SHUZILUOJI
ZHENDUAN YU
KEKAOXING
SHEJI

数字逻辑
诊断与可靠性设计

范成荣 编

国防科技大学出版社

数字逻辑
诊断与可靠性设计

范成荣　编

国防科技大学出版社

内 容 简 介

本书主要是讨论数字逻辑电路和系统中的测试码生成，数字系统的可测性设计，硬件故障检测技术和容错技术。

测试码生成主要介绍布尔差分法和D算法等测试生成算法，面向的故障类型是单固定故障，多固定故障和搭接故障。可测性设计主要讨论数字系统可测性的改善设计，LSSD等结构可测性设计和内建测试电路设计。硬件故障检测技术介绍完全自校验电路的设计。容错技术主要包括数字系统的可靠性概率描述，系统的可靠性分析方法，静态冗余技术和混合冗余技术，冗余系统的可靠性分析。

全书包含大量例题，便于自学，可作为计算机及应用专业的教材，并可作为自学用书。

数字逻辑诊断与可靠性设计

范成荣 编

*

责任编辑 王金荣

装帧设计 侯 云

*

国防科技大学出版社出版

*

湖南省新华书店发行

国防科技大学印刷厂印装

*

开本：787×1092 $\frac{1}{32}$ 印张：8 $\frac{3}{16}$ 字数：195千字

1986年6月第1版 1986年6月第1次印刷 印数：0,001—5,000

统一书号：15415·012 定价：1.38元

前　言

从六十年代初开始，对数字系统的維护和可靠性的研究就引起了人们的重视。随着计算机的发展和计算机应用领域愈来愈广泛，数字系统的可靠性也愈来愈重要，它直接影响计算机的发展和广泛应用，因此，数字系统可靠性研究逐渐成为计算机科学和技术的一个重要分支，而诊断和可靠性设计是提高数字系统可靠性的主要途径。近年来，由于数字系统复杂性的增加及大规模和超大规模集成电路的出现，在新的系统设计中，诊断和可靠性设计已经成为突出问题。如果设想一个系统的设计不考虑可测性等可靠性设计，那么，这样的系统的测试将变得很复杂，将出现用于测试的研制费用超过系统本身的研制费用，所以数字系统可测性和容错计算等可靠性设计成为目前一个非常活跃的研究领域。本书着重讨论数字逻辑系统的诊断和可测性设计的基本方法及容错设计的基础理论和方法。

本书是为计算机及应用专业编写的教材，编写过程中着重讨论基本概念和基本方法，而不是叙述实际系统，阐述力求通俗易懂，以便于自学，也可作为高等教育自学考试的计算机及应用专业的自学用书。书的第一章主要是故障分析，为以后的测试生成建立故障模型。第二、三章主要介绍组合电路和时序电路的测试生成算法。第四章研究数字系统的可测性设计。第五章讨论硬件故障检测技术。最后一章包括可靠性分析的基础理论，数字系统可靠性的分析方法，容错设计的基本方法和冗余系统的可靠性分析。

本书在编写过程中得到了杨晓东副教授、盛运焕同志的指导和帮助，也得到了李勇副教授、王凤学和张绍贤等同志的支持和帮助，在此一并表示感谢！

由于作者水平所限，错误和不妥之处在所难免，恳請读者批评指正。

编　者

1986年2月

目　　录

第一章 绪 论

随着现代数字系统复杂性的增加和其应用领域越来越广泛，系统的可靠性变得越来越重要。数字系统可靠性的基础是元、器件的可靠性。目前虽然大规模和超大规模集成电路的发展，使得元、器件的可靠性大大提高，但是数字系统也越来越复杂。元、器件可靠性的提高已经被系统复杂性的增加所抵消。单纯从增加元、器件可靠性来保证系统的可靠性远不能满足系统可靠性的要求。因此，数字系统的故障诊断和可靠性设计对提高数字系统的可靠性和使用效率的影响更加引起人们的重视。现在关于数字系统的诊断与可靠性设计已逐渐形成一套完整的理论。

数字系统的可靠性和使用效率是系统性能的一个很重要的评价标准。对一个数字系统常常采用可靠性 (Reliability)R，可維性 (Serviceability) S 和可用性 (Availability) A 来描述其性能。可靠性R的一种单值指标是平均无故障时间 ($MTBF$)，可維性S的单值指标是平均故障修复时间 ($MTRF$)，描述可用性A的指标为

