10 Axiom system for propositional logic

Resolution provides a procedure for verifying contradictions, and hence, tautologies. For Mathematical logic, a 'generating' view is taken rather than a verification: axioms are supplied, and tautologies are verified by being deduced from the axioms. The system is due to Frege (I think): anyway, it is the system covered in Mendelson's book.

A *logical system* involves *formulae, axioms,* and *rules of inference.* Resolution is an example of a rule of inference. Our system for propositonal logic uses *modus ponens,* which is a restricted form of resolution.

Formulae are built using the two connectives $\neg$ and $\implies$. Since $X \vee Y$ is equivalent to $(\neg X) \implies Y$, and $X \wedge Y$ is equivalent to $\neg(X \implies \neg Y)$, any CNF can easily be translated into a formula using only these connectives. Therefore the two connectives $\neg$, $\implies$, are adequate for expressing all truth-functions.

There are three groups of *logical axioms* in our system. Each group represents infinitely many axioms, since A, B, and C can be any formula:

(I) $A \implies (B \implies A)$

(II) $(A \implies (B \implies C)) \implies ((A \implies B) \implies (A \implies C))$

(III) $((\neg B) \implies (\neg A)) \implies (((\neg B) \implies A) \implies B)$

(10.1) Lemma *Every logical axiom is a tautology.*

Sketch proof. Easily proved by analysing the truth-tables of each logical axiom. ∎

There is one rule of inference:

Modus ponens.[1] From A and $A \implies B$, deduce B.

Systems may also include some extra *proper axioms.*

Supposing that Γ is the set of proper axioms, possibly empty, and Z a formula, a *deduction or proof of Z from Γ in the system* is a finite sequence of formulae with justifications, where the justification of each step A is that either

- A is a logical axiom,
- A is a proper axiom, i.e., $A \in \Gamma$, or
- A is deduced from two earlier formulae B and $B \Rightarrow A$ by Modus Ponens.

and Z occurs in one of the steps of the proof. We write

$$\Gamma \vdash Z \quad \text{or} \quad \Gamma \vdash_{\text{SC}} Z$$

when Z can be deduced from Γ, and

$$\vdash Z \quad \text{or} \quad \vdash_{\text{SC}} Z$$

when $\emptyset \vdash Z$. In this case, i.e, $\Gamma = \emptyset$, Z is called a *theorem* (of SC).

[1]This is a restricted kind of resolution.

(10.2) Definition *A system of the above kind, with logical axioms I–III and Modus ponens, is called a* sentential calculus. *When there are no proper axioms, we call the system a* pure *sentential calculus.*

(10.3) Lemma *Suppose $\Gamma \vdash Z$, a particular proof being given. Let I be an intepretation of all the Boolean variables occurring in Γ and in the formulae occurring in the proof. Suppose*

$$I(A) = 1 \text{ for all } A \in \Gamma.$$

Then $I(Z) = 1$. In particular if $\vdash Z$ then Z is a tautology.

Proof. (By induction on the length of the given proof.) If Z is a proper axiom then $I(Z) = 1$. If Z is a logical axiom then it is a tautology (this is easily checked with truth-tables), so $I(Z) = 1$. If Z is deduced from earlier formulae A and $A \Rightarrow Z$, then $I(A) = 1$ and $I(A \implies Z) = 1$. Now, if Z were false under I, then since A is true, $A \implies Z$ would be false (from the truth-table). It isn't: $I(A \implies Z) = 1$. Therefore $I(Z) = 1$ also. ∎

Now to prove our first theorem within the system.

(10.4) Lemma $\vdash A \Rightarrow A$.

Proof. The following is a proof of $A \implies A$.

1. $(A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$ (Axioms II).
2. $A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$ (Axioms I).
3. $((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$ (1,2, MP).
4. $(A \Rightarrow (A \Rightarrow A))$ (Axioms I).
5. $A \Rightarrow A$ (3,4, MP). ∎

(10.5) Corollary $(\neg A \implies A) \vdash A$

Proof.

