

高可靠软件研究： 向信息技术的未来投资

林惠民

软件研究所计算机科学重点实验室 北京 100080)

摘要 随着社会对信息技术的依赖性日益增长,如何提高处于信息技术核心的计算机软件的可靠性成为一个紧迫的问题。测试仍然是目前工业界广泛采用的确认软件是否正确可靠的主要手段,而形式化方法被认为是非常有希望的新途径。高可靠软件的研究将直接影响到下一代软件技术的形成。

关键词 信息技术,高可靠软件,测试,形式化方法



信息技术的飞速进步极大地推动了社会生产力的发展,并深刻地改变着人类生活和工作方式。处于信息技术核心的计算机软硬件系统越来越深地渗入了社会生活的各个方面。从银行到自动生产线,从人事管理到导弹控制,从

医疗到购物,我们正在前所未有的规模上,以前所未有的速度依赖于计算机系统,特别是软件系统。

任何新技术都是双刃剑。在我们讴歌计算机软硬件技术给人类社会带来巨大进步的同时,也应当清醒地认识到这种技术可能产生的负面作用。由于我们对计算机软件的高度依赖,一旦软件失效将可能造成难以估量的损失。很多人都曾遭遇到由于 Windows 突然“死机”而造成的文件丢失,导致数小时或数天工作前功尽弃的不愉快经历。由于软件失效造成通讯系统中断的报道屡见不鲜。今年 7 月 3 日深圳证交所因计算机系统故障而停止交易,7 月 25 日北京首都机场由于类似原因造成乘客无法登机,有半天时间航班不能起飞。这是最近发生在我们身边的例子。

软件常常出错的重要原因在于其生产仍然是手工进行的,并且至今仍然缺乏成熟的生产标准。多数的软件产品在发布时依然含有已经查出但尚未排除的错误,更不用说还没有查出的缺陷了。也就是说,人们所使用的大量软件是“带病运行”的。

1999 年美国信息技术总统顾问委员会组织力量对美国信息技术的现状进行大规模的调查,向白宫呈递了一份题为“信息技术研究:向未来投资”的长达 80 页的报告。报告列举了因软件缺陷造成的大量问题,惊呼美国“所依赖的软件往往是脆弱的、不可靠的,其开发、测试和演化极为困难,极费人工。”报告对美国政府提出的首要建议是“将软件基础研究列为绝对的优先”^[1]。这份报告对西方信息技术基础研究产生了广泛和深远的影响。美国国家自然科学基金会在 2000 财政年度启动了迄今为止规模最大的“信息技术研究”计划,重点是软件基础研究。据美国国家科学与技术委员会 2001 年的“信息技术:21 世纪的革命”白皮书报道,在 2001 财政年度美国信息技术支持的 6 个研究领域中软件就占了两个(“软件设计与生产率”和“高可靠性软件与系统”)^[2]。

1 可靠性是衡量软件质量的首要指标

软件产品的质量包括正确性 是否具有用户要

* 收稿日期:2002 年 10 月 11 日

求的功能)、可靠性(不出错,少出错)、友善性(是否易于使用)、可维护性和可扩充性(维护升级和增加新功能是否方便)以及时空效率(运行时所需的时间和空间资源)诸方面。其中正确性和可靠性是衡量软件质量的首要指标。

软件与其它产品不同,软件不会磨损,不会疲劳,因此,不会因长期使用损耗而造成可靠性降低。软件失效的原因在于内在的缺陷。这种缺陷在软件产品交付使用时就已经存在。因此,提高可靠性的关键在于软件的生产过程。

软件的生产过程包括需求分析、设计、编程、测试几个阶段。需求分析的任务是了解用户对软件产品的要求,形成产品所应具备的功能的明确描述。这种描述通常称为“规约”。在设计阶段,工程师根据规约确定软件的构架,将系统分解成大小适度的模块,并给出各模块的实现方案。编程阶段的任务则是将设计产生的方案用选定的程序语言编成程序。上述每一阶段都可能产生错误。测试的任务是尽可能地排除错误。

测试仍然是目前工业界广泛采用的确认软件是否正确可靠的主要手段。软件测试是对一组选定的输入数据运用被测软件,将所产生的输出与预期的结果比较,如不相符则说明被测软件含有错误,需要修正。测试极为耗工耗时。在大型软件企业(如微软),测试人员与编程人员的比例达到 2:1,即一个人编的程序需要两个人测试。比尔·盖茨曾为此而感叹:微软快变成测试公司了。即使这样,出厂的软件产品中仍然含有许多缺陷。因为测试有其固有的局限性。软件大师、国际计算机科学基础研究的最高奖 ACM 图灵奖获得者 Dijkstra 有一句名言:“测试只能证实错误的存在,而不能证明没有错误。”这是因为测试数据不可能穷尽所有可能的输入,因此,无法保证在实际运行中遇到其它数据时不出问题。另外,并发系统(如网络上运行的软件)由于不同进程间的相互影响和制约而具有“非确定性”,即对同样的初始数据,第二次运行可能会得到与第一次运行不同的结果。因此,测试对并发软件的作用极为有限。