$$A=\frac{MTBF}{MTBF+MTRF}$$

从可用性A的表达式可以看到，为提高系统的使用效率，需要减小平均故障修复时间 $MTRF$，增加平均无故障时间。

本书旨在研究缩短維修时间的诊断技术和提高可靠性的容错技术。主要包括测试生成的基本方法，数字系统的可测性设

计，数字系统的硬件故障检测技术和系统可靠性评价及提高可靠性的容错技术。

诊断技术的主要对象是故障，这一章是从分析故障的物理原因入手，建立便于诊断研究的故障模型，介绍现代测试的基本方法，提出诊断技术研究的主要问题。

1.1 物 理 故 障

一个数字系统，例如一台数字计算机或者一块计算机的插件，当它表现出与设计规定的功能不一致，出现错误的输出响应，我们就说系统出现了故障。引起系统故障具体的物理原因称为物理故障。以图 1.1 所示的简单的门电路为例。门的正确功能为 $Z=\overline{x_1x_2x_3}$，如果 a 点开路，门的功能变为 $Z=\overline{x_2x_3}$，线路功能与规定的功能不一致，门发生故障。a 开路即为物理故障。如果三极管 T 击穿短路，Z 变为 0．使 $Z=0$ 的三极管击穿短路也为物理故障。

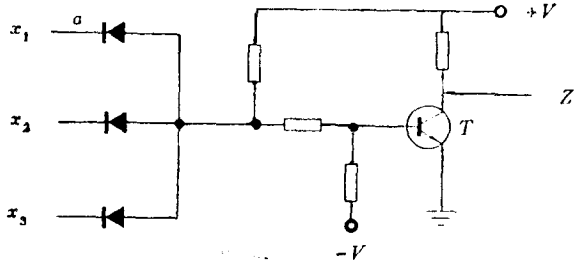


图 1.1

引起数字系统功能错误的物理故障是多种多样的。一个系统在生产、装配调试、存放和工作期间都可能产生各种物理故障。在生产阶段，生产工艺中的缺陷，例如，印制线断路、线间

短路、元件虚焊等；装配调试阶段，底板线漏线、虚焊和接插件接触不良；在存放期间，由于环境温度和湿度的影响，密封元件漏气使元件性能变差，元件损坏；工作期间除了温度和湿度影响之外还有振动、散热不良和元件逐渐老化也会使元件损坏，工作域变小。此外，工作期间外界电磁干扰和供电电源的波动也会使系统工作出现错误。

物理故障对电路功能影响主要表现在两方面，一是影响电路的逻辑特性，称为逻辑故障。二是引起电路参数改变，如速度，电压和电流等，称为参数故障。故障诊断测试将要研究的是逻辑故障和参数故障，因为具体的物理故障分析起来比较复杂。对数字系统，我们关心的不是具体的物理故障，而是功能特性。具体的物理故障分析不是本书的内容。

1.2 逻辑故障及其故障模型

实际存在的物理故障使得电路工作时出现逻辑上的错误，这种电路逻辑错误称为逻辑故障。逻辑故障实际就是各种不同的物理故障在逻辑上的反映，或者称为逻辑等效。一种逻辑故障可能等效几种不同的物理故障。也就是说一种逻辑故障可能由几种不同的物理故障引起。例如图 1.1 引起 x_1 出现固定于 1 值的逻辑故障可能是输入引线断路，或对电源短路。输出 Z 固定 0 值可能是三极管击穿短路或输出引线对地短路。把物理故障等效为逻辑故障，使故障分析问题变为逻辑网络的分析问题。

为了简化故障分析，常常对故障特性作若干假设，称为建立故障模型。故障模型一定要既能反映实际存在的故障情况，又便于分析研究。建立故障模型主要考虑的问题是：故障存在的时间性，是永久的还是瞬间的。永久性的故障使电路的故障特征有重复性，便于分析。瞬时故障的特征则无重复性，分析比

较困难；故障的数量，单故障，可以简化分析，多故障分析比单故障复杂得多；故障的表现形式，是固定的还是振荡的。现在实际应用的故障模型有如下几种。后面几章的研究就是建立在这些故障模型的基础上。

(1) **永久故障和间歇故障** 永久故障引起电路的错误始终存在，电路中的故障特征有重复性。生产工艺的缺陷和元件的损坏绝大部份呈现永久性故障。永久性故障便于诊断测试。而间歇故障无一定规律性，在某一测试期间出现，能够被检测，而另一测试期间可能不出现，就不能被检测，这给故障定位造成很大困难。所以在诊断测试研究中，假设故障是永久性的故障。

(2) **固定性故障** 固定故障是假设电路中的信号线、元件输入和输出的逻辑值固定在常值。如果固定在“1”称为固定“1”故障，简记为 s-a-1 (Stuck-at-1)。如果固定在“0”称为固定“0”故障，简记为 s-a-0 (Stuck-at-0)。

