Lecture 2: Logic and Proof

Xiaoxing Ma

Nanjing University

xxm@nju.edu.cn

October 9, 2017

Acknowledgement: These Beamer slides are totally based on the textbook *Discrete Mathematical Structures* by B. Kolman, R. C. Busby and S. C. Ross, and Prof. Daoxu Chen's PowerPoint slides.

At the Last Class

1. Sets, Sequences and Structures
    - Sets: fundamental model in mathematics
    - Sequences: elements and order
    - Structures: sets with operations
2. Some Useful Tools
    - Division, prime and algorithm
    - Matrices and operations on them

Overview

1. Propositional and Predicate Logic
    - Logical operations and truth tables
    - Predicates and Quantifiers
    - Logic statements
2. Methods of Proof
    - Rules of inference
    - Indirect method of proof
    - Proof by contradiction
    - Disproving by counterexamples

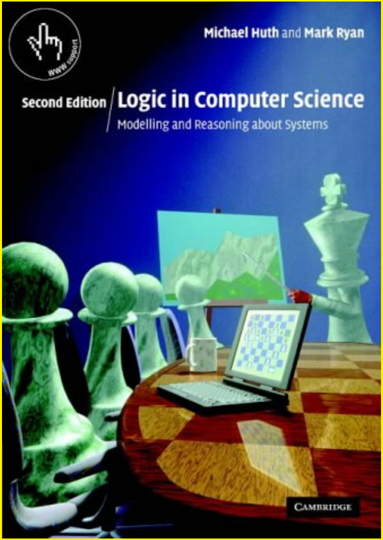
Overview

1 Pro

2 M

- D

Additional Reading:


Michael Huth and Mark Ryan
www support
Second Edition
Logic in Computer Science
Modelling and Reasoning about Systems
CAMBRIDGE

Example: Logic about Award

- Smith, Brown, Jones, Robinson will be granted awards for Math, English, French and Logic, respectively, with each award for one person.
- They guessed which-for-which as following:
  - Smith: Robinson will win the award for Logic.
  - Brown: Jones will win the award for English.
  - Jones: Smith will not win the award for Math.
  - Robinson: Brown will win the award for French.
- It turned out that only winners of Math and Logic Awards made the correct guesses.
- Problem: Can you tell who win what exactly?

Example: Looking for Solution

- Describe the problem as clearly as possible.
  For example, we use $P(x)$ denoting a person x win the award P.
- List all related useful information and rules. For example:
  - If x wins P, other one cannot win the same award.
  - If we can decide x didn't win any three of the four awards, then he must win the fourth.
  - If x makes the wrong guess, the negation of the guess must be true.
- **THE approach**: guess + reasoning
  We may begin by guess, but guess what?

Example: Possible Reasoning

- If we guess BJ, that is, "Brown and Jones win the awards for Math and logic", then, what Brown said is true: Jones wins the award for English. Contradiction!
  So, one possibility is excluded.

Example: Possible Reasoning

- If we guess BJ, that is, “Brown and Jones win the awards for Math and logic”, then, what Brown said is true: Jones wins the award for English. Contradiction!
  So, one possibility is excluded.
- If we guess RS, that is: “Robinson and Smith win the awards of Math and Logic”, then, what Robinson said is true: Brown wins the award for French. So, Jones wins the award for English. So, what Brown said is true, but Brown is not the winner of award of Math or Logic. Contradiction!
  One more possibility is excluded.

Example: Possible Reasoning

- If we guess BJ, that is, "Brown and Jones win the awards for Math and logic", then, what Brown said is true: Jones wins the award for English. Contradiction!
  So, one possibility is excluded.
- If we guess RS, that is: "Robinson and Smith win the awards of Math and Logic", then, what Robinson said is true: Brown wins the award for French. So, Jones wins the award for English. So, what Brown said is true, but Brown is not the winner of award of Math or Logic. Contradiction!
  One more possibility is excluded.
- If we guess JR, that is, "Jones and Robinson win the awards for Math and Logic". Then we know that Brown wins the award for French, and Smith wins the award for English. So what Smith said about Robinson is false, that means Robinson wins the award for Math. And the award for Logic goes to Jones. Done!

Rules of Reasoning

Are there any rules in reasoning, unrelated to the concrete contents?

How can we describe these rules, and how can we make use of them effectively?

Proposition

Proposition (statement): A declarative sentence that is either true or false, but not both.

Example

- $1 + 1 = 2$
- John is a student.
- Today is Tuesday.

More examples of Proposition

Example

- Do you speak English?
  This is a question, not a statement.
- $3 - x = 5$
  x is a variable, so the truth value of this sentence is open.
- Lets go!
  It is not a statement, but a command.
- The 4-color guess is true.
  We believe that it is true or false, but not both even before it was solved.
- He is a good man.
  What's the meaning of "good man"?

