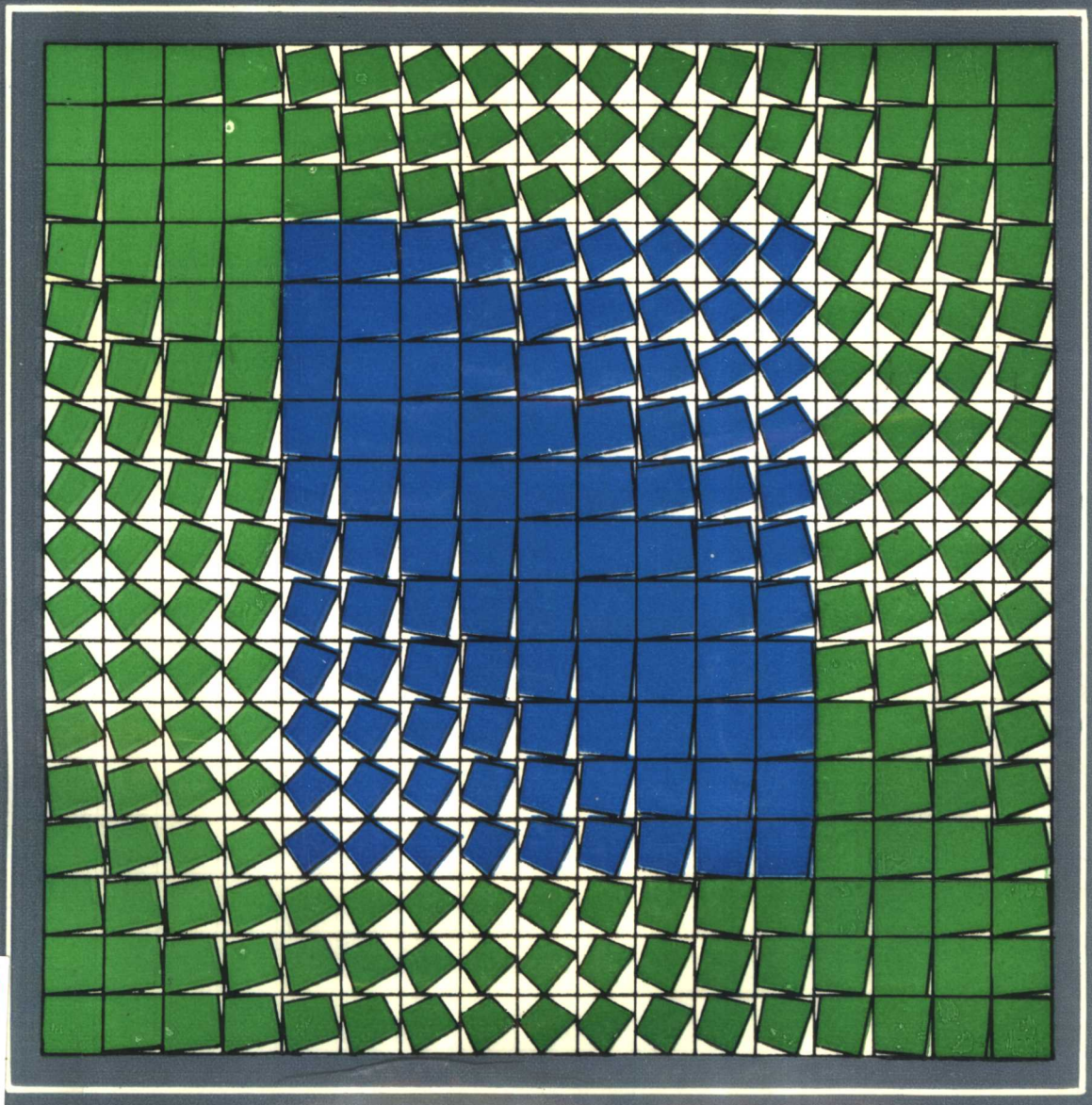
容错控制系统的分析与综合

葛建华　孙优贤　著

浙江大学出版社



容错控制系统的分析与综合

葛建华　孙优贤　著

浙江大学出版社

(浙)新登字 10 号

内容简介

本书以作者的研究成果为基础，系统地介绍了容错控制的基本理论和最新研究成果，提出了结构化不确定系统的鲁棒控制、同时镇定、完整性控制器的综合等方法，重点研究了基于分析冗余的故障诊断、不确定动态系统的故障诊断、基于人工智能的故障诊断等技术和故障补偿方法，介绍了容错控制的应用实例。

