A proof system for propositional logic

Suppose L is a propositional language. Since every formula is tautologically equivalent to one not containing $\wedge, \rightarrow, \leftrightarrow$, we shall only consider such formulas. The set of logical axioms are all formulas of the form $(\neg A \vee A)$, where A is a formula.

The logical inference rules are the following:

(a) Expansion: Infer $(B \vee A)$ from A.

(b) Contraction: Infer A from $(A \vee A)$

(c) Associative rule: Infer $((A \vee B) \vee C)$ from $(A \vee (B \vee C))$

(d) Cut rule: Infer $(B \vee C)$ from $(A \vee B)$ and $(\neg A \vee C)$

where A, B, C are formulas.

Given a set of formulas $\mathcal{A}$, called a theory, a proof from $\mathcal{A}$ is a finite list of formulas

$$A_1, A_2, \ldots, A_n$$

where each A_i is either a logical axiom, belongs to $\mathcal{A}$ or can be inferred from formulas $A_1, \ldots, A_{i-1}$ by the inference rules.

In this case, we say that $A_1, \ldots, A_n$ is a *proof of A_n* from $\mathcal{A}$.

In case a formula B has a proof from $\mathcal{A}$, we say that B is a *theorem* of $\mathcal{A}$ and write $\mathcal{A} \vdash B$. In case $\mathcal{A} = \emptyset$, we just write $\vdash B$.

A set $\mathcal{A}$ is said to be *inconsistent* in case there is a formula B s.t. $\mathcal{A} \vdash B$ and $\mathcal{A} \vdash \neg B$. Otherwise, $\mathcal{A}$ is *consistent*.

Example

$\{A \vee B\} \vdash B \vee A$, i.e., $B \vee A$ is a theorem of the set $\mathcal{A} = \{A \vee B\}$. To see this, we give the following proof:

$$\underset{\text{in } \mathcal{A}}{\underset{\uparrow}{A \vee B}}, \quad \underset{\text{logical axiom}}{\underset{\uparrow}{\neg A \vee A}}, \quad \underset{\text{using cut rule.}}{\underset{\uparrow}{B \vee A}}$$

<u>Example</u> (Modus Ponens)

Suppose $\vdash A$ and $\vdash \neg A \vee B$, i.e., that A and B are theorems of the empty theory. Then also $\vdash B$.

To see this, note that since $\vdash A$ and $\vdash \neg A \vee B$ there are proofs

$$A_1, A_2, \ldots, A_n, A$$

and

$$B_1, B_2, \ldots, B_n, \neg A \vee B \, .$$

Thus, also

$$A_1, A_2, \ldots, A_n, A, B_1, B_2, \ldots, B_n, \neg A \vee B,$$

$$\underset{\substack{\uparrow \\ \text{by expansion} \\ \text{of } A}}{B \vee A}, \quad \underset{\substack{\uparrow \\ \text{axiom}}}{\neg B \vee B}, \quad \underset{\substack{\uparrow \\ \text{cut}}}{A \vee B}, \quad \underset{\substack{\uparrow \\ \text{cut}}}{B \vee B}, \quad \underset{\substack{\uparrow \\ \text{contraction}}}{B}$$

is a proof of B. So $\vdash B$.

<u>Recall</u>: $\mathcal{A} \models A \iff$

for any valuation v, if v satisfies $\mathcal{A}$, then $v(A) = T$.

$\mathcal{A} \vdash A \iff$ there is a proof of A from $\mathcal{A}$.

We shall show that $\mathcal{A} \models A \iff \mathcal{A} \vdash A$.

<u>Theorem</u> Suppose L is a propositional language and A is a formula. Then

$$\vdash A \implies \models A.$$

<u>Pf</u> Suppose $A_1, A_2, \ldots, A_n$ is a proof of $A = A_n$, and let v be any valuation of L. By induction on i, we show that $v(A_i) = T$, whereby also $v(A) = v(A_n) = T$. Since v is arbitrary, A is a tautology, so $\models A$.

