ITCS112 - Discrete Structures

Summer 2023

WHAT is this course about?

WHY do you need this course?

HOW to do well in this course?

Topics for the MIDTERM

These will be adjusted as we go along.

Aj.Pla
piyanuch.sil@mahidol.edu

Weeks 1-2 Logic and Proof	Weeks 3-5 Sets and Counting	Weeks 6-8 Properties of Integers
Propositions & Logical Operators Rules of Inference and Validity Mathematical Induction	Sets, Operations on Sets PIE, Sum and Product Rules Counting and Combinatorics	Divisibility and Modulo Binary and Base Arithmetic Applications in Cryptography

Topics for the **FINAL**

These will be adjusted as we go along.

Aj. Tee
rawesak.tan@mahidol.ac.th

Weeks 9-10 Relations	Weeks 11-12 Prop. of Relations	Weeks 13-14 Functions	Week 15 Summary
Product Sets, Partitions Relations and Digraphs Boolean Matrix of Rel.	Properties of Relations Equivalence Relations Transitive Closure	Functions in CS Growth of Functions Permutation Functions	Conclusion Add. Topics Exam Review

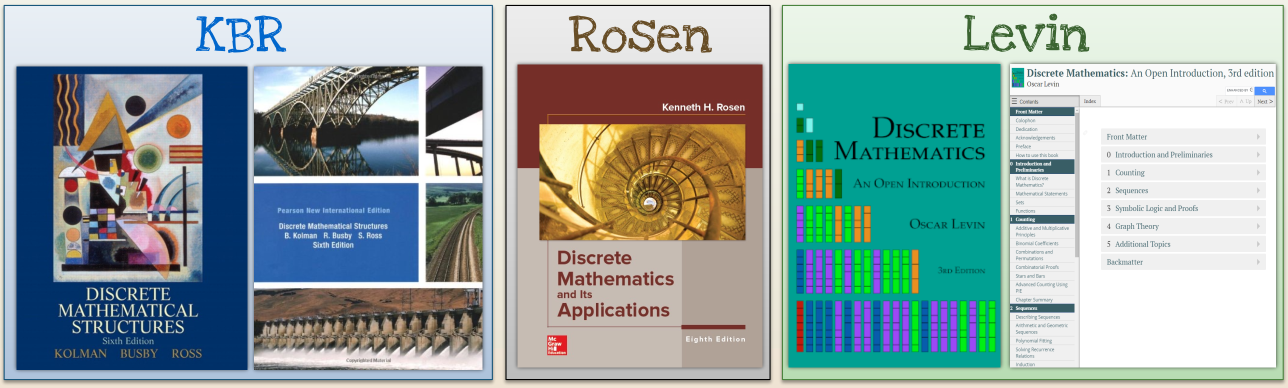
Course Learning Outcomes 3 – 0 – 6 HOURS/WEEK

- Recall fundamental mathematical concepts in arithmetic and algebra
- Demonstrate knowledge of key theories and concepts in discrete math
- Demonstrate the abilities and skills to solve problems in discrete math

Class materials and resources

Many practice problems for your self-study!!

- **Reading and practice exercises (problems with hints and solutions)**
  - Discrete Mathematical Structures by Kolman, Busby, and Ross
  - Discrete Mathematics and Its Applications by Rosen
  - Discrete Math by Levin – http://discrete.openmathbooks.org/dmoi3/



IN-CLASS
Live-Lecture, Videos
Step-by-step worked examples & exercises

AT-HOME
Review the concepts
Practice problem sets
Collaborate with friends

PAPER-BASED QUIZ
- At the beginning of class, 9:05 – 9:25am
- No makeup, 5 of 6
- Materials from the previous class

QUIZ
Closed-book
No calculator
10 quizzes
3% each

EXAM
Midterm and Final

Assessment score and evaluation 30% 70%

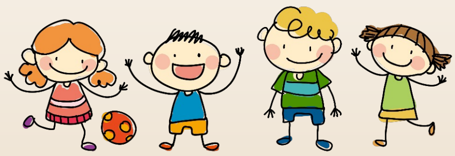
WORKED EXAMPLES

Give it a try! Take good notes!
We will go over these together in-class.

PRACTICE

PRACTICE PROBLEMS

End-of-class exercises: check your understanding & prepare for a quiz. For answers or solutions, consult your instructor or TA.



