

M·A·布鲁尔 A·D·弗里德曼 著

数字系统的 诊断和可靠性设计

沈理 董一仁 译

人 民 邮 电 出 版 社

73.8/237

158

数字系统的诊断和 可靠性设计

【美】 M.A.布鲁尔 著
A.D.弗里德曼

沈理董一仁 译

魏道政 校

人民邮电出版社

57/16

DIAGNOSIS &
RELIABLE DESIGN
OF DIGITAL SYSTEMS

Melvin A. Breuer
Arthur D. Friedman
Computer Science Press, Inc.

1976

内 容 提 要

本书主要是讨论数字电路和系统中的测试码产生,逻辑模拟以及提高可靠性的设计方法。主要内容有:介绍D算法,布尔差分法等各种实际的测试产生算法,贝尔实验室的自动测试产生系统和LASAR测试产生系统。本书研究的故障类型有单固定和多固定故障、短路故障、桥接故障、存储器中的模式敏感故障;并介绍了用自动测试设备进行变换计数测试;并行模拟,故障表(演绎)模拟和同时模拟;利用各种编码技术的自检查和容错电路的设计,混合冗余技术,自诊断系统的模型,以及移位寄存器诊断方式的设计。全书包括大量的例子,每章附有习题。可作为从事电子计算机研究设计、技术工作人员的自学读物、大专院校计算机专业的教学参考书。

数字系统的诊断和可靠性设计

[美]M.A.布 鲁 尔 著
A.D.弗里德曼

沈 理 董一仁 译
魏 道 政 校

人民邮电出版社出版
北京东长安街27号

河北省邮电印刷厂印刷
新华书店北京发行所发行
各地新华书店经售

开本: 850×1168 1/32 1983年8月 第 一 版
印张: 9 24/32 页数: 156 1983年8月河北第一次印刷
字数: 257千字 印数 1—9,000 册

统一书号: 15045·总2694—有5284

定价: 1.55 元

中译本作者序

随着数字系统复杂性的增加以及大规模集成电路的出现, 在新系统的设计中, 测试和可靠性设计已成为突出的问题。可以设想, 到1982年, 如果系统中没有考虑可测性设计, 那么用于测试方面的研制费用将会超过系统的设计费用。由于半导体工艺的发展, 在一块芯片上大约可安放近一百万个晶体管。因此, 设计验证以及含有不可靠元件的测定等问题已成为日益重要的课题。

我们希望这本书将有助于数字系统领域中的大学生, 系统设计和研究人员更好地了解容错计算方面的问题, 从而设计更加可靠的系统。

最后, 我们向参加此书翻译工作的魏道政教授、沈理、董一仁先生表示谢意。

M.A. 布鲁尔

A.D. 弗里德曼

1980年4月2日

译者序

电子计算机在科学研究、工业、农业、国防建设和社会生活的各个方面获得了愈来愈广泛的应用，产生了深刻的影响。计算机进一步的推广应用，可靠性便成为一个十分重要的研究课题。国际上，随着计算机的不断发展，作为计算机科学技术的一个分支，直到六十年代末才逐步形成容错计算(Fault-Tolerant Computing)这个研究领域。因此近十年来这方面的研究特别活跃。

我们希望通过本书，系统介绍国外在这个领域若干方面的研究内容和进展情况，有助于我国迅速开展在这个领域的研究工作。

本书综合了在数字系统中诊断和可靠性设计方面近十五年来研究成果，介绍这方面的基本原理，各种算法和设计方法。主要内容包括：(1)组合和时序逻辑电路中故障检测和定位用的各种测试产生方法。(2)初始系统设计验证和测试产生所用的各种门级数字逻辑模拟方法。(3)高可靠性系统设计中的容错，自检查，易测性等问题。每章附有参考资料和习题。本书内容丰富，可作为从事计算机科学技术工作的各类人员的自学读物，以及高等院校计算机专业的教学参考书。