Propositional Variable

- A propositional variable assumes a value from the set $\{\textbf{True}, \textbf{False}\}$ (or simply $\{\textbf{T}, \textbf{F}\}$).
- A propositional variable is often denoted as p, q, r, etc.
- A statement can be represented by a propositional variable, e.g.
  - p: Today is Tuesday.
  - q: $2+2=4$

Logical Connectives

- A simple declarative sentence can be represented by an atom proposition.
- More than one atom propositions can be combined into a compound statement.
- The combination is achieved using **connectives**. Usually, the connective roughly corresponds some conjunctive in the natural language.
- The connective is defined exactly using **truth table**.

Negation

$\sim p$: it is not the case that p.

Table: The truth table for $\sim$

p	$\sim p$
T	**F**
F	**T**

Negation

$\sim p$: it is not the case that p.

Table: The truth table for $\sim$

p	$\sim p$
T	**F**
F	**T**

All possible values of p.

Conjunction

p and q is denoted as $p \wedge q$.

Table: The truth table for $\wedge$

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

Conjunction

p and q is denoted as $p \wedge q$.

Table: The truth table for $\wedge$

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

All possible values of $\langle p, q \rangle$.

Conjunction

p and q is denoted as $p \wedge q$.

Table: The truth table for $\wedge$

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

$p \wedge q =$ **T** iff. both p and q

All possible values of $\langle p, q \rangle$.

Disjunction

p or q is denoted as $p \vee q$, but not exactly.

Table: The truth table for $\vee$

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

Disjunction

p or q is denoted as $p \vee q$, but not exactly.

Table: The truth table for $\vee$

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

All possible value of $\langle p, q \rangle$.

Disjunction

p or q is denoted as $p \vee q$, but not exactly.

Table: The truth table for $\vee$

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

$p \vee q =$ **F** iff.
both $\sim p$ and $\sim q$

All possible value of $\langle p, q \rangle$.

Exclusive Disjunction

“exclusive” means “exactly one is true”.

The truth table for exclusive disjunction $\alpha(p, q)$

p	q	$\alpha(p, q)$
T	**T**	**F**
T	**F**	**T**
F	**T**	**T**
F	**F**	**F**

Exclusive Disjunction

“exclusive” means “exactly one is true”.

The truth table for exclusive disjunction $\alpha(p, q)$

p	q	$\alpha(p, q)$
T	**T**	**F**
T	**F**	**T**
F	**T**	**T**
F	**F**	**F**

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

Predicate

- If x is an integer, "x is larger than 2" is not a proposition, and its truth value depends on the value of x.

Predicate

- If x is an integer, "x is larger than 2" is not a proposition, and its truth value depends on the value of x.
- It can be denoted as $P(x)$, a propositional function.
    - The domain of P is the set of all integers, and
    - The range of P is $\{\mathbf{T}, \mathbf{F}\}$.

Predicate

- If x is an integer, "x is larger than 2" is not a proposition, and its truth value depends on the value of x.
- It can be denoted as $P(x)$, a propositional function.
    - The domain of P is the set of all integers, and
    - The range of P is $\{\mathbf{T}, \mathbf{F}\}$.
- A propositional function is called a **predicate**.

Universal and Existential Quantifications

- If $P(x)$ is a predicate, $\forall x P(x)$ means "for all x, $P(x)$".
  $\forall$ is called **universal quantifier**.
  - Given the domain, "for all x, $P(x)$" is a statement, that is, the sentence is either true or false, but not both.
  - E.g., if x is a real number, $\forall x P(x)$ is true if $P(x)$ represents "-(-x)=x".

Universal and Existential Quantifications

- If $P(x)$ is a predicate, $\forall x P(x)$ means "for all x, $P(x)$".
  $\forall$ is called **universal quantifier**.
  - Given the domain, "for all x, $P(x)$" is a statement, that is, the sentence is either true or false, but not both.
  - E.g., if x is a real number, $\forall x P(x)$ is true if $P(x)$ represents "-(-x)=x".
- If $P(x)$ is a predicate, $\exists x P(x)$ means "there is some x, $P(x)$".
  $\exists$ is called **existential quantifier**.
  - Given the domain, "there is some x, $P(x)$" is a statement, that is the sentence is either true or false, but not both.
  - E.g., if a, b are real constants, $a < b$, in the domain of real number, $\exists x P(x)$ is true if $P(x)$ means "$a < x < b$".

Negation of Quantifications

- Negation of universal quantification:
  $\sim(\forall x P(x)) = \exists x(\sim P(x))$
  - For all x, the square of x is positive. (Assuming a domain of real numbers.)
  - There exists some x, the square of x is not positive.