PROPOSITIONS AND LOGICAL OPERATIONS

Propositional Logic and Proofs

The basic building blocks of logic – propositions

- A **proposition** is a declarative sentence (that is, a sentence that declares a fact) that is **either true or false, but not both**.

Is it a proposition?
5 is a prime number
12 + 7 = 8
Do you speak French?
Happy Birthday!
Please pass the salt.
3 – x = 5

Compound statements and logical operators

Math

x, y, z, … conventional (common) variables representing real numbers
+, −, ×, ÷, … mathematical operators that are used to combined variables

Logic

p, q, r, s, … **propositional variables**, representing propositions

$\neg, \land, \lor, \oplus, \rightarrow, \leftrightarrow, \ldots$ **logical operators** are used to form **compound propositions**

- The negation operator, ¬*p: it is not the case that p*, constructs a new proposition from a single existing proposition. Other logical operators, i.e., ∧, ∨, ⊕, →, ↔, …, are **connectives**, combing two or more existing propositions.
- **Atomic propositions** are ones that cannot be expressed in a simple proposition

Unary operation

- The **negation** (i.e. not) logical operator
- ¬p is a proposition if p is a proposition
- ¬p means *it is not the case that p*

not

negation

p	¬p
T	**F**
F	**T**

A truth table: giving the truth value of a compound proposition for every combination of its component parts

Logical connectives

and

conjunction

p	q	p ∧ q
T	T	
T	F	
F	T	
F	F	

or

disjunction

p	q	p ∨ q
T	T	
T	F	
F	T	
F	F	

xor

exclusive disjunction

p	q	p ⊕ q
T	T	
T	F	
F	T	
F	F	

Logical connectives

if p then q
implication

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

p if-and-only-if q
double implication

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

- **$p \leftrightarrow q$** or **p iff q** is an **equivalence** or called **bicondition**
- $p \leftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$

Precedence of logical operators

- $\neg p \wedge q$ means_______________
- $p \vee q \wedge r$ means_____________
- $p \rightarrow q \vee r$ means____________
- To make it clear, **use parenthesis!**

operators	precedence
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

Analogously, we do ^ (exponent or power) before ×, ÷ before +, − ***Math***

A truth table for $(p \land q) \lor (\neg p)$

p	q	$p \land q$	$\neg p$	$(p \land q) \lor (\neg p)$
T	T			
T	F			
F	T			
F	F			

know this …

If a compound statement contains n propositional statements, then how many rows will there be in the truth table?

PRACTICE PROBLEMS

- Construct a truth table for a proposition $(p \lor \neg q) \oplus (r \to q)$

WORKED EXAMPLES

Find the truth value of each proposition if p, r are true and q, s, t are false.

- $p \vee q \vee r$
- $(\neg p \vee q) \wedge r$
- $(p \oplus t) \rightarrow (\neg r \oplus (q \leftrightarrow \neg s))$

PRACTICE PROBLEMS

Find the truth value of each statement if p, q are true and r, s, t are false

- $(\neg q) \rightarrow (r \rightarrow (r \rightarrow (p \vee s)))$
- $(r \wedge s \wedge t) \leftrightarrow (p \vee q)$
- $(\neg t) \rightarrow (r \vee (\neg s \rightarrow (q \oplus p)))$
- $(q \rightarrow (r \rightarrow s)) \wedge ((p \rightarrow s) \rightarrow (\neg t))$

Tautology, contradiction, and contingency

Tautology	Contradiction	Contingency
Always true	Always false	Some true some false
$p \lor \neg p$	**$p \land \neg p$**	**$p \to \neg p$**

p	$p \lor \neg p$
T	T
F	T

p	$p \land \neg p$
T	F
F	F

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

WORKED EXAMPLES

Construct truth tables to determine whether the given statement is a tautology, a contradiction, or a contingency.

- $p \land q \land (q \to \neg p)$

p	q	$p \land q$	$q \to \neg p$	$p \land q \land (q \to \neg p)$
T	T			
T	F			
F	T			
F	F			

PRACTICE PROBLEMS 2 variables

Construct truth tables to determine whether the given statement is a tautology, a contradiction, or a contingency.

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

PRACTICE PROBLEMS 3 variables

Is the given proposition is a tautology, a contradiction, or a contingency. If it is a contingency, give one truth assignment for which the proposition is true and one for which it is false.

- $[\neg(\neg p \vee \neg(q \wedge \neg r))] \vee \neg\neg(q \vee \neg p)$

PROPOSITIONAL EQUIVALENCES

Propositional Logic and Proofs

Logically Equivalence

Are two statements equivalent?