Base: Note that A_1 must be a logical axiom, $\neg B \vee B$, so $v(A_1) = v(\neg B \vee B) = T$.

Induction step: Now, suppose ~~that~~ for every $j < i$, $v(A_j) = T$.

Again if A_i is a logical axiom, we have $v(A_i) = T$.

Now, suppose instead that A_i is obtained by inference rules from $A_1, \dots, A_{i-1}$.

Four cases:

Case 1: $A_i = B \vee A_j$ is obtained by expansion from A_j, $j < i$. Then as $v(A_j) = T$, also $v(A_i) = T$.

Case 2: Contraction

Case 3: Associative rule

Case 4: Cut rule

$\square$

As we can see, proofs quickly become unwieldy, so a few general principles are needed:

__Proposition__ Suppose $\mathcal{A}$ is a set of formulas and $A_1, \dots, A_n$ is a sequence s.t. for each i, either A_i is an axiom, $\mathcal{A} \vdash A_i$ or A_i can be inferred from some of A_j, $j < i$, then also $\mathcal{A} \vdash A_n$.

__Proof__ If $\mathcal{A} \vdash A_i$, we can replace A_i in the list $A_1, \dots, A_n$ with a proof $B_1, \dots, B_m, A_i$ of A_i from $\mathcal{A}$. The resulting expanded list is then a proof of A_n from $\mathcal{A}$. $\square$

__Lemma__ (syntactical compactness)

If $\mathcal{A} \vdash A$, then there is a finite set $\mathcal{B} \subseteq \mathcal{A}$ such that $\mathcal{B} \vdash A$.

__Pf__ This is just because any proof of A from $\mathcal{A}$ only uses finitely many formulas of $\mathcal{A}$. $\square$

Soundness Theorem for propositional logic:

If L is a prop. language and $\mathcal{A}$ a set of formulas, B a formula, then

$$\mathcal{A} \vdash B \quad \Rightarrow \quad \mathcal{A} \models B.$$

Similar proof as before.

Lemma If $\vdash A \vee B$ then $\vdash \neg\neg A \vee B$.

Pf We shall use the proposition and just prove $\neg\neg A \vee B$ from $A \vee B$:

$$\underset{\text{axiom}}{\neg\neg A \vee \neg A}, \quad \underset{\text{by an example}}{\neg A \vee \neg\neg A}, \quad \underset{\text{by hyp.}}{A \vee B}, \quad \underset{\text{cut}}{B \vee \neg\neg A},$$

$$\underset{\text{by an example.}}{\neg\neg A \vee B}.$$

$\square$

Lemma Suppose $B_1, \dots, B_n$ are formulas, $1 \leq i < j \leq n$ and $\vdash B_i \vee B_j$. Then

$\vdash B_1 \vee B_2 \vee \dots \vee B_n$ [these parentheses are always put to the right, so $B_1 \vee \dots \vee B_n$ $= B_1 \vee (B_2 \vee \dots \vee (B_{n-1} \vee B_n) \dots)$]

Proof We prove this by induction on $n \geq 2$.

Case $n = 2$. Then $\vdash B_1 \vee B_2$ implies $\vdash B_1 \vee B_2$. ✓

Suppose now it holds for all $n < k$ and now assume $n = k$.

If $i \geq 2$, then, by the induction hypothesis,

$\vdash B_2 \vee \dots \vee B_n$, whence by expansion

$\vdash B_1 \vee \dots \vee B_n$. (Recall, parentheses are put from the right),

If $i = 1$, $j \geq 3$: By the induction hypothesis:

$\vdash B_1 \vee B_3 \vee \dots \vee B_n$, also,

$$B_1 \vee B_3 \vee \dots \vee B_n \;,\; \underset{\text{by example}}{(B_3 \vee \dots \vee B_n) \vee B_1} \;,\; \underset{\text{exp.}}{B_2 \vee ((B_3 \vee \dots \vee B_n) \vee B_1)},$$

$$\underset{\text{associative}}{(B_2 \vee (B_3 \vee \dots \vee B_n)) \vee B_1} \;,\; \underset{\text{example}}{B_1 \vee (B_2 \vee (B_3 \vee \dots \vee B_n))}$$

Since $B_1 \vee (B_2 \vee (B_3 \vee \dots \vee B_n)) = B_1 \vee \dots \vee B_n$, we are done.