2 形式化方法与软件可靠性

如何保证软件的正确性和可靠性是一项非常

困难的基础研究。研究人员在这一领域已进行 30 多年的艰苦探索。在所提出的各种可能的理论和方法中,形式化方法被认为是非常有希望的途径。这里“形式化”指的是严格的数学符号和理论。形式化方法的基本点在于软件的主体——计算机程序是形式对象。程序是由一组基本指令(语句)复合而成的。每个语句都有严格的形式和意义。这里的主要困难在于:当程序的规模达到上百万行甚至上千万行语句时,其意义将复杂到人脑难以把握的程度。如何对各种类型的程序给出简明的语义,并发展有效的方法对复杂程序进行基于语义的检查和推理,是形式化方法研究的中心课题。近几年来,基于逻辑理论的模型检测技术取得了重大进展,开始应用于解决实际问题。

形式化方法目前的应用范围主要是那些安全性、可靠性至关重要的系统,如航天飞机、导弹、核电站等。这些要求“万无一失”的系统其关键软件模块一般说来需求说明比较明确,规模不是很大(1 万行代码上下),但是程序的控制结构复杂,通常涉及并发性与实时性,容易在设计和编程阶段出错。

美国国家航天局 Ames 研究中心的一个研究小组应用形式化方法,在 1998 年对基于人工智能的航天器控制系统构架的执行器模块(称为“新纪元远程主体”)进行了分析,他们将该模块的程序用手工翻译到模型检测工具 SPIN 的界面语言 Promela,然后用 SPIN 进行自动分析和检测。结果发现该软件中含有 5 个潜在的错误。执行器模块的设计和实现人员对此十分惊讶,因为作为航天控制系统中的一个关键部件,该模块已经经受了大量、严格的测试和模拟。他们认为这 5 个错误若不用形式化方法几乎不可能查出,并且其中有 4 个是致命的。

在这一工作中,形式化方法所起的作用与测试类似,是在全部代码完成后,用逆向工程的方法建模,然后交给模型检测工具,查出错误后再对设计和程序进行修改。这种事后进行分析与验证的方式,不仅要修改设计,还要修改已按照原设计编写好的程序,代价比较高。更为有效的做法是在设计阶段就引入形式化方法,在保证设计正确后再着手编程。这需要设计人员与分析/验证人员密切配合。

从事形式化方法研究的人员来自各国一流大

学和研究所。欧盟 ITEA 计划 (Information Technology for Europe Advancement) 于 2001 年 3 月发表了题为“软件密集系统技术展望”的报告^[1], 在展望软件工程技术发展趋势时, 形式化方法被列为将在近期、中期和长期起作用的技术。值得注意的是, 该报告的执笔者均来自欧洲各大信息技术公司 (Philips, Alcatel, IMEC, Nokia 等), 而不是学术界。这从一个侧面反映了欧洲信息工业界对形式化方法的期望。

3 应加强我国高可靠软件的研究

在我国, 高可靠软件的研究虽然起步较晚, 但已在某些方面 (如实时与混成系统的描述与验证, 传值并发系统的理论与工具等) 做出了令国际同行瞩目的工作。不过从整体上讲, 我们与欧美相比还有很大的差距。关于高可靠软件的研究涉及到计算模型、语义理论、分析与验证算法以及支撑工具等各个层面, 是综合性很强的基础研究。从近期看, 其

研究成果将对航天、军事等领域的软件研制起积极作用; 从长远看, 这方面的进展将直接影响到下一代软件技术的形成。这是当前计算机科学基础研究中一个非常活跃的领域, 目前国际上尚未形成广泛接受的理论和方法。加强高可靠软件的研究, 力争在新一代软件技术的形成过程取得主动权, 从而为我国软件产业实现跨越式发展提供技术保证, 是现阶段我国从事软件基础研究的科研人员义不容辞的历史使命。

主要参考文献

- 1 PITAC Reports to the President. <http://www.itrd.gov> ("Publications").
- 2 Supplement to the President's budget. <http://www.itrd.gov> ("Publications").
- 3 Technology Roadmap on Software Intensive Systems. <http://www.itea-office.org>.

Research on High Reliability Software: Investing into the Future of Information Technology

Lin Huimin

Laboratory for Computer Science, Institute of Software, CAS, 100080 Beijing)

As our society more and more relies on information technology, it is an urgent issue to enhance the reliability of computer software which lies at the heart of information technology. While testing is still currently the most widely used validation technique in the software industry, formal methods are regarded a new promising approach. Research on high reliability software is shaping the future of software technology.

林惠民 中国科学院院士, 软件研究所计算机科学重点实验室主任, 研究员。1947 年 11 月 13 日生于福建省福州市。1982 年 2 月获福州大学计算机软件专业学士学位, 1986 年 6 月获中国科学院软件研究所计算机科学理论专业博士学位。长期从事计算机程序, 特别是开发程序的形式语义学及形式化方法的研究。在进程代数的验证工具、消息传递进程的语义理论和 π -演算的公理化等方向上取得了一系列国际领先水平的成果, 是国际上有影响的计算机科学家, 多次在重要国际会议上做特邀报告, 1996 年获中国科学院自然科学奖一等奖(惟一获奖人)。