The compound propositions P & Q always have the same truth values

Proof of equivalence

p	q	$p \to q$	$\neg p \lor q$	$(p \to q) \leftrightarrow (\neg p \lor q)$
T	T			
T	F			
F	T			
F	F			

These two columns are the same

Join P and Q by a bijection (iff) results in a tautology

$P \equiv Q$ iff $P \leftrightarrow Q$ is a tautology

Proof non-equivalence

Find a counterexample – assign truth values so that P evaluates to true and Q false or vice versa (i.e. the two statements disagree)

NOT logically equivalence

Example: show that the negation of $p \leftrightarrow q$ is not equivalent to $(\neg p \rightarrow q)$

How? -- join the two statements using $\leftrightarrow$ (iff), and construct a truth table

The two statements are NOT equivalent if there is a row evaluated to false

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

The two statements are not equivalence because when p is ______ and q is ______, their the truth values of the two statements are not the same.

PRACTICE PROBLEMS

Are two statements logically equivalent: $\neg(p \lor (\neg p \land q))$ and $\neg p \land \neg q$?

Use a truth table

PRACTICE PROBLEMS

Show that $(p \to q) \to r$ and $p \to (q \to r)$ are not equivalent?

Give a counterexample

Methods of proof for logical equivalence

- **Use a truth table** to show that two propositions are equivalent – join them by iff and that all cases of $p \leftrightarrow q$ evaluate to true (a tautology)
- **Too many row**, when there are more than a few variables, a truth table is impractical, e.g. when n=10, a table has $2^n = 2^{10} = 1024$ rows.

- **Use common logical equivalences** as a building block to prove/show/verify or to construct new logical equivalences.

This is just like how we solve equations in algebra using algebraic properties

Statements	Reasons
1. $6x - 3 = 4x + 1$	1. Given
2. $6x - 4x - 3 = 4x - 4x + 1$	2. Subtraction prop
3. $2x - 3 = 1$	3. Substitution
4. $2x - 3 + 3 = 1 + 3$	4. Addition prop.
5. $2x = 4$	5. Substitution
6. $2x/2 = 4/2$	6. Division prop.
7. $x = 2$	7. Substitution

Logically equivalence

- The equivalence we have verified using a truth table is known as, the **conditional disjunction** equivalence, $p \rightarrow q \equiv \neg p \vee q$

  In the same family, we have a **contraposition**, $p \rightarrow q \equiv \neg q \rightarrow \neg p$

- Another commonly used equivalence are the **De Morgan's Laws**

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

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

Try verifying these using truth tables

IDENTITY

Identity does not change the value of the operand

$a + 0 = a$
$a \times 1 = a$

INVERSE

Inverse changes the number to the identity

$a + (-a) = 0$
$a \times (1/a) = 1$

COMMUTATIVE

Changing the order of the operands

$a + b = b + a$
$a \times b = b \times a$

properties in mathematics

ASSOCIATIVE

Changing the group of the operands

$a + (b + c) = (a + b) + c$
$a \times (b \times c) = (a \times b) \times c$

DISTRIBUTIVE

This involves two operators, e.g. combining addition & multiplication

$a \times (b + c) = (a \times b) + (a \times c)$

Common logically equivalent statements

Identity	$p \wedge T \equiv p$	$p \vee F \equiv p$
Domination	$p \wedge F \equiv F$	$p \vee T \equiv T$
Idempotent	$p \wedge p \equiv p$	$p \vee p \equiv p$
Negation	$p \wedge \neg p \equiv F$	$p \vee \neg p \equiv T$
Double negation	$\neg(\neg p) \equiv p$	

IDENTITY

does not change the value of the operand

$a + 0 = a$

$a \times 1 = a$

INVERSE

changes the number to the identity

$a + (-a) = 0$

$a \times (1/a) = 1$

Commutation	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Association	$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	$p \vee (q \vee r) \equiv (p \vee q) \vee r$
Distribution	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Absorption	$p \wedge (p \vee q) \equiv p$	$p \vee (p \wedge q) \equiv p$
Exportation	$p \rightarrow (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$	

COMMUTATIVE

Changing the order of the operands

$a + b = b + a$

$a \times b = b \times a$

ASSOCIATIVE

Changing the group of the operands

$a + (b + c) = (a + b) + c$

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

DISTRIBUTIVE

This involves two operators, e.g. combining addition & multiplication

$a \times (b + c) = (a \times b) + (a \times c)$

WORKED EXAMPLES

Use series of logical equivalences to show that $\neg(p \rightarrow q) \equiv p \land \neg q$

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

$$\equiv$$

PRACTICE PROBLEMS

Use series of logical equivalences to show that $\neg(p \lor (\neg p \land q)) \equiv \neg p \land \neg q$

we prove this earlier
by using a truth table

$$\neg(p \lor (\neg p \land q))$$

$$\equiv$$

PRACTICE PROBLEMS

Use series of logical equivalences to derive the exportation equivalence:

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

You are not allowed to use the "exportation" rule in your proof.

