THE UNIVERSITY OF NEWCASTLE AUSTRALIA
FACULTY OF ENGINEERING AND BUILT ENVIRONMENT
www.newcastle.edu.au

Theory of Computation
Week 1

Much of the material on this slides comes from the recommended textbook by Elaine Rich

Detailed content

Weekly program

- **Week 1 – Background knowledge revision: logic, sets, proof techniques**

- Week 2 – Languages and strings. Hierarchies. Computation. Closure properties
- Week 3 – Finite State Machines: non-determinism vs. determinism
- Week 4 – Regular languages: expressions and grammars
- Week 5 – Non regular languages: pumping lemma. Closure
- Week 6 – Context-free languages: grammars and parse trees
- Week 7 – Pushdown automata
- Week 8 – Non context-free languages: pumping lemma and decidability. Closure
- Week 9 – Decidable languages: Turing Machines
- Week 10 – Church-Turing thesis and the unsolvability of the Halting Problem
- Week 11 – Decidable, semi-decidable and undecidable languages (and proofs)
- Week 12 – Revision of the hierarchy
- Week 13 – Extra revision (if needed)

Week 01 Lecture Outline

Logic, Sets Theory, Proof Techniques

- ❑ Boolean Logic WFFs
- ❑ Properties of Boolean Operators
- ❑ Terminologies: Axiom, Theorem, Proof
- ❑ Inference Rules
- ❑ First Order Logic
- ❑ Set Theory, Function and Relation
  - ➢ Watch Video + Supplementary Slides
- ❑ Closure
- ❑ Proof Techniques

Boolean Logic WFFs

A ***well-formed formula (wff)*** is any string that is formed according to the following rules:

- *True* and *False* are wff
- A **propositional symbol** (or variable) is a wff.
- If P is a wff, then $\neg P$ is a wff.
- If P and Q are wffs, then so are:

  $P \vee Q$, $P \wedge Q$, $P \to Q$, and $P \leftrightarrow Q$.

- If P is a wff, then (P) is a wff.

Truth Tables Define Operators

P	Q	$\neg P$	$P \vee Q$	$P \wedge Q$	$P \rightarrow Q$	$P \leftrightarrow Q$
True	*True*	*False*	*True*	*True*	*True*	*True*
True	*False*	*False*	*True*	*False*	*False*	*False*
False	*True*	*True*	*True*	*False*	*True*	*False*
False	*False*	*True*	*False*	*False*	*True*	*True*

Example: WFF

$(p \rightarrow (q \wedge r)) \rightarrow (s \vee ((\neg q) \wedge (\neg s)))$
$(((A \,\&\, B) \rightarrow (C \vee D)) \rightarrow (E \leftrightarrow F))$

Example: non-WFF

$(p \rightarrow \rightarrow (s \vee q))$
$(A\neg B)$

When WFFs are True

- A Boolean wff is ***valid*** or is a ***tautology*** iff it is true for all assignments of truth values to the variables it contains.

- A Boolean wff is ***satisfiable*** iff it is true for at least one assignment of truth values to the variables it contains.

- A Boolean wff is ***unsatisfiable*** or is ***contradiction*** iff it is false for all assignments of truth values to the variables it contains.

- Two wffs P and Q are ***equivalent***, written $P \equiv Q$, iff they have the same truth values regardless of the truth values of the variables they contain.

Using Truth Tables

$P \vee \neg P$ is a tautology:

P	$\neg P$	$P \vee \neg P$
True	*False*	*True*
False	*True*	*True*

Using Truth Tables

Is $P \land \neg P$ satisfiable?

Using Truth Tables

Is $P \wedge \neg P$ satisfiable?

What about $(P \wedge \neg Q) \vee (S \wedge \neg Q)$?

Properties of Boolean Operators

- $\lor$, $\land$ and $\leftrightarrow$ are commutative and associative.

- $\lor$ and $\land$ are idempotent:

  (e.g., $(P \lor P) \equiv P$).

- $\lor$ and $\land$ distribute over each other:
  - $P \land (Q \lor R) \equiv (P \land Q) \lor (P \land R)$.
  - $P \lor (Q \land R) \equiv (P \lor Q) \land (P \lor R)$.

