Propositional Calculus

Declaration

This note was prepared based on the book *Logic for Computer Science* by A. Singha.

To keep the matter simple, we plan to work with a subset of connectives. We choose the subset $\{\neg, \to\}$. We may introduce other connectives by way of definitions later. We thus choose our language for propositional calculus (PC, for short) as the fragment of **PROP** having all propositional variables and the connectives $\neg$ and $\to$.

In PC, right now, we do not have the propositional constants $\top$ and $\bot$; and we do not have the connectives $\wedge, \vee$, and $\leftrightarrow$. Again, we use the grammar of **PROP** appropriate for this fragment. We also use the precedence rules to abbreviate our PC-propositions with the usual conventions of omitting brackets and subscripts in the propositional variables. Moreover, we use capital letters $A, B, C, \ldots$ as generic symbols for propositions.

The axiom schemes of PC are:

$$\text{(A1)} \quad A \to (B \to A)$$
$$\text{(A2)} \quad (A \to (B \to C)) \to ((A \to B) \to (A \to C))$$
$$\text{(A3)} \quad (\neg A \to \neg B) \to ((\neg A \to B) \to A)$$

An **axiom** is any instance of an axiom scheme, obtained by replacing throughout the letters A, B, C by propositions. For example, $p \to (q \to p)$ is an axiom as it is obtained from **A1** by replacing A by p and B by q throughout. We thus refer to $p \to (q \to p)$ as **A1**. Similarly, $(p \to q) \to ((q \to p) \to (p \to q))$ is also **A1**.

In addition to the axioms, PC has a rule of inference; it is as follows:

Modus Ponens (MP): If A and $A \to B$ are both propositions (assumptions), then B can be inferred. Formally:

$$\frac{A,\ A \to B}{B}$$

The inference rule **Modus Ponens (MP)** is an incarnation of the valid consequence *Modus Ponens*:

$$\{A, A \to B\} \vdash B.$$

Since in an axiomatic system there is no concept of truth or falsity, we simply write the consequence as a fraction:

$$\frac{A,\ A \to B}{B}.$$

You may read the rule **MP** as: *From A and $A \to B$, derive B.*

This is again a *rule scheme* in the sense that any instance of this scheme is a rule. That is, if you have already *derived* the propositions p and $p \to q$, then the rule allows you to derive q.

The rule allows you to derive q. Deriving $q \to r$ from $p \to q$ and $(p \to q) \to (q \to r)$ is an application of the rule **MP**. Informally, the word 'derive' signals deductions; formally, it just allows us to write the propositions one after another.

The axiomatic system **PC** has all the propositions having only the connectives $\neg$ and $\to$. **PC** has the axiom schemes **A1**, **A2**, **A3**, and the inference rule **MP**. A *proof* in **PC** is defined to be a finite sequence of propositions, where each one is either an axiom or is obtained (derived) from two earlier propositions by an application of **MP**. The last proposition of a proof is called a *theorem* of **PC**; the proof is said to *prove* the theorem.

The fact that "A is a theorem in **PC**" is written as $\vdash_{\mathrm{PC}} A$. We also read $\vdash_{\mathrm{PC}} A$ as "A is provable in **PC**." If no other axiomatic system is in sight, we may abbreviate $\vdash_{\mathrm{PC}}$ to $\vdash$ without the subscript **PC**. In that case, the phrases 'proof in **PC**', '**PC**-proof', and 'proof' mean the same thing.

The symbol $\vdash$ will have the least precedence. For example, $\vdash p \to p$ is a shorthand for writing $\vdash (p \to p)$; and $\vdash \neg p \to (p \to q)$ abbreviates $\vdash (\neg p \to (p \to q))$.

Example 0.1. *The following is a proof of $\vdash_{PC} r \to (p \to (q \to p))$:*

1. $(p \to (q \to p)) \to (r \to (p \to (q \to p)))$ — *A1, $A := p \to (q \to p), B := r$*
2. $p \to (q \to p)$ — *A1, $A := p, B := q$*
3. $r \to (p \to (q \to p))$ — *1, 2, MP*

Example 0.2. *Show that $p \to p$.*

1. $p \to ((q \to p) \to p)$ — *A1*
2. $(p \to ((q \to p) \to p)) \to ((p \to (q \to p)) \to (p \to p))$ — *A2*
3. $(p \to (q \to p)) \to (p \to p)$ — *1, 2, MP*
4. $p \to (q \to p)$ — *A1*
5. $p \to p$ — *3, 4, MP*

In an axiomatic system such as PC, the notion of a proof is effective, i.e., if it is claimed that some object is a proof of a theorem, then it can be checked whether the claim is correct or not in an algorithmic manner. However, construction of a proof may not be effective; there may or may not be an algorithm to construct a proof of a given theorem.