容错控制系统的分析与综合

葛建华　孙优贤　著

责任编辑　王文文

* * * * * * * * * * * * * * * * * * *

浙江大学出版社出版发行

浙江大学工业控制技术研究所电脑部排版

富阳何云印刷厂印刷

* * * * * * * * * * * * * * * * * * *

787×1092　16 开　18.75 印张　470 千字

1994 年 3 月第 1 版　1994 年 3 月第 1 次印刷

印数：0001—1000

ISBN 7-308-01167-4

TP・083　　定价：8.85 元

前　言

随着控制理论与计算机技术的迅速发展，计算机控制技术及其应用已经取得了相当丰硕的成果。同时，对控制系统安全和高可靠性运行的要求也向控制界提出了新的命题。当前，容错控制的研究已成为国内外广大控制工程师和科学家们共同关注的问题。

基于“功能冗余”的容错控制是在鲁棒控制和自适应控制基础上出现的一类新型的控制技术，它把控制系统的性能要求提高到对系统内部的某些故障具有容忍能力的程度。容错控制系统是一种高可靠性的、经济的和具有广泛应用前景的控制系统。容错控制理论的发展将对计算机控制技术产生极深刻的影响。但是，遗憾的是国内外尚无一本系统地介绍容错控制理论的专著，这使得容错控制还远未发挥其应有的作用。

本书以作者多年从事这一领域研究为背景，系统地介绍了容错控制的基本理论和国内外最新研究成果，同时也介绍了容错控制在工程中应用的例子，力求读者可以充分理解本书的内容，并引以借鉴或应用。如能达到这一效果，作者会感到十分欣慰。

值此机会，作者感谢国家自然科学基金和中国博士后研究基金对本研究工作的支持。

周春晖教授细心审阅了全书，并提出许多宝贵意见，对此，作者表示衷心感谢。对林庆女士打印的全部书稿，冯旭的精心校对，对责任编辑王文文同志所花费的巨大精力，在此，一并向他们表示最衷心的感谢。

