CS220: Applied Discrete Mathematics

Summer 2022

Instructor: Bang Tran

UMass Boston

1

About this course

- Textbook

  Discrete Mathematics and Its Applications, by Kenneth H. Rosen, WCB/McGraw-Hill, 2019 (8th Edition).

- Course webpage:
  https://cs.umb.edu/~bangtqh/teaching/cs220_summer22/

- Gradescope: For homework & exam submissions!
  https://www.gradescope.com/courses/367617

- Piazza: For discussing outside of the class

UMass Boston

2

Course staff

- Instructor: Bang Tran (Ben/Benzie/Bang)
  Email: bang.tran001@umb.edu
  Office hours: 10:30 AM – 12:30 PM (Tuesday & Thursday) via Zoom

- Tutor: Kleopatra Gjini (Kleo)
  Email: Kleopatra.Gjini001@umb.edu
  Office hours: 1:30 PM – 2:30 PM (Wednesday) via BlackBoard

- SI: TBD
  Email: TBD
  Office hours: TBD

UMass Boston

3

Evaluations

- Attendances (20%)
  - Fill an online forms (must have attendance code)
  - Two sections mean two form (must choose the correct form)

- Homework (50%)
  - 7 assignments
  - The 8th homework for make-up grade
  - Submit to gradescope

- Exam (30%)
  - August 24, 2022 (Time: TBD)

$95 \leq P$	A
$90 \leq P < 95$	A–
$85 \leq P < 90$	B+
$75 \leq P < 85$	B
$70 \leq P < 75$	B–
$65 \leq P < 70$	C+
$55 \leq P < 65$	C
$50 \leq P < 55$	C–
$45 \leq P < 50$	D+
$40 \leq P < 45$	D
$35 \leq P < 40$	D–
$P < 35$	F

UMass Boston

4

Logic and Proofs

Chapter 1 in the textbook

5

Logic in computer science

- Crucial for mathematical reasoning
- Used for designing electronic circuitry
- Logic is a system based on propositions.
- A proposition is a statement that is either true or false (not both)
- Corresponds to 1 and 0 in digital circuits

6

Propositional Logic

- A *proposition* is a statement that is either true or false.

- Examples of propositions:
  - Two plus two is four.
  - Toronto is the capital of Canada.
  - There is an infinite number of primes.
- Not propositions:
  - What time is it?
  - Have a nice day!

- A proposition's *truth value* is a value indicating whether the proposition is *true* or *false*.

The Statement/Proposition Game

"Elephants are bigger than mice."

- Is this a statement ? Yes
- Is this a proposition ? Yes
- What is the truth value of the proposition ? true

520 < 111

- Is this a statement ? Yes
- Is this a proposition ? Yes
- What is the truth value of the proposition ? false

y < 210

- Is this a statement ? Yes
- Is this a proposition ? No
- What is the truth value of the proposition ?

Its truth value depends on the value of y, but this value is not specified. We call this type of statement a **propositional function** or **open sentence**.

The Statement/Proposition Game

"Today is January 23 and 99 < 5."

- Is this a statement ? Yes
- Is this a proposition ? Yes
- What is the truth value of the proposition ? false

"Please do not fall asleep."

- Is this a statement ? No
- Is this a proposition ? No
- What is the truth value of the proposition ? Doesn't exits

"If elephants were red, they could hide in cherry trees"

- Is this a statement ? Yes
- Is this a proposition ? Yes
- What is the truth value of the proposition ? Probably false

The Statement/Proposition Game

"x < y if and only if y > x."

- Is this a statement ? Yes
- Is this a proposition ? Yes
- What is the truth value of the proposition ? true

Combining Propositions

- As we have seen in the previous examples, one or more propositions can be combined to form a single compound proposition.
- We formalize this by denoting propositions with letters such as P, Q, R, S, and introducing several logical operators.