(3) **单故障和多故障** 在某一时刻，系统中仅存在一个故障，称之为单故障。一个系统在正常的工作期间出现的故障绝大多数属于单故障。在某一时刻，系统中存在一个以上故障称为多故障。多故障的诊断测试要比单故障的诊断测试复杂得多。例如图 1.2 的电路，输出的逻辑函数为 $f(x_1,x_2,\cdots,x_n)$。电路具有 n 个输入，如果只考虑输入端的逻辑故障，在单故障假设条件下，需要测试的故障数是 $2n$ 个。而在多故障假设条件下，多故障（包括单故障）数为 $2C_n^1+2^2C_n^2+2^3C_n^3+\cdots+2^nC_n^n=3^n-1$. 取 $n=10$，单故障假设仅需研究 20 个故障的诊断测试，而多故障假设需要研究 $3^{10}-1=59048$ 个故障的诊断测试。

实际上经常采用的是单故障假设。实践证明由单故障假设推导的测试也能检测绝大部份多故障，但是，不能检测所有的

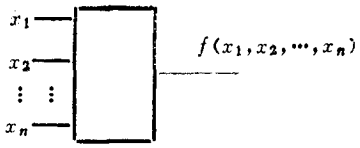
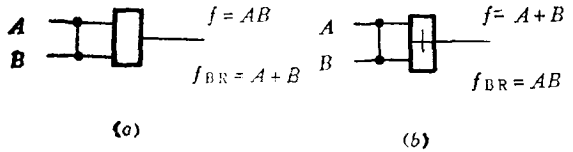


图 1.2

多故障。本书主要讨论单故障测试，对多故障作简单介绍。

（4）搭接故障（桥故障） 搭接故障的物理表现是两条或多条信号线短接，这是一种常见的故障。搭接故障在逻辑上的反映，有的呈现或，有的呈现与。两条信号线搭接后呈现或的关系称为或搭接，两条信号线搭接后呈现与的关系称为与搭接。例如图 1.3 给出的两类搭接故障，与门的二输入 A 和 B，搭接后使输出变为 A 和 B 的或，而或门的二输入 A 和 B，搭接后使输出变为 A 和 B 的与。决定是与搭接还是或搭接的主要因素是实现电路的工艺。对 TTL 门电路，输入搭接故障呈现与搭接。而 ECL 门电路输入搭接故障呈现或搭接。



(a) 与门或搭接
正常输出 $f = AB$
故障输出 $f = A + B$

(b) 或门与搭接
正常输出 $f = A + B$
故障输出 $f = AB$

图 1.3

在电路不同门的输入相互搭接可能引起电路的振荡，还可能使组合电路变成时序电路。例如图 1.4(a) 中的 a 和 b 搭接，在 $x_1 = 1$ 时电路将产生振荡。图 1.4(b) 中的 a 和 c 搭接使 G_3 和 G_4 组成门闩电路，组合电路转变为时序电路。这种搭接故

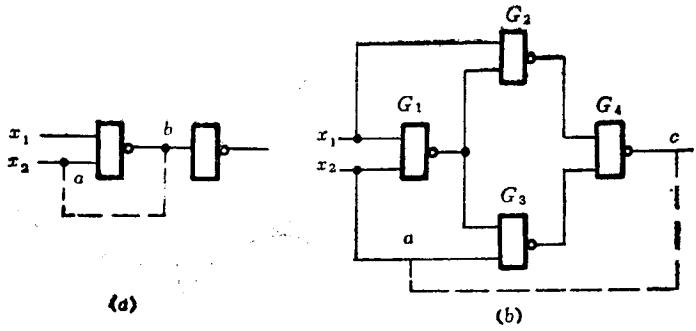


图 1.4

障测试比较困难。我们只研究同一门的与搭接和或搭接故障。

(5) 单向故障　固定在同一逻辑值的多故障称为单向故障。对大规模集成电路，单向故障是一种经常出现的故障类型。例如存贮器的地址计数功能失效，多地址访问得到的是单地址结果，这就是一种单向故障。

1.3　故障测试及测试码

一个数字系统从生产调试到整个运行寿命期间都可能发生故障。在生产过程中，各种测试是很重要的。在运行过程中测试是系统維护的基本手段。现在我们从分析系统的生产过程来看测试的重要意义及测试的类别，并介绍现代的自动测试系统的组成，给出测试码的定义，并根据定义求故障的测试码。

图 1.5 给出了数字系统的生产流程图。从图中可以看到，生产过程的每一个环节都离不开测试。图中的测试环节基本包含三种类型：其一是静态测试或称为功能测试，例如元件的功能测试，插件板的功能测试及系统的功能测试。第二是动态测试或称为参数测试，例如元件的时间特性及参数的一致性的筛选测试和插件的动态测试等。第三是系统的时钟频率测试。本书