由于水平所限，书中难免存在缺点和错误，恳请读者批评指正。

作　者

1993 年 10 月

符号一览表

$\boldsymbol{A},\boldsymbol{B},\boldsymbol{P}$	黑体大写字母表示集合
A,B,P	白斜体大写字母表示矩阵
$\boldsymbol{u},\boldsymbol{y},\boldsymbol{\alpha}$	黑体小写字母表示向量
u,y,α	白斜体小写字母表示标量函数或标量
$A^T,\boldsymbol{x}^T$	矩阵 A 和向量 $\boldsymbol{x}$ 的转置
$A^*,\boldsymbol{x}^*$	矩阵 A 和向量 $\boldsymbol{x}$ 的共轭转置
$\det A$	矩阵 A 的行列式
$\bar{\sigma}(A),\underline{\sigma}(A)$	矩阵 A 的最大、最小奇异值
$\mathrm{rank}(A),\gamma(A)$	矩阵 A 的秩和零度
$a\|b$	a 是 b 的一个因子
$B(x,\varepsilon)$	以 x 为圆心，ε 为半径的球体
$\boldsymbol{C},\boldsymbol{R}$	复数域，实数域
C_+,C_{+e},C_-	复平面上三个区域：闭右半平面 C_+；无穷远点和 C_+ 之和为 C_{+e}；开左半平面 C_-
$\boldsymbol{D}$	通常的稳定域，是 C_- 的一个子集
$\boldsymbol{R},\boldsymbol{R}[s]$	含单位 1 的交换整区环和环 $\boldsymbol{R}$ 上的多项式
$\boldsymbol{F},\boldsymbol{F}[s]$	$\boldsymbol{R}$ 上的分式域，系数在 $\boldsymbol{F}$ 中的多项式
$\boldsymbol{R}[s],\boldsymbol{R}(s)$	实系数多项式和实系数有理分式
$\boldsymbol{S}$	$\boldsymbol{R}(s)$ 的子集，由真稳定有理函数组成
$\boldsymbol{S}_D$	稳定域在 $\boldsymbol{D}$ 上的真稳定有理函数集合
$\boldsymbol{U}$	$\boldsymbol{S}$ 中单模元的集合
$M(\boldsymbol{S}),M(\boldsymbol{R})$	元素分别在 $\boldsymbol{S}$ 中和 $\boldsymbol{R}$ 中的矩阵
$M[\boldsymbol{R}(s)]$	元素为实系数有理分式的矩阵
$U(\boldsymbol{S}),U(\boldsymbol{R})$	元素分别在 $\boldsymbol{S}$ 和 $\boldsymbol{R}$ 中的单模态矩阵
$\boldsymbol{S}(P)$	使对象 P 稳定的反馈补偿器的集合
$W(P,C)$	由对象 P、反馈补偿器 C 组成的闭环传递矩阵
$\boldsymbol{Z},\boldsymbol{Z}_+$	整数和正整数集合
$\|\cdot\|$	各种向量与矩阵的范数
$\sim$	等价关系
$a\in\boldsymbol{U}(a\notin\boldsymbol{U})$	a 是(不是)$\boldsymbol{U}$ 中的一个元素
$\cup,\cap,\oplus$	二个集合的和、交及直和
$\supseteq(\subseteq)$	左面的集合包含(被包含于)右面的集合
r. c. f. ,l. c. f.	右互质分式和左互质分式
l. c. m. ,g. c. d.	最小公倍数和最大公因子

目　录

第一章　引论

§1.1　什么是容错控制系统

容错原是计算机系统设计技术的一个概念，它是指系统虽然遭受到内部环节的局部故障或失效，但仍可继续正常运行的一种特性。人们虽然无法保证构成系统的各个环节的绝对可靠，但若把容错的概念引入到控制系统，从而构成容错控制系统，使系统中的各个故障因素对控制性能的影响被显著削弱，那就意味着间接地提高了控制系统的可靠性。尤其是当构成控制系统的各个部件的可靠度验前未知时，容错更是在系统设计阶段保证系统可靠性的主要途径。

控制系统是一类由被控对象、控制器、传感器、执行器乃至计算机等部件组成的复杂系统，而各个部件又是电子、机械、软件及其它因素的复合体。一个典型的控制系统结构如图 1.1.1 所示。控制系统的各个基本组成环节都有可能发生故障。具体来讲，故障可划分为三种类型：

(1) 被控对象故障，指对象的某一部分设备不能完成原有的功能；

(2) 仪表故障，包括传感器、执行器和计算机接口的故障；

(3) 软件故障，指计算机诊断程序和控制程序发生故障。

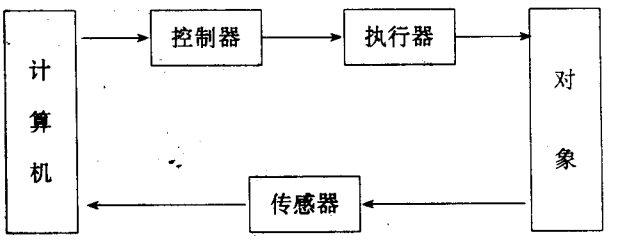


图1.1.1 控制系统结构框图

系统的可靠性除了取决于各环节的可靠性之外，还在很大程度上取决于系统的结构、控制方案、对系统的性能要求、系统的安装情况以及环境对系统的扰动等。控制系统的可靠性 R 可描述为：

$$R = R_1R_2R_3R_4$$

其中，R_1 ——控制作用处于设计允许公差范围之内的概率，即控制作用的可靠性；

R_2 ——控制系统参数处于选定的公差范围之内的概率；

R_3 ——被控对象的可靠性，以对象参数处于规定的允许范围之内的概率来度量；

R_4 ——干扰特性处于设计允许范围之内的概率。

上述公式说明，提高控制系统可靠性是一件涉及范围很广的工作，它既包括了形形色色的被控对象的故障特性，也与系统的控制作用有关。

提高控制系统的可靠性有以下两种途径。

1.1.1 硬件冗余技术

硬件冗余技术，即设置各种备份元器件或组件，合理地组织它们的工作方式，对故障部分进行删除或自动更换；或者，使个别故障不能影响整个系统的正常工作。

硬件冗余技术已成为工程可靠性技术中提高系统可靠性的一种基本方法。将之引用于控制系统，对某些关键装置设置一定的备份，同样可成为一种有效的容错控制方式。只要能够在物理上建立起冗余的信号通道，这种方式原则上可用于对任何硬件环节失效的容错控制。