Logical Operators (Connectives)

- We will examine the following logical operators:
  - Negation (NOT) $\neg$
  - Conjunction (AND) $\wedge$
  - Disjunction (OR) $\vee$
  - Exclusive or (XOR) $\oplus$
  - Implication (if – then) $\rightarrow$
  - Biconditional (if and only if) $\leftrightarrow$
- Truth tables can be used to show how these operators can combine propositions to compound propositions.

Negation (NOT)

- Unary Operator, Symbol: ¬

P	¬P
true	false
false	true

Conjunction (AND)

- Binary Operator, Symbol: ∧

P	Q	P∧Q
true	true	true
true	false	false
false	true	false
false	false	false

Disjunction (OR)

- Binary Operator, Symbol: $\vee$

P	Q	P∨Q
true	true	true
true	false	true
false	true	true
false	false	false

Exclusive Or (XOR)

- Binary Operator, Symbol: $\oplus$

P	Q	P ⊕ Q
true	true	false
true	false	true
false	true	true
false	false	false

Implication (if - then)

- Binary Operator, Symbol: $\rightarrow$

P	Q	$P \rightarrow Q$
true	true	true
true	false	false
false	true	true
false	false	true

Biconditional (if and only if)

- Binary Operator, Symbol: $\leftrightarrow$

P	Q	$P \leftrightarrow Q$
true	true	true
true	false	false
false	true	false
false	false	true

Proposition exercises

- Given following statements:
  - P = I finish writing my computer program before the lunch
  - Q = I shall play tennis in the afternoon
  - R = The sun is shining
  - S = The humidity is low
- Translate these sentences into proposition logic:
  - If the sun is shining, I shall play tennis this afternoon.

    $R \rightarrow Q$
  - Finishing the writing of my computer program before lunch is necessary for my playing tennis this afternoon.

    $Q \rightarrow P$
  - Low humidity and sunshine are sufficient for me to play tennis this afternoon.

    $S \wedge R \rightarrow Q$

P is necessary for Q: $Q \rightarrow P$

P is sufficient for Q: $P \rightarrow Q$

Equivalence

- The two formulas P and Q are logically equivalent iff the truth conditions of P are the same as the the truth conditions of Q
- Notation: $p \equiv q$
- Example: $\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$

P	Q	¬(P∧Q)	(¬P)∨(¬Q)	¬(P∧Q) ↔ (¬P)∨(¬Q)
true	true	false	false	?
true	false	true	true	?
false	true	true	true	?
false	false	true	true	?

Equivalence

- Is $(P \wedge Q) \equiv \neg\, (P \vee Q)$?

- Answer: No

P	Q	(P∧Q)	¬(P∨Q)
true	true	true	false
true	false	false	true
false	true	false	true
false	false	false	true

Logical equivalances

- Identity laws
  - $p \wedge true \equiv p$
  - $p \vee false \equiv p$
- Domination laws
  - $p \wedge false \equiv false$
  - $p \vee true \equiv true$
- Idempotent laws
  - $p \wedge p \equiv p$
  - $p \vee p \equiv p$
- Commutative laws
  - $p \wedge q \equiv q \wedge p$
  - $p \vee q \equiv q \vee p$
- Double negation law
  - $\neg(\neg p) \equiv p$
- Associate 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
  - $p \vee (q \wedge r) \equiv (p \vee r) \wedge (p \vee r)$
  - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
- De Morgan's laws
  - $\neg(p \wedge q) \equiv \neg q \vee \neg p$
  - $\neg(p \vee q) \equiv \neg p \wedge \neg q$
- Absorption laws
  - $p \vee (p \wedge q) \equiv p$
  - $p \wedge (p \vee q) \equiv p$
- Negation laws
  - $p \vee \neg \mathrm{p} \equiv true$
  - $p \wedge \neg p \equiv false$

Tautologies and Contradictions

- A **tautology** is a statement that is always true.
- Examples:
  - $R \vee (\neg R)$
  - $\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$
- If $S \rightarrow T$ is a tautology, we write $S \Rightarrow T$.
- If $S \leftrightarrow T$ is a tautology, we write $S \Leftrightarrow T$.