1. $(\neg A) \implies \neg A$ Lemma 10.4
2. $((\neg A) \implies \neg A) \implies (((\neg A) \implies A) \implies A)$ (Axiom III)
3. $((\neg A) \implies A) \implies A$ (1,2,MP)
4. $(\neg A) \implies A$ (Given)
5. A (4,3,MP). ∎

(10.6) In mathematical proofs, in order to prove $A \Rightarrow B$, it is customary to assume A and deduce B. In fact, this is almost the invariable practice. The following simple yet very important result shows that the practice is a very useful short-cut, and is correct.

Note that the 'opposite' of the Deduction Theorem is true, and easy to prove.

(10.7) Lemma *If $\Gamma \vdash A \Rightarrow B$ then $\Gamma, A \vdash B$.* ∎

(10.8) Theorem (the Deduction Theorem for Sentential Calculus).
If $\Gamma, A \vdash B$ then $\Gamma \vdash A \Rightarrow B$.

Proof. By induction on the length of proofs. In proofs of length 1 either (i) $B = A$, (ii) $B \in \Gamma$, or (iii) B is a logical axiom.

In case (i) $\Gamma \vdash A \Rightarrow B$ by Lemma 10.4.
In cases (ii) and (iii), $\Gamma \vdash B$, and $\Gamma \vdash B \Rightarrow (A \Rightarrow B)$ (Axioms I), so $\Gamma \vdash A \Rightarrow B$ by MP.

For the inductive step, suppose that B is the formula given in the $n+1$st step of a proof. If B is justified under cases (i)–(iii) above, the same arguments apply. Otherwise (iv) B arises from using MP from two previous formulae in the proof, so $\Gamma \vdash C$ and $\Gamma \vdash C \Rightarrow B$ in a proof of length $\leqslant n$. By induction

$$\Gamma \vdash A \Rightarrow (C \Rightarrow B) \qquad \text{and} \qquad \Gamma \vdash A \Rightarrow C.$$

Since

$$\Gamma \vdash (A \Rightarrow (C \Rightarrow B)) \Rightarrow (A \Rightarrow C) \Rightarrow (A \Rightarrow B)$$

(Axioms II), $\Gamma \vdash A \Rightarrow B$ by two applications of MP. This completes the inductive step. ∎

(10.9) Corollary *Implication is transitive, i.e.,*

$$A \implies B, B \implies C \vdash A \implies C$$

Proof.
1. A hypothesis
2. $A \implies B$ given
3. B 1,2,MP
4. $B \implies C$ given
5. C 3,4,MP.

Thus, $A, A \implies B, B \implies C \vdash C$, so by the Deduction Theorem, $A \implies B, B \implies C \vdash A \implies C$. ∎

The goal of this section is to prove that Sentential Calculus is sound and complete in the following sense.

(10.10) Theorem *A formula S is a tautology if and only if $\vdash S$.*

This will be proved by connecting SC with resolution proofs. The main point is that resolution can be imitated in SC.

(10.11) Lemma $\neg\neg A \vdash A$

Proof. 1. $\neg\neg A$ given
2. $\neg A \implies \neg\neg A$ 1, I, MP
3. $\neg A \implies \neg A$ Lemma 10.4
4. $(\neg A \implies \neg\neg A) \implies ((\neg A \implies \neg A) \implies A)$ III
5. A 2,3,4, MP twice. ∎

(10.12) Lemma (counterpositive). $(A \implies B) \vdash (\neg B) \implies (\neg A)$

Proof. It is enough to prove $A \implies B, \neg B \vdash \neg A$.
1. $(\neg\neg A) \implies A$ (Lemma 10.11)
2. $A \implies B$ given
3. $(\neg\neg A) \implies B$ 1,2,Transitivity
4. $\neg B$ given
5. $(\neg\neg A) \implies \neg B$ I,4,MP
6. $\neg A$ 5,3,III, MP twice. ∎

(10.13) Lemma $A \vdash \neg\neg A$

Proof: exercise.

