# Propositional Calculus (Part 2)

CS 4710 Course Notes

January 18, 2019

## Satisfaction

**Def. 1** A valuation $V$ *satisfies* a set of statements $S$ iff, for all $P \in S$: $[\![P]\!]^V = \top$.

**Def. 2** A set of statements $S$ is *satisfiable* iff there exists a valuation $V$ that satisfies $S$.

**Def. 3** Statement $P$ is a *tautology* iff for all $V$, $V$ satisfies $S$.

**Note.** If $P$ is a tautology, $S \vdash P$ for all $S$ (including the empty set, in which case we write $\vdash P$).

**Def. 4** We will be dealing with the sole inference rule "modus ponens" (MP) in PC. Suppose we have a derivation $R = R_1, \ldots, R_n$. If there exist some $R_i, R_j \in R$ such that $R_i = P \to Q$ and $R_j = P$, MP allows us to derive (or "generate") $Q$. In other words: $P \to Q, P \vdash Q$.

**Def. 5** Let $S$ be a set of statements, and $i, n$ denote indices such that $1 \leq i \leq n$. A *deduction* (also "derivation") is a finite sequence of statements $P_1, \ldots, P_n$ such that one of the following holds:

1. $P_i$ is a tautology
2. $P_i \in S$
3. There exist $j, k$ such that $1 \leq j, k < i$ and $P_i$ is derivable from $P_j$ and $P_k$ using MP.

**Def. 6** $S \vdash P$ can be read as "$S$ derives $P$".

## The Deduction Theorem

For any set of statements $S$ and any statements $P, Q$:

$$S, P \vdash Q \text{ iff } S \vdash P \to Q$$

**Proof.** ($\Leftarrow$ direction first)

Assume $S \vdash P \to Q$. By the definitions of $\vdash$ and deduction, there exists a sequence $R_1, \ldots, R_n$ with $R_n = P \to Q$. Recall we are trying to prove $S, P \vdash Q$, so by supposition append $P$ to $S$, yielding $S, P$. Given that $R_n = P \to Q$, we can append $Q$ to the end of our sequence by an application of MP to $P, P \to Q$. By the definition of deduction, this sequence is a deduction of $Q$ from $S, P$, and

so $S, P \vdash Q$. ■

(now we prove the $\Rightarrow$ direction)

Assume $S, P \vdash Q$. By the definition of $\vdash$ and deduction, there exists a sequence $R_1, \ldots, R_n$ such that $R_n = Q$. We will now use proof by contradiction to get at our goal.

Goal: $S \vdash P \to R_k$ for $1 \leq k \leq n$.

First, we will assume the negation of our goal – suppose $S \vdash P \to R_k$ is false. (This strategy is called proof by contradiction.) We will use this supposition in each of the cases delineated by the definition of deduction to produce a counterexample. Once a counterexample has been demonstrated for each case, we will have shown that our supposition itself must be false (thus proving our goal). Consider the four possible cases for $R_k$:

1. $R_k$ is a tautology
2. $R_k \in S$
3. $R_k$ is derivable from some $R_i, R_j$ with $1 \leq i, j < k$ using MP

We will show (1) produces a counterexample to our negated goal (the rest of the cases are left as an exercise to check your understanding). If $R_k$ is an axiom, then by the definition of $\to$, $[\![X \to R_k]\!] = \top$ for any statement $X$. Thus $P \to R_k$ is also a tautology, given that it is true under any possible valuation (by the definition of $\to$). Note that $S \vdash X$ for any tautology $X$, and therefore $S \vdash P \to R_k$ **(COUNTEREXAMPLE)**.

Assuming we have shown each case produces a contradiction, we have proven this direction. ■

As both directions have been proven, we have proven the deduction theorem. ■

**Mathematical induction**

Mathematical induction is a proof strategy that exploits recursion. Given that the natural numbers are a **recursively enumerable set** (producible by recursion), we can use mathematical induction to prove statements about all natural numbers. Also, given that a finite sequence is enumerable by a sequence of indices, we can use mathematical induction to prove statements "for all sequences" by inducing over indices. We simply have to phrase the problem in the proper way.

Inductive proofs consist of (at the highest level) two cases: the "base" case, and the "step" case. This mirrors how one constructs a recursive function, or definition.

Suppose we are trying to prove some statement about the natural numbers. For notation's sake, say for natural number $x$ that $P(x)$ reads "property $P$ holds of $x$". If we were trying to prove $P(x)$ for any natural number $x$, we use the base case 1 – first we demonstrate that $P(1)$ is true.

In the step case, we seek to prove that if $P(n)$ holds for some arbitrary number $n$, that $P(n+1)$ must also hold. In other words, we seek to prove:

$$P(n) \Rightarrow P(n+1)$$

In doing so, we are permitted (in fact, we must) assume $P(n)$ holds. This is called the *inductive hypothesis*.

Note that if $P(1)$ holds, and if $P(n)$ holding ensures $P(n+1)$ holds for arbitrary $n$, then it follows that $P(1), P(2), \ldots$ all hold as well (by recursive application of our step case, starting with the base case).

**Example.** Prove: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

**Proof by induction.**

**Base case (k=1)**

$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$ ■

**Step case** Let $S_n = \frac{n(n+1)}{2}$. As our inductive hypothesis, assume $S_n$ holds. Now we must show that $S_{n+1} = \frac{(n+1)(n+2)}{2}$ holds. Note that, by definition, $S_{n+1} = S_n + (n+1)$. Using a bit of algebra:

$S_{n+1} = \frac{n(n+1)}{2} + (n+1)$ (by our inductive hypothesis)

$\frac{n(n+1)}{2} + (n+1) = \frac{n^2+3n+2}{2} = \frac{(n+1)(n+2)}{2}$ (with a bit of algebra)

Thus: $S_{n+1} = \frac{(n+1)((n+1)+1)}{2}$. ■

We will use proof by induction next time to prove **soundness** for PC.