Negation of Quantifications

- Negation of universal quantification:
  $\sim(\forall x P(x)) = \exists x(\sim P(x))$
  - For all x, the square of x is positive. (Assuming a domain of real numbers.)
  - There exists some x, the square of x is not positive.
- Negation of existential quantification:
  $\sim(\exists x P(x)) = \forall x(\sim P(x))$
  - There exists some x, $5x = x$.
  - For all x, $5x$ is not equal to x.

Multiple Quantifiers

Considering the set of real numbers

- $\forall x \forall y P(x, y)$ and $\forall y \forall x P(x, y)$ have the same truth values, and they are true if $P(x, y)$ means $x + y = y + x$.

Multiple Quantifiers

Considering the set of real numbers

- $\forall x \forall y P(x, y)$ and $\forall y \forall x P(x, y)$ have the same truth values, and they are true if $P(x, y)$ means $x + y = y + x$.
- $\exists x \exists y P(x, y)$ and $\exists y \exists x P(x, y)$ have the same truth values, and they are true if $P(x, y)$ means $x = y + 1$.

Multiple Quantifiers

Considering the set of real numbers

- $\forall x \forall y P(x,y)$ and $\forall y \forall x P(x,y)$ have the same truth values, and they are true if $P(x,y)$ means $x + y = y + x$.
- $\exists x \exists y P(x,y)$ and $\exists y \exists x P(x,y)$ have the same truth values, and they are true if $P(x,y)$ means $x = y + 1$.
- If P(x,y) means "$y > x$" then $\forall x \exists y P(x,y)$ is true, but $\exists y \forall x P(x,y)$ is false.

Implication

“if p then q” can be denoted as $p \Rightarrow q$

Table: The truth table for $\Rightarrow$

p	q	$p \Rightarrow q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**T**
F	**F**	**T**

- However, “$\Rightarrow$” doesn’t exactly means “if...then...”.
- $p \Rightarrow q$ is true has nothing to do with the connection between p and q in common sense.
- In fact, a false hypothesis implies any conclusion.

Equivalence

$p \Leftrightarrow q$ means p and q always have the same truth value.

Truth table for $\Leftrightarrow$

p	q	$p \Leftrightarrow q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**F**
F	**F**	**T**

$$p \Leftrightarrow q \;\equiv\; (p \Rightarrow q) \wedge (q \Rightarrow p)$$

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$
T	**T**	**T**	**T**	**T**
T	**F**	**F**	**T**	**F**
F	**T**	**T**	**F**	**F**
F	**F**	**T**	**T**	**T**

Equivalence

$p \Leftrightarrow q$ means p and q always have the same truth value.

Truth table for $\Leftrightarrow$

p	q	$p \Leftrightarrow q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**F**
F	**F**	**T**

Logical equivalence

$$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$$

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$
T	**T**	**T**	**T**	**T**
T	**F**	**F**	**T**	**F**
F	**T**	**T**	**F**	**F**
F	**F**	**T**	**T**	**T**

Equivalence

$p \Leftrightarrow q$ means p and q always have the same truth value.

Truth table for $\Leftrightarrow$

p	q	$p \Leftrightarrow q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**F**
F	**F**	**T**

Logical equivalence

$$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$$

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$
T	**T**	**T**	**T**	**T**
T	**F**	**F**	**T**	**F**
F	**T**	**T**	**F**	**F**
F	**F**	**T**	**T**	**T**

same

Examples of Quantification

Example (“All people know China.”)

$\forall x(P(x) \Rightarrow Q(x))$, where

- $P(x)$: x is a person;
- $Q(x)$: x knows China;

Example (“Some people know Guatemala.”)

$\exists x(P(x) \wedge Q(x))$, where

- $P(x)$: x is a person;
- $Q(x)$: x knows Guatemala;

Pay attention to the connectives!

Ex: Statement about Prime Numbers

Example (Tchebyscheff's theorem)

There is a prime number between n and $2n$.

$$\forall n(N(n) \Rightarrow \exists x(N(x) \wedge x \geq n \wedge x \leq 2n \wedge \forall y(y|x \Rightarrow (y = 1 \vee y = x))))$$

where

- $N(x)$: x is a positive integer;
- $y|x$: y divides x.

Ex: Statement about Prime Numbers

Example (Tchebyscheff's theorem)

There is a prime number between n and $2n$.

$$\forall n(N(n) \Rightarrow \exists x(N(x) \wedge x \geq n \wedge x \leq 2n \wedge \forall y(y|x \Rightarrow (y = 1 \vee y = x))))$$

where

- $N(x)$: x is a positive integer;
- $y|x$: y divides x.

Exercise

"There is no largest prime number."