(10.14) Definition *Two formulae B and B' in SC are* equivalent in SC *if $B \vdash B'$ and $B' \vdash B$.*

(10.15) Corollary (subformula substitution).[2] *Suppose A, B, B' are formulae where B, B' are equivalent in SC. Let A' be the formula obtained from A by replacing some occurrences of B in A by B'. Not all occurrences of B need be replaced by B'. Then A and A' are equivalent in SC.*

Sketch proof. The proof is by induction on the length of A. If A is a boolean variable then if B is the same variable then $A = B$ and $A' = A$ or $A' = B'$. The result holds in this case.

If A is $\neg C$ then A' is $\neg C'$ where by induction we can assume that C and C' are equivalent in SC. Thus

$$C \vdash C' : \quad \vdash C \implies C' : \quad \vdash (\neg C') \implies (\neg C)$$

by Lemma 10.12. By symmetry, $\vdash (\neg C') \implies (\neg C)$.

If A is $(C \implies D)$, then A' is $(C' \implies D')$. By induction, assuming A, $C' \implies C$ and $D \implies D'$, so by transitivity, $C' \implies D'$: $A \vdash A'$. Similarly $A' \vdash A$. ∎

(10.16) Definition *We introduce $\vee$, $\wedge$, and $\iff$ and define them in terms of $\neg$ and $\implies$ as follows.*

$$\begin{aligned} (A \vee B) &= (\text{definition}) \quad (\neg A) \implies B \\ (A \wedge B) &= (\text{definition}) \quad (\neg((\neg A) \vee (\neg B))) \\ (A \iff B) &= (\text{definition}) \quad (A \Rightarrow B) \wedge (B \Rightarrow A) \end{aligned}$$

(10.17) Lemma (i) $B \vdash A \vee B$
(ii) $\vee$ *is commutative, i.e.,* $A \vee B \vdash B \vee A$
(iii) $A \vdash A \vee B$
(iv) $A \wedge B \vdash A$
(v) $A \wedge B \vdash B$
(vi) $A, B \vdash A \wedge B$

[2] This had been accidentally deleted.

(vii) $\wedge$ *is associative*
(viii) $\vee$ *distributes over* $\wedge$
(ix) $\wedge$ *is commutative and* $\vee$ *is associative*
(x) $\wedge$ *distributes over* $\vee$

Proof. (i) $B \vdash A \vee B$ from I and MP.

(ii) Suppose $A \vee B$, i.e., $(\neg A) \implies B$.

1. $(\neg A) \implies B$ given
2. $(\neg B) \implies \neg\neg A$ (Lemma 10.12)
3. $(\neg B) \implies A$ (2, Lemma 10.11, transitivity)

i.e. $B \vee A$ as required.

(iii) Immediate from (i) and (ii).

(iv) Suppose $A \wedge B$, i.e., $\neg((\neg A) \vee (\neg B))$.

1. $(\neg A) \implies ((\neg A) \vee (\neg B))$ from (iii)).
2. $(\neg((\neg A) \vee (\neg B))) \implies \neg\neg A$ (1, Lemma 10.12), i.e.

$A \wedge B \implies \neg\neg A$. 3. $\neg\neg A \implies A$ (Lemma 10.11).
By transitivity, $A \wedge B \implies A$, which is equivalent to (iv).

(v) Similarly, using commutativity of $\vee$.

(vi) Let X be $\neg\neg A \implies \neg B$, so $\neg X$ is identical to $A \wedge B$.

1. A (given)
2. X (hyp)
3. $\neg\neg A$ (1, Lemma 10.13)
4. $\neg B$ (3,2,MP)
5. $\vdash X \implies \neg B$ (1–4,DT)
6. $\neg\neg B \implies \neg X$ (Lemma 10.12)
7. B (given)
8. $\neg\neg B$ (7, Lemma 10.13)
9. $\neg X$ (8,6,MP) as required.

(vii – ix): exercises.

(x) can be deduced from (viii), proof omitted. ∎

(10.18) Lemma (resolution valid in SC). $L \vee A, (\neg L) \vee B \vdash A \vee B$. *(Here A or B can be empty, but not both).*

Proof. 1. $L \vee A \vdash L \vee A \vee B$ Above lemmas.

