软件故障诊断探讨

单锦辉　徐克俊
(兰州市 27 支局 15 信箱 14 号　732750)

摘　要: 软件在国民经济和社会生活中发挥着重要作用。软件出现故障可能造成严重危害。但是,目前尚未明确提出软件故障诊断的概念,缺乏对软件故障诊断的系统深入研究。当前硬件系统故障诊断的研究和实践都取得了较大的进展。本文分析软件故障产生的原因和软件失效机理,介绍各种硬件系统故障诊断技术,并对软件故障诊断进行了初步的探讨。

关键词: 软件故障; 故障诊断; 故障检测; 故障定位; 故障排除
中图分类号: TP311

引　言

随着社会的不断进步和计算机科学技术的飞速发展,计算机应用越来越广泛。作为计算机的灵魂,软件起着举足轻重的作用。软件一旦出现故障,有可能造成巨大的危害。例如,1996 年 Ariane 5 运载火箭的发射失败是由软件故障引起的[1]。因此,研究如何诊断软件故障具有重要意义。

目前国内外开展了与软件故障诊断有关的研究。文献[2]将软件故障定义为计算机程序中不正确的步骤、处理或者数据定义。文献[3]将软件故障定义为软件运行过程中出现的一种不希望或不可接受的内部状态。文献[4]则将软件故障分为语法大小和语义大小,语法大小为受一个故障影响的代码行数,语义大小为其输出不正确的输入空间的大小。文献[5]将软件故障定义为软件系统中的结构不完善,它可能导致系统的最终失效。

文献[6]认为软件故障模型是软件物理错误的抽象,是一些基本故障的组合。已有的研究工作建立了以下软件故障模型[7]: ①根据错误发生阶段分类,有需求分析错误、概要设计错误、详细设计错误、编码错误等; ②根据故障引起后果分类,有小错误、中等错误、较严重错误、严重错误、非常严重错误、最严重错误; ③根据错误性质分类,有需求错误、功能和性能错误、结构错误、数据错误、实现和编码错误、集成错误、测试错误等; ④根据错误类型分类,有文档错误、语法错误、联编打包错误、赋值错误、接口错误、数据错误、函数错误、系统错误、环境错误等。文献[8]针对 C 语言程序建立以下几种故障模型:坏的存储分配、内存泄漏故障、初始化变量错误、指针和越界指针的引用错误、数组越界错误、非法算术运算错误、整数或浮点数错误、非法类型转换错误、不可达代码错误等。

但是,总体来看,目前尚未明确提出软件故障诊断的概念,也没有系统地开展软件故障诊断技术的研究,甚至软件故障的概念都比较模糊,与软件错误、缺陷、失效等概念相混淆。

当前硬件系统故障诊断研究和实践取得了较大的进展,并且有大量的成功案例。我们认为,软件故障诊断可以借鉴硬件系统故障诊断的思路。本文在分析现有硬件系统故障诊断技术的基础上,对软件故障诊断进行初步探讨。

1　硬件系统故障诊断技术

当前硬件系统故障诊断研究和实践取得了较大的进展。硬件系统故障诊断过程包括故障检测、故障分离、故障治理与预防等步骤。故障检测是采集系统运行参数,获取系统状态信息,为系统进行状态分析、状态识别奠定基础,提供条件。故障分离是根据故障检测所获得的系统状态信息进行故障分析,以识别系统是否存在故障,识别故障特性进行故障隔离,即对故障定位。治理与预防,是指根据故障诊断的结果,采取有针对性的纠正措施,消除故障;或者预测未来、决定防治潜在故障发生的维修对策。

收稿日期: 2007-04-30
第一作者: 男,1970 年生,高级工程师,博士
E-mail: shanjh@163.com

硬件系统故障诊断的技术一般可按方法复杂程度、检测手段和方法理论基础进行分类。

1.1 按方法复杂程度分类

按故障诊断方法的复杂程度分类,可分为简易诊断和精密诊断。简易诊断是初级诊断,一般由现场人员实施,对监测结果不作进一步的处理和分析。当简易诊断发现设备或系统存在异常时,应转入精密诊断。