- $\leftrightarrow$ is not distributive

More Properties

- ***Absorption laws***:
  - $P \wedge (P \vee Q) \equiv P$.
  - $P \vee (P \wedge Q) \equiv P$.

- ***Double negation***: $\neg\neg P \equiv P$.

- ***de Morgan's Laws***:
  - $\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$.
  - $\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$.

Entailment

A set *A* of wffs ***logically implies*** or ***entails*** a conclusion *Q* iff, whenever all of the wffs in *A* are true, *Q* is also true.

Example:

$\{A, B, C\}$	entail	$A \wedge B \wedge C$
$\{A\}$	entail	$A \vee B \vee C$

Axiom, Theorem and Proof

- An ***axiom*** is a wff that is asserted *a priori* to be true.

- Given a set of axioms, rules of inference can be applied to create new wffs, to which the inference rules can then be applied, and so forth. Any statement so derived is called a ***theorem***.

- Let A be a set of axioms plus zero or more theorems that have already been derived from those axioms. Then a ***proof*** is a finite sequence of applications of inference rules, starting from A.

Inference Rules

- An inference rule is ***sound*** iff, whenever it is applied to a set A of axioms, any conclusion that it produces is entailed by A. An entire proof is sound iff it consists of a sequence of inference steps each of which was constructed using a sound inference rule.

- A set of inference rules R is ***complete*** iff, given any set A of axioms, all statements that are entailed by A can be proved by applying the rules in R.

Some Sound Inference Rules

• ***Modus ponens***:	From	$(P \rightarrow Q)$ and P
	Conclude	Q
• ***Modus tollens***:	From	$(P \rightarrow Q)$ and $\neg Q$
	Conclude	$\neg P$
• ***Or introduction***:	From	P
	Conclude	$(P \vee Q)$
• ***And introduction***:	From	P and Q
	Conclude	$(P \wedge Q)$
• ***And elimination***:	From	$(P \wedge Q)$
	Conclude	P or Conclude Q

First-Order Logic

An expression that describes an object is a ***term***.

- A variable is a term
- An n-ary function is a term where each of its arguments are also a term

First-Order Logic wff

A ***well-formed formula (wff)*** in first-order logic is an expression that can be formed by:

- If P is an n-ary predicate and each of the expressions x_1, x_2, … , x_n is a term, then an expression of the form $P(x_1, x_2, \dots, x_n)$ is a wff. If any variable occurs in such a wff, then that variable is ***free***.
- If P is a wff, then $\neg P$ is a wff.
- If P and Q are wffs, then so are $P \vee Q$, $P \wedge Q$, $P \rightarrow Q$, and $P \leftrightarrow Q$.
- If P is a wff, then (P) is a wff.
- If P is a wff, then $\forall x\ (P)$ and $\exists x\ (P)$ are wffs. Any free instance of x in P is ***bound*** by the quantifier and is then no longer free.

Sentences

A wff with no free variables is called a ***sentence*** or a ***statement***.

1. $Bear(Smoky)$.
2. $\forall x\ (Bear(x) \rightarrow Animal(x))$.
3. $\forall x\ (Animal(x) \rightarrow Bear(x))$.
4. $\forall x\ (Animal(x) \rightarrow \exists y\ (Mother\text{-}of(y, x)))$.
5. $\forall x\ ((Animal(x) \wedge \neg Dead(x)) \rightarrow Alive(x))$.

A ***ground instance*** is a sentence that contains no variables.

Truth

1. $Bear(Smoky)$.
2. $\forall x\ (Bear(x) \rightarrow Animal(x))$.
3. $\forall x\ (Animal(x) \rightarrow Bear(x))$.
4. $\forall x\ (Animal(x) \rightarrow \exists y\ (Mother\text{-}of(y, x)))$.
5. $\forall x\ ((Animal(x) \land \neg Dead(x)) \rightarrow Alive(x))$.

Which of these are true in the everyday world?