PRACTICE PROBLEMS

Determine whether or not the given pair of statements is logically equivalent.

- $\neg(\neg p \to q)$ and $p \to \neg q$
- $\neg((p \lor \neg q) \land r)$ and $(\neg p \land q) \lor \neg r$
- $\neg(p \land \neg q) \land \neg(p \lor q)$ and $p \land (p \land q)$

RULE OF INFERENCE

Valid Arguments in Propositional Logic

Propositional Logic and Proofs

An argument is a sequence of statements that ends with a conclusion

An **argument is valid** when the **implication is a tautology**

q logically follows from p_i's

$$\underbrace{(p_1 \land p_2 \land \cdots \land p_n)}_{\text{premises}} \rightarrow \underbrace{q}_{\text{conclusion}}$$

premise 1
premise 2
⋮
premise n

∴ conclusion

Equivalence vs validity

$P \equiv Q$ iff $P \leftrightarrow Q$ is a tautology

P & Q have the same truth values

$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$ is a tautology

p q	p→q	¬p∨q	(p→q) ↔ (¬p∨q)
T T	T	T	T
T F	F	F	T
F T	T	T	T
F F	T	T	T

Construct a truth table

$\neg(p \rightarrow q)$

$\equiv \neg(\neg p \vee q)$ *Cond. disjunction*

$\equiv \neg(\neg p) \wedge \neg q$ *De Morgan's law*

$\equiv p \wedge \neg q$ *Double negation*

By deduction – applying equivalence properties

Proof of equivalence/ validity

- Construct a truth table (implication is all true)
- Use a short truth table
- By deduction (apply equivalence properties and/or rules of inference)

Give counterexample – assign truth values so P evaluates to true and Q false or vice versa (they disagree)

Proof non-equivalence/ invalidity

Give counterexample – assign truth values that make an argument false (all premises true, conclusion false)

Is the given argument valid? "implication is a tautology"

$p \wedge q$

$\neg q \rightarrow r$

$\therefore r$

Answer with the least amount of work (fill in as few cells as you can)!!!

p	q	r	p∧q	¬q→r	(p∧q) ∧ (¬q→r)	r	implication
T	T	T					
T	T	F					
T	F	T					
T	F	F					
F	T	T					
F	T	F					
F	F	T					
F	F	F					

PRACTICE PROBLEMS

$p \lor (q \lor r)$
$\neg r$
$\therefore p \lor q$

Answer with the least amount of work (fill in as few cells as you can)!!!

Is the argument valid or invalid? Prove it.

p	q	r	p∨(q∨r)	¬r	(p∨(q∨r)) ∧ (¬r)	p∨q	implication
T	T	T					
T	T	F					
T	F	T					
T	F	F					
F	T	T					
F	T	F					
F	F	T					
F	F	F					

Short truth table method for validity

- In a full truth table, an argument is invalid when we find one or more rows where all premises are true and the conclusion is false
- In a **short truth table** method, we attempt to find this **"invalid" row** without constructing the entire table
- **HOW**: assume such a row exists where *all premises true and conclusion false*
  - Make every premise true (assign it a T) and the conclusion false (assign it an F)
  - Work logically, assigning one variable after another, see if you can build this row:
    - If so, we **find a truth assignment** that make the argument false. It is **INVALID**.
    - If not (we **arrive at a contradiction**), then we conclude that it is not possible to make the argument false. That is, the argument is always true. It is **VALID**.

Is the given argument valid?

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

p q r	p ∧ q	¬ q → r	r

Is the given argument valid?

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

p q r	p ∨ (q ∨ r)	¬ r	p ∨ q

Try verifying this using a truth table (fill in as few cells as you can).

PRACTICE PROBLEMS

$$\begin{array}{l} p \to q \\ r \to F \\ \hline \therefore (p \wedge r) \to (q \vee F) \end{array}$$

Is the argument valid or invalid? Prove it.