本书原文中个别错误在译文中作了更正。

译者 1982年4月

作 者 序

自六十年代初以来，对数字系统维护和可靠性课题的研究受到工业界和科学界的极大重视。当前，系统复杂性的增加更说明了它的重要性。维护这种系统的费用是很大的，它在系统总成本中所占的比例还在继续增长中。本书讨论有关数字系统的故障诊断和故障定位问题；高可靠性系统，即存在实际故障的情况下仍不失效的容错系统，能诊断自身故障的自检查系统，容易测试的系统等问题。虽然理论上许多问题尚难处理，但是实践中大多数问题都有实际而有效的解决方法。本书着重讨论这些方法，并且尽可能对每个问题介绍若干种方法。

随着对这方面课题的日益重视，许多大学开设了有关的课程。本书可作为这类课程的教材，也可供从事数字电路和系统工作的工程技术人员自学。第一章介绍本书主要内容和符号说明。以下两章分别详细讨论组合电路和时序电路故障的有效检测及定位问题。第四章讨论数字模拟问题，它是数字系统维护工程师很重要的一种手段。最后一章讨论系统设计中的易测性，自检查和容错问题。本书不叙述实际的系统，而是着重于概念以及提供达到这些目标的一般设计方法。每章都有一些例子以及未作解答的课外习题。

在这里对于朋友和同事们的帮助及建议表示感谢。他们是加利福尼亚大学的海斯 (J.P.Hayes) 和利文德尔 (Y. Levendel)，休斯飞机公司的贝诺威茨 (N.Benowitz)，贝尔电话实验室的查佩尔 (S.Chappell)。

布鲁尔 (M.A.Breuer)

弗里德曼 (A.D.Friedman)

目 录

第一章 绪论	(1)
1.1 数字电路	(2)
1.1.1 组合电路	(2)
1.1.2 同步时序电路	(5)
1.1.3 异步时序电路	(7)
1.2 实际故障和测试	(14)
1.3 逻辑故障模型	(18)
参考资料	(21)
习题	(22)
第二章 组合电路测试的产生	(24)
2.1 布尔差分法	(25)
2.2 测试产生的其它代数方法	(33)
2.3 路径敏化法和D算法	(34)
2.4 临界路径测试产生法	(50)
2.5 故障等效、支配和收缩	(54)
2.6 测试简化和最小化	(57)
2.7 冗余电路	(57)
2.8 用于其它故障模型的测试产生法	(62)
2.8.1 多固定故障	(63)
2.8.2 二极管短路故障和桥接故障	(66)
2.9 区分故障用的测试产生法	(73)
2.10 特殊电路	(75)
2.10.1 无扇出电路	(76)
2.10.2 实现单边函数的电路	(76)
2.10.3 线性组合电路	(77)

2.10.4 迭代阵列	(77)
参考资料	(79)
习题	(81)
第三章 时序电路测试的产生	(87)
3.1 同步时序电路测试的产生	(89)
3.1.1 时序电路中D-算法的推广	(91)
3.1.2 置初值	(97)
3.1.3 同步时序电路中临界路径测试算法的推广	(102)
3.1.4 测试组的简化	(105)
3.2 异步电路测试的产生	(106)
3.2.1 异步电路的迭代阵列模型	(107)
3.2.2 无临界冒险测试的产生	(112)
3.2.3 延迟故障的测试产生	(118)
3.2.4 电路-时间方程	(121)
3.3 与电路实现无关的测试产生方法	(127)
3.3.1 功能测试	(127)
3.3.2 检查序列	(128)
3.4 故障支配和特殊故障	(131)
3.5 半导体随机访问存储器的测试	(134)
3.6 随机测试的产生和测试	(141)
3.6.1 实践	(141)
3.6.2 理论	(147)
3.7 利用跳变计数测试电路	(148)
附录: 常用的RAM功能测试模式	(152)
参考资料	(156)
习题	(158)
第四章 逻辑级模拟	(168)
4.1 逻辑模拟系统的概述	(169)
4.1.1 输入电路描述	(170)
4.1.2 模型建立	(172)

