模型检测技术的发展研究

杨茜茜
西南交通大学，四川乐山　614200

摘　要　模型检测（model checking）是一种能够自动验证有限状态并发系统的技术。该文从模型检测技术的背景入手，先阐述了模型检测技术基本原理及其相关过程。而后介绍了阻碍模型检测技术发展的状态爆炸问题，再者对 NuSMV、SPIN 和 UPPAAL 等模型检测工具进行了介绍与比较。最后总结了模型检测技术在新的领域、工具研制、算法研究和与其他技术相结合等几个方面的研究进展，可为今后进一步对计算机硬件、通信协议、控制系统、安全认证协议等方面的分析与验证中提供借鉴。

关键词　模型检测技术；形式化验证；状态爆炸；状态约简；研究进展
中图分类号　TP3　　**文献标识码**　A　　**文章编号**　2095-6363（2016）10-0019-001

1 模型检测研究背景

当今的工业系统规模越来越大，如集成电路、电子系统、软件系统等，如果设计过程中的缺陷不被发现，将对系统运行带来隐患，尤其是在高速铁路以及核电站等关键领域。传统的模拟和测试技术已经不能满足对系统设计有效性的保证，亟须一种新的方法来有效地保证复杂系统开发过程中的正确性。

2 模型检测发展历程

模型检测最早由 Clarke 和 Emerson 以及 Quielle 和 Sifakis 在 1981 年分别提出，在亚里士多德时期就有了用自然语言来进行时序分析，A.Pnueli 在 1977 年首先提出对并发程序的推理使用线性时序逻辑。直到 20 世纪 80 年代初期，时序逻辑模型检测算法的引入使该类型的推理可以自动化进行。

3 模型检测的基本原理和过程

模型检测是对给定的一个程序或系统和一些性质用严格的模型方法证明程序是否满足给定的性质。设 M 为一个 Kripke 结构，f 为一个时序逻辑公式，找出 M 的所有状态 s，是否均满足下列的公式：

$$M,s=f^{[1]}$$

在描述程序性质 f 时使用程序逻辑。程序逻辑可分为两类：线性时序逻辑（LTL）和计算树逻辑（CLT）。

其检验原理如图 1 所示：

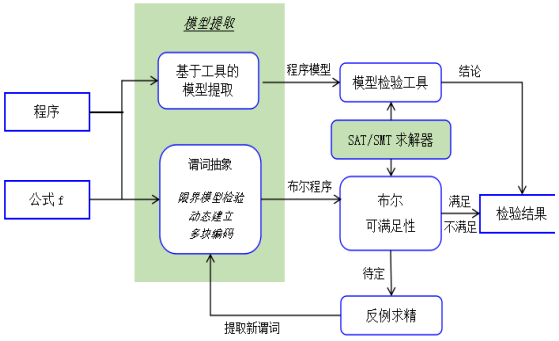

图1　模型检验原理图

模型检测是基于对状态空间的穷举搜索，其主要的缺点是状态爆炸，对于这一缺点，科学家们首先想到的是通过缩减状态空间的方法来减少其计算量，如符号模型检测、偏序规约、程序切片、对称模型检测等技术。

4 模型检测关键技术

4.1　谓词抽象

谓词抽象技术由 Saidi 和 Gref 在 1997 年提出。该项技术实现了将无穷状态系统自动映射到有穷的状态系统，而且在谓词抽象的软件模型检测基础上有效地结合了定理与模型检测技术。在该项技术中，抽象状态对应在该状态上成立的谓词公式的所有集合。

4.2　反例求精

有效的抽象应该满足如下 1 个条件：1）产生的抽象模型足够小，这样才可以使模型检测有效完成；2）生成的模型要精细，否则就不可保证在模型中保留所需的检测信息。而且在抽象的模型检测中，还有一个目标就是抽象系统的自动生成。通过反例求精技术自动生成抽象系统。

4.3　布尔可满足性

布尔可满足性是解决给定的布尔程序，是否存在一组变量赋值使问题为可满足的，或是给出证明该函数在任何赋值下都为假，即是不可满足的。布尔可满足性原理广泛应用于计算机科学基础理论、算法、人工智能、硬件设计等。

4.4　限界模型检验（BMC）

BMC 的基本思想是在有限的局部空间中逐步搜索属性成立的证据，或者失效的反例，从而达到约简状态空间的目的。BMC 技术的提出主要用来解决状态爆炸问题。BMC 适合于查错，即在规定步数内找到系统的错误状态，解决了 BDD 技术无法解决的许多问题。

5 模型检测的工具

模型检测技术可以实现对待检测系统的自动验证，到现在已研究出了诸多模型检测工具。一般常用的模型检测工具主要有 SMV、NuSMV、Spin 和 UPPAAL 等。

5.1　NuSMV 工具

NuSMV 是由卡内基梅隆大学和意大利科学技术研究中心在基于 SMV 上联合研发的，该工具从系统的功能和实现方案上对 SMV 进行了一定的扩展和升级，并且同时将界模型检测算法引入其中。

