MA/CSSE 474

Theory of Computation

More Math Review

Many of today's ICQ questions involve working with another student. Find a partner and sit beside that person.

Logic: Propositional and first-order

From Rich, Appendix A

Most of this material also appears in Grimaldi's Discrete Math book, Chapter 2

Boolean (Propositional) Logic Wffs

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

1. A propositional symbol (variable or constant) is a wff.
2. If P is a wff, then $\neg P$ is a wff.
3. If P and Q are wffs, then so are:
   $P \vee Q$, $P \wedge Q$, $P \rightarrow Q$, $P \leftrightarrow Q$, and (P).

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*

When Wffs are True

- A wff is ***valid*** or is a ***tautology*** iff it is true for all assignments of truth values to the variables it contains.
- A wff is ***satisfiable*** iff it is true for at least one assignment of truth values to the variables it contains.
- A wff is ***unsatisfiable*** 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 for every assignment of truth values to the variables they contain.

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

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

Q1

Entailment

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

Example:

$\{A \wedge B \wedge C, D\}$ entails $A \rightarrow D$

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*.

Q2

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.
- ***Syllogism***: From $(P \rightarrow Q)$ and $(Q \rightarrow R)$, conclude $(P \rightarrow R)$.

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 $\exists x\ (P(x))$.

First-Order Logic

A **term** is a variable, constant, or function application.
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 $x_1, x_2, \ldots, x_n$ is a term, then an expression of the form $P(x_1, x_2, \ldots, x_n)$ is a wff. If any variable occurs in such a wff, then that variable occurs ***free*** *in* $P(x_1, x_2, \ldots, x_n)$.
- 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.

Q3

Sentences

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

1. $Bear(Smokey)$.
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. $\forall x\ ((Animal(x) \wedge \neg Dead(x)) \rightarrow Alive(x))$.

Which of these sentences are true in the everyday world?

A ***ground instance*** is a sentence that contains no variables, such as #1

Q4

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.

Q5

Examples

- $\forall x\ ((P(x) \wedge Q(Smokey)) \rightarrow P(x))$.
- $\neg(\forall x\ (P(x) \vee \neg(P(x)))$.
- $\forall x\ (P(x, x))$.

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:

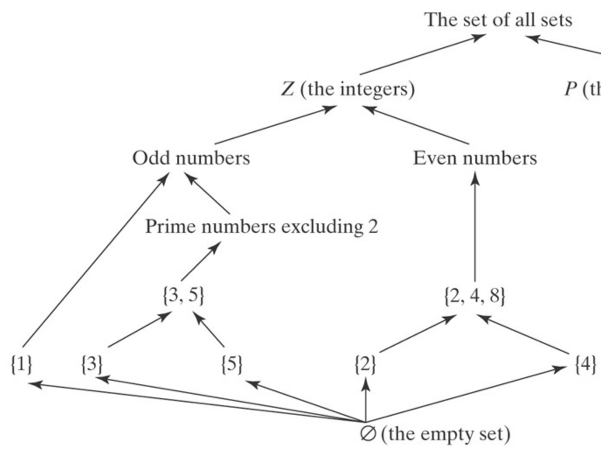
[4] $P(X_1) \wedge Q(X_1) \rightarrow R(X_1)$. (Universal instantiation, [1].)
[5] $P(X_1) \wedge Q(X_1)$. (And introduction, [2], [3].)
[6] $R(X_1)$. (Modus ponens, [5], [4].)

Q6

Definition of a Theory

- A first-order **theory** is a set of axioms and the set of all theorems that can be proved, using a set of sound and complete inference rules, from those axioms.
- A theory is logically **complete** iff, for every sentence P in the language of the theory, either P or ¬P is a theorem.
- A theory is **consistent** iff there is no sentence P such that both P and ¬ P are theorems.
  - If there is such a sentence, then the theory contains a **contradiction** and is **inconsistent**.
- Let w be an interpretation of a theory. The theory is **sound** with respect to w if every theorem in the theory corresponds to a statement that is true in w.