Interpretations and Models

- An ***interpretation*** for a sentence w is a pair (D, I), where D is a universe of objects. I assigns meaning to the symbols of w: it assigns values, drawn from D, to the constants in w and it assigns functions and predicates (whose domains and ranges are subsets of D) to the function and predicate symbols of w.

- A ***model*** of a sentence w is an interpretation that makes w true. For example, let w be the sentence:

  $$\forall x\ (\exists y\ (y < x)).$$

- A sentence w is ***valid*** iff it is true in all interpretations.

- A sentence w is ***satisfiable*** iff there exists *some* interpretation in which w is true.

- A sentence w is ***unsatisfiable*** iff $\neg w$ is valid.

Examples

- $\forall x\ ((P(x) \land Q(Smoky)) \rightarrow P(x))$.

- $\neg(\forall x\ (P(x) \lor \neg(P(x)))$.

- $\forall x\ (P(x, x))$.

Additional Sound Inference Rules

- ***Quantifier exchange***:
  - From $\neg\exists x\ (P)$, conclude $\forall x\ (\neg P)$.
  - From $\forall x\ (\neg P)$, conclude $\neg\exists x\ (P)$.
  - From $\neg\forall x\ (P)$, conclude $\exists x\ (\neg P)$.
  - From $\exists x\ (\neg P)$, conclude $\neg\forall x\ (P)$.

- ***Universal instantiation***: For any constant C, from $\forall x\ (P(x))$, conclude $P(C)$.

- ***Existential generalization***: For any constant C, from $P(C)$ conclude $\exists x\ (P(x))$.

A Simple Proof

Assume the following three axioms:

[1] $\forall x\, (P(x) \wedge Q(x) \rightarrow R(x))$.
[2] $P(X_1)$.
[3] $Q(X_1)$.

We prove $R(X_1)$ as follows:

[4] $P(X_1) \wedge Q(X_1) \rightarrow R(X_1)$. (Universal instantiation, [1].)
[5] $P(X_1) \wedge Q(X_1)$. (And introduction, [2], [3].)
[6] $R(X_1)$. (Modus ponens, [5], [4].)

Sets: What you need to know

- ❑ Definitions: ***set, set elements*** / ***members, subset, empty set, infinite set***
- ❑ *How can we define a set:* ***Enumeration*** *and* ***Characteristic function***
- ❑ ***Set Cardinality***
- ❑ Set operations: **union, intersection, difference, complement**
- ❑ How can you prove that two sets are equal?
- ❑ Venn diagrams for relating sets to each other
- ❑ **Power set** and **set partition**

Check Supplementary slides and Week 1 videos

Relations: What you need to know

- Definitions: **Ordered pair, *Cartesian product, relation***
- *Types:* ***Binary relation, n-ary relations***
- *Properties:* ***reflexive, symmetric, transitive, equivalence relation***
- ***Equivalence classes***

Check Supplementary slides and Week 1 videos

Function: What you need to know

- ❑ Understand the difference between function and relation
- ❑ Definitions: **function**
- ❑ *Types:* ***Unary function, Binary function, n-ary function***
- ❑ *Properties:* ***total function, partial function, one-to-one, onto***
- ❑ *Properties of functions on sets: Commutativity, Associativity, Idempotency, Distributivity, Absorption, Identity, Zero, Self Inverse, De Morgan's Law*

Check Supplementary slides and Week 1 videos

Set Cardinality

- How many elements does *S* contain?

- If $S=\{2,7,11\}$ then $|S| = |\{2,7,11\}| = 3$.

- We can have three different kinds of answers
  - If S is finite then a natural number
  - If S has the same number of elements as there are integers then it is ‘countably infinite’
  - If S has more elements than there are integers then ‘uncountably infinite’ or ‘uncountable’

Set Cardinality

- The Infinite Hotel Paradox - Jeff Dekofsky

https://www.youtube.com/watch?v=Uj3_KqkI9Zo

Properties of Relations

$R \subseteq A \times A$ is ***reflexive*** iff, $\forall x \in A\ ((x, x) \in R)$.

Examples:

- $\leq$ defined on the integers. For every integer x, $x \leq x$.