Contrapositive

p	q	$p \Rightarrow q$	$\sim q$	$\sim p$	$\sim q \Rightarrow \sim p$	$(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$
T	**T**	**T**	**F**	**F**	**T**	**T**
T	**F**	**F**	**T**	**F**	**F**	**T**
F	**T**	**T**	**F**	**T**	**T**	**T**
F	**F**	**T**	**T**	**T**	**T**	**T**

$p \Leftrightarrow q$ if and only if $p \equiv q$

Tautology, Contradiction and Contingency

- $(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$ is a **tautology**.
- $p \wedge \sim p$ is a **contradiction**.
- $(p \Rightarrow q) \wedge (p \vee q)$:
  - this logical expression is true when: $(p, q) = (\mathbf{T}, \mathbf{T})$ or $(\mathbf{F}, \mathbf{T})$
  - and is false when: $(p, q) = (\mathbf{T}, \mathbf{F})$ or $(\mathbf{F}, \mathbf{F})$
  - this is a **contingency**, i.e. neither tautology nor contradiction.

Properties of Logical Operations

Theorem (Th.1)

1	$p \vee q \equiv q \vee p$	*Commutative Properties*
2	$p \wedge q \equiv q \wedge p$	
3	$p \vee (q \vee r) \equiv (p \vee q) \vee r$	*Associative Properties*
4	$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	
5	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	*Distributive Properties*
6	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	
7	$p \vee p \equiv p$	*Idempotent Properties*
8	$q \wedge q \equiv q$	
9	$\sim\sim p \equiv p$	*Properties of Negation*
10	$\sim(p \vee q) \equiv \sim p \wedge \sim q$	*De Morgan's laws*
11	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	

Substitution of Connectives

Theorem (Th.2)

(a) $(p \Rightarrow q) \equiv ((\sim p \vee q)$

(b) $(p \Rightarrow q) \equiv ((\sim q \Rightarrow \sim p)$

(c) $(p \Leftrightarrow q) \equiv ((p \Rightarrow q) \wedge (q \Rightarrow p))$

(d) $(\sim (p \Rightarrow q)) \equiv (p \wedge \sim (q))$

(e) $(\sim (p \Leftrightarrow q) \equiv ((p \wedge \sim q) \vee (q \wedge \sim p))$

Substitution of Connectives

Theorem (Th.2)

(a) $(p \Rightarrow q) \equiv ((\sim p \vee q)$

(b) $(p \Rightarrow q) \equiv ((\sim q \Rightarrow \sim p)$

(c) $(p \Leftrightarrow q) \equiv ((p \Rightarrow q) \wedge (q \Rightarrow p))$

(d) $(\sim(p \Rightarrow q)) \equiv (p \wedge \sim(q))$

(e) $(\sim(p \Leftrightarrow q) \equiv ((p \wedge \sim q) \vee (q \wedge \sim p))$

Proof of Th.2(d) not using truth table:

$$\begin{aligned} \sim(p \Rightarrow q) &= \sim(\sim p \vee q) && \text{Formula (a)} \\ &= \sim\sim p \wedge \sim q && \text{De Morgan's law} \\ &= p \wedge \sim q && \text{Double Negtion} \end{aligned}$$

Inference by Logical Equivalence

We know that Bill, Jim and Sam are from Boston, Chicago and Detroit, respectively. Each of following sentence is half right and half wrong:

1. Bill is from Boston (p_1), and Jim is from Chicago (p_2).
2. Sam is from Boston (p_3), and Bill is from Chicago (p_4).
3. Jim is from Boston (p_5), and Bill is from Detroit (p_6).

Tell the truth about their home town.

We have:

$$\begin{aligned}
& ((p_1 \wedge \sim p_2) \vee (\sim p_1 \wedge p_2)) && (1)\\
\wedge\quad & ((p_3 \wedge \sim p_4) \vee (\sim p_3 \wedge p_4)) && (2)\\
\wedge\quad & ((p_5 \wedge \sim p_6) \vee (\sim p_5 \wedge p_6)) && (3)
\end{aligned}$$

Inference by Logical Equivalence (cont.)

We have:

$$
\begin{aligned}
&((p_1 \wedge \sim p_2) \vee (\sim p_1 \wedge p_2)) \wedge ((p_3 \wedge \sim p_4) \vee (\sim p_3 \wedge p_4)) \\
=&(\sim p_1 \wedge p_2 \wedge p_3 \wedge \sim p_4)
\end{aligned}
$$

And,

$$
\begin{aligned}
&(\sim p_1 \wedge p_2 \wedge p_3 \wedge \sim p_4) \wedge ((p_5 \wedge \sim p_6) \vee (\sim p_5 \wedge p_6)) \\
=&(\sim p_1 \wedge p_2 \wedge p_3 \wedge \sim p_4 \wedge \sim p_5 \wedge p_6)
\end{aligned}
$$

So, Jim is from Chicago, Sam is from Boston, and Bill is from Detroit.

