Week 14 - Friday

COMP 2230

Last time

- Context-free languages
- Pushdown automata
- Chomsky's hierarchy of grammars
- Halting Problem

Questions?

Assignment 6

Final exam

- **Final exam:**
  - **Wednesday, April 29, 2026**
  - **8:00 to 10:00 a.m.**
  - **50% longer than previous exams, but you'll have 100% more time**
- There will be short answer, diagrams, and proofs
- It will be comprehensive but weighted toward the last quarter of the course

Propositional Logic Review

Propositional logic

- Statements
- AND, OR, NOT, IMPLIES
- Truth tables
- Logical equivalence
- De Morgan's laws
- Tautologies and contradictions

Laws of Boolean algebra

Name	Law	Dual
Commutative	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associative	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identity	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
Negation	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
Double Negative	$\sim(\sim p) \equiv p$	
Idempotent	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universal Bound	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathrm{c}$
De Morgan's	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
Absorption	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negations of **t** and **c**	$\sim\mathbf{t} \equiv \mathbf{c}$	$\sim\mathbf{c} \equiv \mathbf{t}$

Implications

- Can be used to write an if-then statement
- Contrapositive is logically equivalent
- Inverse and converse are not (though they are logically equivalent to each other)
- Biconditional:
  - $p \rightarrow q \wedge q \rightarrow p$

Arguments

- A series of **premises** and a **conclusion**
- Using the premises and rules of inference, an argument is **valid** if and only if you can show the conclusion
- Rules of inference:
  - Modus Ponens
  - Modus Tollens
  - Generalization
  - Specialization
  - Conjunction
  - Elimination
  - Transitivity
  - Division into cases
  - Contradiction rule

Practice

- Show that the following is a valid argument

1. $\sim p \vee q \rightarrow r$
2. $s \vee \sim q$
3. $\sim t$
4. $p \rightarrow t$
5. $\sim p \wedge r \rightarrow \sim s$

$$\therefore \sim q$$

Practice

- Make a truth table for:
  - $\sim(q \rightarrow r) \vee (s \wedge p) \leftrightarrow (p \vee r)$

Predicate Logic Review

Predicates

- A **predicate** is a sentence with a fixed number of variables that becomes a **statement** when specific values are substituted for to the variables
- The **domain** gives all the possible values that can be substituted
- The **truth set** of a predicate $P(x)$ are those elements of the domain that make $P(x)$ true when they are substituted

Sets

- We will frequently be referring to various sets of numbers in this class
- Some typical notation used for these sets:

Symbol	Set	Examples
$\mathbb{R}$	Real numbers	Virtually everything
$\mathbb{Z}$	Integers	$\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{Z}^-$	Negative integers	$\{-1, -2, -3, \dots\}$
$\mathbb{Z}^+$	Positive integers	$\{1, 2, 3, \dots\}$
$\mathbb{N}$	Natural numbers	$\{1, 2, 3, \dots\}$
$\mathbb{Q}$	Rational numbers	a/b where $a, b \in \mathbb{Z}\ and\ b \neq 0$

- Some authors use $\mathbb{Z}^+$ to refer to non-negative integers and only $\mathbb{N}$ for the natural numbers

Quantifiers

- The universal quantifier ∀ means "for all"
- The statement "All DJ's are mad ill" can be written more formally as:
- $\forall x \in D, M(x)$
  - Where D is the set of DJ's and $M(x)$ denotes that x is mad ill
- The existential quantifier ∃ means "there exists"
- The statement "Some emcee can bust a rhyme" can be written more formally as:
- $\exists y \in E, B(y)$
  - Where E is the set of emcees and $B(y)$ denotes that y can bust a rhyme

Negating quantified statements

- When doing a negation, negate the predicate and change the universal quantifier to existential or vice versa
- Formally:
  - $\sim\big(\forall x, P(x)\big) \equiv \exists x, \sim P(x)$
  - $\sim\big(\exists x, P(x)\big) \equiv \forall x, \sim P(x)$
- Thus, the negation of "Every dragon breathes fire" is "There is one dragon that does not breathe fire"

Vacuously true

- Any statement with a universal quantifier whose domain is the empty set is **vacuously true**
- When we talk about "all things" and there's nothing there, we can say anything we want
- "All mythological creatures are real."
- Every single one of the (of which there are none) is real