$R \subseteq A \times A$ is ***symmetric*** iff $\forall x, y\ ((x, y) \in R \rightarrow (y, x) \in R)$.

Examples:
- = defined on the integers is symmetric but $\leq$ is not.

$R \subseteq A \times A$ is ***transitive*** iff:

$$\forall x, y, z\ (((x, y) \in R \wedge (y, z) \in R) \rightarrow (x, z) \in R).$$

Examples:
- $<$ defined on the integers is transitive

Closure

- A binary relation *R* on a set *A* is ***closed under*** property *P* if and only if *R* ***possesses*** *P*.

  Examples

  $<$ on the integers, *P* = transitivity

  $\leq$ on the integers, *P* = reflexive

- The ***closure*** of *R* under *P* is a smallest set that includes *R* and that is closed under *P*.

Closure

- Let R = {(1, 2), (2, 3), (3, 4)} defined on a set A={1,2,3,4}.

- The reflexive closure of R is:

- The transitive closure of R is:

Closure

- Let R = {(1, 2), (2, 3), (3, 4)} defined on a set A={1,2,3,4}.

- The reflexive closure of R is:

  {(1, 2), (2, 3), (3, 4), (1, 1), (2, 2), (3, 3), (4, 4)}

- The transitive closure of R is:

  {(1, 2), (2, 3), (3, 4), (1, 3), (1, 4), (2, 4)}

Proof Techniques

- Proof by construction
- Proof by contradiction
- Proof by counterexample
- Proof by case enumeration
- Mathematical induction
- The pigeonhole principle
- Proving cardinality
- Diagonalization

Proof Technique: Construction

- Suppose we want to prove $\exists x\ (Q(x))$ *or* $\forall x\ (\exists y\ (P(x, y)))$
- Show that an algorithm that finds the value that we claim must exists
- For example: we want to prove that every pair of integers has a greatest common divisor

Proof Technique: Contradiction

Assume that the opposite is true and reach a contradiction

- ***Example:*** To prove that $\sqrt{2}$ is an irrational number we assume that it is rational.
- $\sqrt{2}$ = *i*/*j*. [So - it is the quotient of two integers, *i* and *j*.]
- $\sqrt{2}$ = *k*/*n*, [reduce by common factor, where *k* and *n* have no common factors]
- Thus, $2 = k^2/n^2$ and so $2n^2 = k^2$.
- Since 2 is a factor of k^2, k^2 must be even and so *k* is even. Since *k* is even, we can rewrite it as $k=2m$ for some integer *m*. Substituting $k=2m$, we get:

$$2n^2 = (2m)^2 \Rightarrow 2n^2 = 4m^2 \Rightarrow n^2 = 2m^2.$$

- So n^2 is even and thus *n* is even. But now both *k* and *n* are even and so have 2 as a common factor. But we had reduced them until they had no common factors. The assumption that $\sqrt{2}$ is rational has led to a contradiction. So $\sqrt{2}$ cannot be rational.

Proof Technique: Counterexample

One Counterexample is enough

Consider a claim of the form $\forall x\ (P(x))$. Such a claim can be proven false if $\exists x\ (\neg P(x, y))$. Just find such an x.

- ***Example:*** Consider the following claim:
- Let A, B, and C be any sets. If $A - C = A - B$ then $B = C$.
- We show that this claim is false with a counterexample:
- Let $A = \emptyset$, $B = \{1\}$, and $C = \{2\}$.
- $A - C = A - B = \emptyset$.
- But $B \neq C$.

Proof Technique: Enumeration

For a case like $\forall x \in A$, $((P(x))$. Divide A into two or more subsets and prove individually that P holds for each subset

- ***Example:*** Suppose that the postage required to mail a letter is always at least 6¢. Prove that it is possible to apply any required postage to a letter given only 2¢ and 7¢ stamps.