4.1.3	输入数据语言	(172)
4.1.4	预处理程序模块	(173)
4.1.5	结构模块	(173)
4.1.6	模拟模块	(174)
4.1.7	输出模块	(176)
4.1.8	中央处理机的模拟时间	(176)
4.2	电路延迟	(177)
4.2.1	传输延迟 (Δ_T)	(177)
4.2.2	模糊延迟 ($\Delta_M - \Delta_m$)	(178)
4.2.3	上升-下降延迟 (Δ_R, Δ_F)	(180)
4.2.4	惯性延迟 (Δ_I)	(181)
4.3	多值逻辑系统	(183)
4.3.1	三值逻辑对检测冒险的应用	(184)
4.3.2	五值逻辑系统	(191)
4.3.3	八值逻辑模拟	(192)
4.3.4	电路置初值	(194)
4.4	基本模拟程序的结构	(195)
4.4.1	编辑驱动模拟	(196)
4.4.2	面向事件(活动)的模拟	(199)
4.4.3	数据结构	(202)
4.4.4	时间流控制机构和事件登记	(206)
4.5	元件计算	(211)
4.5.1	并行模拟	(212)
4.5.2	两值逻辑模拟的元件计算方法	(213)
4.5.3	多值逻辑模拟的元件计算方法	(214)
4.6	故障模拟	(216)
4.6.1	引言	(216)
4.6.2	并行故障模拟	(219)
4.6.3	演绎模拟	(221)
4.6.3.1	两值演绎模拟	(222)
4.6.3.2	三值演绎模拟	(227)

4.6.4	同时故障模拟	(229)
4.6.5	超活动故障	(233)
4.6.6	故障模拟方法的比较	(233)
4.7	模拟的振荡	(234)
4.7.1	局部振荡控制	(234)
4.7.2	全局振荡控制	(235)
4.8	模型的建立	(236)
	参考资料	(238)
	习题	(240)
第五章	可靠性设计——理论和方法	(245)
5.1	自检查电路	(245)
5.1.1	错误检测和校正码的应用	(246)
5.1.2	检查电路	(254)
5.1.3	自检查时序电路	(261)
5.2	容错设计	(262)
5.2.1	三模冗余	(263)
5.2.2	N 模冗余和混合冗余	(265)
5.2.3	故障保险设计	(268)
5.2.4	冗余系统的覆盖率	(270)
5.3	系统诊断的数学模型	(272)
5.4	简化测试的设计	(279)
5.4.1	用奇偶级联电路实现组合函数	(280)
5.4.2	观察点和控制点的设置	(282)
5.4.3	含有移位寄存器的时序电路设计	(285)
	参考资料	(289)
	习题	(292)
索引		(294)

第一章 绪 论

随着当前数字系统复杂性的增加，可靠性的研究愈来愈重要。数字电路是物理器件，虽然用目前的工艺技术所构成的数字系统比过去更为可靠，但是它还会发生故障，现在单个元件失效率的降低往往被电路复杂性的增加所抵销。我们把故障定义为使得系统不能正常运行时所发生的任何变化。在数字系统中，一般的维护要求是快速检测、定位和修复任何系统故障。

许多数字系统，包括电话交换网络，飞机或宇宙飞船的飞行控制器等这样的实时处理系统，需要连续监视、试验和测试，以确定系统是否在按预定的要求运行。这种监视可通过定期测试或利用编码和检查电路（例如自测试或自检查电路）来实现故障自动检测，或者使得在有故障情况下能继续工作（即容错），并通过开关网络进行自动修复。为了达到这些可靠性目的，在这类系统中必须具有专用的硬件和软件。书中将研究与数字系统测试有关的故障检测和定位问题，以及与发展高可靠性数字系统有关的理论和实际的设计方法。

主要内容包括（1）数字电路故障检测和定位测试的产生（即诊断程序研制）；（2）数字模拟的应用，它是测试产生和初始系统设计验证的一种工具，（3）自检查和容错系统的设计。

与故障检测有关的一个问题是初始电路设计的验证。由于设计错误不能象大部分实际电路故障那样合理地加以限制，因此，验证问题更为困难。对于这个问题理论上的一种方法，是采用功能测试法。这里，我们将讨论一种称为**检查序列**的功能测试法。