Tautologies and Contradictions

- A **contradiction** is a statement that is always false.
- Examples:
  - $R \wedge (\neg R)$
  - $\neg(\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q))$
- The negation of any tautology is a contradiction, and
- The negation of any contradiction is a tautology.

Exercises

1. Show that $(P \vee \neg \mathrm{P})$ is a tautology
2. Show that $(P \wedge \neg P)$ is a contradiction
3. Show that $\neg(P \vee \neg Q) \Rightarrow \neg P$
4. Show that $\big(P \wedge (P \rightarrow Q)\big) \Rightarrow Q$
5. Determine whether $(P \oplus Q) \oplus P$ is a tautology, contradiction or neither
6. Determine whether $(P \oplus Q) \vee (P \oplus \neg Q)$ is a tautology, contradiction or neither

Mathematical Reasoning

- We need mathematical reasoning to
  - Determine whether a mathematical argument is correct or incorrect and
  - Construct mathematical arguments.

- Mathematical reasoning is not only important for conducting proofs and program verification, but also for artificial intelligence systems (drawing inferences).

Terminology

- An **axiom** is a basic assumption about mathematical structures that needs no proof.
- We can use a **proof** to demonstrate that a particular statement is true. A proof consists of a sequence of statements that form an argument.
- The steps that connect the statements in such a sequence are the **rules of inference**.
- Cases of incorrect reasoning are called **fallacies**.
- A **theorem** is a statement that can be shown to be true.

Terminology

- A **lemma** is a simple theorem used as an intermediate result in the proof of another theorem.
- A **corollary** is a proposition that follows directly from a theorem that has been proved.
- A **conjecture** is a statement whose truth value is unknown. Once it is proven, it becomes a theorem.
- **Rules of inference** provide the justification of the steps used in a proof.
- One important rule is called **modus ponens** or the **law of detachment**. It is based on the tautology $(p \wedge (p \rightarrow q)) \rightarrow q$. We write it in the following way:

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

Rules of Inference

- The general form of a rule of inference is:

$$\begin{array}{l} p_1 \\ p_2 \\ . \\ . \\ . \\ p_n \\ \hline \therefore q \end{array}$$

The rule states that if p_1 and p_2 and … and p_n are all true, then q is true as well.

These rules of inference can be used in any mathematical argument and do not require any proof.

Rules of Inference

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

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

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

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

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

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

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

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

Arguments

- Just like a rule of inference, an **argument** consists of one or more hypotheses and a conclusion.
- We say that an argument is **valid**, if whenever all its hypotheses are true, its conclusion is also true.
- However, if any hypothesis is false, even a valid argument can lead to an incorrect conclusion.

Arguments

- Example:

  "If 101 is divisible by 3, then 101^2 is divisible by 9. 101 is divisible by 3. Consequently, 101^2 is divisible by 9."

- Although the argument is valid, its conclusion is incorrect, because one of the hypotheses is false ("101 is divisible by 3.")
- Which rule was ued ?
  P = "101 is divisible by 3."
  Q = "101^2 is divisible by 9."

$$\begin{array}{l} P \\ P \rightarrow Q \\ \hline \therefore Q \end{array}$$

Modus ponens

- Unfortunately, one of the hypotheses (P) is false. Therefore, the conclusion Q is incorrect.
- If in the above argument we replace 101 with 102, we could correctly conclude that 102^2 is divisible by 9.

Arguments

- Another example:
  - "If it rains today, then we will not have a barbeque today. If we do not have a barbeque today, then we will have a barbeque tomorrow.
    Therefore, if it rains today, then we will have a barbeque tomorrow."
- This is a valid argument: If its hypotheses are true, then its conclusion is also true.
- Let us formalize the previous argument:
  - p: "It is raining today."
  - q: "We will not have a barbecue today."
  - r: "We will have a barbecue tomorrow."
- So the argument is of the following form:

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

Hypothetical syllogism

Arguments

- Another example:
  - Gary is either intelligent or a good actor.
  - If Gary is intelligent, then he can count from 1 to 10.
  - Gary can only count from 1 to 2.
  - Therefore, Gary is a good actor.
- Let us formalize the argument as:
  - I: "Gary is intelligent."
  - A: "Gary is a good actor."
  - C: "Gary can count from 1 to 10."

