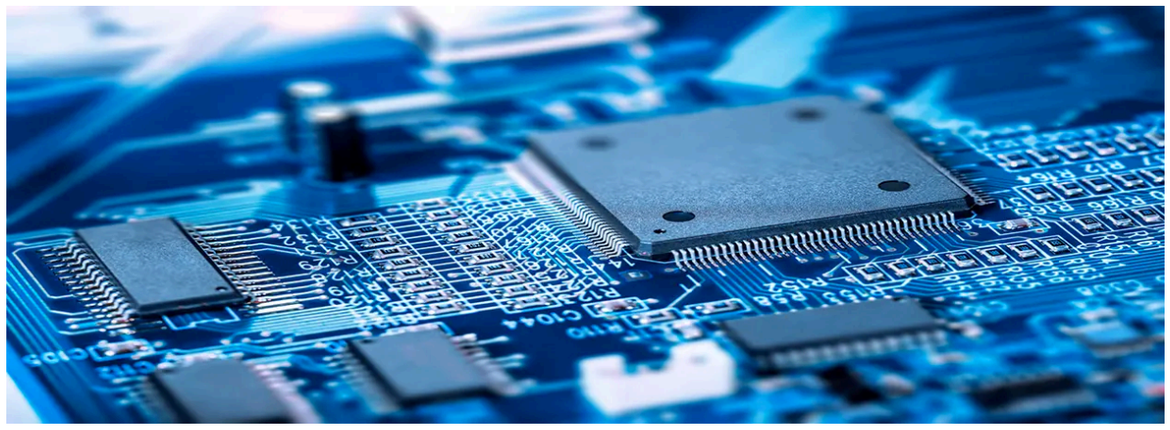
02 Logic and Proofs

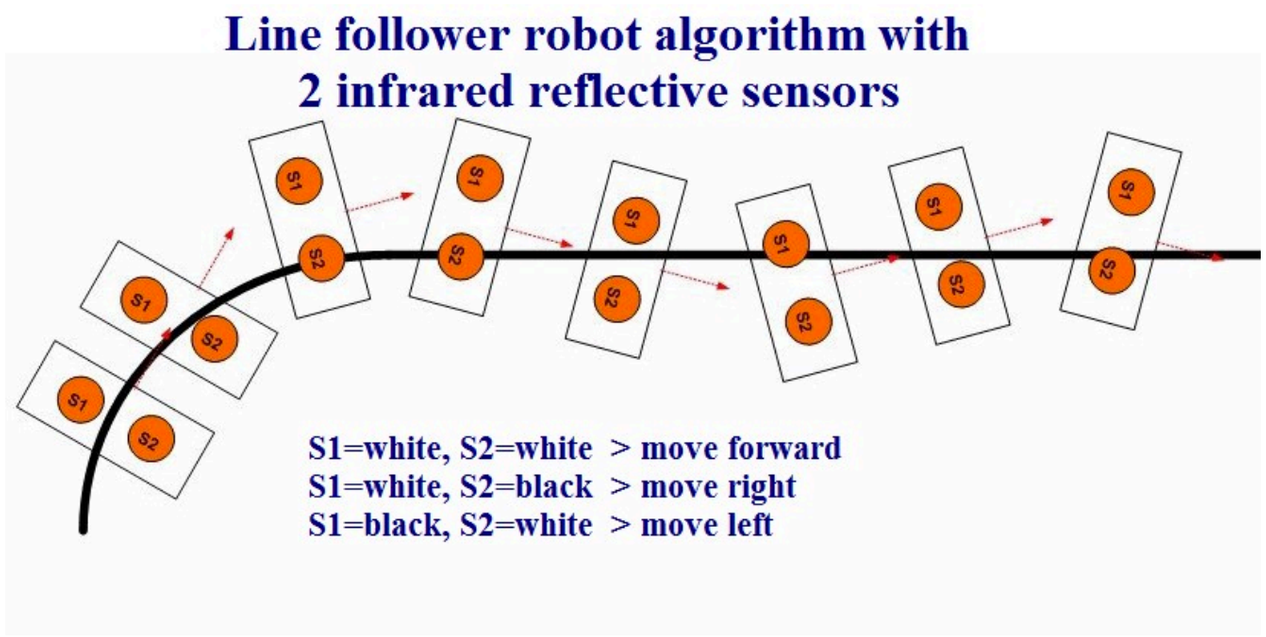
CS201 Discrete Mathematics

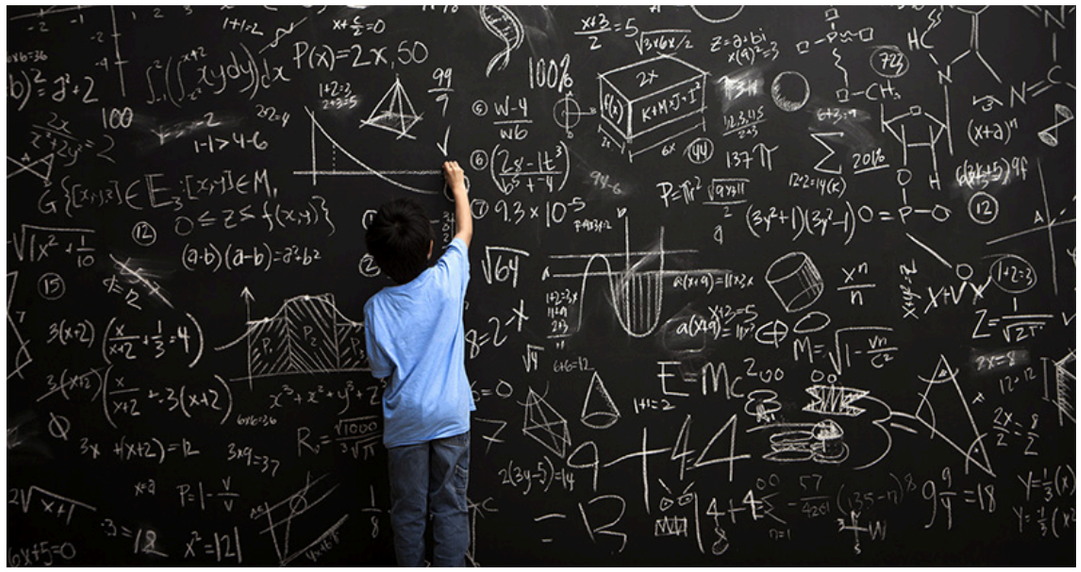
Instructor: Shan Chen

What is Logic?

- Logic is the basis of all mathematical reasoning
  - syntax of statements
  - meaning of statements
  - rules of logical inference







SUSTech

Propositional Logic

Propositions

- **Proposition:** a declarative statement that is either true or false

  ** declarative: making an explicit statement*

- Examples:
  - SUSTech is located in Shenzhen. *T (true)*
  - 1 + 1 = 2 *T (true)*
  - 2 + 2 = 3 *F (false)*

- Counter-Examples:
  - No parking. *where?*
  - How old are you? *questions are not declarative*
  - $x + 2 = 5$ *x is uncertain*
  - She is very talented. *who?*

Propositions: More Examples

- Are the following sentences propositions?
  - It will rain in Shenzhen tomorrow.
  - $P = NP$
  - There are other life forms on other planets in the universe.
- Yes! They are declarative, i.e., either true or false.
  - It's OK that you do not know if the statement is true or false.

Compound Propositions

- **Compound proposition:** a proposition that is built from multiple elementary propositions using logical connectives
- Example:
  - Proposition A: It rains outside.
  - Proposition B: We will watch a movie.
  - A new proposition: If it rains outside, then we will watch a movie.
- Logical connectives:
  - Negation
  - Conjunction
  - Disjunction
  - Exclusive or
  - Implication
  - Biconditional

Negation (not)

- Let p be a proposition. The proposition "It is not the case that p." is called the negation of p, denoted by $\neg p$, and read as "not p".

- Examples:
  - p SUSTech is located in Shenzhen. *T*
  - $\neg p$ SUSTech is not located in Shenzhen. *F*

  It is not the case that SUSTech is located in Shenzhen.