↓↓（下转第22页）↓↓

作者简介：杨茜茜，本科在读，西南交通大学。

2）评分计算方法。（1）舰船损管指挥命令应用效果评分计算。将指挥体系中下达的第 i 个指令的指挥权重表示为 Wi，并将其所处的损害难度系数表示为 N_i，应用该指令的可产生的贡献度值为 Q。当该指令被顺利完成后，其任务指标 T 的计算公式主要包含以下 2 种情况：当贡献度值 Qi 为正数时：$T_i=N_i \cdot W_i \cdot Q_i$；

当贡献度值 Qi 为负数时：$T_i=\frac{WQ_i}{N_i}$

在舰船的整个损管过程中，由指挥体系所下达的命令总数为 m 条，因此，该过程中每条命令的完成度指标 Y 的计算公式如下：$Y=\sum_{i=1}^{n} T_i / \sum_{i=1}^{m} T_i$

在该模型中，所使用的第一部分舰船损管资源管理分数的计算公式为：

$M_1=Y \times 0.6 \times 70$

在上述公式中，舰船损管指挥兵力为 e，第 j 个被调度使用的指挥兵力在整个过程中完成命令任务为 m_j，该兵力的实际任务指标值为 C_j。P 表示被调度使用的舰船损管兵力的平均任务密度，ρ_{max} 则表示其中最忙碌的单元。

第二部分舰船损管兵力的实际调度分数计算公式为：

$M_2=B_{-1} \cdot 70 \cdot 0.25$

第三部分舰船舱室排水效果的计算公式为：

$$V=\frac{\sum_{k=1}^{a} V_{bk}}{\sum_{k=1}^{a} V_{0k}}$$

在该公式中，a 表示该舰船中所有进水舱室的总数；Vb 表示该舰船中所有舱室的实际进水体积；V0 表示该舰船中所有舱室的中体积[6]。因此，可以将第三部分舰船舱室排水效果处理的分数表示为：

$M_3=(1-\frac{V_b}{V_0}) \times 70 \times 0.25$

因此，应用舰船损管指令的效果分数为：$M=M_1+M_2+M_3$

该指挥员所进行的舰船损管指挥训练的分数计算公式为：$Mark=M+M_{ship}$

3）舰船状态参数评分计算。

舰船状态参数分数计算公式为：

$M_{ship}=20\alpha W \frac{W}{W_0}+30\alpha H \frac{H}{H_0}+30(1-\frac{\min\{\theta|\theta_0\}}{|\theta_0|})+30\alpha F \frac{F_{min}}{F_{min0}}$

在该公式中，W 表示舰船的储备浮力；H 表示舰船横稳度；θ 表示舰船横倾斜角；F_{min} 表示舰船干舷高度的最小值；α 表示舰船的实际评估权重。

4 结论

舰船受损事故的发生不仅会对人们的人身安全产生影响，还会带来一定的经济损失，因此需要通过舰船损管指挥训练的进行对由舰船受损事故带来的影响进行合理控制。为了对训练效果进行有效分析，可以将舰船损管中涉及的舰船损害规模、舰船损管兵的调度使用等重要因素作为评估要素，结合这些评估要素构件舰船损管指挥训练评估模型。

参考文献

[1]陈晓洪，任凯，金卫东.舰船损管指挥训练评估体系模型的构建方法[J].江苏船舶，2010（2）：5-8，47.

[2]郑环宇，吴晞，韩晓光.损管训练模拟系统在舰船中的应用研究[J].舰船电子工程，2010（12）：116-119.

[3]任凯，浦金云.利用OpenGL实现舰船损管虚拟训练舱实时操作的方法[C]//.中国科学技术协会.节能环保和谐发展——2007中国科协年会论文集（一），中国科学技术协会，2007：6.

[4]吴晞，韩晓光.舰船长损管决策指挥训练模拟系统设计与实现[J].舰船电子工程，2014（9）：82-85，103.

[5]于多.舰船破损进水识别及破舱稳性计算方法研究[D].大连：大连理工大学，2008.

[6]李骆.舰船火灾结构建模及消防系统故障分析研究[D].哈尔滨：哈尔滨工程大学，2012.

（上接第19页）

5.2 Spin 工具

Spin 工具是由美国学者霍尔茨曼研发出的另一种模型检测工具。并于 2001 年荣获了 ACM 软件系统奖，该工具可检测有限状态系统是否满足线性时序逻辑公式和其他性质。

5.3 UPPAAL 工具

UPPAA 是实时系统的模型检测工具。该工具以时间自动机作为系统的实现模型，并以 μ－算子时间扩展作为解释说明语言，同时运用约束求解来解决系统无穷状态的空间难题，采用 on-the-fly 技术解决状态爆炸问题。

6 结论

模型检测技术作为一种对有限状态反应式系统的自动检验技术已被广泛地应用于通信、计算机硬件、控制系统和安全认证等诸多广大领域，并且取得了瞩目的成功。本文从模型检测技术的相关背景入手，阐述了该项技术主要原理和发展状况，同时对比分析了模型检测的几种基本工具，为今后进一步研究相关技术提供参考和借鉴。

参考文献

[1]王红.软件资源竞争的模型检验方法研究[J].计算机应用技术，2015（5）：5-8.

[2]Edmund M.Clarke Jr.Orna Grumberg Doron A.Peled.Model Checking.The MIT Press，January，2000.

[3]化希耀，苏博妮.模型检测技术研究综述[J].塔里木大学学报，2013（12）：119-124.