精密诊断是对异常设备或系统进行的精确诊断。精密诊断不仅要对检测数据作进一步处理、分析,确认设备或系统是否存在故障,还要检测、隔离故障,分析产生故障的原因和机理,判断故障性质和程序,提出治理和预防的措施。

1.2 按检测手段分类

按检测手段分类,故障诊断可分为以下 6 种。

(1)直接观察诊断法。根据人的经验,对设备状态进行直接观察判断的方法称为直接观察法。

(2)性能参数测定法。通过测定系统或设备的性能参数来判定系统或设备状态的方法称为性能参数判定法。性能参数一般包括电信号、磁特性、功率、物体运动、系统特征量、机械设备性能等。

(3)无损检测诊断法。对被测设备不造成损坏的非接触式检测方法称为无损检测诊断法,一般包括声、光、热等检测方法。主要用于一些无法或不便于安装接触式传感器的设备故障的诊断。

(4)振动与噪声测定诊断法。振动与噪声测定诊断法通过测量振动体的位移、速度、加速度,以及振动的频率、周期、相位角、频谱图等,对设备的故障进行诊断。

(5)高低温诊断法。通过设置高温环境或低温环境,对设备性能进行测定的方法称为高低温诊断法。

(6)化学成份测定法。通过测定设备零部件或元器件内部化学成份来判定设备故障的方法称为化学成份测定法。

1.3 按方法理论基础分类

按故障诊断方法理论基础,可分为以下 3 类。

(1)基于模型的诊断方法。核心思想是用解析冗余取代硬件冗余,通过构造观测器估计出系统的输出值,将其同输出测量值相比较,从中获取故障信息。基于模型的诊断方法一般可分为基于参数估计的诊断方法和基于状态估计的诊断方法两种。

基于参数估计的故障诊断方法的思路是:由机理分析确定系统的模型参数和物理元器件参数之间的关系方程 $u = f(v)$,由实时辨识求得系统的实际模型参数 u',由 $u = f(v)$ 和 u' 求解实际的物理元器件参数 p',将 p 和 p' 的标称值比较从而得知系统是否有故障及故障的程度。

基于状态估计的故障诊断方法现已形成三种基本方法:①Beard 提出的故障检测滤波器的方法;②Menra 和 Peshon 提出的基于卡尔曼滤波器的方法、Dlark 提出的构造卡尔曼滤波器阵列;③Deckert 提出的一致性空间的方法。

(2)基于信号的诊断方法。核心思想是利用信号模型,如相关函数、频谱等,提取诸如方差、幅值、频率等特征值,检测出故障。基于信号的诊断方法一般可分为:直接测量系统输入输出方法、小波变换方法、主元分析方法和基于信号融合的方法。

(3)基于知识的诊断方法。基于知识的诊断方法将诊断对象作为一个有机整体被研究,以知识处理技术为基础,诊断问题的求解致力于通过模拟领域专家在推理过程中控制和运用各种诊断知识的行为而获得解决。基于知识的诊断方法一般可分为:专家系统诊断法、模糊故障诊断法、基于故障树的故障诊断法、基于神经网络的故障诊断法和基于智能体的故障诊断法。

2 软件失效机理

明确软件失效机理是软件故障诊断的前提。由于软件内部逻辑复杂,运行环境动态变化,且不同的软件差异可能更大,因而软件失效机理常常有不同的表现形式。但总的来说,软件失效机理可以描述为:软件错误→软件缺陷→软件故障→软件失效的过程[3]。

2.1 软件错误(software error)