- More examples:

• $5 + 2 = 8$	$5 + 2 \neq 8$
• 10 is a prime number.	10 is not a prime number.
• Classes begin at 8:00am.	Classes do not begin at 8:00am.

Truth Table (not)

- **Truth table:** displays the relationships between truth values (i.e., *T* or *F*) of different propositions.

p	$\neg p$
T	F
F	T

Rows: contains all possible values of the proposition *p*

Conjunction (and)

- Let p and q be propositions. The conjunction of p and q, denoted by $p \wedge q$, is true when both p and q are true and false otherwise.

- Examples:
  - p SUSTech is located in Shenzhen.
  - q 5 + 2 = 8
  - $p \wedge q$ SUSTech is located in Shenzhen and 5 + 2 = 8

- More Examples:
  - There are infinitely many twin prime numbers and 2 + 2 = 3
  - 2 is a prime number and 9 is a prime power.

Disjunction (or)

- Let p and q be propositions. The disjunction of p and q, denoted by $p \vee q$, is true when p or q is true and false otherwise.

- Examples:
  - p SUSTech is located in Shenzhen.
  - q 5 + 2 = 8
  - $p \vee q$ SUSTech is located in Shenzhen or 5 + 2 = 8

- More Examples:
  - There are infinitely many twin prime numbers or 2 + 2 = 3
  - 2 is a prime number or 9 is a prime power.

Truth Table (and, or)

- The truth table for conjunction and disjunction

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

Rows: contains all possible ($2^2 = 4$) values of 2 elementary propositions

Exclusive Or (xor)

- Let p and q be propositions. The exclusive or of p and q, denoted by $p \oplus q$, is true when either p or q is true (i.e., exactly one of p and q is true) and false otherwise.

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

Implication (Conditional Statement)

- Let p and q be propositions. The implication (also known as conditional statement) "if p, then q", denoted by $p \rightarrow q$, is false when p is true and q is false, and true otherwise.
  - p is called the hypothesis or premise and q is the conclusion
  - Example: If you get 100 on the final, then you get an *A*.

    Is this grading rule false when you don't get 100 on the final? NO!

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

Note: $p \rightarrow q$ is equivalent to $\neg p \vee q$ (compare their truth tables)

Implication

- $p \rightarrow q$ is read in a variety of equivalent ways:
  - if p then q
  - p implies q
  - p is sufficient for q
  - q is necessary for p
  - q follows from p
  - q unless $\neg p$ ** this means $q \vee \neg p$*
  - p only if q
- Example:
  - If you get 100 on the final, then you get an *A*.

    p q

Implication

- The converse of $p \rightarrow q$ is $q \rightarrow p$.
- The contrapositive of $p \rightarrow q$ is $\neg q \rightarrow \neg p$
- The inverse of $p \rightarrow q$ is $\neg p \rightarrow \neg q$.
- Examples: (*p:* you get 100 on the final *q:* you get an *A*)
  - $p \rightarrow q$ If you get 100 on the final, then you get an *A*.
  - $q \rightarrow p$ If you get an *A*, then you get 100 on the final.
  - $\neg q \rightarrow \neg p$ If you don't get an *A*, then you don't get 100 on the final.
  - $\neg p \rightarrow \neg q$ If you don't get 100 on the final, then you don't get an *A*.
- Which one is logically equivalent to implication $p \rightarrow q$?
  - contrapositive $\neg q \rightarrow \neg p$

Biconditional

- Let p and q be propositions. The biconditional statement (also known as bi-implications) "p if and only if q", denoted by $p \leftrightarrow q$,

  is true if p and q have the same truth values, and false otherwise.

  - the opposite of $p \leftrightarrow q$ is exclusive or $p \oplus q$

- $p \leftrightarrow q$ is read in the following ways:

  - p if and only if q (or "p iff q" for short)
  - p is necessary and sufficient for q
  - if p then q, and conversely

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

The Propositional Logic Basics

- **Proposition:** a declarative statement that is either true or false
- **Compound proposition:** a proposition that is built from multiple elementary propositions using logical connectives
- **Logical connectives:**
  - $\neg p$ *Negation*
  - $p \wedge q$ *Conjunction*
  - $p \vee q$ *Disjunction*
  - $p \oplus q$ *Exclusive Or*
  - $p \rightarrow q$ *Implication*
  - $p \leftrightarrow q$ *Biconditional*
- **Order of precedence:** $\neg > \wedge > \vee > \rightarrow > \leftrightarrow$ (if same: from left to right)
  - Example: do you understand this formula? $p \rightarrow q \rightarrow r \vee \neg s \wedge t$

    It can be rewritten using parentheses as $(p \rightarrow q) \rightarrow (r \vee (\neg s \wedge t))$

Exercise *(2 mins)*

- p: 2 is a prime (T) q: 6 is a prime (F)
- Determine the truth value of the following:
  - $\neg p$
  - $p \wedge q$
  - $p \wedge \neg q$
  - $p \vee q$
  - $p \oplus q$
  - $p \rightarrow q$
  - $q \rightarrow p$
  - $p \leftrightarrow q$

Exercise *(3 mins)*

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

p	q	r	¬r	p ∨ q	p ∨ q → ¬r

Hint: refer to the truth table for $p \wedge q$ (“and”) and $p \vee q$ (“or”)

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

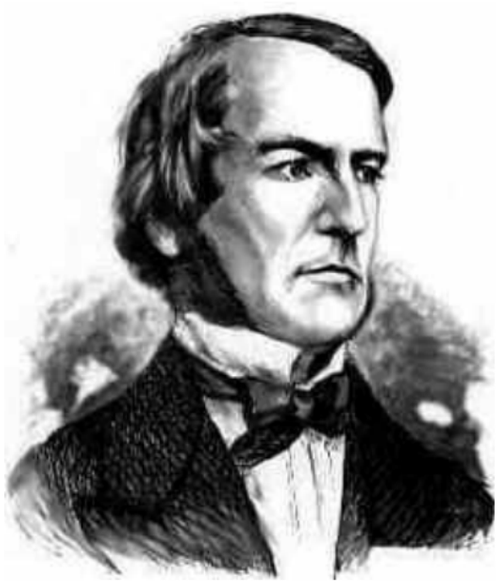
Computer Representation of T/F

- Bit: a unit that represents 2 possible values: 1 (*T*) or 0 (*F*)
- Bit string: a sequence of bits (might be empty)
  - Its length is the number of bits in the string.
- Bitwise operations: replace *T* and *F* with 1 and 0
  - Example: bitwise OR operation

$$\begin{array}{r} 1011\ 0011 \\ \vee\ 0110\ 1010 \\ \hline 1111\ 1011 \end{array}$$

Boolean Algebra

- Boolean algebra is intimately connected to propositional logic:
  - focuses on Boolean variables, i.e., with only 2 values 1 (*T*) and 0 (*F*)
  - invented by British mathematician George Boole (1815~1864)
  - independent from Leibniz's logic work in the 17th century
  - mathematical foundation of digital/logic circuits