本章将叙述必要的基础知识。1.1节简述数字电路的基本概念，包括组合电路，同步时序电路和异步时序电路。1.2节讨论数字电

路中各种实际故障和现行的测试方法。

1.3节介绍逻辑故障模型的概念，并提出所要考虑的逻辑故障的一些模型。

1.1 数 字 电 路

数字电路的特点是静态电路的稳态信号只能取“0”和“1”两种值。这种电路可在电路级或逻辑级上来讨论。在电路级上关心的是诸如晶体管、二极管、电阻等电气元件以及电压、电流、波形等的分析和综合。在逻辑级上，电路被看作是由输入和输出仅取0和1值的元件所组成的。元件的逻辑功能完全可以用各种可能的输入值组合所确定的输出值来描述。本书所讨论的是数字电路在逻辑级上的分析和综合。

1.1.1 组合电路

组合电路的基本元件称为门。门的工作可用各种可能的输入值组合所确定的输出值来描述，图1.1(a)是常用门的符号及其表示方法。图1.1(b)是二极管—晶体管与非门(NAND)。正如门的名称的含义一样，当且仅当与门(AND)的所有输入为1，则输出为1；当且仅当或门(OR)的任一输入为1，则输出为1；当且仅当反相器的输入为0，则输出为1；当且仅当与非门(NAND(NOT AND))的任一输入为0，则输出为1；当且仅当或非门(NOR(NOT OR))的所有输入为0，则输出为1。

布尔代数是分析数字电路的基本工具，运算符号“+”和“ $\cdot$ ”对应于“或”和“与”，反相(补)用上横线来表示。如果用变量 x_1 和 x_2 表示与门的输入， z 表示其输出，那么 $z = x_1 \cdot x_2$ 。同样，两输入或门的输出表示为 $z = x_1 + x_2$ ；非门(NOT)的输出表示为 $z = \overline{x}$ ；与非门和或非门的输出分别表示为 $z = \overline{x_1 x_2} =$

注1：不发生混淆的情况下，乘积项中可省略运算符号“ $\cdot$ ”。

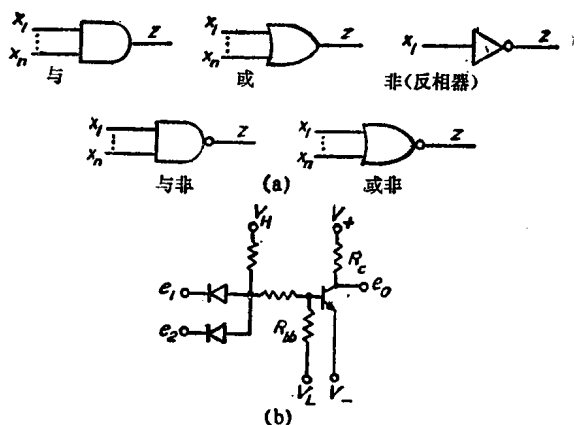


图 1.1 (a)常用门的符号(b)与非门电路

$\overline{x_1 + x_2}$ 和 $z = \overline{x_1 + x_2} = \overline{x_1} \overline{x_2}$ 。

数字电路可分为**组合电路**和**时序电路**两类。组合电路是不带反馈回路¹⁾门的集合(非循环电路)。组合电路可用来实现**组合函数**。组合电路当前的输出值仅取决于输入变量的当前值,而和输入在过去值无关。组合函数可用**真值表**,卡诺图,或1-点表²⁾来表示。图1.2为三输入变量组合函数的三种表示形式,其中图1.2(c)中的1-点表是立方形式,表中“—”号表示函数值1与“—”号对应变量的值无关。

组合逻辑电路的三个重要特性是**冗余**,**扇出**和**再汇聚扇出**。冗余是指电路存在某些故障的情况下仍能正常工作。对于一定类型的故障,冗余意味着为了产生所需的输出功能,要求比实际需要还多的元件和线。

扇出表示一个信号输入到两个或两个以上的门。再汇聚扇出表示一个信号通过两条或两条以上的路径到达另一个门的两个或两个

注1: 如果从某个门G的输出经过其他一连串的门(可以没有也可以有若干个门)到该G的输入存在一条通路,则称该电路是有反馈的。

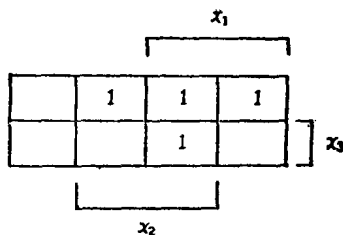
2: 1-点表示输入使函数输出为1的点。一译者注

x_1	x_2	x_3	f
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1

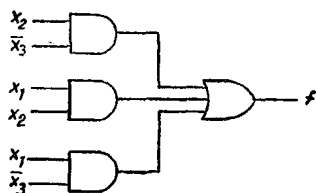
(a)

x_1	x_2	x_3
—	1	0
1	1	—
1	—	0

(c)