Of course, proofs can be generated mechanically by following the specified rules. The problem comes when a proof is targeted towards proving a given theorem. We will see by way of examples how to do it. We may have to rely on our intuition in constructing proofs.

Example 0.3. *Show that $q \to (p \to p)$. Here is the proof:*

1. $p \to ((q \to p) \to p)$
2. ...
3. ...
4. ...
5. $p \to p$ *(Example 0.2)*
6. $(p \to p) \to (q \to (p \to p))$ *(A1)*
7. $q \to (p \to p)$ *(5, 6, MP)*

Remark: Just like axiom schemes and inference rules, theorems are theorem schemes. Once you have a proof of $p \to p$, you can have a proof of $(p \to q) \to (p \to q)$. It is simple; just replace p by $p \to q$ throughout the proof. Thus, known theorems can be used in proving new theorems. We will mention 'Th' in the rightmost column of a proof, when we use an already proved theorem.

The proof in Example 0.3 can be rewritten as:

1. $p \to p$ (Th)
2. $(p \to p) \to (q \to (p \to p))$ (Axiom A1)
3. $q \to (p \to p)$ (1, 2, MP)

Exercise 0.1. *Show that $(\neg q \to q) \to q$.*

Let Σ be a set of propositions, and let w be any proposition. A proof of the consequence $\Sigma! \vdash w$ in PC is defined to be a finite sequence of propositions where:

- Each proposition is either an axiom, a proposition in Σ, or is obtained from earlier two propositions by an application of MP (Modus Ponens); and
- The last proposition in the sequence is w.

In the consequence $\Sigma \vdash w$, each proposition from Σ is called a **premise**, and w is called the **conclusion**.

We write $\Sigma \vdash_{PC} w$ to say that there exists a proof of the consequence $\Sigma \vdash w$ in PC. This fact is also expressed as "the consequence $\Sigma! \vdash w$ is provable in PC." Informally, a proof of $\Sigma! \vdash w$ is also called a proof of $\Sigma \vdash_{PC} w$.

When $\Sigma = \{w_1, \ldots, w_n\}$, a finite set, we write $\Sigma \vdash_{PC} w$ as:

$$w_1, \ldots, w_n \vdash_{PC} w.$$

As earlier, we will write $\Sigma \vdash w$ if no confusion arises.

We observe that when $\Sigma = \emptyset$, $\Sigma \vdash w$ boils down to $\vdash w$. Moreover, it is not mandatory that a proof uses all axioms; similarly, a proof of a consequence need not use all given premises.

Proofs of consequences are written in three columns, like proofs of theorems. We mention the letter 'P' in the documentation to indicate that the proposition used in that line of the proof is a premise.

Example 0.4. *Construct a proof to show that $\neg p, p \vdash q$. Here is the proof:*

1. p *(P)*

2. $p \to (\neg q \to p)$ *(A1)*

3. $\neg q \to p$ *(1, 2, MP)*

4. $\neg p$ *(P)*

5. $\neg p \to (\neg q \to \neg p)$ *(A1)*

6. $\neg q \to \neg p$ *(4, 5, MP)*

7. $(\neg q \to \neg p) \to ((\neg q \to p) \to q)$ *(A3)*

8. $(\neg q \to p) \to q$ *(6, 7, MP)*

9. q *(3, 8, MP)*

Example 0.5. *Show that $p \to q, q \to r \vdash p \to r$.*

Here is the proof:

1. $q \to r$ *(P)*

2. $p \to (q \to r)$ *(1, A1)*

3. $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$ *(A2)*

4. $(p \to q) \to (p \to r)$ *(2, 3, MP)*

5. $p \to q$ *(P)*

6. $p \to r$ *(4, 5, MP)*

Derived Rules of Inference: Theorems can be used as new axioms. In the same way, already derived consequences can be used as new inference rules. The reason: proof of such a consequence can be duplicated with necessary replacements. Such new inference rules are referred to as **derived rules of inference**.