PRACTICE PROBLEMS

$$\begin{array}{l} p \to (q \vee \neg r) \\ q \to (p \wedge r) \\ \hline \therefore p \to r \end{array}$$

Is the argument valid or invalid? Prove it.

Methods of proof for validity of arguments

- **Use a truth table** to show that an argument form is valid – whenever the premises are true, the conclusion must also be true ($\rightarrow$ is a tautology)
- **Use a short truth table**, a kind of indirect proof, **a proof by contradiction** – assume the argument is false then solve it to find possible truth assignments.
- Next, we establish validity of simple arguments, called **rules of inference**. Then, use them as building blocks to prove or to build other arguments.
- Validity of rules of inference depends only on **the form of the statements** involved and not on the truth values of the variables they contain.

Again, this is just like how we solve algebraic equations.

Rules of Inference – known valid argument forms

MODUS PONENS

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

MODUS TOLLENS

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

HYPOTHETICAL SYLLOGISM

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

DISJUNCTIVE SYLLOGISM

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

RESOLUTION

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

CONJUNCTION

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

SIMPLIFICATION

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

ADDITION

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

Prove by deduction that the argument is VALID

$$
\begin{array}{l}
(p \lor q) \rightarrow s \\
q \land r \\
\neg p \\
\hline
\therefore r \land s
\end{array}
$$

Step	Reason
1	premise
2	simplification (1)
3	simplification (1)
4	premise
5	premise
6	disjunctive syllogism (4,5)
7	modus ponens (2,6)
8	conjunction

Since the conclusion $r \land s$ is logically followed from the premises $(p \lor q) \rightarrow s$, $q \land r$, $\neg p$, therefore the argument is valid.

Prove by deduction that the argument is VALID

- p := You send me an email
- q := I finish my program
- r := I go to sleep early
- s := I wake up refreshed

Premises: $p \rightarrow q$, $\neg p \rightarrow r$, $r \rightarrow s$

Conclusion: $q \lor s$

From the proof, it is valid

	Step	Reason
1	$p \rightarrow q$	
2	$\neg q \rightarrow \neg p$	
3	$\neg p \rightarrow r$	
4	$\neg q \rightarrow r$	
5	$r \rightarrow s$	
6	$\neg q \rightarrow s$	
7	$q \lor s$	

Reasons can be common logical equivalences or rules of inference

PRACTICE PROBLEMS

$p \leftrightarrow q$

$\neg q$

$\therefore \neg p \vee r$

Hint: use an addition

Prove by deduction that the argument is VALID

	Step	Reason
1	$p \leftrightarrow q$	premise
2	$(p \rightarrow q) \wedge (q \rightarrow p)$	bicondition equivalence (1)
3		
4		
5		
6		

Since the conclusion $\neg p \vee r$ is logically followed from the premises $p \leftrightarrow q$, $\neg q$, therefore the argument is valid.

PRACTICE PROBLEMS

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

$r \rightarrow p$

$\therefore q \vee \neg r$

Hint: this is a resolution

Prove by deduction that the argument is VALID

	Step	Reason
1		
2		
3		
4		
5		
6		

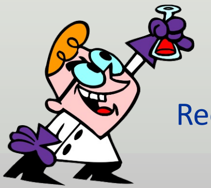
Since the conclusion $q \vee \neg r$ is logically followed from the premises $\neg(p \wedge \neg q)$, $r \rightarrow p$, therefore the argument is valid.

PRACTICE PROBLEMS

Show that the following argument is invalid.

Premises: $(q \vee r) \rightarrow p$, $\neg q$, p

Conclusion: r



Recall: to prove invalidity, find a truth assignment (give each variable a truth value) that makes an argument false, i.e. all premises true and the conclusion false

PRACTICE PROBLEMS

Determine if the following statements are valid or invalid. Detail a proof of validity or give a truth-assignment that makes the argument false (invalid).

- $(p \rightarrow q) \wedge (q \rightarrow r), (\neg q) \wedge r \;\therefore p$
- $\neg(p \rightarrow q), p \;\therefore \neg q$
- $(p \vee q), \neg(q \wedge \neg\neg r) \;\therefore \neg(r \vee p)$
- $(p \vee q), (\neg p \vee r), \neg(q \wedge s) \;\therefore \neg(\neg r \wedge s)$
- $(q \wedge r) \leftrightarrow (p \vee r), (q \rightarrow \neg p) \;\therefore (r \rightarrow \neg p)$