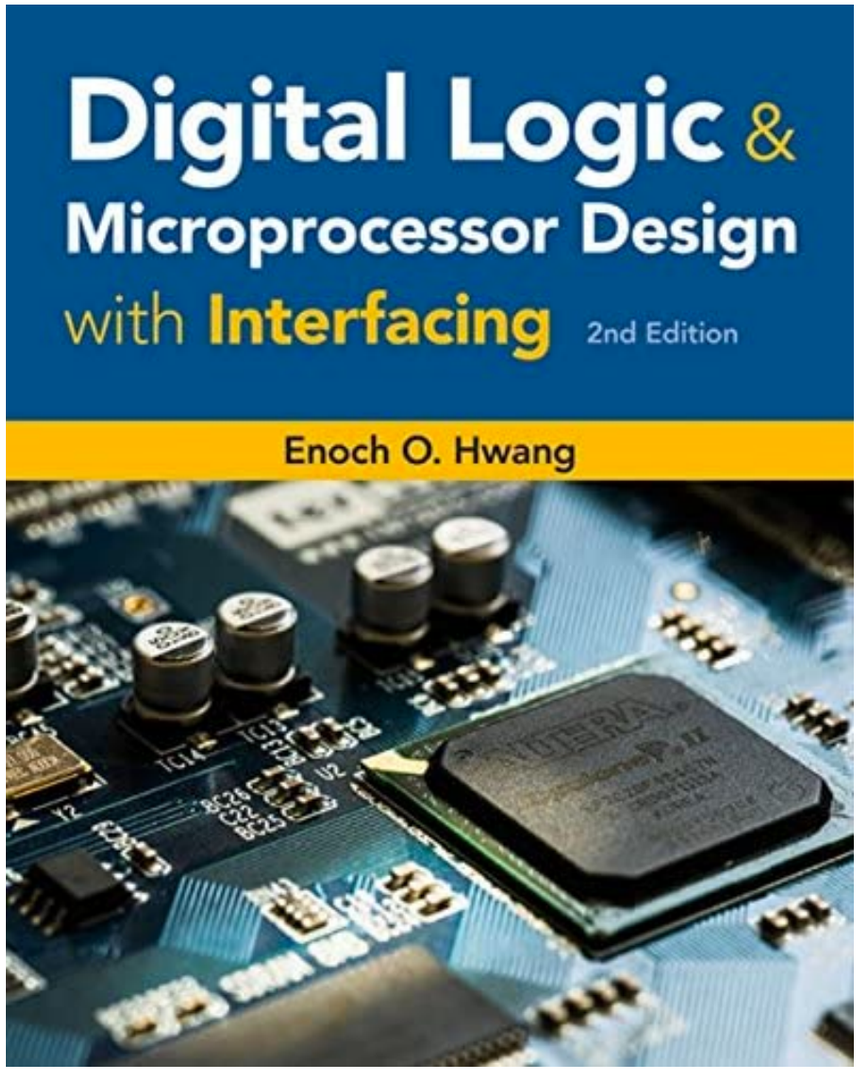


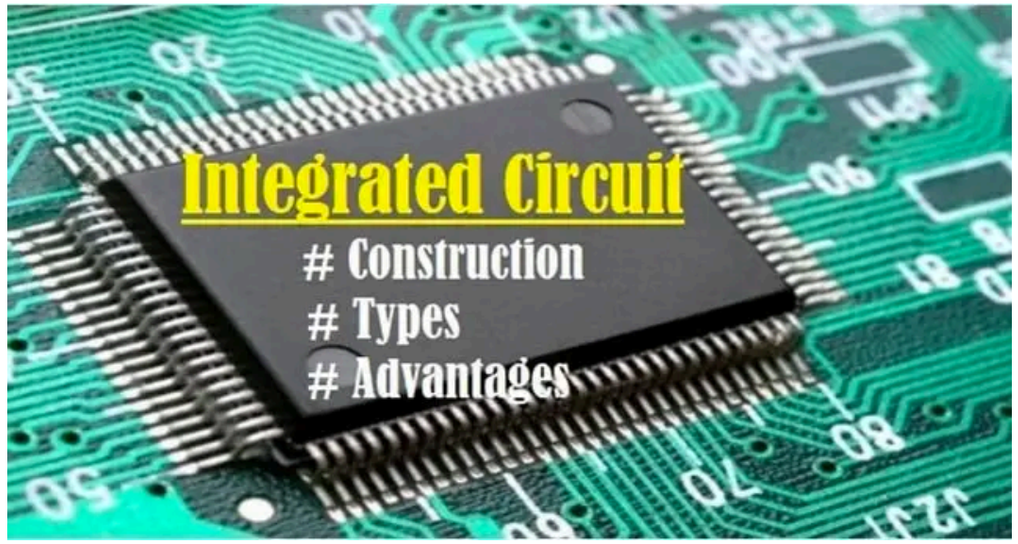
Although Boole's work was not originally perceived as particularly interesting, even by other mathematicians, he is now regarded as one of the founders of the field of computer science.

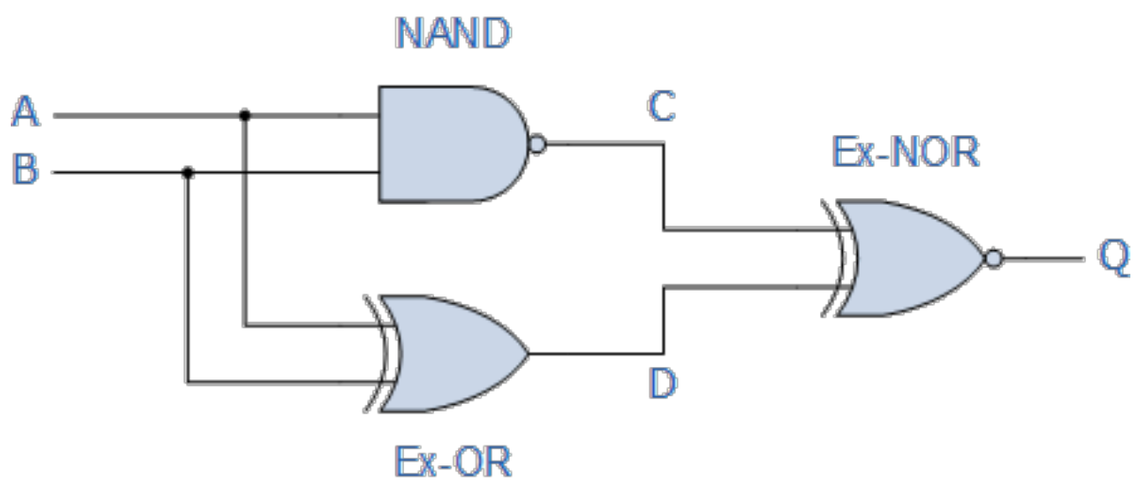
Applications of Logic

Design of Logic Circuits

- Hardware of digital devices (e.g., computers, phones, etc.)







SUSTech

Boolean Search

- Search with logical operators AND, OR, NOT, etc.

Google

Advanced Search

Find pages with...

	To do this in the search box
all these words:	
	Type the important words: `tricolor rat terrier`
this exact word or phrase:	
	Put exact words in quotes: `"rat terrier"`
any of these words:	
	Type `OR` between all the words you want: `miniature OR standard`
none of these words:	
	Put a minus sign just before words you don't want: `-rodent, -"Jack Russell"`
numbers ranging from:	to
	Put 2 periods between the numbers and add a unit of measure: `10..35 lb, $300..$500, 2010..2011`

Logical Inference

- Process of reasoning from premises to logical conclusions
- Example:
  - Statement: **If** you are older than 13 **or** you are with your parents **then** you can watch this movie
  - Elementary propositions:

    p - you are older than 13

    q - you are with your parents

    r - you can watch this movie
  - Translation: $p \vee q \rightarrow r$
  - Logical inference example:

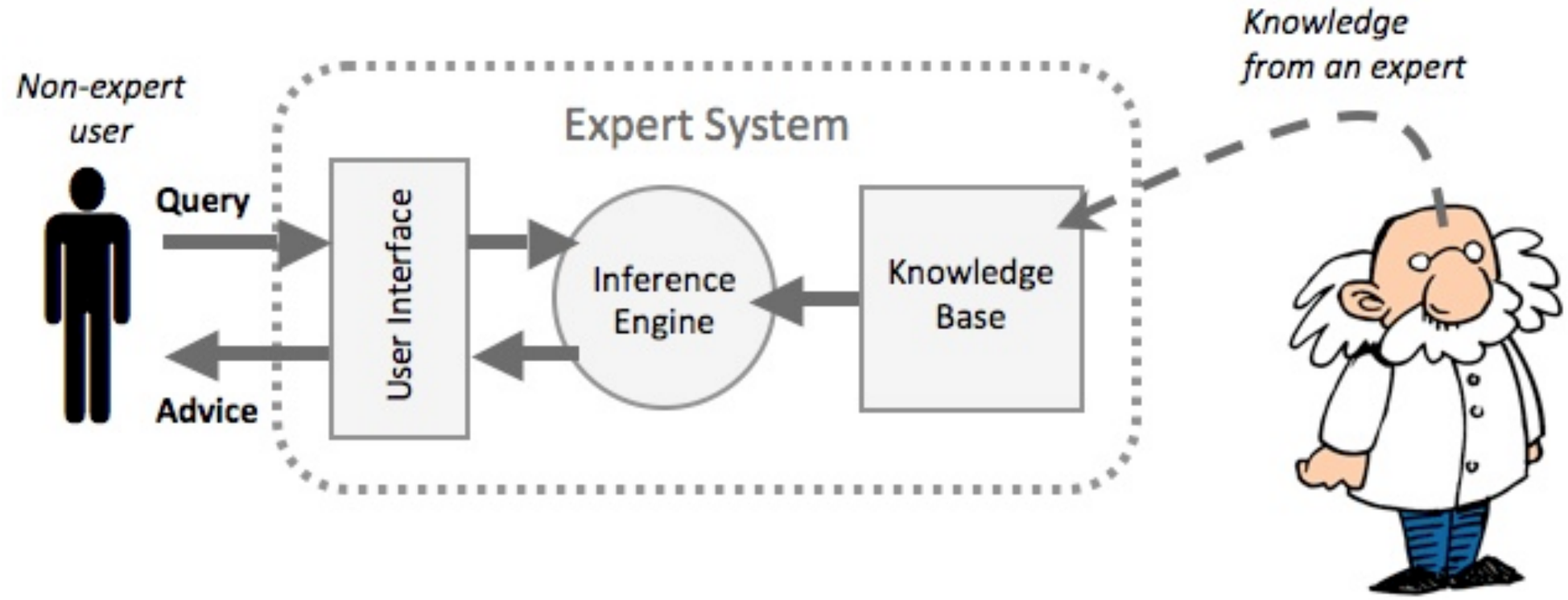
    Suppose p is true (i.e., you are older than 13), then with the help of logic we can infer that r is true (i.e., you can watch this movie).

** Looks trivial? Actually inference is very powerful in many tasks…*

Inference in Artificial Intelligence

- Artificial intelligence builds programs that act intelligently:
  - Programs often rely on symbolic manipulations (logical inference).

Expert System

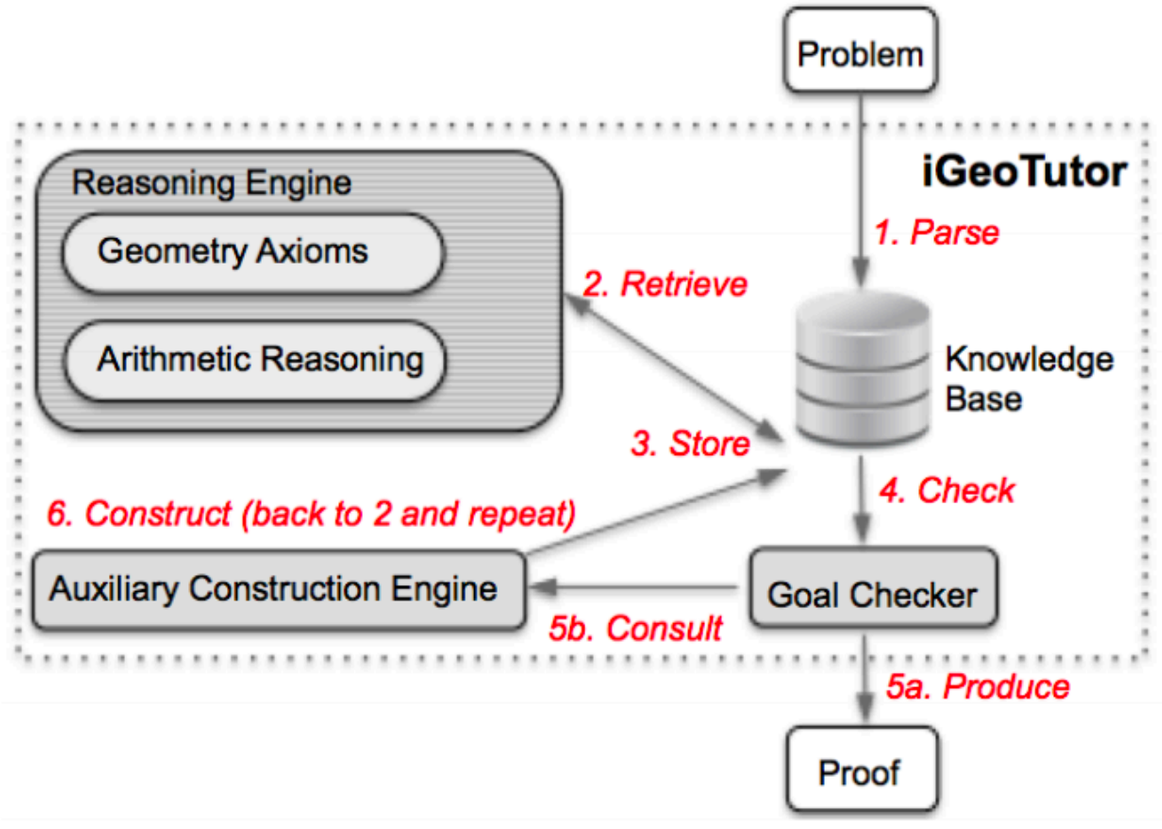


SUSTech

Inference in Artificial Intelligence

- Artificial intelligence builds programs that act intelligently
  - Programs often rely on symbolic manipulations (logical inference).

Automated Theorem Proving



** Wang and Su, Automated Geometry Theorem Proving for Human-Readable Proofs, IJCAI 2015*

What's Next…

- Logical equivalence (basis of proofs and circuit design)
  - important laws of logical equivalence
- Predicate logic (remedies limitations of propositional logic)
  - predicates, quantifiers, etc.
- Proofs
  - rules of inference (formal proofs)
  - theorem proving methods (informal proofs)

Logical Equivalence

Tautology / Contradiction / Contingency

- **Tautology:** a compound proposition that is always true for all possible truth values

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

- **Contradiction:** a compound proposition that is always false for all possible truth values

- **Contingency:** a compound proposition that is neither a tautology nor a contradiction

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

Equivalent Propositions

- Two propositions are equivalent if they always have the same truth value.
- Example:
  - Consider the two pieces of codes taken from two different versions of merge sort. Do they do the same thing?

```
(1) if ((i+j ≤ p+q) && (i ≤ p) &&
    ((j > q) || (List1[i] ≤ List2[j])))
(2)   List3[k] = List1[i]
(3)   i = i+1
(4) else
(5)   List3[k] = List2[j]
(6)   j = j+1
(7) k = k+1
```

```
(1) if (((i+j ≤ p+q) && (i ≤ p) && (j > q))
    || ((i+j ≤ p+q) && (i ≤ p)
        && (List1[i] < List2[j])))
(2)   List3[k] = List1[i]
(3)   i = i+1
(4) else
(5)   List3[k] = List2[j]
(6)   j = j+1
(7) k = k+1
```

Equivalent Propositions

- Two propositions are equivalent if they always have the same truth value.
- Example:
  - Consider the two pieces of codes taken from two different versions of merge sort. Do they do the same thing?

```
(1) if ((i+j ≤ p+q) && (i ≤ p) &&
    ((j > q) || (List1[i] ≤ List2[j])))
```

```
(1) if (((i+j ≤ p+q) && (i ≤ p) && (j > q))
    || ((i+j ≤ p+q) && (i ≤ p)
        && (List1[i] ≤ List2[j])))
```

- Let's rewrite using

  $s \sim (i + j \leq p + q)$, $t \sim (i \leq p)$, $u \sim (j > q)$, $v \sim (List1[i] \leq List2[j])$

  (1): $s \wedge t \wedge (u \vee v)$ (1'): $(s \wedge t \wedge u) \vee (s \wedge t \wedge v)$

- Now set $w \sim (s \wedge t)$

  (1): $w \wedge (u \vee v)$ (1'): $(w \wedge u) \vee (w \wedge v)$

Equivalent Propositions

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

- Example:
  - Consider the two pieces of codes taken from two different versions of merge sort. Do they do the same thing?

