

王少辉：模型检测：原理与应用（2008）

本文介绍了模型检测技术的基本原理，并且通过实际应用的例子说明了如何解决模型检测技术中的关键问题。文章首先介绍了模型检测技术中的形式化建模、形式化描述和形式化验证这三个主要问题。在形式化建模部分，通过简单例子深入介绍了使用Kripke结构和Petri网建立模型的方法，给出了两种模型的形式化定义，比较了两种模型的不同，并给出了将Petri网模型转换成Kripke模型的方法。在形式化验证部分，介绍了时态逻辑的语法和语义，并说明了模型检测技术的基本任务和实现原理。在此基础上，文章介绍了两种常用的模型检测和系统分析工具SMV和SMART。文章后半部分包括两个对系统形式化建模和验证的实例：IEEE 1394通信协议和航天器控制系统。在IEEE 1394通信协议建模和验证的工作中，文章对他人先前的建模进行了改进，使得模型行为能更好地描述实际系统。同时文章还使用SMART工具对模型进行了形式化验证。在航天器控制系统的验证工作中，文章使用软件工具对现有系统进行建模，为进一步找出现有系统中的那些不能用传统测试方法找到的问题提供了可能。