实现硬件冗余技术的基本方法为重复线路、备份线路和复合方法。

重复线路是指用多个相同品种和规格的元件或组件并联起来，当作一个元件或组件来使用，只要有一个不出故障，系统就能够正常工作。这一组相同的组件在输入端和输出端都并联起来，其中某几个发生故障时并不影响其它组件的正常工作。也就是说，在并联工作时，每一个组件的可靠性概率是相互独立的。备份线路与并联线路的差别是参加备份的组件并不接入系统，只有在处于工作状态的组件发生故障后，才把输入和输出端转接到备份组件上来，同时切断故障组件的输入和输出端。为了实现这种转接，当然系统应该具有自动发现故障的能力，同时还应有自动转接的设备。重复线路和备份线路是硬件冗余技术中最常用到的基本线路。复合线路是由包含几个与非门的随机重复线路的串联，该方法需付出大的硬设备代价来提高可靠性。

无论哪一种硬件冗余技术，都遵循由冯·诺伊曼(J. V. Neumann)提出的容错的基本思想：应用概率论中最基本的概念，可以用不甚可靠的器件堆积成一个可靠的具有相同功能的组件，把自修复和容忍故障的能力引入到系统设计中，就可以达到高可靠性系统的目的。

在过去 30 年中，硬件冗余技术在计算机领域得到了广泛而成功的应用。容错计算机技术的发展和成熟为计算机控制技术提供了高可靠性的工业控制计算机。同时，计算机软件的容错技术也得到相应的发展，它是通过对关键性的操作配置若干个可供选择的程序，并增加测试检错或诊断的外加程序，来诊断软件的故障并隔离故障的软件，从而达到软件容错的目的。

对控制系统的其它环节，如被控对象子设备、传感器和执行器等，都可用硬件冗余技术提高其可靠性。但这种方法使系统重量、体积、投资和能耗增加。因此，针对控制系统是动态系统的特点，寻找一类新的、经济的和具有高可靠性的容错控制方法是控制工程师和科学家们一直努力追求的目标。

1.1.2 基于“功能冗余”的容错控制

与“硬件冗余”相对的“功能冗余”(也称“解析冗余”)是指系统中诸部件间在功能上有重叠，其中一个部件的部分或全部功能可由别的部件的功能来代替。基于“功能冗余”的容错控制的最大特点是：控制系统中所有的部件在正常时都处于工作状态，为维护控制系统的性能作出贡献，当某些部件失效时，其余完好部件部分或甚至全部地承担起故障部件所丧失的控制作用，以维持控制系统的性能在允许的范围内。显然地，系统中部件的“功能冗余”程度越高，它的容错能力也就越强。这里，容错控制被定义为：当控制系统中的某些部件出现故障时，尽可能地利用“功能冗余”，通过控制手段使故障系统继续保持规定的性能或不丧失最基本的功能，如稳定性等。

基于“功能冗余”的容错控制，不引入任何部件的备份，而是在常规的系统结构下，通过建

立控制系统的动态数学模型，得到诸部件间的“功能冗余”，进而通过控制器的设计实现对局部故障的容错，它为设计经济的和高可靠性的容错控制系统提供了一条崭新的途径。

基于“功能冗余”的容错控制方法可分为二类：第一类是鲁棒控制器的设计，即预先针对一定的故障模式，设计一个固定的控制器使得控制系统对可能出现的故障具有容错性。第二类是故障检测、分离和补偿，它是在常规控制系统的基础上设置故障检测机构，实时监视控制系统的运行及故障情况，并依据故障信息及时改变系统的结构及控制作用。

