow (p \vee q)$

- Let p be "I will study discrete math."
- Let q be "I will visit Las Vegas."
- "I will study discrete math."
- "Therefore, I will study discrete math or I will visit Las Vegas."

Simplification

$\dfrac{p \wedge q}{\therefore p}$	Corresponding Tautology $(p \wedge q) \rightarrow p$

- Let p be "I will study discrete math."
- Let q be "I will study English literature."
- "I will study discrete math and English literature"
- "Therefore, I will study discrete math."

Conjunction

$$\begin{array}{l} p \\ q \\ \hline \therefore p \wedge q \end{array}$$

Corresponding Tautology

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

- Let p be "I will study discrete math."
- Let q be "I will study English literature."
- "I will study discrete math."
- "I will study English literature."
- "Therefore, I will study discrete math and I will study English literature."

Resolution

Resolution plays an important role in AI and is used in Prolog.

	Corresponding Tautology
$\neg p \vee r$ $p \vee q$ $\therefore q \vee r$	$((\neg p \vee r) \wedge (p \vee q)) \rightarrow (q \vee r)$

- Let p be "I will study discrete math."
- Let r be "I will study English literature."
- Let q be "I will study databases."
- "I will not study discrete math or I will study English literature."
- "I will study discrete math or I will study databases."
- "Therefore, I will study databases or I will study English literature."

Using the Rules of Inference to Build Valid Arguments

A *valid argument* is a sequence of statements. Each statement is either a premise or follows from previous statements by rules of inference. The last statement is called conclusion.

$$
\begin{array}{l}
S_1 \\
S_2 \\
\vdots \\
S_n \\
\therefore C
\end{array}
$$

Valid Arguments

From the single proposition

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

Show that q is a conclusion.

Step	Reason
1. $p \wedge (p \rightarrow q)$	Premise
2. p	Simplification using (1)
3. $p \rightarrow q$	Simplification using (1)
4. q	Modus Ponens using (2) and (3)

Valid Arguments

With these hypotheses:

- "It is not sunny this afternoon and it is colder than yesterday."
- "We will go swimming only if it is sunny."
- "If we do not go swimming, then we will take a canoe trip."
- "If we take a canoe trip, then we will be home by sunset."

Using the inference rules, construct a valid argument for the conclusion:

"We will be home by sunset."

Choose propositional variables:

- p : "It is sunny this afternoon.", q : "It is colder than yesterday."
- r : "We will go swimming.", t : "We will be home by sunset."
- s : "We will take a canoe trip."

Translation into propositional logic:

- Hypotheses: $\neg p \wedge q, r \rightarrow p, \neg r \rightarrow s, s \rightarrow t$.
- Conclusion: t (show using resolution).

Valid Arguments

Step	Reason
1. $\neg p \wedge q$	Premise
2. $\neg p$	Simplification using (1)
3. $r \rightarrow p$	Premise
4. $\neg r$	Modus tollens using (2) and (3)
5. $\neg r \rightarrow s$	Premise
6. s	Modus ponens using (4) and (5)
7. $s \rightarrow t$	Premise
8. t	Modus ponens using (6) and (7)

Handling Quantified Statements

Valid arguments for quantified statements are a sequence of statements. Each statement is either a premise or follows from previous statements by rules of inference which include:

- Rules of Inference for Propositional Logic
- Rules of Inference for Quantified Statements

The rules of inference for quantified statements are introduced in the next several slides.

Universal Instantiation (UI)

$$\frac{\forall x\, P(x)}{\therefore P(c)}$$

Example: Our domain consists of all dogs and Fido is a dog.

- "All dogs are cuddly."
- "Therefore, Fido is cuddly."

Universal Generalization (UG)

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x\, P(x)}$$

Used often implicitly in Mathematical Proofs.

Existential Instantiation (EI)

$$\frac{\exists x\, P(x)}{\therefore P(c) \text{ for some element } c}$$

- "There is someone who got an A in the course."
- "Let's call her a and say that a got an A"

Existential Generalization (EG)

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x\, P(x)}$$

- "Michelle got an A in the class."
- "Therefore, someone got an A in the class."

Using Rules of Inference

Using the rules of inference, construct a valid argument to show that "John Smith has two legs" is a consequence of the premises:

- "Every man has two legs."
- "John Smith is a man."

Let $M(x)$ denote "x is a man", $L(x)$ "x has two legs", and let John Smith be a member of the domain.