If $i=1, j=2$:

$$B_1 \vee B_2 \;,\; \underset{\text{expansion}}{(B_3 \vee \dots \vee B_n) \vee (B_1 \vee B_2)} \;,\; \underset{\text{associative rule}}{((B_3 \vee \dots \vee B_n) \vee B_1) \vee B_2},$$

$$\underset{\text{example}}{B_2 \vee ((B_3 \vee \dots \vee B_n) \vee B_1)} \;,\; \underset{\text{associative rule}}{(B_2 \vee (B_3 \vee \dots \vee B_n)) \vee B_1},$$

$$\underset{\text{example}}{B_1 \vee (B_2 \vee (B_3 \vee \dots \vee B_n))}$$

$\boxed{}$

Lemma Let $m, n \geq 1$ and $1 \leq i_1, i_2, \dots, i_m \leq n$.

Suppose $\vdash A_{i_1} \vee A_{i_2} \vee \dots \vee A_{i_m}$.

Then $\vdash A_1 \vee A_2 \vee \dots \vee A_n$.

Proof The proof is by induction on m uniformly for all formulas A_i.

Let also $B = A_1 \vee A_2 \vee \dots \vee A_n$.

$m=1$ Set $i = i_1$. So by assumption $\vdash A_i$.

Now, the following is a proof of B from A_i:

$$A_i, \quad \underbrace{(A_{i+1} \vee \dots \vee A_n) \vee A_i}_{\text{expansion}}, \quad \underbrace{A_i \vee (A_{i+1} \vee \dots \vee A_n)}_{\text{by example}},$$

$$A_{i-1} \vee A_i \vee A_{i+1} \vee \dots \vee A_n, \quad A_{i-2} \vee A_{i-1} \vee A_i \vee A_{i+1} \vee \dots \vee A_n,$$

$\dots$, $A_1 \vee \dots \vee A_n$ (by repeated expansion).

$m=2$ Suppose first $i_1 = i_2$. Since $\vdash A_{i_1} \vee A_{i_2}$, also $\vdash A_{i_1}$ (by contraction), so $\vdash B$ by case $m=1$.

Now, suppose $i_2 < i_1$. Then as $\vdash A_{i_1} \vee A_{i_2}$, also $\vdash A_{i_2} \vee A_{i_1}$, so we can suppose $i_1 < i_2$.
But then the result follows from the previous lemma.

<u>Case $m > 2$:</u>

Since $\vdash A_{i_1} \vee (A_{i_2} \vee (A_{i_3} \vee \ldots \vee A_{i_m}))$

by the associative law

$$\vdash (A_{i_1} \vee A_{i_2}) \vee (A_{i_3} \vee \ldots \vee A_{i_m}).$$

Applying the induction hypothesis to $B_{i_1} = (A_{i_1} \vee A_{i_2})$ and $B_{i_2} = A_{i_3}, \ldots, B_{i_{m-1}} = A_{i_m}$, we have

$$\vdash (A_{i_1} \vee A_{i_2}) \vee \underbrace{(A_1 \vee \ldots \vee A_n)}_{=B}$$

example $\vdash B \vee (A_{i_1} \vee A_{i_2})$

association $\vdash (B \vee A_{i_1}) \vee A_{i_2}$

by case $m = 2$:

$$\vdash (B \vee A_{i_1}) \vee B$$

$$\vdash B \vee (B \vee A_{i_1})$$

ass. $\vdash (B \vee B) \vee A_{i_1}$

case $m=2$ $\vdash (B \vee B) \vee B$

case $m=2$ $\vdash (B \vee B) \vee (B \vee B)$

contra. $\vdash B \vee B$

contra. $\vdash B$

$\square$