Properties of Quantifications

Theorem (Th.3)

$$\sim(\forall x P(x)) \equiv \exists x(\sim P(x)) \quad \text{(a)}$$

$$\sim(\exists x P(x)) \equiv \forall x(\sim P(x)) \quad \text{(b)}$$

$$\exists x(P(x) \Rightarrow Q(x)) \equiv \forall x P(x) \Rightarrow \exists x Q(x) \quad \text{(c)}$$

$$\exists x(P(x) \vee Q(x)) \equiv \exists x P(x) \vee \exists x Q(x) \quad \text{(d)}$$

$$\forall x(P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x) \quad \text{(e)}$$

$$((\forall x P(x) \vee (\forall x Q(x))) \Rightarrow \forall x(P(x) \vee Q(x))) \textit{ is a tautology.} \quad \text{(f)}$$

$$\exists x(P(x) \wedge Q(x)) \Rightarrow \exists x P(x) \wedge \exists x Q(x) \textit{ is a tautology.} \quad \text{(g)}$$

Properties of Quantifications

Theorem (Th.3)

$$\sim(\forall x P(x)) \equiv \exists x(\sim P(x)) \tag{a}$$

$$\sim(\exists x P(x)) \equiv \forall x(\sim P(x)) \tag{b}$$

$$\exists x(P(x) \Rightarrow Q(x)) \equiv \forall x P(x) \Rightarrow \exists x Q(x) \tag{c}$$

$$\exists x(P(x) \vee Q(x)) \equiv \exists x P(x) \vee \exists x Q(x) \tag{d}$$

$$\forall x(P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x) \tag{e}$$

$$((\forall x P(x) \vee (\forall x Q(x))) \Rightarrow \forall x(P(x) \vee Q(x))) \textit{ is a tautology.} \tag{f}$$

$$\exists x(P(x) \wedge Q(x)) \Rightarrow \exists x P(x) \wedge \exists x Q(x) \textit{ is a tautology.} \tag{g}$$

For quantifications, truth table is invalid, so some axioms are needed for strict proof.

Logical Inference

Premises: $A_1, A_2, \cdots, A_k$

Conclusion: B

Valid inference: For any assignment of values of the variables in all A_i and B, if the conjunction of all A_i is true, then B must be true.

That is, the inference is valid if and only if:

$$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \Rightarrow B$$

is a tautology.

Modus Ponens

We have $(p \wedge (p \Rightarrow q)) \Rightarrow q$, so the rule

$$p, p \Rightarrow q \;\; \rightarrow \;\; q$$

Example (*A classic inference, dating back to ancient Greece*)

$P(x)$: x is a man.

$Q(x)$: x will die.

$\forall x(P(x) \Rightarrow Q(x))$: Every mand will die.

$P(s)$: Socrates is a man.

Conclusion: Socrates will die ($Q(s)$).

Proof

The proof for $A_1, A_2, \cdots, A_k \to B$ is a sequence of statements, in which, each statement is one of the following: (the last one should be B)

- a tautology, or
- any one of $A_1, A_2, \cdots, A_k$, or
- a new statement obtained by applying logical equivalences on any prior statement
- a new statement obtained by applying modus ponens on one or more prior statements

Some Important Tautologies

Theorem (Th.4)

Propositional Tautologies:

(a) $(p \wedge q) \Rightarrow p$

(b) $(p \wedge q) \Rightarrow q$

(c) $p \Rightarrow (p \vee q)$

(d) $q \Rightarrow (p \vee q)$

(e) $\sim p \Rightarrow (p \Rightarrow q)$

(f) $\sim(p \Rightarrow q) \Rightarrow p$

(g) $(p \wedge (p \Rightarrow q)) \Rightarrow q$

(h) $(\sim p \wedge (p \vee q)) \Rightarrow q$

(i) $(\sim q \wedge (p \Rightarrow q)) \Rightarrow \sim p$

(j) $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$

Predicate Tautologies:

1. $(\forall x P(x) \vee \forall(x) Q(x)) \Rightarrow \forall x(P(x) \vee Q(x))$
2. $\exists x(P(x) \wedge Q(x)) \Rightarrow \exists x P(x) \wedge \exists x Q(x)$

Rule of Inference

Tautology and rule of inference

- For each tautology with implication

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

  we get a rule of inference:

  $$p_1, p_2, \cdots, p_n \rightarrow q$$

- p_i's are hypotheses or premises, and q is called the conclusion.

Proof of Implication

If $p_1, p_2, \cdots, p_n \rightarrow q$, then:

- $(p_1 \Rightarrow (p_2 \Rightarrow (\cdots \Rightarrow (p_n \Rightarrow q))))$ is a tautology.
- $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \Rightarrow q$ is a tautology.

