

72-73, 56

计算机科学 1994Vol. 21No. 2

分布式计算机

故障

诊断

14

分布式系统级故障诊断概况 TP338.8

蔡兵 周六丁 陈廷槐

(重庆大学计算机研究所 重庆 630044)

摘要 This paper describes the history and the present case of distributed system-level fault diagnosis, including the successes which have been obtained and the problems which need to be solved.

关键词 Distributed systems, System-level fault diagnosis, Diagnosis algorithm, Syndrome, Diagnosability.

一、引言

系统级故障诊断的概念自从 1976 年由 Preparata, Metze 和 Chien 提出以来,有关系统级故障诊断的问题得到了越来越多的重视,并取得了迅猛的发展。故障诊断最初只局限于对单个元器件的故障与无故障状态进行检测,后来随着系统规模的不断扩大,特别是大规模、超大规模集成电路系统的出现,对某种复杂部件(如微处理机)的状态的检测却越来越需要。所谓系统级故障诊断是指对系统中各种部件都进行诊断,包括微处理机。由于处理机相对于其它部件来说更重要且更敏感,因此在讨论系统级故障诊断时,多是指有关系统中处理机的故障诊断。

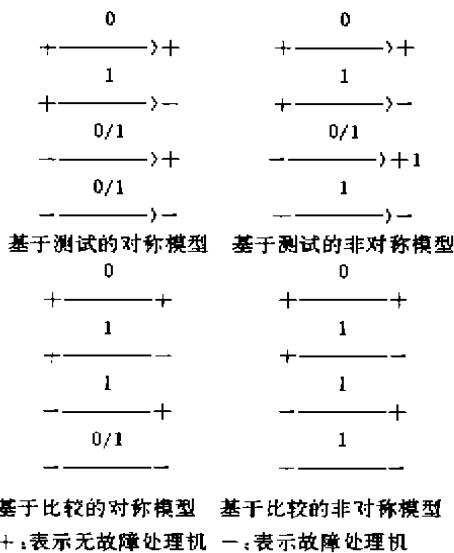


图 1

系统级故障诊断来源于实际,已从复杂的实际情况中抽象出了很多种模型,主要有四种:基于测试的对称模型、基于测试的非对称模型、基于比较的对称模型、基于比较的非对称模型,分别如图 1 所示,其中 PMC 模型属于基于测试的对称模型, BGM 模型属于基于测试的非对称模型, Chaw & Hakimi 模型属于基于比较的对称模型, Malek 模型属于基于比较的非对称模型。

系统级故障诊断可分为两大类:集中式诊断和分布式诊断,有关它们的含义在本文中都有所述,它们按研究方法又可分为二类,一类是一步 t -故障诊断(即假定系统中故障处理机数不超过 t 时,在一次诊断过程中,将系统中所有故障处理机全部确定),一类是顺序 t -故障诊断(即假定系统中故障处理机数不超过 t 时,在一次诊断过程中,找到至少一个故障处理机,然后将这个处理机替换掉,再重复前面诊断过程,直到将系统中所有故障处理机全部确定),显然一步 t -故障诊断更有吸引力;另外,它们也可按所依据的测试策略分为二类,一类是非自适应故障诊断(即测试在诊断前已全部完成),一类是自适应故障诊断(即测试与诊断是同步进行的,下一步测试的进行依赖于上一步测试的结果),由此可见,自适应故障诊断效率更高。

分布式故障诊断虽然发展的历史不长,但它一出现就显示了广阔的应用前景,为系统级故障诊断开辟了新的研究方向,为系统级故障诊断注入了新的活力,由于分布式故障诊断自身的特点,使它在实际应用方面已取得比集中式诊断更多的成果。

蔡兵 博士生,主要研究兴趣:计算机网络、故障诊断、计算机安全与保密。

二、发展历史

系统级故障诊断的概念是首先由 Preparata、Metze 和 Chien 三人于 1967 年提出的,其基本思想是系统中各处理机通过互相测试,获得一个系统中各处理机的测试结果集(即症候),把这个测试结果集送给一个系统外的高可靠处理机,由这个高可靠处理机对所获得的测试结果集进行处理,最后得到有关这个系统中的各处理机的状态(即故障或无故障)。这实际上是一种集中式的故障诊断方法,需要一个高可靠的外部处理机,这在实际系统中是不适宜的假设。

