8 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 propositional logic uses modus ponens, which is a restricted form of resolution.

Formulae are built using the two connectives ¬ and →. Since X ∨ Y is equivalent to (¬X) → Y, and X ∧ Y is equivalent to ¬(X → ¬Y), any CNF can easily be translated into a formula using only these connectives. Therefore the two connectives ¬, →, 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 → (B → A)
(II) (A → (B → C)) → ((A → B) → (A → C))
(III) ((¬B) → (¬A)) → (((¬B) → A) → B)

(8.1) 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. From A and A → 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 ∈ Γ, or
- A is deduced from two earlier formulae B and B → A by Modus Ponens.

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

Γ ⊢ Z or Γ ⊩_{SC} Z

when Z can be deduced from Γ, and

⊢ Z or ⊩_{SC} Z

when ∅ ⊢ Z. In this case, i.e, Γ = ∅, Z is called a theorem (of SC).

1This is a restricted kind of resolution.
(8.2) 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.

(8.3) Lemma Suppose $\Gamma \vdash Z$, a particular proof being given. Let $I$ be an intepretation of all the Boolean variables occurring in $\Gamma$ and in the formulae occurring in the proof. Suppose $I(A) = 1$ 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 $I(A \rightarrow Z) = 1$. Now, if Z were false under I, then since A is true, $A \rightarrow Z$ would be false (from the truth-table). It isn’t: $I(A \rightarrow Z) = 1$. Therefore $I(Z) = 1$ also. Q.E.D.

Now to prove our first theorem within the system.

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

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

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). Q.E.D.

(8.5) Corollary $(\neg A \Rightarrow A) \vdash A$

Proof.

$\neg A \Rightarrow A$ given

$\neg A \Rightarrow \neg A$ Lemma 8.4

A (2,1,III,MP twice) Q.E.D.

(8.6) 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 just a convenient short-cut.

(8.7) 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 8.4.

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 \( \leq n \). By induction

\[
\Gamma \vdash A \Rightarrow (C \Rightarrow B) \quad \text{and} \quad \Gamma \vdash A \Rightarrow C.
\]

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. **Q.E.D.**

**8.8 Corollary** *Implication is transitive, i.e.,*

\[
A \Rightarrow B, B \Rightarrow C \Rightarrow C
\]

**Proof.**

1. \( A \) hypothesis
2. \( A \Rightarrow B \) given
3. \( B \) 1,2,MP
4. \( B \Rightarrow C \) given
5. \( C \) 3,4,MP, 

Thus, \( A, A \Rightarrow B, B \Rightarrow C \Rightarrow C \), so by the Deduction Theorem, \( A \Rightarrow B, B \Rightarrow C \Rightarrow A \Rightarrow C \). **Q.E.D.**

**8.9 Implication and deduction.** Suppose \( A \Rightarrow B \). By the Deduction Theorem, \( \vdash A \Rightarrow B \). Suppose \( \vdash A \Rightarrow B \). By Modus Ponens, \( A \Rightarrow B \). Thus, in Sentential Calculus, if we can prove \( A \Rightarrow B \) then we can deduce \( B \) from \( A \), and vice-versa.

Our aim is

**8.10 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.

**8.11 Lemma** \( \neg
\neg A \vdash A \)

**Proof.**

1. \( \neg
\neg A \) given
2. \( \neg
A \Rightarrow \neg
A \) 1, I, MP
3. \( \neg
A \Rightarrow \neg
A \) Lemma [S.4]
4. \( \neg
A \Rightarrow \neg
A \Rightarrow (\neg
A \Rightarrow \neg
A) \Rightarrow (\neg
A \Rightarrow \neg
A) \Rightarrow A \) III
5. \( A \) 2,3,4, MP twice. **Q.E.D.**

**8.12 Lemma (counterpositive).** \( (A \Rightarrow B) \vdash (\neg B) \Rightarrow (\neg A) \)

**Proof.** It is enough to prove \( A \Rightarrow B, \neg B \vdash \neg A \).

1. \( (\neg
A) \Rightarrow A \) (Lemma [S.11])
2. \( A \Rightarrow B \) given
3. \( (\neg
A) \Rightarrow B \) 1,2,Transitivity
4. \( \neg
B \) given
5. \( (\neg
A) \Rightarrow \neg
B \) I,4,MP
6. \( \neg
A \) 5,3,III, MP twice. **Q.E.D.**
(8.13) Lemma \( A \vdash \neg\neg A \)

Proof: exercise.