Conditionals

- Recall:
  - Statement: $p \to q$
  - Contrapositive: $\sim q \to \sim p$
  - Converse: $q \to p$
  - Inverse: $\sim p \to \sim q$
- These can be extended to universal statements:
  - Statement: $\forall x, P(x) \to Q(x)$
  - Contrapositive: $\forall$ x, ~$Q(x) \to$ ~$P(x)$
  - Converse: $\forall$ x, $Q(x) \to P(x)$
  - Inverse: $\forall$ x, ~$P(x) \to$ ~$Q(x)$
- Similar properties relating a statement equating a statement to its contrapositive (but not to its converse and inverse) apply

Necessary and sufficient

- p is a **sufficient condition** for q means $p \to q$
- p is a **necessary condition** for q means $q \to p$

- These come over into universal conditional statements as well:
- $\forall x, P(x)$ is a **sufficient condition** for $Q(x)$ means $\forall x, P(x) \to Q(x)$
- $\forall x, P(x)$ is a **necessary condition** for $Q(x)$ means $\forall x, Q(x) \to P(x)$

Multiple quantifiers

- With multiple quantifiers, we imagine that corresponding "actions" happen in the same order as the quantifiers
- The action for $\forall x \in A$ is something like, "pick any x from A you want"
- Since a "for all" must work on everything, it doesn't matter which you pick
- The action for $\exists y \in B$ is something like, "find some y from B"
- Since a "there exists" only needs one to work, you should try to find the one that matches

Negating or changing multiple quantifiers

- For negation,
  - Simply switch every ∀ to ∃ and every ∃ to ∀
  - Then negate the predicate
- Changing the order of quantifiers can change the truth of the whole statement but does not always
- Furthermore, quantifiers of the same type are commutative:
  - You can reorder a sequence of ∀ quantifiers however you want
  - The same goes for ∃
  - Once they start overlapping, however, you can't be sure anymore

Practice

- Use a statement of predicate logic to write the following statement:
  - "There is a person who can take every sad song and make it better"
  - Now negate the statement and read back the equivalent informal version

- Rewrite the following without negations outside the predicates:
  - $\sim (\forall x \in D, \forall y \in E, P(x, y)))$

Quantification in arguments

- **Universal instantiation:** If a property is true for everything in a domain (universal quantifier), it is true for any specific thing in the domain
- **Universal modus ponens:**
  - $\forall x, P(x) \rightarrow Q(x)$
  - $P(a)$ for some particular a
  - $\therefore Q(a)$
- **Universal modus tollens:**
  - $\forall x, P(x) \rightarrow Q(x)$
  - $\sim Q(a)$ for some particular a
  - $\therefore \sim P(a)$

Proofs Review

Proving existential statements and disproving universal ones

- To prove $\exists x \in D, P(x)$ we need to find at least one element of D that makes $P(x)$ true

- To disprove $\forall x \in D, P(x) \rightarrow Q(x)$, we need to find an x that makes $P(x)$ true and $Q(x)$ false

Proving universal statements

- If the domain is finite, we can use the **method of exhaustion**, by simply trying every element
- Otherwise, we can use a **direct proof**
  1. Express the statement to be proved in the form $\forall x \in D$, if $P(x)$ then $Q(x)$
  2. Suppose that x is some specific (but arbitrarily chosen) element of D for which $P(x)$ is true
  3. Show that the conclusion $Q(x)$ is true by using definitions, other theorems, and the rules for logical inference
- Direct proofs should start with the word **Proof**, end with a box or the word **QED**, and have a justification for every step in the argument
- For proofs with cases, number each case clearly and show that you have proved the conclusion for all possible cases

Definitions

- If n is an integer, then:
  - n is even $\leftrightarrow \exists\, k \in \mathbb{Z},\ n = 2k$
  - n is odd $\leftrightarrow \exists k \in \mathbb{Z},\ n = 2k + 1$
- If n is an integer where $n > 1$, then:
  - n is prime $\leftrightarrow \forall\, r \in \mathbb{Z}^+, \forall\, s \in \mathbb{Z}^+$, if $n = r \cdot s$, then $r = 1$ or $s = 1$
  - n is composite $\leftrightarrow \exists\, r \in \mathbb{Z}^+, \exists\, s \in \mathbb{Z}^+, n = r \cdot s$ and $r \neq 1$ and $s \neq 1$
- r is rational $\leftrightarrow \exists\, a, b \in \mathbb{Z},\ r = a/b$ and $b \neq 0$
- For $n, d \in \mathbb{Z}$,
  - n is divisible by $d \leftrightarrow \exists k \in \mathbb{Z},\ n = dk$
- For any real number x, the floor of x, written $\lfloor x \rfloor$, is defined as follows:
  - $\lfloor x \rfloor =$ the unique integer n such that $n \leq x < n + 1$
- For any real number x, the ceiling of x, written $\lceil x \rceil$, is defined as follows:
  - $\lceil x \rceil =$ the unique integer n such that $n - 1 < x \leq n$

