Lecture 2.5: Proofs in propositional calculus

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4190, Discrete Mathematical Structures

Motivation

Consider the theorem:

$$a,\ a \to b,\ b \to c,\ \ldots, y \to z\ \Rightarrow\ z.$$

A truth table will have 2^{26} entries. At 1 million cases/sec, it will take 1 hour to verify this.

Now, consider the theorem:

$$p_1,\ p_1 \to p_2,\ p_2 \to p_3,\ \ldots, p_{99} \to p_{100}\ \Rightarrow\ p_{100}.$$

A truth table will have $2^{100} \approx 1.27 \times 10^{30}$ entries. At 1 millions cases/sec, it will take 1.47×10^{14} days to check.

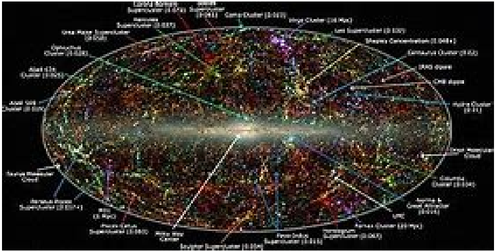

Figure: The observable universe is approximately 5×10^{12} days old.

Clearly, we need alternate methods of proofs.

Direct proof

Theorem 1

$p \to r,\ q \to s,\ p \vee q \Rightarrow s \vee r.$

Proof

Step	Proposition	Justification	
1.	$p \vee q$	Premise	
2.	$\neg p \to q$	(1), conditional rule	$[p \to q \Leftrightarrow \neg p \vee q]$
3.	$q \to s$	Premise	
4.	$\neg p \to s$	(2), (3), transitivity	
5.	$\neg s \to p$	(4), contrapositive	
6.	$p \to r$	Premise	
7.	$\neg s \to r$	(5), (6), transitivity	
8.	$s \vee r$	(7), conditional rule	$\square$

Direct proof

Theorem 2

$\neg p \vee q,\ s \vee p,\ \neg q \Rightarrow s.$

Proof 1

Step	Proposition	Justification	
1.	$\neg p \vee q$	Premise	
2.	$\neg q$	Premise	
3.	$\neg p$	(1), (2), disjunctive simplification	
4.	$s \vee p$	Premise	
5.	s	(3), (4), disjunctive simplification	$\square$

Proof 2

Step	Proposition	Justification	
1.	$\neg p \vee q$	Premise	
2.	$p \to q$	(1), conditional rule	
3.	$\neg q \to \neg p$	(2), contrapositive	
4.	$s \vee p$	Premise	
5.	$p \vee s$	Commutativity	
6.	$\neg p \to s$	(5), conditional rule	
7.	$\neg q \to s$	(3), (6), transitivity	
8.	$\neg q$	Premise	
9.	s	(7), (8) *modus ponens*	$\square$

Direct proof

The conclusion of a theorem is often a conditional proosition.

In this case, the condition of the conclusion can be included as an added premise in the proof.

This rule is justified by the logical law

$$p \to (h \to c) \;\Leftrightarrow\; (p \wedge h) \to c$$

Theorem 3

$p \to (q \to s),\ \neg r \vee p,\ q \Rightarrow (r \to s)$.

Proof

Step	Proposition	Justification
1.	$\neg r \vee p$	Premise
2.	r	Added premise
3.	p	(1), (2), disjunction simplification
4.	$p \to (q \to s)$	Premise
5.	$q \to s$	(3), (4), *modus ponens*
6.	q	Premise
7.	s	(5), (6), *modus ponens*

□

Indirect proof (Proof by contradition)

Sometimes, it is difficult or infeasible to prove a statement directly. Consider the following basic fact in number theory.

Theorem

There are infinitely many prime numbers.

Proving this *directly* might involve a method or algorithm for generating prime numbers of arbitrary size. The following is an indirect proof.

Proof

Assume, for sake of contradiction, that there are finitely many prime numbers, $p_1, \dots, p_n$.

Let's look at what proof by contradiction looks like in propositional calculus.

Indirect proof

Consider a theorem $P \Rightarrow C$, where P represents the premises $p_1, \ldots, p_n$.

The method of indirect proof is based on the equivalence (by DeMorgan's laws)

$$P \to C \;\Leftrightarrow\; \neg(P \wedge \neg C).$$

Said differently, if $P \Rightarrow C$, then $P \wedge \neg C$ is always false, i.e., a contradiction.

In this method, we negate the conclusion and add it to the premises. The proof is complete when we find a contradiction from this set of propositions.

A contradiction will often take the form $t \wedge \neg t$.

Theorem 4

$a \to b$, $\neg(b \vee c)$, $\Rightarrow \neg a$.

Proof

Step	Proposition	Justification
1.	a	Negation of the conclusion
2.	$a \to b$	Premise
3.	b	(1), (2), *modus ponens*
4.	$b \vee c$	(3), disjunctive addition
5.	$\neg(b \vee c)$	Premise
6.	0	(4), (5)

□

Indirect proof

Theorem 1 (revisted)

$p \to r,\ q \to s,\ p \vee q \Rightarrow s \vee r.$

Proof

Step	Proposition	Justification
1.	$\neg(s \vee r)$	Negated conclusion
2.	$\neg s \wedge \neg r$	(1), DeMorgan's laws
3.	$\neg s$	(2), conjunctive simplification
4.	$q \to s$	Premise
5.	$\neg q$	(3), (4), *modus tollens*
6.	$\neg r$	(2), conjunctive simplification
7.	$p \to r$	Premise
8.	$\neg p$	(6), (7), *modus tollens*
9.	$\neg p \wedge \neg q$	Conjunction of (5), (8)
10.	$\neg(p \vee q)$	DeMorgan's law
11.	$p \vee q$	Premise
12.	0	(10), (11)

$\square$

Applications of propositional calculus

For a playful description on how propositional calculus plays a role in artifical intelligence, see the Pulitzer Prize winning book *Gödel, Escher, Bach: an Eternal Golden Braid*, by Douglas Hofstadter.