软件错误是指在软件生存周期内的不希望或不可接受的人为错误,其结果是导致软件缺陷的产生。可见软件错误是一种人为过程,相对于软件本身,是一种外部行为。

例如,考虑一个 C 语言程序,对用户任意输入的 10 个整数,采用冒泡排序算法进行排序,结果按照不减序排列。正确的程序为

```
void Bubble_Sort()
{
  int temp, i, j, X[10];
  scanf("%d %d %d %d %d %d %d %d %d %d",
```

```
    &X[0], &X[1], &X[2], &X[3], &X[4],
    &X[5], &X[6], &X[7], &X[8], &X[9]);
  for (i = 0; i <= 8; i++)
    for (j = 0; j <= 8; j++)
      if (X[j] > X[j+1]){
          temp = X[j];
          X[j] = X[j+1];
          X[j+1] = temp;
      }
  printf("%d, %d, %d, %d, %d, %d, %d, %d, %d, %d",
          X[0], X[1], X[2], X[3], X[4],
          X[5], X[6], X[7], X[8], X[9]);}
```

如果由于人为错误,将外层 for 循环的循环控制变量 i 的终值错误地由"8"写成了"7",这就是一个软件错误。

2.2 软件缺陷(software defect)

软件缺陷是存在于软件(文档、数据、程序)之中的那些不希望或不可接受的偏差,其结果是软件运行于某一特定条件时出现软件故障,此时称软件缺陷被激活。当软件意思是指程序时,软件缺陷(defect)与软件污点(bug)同义。

仍然考虑上面的冒泡排序程序。由于将外层 for 循环的控制变量 i 错误地由"8"写成"7",导致一个软件缺陷产生。软件缺陷是存在于软件内部、静态的一种行为。

2.3 软件故障(software fault)

软件故障是指软件运行过程中出现的一种不希望或不可接受的内部状态。出现软件故障时若无适当措施加以及时处理,便产生软件失效。显然,软件故障是一种动态行为。

例如,对于以上包含缺陷的冒泡排序程序,对于输入数据〈9,1,1,1,1,1,1,1,1,0〉,在外层 for 循环执行结束之后,printf 语句执行之前,数组 X 的值为〈1,0,1,1,1,1,1,1,1,9〉,此时软件出现故障。

2.4 软件失效(software failure)

软件失效是指软件运行时产生的一种不希望或不可接受的外部行为结果。在上述软件故障例子中,由于没有容错措施,所以将得到一个不可接受的程序输出:"1,0,1,1,1,1,1,1,1,9",这便是一个软件失效。而正确的排序结果应该是"0,1,1,1,1,1,1,1,1,9"。

综上所述,软件错误是一种人为错误。一个软件错误必定产生一个或多个软件缺陷。当一个软件缺陷被激活时,便产生一个软件故障。同一个软件缺陷在不同条件下被激活,可能产生不同的软件故障。出现软件故障时如果没有及时的容错措施加以处理,便不可避免地导致软件失效。

3 软件故障诊断

本文认为,软件故障诊断是根据软件(包括程序、数据和文档)的静态表现形式和动态运行状态信息查找故障源,并确定相应决策的一门技术。

人在参与软件生存周期的各个阶段工作时都难免会出现错误。因此,从广义上说,软件故障诊断的目标包括软件需求分析、设计、编码、测试、使用、维护等各阶段所造成的缺陷,所采用的软件评审等也属于软件故障诊断的手段。

软件故障诊断,"诊"在于进行客观的状态检测,包括采用各种测量、分析和诊别方法;"断"则需要确定软件故障特性、软件故障模式、软件故障部位,以及说明软件故障产生的原因,并且提出相应的纠正措施和预防措施等,这是软件诊断技术的关键。软件故障诊断突出了诊断的目的性,即寻找和发现软件故障状态而进行诊断,也包括无故障状态在内,但强调故障状态的重要性。