(1) $w \wedge (u \vee v)$

w	u	v	$u \vee v$	$w \wedge (u \vee v)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	F
F	T	T	T	F
F	T	F	T	F
F	F	T	T	F
F	F	F	F	F

(1') $(w \wedge u) \vee (w \wedge v)$

w	u	v	$w \wedge u$	$w \wedge v$	$(w \wedge u) \vee (w \wedge v)$
T	T	T	T	T	T
T	T	F	T	F	T
T	F	T	F	T	T
T	F	F	F	F	F
F	T	T	F	F	F
F	T	F	F	F	F
F	F	T	F	F	F
F	F	F	F	F	F

- Now set $w \sim (s \wedge t)$

(1): $w \wedge (u \vee v)$ ***is equivalent to*** *(1'): $(w \wedge u) \vee (w \wedge v)$*

** this is actually one of the distributive laws that we will show soon*

Equivalent Propositions

- The propositions p and q are called logically equivalent if $p \leftrightarrow q$ is a tautology, denoted by $p \equiv q$ or $p \Leftrightarrow q$.

- Equivalent propositions are important for logical reasoning since they can be replaced with each other and can help us:
  - make logical arguments
  - infer new propositions (e.g., in proofs)

- Examples:
  - $p \rightarrow q \equiv \neg p \vee q$ implication can be represented as a disjunction
    ** this later will be referred to as the useful law*
  - $p \rightarrow q \equiv \neg q \rightarrow \neg p$ implication is equivalent to its contrapositive

Important 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
  - $\neg(\neg p) \equiv p$
- Commutative laws
  - $p \vee q \equiv q \vee p$
  - $p \wedge q \equiv q \wedge p$
- Associative laws
  - $(p \vee q) \vee r \equiv p \vee (q \vee r)$
  - $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- Distributive laws
  - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
  - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

Important Logical Equivalences

- De Morgan's laws
  - $\neg(p \vee q) \equiv \neg p \wedge \neg q$
  - $\neg(p \wedge q) \equiv \neg p \vee \neg q$
- Absorption laws
  - $p \vee (p \wedge q) \equiv p$
  - $p \wedge (p \vee q) \equiv p$
- Negation laws
  - $p \vee \neg p \equiv T$
  - $p \wedge \neg p \equiv F$
- Useful law ** we call this useful law just for convenience*
  - $p \rightarrow q \equiv \neg p \vee q$

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

Using Logical Equivalences

- Equivalences can be used in proofs. A proposition or its components can be transformed using equivalences.
- Example:
  - Show that $(p \wedge q) \rightarrow p$ is a tautology
  - Verify with the truth table:

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

Using Logical Equivalences

- Equivalences can be used in proofs. A proposition or its components can be transformed using equivalences.

- Example:
  - Show that $(p \wedge q) \rightarrow p$ is a tautology
  - Proof:

$(p \wedge q) \rightarrow p \equiv \neg(p \wedge q) \vee p$	*Useful*
$\equiv (\neg p \vee \neg q) \vee p$	*De Morgan's*
$\equiv (\neg q \vee \neg p) \vee p$	*Commutative*
$\equiv \neg q \vee (\neg p \vee p)$	*Associative*
$\equiv \neg q \vee T$	*Negation*
$\equiv T$	*Domination*

Exercise *(2 mins)*

- Show that $p \rightarrow q \equiv \neg q \rightarrow \neg p$

- 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
  - $\neg(\neg p) \equiv p$
- Commutative laws
  - $p \vee q \equiv q \vee p$
  - $p \wedge q \equiv q \wedge p$
- Associative laws
  - $(p \vee q) \vee r \equiv p \vee (q \vee r)$
  - $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- Distributive laws
  - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
  - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
- De Morgan's laws
  - $\neg(p \vee q) \equiv \neg p \wedge \neg q$
  - $\neg(p \wedge q) \equiv \neg p \vee \neg q$
- Absorption laws
  - $p \vee (p \wedge q) \equiv p$
  - $p \wedge (p \vee q) \equiv p$
- Negation laws
  - $p \vee \neg p \equiv T$
  - $p \wedge \neg p \equiv F$
- Useful law
  - $p \rightarrow q \equiv \neg p \vee q$

Exercise *(5 mins)*

- Show that $\neg(p \oplus q) \equiv p \leftrightarrow q$

  Hint: by definition $p \oplus q \equiv (p \wedge \neg q) \vee (\neg p \wedge q)$

- 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
  - $\neg(\neg p) \equiv p$
- Commutative laws
  - $p \vee q \equiv q \vee p$
  - $p \wedge q \equiv q \wedge p$
- Associative laws
  - $(p \vee q) \vee r \equiv p \vee (q \vee r)$
  - $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- Distributive laws
  - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
  - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
- De Morgan's laws
  - $\neg(p \vee q) \equiv \neg p \wedge \neg q$
  - $\neg(p \wedge q) \equiv \neg p \vee \neg q$
- Absorption laws
  - $p \vee (p \wedge q) \equiv p$
  - $p \wedge (p \vee q) \equiv p$
- Negation laws
  - $p \vee \neg p \equiv T$
  - $p \wedge \neg p \equiv F$
- Useful law
  - $p \rightarrow q \equiv \neg p \vee q$

Predicate Logic

Limitations of Propositional Logic

- **Propositional logic:** the logic world is described in terms of elementary propositions and their logical combinations

- Can we use propositional logic to express the following?
  - *p:* "Every integer squared is ≥ 0" *q:* "$3^2 \geq 0$"

    Given that *p* is true, then *q* is also true as a special case of *p*.
  - *r:* "Some of the integers are prime" *s:* "2 is prime"

    Given that *s* is true, then *r* is also true as evidenced by *s*.

- No! If $p \rightarrow q$ (or its equivalent) is not given as a premise, then the truth value of *p* cannot infer the truth value of *q*.

- **Solution:** use variables to describe objects in a group (universe) and make statements about some or all objects in the group by quantifying the variables

Predicate Logic

- **Predicate logic:** remedies propositional logic by allowing for making statements with variables and quantifiers

- Basic building blocks:
  - Constant – models a specific object

    Examples: “1”, “SUSTech”…
  - Variable – represents an object in a group (universe)

    Examples: *x, y, z*… ** universe can be people, numbers…*
  - Predicate – represents properties or relations among objects

    Examples: S*tudent(x), Married(A, B)…*

Predicates

- A predicate *P(x)* assigns a value *T* or *F* to each *x* depending on whether the property *P(x)* holds or not for *x*.

- Example:
  - Assume *Prime(x)* where the universe of discourse is integers

    Prime(2) *T*

    Prime(6) *F*

    …

- Is *Prime(x)* a proposition?

  No, but after the substitution it becomes one.

Predicates (Generalized)

- A predicate $P(x_1, x_2, \ldots, x_n)$ is a statement that contains n variables $x_1, x_2, \ldots, x_n$ and it becomes a proposition when all variables x_i are substituted by specific values.

- The universe (domain) D of the predicate variables $(x_1, x_2, \ldots, x_n)$ is the set of all values that may be substituted for the variables.

- The truth set of the predicate $P(x_1, x_2, \ldots, x_n)$ is the set of all values of the predicate variables $(x_1, x_2, \ldots, x_n)$ such that the proposition $P(x_1, x_2, \ldots, x_n)$ is true.

- What is the relation between truth set and universe?
  - truth set is a subset of the universe

Example

- Let *P(x)* be the predicate "$x^2 > x$" where the universe is all real numbers.
  - What are the truth values of *P(2)* and *P(1)*?

    P(2) = *T*

    P(1) = *F*
  - What is the truth set of *P(x)*?

    $x > 1$ or $x < 0$

Exercise *(1 min)*

- Let *Q(x, y)* be the predicate "$x = y + 3$" where the universe is all pairs of real numbers.
  - What are the truth values of *Q(1, 2)* and *Q(3, 0)*?
  - What is the truth set of *Q(x, y)*?