随着分布式系统应用的日益广泛,使得用户对分布式系统的可靠性的要求也越来越高。为了提高分布式系统的可靠性(即容错度),目前主要有两种方法:基于系统冗余的方法和基于故障诊断的方法。系统冗余的方法是在分布式系统中,用不只一个处理机对同一任务进行处理,然后通过一个表决器对这些结果进行表决,从而得到这一任务的处理结果;基于故障诊断的方法主要由以下四步构成:a. 故障探测, b. 故障诊断, c. 系统重组以隔离故障或修复故障, d. 系统恢复。系统冗余的方法会造成系统中资源的利用率下降,因此不是最佳的选择。基于故障诊断的方法包括基于自诊断的方法和基于系统级诊断的方法。基于自诊断的方法是系统中的处理机自己运行一段诊断程序,对自己进行诊断,这种方法的不足是可靠程度不高;而基于系统级诊断的方法是通过系统中其它处理机对本处理机进行诊断,其可信度比自诊断大大提高,且没有额外的系统资源开销,因而是一种较优的提高系统可靠性的方法。目前在提高系统可靠性方面,受到了越来越多的重视,并已取得令人瞩目的成果。

分布式系统级故障诊断的出现是在八十年代初,首先由 Kuhl 和 Reddy 提出,其基本思想是在分布式系统中,每个处理机分别独立地对其余处理机进行测试和诊断,不象集中式诊断,已没有一个外部处理机。

在分布式系统级故障诊断中,应考虑到故障诊断只是保证整个系统正常运行的一个小的辅助部分,所以不应占有过多的系统开销,一般采用的是每个处理机各自独立地对其“邻域”处理机进行测试及诊断。每个处理机的“邻域”的定义有两种:静态的方法和动态的方法。前者是对某个分布式系统,确定它的测试图,测试图一经确定就不能改变,即非自适应

方法;后者是采用自适应方法,测试关系是不确定的。

另外,在分布式系统中,处理机的故障分为永久性故障和瞬态故障,而瞬态故障为处理机由故障变为无故障。除了处理机的故障外,链路的故障(也可分为永久性故障和瞬态故障)在分布式故障诊断中也是应考虑的因素。

三、诊断算法

分布式系统级故障诊断发展到现在已出现了很多算法,其中有代表性的算法有三个,即 NEW-SELF 算法、EVENT-SELF 算法和 DSD 算法。NEW-SELF 算法和 EVENT-SELF 算法非常相似,而事实上 EVENT-SELF 算法只是 NEW-SELF 算法的改进。NEW-SELF 算法是一个基于 PMC 模型的非自适应一步 t-故障诊断算法,它采用固定测试图来完成测试及诊断,它能诊断瞬态故障和链路故障,注意,当 NEW-SELF 算法应用于单总线系统时,将不能诊断链路故障,参考文献在这点上不正确,DSD 算法是一个基于 PMC 模型的自适应一步 t-故障诊断算法,它采用自适应方法进行测试及诊断,它能诊断瞬态故障,但不具有诊断链路故障的能力。在诊断链路故障方面,由 Pradhan 等提出的方法能比较好地解决。从测试过程中所需传输的信息量和所需的时延的角度考虑,DSD 算法是目前较优的一种诊断算法。注意,在参考文献中,认为自适应 DSD 算法的诊断性数在 PMC 模型下是 $N-1$ (其中 N 为系统中的处理机个数),这是不正确的;而在 BGM 模型下该算法的诊断性数才能达到 $N-1$ 。

另外,DSD 算法之所以在分布式诊断算法中有如此重要的地位,其最主要的原因还是它是目前世界上第一个已在实际网络系统中运用的分布式诊断算法,它是系统级故障诊断由理论到实践的一个里程碑。

四、已取得的成果

分布式系统级故障诊断是故障诊断中一个较新的,且非常接近实际的分支,许多成果已被应用到实际中。在自适应 DSD 算法中,若采用 BGM 模型,其诊断性数甚至可达 $N-1$,这是集中式诊断所无法达到的。在优化测试方面,特别是分布式故障诊断与自适应诊断相结合而得的自适应分布式故障诊断,使测试数减少到很低的程度,极大地提高了系统的有效性。

(转第 56 页)