Subset-of



Subset-of is a **partial order** (reflexive, antisymmetric, transitive)

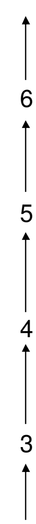
Total Orders

A ***total order*** $R \subseteq A \times A$ is a partial order that has the additional property that:

$$\forall x, y \in A\ ((x, y) \in R \vee (y, x) \in R).$$

Example: $\leq$ on the rational numbers

If R is a total order defined on a set A, then the pair (A, R) is a ***totally ordered set***.



Q7-8

Infinite Descending Chain

- A partially ordered set (S, <) has an infinite descending chain if there is an infinite set of elements $x_0, x_1, x_2, \ldots \in S$ such that $\forall i \in \mathbb{N}(x_{i+1} < x_i)$
- Example:
  In the rational numbers with <,
  1/2 > 1/3 > 1/4 > 1/5 > 1/6 > …
  is an infinite descending chain

Well-Founded and Well-Ordered Sets

Given a partially ordered set (*A*, *R*), an ***infinite descending chain*** is a totally ordered, with respect to *R*, subset *B* of *A* that has no minimal element.

If (*A*, *R*) contains no infinite descending chains then it is called a ***well-founded set***.

•Used for halting proofs.

If (*A*, *R*) is a well-founded set and *R* is a total order, then (*A*, *R*) is called a ***well-ordered set***.

•Used in induction proofs.

•The positive integers are well-ordered

•The positive rational numbers are not well-ordered (with respect to normal <)

Q8

Mathematical Induction

Because the integers $\geq b$ *are well-ordered:*

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.
2. A proof that that P holds for some base case b, the smallest value with which we are concerned.
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***.

Sum of First *n* Positive Odd Integers

The sum of the first n odd positive integers is n^2. We first check for plausibility:

$(n = 1)\ 1 = 1 = 1^2$.
$(n = 2)\ 1 + 3 = 4 = 2^2$.
$(n = 3)\ 1 + 3 + 5 = 9 = 3^2$.
$(n = 4)\ 1 + 3 + 5 + 7 = 16 = 4^2$, and so forth.

The claim appears to be true, so we should prove it.

Sum of First *n* Positive Odd Integers

Let $Odd_i = 2(i-1)+1$ denote the i^{th} odd positive integer. Then we can rewrite the claim as:

$$\forall n \geq 1 \ \ (\sum_{i=1}^{n} Odd_i = n^2)$$

For reference; we will not do this in class

The proof of the claim is by induction on n:
Base case: take 1 as the base case. $1 = 1^2$.

Prove: $\forall n \geq 1((\sum_{i=1}^{n} Odd_i = n^2) \rightarrow (\sum_{i=1}^{n+1} Odd_i = (n+1)^2))$

$$\sum_{i=1}^{n+1} Odd_i = \sum_{i=1}^{n} Odd_i + Odd_{n+1}$$

$= n^2 + Odd_{n+1}$. (Induction hypothesis.)
$= n^2 + 2n + 1$. ($Odd_{n+1} = 2(n+1-1) + 1 = 2n + 1$.)
$= (n+1)^2$.

Note that we start with one side of the equation we are trying to prove, and transform to get the other side. We do **not** treat it like solving an equation, where we transform both sides in the same way.

Strong induction

- To prove that predicate P(n) is true for all n≥b:
  - Show that P(b) is true [and perhaps P(b+1) *]
  - Show that for all j>b, if P(k) is true for all k with b≤ k<j, then P(j) is true. In symbols:

$$\forall j > b\ ((\forall k\ (b \leq k < j \rightarrow P(k)) \rightarrow P(j))$$

* We may have to show it directly for more than one or two values, but there should always be a finite number of base cases.

Fibonacci Running Time

- From Weiss, Data Structures and Problem Solving with Java, Section 7.3.4
- Consider this function to recursively calculate Fibonacci numbers:
  $F_0=0$ $F_1=1$ $F_n = F_{n-1}+F_{n-2}$ if $n \geq 2$.
  - ```
    def fib(n):
        if n <= 1:
            return n
        return fib(n-1) + fib(n-2)
    ```
- Let C_N be the number of calls to fib during the computation of fib(N).
- It's easy to see that $C_0=C_1=1$,
  and if $N \geq 2$, $C_N = C_{N-1} + C_{N-2} + 1$.
- **Prove that** for $N \geq 3$, $C_N = F_{N+2} + F_{N-1} - 1$.

Q10
    ```