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

(8.15) Corollary (subformula substitution). 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 \( A \equiv B \) and \( A' \equiv B' \). 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

\[
C \vdash C' : \vdash C \implies C' : \vdash (\neg C') \implies (\neg C)
\]

by Lemma 8.12. 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 \( A' \vdash A \). Q.E.D.

(8.16) Definition We introduce \( \lor, \land, \text{ and } \equiv \) and define them in terms of \( \neg \) and \( \implies \) as follows.

\[
\begin{align*}
(A \lor B) &= \text{(definition)} \quad (\neg A) \implies B \\
(A \land B) &= \text{(definition)} \quad (\neg((\neg A) \lor (\neg B))) \\
(A \equiv B) &= \text{(definition)} \quad (A \implies B) \land (B \implies A)
\end{align*}
\]

(8.17) Lemma (i) \( B \vdash A \lor B \)

(ii) \( \lor \) is commutative, i.e., \( A \lor B \vdash B \lor A \)

(iii) \( A \vdash A \lor B \)

(iv) \( A \land B \vdash A \)

(v) \( A \land B \vdash B \)

(vi) \( A, B \vdash A \land B \)

(vii) \( \land \) is associative

(viii) \( \lor \) distributes over \( \land \)

(ix) \( \land \) is commutative and \( \lor \) is associative

(x) \( \land \) distributes over \( \lor \)

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

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

1. \( (\neg A) \implies B \) given

2. \( (\neg B) \implies \neg A \) (Lemma 8.12)
3. \((-B) \implies A\) \(\text{(2, Lemma 8.11, transitivity)}\)

i.e. \(B \lor A\) as required.

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

(iv) Suppose \(A \land B\), i.e., \((-((-A) \lor (-B))).

1. \((-A) \implies \((-A) \lor (-B))\) from (iii).

2. \((-((-A) \lor (-B))) \implies -A\) \((1, \text{Lemma 8.12)}, \text{i.e.})\)

By transitivity, \(A \land B \implies A\), which is equivalent to (iv).

(v) Similarly, using commutativity of \(\lor\).

(vi) Let \(X\) be \(-A \implies -B\); so \(-X\) is identical to \(A \land B\).

1. \(A\) (given)

2. \(X\) (hyp)

3. \(-A\) \((1, \text{Lemma 8.13})\)

4. \(-B\) \((3, 2, \text{MP})\)

5. \(\vdash X \implies -B\) \((1-4, \text{DT})\)

6. \(-B \implies -X\) \((\text{Lemma 8.12})\)

7. \(B\) (given)

8. \(-B\) \((7, \text{Lemma 8.13})\)

9. \(-X\) \((8, 6, \text{MP})\) as required.

(vii–ix): exercises.

(x) can be deduced from (viii), proof omitted. \textbf{Q.E.D.}

\textbf{(8.18) Lemma (resolution valid in SC).} \(A \lor L, B \lor -L \vdash A \lor B\). (Here \(A\) or \(B\) can be empty, but not both).

\textbf{Proof.}

1. \(-A\) hyp

2. \(A \lor L\) given, i.e. \((-A) \implies L\)

3. \(L\) \((1, 2, \text{MP})\)

4. \(B \lor -L\) given

5. \((-L) \lor B\), i.e., \(L \implies B\) \((\lor \text{commutative})\)

6. \(B\) \((3, 5, \text{MP})\). In other words,

\[ A \lor L, B \lor -L, -A \vdash B \] (DT). In other words, \(A \lor L, B \lor -L \vdash A \lor B\). \textbf{Q.E.D.}

\textbf{(8.19) Corollary} If \(X\), a formula of \(SC\), is a tautology, then it is a theorem of \(SC\).

\textbf{Proof.} By applying valid transformations to \(-X\), we can get a CNF \(Z'\), where

\[ Z' \] is provably equivalent to \(-X\) in \(SC\)

\(Z'\) has the form

\[ C_1 \land C_2 \land \ldots C_N \]
(Parentheses are unnecessary because $\land$ is associative.) From this, the separate clauses $C_1, C_2, \ldots, C_N$ can be deduced in SC (Lemma 8.17 (iv),(v)).

Since resolution is valid in SC (Lemma 8.18), every step in a resolution refutation, except the last, can be simulated in SC. The last step can’t be simulated, since $\Box$ is outside the scope of SC; so the last step would be to infer $\Box$ 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

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

and MP twice, we have completed a proof of $X$ in SC. Q.E.D.