Step	**Reason**
1. $\forall x(M(x) \rightarrow L(x))$	Premise
2. $M(J) \rightarrow L(J)$	UI from (1)
3. $M(J)$	Premise
4. $L(J)$	Modus Ponens using (2) and (3)

Using Rules of Inference

Use the rules of inference to construct a valid argument showing that the conclusion "Someone who passed the first exam has not read the book." follows from the premises:

- "A student in this class has not read the book."
- "Everyone in this class passed the first exam."

Let

- $C(x)$ denote "x is in this class",
- $B(x)$ denote "x has read the book", and
- $P(x)$ denote "x passed the first exam".

$$\frac{\exists x\,(C(x) \wedge \neg B(x)) \qquad \forall x\,(C(x) \rightarrow P(x))}{\therefore \exists x\,(P(x) \wedge \neg B(x))}$$

Using Rules of Inference

Step	Reason
1. $\exists x\,(C(x) \wedge \neg B(x))$	Premise
2. $C(a) \wedge \neg B(a)$	EI from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x\,(C(x) \rightarrow P(x))$	Premise
5. $C(a) \rightarrow P(a)$	UI from (4)
6. $P(a)$	MP from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \wedge \neg B(a)$	Conj from (6) and (7)
9. $\exists x\,(P(x) \wedge \neg B(x))$	EG from (8)

Returning to the Socrates Example ✗

$$\frac{\forall x\,(Man(x) \rightarrow Mortal(x)) \qquad Man(Socrates)}{\therefore Mortal(Socrates)}$$

Step	**Reason**
1. $\forall x\,(Man(x) \rightarrow Mortal(x))$	Premise
2. $Man(Socrates) \rightarrow Mortal(Socrates)$	UI from (1)
3. $Man(Socrates)$	Premise
4. $Mortal(Socrates)$	MP from (2) and (3)

Universal Modus Ponens

Universal Modus Ponens combines universal instantiation and modus ponens into one rule.

$$\frac{\forall x(P(x) \rightarrow Q(x)) \qquad P(x), \text{ for a specific } a}{\therefore Q(a)}$$

This rule could be used in the Socrates example.

Section 1.7

- Mathematical Proofs
- Forms of Theorems
- Direct Proofs
- Indirect Proofs
  - Proof of the Contrapositive
  - Proof by Contradiction

Proofs of Mathematical Statements ✗

A *proof* is a valid argument that establishes the truth of a statement. In math, CS, and other disciplines, informal proofs which are generally shorter, are generally used.

- More than one rule of inference are often used in a step.
- Steps may be skipped.
- The rules of inference used are not explicitly stated.
- Easier to understand and to explain to people.
- But it's also easier to introduce errors.

Proofs have many practical applications:

- Verification that computer programs are correct,
- Establishing that operating systems are secure,
- Enabling programs to make inferences in artificial intelligence,
- Showing that system specifications are consistent.

Definitions ✗

A *theorem* is a statement that can be shown to be true using:

- Definitions,
- Other theorems,
- Axioms (statements which are given as true),
- Rules of inference.

A *lemma* is a 'helping theorem' or a result which is needed to prove a theorem. A *corollary* is a result which follows directly from a theorem.

Less important theorems are sometimes called *propositions*.

A *conjecture* is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.

Forms of Theorems ✗

Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers, or some of the discrete structures that we will study in this class.

Often the universal quantifier (needed for a precise statement of a theorem) is omitted by standard mathematical convention.

For example, the statement:

If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$

really means

For all positive real numbers x and y, if $x > y$, then $x^2 > y^2$

Proving Theorems

- Many theorems have the form

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

- By universal generalization of $P(c) \rightarrow Q(c)$, where c is an arbitrary element of the domain, the truth of the original formula follows.
- So, we must prove something of the form $p \rightarrow q$.

Proving Conditional Statements: $p \rightarrow q$

- *Trivial Proof*: If we know that q is true, then $p \rightarrow q$ is true as well.
  - "If it is raining, then 1=1".
  - $\neg p \vee q$ basically says that.
- *Vacuous Proof*: If we know that p is false then $p \rightarrow q$ is true as well.
  - "If I am both rich and poor then $2 + 2 = 5$".

Even though these examples seem silly, both trivial and vacuous proofs are often used in mathematical induction, as we will see in Chapter 5.