Step	Reason
1. $\neg C$	Hypothesis
2. $I \rightarrow C$	Hypothesis
3. $\neg I$	Modus Tollens using (1) and (2)
4. $A \vee I$	Hypothesis
5. A	Disjunctive Syllogism using (3) and (4)

- Conclusion: A ("Gary is a good actor.")

Arguments

- Yet another example:
  - If you listen to me, you will pass CS 220.
  - You passed CS 220.
  - Therefore, you have listened to me.
- Is this argument valid?
- No, it assumes $((p \to q) \land q) \to p$.
- This statement is not a tautology. It is false if p is false and q is true.

Predicate Calculus

Chapter 1.4 in the textbook

Universal Quantification

- Let P(x) be a propositional function.
- **Universally quantified sentence:**
  For all x in the universe of discourse P(x) is true.
- Using the universal quantifier $\forall$:
  $\forall$x P(x)   "for all x P(x)" or "for every x P(x)"
- (Note: $\forall$x P(x) is either true or false, so it is a proposition, not a propositional function.)

Universal Quantification

- Example:
  S(x): x is a UMB student.
  G(x): x is a genius.
- What does $\forall$x (S(x) $\rightarrow$ G(x)) mean ?

"If x is a UMB student, then x is a genius."
or
"All UMB students are geniuses."

Existential Quantification

- **Existentially quantified sentence:**
  There exists an x in the universe of discourse for which P(x) is true.

- Using the existential quantifier ∃:
  ∃x P(x) “There is an x such that P(x).”
  “There is at least one x such that P(x).”

- (Note: ∃x P(x) is either true or false, so it is a proposition, but no propositional function.)

Existential Quantification

- Example:
  P(x): x is a UMB professor.
  G(x): x is a genius.

- What does ∃x (P(x) ∧ G(x)) mean ?

“There is an x such that x is a UMB professor and x is a genius.”
or
“At least one UMB professor is a genius.”

Quantification

- Another example:
  Let the universe of discourse be the real numbers.
- What does $\forall x \exists y\ (x + y = 320)$ mean ?

“For every x there exists a y so that x + y = 320.”

Is it true? yes

Is it true for the natural numbers? no

Disproof by Counterexample

- A counterexample to $\forall x\ P(x)$ is an object c so that P(c) is false.
- Statements such as $\forall x\ (P(x) \rightarrow Q(x))$ can be disproved by simply providing a counterexample.

Statement: “All birds can fly.”
Disproved by counterexample: Penguin.

Negation

- $\neg(\forall x\ P(x))$ is logically equivalent to $\exists x\ (\neg P(x))$.
- $\neg(\exists x\ P(x))$ is logically equivalent to $\forall x\ (\neg P(x))$.

Quantification

- Introducing the **universal quantifier** $\forall$ and **the existential quantifier** $\exists$ facilitates the translation of world knowledge into predicate calculus.
- Examples:
  - Paul beats up all professors who fail him.
    $\forall x([\text{Professor}(x) \land \text{Fails}(x, \text{Paul})] \rightarrow \text{BeatsUp}(\text{Paul}, x))$
  - All computer scientists are either rich or crazy, but not both.
    $\forall x\ (\text{CS}(x) \rightarrow [\text{Rich}(x) \land \neg\text{Crazy}(x)] \lor [\neg\text{Rich}(x) \land \text{Crazy}(x)]\ )$
  - Or, using XOR:
    $\forall x\ (\text{CS}(x) \rightarrow [\text{Rich}(x) \oplus \text{Crazy}(x)])$