系统的方法。将来重设计将受到整套工具的支持,包括规格说明演进变换、一致性维护系统以及推导历史的智能重播。

一些研究所中正在探索支持领域分析、设计分析和软件体系的 KBSE 环境。领域分析和设计分析是知识获取的任务。DRACO 是一个领域分析环境的原型,它包括面向应用语言的生成器,还对领域内及领域间的变换规则提供支持。

设计分析是获取控制知识。表示和获取这种知识的关键是对变换推导的结构有一个深刻理解。一些交互式程序变换系统,特别是 KIDS,对变换推导中受过训练的人提供了一个自然的高级接口。然而,我们才刚刚开始去理解如何编码选择设计空间中特定路径的基本原理。这些语义信息是我们泛化推导历史并形成策略所必需的。期望下一个十年中将有重大的进展。

十、总结

直到目前,在软件工程中 AI 主要应用于快速原型。快速原型能够反复求精“需求和系统设计”,然后再手工编码产品级质量的软件。然而,手工编码的产品级质量的软件也难以修改、维护及重用。

在下一世纪中,软件工程将有如下特点:

①变换程序设计将创造新的软件开发风范,正如台式出版所创造的那样。

②软件开发及维护将提升到规格说明级上,从规格说明自动推导出高效代码。

③用于需求说明、规格说明进化和程序综合的基于知识的工具将允许端点用户说明并修改他们的软件。

④软件体系将使小型的软件开发小组能创建大软件系统。

⑤知识表示、知识获取及自动推理的进展将使领域专家和设计专家能在软件体系中把他们的知识编码成可供系统开发人员和端点用户重用的代码。

⑥软件工程将提升为工程学科,掌握目前尚未成文的领域知识和设计知识并使其自动化。

进展到这种新风范的过程是渐进的。在下个十年,KBSE 将开始以更有力的基于知识的工具支持 CASE。当代 AI 技术能大大增强传统维护工具,帮助维护程序员理解软件系统和确定修改的细节。当代 AI 技术也能帮助还原现存的系统。专用程序综合系统很可能变成下一代的应用生成器。与现有应用生成器中所用的技术相比,变换技术能产生更优化代码并提供更高级用户接口。简言之,KBSE 将适应和改进当今实践,变革软件工程。

主要参考文献 Michael R. Lowry, *Software Engineering in the Twenty-First*, 《AI Magazine》, Fall 1992

(接第 73 页)

五、研究方向

到目前为至,分布式故障诊断主要基于 PMC 模型,而对于基于其它模型的分布式故障诊断,如基于 BGM 模型的研究却很少,把分布式故障诊断与其它模型结合起来,也许会得到一些意想不到的结果。但分布式故障诊断不适合与比较模型结合,因为它会人为地提高某些处理机的可靠度。目前已有的分布式系统级故障诊断的特征定理是分别针对各个具体情况而言的,还没有找到对各种情况都适合的特征定理。另外,有关分布式故障诊断算法复杂性的分析还比较少,因为算法复杂性分析对人们评价一个算法的优劣是至关重要的,因此通过对分布式故障诊断算法的复杂性的分析,可以帮助人们了解现有分布式故障诊断算法的不足,进而为寻找时间复杂性更低的算法打下基础,特别是在并行算法中,算法所需时间开销是评价一个算法优劣的非常重要的指

标。在故障诊断中,诊断算法的诊断性数越大,性能越好,因而研究诊断性数尽可能大的诊断算法是一个重要方向。在实际分布式系统中,一个诊断算法若没有考虑瞬态故障和链路故障将不是一个好的分布式故障诊断算法,因为在实际分布式系统中,除了永久性故障外,瞬态故障的出现也是相当频繁的,而链路故障更是不可避免。

分布式系统级故障诊断主要是针对多处理机系统,而这里的多处理机系统是指其中的各个处理机分别拥有自己的存储单元,而不是共有一个存储器。随着计算机网络系统应用的日益广泛,网络在人们日常生活中的作用越来越重要,有关网络的可靠性问题的研究也日益突出,有关网络的故障诊断和容错将是一个全新的领域,虽然我们可以大量借用分布式系统级故障诊断研究中的成果,但由于网络自身的特点,在有些情况下必须从网络的角度对诊断和容错进行研究。

(参考文献共 8 篇略)