Even and Odd Integers

Definition: The integer n is

- even if $\exists$ an integer k such that $n = 2k$, and
- odd if there exists an integer k, such that $n = 2k + 1$.

Note that every integer is either even or odd and no integer is both even and odd.

We will need this basic fact about the integers in some of the example proofs to follow. We will learn more about the integers in Chapter 4.

Proving Conditional Statements: $p \rightarrow q$

Direct Proof: Assume that p is true. Use rules of inference, axioms, and logical equivalences to show that q must also be true.

- Example: Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."
- Assume that n is odd. Then $n = 2k + 1$ for an integer k. Squaring both sides of the equation, we get:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2r + 1,$$

  where $r = 2k^2 + 2k$, an integer.
- We have proved that if n is an odd integer, then n^2 is an odd integer.

Proving Conditional Statements: $p \rightarrow q$

Definition: The real number r is rational if there exist integers p and q where $q \neq 0$ such that $r = p/q$.

- Prove that the sum of two rational numbers is rational. ✗
- Assume r and s are two rational numbers. Then there must be integers p, q and also t, u such that

$$r = p/q, \quad s = t/u, \quad u \neq 0, \quad q \neq 0$$

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu} = \frac{v}{w} \quad \text{where } v = pu + qt, w = qu \neq 0$$

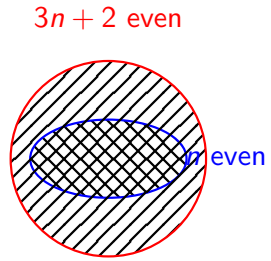
- Thus, the sum is rational.

Proving Conditional Statements: $p \rightarrow q$

- *Proof by Contraposition*: Assume $\neg q$ and show that $\neg p$ is true. This is sometimes called an *indirect proof* method. If we give a direct proof of $\neg q \rightarrow \neg p$ then we have a proof of $p \rightarrow q$.
- Prove that if n is an integer and $3n + 2$ is odd, then n is odd.
- Assume n is even. So, $n = 2k$ for some integer k. Thus,

$$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j \text{ for } j = 3k + 1$$

- Therefore $3n + 2$ is even. Since we have shown $\neg q \rightarrow \neg p$, $p \rightarrow q$ must hold as well. If n is an integer and $3n + 2$ is odd (not even), then n is odd (not even).
- Why does this work?



Proving Conditional Statements: $p \rightarrow q$ ✗

Prove that for an integer n, if n^2 is odd, then n is odd. I.e.,

$$Odd(n^2) \rightarrow Odd(n)$$

- Use proof by contraposition.
- Assume n is even (i.e., not odd). Therefore, there exists an integer k such that $n = 2k$. Hence,

  $$n^2 = 4k^2 = 2(2k^2)$$

  and n^2 is even (i.e., not odd). Or, $\neg Odd(n) \rightarrow \neg Odd(n^2)$.
- We have shown that if n is an even integer, then n^2 is even. $\therefore$ by contraposition, for an integer n, if n^2 is odd, then n is odd.

Proving Conditional Statements: $p \rightarrow q$

Proof by Contradiction: (aka *reductio ad absurdum*)

- To prove p, assume $\neg p$ and derive a contradiction such as $p \wedge \neg p$.
  - This shows that $\neg p \rightarrow F$ is true,
  - $\therefore$ it follows that the contrapositive $T \rightarrow p$ also holds.
- Example: Prove that if you pick 22 days from the calendar, at least 4 must fall on the same day of the week.
  - Assume that no more than 3 of the 22 days fall on the same day of the week.

M	T	W	R	F	S	Su
≤ 3	≤ 3	≤ 3	≤ 3	≤ 3	≤ 3	≤ 3

  - Because there are 7 days of the week, we could only have picked 21 days.
  - This contradicts the assumption that we have picked 22 days. This is also known as the pigeonhole principle.

Proof by Contradiction

Use *proof by contradiction* to show that $\sqrt{2}$ is irrational.

- Suppose that $\sqrt{2}$ is rational. Then,
  - $\exists$ integers a and b with $\sqrt{2} = a/b$, $b \neq 0$ and where
  - a and b have no common factors (see Chapter 4).
- Then
$$2 = \frac{a^2}{b^2}, \quad 2b^2 = a^2$$
- Therefore a^2 must be even.
  - If a^2 is even then a must be even (an exercise).
  - Since a is even, $a = 2c$ for some integer c.
- Thus,
$$2b^2 = 4c^2, \quad b^2 = 2c^2$$
- Therefore b^2 is even. So, b must be even as well.
- But then 2 must divide both a and b. This contradicts our assumption that a and b have no common factors.
- Thus our initial assumption must be false, and therefore $\sqrt{2}$ is irrational.