- We prove this general claim by dividing it into two cases, based on the value of *n*, the required postage:

1. If *n* is even (and 6¢ or more), apply $n/2$ 2¢ stamps.
2. If *n* is odd (and 6¢ or more), then $n \geq 7$ and $n\text{-}7 \geq 0$ and is even. 7¢ can be applied with one 7¢ stamp. Apply one 7¢ stamp and $(n\text{-}7)/2$ 2¢ stamps.

Proof Technique: Mathematical Induction

- The ***principle of mathematical induction***:

  If: $P(b)$ is true for some integer base case b, and

  For all integers $n \geq b$, $P(n) \rightarrow P(n+1)$

  Then: For all integers $n \geq b$, $P(n)$

- An induction proof has three parts:
  1. A clear statement of the assertion P: the ***thesis*** you have to prove
  2. A proof that that P holds for some base case b, the smallest value with which we are concerned: the ***base case***
  3. A proof that, for all integers $n \geq b$, if $P(n)$ then it is also true that $P(n+1)$. We'll call the claim $P(n)$ the ***induction hypothesis***, and the proof of $P(n+1)$, the ***induction step***

Proof Technique: Mathematical Induction

- ***Example:*** $(5^n - 1)$ is divisible by 4
- **Proof:**
  - Step 1**:** **Basis:** verify the statement for ***n=1***

    $(5^n - 1) = (5^1 - 1) = (5 - 1) = 4$ which is divisible with 4. Hence the statement is true for n=1

  - Step 2: **Induction Hypothesis: a**ssume that the statement is true for ***n=k***,

    $(5^k - 1)$ is divisible by 4 $\Rightarrow (5^k - 1) = 4a$ where 'a' is the quotient of the division of $(5^k - 1)$ with 4 $\Rightarrow 5^k = 4a + 1$

  - Step 3: **Induction Step:** verify the statement for ***n= (k+1)***

    $(5^{k+1} - 1) = (5^k \cdot 5 - 1) = [(4a+1) 5 - 1] = 20a + 5 - 1 = 20a + 4 = 4 (5a + 1)$ which is divisible by 4.

    Hence for n=k+1 the statement is true

Proof Technique: Pigeonhole principle

- The pigeonhole principle states that if n items are put into m pigeonholes with n > m, then at least one pigeonhole must contain more than one item, or more mathematically:

  Consider any function $f: A \to B$.

  If $|A| > |B|$ then f is not one-to-one.

- Despite seeming intuitive it can be used to demonstrate possibly unexpected results (which we will see later in the course!)

Proof Technique: Cardinality

We will be concerned with three cases:

- finite sets,
- countably infinite sets, and
- uncountably infinite sets.

A set A is ***finite*** and has cardinality $n \in \mathbb{N}$ iff either:

  - $A = \varnothing$, or
  - there is a bijection from $\{1, 2, \ldots n\}$ to A, for some n.

A set is ***infinite*** iff it is not finite.

Proof Technique: Cardinality

- $\mathbb{N}$ is countably infinite. Call its cardinality $\aleph_0$.

- A is ***countably infinite*** and also has cardinality $\aleph_0$ iff there exists some bijection $f : \mathbb{N} \rightarrow A$.

- A set is ***countable*** iff it is either finite or countably infinite.

- To prove that a set A is countably infinite, it suffices to find a bijection from $\mathbb{N}$ to it.

Proof Technique: Diagonalization

- The cardinality of the set of Real Numbers (that is the set containing the natural numbers, the fractions and all those funny numbers like *e*, π and $\sqrt{2}$) is bigger than that of the set of Natural number.
- Thus, the real numbers are ***uncountable***
- ***Cantor Diagonalization***
  - *Proof by contradiction*

3.14159...
1.41421...
1.73205...
2.23606...
2.71828...
0.14285...

$\Downarrow$

3.43625...

$\Downarrow$

2.32514...

Summary

- Boolean Logic
  - WFF, Tautologies, Contradiction, Satisfiable
- Axiom, Theorem, Proof, Inference Rules
- First Order Logic
- Sets Theory: Sets, Relations and Functions
- Closures
- Different Proof Techniques

References

- **Automata, Computability and Complexity. Theory and Applications**
- By Elaine Rich
- Appendix A:
  - Page : 745~765, 769~792.