The consequence $\{p \to q, q \to r\} \vdash p \to r$ in the above example is rewritten as the derived rule of **Hypothetical Syllogism**:

$$\text{(HS)} \quad \frac{A \to B \quad B \to C}{A \to C}$$

Example 0.6. *Show that* $\neg q \to \neg p \vdash p \to q$*.*

We use the derived rule HS in the following proof:

1. $\neg q \to \neg p$ *(P)*

2. $(\neg q \to \neg p) \to ((\neg q \to p) \to q)$ *(A3)*

3. $(\neg q \to p) \to q$ *(1, 2, MP)*

4. $p \to (\neg q \to p)$ *(A1)*

5. $p \to q$ *(4, 3, HS)*

Example 0.7. *Show that* $\vdash \neg\neg p \to p$*.*

1. $\neg\neg p \to (\neg p \to \neg\neg p)$ *(A1)*

2. $(\neg p \to \neg\neg p) \to ((\neg p \to \neg p) \to p)$ *(A3)*

3. $\neg\neg p \to ((\neg p \to \neg p) \to p)$ *(1, 2, HS)*

4. $(\neg\neg p \to ((\neg p \to \neg p) \to p)) \to ((\neg\neg p \to (\neg p \to \neg p)) \to (\neg\neg p \to p))$ *(A3)*

5. $(\neg\neg p \to (\neg p \to \neg p)) \to (\neg\neg p \to p)$ *(3, 4, MP)*

6. $\neg p \to \neg p$ *(Th)*

7. $(\neg p \to \neg p) \to (\neg\neg p \to (\neg p \to \neg p))$ *(A1)*

8. $\neg\neg p \to (\neg p \to \neg p)$ *(6, 7, MP)*

9. $\neg\neg p \to p$ *(8, 5, MP)*

0.1 Exercises

Try to construct PC-proofs of the following consequences:

1. $p \to q, q \to r, p \vdash r$
2. $\neg q \to \neg p, p \vdash q$
3. $p \to q, \neg q \vdash \neg p$
4. $p \vdash \neg\neg p$
5. $p \to (q \to r), q \vdash p \to r$
6. $\vdash (p \to q) \to (\neg q \to \neg p)$

1 Metatheorems

To prove "if x then y" we assume x and derive y. It is accepted in each branch of mathematics. Since we are questioning the process of reasoning itself, can we accept it in PC? We should rather prove this principle.

Theorem 1.1 (DT: Deduction Theorem)**.** *Let Σ be a set of propositions, and let p, q be propositions. Then, $\Sigma \vdash p \to q$ iff $\Sigma \cup \{p\} \vdash q$.*

Proof. Suppose that $\Sigma \vdash p \to q$. To show $\Sigma \cup \{p\} \vdash q$, take the proof of $\Sigma \vdash p \to q$, adjoin to it the lines (propositions) p, q. It looks like:

1. $\cdots$
2. $\cdots$
3. $p \to q$ (Proof of $\Sigma \vdash p \to q$)
4. p (P)
5. q (3, 4, MP)

This is a proof of $\Sigma \cup \{p\} \vdash q$.

Conversely, suppose that $\Sigma \cup \{p\} \vdash q$; we have a proof of it. We construct a proof of $\Sigma \vdash p \to q$ by induction on the number of propositions (number of lines) used in the proof of $\Sigma \cup \{p\} \vdash q$.

Basis step: Suppose that the proof of $\Sigma \cup \{p\} \vdash q$ has only one proposition. Then this proposition has to be q. Now, why is this a proof of $\Sigma \cup \{p\} \vdash q$? There are three possibilities:

(a) q is an axiom.

(b) $q \in \Sigma$.

(c) $q = p$.

In each case, we show how to get a proof of $\Sigma \vdash p \to q$:

(a) In this case, our proof is:

(a) q (An axiom)
(b) $q \to (p \to q)$ (A1)
(c) $p \to q$ (1, 2, MP)

It is a proof of $\Sigma \vdash p \to q$ since it uses no proposition other than axioms.

(b) In this case, the above proof still works, only the first line would be documented as 'P', a premise in Σ, rather than an axiom.

(c) Here, $q = p$. We just repeat the proof given in Example 0.2:

(a) $\cdots$
(b) $\cdots$
(c) $p \to p$ (MP)

Induction step: Lay out the induction hypothesis:

> If there exists a proof of $\Sigma \cup \{p\} \vdash q$ having less than n propositions in it (in the proof), then there exists a proof of $\Sigma \vdash p \to q$.

Suppose now that we have a proof P of $\Sigma \cup \{p\} \vdash q$ having n propositions in it. Observe that we have four cases to consider based on what q is. They are:

(i) q is an axiom, (ii) $q \in \Sigma$, (iii) $q = p$ The cases (i)–(iii) are similar to the basis case.