Proof by Contradiction

Prove that there is no largest prime number.

- Assume that there is a largest prime number. Call it p_n. Hence, we can list all the primes $2, 3, \ldots, p_n$. Form

$$r = p_1 \times p_2 \times \cdots \times p_n + 1$$

- None of the prime numbers on the list divides r.
- Therefore, (by a theorem in Chapter 4), either r is prime or there is a smaller prime that divides r.
- This contradicts the assumption that there is a largest prime, or that $p_1 \ldots p_n$ are the only primes.
- Therefore, there is no largest prime.

Theorems that are Biconditional Statements

To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.

Example: Prove that "If n is an integer, then n is odd if and only if n^2 is odd."

We have already shown (previous slides) that both $p \rightarrow q$ and $q \rightarrow p$. Therefore we can conclude that $p \leftrightarrow q$.

Sometimes *iff* is used as an abbreviation for "if and only if," as in "If n is an integer, then n is odd *iff* n^2 is odd."

What is wrong with this? ✗

"Proof" that $1 = 2$.

	Step	Reason
1	$a = b$	Premise
2	$a^2 = a \times b$	Multiply both sides of (1) by a
3	$a^2 - b^2 = a \times b - b^2$	Subtract b^2 from both sides of (2)
4	$(a - b)(a + b) = b(a - b)$	Algebra on (3)
5	$a + b = b$	Divide both sides by $a - b$
6	$2b = b$	Replace a by b in (5) because $a = b$
7	$2 = 1$	Divide both sides of (6) by b

Looking Ahead ✗

If direct methods of proof do not work:

- We may need a clever use of a proof by contraposition.
- Or a proof by contradiction.
- In the next section, we will see strategies that can be used when straightforward approaches do not work.
- In Chapter 5, we'll see mathematical induction and related techniques.
- In Chapter 6, we'll see combinatorial proofs

Section 1.8

- Proof by Cases
- Existence Proofs
  - Constructive
  - Nonconstructive
- Disproof by Counterexample
- Nonexistence Proofs
- Uniqueness Proofs
- Proof Strategies
- Proving Universally Quantified Assertions
- Open Problems

Proof by Cases

To prove a conditional statement of the form:

$$(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$$

Use the tautology

$$[(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q] \leftrightarrow$$
$$[(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)]$$

Each of the implications $p_i \rightarrow q$ is a case.

Proof by Cases ✗

Example: Let $a \circledcirc b = max(a, b) = a$ if $a \geq b$, otherwise b.

Show that for all real numbers a, b, c

$$(a \circledcirc b) \circledcirc c = a \circledcirc (b \circledcirc c)$$

This means the operation $\circledcirc$ is associative.

Let a, b, c be arbitrary real numbers. Then one of the following 6 cases must hold.

1. $a \geq b \geq c$
2. $a \geq c \geq b$
3. $b \geq a \geq c$
4. $b \geq c \geq a$
5. $c \geq a \geq b$
6. $c \geq b \geq a$

Proof by Cases ✗

Case 1: $a \geq b \geq c$

- $(a \mathbin{@} b) = a, a \mathbin{@} c = a, b \mathbin{@} c = b$
- Hence $(a \mathbin{@} b) \mathbin{@} c = a = a \mathbin{@} (b \mathbin{@} c)$

Therefore the equality holds for the first case.

A complete proof requires that the equality be shown to hold for all 6 cases. But the proofs of the remaining cases are similar. Try them.

Without Loss of Generality ✗

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

Use proof by contraposition. Suppose x and y are not both even. Then, one or both are odd. Without loss of generality, assume that x is odd. Then $x = 2m + 1$ for some integer m.

- Case 1: y is even. Then $y = 2n$ for some integer n, so

$$x + y = (2m + 1) + 2n = 2(m + n) + 1$$

  is odd.

- Case 2: y is odd. Then $y = 2n + 1$ for some integer n, so

$$x \cdot y = (2m + 1) \cdot (2n + 1) = 2(2m \cdot n + m + n) + 1$$

  is odd.