(b)



(d)

图 1.2 组合函数 $f(x_1, x_2, x_3)$ 的表示方法 (a) 真值表
(b) 卡诺图 (c) 最小覆盖的 1-点表 (d) 电路

以上的输入端。从图1.3可知门 G_1 扇出到 G_3 和 G_4 ，输入 x_3 扇出到 G_1 和 G_2 。 G_1 和 G_3 之间以及 x_3 和 G_4 之间存在再汇聚扇出。再汇聚扇出会使测试产生和模拟出现一些问题。因为在一个信号源（门的输出）上信号的改变能引起某个门的若干输入变化，由于电路存在延迟，这些输入变化是在不同的时间发生的。

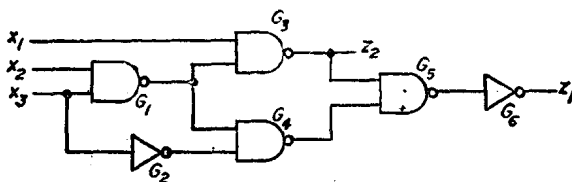


图 1.3 具有再汇聚扇出的电路

1.1.2 同步时序电路

时序函数是输出同时依赖于当前输入和过去输入的一个映射。与这种函数有关的概念是**存储或状态**，它表示函数过去输入的情况¹⁾。

用于表示组合函数的真值表不适合于描述时序函数。有限状态时序函数可用**时序机**作为模型，时序机接收可能输入的有限集合中的输入，产生可能输出的有限集合中的输出。它具有数量有限的**内部状态**（简称**状态**）。有限状态时序机的动作是这样的，设开始处于某个当前状态 q ，接收输入 I_m ，机器就进入下一状态 q_i 并产生输出 z_k 。下一状态 q_i 以及输出 z_k 由当前状态和输入唯一确定，并且只考虑由输入序列所规定的离散时刻的情况。

有限状态时序机可用**状态表**来表示，状态表的行对应于机器的每个内部状态，列对应于每个可能的输入。 q_i 行 I_m 列的表列值，表示机器在状态 q_i 时外加 I_m 所产生的下一状态和输出。这个表列值用 $N(q_i, I_m)$ 、 $Z(q_i, I_m)$ 表示。 N 和 Z 分别为机器的**下一状态函数**和**输出函数**。

图1.4是状态表的一个例子。这个机器有4种编号为1、2、3、4的内部状态，有一个二进制输入 x ，可能的值是 $x=0$ 和 $x=1$ ，一个二进制输出 z ，可能的值是 $z=0$ 和 $z=1$ 。状态表可以确定对于从任何初始状态开始，加任何输入序列后所产生的输出序列。例如，1行0列的表列值说明在初始状态1，加输入 $x=0$ ，使机器进入状态2以及产生输出 $z=1$ 。同样，从初始状态1开始，输入序列010使机器经历状态序列243以及产生输出序列101。

用上述方法表示时序函数有一个基本的前题，即**同步**，它在状态表中没有明确地表示出来。所加的输入是按某个时间序列 $t(1)$ ， $t(2)$ ， $\dots$ ， $t(n)$ 同步，即在时间 $t(1)$ 选取输入，使机器