自 1971 年 Beard 博士首先研究基于“功能冗余”的容错控制以来，学者们针对各自应用背景，陆续开展了这类新型的容错控制的研究工作，经过近 20 年的努力，无论是在理论上，还是在应用上，都取得了可喜的成果。本书系统全面地总结了基于“功能冗余”的容错控制（以下简称为容错控制）的设计理论和国内外最新研究成果，其中包括作者长期以来的研究成果，以期读者对容错控制理论有系统的理解。

§1.2 故障的分类

上面我们已谈到，控制系统的故障类型主要有：被控对象的故障、仪表故障和软件故障。容错控制理论主要是涉及应用控制手段实现对被控对象和仪表故障的容错，因此本节将对这两类故障作更深入的描述。

故障泛指破坏工作能力的事件。按照故障发生的特点，可分为下列的形式：(1)突发性故障；(2)渐变性故障。无论是哪一类故障，都表现在数学模型的变化上。

1.2.1 被控对象的故障

(1) 故障的参数表示法

这种表示法的基本原理是用系统某几个参数所发生的不期望的显著变化来表征系统的故障。考虑动态系统

$$\dot{x}(t) = f(x(t),q,t) + v \tag{1.2-1a}$$

$$y(t) = h(x(t),q,t) + \eta \tag{1.2-1b}$$

其中，$x(t)$，$y(t)$分别是状态变量和输出向量，v，η 分别是输入噪声和输出噪声，q 是特征参数向量。

设对应于系统正常状况的特征参数向量为

$$q=q_0 \tag{1.2-2}$$

如果由于受各种因素的影响，特征参数向量较大地偏离了 q_0 值，则可以认为系统已发生了故障，其位置由向量$(q-q_0)$中非零元素的位置来体现。

(2) 状态的突变

被控对象的故障有时可以状态的突变来描述，其表述方法为

$$\dot{x}(t)=f(x(t),q_0,t)+v+\gamma\delta_{t,\tau} \tag{1.2-3}$$

其中，$\gamma\in R^n$ 表示故障大小的未知向量，τ 表示故障的发生时间，$\delta_{t,\tau}$为 Kronecker δ-函数。

$$\delta_{t,\tau}=\begin{cases}1 & \text{如果 } t=\tau\\ 0 & \text{如果 } t\neq\tau\end{cases}$$

1.2.2 仪表故障

仪表(包括传感器和执行器等)故障主要表现为仪表增益和零点的慢漂或跳变。以数学形式表示为

$$M_{out} = \alpha M_{in} + \beta \tag{1.2-4}$$

其中，M_{in} 和 M_{out} 分别是仪表的输入和输出，α 和 β 依据不同的故障类型取不同的值，也可能是时变的。根据不同的 α 和 β 值，我们给出仪表的典型故障类型。

(1) $\alpha = 1, \beta = 0$，仪表正常；

(2) $\alpha = 1, \beta \neq 0$，仪表出现零飘；

(3) $\alpha = 0$，β 任意，仪表卡死在 β 值处；

(4) α 任意，$\beta = 0$，仪表增益变化；

(5) $\alpha \neq 1, \beta \neq 0$，仪表同时出现增益变化和零点飘移。

依照控制系统故障的严重程度，故障可分为“致命性的”和“局部的可修复的”故障。“致命性”故障即指系统从根本上遭到破坏，例如电源被切断，主要部件被全部损坏等。这类故障将导致全系统的破坏，因而是不能被修复的。在这种情况下，系统的工作不可能继续正常地进行。容错系统当然不是针对这类问题而言的，而是指对“局部的可修复的”故障实现容错。

§1.3 容错控制方法(一)——鲁棒控制

鲁棒性是指控制系统在一定(结构、大小)的参数摄动下，维持某些性能的特性。根据对性能的不同定义，可分为稳定鲁棒性和性能鲁棒性。以闭环系统的鲁棒性作为目标设计得到的固定控制器称为鲁棒控制器。

