前言

软件产品的功能对社会的各方面起着重要的作用。很多产品有着非常复杂的结构。因而软件的生产需要理论上的支持以构建可靠的软件系统。计算机科研人员在形式验证的理论和算法方面做了长期的研究，积累了丰富的程序正确性验证方面的知识。

程序正确性的最终体现就是给定的程序以及程序的计算环境所组成的软件系统具备我们期望的性质、不出现我们不期望出现的问题。

程序正确性的形式验证是基于系统模型的。通过程序与系统的建模，我们将给定的程序以及程序的计算环境所组成的软件系统抽象为模型，用形式语言进行描述，又通过形式语言的语义定义，将其描述的模型对应于软件系统的运行。对于我们期望软件系统具备的性质，我们将这样的性质用逻辑公式表示，进而查看系统模型和这些逻辑公式的关系。因此通过形式验证进行的程序正确性验证的主要过程为用形式语言为程序与系统建立模型、用逻辑公式描述程序性质、然后是用形式验证方法证明系统模型是否具备所声明的性质。

形式验证的主要问题就是对于给定一个系统模型和一些逻辑公式，用严格的方法证明所给定的系统模型是否能够满足这些逻辑公式。验证的方法主要包括推理验证和模型检测。程序推理验证的理论工作在上世纪六十、七十年代取得了奠基性的成果。但是由于程序推理的复杂性，推理证明只能证明系统满足给定的性质。而对于不能证明的性质，推理验证在一般情况下，不能确定是性质不满足或是证明的思路不对或证明的过程过于复杂。对于并发系统而言，由于其计算过程的复杂以及系统性质的多样，基于程序推理的验证更加困难。八十年代兴起的模型检测研究试图寻求有效的算法来验证系统和系统性质的关系。模型检测已被应用于计算机硬件、软件、通信协议、控制系统、安全认证协议等领域，成为分析、验证并发系统性质的最重要的技术。

本书结合推理验证方法和模型检测方法介绍形式验证方面的基楚知识。分五个部分：预备知识，程序与系统模型、程序逻辑、推理验证方法、模型检测方法。具体内容如下：

（ 1 ）预备知识部分包括逻辑、集合、关系、函数和有向图等内容。

（ 2 ）程序与系统模型部分包括隐式迁移系统、显式状态迁移系统、标号迁移系统、时间迁移系统、 Petri 网、通讯系统等内容。

（ 3 ）程序逻辑部分包括线性时序逻辑、分枝时序逻辑、 μ- 演算等内容。

（ 4 ）推理验证方法部分包括卫式迁移系统的推理、流程图程序的推理、结构化程序的推理等内容。

（ 5 ）模型检测方法部分包括基于状态分析的模型检测、基于路径分析的模型检测、限界模型检测等内容。