注1：这里原文有误，现按时序函数的一般定义作了改正——译者注

	x	
	0	1
1	2,1	3,0
2	2,1	4,0
3	1,0	4,0
4	3,1	3,0

$N(q, I), Z(q, I)$

图 1.4 状态表的一个例子

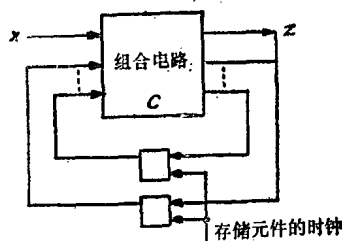


图 1.5 同步时序电路的标准形式

进入下一个状态并产生下一个输出。在时间 $t(2)$ 又重复这一过程，依此类推。

时序函数在电路实现时，同步这一基本性质是利用增加一个一般称为时钟线（简称时钟）的附加输入来完成。例如，在 $t(1)$ 产生一个事件，可用电路时钟线上某种形式的信号变化，即通常所谓时钟脉冲来表示。由于时序电路必须存储或记忆时钟线上所发生的事件之间的电路状态，因而需要称为时钟同步触发器的双稳态存储元件。时钟同步触发器只是在接收时钟脉冲时才改变状态。这些时钟脉冲用于同步和输入。因此，时序函数具有离散的性质。

同步时序电路的示意图如图 1.5 所示。

触发器一般有两个输出 y 和 $\bar{y}$ ，两个稳定状态（ $y = 0, \bar{y} = 1$ ）和（ $y = 1, \bar{y} = 0$ ）。本书将采用一些不同类型的触发器。SR 触发器是由两个交叉连接的与非门和输入定时脉冲的同步电路所构成的（图 1.6）。如果输入激励（在时钟脉冲时刻）为 $s = 1, R = 0$ ，触发器置“1”（ $y = 1, \bar{y} = 0$ ）。如果 $R = 1, s = 0$ ，触发器置“0”（ $y = 0, \bar{y} = 1$ ）。如果 $S = R = 0$ ，触发器保持当前的稳定状态，即表现为存储作用。输入条件 $S = R = 1$ 是禁止的（状态表中用不定的表列值表示），因为这种输入使两个输出均为 0。而当输入从 $S = R = 1$ 变为 $S = R = 0$ 时，下一个状态就不能确定，因为它取决于 y 和 $\bar{y}$ 变化的确切次序。

注 1：交叉连接的或非门门号其功能是相同的。

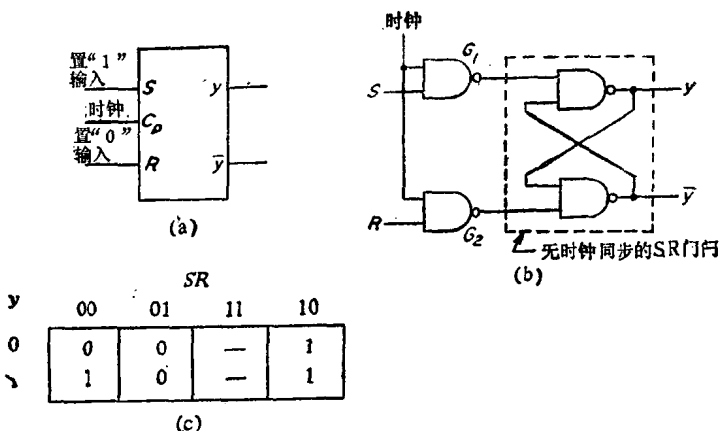


图 1.6 SR触发器的三种表示法
(a) 功能符号 (b) 电路 (c) 状态表

注意，触发器元件虽然是由基本门元件构成的，但包含有反馈，因此不是组合电路。为了使元件有存储作用，反馈是必需的。

触发器的特性方程表示触发器的下一状态(y)是当前状态 y 和输入激励的函数。对于SR触发器，由于输入 $S = R = 1$ 是被禁止的，因此特性方程为 $y = S + \bar{R}y$ 。其他常用的触发器如图1.7所示。

JK触发器和SR触发器类似(J 对应于 S ， K 对应于 R)，所不同的是输入 $J = K = 1$ 是允许的，它可使触发器改变状态，也就是说如果当前状态为 $y = 1$ ， $\bar{y} = 0$ ，那么当 $J = K = 1$ 时，状态变为 $y = 0$ ， $\bar{y} = 1$ ，反之亦然。 T 触发器就是 $J = K$ 的JK触发器。如果 $T = 0$ ，触发器保持当前状态，如果 $T = 1$ ，触发器改变状态。 D 触发器就是在 $S = \bar{R}$ 的条件下的SR触发器。这种触发器的状态总是等于输入激励 D 的过去值。

1.1.3 异步时序电路

时序电路的设计也可以不用同步时钟，这种电路一般称为异步