(iv) q has been derived by an application of MP in the proof P . In this case, the proof P looks like:

$$
P : \quad \begin{array}{rll}
1. & \cdots & \\
 & \vdots & \\
m. & r \cdots & \\
 & \vdots & \\
m+k. & r \to q & \\
 & \vdots & \\
n. & q & \qquad (m, m+k, \mathrm{MP})
\end{array}
$$

where $m < n$, $m + k < n$, and r is some proposition.

The proof segment P_1 (lines 1 through m) proves $\Sigma \cup \{p\} \vdash r$.

The proof segment P_2 (lines 1 through $m + k$) proves $\Sigma \cup \{p\} \vdash r \to q$.

The proofs P_1, P_2 have less than n propositions. By the induction hypothesis, corresponding to P_1 and P_2, there exist proofs P_3 and P_4 such that:

- P_3 proves $\Sigma \vdash p \to r$.
- P_4 proves $\Sigma \vdash p \to (r \to q)$.

Suppose that P_3 has i propositions and P_4 has j propositions. We use P_3 and P_4 to construct a proof P_5 of $\Sigma \vdash p \to q$. The proof P_5 is constructed by adjoining P_4 to P_3, and then adding some more propositions:

$$
P_5 : \quad \begin{array}{rlr}
1. & \cdots & (P_3 \text{ begins}) \\
 & \vdots & \\
i. & p \to r & (P_3 \text{ ends}) \\
i+1. & \cdots & (P_4 \text{ begins}) \\
 & \vdots & \\
i+j. & p \to (r \to q) & (P_4 \text{ ends}) \\
i+j+1. & (p \to (r \to q)) \to ((p \to r) \to (p \to q)) & (\mathrm{A2}) \\
i+j+2. & (p \to r) \to (p \to q) & (i+j, i+j+1, \mathrm{MP}) \\
i+j+3. & p \to q & (i, i+j+2, \mathrm{MP})
\end{array}
$$

Now, P_5 is a proof of $\Sigma \vdash p \to q$ since the premises used in it are either axioms or propositions from Σ. □

Let Σ be a set of propositions.

We say that Σ is **inconsistent** iff there exists a proposition w such that $\Sigma \vdash w$ and $\Sigma \vdash \neg w$. That is, Σ is inconsistent iff there exists a proof, possibly using premises from Σ, where some proposition and its negation both occur. We say that Σ is **consistent** iff Σ is not inconsistent.

In case of consequences, each premise is also a conclusion since it has a one line proof, with the justification that it is a premise. Similarly, any conclusion that has been derived from a set of premises can still be derived if some more premises are added. This is monotonicity.

Theorem 1.2 (M: Monotonicity). *Let Σ and Γ be sets of propositions, $\Sigma \subseteq \Gamma$, and let w be a proposition.*

1. *If $\Sigma \vdash w$, then $\Gamma \vdash w$.*
2. *If Σ is inconsistent, then Γ is inconsistent.*

Proof. (1) Let $\Sigma \vdash w$. We then have a proof where some (or all) of the premises from Σ are used to have its last line as w. The same proof shows that $\Gamma \vdash w$.

(2) If Σ is inconsistent, then there exists a proposition p such that $\Sigma \vdash p$ and $\Sigma \vdash \neg p$. By (1), $\Gamma \vdash p$ and $\Gamma \vdash \neg p$. Therefore, Γ is inconsistent.

□

Theorem 1.3 (RA: Reductio ad Absurdum). *Let Σ be a set of propositions, and let w be a proposition.*

1. *$\Sigma \vdash w$ iff $\Sigma \cup \{\neg w\}$ is inconsistent.*
2. *$\Sigma \vdash \neg w$ iff $\Sigma \cup \{w\}$ is inconsistent.*

Proof. (1) Suppose that $\Sigma \vdash w$. By monotonicity, $\Sigma \cup \{\neg w\} \vdash w$. With a one-line proof, $\Sigma \cup \{\neg w\} \vdash \neg w$. Therefore, $\Sigma \cup \{\neg w\}$ is inconsistent.