Example (Prove $((p \Rightarrow q) \wedge (\sim q)) \Rightarrow (\sim p)$)

1	$(p \Rightarrow q) \wedge (\sim q)$	Premis
2	$p \Rightarrow q$	Th.4(a)
3	$\sim q$	Th.4(b)
4	$\sim p \vee q$	Th.2(a),2
	Partially or wholly substituted with logically equivalent expressions	
5	$q \vee \sim p$	Th.1(1),4
6	$\sim\sim q \vee \sim p$	Th.1(9),5
7	$\sim q \Rightarrow \sim p$	Th.2(a),6
8	$\sim p$ (conclusion)	Th.4(g),3,7 (modus ponens)

Basic Rules about Quantification

US: $\forall x P(x) \rightarrow P(x)$

UG: $P(x) \rightarrow \forall x P(x)$

ES: $\exists x P(x) \rightarrow P(c)$

EG: $P(c) \rightarrow \exists x P(x)$

$$\forall x(\sim P(x) \Rightarrow Q(x)) \;\Rightarrow\; (\forall x(\sim Q(x)) \Rightarrow \exists x P(x))$$

1	$\forall x(\sim P(x) \Rightarrow Q(x))$	Premise
2	$\forall x(\sim Q(x))$	Premise
3	$\sim P(x) \Rightarrow Q(x)$	US, 1
4	$\sim Q(x)$	US, 2
5	$\sim\sim P(x)$	Th.4(i), 4, 3
6	$P(x)$	Double negation, 5
7	$\exists x P(x)$	EG, 6

Example (Somebody don't want to walk)

Premises:

1. Those who like walking don't want to take bus.
2. Everyone either likes taking bus or likes riding bike.
3. Someone don't want to ride bike.

Conclusion: There are someone who don't want to walk.

Let $W(x)$ be "x likes walking", $B(x)$ "x likes taking bus", and $K(x)$ "x likes riding bike".

Premises:

1. $\forall x(W(x) \Rightarrow \sim B(x))$
2. $\forall x(B(x) \vee K(x))$
3. $\exists x(\sim K(x))$

Conclusion: $\exists x(\sim W(x))$

Example (Somebody don't want to walk (cont.))

1. $\forall x(W(x) \Rightarrow \sim B(x))$ Premises
2. $\forall x(B(x) \vee K(x))$ Premises
3. $\exists x(\sim K(x))$ Premises
4. $\sim K(c)$ ES, 3
5. $W(c) \Rightarrow \sim B(c)$ US, 1
6. $B(c) \vee K(c)$ US, 2
7. $\sim\sim B(c) \vee K(c)$ Double negation, 6
8. $\sim B(c) \Rightarrow K(c)$ Th.2(a), 7
9. $\sim\sim B(c)$ Th.4(i), 4, 8
10. $\sim W(c)$ Th.4(i), 9, 5
11. $\exists x(\sim W(x))$ EG, 10

What's Wrong

Somebody proves the expression:

$$\exists x A(x) \land \exists x B(x) \Rightarrow \exists x (A(x) \land B(x))$$

as follows:

1. $\exists x A(x) \land \exists x B(x)$ Premises
2. $\exists x A(x)$ Th.2(a), 1
3. $\exists x B(x)$ Th.2(b), 1
4. $A(c)$ ES, 2
5. $B(c)$ ES, 3
6. $A(c) \land B(c)$ Def. $\land$
7. $\exists x (A(x) \land B(x))$ EG, 6

What's Wrong

Somebody proves the expression:

$$\exists x A(x) \land \exists x B(x) \Rightarrow \exists x (A(x) \land B(x))$$

as follows:

1	$\exists x A(x) \land \exists x B(x)$	Premises
2	$\exists x A(x)$	Th.2(a), 1
3	$\exists x B(x)$	Th.2(b), 1
4	$A(c)$	ES, 2
5	$B(c)$	ES, 3
6	$A(c) \land B(c)$	Def. $\land$
7	$\exists x (A(x) \land B(x))$	EG, 6

Indirect Proof – Using Contraposition

Example (Prove that if n^2 is odd, then n is odd.)

Proof

- Let p: n^2 is odd, and q: n is odd.
- What is to be proved is: $p \Rightarrow q$.
- Easy to see that:
    - Dealing with even number ($n = 2k$) is easier than dealing with odd ($n = 2k - 1$)
    - Dealing with square (n to n^2) is easier than dealing with square root (n^2 to n)
- So, we prove "if n is even, then n^2 is even, which is "$\sim q \Rightarrow \sim p$" and is equivalent to $p \Rightarrow q$.

Proof by Contradiction

The tautology:

$$((p \Rightarrow q) \wedge (\sim q)) \Rightarrow (\sim p)$$

The rule:

$$p \Rightarrow q, \sim q \;\rightarrow\; \sim p$$

The method:

Goal: $p_1, p_2, \cdots, p_n \rightarrow q$

Extra hypothesis: $\sim q$

Process: $p_1, p_2, \cdots, p_n, \sim q \rightarrow$ an absurdity

Conclusion: there must be at least one false in $\{p_1, p_2, \cdots, p_n, \sim q\}$, that must be $\sim q$, so, q is true.