软件故障诊断的过程包括故障检测、故障定位、故障排除、回归测试、系统测试和交付等几个阶段。软件故障检测是软件故障诊断的第一步,通过静态检查、动态运行等方法获取软件中的各种信息,获得可能出现软件故障的征兆,识别软件是否正常运行或存在故障,并为软件故障定位提供依据。

软件故障定位,是指根据软件故障检测提供的能反映软件状况的征兆或特征参数的变化情况,或与某故障状态参数(模式)进行比较,并进一步收集软件的历史和使用信息,识别软件是否正常运行或存在故障,复现软件故障过程,诊断软件故障的性质和程度、产生原因或发生部位,确定缺陷,为纠正缺陷、排除软件故障做好准备。

软件故障排除是指当诊断出软件中存在缺陷,就其原因、部位和危险程度进行研究,决定纠正缺陷、排除故障的办法,包括修改程序代码、数据或软件文档等。软件故障排除属于软件维护的范畴。

一般来说,在工程应用中进行软件故障诊断的前提是:系统故障经分析、检测确认不是由硬件故障引起,或重点怀疑是由软件故障引起。盲目地进行

软件故障诊断将影响系统故障诊断效率。系统出现复杂故障时,也可结合硬件检测,同时进行软件静态检测,这样可以提高系统故障诊断速度。

4 结束语

软件在国民经济和社会生活中发挥着重要作用。软件出现故障会给人们造成很大的危害。研究软件故障诊断具有重要意义。本文研究了软件和硬件的区别,分析软件故障产生的原因和软件失效机理。当前硬件系统故障诊断的研究和实践取得较大的进展,本文在介绍现有硬件系统故障诊断技术的基础上,对软件故障诊断进行了初步探讨。

在今后的工作中,我们将进一步深入研究软件故障的特点和各种硬件系统故障诊断技术,分析硬件系统故障诊断案例,研究软件故障诊断技术,并且应用于软件故障诊断实践。

参考文献:

[1] WEYUKER E J. Testing component-based software: A cautionary tale[J]. IEEE Software, 1998, 15(5): 54-59.

[2] IEEE. IEEE Std 610.12-1990[G]// IEEE standard glossary of software engineering terminology. December, 1990.

[3] 蔡开元. 软件可靠性工程基础[M]. 北京: 清华大学出版社, 1995.

[4] OFFUTT A J, HAYES J H. A semantic model of program faults[C]//Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA'96), San Diego, CA, USA, January, 1996: 195-200.

[5] MUNSON J C, NIKORAB A P, SHERIF J S. Software faults: A quantifiable definition[J]. Advances in Engineering Software, 2006, 37(5): 327-333.

[6] 朱荣, 徐拾义. 软件测试中故障模型的建立[J]. 计算机工程与应用, 2003, 17: 69-71,91.

[7] 郑人杰. 计算机软件测试技术[M]. 北京: 清华大学出版社, 1992.

[8] 宫云战. 一种面向故障的软件测试新方法[J]. 装甲兵工程学院学报, 2004, 18(1): 21-25.

[9] 齐治昌, 谭庆平, 宁洪. 软件工程[M]. 北京: 高等教育出版社, 2001.

[10] 黄锡滋. 软件可靠性、安全性与质量保证[M]. 北京: 电子工业出版社, 2002.

A discussion about software fault diagnosis

SHAN JinHui XU KeJun

(No.14, P.O.Box 15, Sub-post Office 27, Lanzhou, Gansu 732750, China)

Abstract: While rapid progress has been made in the research and practice of hardware fault diagnosis, the concept of software fault diagnosis, on the other hand, is not clearly defined yet, and diagnosing technologies of software fault have not been studied systematically and thoroughly. This paper compares the differences between software and hardware, analyzes the causes of software faults and the mechanism of software failure, introduces various kinds of diagnosis technologies for hardware fault, and makes a preliminary investigation of software fault diagnosis issue.

Key words: software fault; fault diagnosis; fault detection; fault localization; fault removal