More Practice for Predicate Logic

- **Important points:**
  - Define propositional functions in a useful and reusable manner, just like functions in a computer program.
  - Make sure your formalized statement evaluates to "true" in the context of the original statement and evaluates to "false" whenever the original statement is violated.
- **More Examples:**
  - Jenny likes all movies that Peter likes (and possibly more).
    $\forall x$ [Movie(x) $\wedge$ Likes(Peter, x) $\rightarrow$ Likes(Jenny, x)]
  - There is exactly one UMass professor who won a Nobel prize
    $\exists x$[UMBProf(x) $\wedge$ Wins(x, NobelPrize)] $\wedge$
    $\neg\exists y,z$[y $\neq$ z $\wedge$ UMBProf(y) $\wedge$ UMBProf(z) $\wedge$
    Wins(y, NobelPrize) $\wedge$ Wins(z, NobelPrize)]

Rules of Inference for Quantified Statements

$\forall x$ P(x)
―――――
$\therefore$ P(c) if c $\in$ U

Universal instantiation

P(c) for an arbitrary c $\in$ U
―――――
$\therefore$ $\forall x$ P(x)

Universal generalization

$\exists x$ P(x)
―――――
$\therefore$ P(c) for some element c $\in$ U

Existential instantiation

P(c) for some element c $\in$ U
―――――
$\therefore$ $\exists x$ P(x)

Existential generalization

Rules of Inference for Quantified Statements

- Example:
  - Every UMB student is a genius.
  - George is a UMB student.
  - Therefore, George is a genius.
- The following steps are used in the argument:

U(x): "x is a UMB student."
G(x): "x is a genius."

Step	**Reason**
1. $\forall x\, U(x) \rightarrow G(x)$	Hypothesis
2. U(George) → G(George)	Universal instantiation using (1)
3. U(George)	Hypothesis
4. G(George)	Modus ponens using (2) and (3)

Proving Theorems

Direct proof:

- An implication p→q can be proved by showing that if p is true, then q is also true.
- Example: Give a direct proof of the theorem "If n is odd, then n^2 is odd."
- Idea: Assume that the hypothesis of this implication is true (n is odd). Then use rules of inference and known theorems to show that q must also be true (n^2 is odd).

Proving Theorems

n is odd.

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

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

Since n^2 can be written in the form of 2K + 1, it is odd.

Proving Theorems

Indirect proof:

- An implication $p \rightarrow q$ is equivalent to its contra-positive $\neg q \rightarrow \neg p$. Therefore, we can prove $p \rightarrow q$ by showing that whenever q is false, then p is also false.
- Example: Give an indirect proof of the theorem
  "If 3n + 2 is odd, then n is odd."
- Idea: Assume that the conclusion of this implication is false (n is even). Then use rules of inference and known theorems to show that p must also be false (3n + 2 is even).

Proving Theorems

n is even.

Then n = 2k, where k is an integer.

It follows that: 3n + 2 = 3(2k) + 2
= 6k + 2
= 2(3k + 1)

Therefore, 3n + 2 is even.

We have shown that the contrapositive of the implication is true, so the implication itself is also true (If 3n + 2 is odd, then n is odd).

Proving Theorems

Proof by cases

- A proof by cases must cover all possible cases that arise in a theorem.
- Example: For every positive integer n, n(n + 1) is even.
- Idea: Let us first show that the product of an even number m and an odd number n is always even:
  m = 2k
  n = 2p + 1
  mn = 2k (2p + 1) = 4kp + 2k
  mn = 2(2kp + k)
- Since k and p are integers, (2kp + k) is an integer as well, and we have shown that mn is even.

Proving by Cases

- The remainder of the proof becomes easy if we separately consider each of the two main situations that can occur:
- **Case I:** n is even.
  - Then n(n + 1) means that we multiply an even number with an odd one. As shown above, the result must be even.
- **Case II:** n is odd.
  - Then n(n + 1) means that we multiply an odd number with an even one. As shown above, the result must be even.

- Since there are no other cases, we have proven that n(n + 1) is always even.

Summary of Proofs (Theorem)

- Direct proof
- Indirect proof
- Prove by cases
- Proof by contradiction

- A direct proof of $p \rightarrow q$ is true by showing that if p is true, then q must also be true, so that the combination p true and q false never occurs.
  - ➢ First step: assuming that p is true
  - ➢ Second step: showing that q is also true