最初研究鲁棒控制的动机是为了实现不确定系统的控制，当时的不确定性的定义是指控制器设计所基于的数学模型与实际对象数学模型之偏差大小。实际上，控制系统的各种故障都将导致数学模型的这种或那种的变化，自然地，希望设计一个固定的控制器实现对某些故障的容错，鲁棒控制就是这样一类容错控制方法。

故障导致系统中参数的变化，这种变化是有界扰动而不是无穷小扰动。现代鲁棒性分析的最重要特点就是讨论参数在有界扰动下系统性能保持的能力。

在过去 20 年中，鲁棒控制一直是国际自控界的研究热点，以下几个方面的开创性工作大大推动了鲁棒控制的发展：

(1) Belletrutti 和 MacFarlane[5]于 1971 年提出多变量系统的完整性问题。完整性是指多变量系统在某些部件(如传感器和/或执行器)失效时系统仍保持稳定的特性。显然，完整性是指控制系统在稳定性意义上对部件故障的容错。

(2) Youla 等人[6]于 1976 年针对一个特定对象给出了所有镇定补偿器的参数化表示。该参数化方法使得控制器自动产生一个闭环稳定系统。

(3) Kharitonov[7]于 1978 年针对区间多项式族，提出由四个区间端点作为系数的多项式的稳定性来判别区间多项式族的哈氏定理。

(4) Zames[8]于 1981 年提出控制系统的 H_∞ 设计方法。在假定干扰属于某一已知信号集的情况下，Zames 提出用其相应的灵敏度函数的 H_∞ 范数作为指标，设计目标是在可能发生的最

坏干扰下使系统的误差在这种范数意义下达到极小，从而将抗干扰问题化为求解使闭环系统稳定，并使相应的 H_∞ 范数指标极小化的输出反馈控制器设计问题。

(5) Doyle 等人[9]提出可根据范数界限扰动有效地描述模型不确定性，由此他发展了判别鲁棒稳定性和鲁棒性能的强有力工具——结构奇异值[10]。

(6) Vidyasagar 等人[11-12]于 1982 年提出了同时镇定化问题：给定 r 个被控对象 $P_1, P_2, \cdots, P_r$，能否找到一个控制器 C，镇定所有受控对象。这里被控对象多个模型描述主要是由故障或非线性系统在多个工作点的线性化所造成的。

(7) Lyapunov 函数在鲁棒性分析与控制器设计中的应用[13]。

根据研究所基于模型的不同，系统鲁棒性研究方法主要有两类：研究对象是闭环系统的状态矩阵或特征多项式的，一般用代数方法；研究是从系统的传递函数或传递函数矩阵出发的，就常采用频率域方法。

§1.4 容错控制方法(二)——故障检测、分离与补偿

平行于鲁棒控制，故障检测、分离与补偿是实现容错控制的一个重要方法。在实际系统中，由于故障的多样性与对系统性能的高要求，鲁棒控制一般较难保证系统在故障后性能依然优异。所以，一个完整的容错控制系统，除了采用鲁棒控制外，还需采用故障检测与诊断技术(FDD)，建立一套监控系统，进行实时故障监测与估计，并根据故障特征进行补偿，保证系统在故障状态仍能获得良好的控制效果。

基于“解析冗余”的 FDD 方法是利用系统中固有的不同部件在功能上的冗余性，在线得到系统的运行信息，通过估计技术或其它软算法来检测和分离系统的故障，并进而采用控制律重构，必要时重新自动组织系统，以实现故障的补偿。

现有的 FDD 方法，概括起来可分成以下四大类：

(1) 基于直接测量系统输出及信号处理的方法。

(2) 基于状态估计的 FDD 方法。

(3) 基于参数估计的 FDD 方法。

(4) 基于人工智能的 FDD 方法。

故障的补偿可以通过两种方式来实现：

(1) 故障模式没有事先确定——→检测故障——→根据系统中部件的状态重新设计控制律，甚至重组态。

(2) 故障模式事先确定——→检测故障——→从存贮的针对各种故障模式的控制方案中取出已发生故障的控制方案。

显然，计算机技术的发展为 FDD 方法的应用奠定了基础。目前，故障检测、分离与补偿方法在理论上正逐渐成熟，并已开始在航天航空、工业过程等领域得到应用[14-18]。