We only cover the case where x is odd because the case where y is odd is similar. The use phrase *without loss of generality* (WLOG) indicates this.

Existence Proofs

Proof of theorems of the form $\exists x\, P(x)$.

Constructive existence proof:

- Find an explicit value of c, for which $P(c)$ is true.
- Then $\exists x\, P(x)$ is true by Existential Generalization (EG).

Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways:

- 1729 is such a number since

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

Nonconstructive Existence Proofs

In a *nonconstructive* existence proof, we assume no c exists which makes $P(c)$ true and derive a contradiction.

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

We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

- If it is rational, we have two irrational numbers x and y with x^y rational, namely $x = \sqrt{2}$ and $y = \sqrt{2}$.
- But if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ so that

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$$

Counterexamples

- Recall $\exists x \neg P(x) \equiv \neg \forall x P(x)$.
- To establish that $\neg \forall x P(x)$ is true (or $\forall x P(x)$ is false), find a c such that $\neg P(c)$ is true or $P(c)$ is false.
- c is called a *counterexample* to the assertion $\forall x P(x)$.

Example: "Every positive integer is the sum of the squares of 3 integers."

The integer 7 is a counterexample. So the claim is false.

Uniqueness Proofs

Some theorems assert the existence of a unique element with a particular property, $\exists! x\, P(x)$. The two parts of a *uniqueness proof* are

- *Existence*: We show that an element x with the property exists.
- *Uniqueness*: We show that if $y \neq x$, then y does not have the property.

Example: Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

- *Existence*: The real number $r = -b/a$ is a solution of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$.
- *Uniqueness*: Suppose that s is a real number such that $as + b = 0$.
  - Then $ar + b = as + b$, where $r = -b/a$.
  - Subtracting b from both sides and dividing by a shows that $r = s$.
  - I.e., a has a multiplicative inverse.

Proof Strategies for proving $p \rightarrow q$ ✗

Choose a method.

- First try a direct method of proof.
- If this does not work, try an indirect method (e.g., try to prove the contrapositive).

For whichever method you are trying, choose a strategy.

- First try *forward reasoning*. Start with the axioms and known theorems and construct a sequence of steps that end in the conclusion. Start with p and prove q, or start with $\neg q$ and prove $\neg p$.
- If this doesn't work, try *backward reasoning*. When trying to prove q, find a statement p that we can prove with the property $p \rightarrow q$.

Backward Reasoning ✗

Suppose that two people play a game taking turns removing, $1, 2,$ or 3 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 player can win the game no matter what the second player does.

Proof: Let n be the last step of the game.

- Step n: P_1 can win if the pile contains $1, 2, 3$ stones.
- Step $n-1$: P_2 will have to leave such a pile if the pile that he/she is faced with has 4 stones.
- Step $n-2$: P_1 can leave 4 stones when there are $5, 6, 7$ stones left at the beginning of his/her turn.
- Step $n-3$: P_2 must leave such a pile, if there are 8 stones.
- Step $n-4$: P_1 has to have a pile with $9, 10, 11$ stones to ensure that there are 8 left.
- Step $n-5$: P_2 needs to be faced with 12 stones to be forced to leave $9, 10, 11$.
- Step $n-6$: P_1 can leave 12 stones by removing 3 stones.
- Now reasoning forward, the first player can ensure a win by removing 3 stones and leaving 12.

Universally Quantified Assertions

To prove theorems of the form $\forall x\, P(x)$, assume x is an arbitrary member of the domain and show that $P(x)$ must be true. Using UG it follows that $\forall x\, P(x)$.

Example: An integer x is even if and only if x^2 is even.

- The quantified assertion is $\forall x[x \text{ is even} \leftrightarrow x^2 \text{ is even}]$
- We assume x is arbitrary.
- Recall that $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p) \equiv p \rightarrow q \wedge \neg p \rightarrow \neg q$
  - x is even $\rightarrow x^2$ is even by direct proof.
  - x is not even $\rightarrow x^2$ is not even.

Bibliography I


Ashutosh Gupta and S. Krishna.
CS 228: Logic for Computer Science 2022.
https://www.cse.iitb.ac.in/~akg/courses/2022-logic/, January 2022.


Hyunyoung Lee.
Discrete structures for computing.
Class slides for TAMU CSCE 222, 2019.


Phillip Rogaway.
ECS20 Fall 2021 Lecture Notes, 2021.