Example (Proof by Contradiction – I)

There is no rational number whose square is 2.

Proof:

- Extra hypothesis: $(\frac{p}{q})^2 = 2$, and p, q are integers which have no common factors except for 1.
- Then,

$$\begin{aligned} p^2 = 2q^2 &\rightarrow p^2 \text{ is even} \\ &\rightarrow p \text{ is even} \\ &\rightarrow p^2 \text{ is multiple of 4} \\ &\rightarrow q^2 \text{ is even} \\ &\rightarrow q \text{ is even} \\ &\rightarrow p, q \text{ have 2 as common factor} \\ &\rightarrow \textbf{contradiction} \end{aligned}$$

Example (Proof by Contradiction – II)

If $d = GCD(a, b)$, then, existing integer s and t, satisfying $d = sa + tb$.

Proof: Let x be the smallest positive integer that can be written as $sa + tb$ for some s and t. If $c|a, c|b$ then $c|x$.

1. Proof of $x|a$: Let $a = qx + r(0 \leq r < x)$, then $r = a - qx = a - q(sa + tb) = (1 - as)a - qtb$, then r is of the form of $s'a + t'b$.
   Since $r < x$, r must be 0, otherwise x would not be the smallest positive integer that can be written as $sa + tb$. So $x|a$.
2. Same with $x|b$.

Dealing with Disjunction

Example

Prove: $n^2 = m^2$ if and only if $m = n$ or $m = -n$, where m, n are integers.
Proof: Let: $p : n^2 = m^2, q : m = n,$ and $r : m = -n$.
Then, what is to be proved is: $p \Leftrightarrow (q \vee r)$

$\leftarrow$ (premise is a disjunction)
$(q \vee r) \Rightarrow p$ is true when both $q \Rightarrow p$ and $r \Rightarrow p$.
$q \Rightarrow p$: $m = n \rightarrow n^2 = m^2$,
$r \Rightarrow p$: $m = -n \rightarrow n^2 = m^2$

Dealing with Disjunction (cont.)

Example

$\rightarrow$ (conclusion is a disjunction)
$p \Rightarrow (q \vee r) \equiv p \Rightarrow (\sim q \Rightarrow r)$, which can be proved by

$$p, \sim q \ \rightarrow r$$

that is: $n^2 = m^2, m \neq n \ \rightarrow \ m = -n$

Proof:
$n^2 = m^2 \rightarrow n^2 - m^2 = 0 \rightarrow (n+m)(n-m) = 0$
since $m \neq n$, we have $n - m \neq 0$, so, $n + m = 0$
So, $m = -n$

Negating a Statement Using Counterexample

Prove or disprove:

$$\exists x(A(x) \wedge B(x)) \Leftrightarrow \exists x A(x) \wedge \exists x B(x)$$

Assume that:

- The domain is the set of all natural number
- $A(x)$: x is odd
- $B(x)$: x is even

Then, $\exists x A(x) \wedge \exists x B(x) = \mathbf{T}$, and $\exists x(A(x) \wedge B(x)) = \mathbf{F}$. So the above equivalence is disproved.

Loop Invariant

Computing the square of A (A is a positive integer).

```
FUNCTION SQ($A$)
  1  $C \leftarrow 0$
  2  $D \leftarrow 0$
  3  WHILE ($D \neq A$)
       (a) $C \leftarrow C + A$
       (b) $D \leftarrow D + 1$
  4  RETURN($C$)
END OF FUNCTION SQ
```

Loop Invariant

Computing the square of A (A is a positive integer).

```
FUNCTION SQ($A$)
  1  $C \leftarrow 0$
  2  $D \leftarrow 0$
  3  WHILE ($D \neq A$)
       (a) $C \leftarrow C + A$
       (b) $D \leftarrow D + 1$
  4  RETURN($C$)
END OF FUNCTION SQ
```

This is a loop, the body of which (statements a and b) will be executed repeatedly until $D = A$.

C and D assume new values at the beginning of each new cycle of the loop. Let the value of C, D be C_n and D_n just after the nth cycle, with initial values of C_0 and D_0. Then the relation $C_n = A \times D_n$ will be invariate all the time.

Loop Invariant

Computing the square of A (A is a positive integer).

```
FUNCTION SQ($A$)
  1. $C \leftarrow 0$
  2. $D \leftarrow 0$
  3. WHILE ($D \neq A$)
       (a) $C \leftarrow C + A$
       (b) $D \leftarrow D + 1$
  4. RETURN($C$)
END OF FUNCTION SQ
```

According to the execution procedure, $C_n = C_{n-1} + A$ and $D_n = D_{n-1} + 1$, but $C_{n-1} = A \times D_{n-1}$ by induction hypothesis. So $C_n = (A \times D_{n-1}) + A = A \times D_n$.