Theorems

- **Unique factorization theorem:** For any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}$$

- **Quotient remainder theorem:** For any integer n and any positive integer d, there exist unique integers q and r such that
  - $n = dq + r$ and $0 \leq r < d$

Practice

- Prove or disprove the following statements:
  - For all integers a, b, and c, if $a \mid b$ and $a \mid c$ then $a \mid (2b - 3c)$
  - For all integers a, b, and c, if $a \mid (b + c)$ then $a \mid b$ or $a \mid c$

- Use the quotient-remainder theorem with $d = 3$ to prove that the square of any integer has the form $3k$ or $3k + 1$ for some integer k

Indirect Proofs

Proof by contradiction

- In a proof by contradiction, you begin by assuming the negation of the conclusion
- Then, you show that doing so leads to a logical impossibility
- Thus, the assumption must be false and the conclusion true

Contradiction formatting

- A proof by contradiction is different from a direct proof because you are **trying** to get to a point where things don't make sense
- You should always mark such proofs clearly
- Start your proof with the words **Proof by contradiction**
- Write **Negation of conclusion** as the justification for the negated conclusion
- Clearly mark the line when you have both p and $\sim p$ as a **contradiction**
- Finally, state the conclusion with its justification as the contradiction found before

Practice

- Use a proof by contradiction to prove the following:
  - For all prime numbers a, b, and c, $a^2 + b^2 \neq c^2$

Sequences and Induction

Sequences

- Mathematical sequences can be represented in **expanded form** or with **explicit formulas**
- Examples:
  - $2, 5, 10, 17, 26, \ldots$
  - $a_i = i^2 + 1, i \geq 1$
- **Summation notation** is used to describe a summation of some part of a series

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + a_{m+2} + \ldots + a_n$$

- **Product notation** is used to describe a product of some part of a series

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot a_{m+2} \cdot \ldots \cdot a_n$$

Proof by mathematical induction

- To prove a statement of the following form:
  - $\forall n \in \mathbb{Z}$, where $n \geq a$, property $P(n)$ is true
- Use the following steps:
  1. Basis Step: Show that the property is true for $P(a)$
  2. Induction Step:
     - Suppose that the property is true for some $n = k$, where $k \in \mathbb{Z}, k \geq a$
     - Now, show that, with that assumption, the property is also true for $k + 1$

Practice

- Write the following in closed form:
  - $1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots \frac{1}{2^n}$

- Use mathematical induction to prove:
  - For all integers $n \geq 1, \ 2 + 4 + 6 + \cdots + 2n = n^2 + n$

Recursion

- Using recursive definitions to generate sequences
- Writing a recursive definition based on a sequence
- Using mathematical induction to show that a recursive definition and an explicit definition are equivalent

Solving recursion by iteration

- Expand the recursion repeatedly without combining like terms
- Find a pattern in the expansions
- When appropriate, employ formulas to simplify the pattern
  - Geometric series: $1 + r + r^2 + \ldots + r^n = \frac{r^{n+1}-1}{r-1}$
  - Arithmetic series: $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$

Practice

- Use the method of iteration to find an explicit formula for the following recursively defined sequence:
  - $d_k = 2d_{k-1} + 3$, for all integers $k \geq 2$
  - $d_1 = 2$
- Use a proof by induction to show that your explicit formula is correct

Solving second order linear homogeneoous recurrence relations with constant coefficients

- To solve sequence $a_k = Aa_{k-1} + Ba_{k-2}$
- Find its characteristic equation $t^2 - At - B = 0$
- If the equation has two distinct roots r and s
  - Substitute a_0 and a_1 into $a_n = Cr^n + Ds^n$ to find C and D
- If the equation has a single root r
  - Substitute a_0 and a_1 into $a_n = Cr^n + Dnr^n$ to find C and D

Practice

- Find an explicit formula for the following:
  - $r_k = 2r_{k-1} - r_{k-2}$, for all integers $k \geq 2$
  - $r_0 = 1$
  - $r_1 = 4$

Upcoming

Next time…

- Review of second third of the course

Reminders

- Keep working on Assignment 6
  - Due next Wednesday