Compound Statements

- **Compound statements** are obtained from multiple statements (including predicates and propositions) via logical connectives

- Examples:
  - *Prime(2)* $\wedge$ *Prime(3)*

    Translation: “Both 2 and 3 are primes.” (T)

  - *City(Shenzhen)* $\vee$ *River(Shenzhen)*

    Translation: “Shenzhen is a city or a river.” (T)

  - *CS-major(x)* $\rightarrow$ *Student(x)*

    Translation: “If *x* is CS-major then *x* is a student.”

    ** not a proposition because x is not explicit*

Predicates vs Propositions

- A predicate of form *P(x)* is not a proposition because there are many objects that it can be applied to.
- However, with predicates, predicate logic allows us to
  - explicitly manipulate the objects with variables
  - capture quantified statements with quantifiers, where variables are substituted for to make statements about a group of objects

Quantified Statements

- Universally quantified
  - Example: “All CS-major graduates have to pass CS201.”
    (This is true for all CS-major graduates.)
- Existentially quantified
  - Example: “Some CS-major students graduate with honor.”
    (This is true for some students.)

Universal Quantifier

- The universal quantification of $P(x)$ is the proposition: "$P(x)$ is true for all values of x in the universe of discourse." This is denoted by $\forall x\, P(x)$ and expressed as "for every x, $P(x)$ *is true*".

- Example: $P(x)$: *"$x > x - 1$"* where the universe is all real numbers
  - What is the truth value of $\forall x\, P(x)$?

    T

  - Is $P(x)$ a proposition?

    No. Many possible substitutions.

  - Is $\forall x\, P(x)$ a proposition?

    Yes. It is true if and only if for all x from the universe $P(x)$ is true.

Existential Quantifier

- The existential quantification of $P(x)$ is the proposition: "There exists an element in the universe of discourse such that $P(x)$ is true ." This is denoted by $\exists x\, P(x)$ and expressed as "there is an x such that $P(x)$ *is true*".

- Example: $P(x)$: "$x > 5$" where the universe is all real numbers
  - What is the truth value of $\exists x\, P(x)$?

    T
  - Is $P(x)$ a proposition?

    No. Many possible substitutions.
  - Is $\exists x\, P(x)$ a proposition?

    Yes. It is true if and only if there is an x from the universe s.t. $P(x)$ is true.

Exercise *(2 mins)*

- *P(x): "x ≥ 0"* where *x* is a natural number
  - What is the truth value of ∀*x P(x)*?

- *Q(x): "x = x + 2"* where *x* is a real number
  - What is the truth value of ∃*x Q(x)*?

- *C(x): CS-major(x) ∧ Honor-student(x)* where *x* is a SUSTech student

  Assume all CS-major students graduate with honor

  - What is the truth value of ∀*x C(x)*?

  - What is the truth value of ∃*x C(x)*?

Summary of Quantified Statements

- When are $\forall x\ P(x)$ and $\exists x\ P(x)$ true and false?

Statement	When true?	When false?
$\forall x\ P(x)$	P(x) true for all x	There is an x where P(x) is false.
$\exists x\ P(x)$	There is some x for which P(x) is true.	P(x) is false for all x.

- Suppose that the elements in the universe can be enumerated as $a_1, a_2, \ldots, a_n$, then:
  - $\forall x\ P(x)$ is true whenever $P(a_1) \wedge P(a_2) \wedge \ldots \wedge P(a_n)$ is true
  - $\exists x\ P(x)$ is true whenever $P(a_1) \vee P(a_2) \vee \ldots \vee P(a_n)$ is true

The Universe Matters

- The truth values of $\exists x\, P(x)$ and $\forall x\, P(x)$ depend on both the predicate $P(x)$ and the universe.

- Example: $P(x)$: "$x < 2$"
  - universe: the positive integers

    $\exists x\, P(x)$ – T $\forall x\, P(x)$ – F
  - universe: the negative integers

    $\exists x\, P(x)$ – T $\forall x\, P(x)$ – T
  - universe: $\{3, 4, 5\}$

    $\exists x\, P(x)$ – F $\forall x\, P(x)$ – F

Precedence of Quantifiers

- The quantifiers ∀ and ∃ have higher precedence than all other logical operators, i.e., ∀/∃ > ¬ > ∧ > ∨ > → > ↔

- Example: what does $\exists x\, P(x) \vee Q(x)$ mean?
  - It means $(\exists x\, P(x)) \vee Q(x)$ rather than $\exists x\, (P(x) \vee Q(x))$

Translation with Quantifiers

- Statement: "All SUSTech students are smart."
  - universe: all SUSTech students

    translation: $\forall x\ Smart(x)$
  - universe: all students

    translation: $\forall x\ (At(x, SUSTech) \rightarrow Smart(x))$

    What about this? $\forall x\ (At(x, SUSTech) \wedge Smart(x))$

    This means every student is at SUSTech and is smart!
  - universe: all people

    translation: $\forall x\ (Student(x) \wedge At(x, SUSTech) \rightarrow Smart(x))$

Translation with Quantifiers

- Statement: "Someone at SUSTech is smart."
  - universe: all SUSTech affiliates

    translation: $\exists x\ Smart(x)$
  - universe: all people

    translation: $\exists x\ (At(x, SUSTech) \wedge Smart(x))$

    What about this? $\exists x\ (At(x, SUSTech) \rightarrow Smart(x))$

This is even true if there is someone who is not at SUSTech and nobody at SUSTech is smart!

Negation of Quantified Statements

- Example: “Nothing is perfect.”
  - translation 1: ¬ ∃*x Perfect(x)*
  - translation 2: ∀*x* ¬*Perfect(x)* (“Everything is imperfect.”)
- Conclusion: ¬ ∃*x P(x)* is equivalent to ∀*x* ¬*P(x)*

Negation of Quantified Statements

- Example: “Not all horses are white.”
  - translation 1: $\neg\ \forall x\ (Horse(x) \rightarrow White(x))$
  - translation 2: $\exists x\ (Horse(x) \wedge \neg White(x))$ (“There is non-white horse.”)
    logically equivalent to $\exists x\ \neg(Horse(x) \rightarrow White(x))$ *why?*
    useful and De Morgan’s
- Conclusion: $\neg\ \forall x\ P(x)$ is equivalent to $\exists x\ \neg P(x)$

Negation of Quantified Statements

- De Morgan's laws (logical equivalence) for quantifiers

Negation	Equivalent Statement	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 an 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.

Nested Quantifiers

- More than one quantifier may be necessary to capture the meaning of a statement in the predicate logic.

- Example 1: "Every real number has its corresponding negative."
  - a real number is denoted by x and its negative as y
  - a predicate $P(x, y)$ denotes "$x + y = 0$"

- Translation: $\forall x \exists y\, P(x, y)$

Nested Quantifiers

- More than one quantifier may be necessary to capture the meaning of a statement in the predicate logic.
- Example 2: "There is a person who loves everybody."
  - variables *x* and *y* denote people
  - a predicate *L(x, y)* denotes "*x* loves *y*"
  - Translation: $\exists x \forall y\, L(x, y)$

Order of Quantifiers

- The order of nested quantifiers matters if quantifiers are of different types.