2. $L \vee A$ (Given.)
3. $L \vee A \vee B$ (1,2,MP).
4. $(\neg L) \implies A \vee B$ (Equivalent)
5. $\neg(A \vee B) \implies L$ Counterpositive, equivalents
6. $(\neg L) \vee B$ (given). By steps similar to 1...5,

x. $\neg(A \vee B) \implies \overline{L}$.
y. $(\neg(A \vee B) \implies \overline{L} \implies \neg(A \vee B) \implies L) \implies (A \vee B)$ Axiom III.
z. $A \vee B$ (5, x, y, MP twice. ∎

(10.19) Lemma *Let A be a formula of SC. One can convert A to a provably equivalent CNF.*

Proof. It is assumed that A uses only the connectives $\neg, \Rightarrow$.

We first make substitutions which convert A into a genuine CNF G, in which $\neg, \vee, \wedge$ are primitive connectives, rather than one in which $\vee, \wedge$ are expressed in terms of $\neg, \Rightarrow$.

- First, convert $X \Rightarrow Y$ to $(\neg X) \vee Y$ throughout. This yields a formula using only $\neg, \vee$.
- Then replace formulae $\neg(X \vee Y)$ by $(\neg X) \wedge \neg Y$, and $\neg(X \wedge Y)$ by $(\neg X) \vee \neg Y$. Also replace $\neg\neg X$ by X throughout.

  When no further alterations of this kind are possible, we have a formula which consists of $\vee, \wedge$, and literals.
- Replace subformulae $X \vee (Y \wedge Z)$ by $(X \vee Y) \wedge (X \vee Z)$, and $(X \vee Y) \wedge Z)$ by $(X \vee Z) \wedge (Y \vee Z)$.

This should result in a formula in CNF. One can get it into a more regular form by replacing $(X \vee Y) \vee Z)$ by $X \vee (Y \vee Z)$, and $(X \wedge Y) \wedge Z$ by $X \wedge (Y \wedge Z)$.

Then G is a CNF where the conjunction is arranged as

$$C_1 \wedge (C_2 \wedge \ldots \wedge C_N)$$

and every disjunction has the form

$$L_1 \vee (L_2 \vee \ldots \vee L_k).$$

Finally, rewrite every occurrence of $\wedge, \vee$ in terms of $\neg, \implies$. This gives a correct formula of SC, which is provably equivalent using Lemmas 10.17 and 10.15. ∎

(10.20) Corollary *If X, a formula of SC, is a tautology, then it is a theorem of SC.*

Proof. By applying valid transformations to $\neg X$, we can get a CNF Z', where

$$Z' \quad \text{is provably equivalent to } \neg X \text{ in SC}$$

Z' has the form

$$C_1 \wedge C_2 \wedge \ldots C_N$$

(Parentheses are unnecessary because $\wedge$ is associative.) From this, the separate clauses $C_1, C_2, \ldots, C_N$ can be deduced in SC (Lemma 10.17 (iv),(v)).

Since resolution is valid in SC (Lemma 10.18), every step in a resolution refutation, except the last, can be simulated in SC. The last step can't be simulated, since $\square$ is outside the scope of SC; so the last step would be to infer $\square$ from L and $\overline{L}$ where L is a literal.

Since L and $\overline{L}$ can be derived from $C_1, \ldots, C_N$ by repeated resolution, they can be derived in SC:

$$C_1, \ldots, C_N \vdash L \quad \text{and} \quad C_1, \ldots, C_N \vdash \neg L$$

for some literal L. Therefore

$$Z' \vdash L$$

so

$$\vdash Z' \implies L$$

by the Deduction Theorem. Since Z' and $\neg X$ are equivalent,

$$\vdash \neg X \implies L.$$

Similarly

$$\vdash \neg X \implies \neg L.$$

Using

$$((\neg X \Rightarrow \neg L) \rightarrow (\neg X \rightarrow L)) \implies X,$$

and MP twice, we have completed a proof of X in SC. $\blacksquare$