§1.5 本书内容概况

通过上面对容错控制理论的发展历史和基本内容的扼要介绍，我们不难发现，容错控制系统是一种高可靠性的、经济的和具有广泛应用前景的控制系统。容错控制理论的发展将对计算

机控制技术产生极深刻的影响。

本书以作者多年来从事这一领域研究为背景，系统地介绍了容错控制的基本理论和国内外最新研究成果。全书共分十二章。结构是这样安排的：第二章介绍了本书所用的控制理论基础知识。第三章至第六章是鲁棒控制篇，其中第三章介绍了结构化不确定系统鲁棒性分析与鲁棒控制器综合的方法，第四章讨论了同时镇定问题解存在的条件及一些求解方法，第五章介绍了完整性控制器的综合方法，第六章讨论了分散系统的鲁棒控制问题。第七章至第十章是故障检测、分离与补偿篇，其中第七章介绍了基于状态估计和参数估计的控制系统故障诊断的基本方法，第八章针对不确定系统，介绍了几类典型的鲁棒故障诊断方法，第九章是基于人工智能的故障诊断，主要介绍了基于专家系统和人工神经元网络的故障诊断方法，第十章介绍了一些自动重构控制律补偿故障的方法。第十一章介绍了容错控制的应用例子，最后一章是展望。

第二章　预备知识

本章介绍控制理论的一些基本知识，它们都是本书以后章节要用到的。所有结果都略去了证明，至于对其更全面的论述可参阅有关文献[19—23]。

§2.1　系统的描述

2.1.1　状态空间描述与输入输出描述

在时域中，线性时不变有限维系统能由下面的微分和代数方程所描述：

$$\dot{\boldsymbol{x}}=A\boldsymbol{x}+B\boldsymbol{u} \tag{2.1-1a}$$

$$\boldsymbol{y}=C\boldsymbol{x}+D\boldsymbol{u} \tag{2.1-1b}$$

其中，$\boldsymbol{x}\in\boldsymbol{R}^n$，$\boldsymbol{y}\in\boldsymbol{R}^l$，$\boldsymbol{u}\in\boldsymbol{R}^m$ 分别是状态、输出和输入向量，A，B，C 和 D 是恰当维数的常数矩阵。在零初始条件下取(2.1-1a)和(2.1-1b)的 Laplace 变换：

$$s\boldsymbol{I}\boldsymbol{x}(s)=A\boldsymbol{x}(s)+B\boldsymbol{u}(s) \tag{2.1-2}$$

或

$$\boldsymbol{x}(s)=(sI-A)^{-1}B\boldsymbol{u}(s) \tag{2.1-3a}$$

$$\boldsymbol{y}(s)=C\boldsymbol{x}(s)+D\boldsymbol{u}(s) \tag{2.1-3b}$$

把(2.1-3a)代入(2.1-3b)，我们得到

$$\boldsymbol{y}(s)=(C(sI-A)^{-1}B+D)\boldsymbol{u}(s)=P(s)\boldsymbol{u}(s) \tag{2.1-4}$$

其中，

$$P(s)\triangleq C(sI-A)^{-1}B+D \tag{2.1-5}$$

是系统传递函数矩阵。

$P(s)$的元$\{p_{ij}(s)\}$是表示在特定输入 $u_j(s)$和输出 $y_i(s)$之间关系的传递函数。

定义 2.1.1　如果所有 $P(s)$中的元$\{p_{ij}(s)\}$为真，则 $P(s)$为真；如果所有 $P(s)$中的元$\{p_{ij}(s)\}$为严格真，则 $P(s)$为严格真。

定义 2.1.2　如果$\{p_{ij}(s)\}$是因果的，则 $P(s)$是因果的。

为了物理上的可实现性，传递矩阵必须是真的和因果的。

定义 2.1.3　称矩阵 A 的特征值 λ_i，$i=1,\cdots,n$，为系统(2.1-1)的极点。定义极点多项式为

$$\pi(s)=\prod_{i=1}^{n}(s-\lambda_i) \tag{2.1-6}$$

这样，极点是下面特征方程的根：

$$\pi(s)=0 \tag{2.1-7}$$

极点决定了系统的稳定性。