8
The Axiomatic Method of Hoare

This chapter discusses the verification method of Hoare, well known for proving the partial correctness of while-programs. This method is usually presented in the form of a calculus, the so-called Hoare calculus. Essentially this approach is identical with the inductive assertions method introduced in the last chapter, as may become plausible from the following considerations. The inductive assertions method can be used on while-programs, since every while-program can be easily transformed to an equivalent flowchart program. Because this translation produces flowchart programs of a special form—namely flowchart programs without interleaved loops—the inductive assertions method can be simplified. This simplified form leads naturally to a calculus, namely the Hoare calculus. In the last section it will be seen how (a slight variant of) the well-founded sets method can be likewise incorporated in the Hoare calculus to achieve a method for proving the total correctness of while-programs.

8.1 Hoare Logic and Hoare Calculus

The Hoare calculus is a calculus for a logic, called Hoare logic, in which one can formulate propositions about the partial correctness of while-programs. This logic will now be introduced. Just as in the definition of the while-programming language, the definition of the Hoare logic builds on the predicate logic.

**Definition 8.1 (Syntax of Hoare Logic)** Let $B$ be a basis for predicate logic. A *Hoare formula* over the basis $B$ is an expression of the form

$\{p\} S \{q\}$

where $p, q \in WFF_B$ are formulas of the predicate logic and $S \in L^B_2$ is a while-program.

The set of all Hoare formulas over the basis $B$ will be denoted by $HF_B$. Unlike the predicate logic where there were two sorts of syntactic objects—terms and formulas—here there is only one (new) object, the Hoare formula.
Thus the semantics of the Hoare logic need only describe the meaning of Hoare formulas.

**Definition 8.2 (Semantics of Hoare Logic)**  Let an interpretation $I$ of a basis $B$ for predicate logic be given, and let $\Sigma$ be the corresponding set of states. Every Hoare formula $\{p\} S \{q\} \in HF_B$ is mapped by a semantic functional—also denoted $I$—to a function

$$\mathcal{I}(\{p\} S \{q\}): \Sigma \rightarrow \text{Bool}$$

defined as follows:

$$\mathcal{I}(\{p\} S \{q\})(\sigma) = \text{true} \quad \text{iff} \quad \mathcal{I}(p)(\sigma) = \text{false}, \quad \text{and if} \quad \mathcal{M}_I(S)(\sigma) \text{ is defined,} \quad \text{then} \quad \mathcal{I}(q)(\mathcal{M}_I(S)(\sigma)) = \text{true}. \quad \Box$$

It is naturally a matter of indifference whether the meaning $\mathcal{M}_I(S)$ of the program $S$ is defined by operational or denotational semantics.

Analogously to the predicate logic, the Hoare formula $\{p\} S \{q\}$ is said to be **valid** in an interpretation $I$—denoted

$$I \vdash I \{p\} S \{q\}$$

—if $\mathcal{I}(\{p\} S \{q\})(\sigma) = \text{true}$ for all states $\sigma \in \Sigma$. If $I \vdash I \{p\} S \{q\}$ for all interpretations $I$, then the Hoare formula is called **logically valid**; this fact is denoted

$$I \vdash \{p\} S \{q\}.$$

A Hoare formula is called a **logical consequence** of a set $W \subseteq WFF_B$ of formulas of the predicate logic—denoted

$$W \vdash \{p\} S \{q\}$$

—if $I \vdash I \{p\} S \{q\}$ holds for all models $I$ of $W$.

Notice that $\mathcal{I}(\{p\} S \{q\})(\sigma)$ is true whenever $\mathcal{I}(p)(\sigma)$ is false—like $\mathcal{I}(p \supset q)(\sigma)$ in the predicate logic—or whenever $\mathcal{M}_I(S)(\sigma)$ is undefined. This is why $I \vdash I \{p\} S \{q\}$ means exactly that $S$ is partially correct with respect to the formulas $p$ and $q$ in the interpretation $I$. Thus Hoare logic essentially expresses partial correctness.

**Example 8.3** (1) Let $\{p\} S \{q\}$ be the Hoare formula

$$\{x > 5\} \ x := 2 \ast x \ \{x > 20\}.$$

Then in the usual interpretation $I$:

$$\mathcal{I}(\{p\} S \{q\})(\sigma) = \text{true} \quad \text{iff} \quad \mathcal{I}(p)(\sigma) = \text{false}, \quad \text{or} \quad \mathcal{I}(q)(\mathcal{M}_I(S)(\sigma)) = \text{true} \quad \text{iff} \quad \sigma(x) \leq 5, \quad \text{or} \quad \mathcal{M}_I(S)(\sigma)(x) > 20 \quad \text{iff} \quad \sigma(x) \leq 5, \quad \text{or} \quad \sigma(x) > 10.$$