Conversely, suppose that $\Sigma \cup \{\neg w\}$ is inconsistent. Then there is a proposition, say p, such that $\Sigma \cup \{\neg w\} \vdash p$ and $\Sigma \cup \{\neg w\} \vdash \neg p$. By the deduction theorem, $\Sigma \vdash \neg w \to p$ and $\Sigma \vdash \neg w \to \neg p$. Suppose P_1 is a proof of $\Sigma \vdash \neg w \to \neg p$ containing m propositions and P_2 is a proof of $\Sigma \vdash \neg w \to p$ containing n propositions. Construct a proof P of $\Sigma \vdash w$ as follows:

$$P : \begin{array}{ll}
1. & \cdots \quad P_1 \text{ begins} \\
 & \vdots \\
m. & \neg w \to \neg p \quad P_1 \text{ ends} \\
m+1. & \cdots \quad P_2 \text{ begins} \\
 & \vdots \\
m+n. & \neg w \to p \quad P_2 \text{ ends} \\
m+n+1. & (\neg w \to \neg p) \to ((\neg w \to p) \to w) \quad \text{A3} \\
m+n+2. & (\neg w \to p) \to w \quad m, m+n+1, \text{MP} \\
m+n+3. & w \quad m+n, m+n+2, \text{MP}
\end{array}$$

(2) If $\Sigma \vdash \neg w$, then by monotonicity, $\Sigma \cup \{w\} \vdash \neg w$. Also, $\Sigma \cup \{w\} \vdash w$, trivially. Hence, $\Sigma \cup \{w\}$ is inconsistent.

Conversely, suppose that $\Sigma \cup \{w\}$ is inconsistent. We show that $\Sigma \cup \{\neg\neg w\}$ is also inconsistent. Now, inconsistency of $\Sigma \cup \{w\}$ implies that there exists a proposition p such that $\Sigma \cup \{w\} \vdash p$ and $\Sigma \cup \{w\} \vdash \neg p$. So, there exist proofs P_1 and P_2 such that:

$$P_1 \text{ proves } \Sigma \cup \{w\} \vdash p$$
$$P_2 \text{ proves } \Sigma \cup \{w\} \vdash \neg p$$

Observe that $\Sigma \cup \{\neg\neg w, \neg w\} \vdash \neg\neg w$ and $\Sigma \cup \{\neg\neg w, \neg w\} \vdash \neg w$. That is, $\Sigma \cup \{\neg\neg w, \neg w\}$ is inconsistent. By (1), we obtain $\Sigma \cup \{\neg\neg w\} \vdash w$. Then there exists a proof P_3 such that P_3 proves $\Sigma \cup \{\neg\neg w\} \vdash w$.

Now, construct a proof P_4 by taking P_3 followed by P_1. If w is actually used in P_1, then it is mentioned as 'P' in it. In P_4, mention it as 'Th'. This is justified since in the P_3 portion, w has already been proved. The proof P_4 is a proof of $\Sigma \cup \{\neg\neg w\} \vdash p$. If w is not used in P_1, then as it is, P_4 is a proof of $\Sigma \cup \{\neg\neg w\} \vdash p$.

Similarly, construct the proof P_5 by taking P_3 followed by P_2, and change the justification corresponding to the line $\neg w$ in the P_2 portion to 'Th', if necessary. Now, P_5 is a proof of $\Sigma \cup \{\neg\neg w\} \vdash \neg p$.

Therefore, $\Sigma \cup \{\neg\neg w\}$ is inconsistent. By (1), we conclude that $\Sigma \vdash \neg w$.

□

Theorem 1.4 (Finiteness). *Let Σ be a set of propositions, and let w be a proposition. Then the following are true:*

1. *If $\Sigma \vdash w$, then there exists a finite subset $\Gamma \subseteq \Sigma$ such that $\Gamma \vdash w$.*
2. *If Σ is inconsistent, then there exists a finite inconsistent subset of Σ.*

Proof. Left as an exercise. □

Theorem 1.5 (Paradox of Material Implication). *Let Σ be a set of propositions. Then, Σ is inconsistent if and only if $\Sigma \vdash x$ for every proposition x.*

Proof. Left as an exercise. □

1.1 Exercises

1. Assume that $\vdash \neg x \to (x \to y)$. Prove Deduction Theorem by using Reductio ad Absurdum (RAA).
2. Let Σ be a set of propositions. Show that Σ is consistent if and only if there exists a proposition w such that $\Sigma \nvdash w$ and $\Sigma \nvdash \neg w$.

3. **Transitivity**: Let Σ be a set of propositions, and let x, y be propositions. Show that if $\Sigma \vdash x$ and $x \vdash y$, then $\Sigma \vdash y$.

4. Let Σ and Γ be sets of propositions, and let w be a proposition. Let $\Sigma \vdash x$ for each $x \in \Gamma$. Show that if $\Sigma \cup \Gamma \vdash w$, then $\Sigma \vdash w$.