- Example: $\forall x \exists y\ L(x, y) \not\equiv \exists y \forall x\ L(x, y)$ *L(x, y) denotes "x loves y"*
  - $\forall x \exists y\ L(x, y)$: Everybody loves somebody
  - $\exists y \forall x\ L(x, y)$: There is someone who is loved by everyone

Order of Quantifiers

- The order of nested quantifiers does not matter if quantifiers are of the same type.
- Example: $\forall x \forall y\ (Parent(x, y) \rightarrow Child(y, x))$
  - This means: for all x and y, if x is a parent of y, then y is a child of x.
  - $\forall y \forall x\ (Parent(x, y) \rightarrow Child(y, x))$ means the same

Exercise *(3 mins)*

- Variables *x, y* denote people, and *L(x, y)* denotes "*x* loves *y*" Translate the following to quantified formulas.
  1. Everybody loves Raymond.
  2. Everybody loves somebody.
  3. There is somebody whom everybody loves.
  4. There is somebody whom Raymond doesn't love.
  5. There is somebody whom no one loves.
  6. There is exactly one person whom everybody loves. * *try =, ≠*

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

Negating Nested Quantifiers

- Example: "for every real number x, there exists a real number y such that $xy = 1$."
- Translation: $\forall x \exists y\ (xy = 1)$
- Negation: $\neg\forall x \exists y\ (xy = 1)$

  $\equiv \exists x \neg\exists y\ (xy = 1)$ *De Morgan's* *P(x): ∃y (xy = 1)*

  $\equiv \exists x \forall y\ \neg(xy = 1)$ *De Morgan's* *P(y): xy = 1 for some x**

  $\equiv \exists x \forall y\ (xy \neq 1)$ *Definition*

- What is the negation of $\forall x \exists y\ P(x, y)$? What about $\exists x \forall y\ P(x, y)$?
  - $\neg\forall x \exists y\ P(x, y) \equiv \exists x \forall y\ \neg P(x, y)$
  - $\neg\exists x \forall y\ P(x, y) \equiv \forall x \exists y\ \neg P(x, y)$

Proofs

Axiom / Theorem / Lemma / Proof

- **Axiom (or postulate):** a statement or proposition which is regarded as being established, accepted, or self-evidently true.
  - E.g., “A straight line segment can be drawn joining any two points.”
- **Theorem:** a statement that can be proved to be true.
  - E.g., “There are infinitely many prime numbers.”
- **Lemma:** a statement that can be proved to be true, and is used in proving a theorem.
- **Proof:** a correct supporting argument that shows the truth value of a statement following from other statements (e.g., premises, axioms, theorems, lemmas, etc.)

Theorems

- Typically, a theorem looks like this:

$$p_1 \wedge p_2 \wedge \ldots \wedge p_n \rightarrow q$$

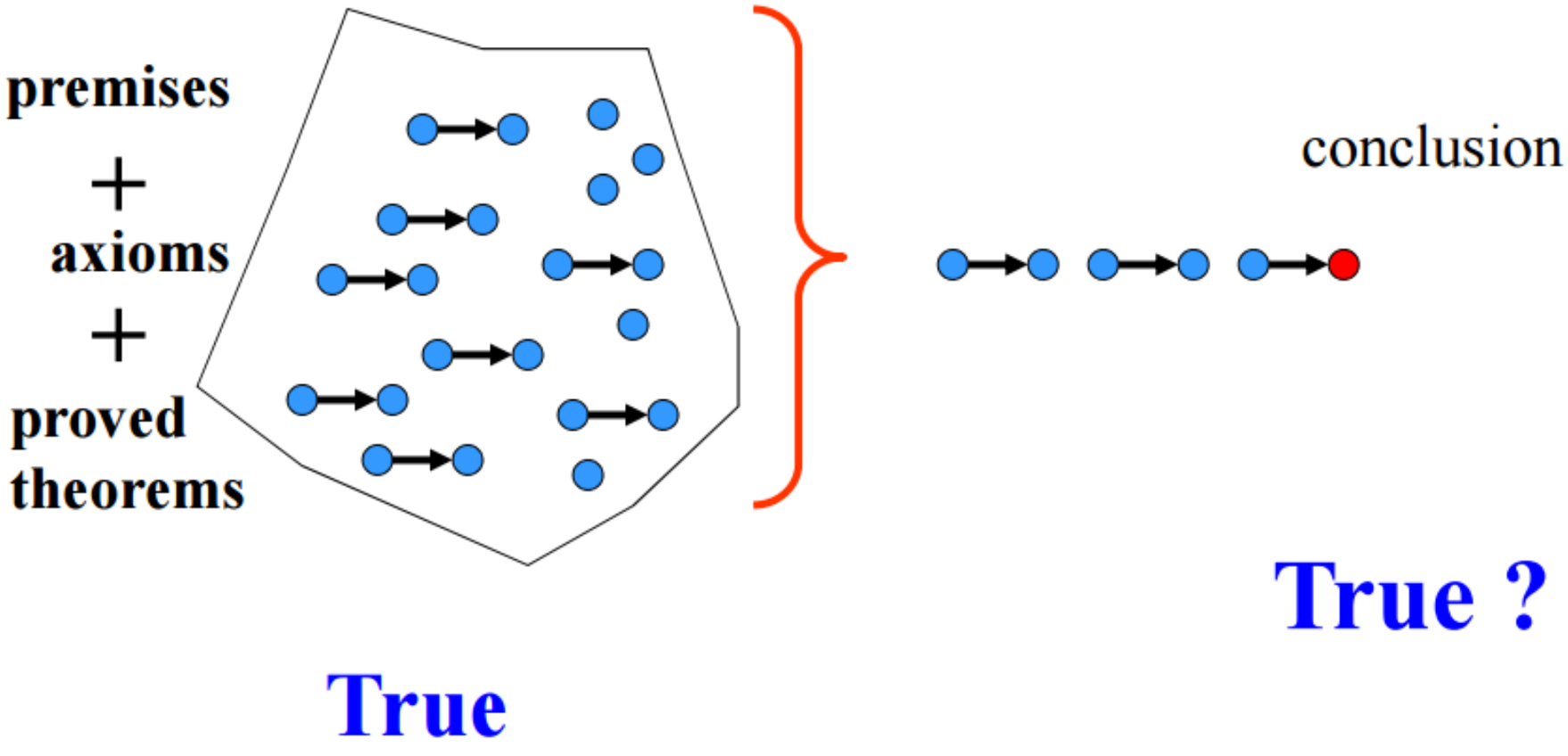
premises *conclusion*

- Example: Fermat's little theorem
  - If p is a prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Formal Proofs

- In formal proofs, steps follow logically from the set of premises, axioms, lemmas, and proved theorems.



Using Logical Equivalence Rules

- Proofs based on logical equivalences: a statement can be transformed using a sequence of equivalence rewrites until some conclusion can be reached.

- Example:
  - Show that $(p \wedge q) \rightarrow p$ is a tautology
  - Proof:

$(p \wedge q) \rightarrow p$	$\equiv \neg(p \wedge q) \vee p$	*Useful*
	$\equiv (\neg p \vee \neg q) \vee p$	*De Morgan's*
	$\equiv (\neg q \vee \neg p) \vee p$	*Commutative*
	$\equiv \neg q \vee (\neg p \vee p)$	*Associative*
	$\equiv \neg q \vee T$	*Negation*
	$\equiv T$	*Domination*

Rules of Inference for Propositional Logic

- **Rules of inference** (premises are true implies conclusion is true)
  - allow to infer new true statements from existing true statements
  - represent logically valid inference patterns
- List of rules:
  - Modus ponens
  - Modus tollens
  - Hypothetical syllogism
  - Disjunctive syllogism
  - Addition
  - Simplification
  - Conjunction
  - Resolution

Rules of Inference for Propositional Logic

- Modus ponens (Affirming the antecedent/Conditional elimination)

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

corresponding tautology:
$((p \to q) \wedge p) \to q$

- Example:
  - p "It is raining."
  - q "I will study discrete math."
  - $p \to q$ "If it is raining, then I will study discrete math."
  - p "It is raining."
  - q "Therefore, I will study discrete math."

Rules of Inference for Propositional Logic

- Modus tollens (Denying the consequent)

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

corresponding tautology:
$((p \rightarrow q) \wedge \neg q) \rightarrow \neg p$

- Example:
  - p "It is raining."
  - q "I will study discrete math."
  - $p \rightarrow q$ "If it is raining, then I will study discrete math."
  - $\neg q$ "I will not study discrete math."
  - $\neg p$ "Therefore, it is not raining."

Rules of Inference for Propositional Logic

- Hypothetical syllogism

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

corresponding tautology:
$(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$

- Disjunctive syllogism

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

corresponding tautology:
$((p \vee q) \wedge \neg p) \rightarrow q$

Rules of Inference for Propositional Logic

- Addition

$$\frac{p}{\therefore p \vee q}$$

corresponding tautology:

p → *(p* ∨ *q)*

- Simplification

$$\frac{p \wedge q}{\therefore q}$$

corresponding tautology:

(p ∧ *q)* → *q* * *of course we also have (p* ∧ *q)* → *p*

Rules of Inference for Propositional Logic

- Conjunction

$$\frac{p \quad q}{\therefore p \wedge q}$$

corresponding tautology:

(p) ∧ (q) → p ∧ q

- Resolution

** this rule may not look straightforward*

$$\frac{\neg p \vee r \quad p \vee q}{\therefore q \vee r}$$

corresponding tautology: *(p is either true or false)*

(¬p ∨ r) ∧ (p ∨ q) → (q ∨ r)

Example

- Premises:
  - “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.”
- Show that all these lead to a conclusion:
  - “We will be home by sunset.”