主要是研究电路的功能测试，即元件、插件和系统的逻辑功能测试。

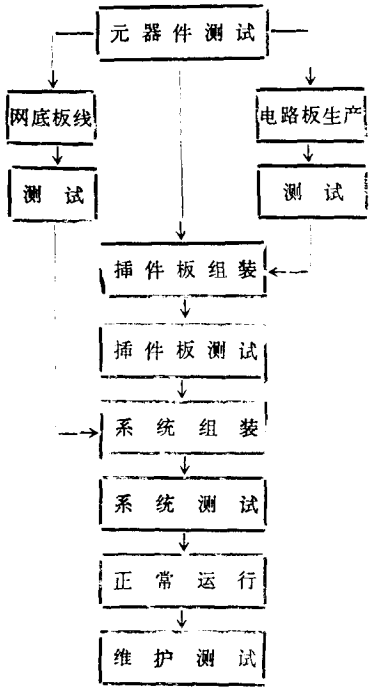


图 1.5

数字系统的故障测试，一般是指对一个电路的输入施加一定的测试输入码，观察输出响应，并与正确的输出比较，判定电路中是否有故障，并为故障定位。最早的测试方法是人工测试，技术人员借助一定的测试设备，如电压表和示波器等，在一定的输入条件下观察输出响应。由技术人员分析、比较，判定是否存在故障及故障位置。人工测试要求测试者有比较高的技术水平，并对被测对象的设计比较了解。人工测试的效率比

较低，为了提高测试效率，现在发展起来的是利用计算机构成自动测试系统。测试码的产生和加入，测试结果的分析和比较，故障和故障位置的判定，都是用计算机测试程序自动进行。一个完整的自动测试系统由两个子系统组成。一是测试码的生成系统，二是自动测试执行系统。图 1.6 给出的是一个插件板的自动测试执行系统的框图。

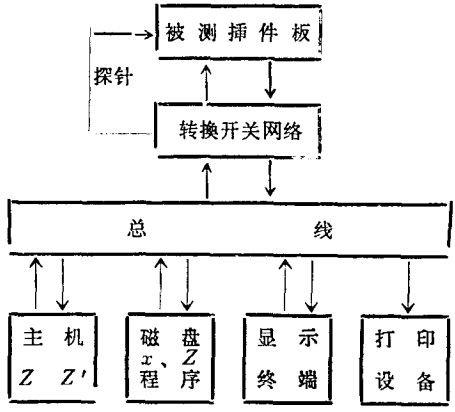


图 1.6

图中的磁盘存放测试程序，测试码 x 和正常的输出 Z。主机执行测试程序，将各种测试码 x，以一定的次序加给被测部件，并回收测试条件下的实际输出 Z'，比较 Z 和 Z'，判定故障及故障位置。通过显示终端或打印设备输出测试结果。自动测试系统回收的信息仅是被测部件输出引腿的信息，不能自动回收被测部件内部的信息。而人工测试可以观察内部各点的状态，准确判定故障位置。所以自动测试系统的可观察性降低了。为了弥补此不足，采用探针，人工适当干预，可以回收内部信息，以提高可观察性，增加故障定位能力。

图 1.7 给出了测试码的自动生成系统的框图。

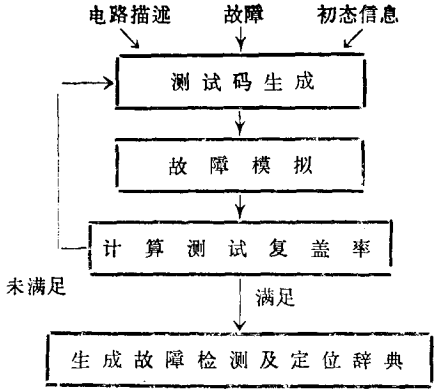


图 1.7

系统输入的是被测系统的电路描述、需要检测的故障及初始状态信息。利用一定测试生成算法结合故障模拟，对所有被测故障产生测试并建立故障检测和定位辞典。

图 1.8 给出的是一种工程实践常用的双比测试法。具体实现可以纯硬件，也可以软硬件结合。测试码可以穷举，也可以用伪随机码。

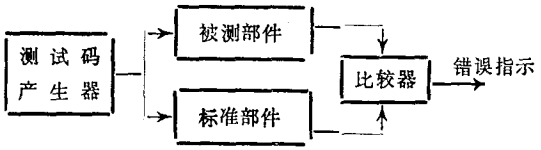


图 1.8

电路中的一个故障在一定的输入条件下，可能引起输出错误，在另外的输入条件下就不会引起输出错误。例如，研究图 1.9 的与门电路。对 $a(s\text{-}a\text{-}0)$故障，如果输入 $x_1x_2x_3=111$，电路的正常输出 $f=1$，若 a 出现固定 0 故障，则输出为 $f=0$，引起输出错误。如果输入 $x_1x_2x_3=001$，电路的正常输出和故障输出都是 $f=0$，在这样的输入条件下，$a(s\text{-}a\text{-}0)$ 故障不会