Correctness of Function SQ

Computing the square of A (A is a positive integer).

```
FUNCTION SQ($A$)
  1  $C \leftarrow 0$
  2  $D \leftarrow 0$
  3  WHILE ($D \neq A$)
       (a) $C \leftarrow C + A$
       (b) $D \leftarrow D + 1$
  4  RETURN($C$)
END OF FUNCTION SQ
```

Termination: Since A is positive, D will be equal to A after finite cycles.

According to the execution procedure, $C_n = C_{n-1} + A$ and $D_n = D_{n-1} + 1$, but $C_{n-1} = A \times D_{n-1}$ by induction hypothesis. So $C_n = (A \times D_{n-1}) + A = A \times D_n$.

Correctness of Function SQ

Computing the square of A (A is a positive int ger).

```
FUNCTION SQ($A$)
  1  $C \leftarrow 0$
  2  $D \leftarrow 0$
  3  WHILE ($D \neq A$)
       (a) $C \leftarrow C$
       (b) $D$
  4  RETU
END OF FUN      SQ
```

Ter   nce A is positive, A after finite

It is easy to prove that the loop will terminate after exactly A cycles, which means that $D = A$ at the end, so $C = A^2$ for any positive input A.

cording to the execution procedure, $C_n = C_{n-1} + A$ and $D_n = D_{n-1} + 1$, but $C_{n-1} = A \times D_{n-1}$ by induction hypothesis. So $C_n = (A \times D_{n-1}) + A = A \times D_n$.

Exact Cover Problem

Definition of exact cover of a set:
Given a set A and a finite number of subsets of $A : A_1, A_2, \cdots, A_k$, a exact cover of A with respect to the A_i's is a set $S \subseteq \{A_1, A_2, \cdots, A_k\}$, satisfying:

- Any two sets in S are disjoint, and
- $\bigcup S = A$

Mathematically, we call S a **partition** of A.

Example

$A = \{a, b, c, d, e, f, g, h, i, j\}$;
$A_1 = \{a, c, d\}$, $A_2 = \{a, b, e, f\}$, $A_3 = \{b, f, g\}$, $A_4 = \{d, h, i\}$,
$A_5 = \{a, h, j\}$, $A_6 = \{e, h\}$, $A_7 = \{c, i, j\}$, $A_8 = \{i, j\}$
The exact cover is $\{A_1, A_3, A_6, A_8\}$.

Representation Using Matrix

Let $|A| = n$, and there are m subsets for A_i's, we represent the input of exact cover problem as a $m \times n$ matrix, with each row for a A_i.

$$\mathbf{M} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Solution: Find a collection of rows of $\mathbf{M}$: $r_1, r_2, \cdots, r_k$, satisfying: $r_i \wedge r_j = \mathbf{0}$ for $1 \leq i < j \leq k$, and $r_1 \vee r_2 \vee \cdots \vee r_k = \mathbf{1}$ where $\mathbf{0} = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$, $\mathbf{1} = [1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1]$ and, $\wedge$ is boolean product, $\vee$ is boolean sum.

Algorithm X for Exact Cover

- Input: matrix $\mathbf{A}$
- Initialization: label the rows of $\mathbf{A}$; let

$$\mathbf{M} = \mathbf{A}; L = \{\}$$

- (1) If there is a column of 0's in $\mathbf{M}$, return "No solution"
  (2) Otherwise:
  - Choose the column $\mathbf{c}$ with the fewest 1's;
  - Choose a row $\mathbf{r}$ with a 1 in column $\mathbf{c}$, $L = L \cup \{\mathbf{r}\}$;
  - Eliminate any row $\mathbf{r_i}$ having the property: $\mathbf{r} \wedge \mathbf{r_i} \neq \mathbf{0}$;
  - Eliminate all columns in which $\mathbf{r}$ has a 1;
  - Eliminate row $\mathbf{r}$;
  - If no row and column left, then output L, otherwise repeat (1) and (2) on resulted $\mathbf{M}$;

Solving Soduku by Covering

Describe the problem in suitable form

- 9 constraints for cells
- 9 constraints for columns
- 9 constraints for rows

1	2	3
2	3	1
3	1	2

Construct the matrix of covering

- 27 columns for constraints
- 27 rows for “moves”

Why can the algorithm X solve the 3×3 pseudo-Soduku using the matrix constructed as above?

Home Assignments

To be checked

pp.55- 12, 15-16, 18, 28, 30, 32, 35

pp.60- 6-7, 12-16, 24, 27-35

pp.67- 8, 12, 18, 20, 22-24, 30

pp.73- 20, 22, 26, 28, 30, 34, 36

p.78 20-25

The End