Example

- Premises:
  - “It is not sunny this afternoon and it is colder than yesterday.” $\neg p \wedge q$
  - “We will go swimming only if it is sunny.” $r \rightarrow p$
  - “If we do not go swimming then we will take a canoe trip.” $\neg r \rightarrow s$
  - “If we take a canoe trip, then we will be home by sunset.” $s \rightarrow t$
- Show that all these lead to a conclusion:
  - “We will be home by sunset.” t

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

Example

- Translation:
  - premises: $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, $s \rightarrow t$
  - conclusion: t
- Proof:

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)

Rules of Inference for Quantified Statements

- Universal Instantiation (UI)

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

- Universal Generalization (UG)

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

- Existential Instantiation (EI)

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

- Existential Generalization (EG)

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

Example

- Premises:
  - “A student in this class has not read the book.”
  - “Everyone in this class passed the first exam.”
- Show that all these lead to a conclusion:
  - “Someone who passed the first exam has not read the book.”

Example

- Premises:
  - “A student in this class has not read the book.” $\exists x(C(x) \wedge \neg B(x))$
  - “Everyone in this class passed the first exam.” $\forall x(C(x) \rightarrow P(x))$
- Show that all these lead to a conclusion:
  - “Someone who passed the first exam has not read the book.” $\exists x(P(x) \wedge \neg B(x))$

$C(x)$ “x is in this class.”
$B(x)$ “x has read the book.”
$P(x)$ “x passed the first exam.”

Example

- Translation:
  - premises: $\exists x(C(x) \wedge \neg B(x))$, $\forall x(C(x) \rightarrow P(x))$
  - conclusion: $\exists x(P(x) \wedge \neg B(x))$
- Proof:

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)

Informal Proofs

- Proving theorems in practice:
  - Proof steps are not expressed in any formal language of logic.
  - One must always watch the consistency of the argument made. Logic and its rules can often help us decide the soundness of the argument.

- Next, we use informal proofs to illustrate different methods of theorem proving, i.e., proof strategy.

Methods of Theorem Proving

- Basic methods to prove theorems:
  - Direct proof

    $p \rightarrow q$ is proved by showing that if p is true then q follows
  - Proof by contraposition

    $p \rightarrow q$ is proved by showing the contrapositive $\neg q \rightarrow \neg p$
  - Proof by contradiction

    show that *"p is true but q is false"* contradicts the assumptions
  - Proof by cases

    give proofs for all possible cases
  - Proof by equivalence

    $p \leftrightarrow q$ is replaced with $(p \rightarrow q) \wedge (q \rightarrow p)$

** Proof by induction will be covered in later lectures*

Direct Proof

- $p \rightarrow q$ is proved by showing that if p is true then q follows
- Example: Prove that "if n is odd, then n^2 is odd"
  - Proof:

    Assume that the hypothesis is true, i.e., n is odd.

    That is, $n = 2k + 1$ where k is an integer.

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

    Therefore, n^2 is odd.

Proof by contraposition

- $p \rightarrow q$ is proved by showing the contrapositive $\neg q \rightarrow \neg p$
- Example: Prove that "if $3n + 2$ is odd, then n is odd"
  - Proof:

    Assume that n is even, i.e., $n = 2k$, where k is an integer.

    Then, $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$.

    Therefore, $3n + 2$ is even.

Proof by Contradiction

- To prove $p \rightarrow q$ is true, assume p is true but q is false ($p \wedge \neg q$), then show a contradiction to p or $\neg q$, or other settled results.

- Example: Prove that "if $3n + 2$ is odd, then n is odd"
  - Proof:

    Assume that $3n + 2$ is odd and n is even,

    Then, $n = 2k$ for some integer k, and $3n + 2 = 2(3k + 1)$.

    Thus, $3n + 2$ is even.

    This is a contradiction to the assumption that $3n + 2$ is odd.

    Therefore, n is odd.

- How to prove q (with no explicit premise) by contradiction?
  - Assume $\neg q$ is true (i.e., q is false) and show a contradiction to $\neg q$ or other settled results.

Proof by Cases

- In order to show $(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$, it is equivalent to show $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)$. *Why?*

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

$$\equiv \neg(p_1 \vee p_2 \vee \ldots \vee p_n) \vee q \qquad \textit{Useful}$$

$$\equiv (\neg p_1 \wedge \neg p_2 \wedge \ldots \wedge \neg p_n) \vee q \qquad \textit{De Morgan's}$$

$$\equiv (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \wedge \ldots \wedge (\neg p_n \vee q) \qquad \textit{Distributive}$$

$$\equiv (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q) \qquad \textit{Useful}$$

- Example: Prove that "$|x||y| = |xy|$ for real numbers x, y"
  - Proof: (4 cases)

$x \geq 0, y \geq 0$ $\qquad$ $x \geq 0, y < 0$

$x < 0, y \geq 0$ $\qquad$ $x < 0, y < 0$

Proof by Equivalence

- To prove $p \leftrightarrow q$, show $(p \rightarrow q) \wedge (q \rightarrow p)$.

- Example: Prove that "an integer n is odd if and only if n^2 is odd"
  - Proof: (sketch)

    Proof of $p \rightarrow q$: direct proof

    Proof of $q \rightarrow p$: proof by contraposition

Vacuous Proof and Trivial Proof

- **Vacuous Proof:** To prove $p \rightarrow q$, if p is always false, then $p \rightarrow q$ is always true.

- Example: Let $P(n)$ denote "if $n > 1$ then $n^2 > n$". Show $P(0)$.
  - Proof:

    Since the premise $0 > 1$ is always false, $P(0)$ is true.

- **Trivial Proof:** To prove $p \rightarrow q$, if q is always true, then $p \rightarrow q$ is always true.

- Example: Let $P(n)$ denote "if $a \geq b$ then $a^n \geq b^n$". Show $P(0)$.
  - Proof:

    Since the conclusion $a^0 \geq b^0$ is always true, $P(0)$ is true

Proofs with Quantifiers

- Universally quantified statements
  - positive: prove the property holds for all examples
    e.g., proof by cases to divide the proof into different parts
  - negative: disprove universal statements
    e.g., show counterexamples
- Existentially quantified statements
  - positive: constructive
    e.g., find a specific example to show the statement holds
  - negative: nonconstructive
    e.g., proof by contradiction

Exercise *(5 mins)*

- Prove that "$\sqrt{2}$ is irrational." (rational numbers are of the form $\frac{m}{n}$, where *m, n* are integers with 1 as their greatest common divisor)
  Hint: proof by contradiction

Exercise *(5 mins)*

- Prove that "There are infinitely many prime numbers." (a prime number is a natural number > 1 that is not divisible by any smaller natural number except 1) *Hint: proof by contradiction*

“… mathematical logic is and must be the basis for software design … mathematical analysis of designs and specifications have become central activities in computer science research…”

Edsger W. Dijkstra (1930–2002), Dutch computer scientist

03 Sets and Functions

To be continued…

Assignment 1

- Deadline for Assignment 1: before class on Oct 10th
- Requirements:
  - must be written in English (otherwise your grade will be 0)
  - must submit a single PDF file on Blackboard
  - due roughly 2~3 weeks after the release date excluding holidays
- **DO NOT CHEAT!** Plagiarism will be punished severely.
  - It's OK to form study groups and share ideas, but do not plagiarize!
- Please submit signed Undergraduate Students Declaration Form on Blackboard, otherwise your grade will be 0.
  - The form must carry your **authentic handwritten signature**: signing on a tablet is allowed, but simply typing in your name to the form does NOT count and your assignment will be graded as 0.