清华大学研究生公共课教材——数学系列

应用近世代数（第3版）

胡冠章　王殿军　编著

清华大学出版社

清华大学研究生公共课教材——数学系列

应用近世代数(第3版)

胡冠章　王殿军　编著

清华大学出版社
北京

内容简介

近世代数(又名抽象代数)是现代数学的重要基础,在计算机科学、信息科学、近代物理与近代化学等方面有广泛的应用,是现代科学技术人员所必需的数学基础.本书介绍群、环、域的基本理论与应用.适用于数学与应用数学、计算机科学、无线电、物理、化学、生物医学等专业的本科生、研究生以及专业人员.

图书在版编目(CIP)数据

应用近世代数/胡冠章,王殿军编著.—3版.—北京:清华大学出版社,2006.7
(清华大学研究生公共课教材.数学系列)
ISBN 7-302-12566-X

Ⅰ.应… Ⅱ.①胡… ②王… Ⅲ.抽象代数—研究生—教材 Ⅳ.O153

中国版本图书馆CIP数据核字(2005)第011684号

出 版 者:清华大学出版社　　**地　　址**:北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**:100084
社 总 机:010-62770175　　**客户服务**:010-62776969

责任编辑:佟丽霞
印 装 者:北京国马印刷厂
发 行 者:新华书店总店北京发行所
开　　本:170×230　**印张**:14.75　**字数**:271千字
版　　次:2006年7月第3版　2006年7月第1次印刷
书　　号:ISBN 7-302-12566-X/O·517
印　　数:1～4000
定　　价:23.00元

前　言

本书第 1 版和第 2 版自出版以后，以很好的可读性受到读者的欢迎，有的学生毕业后，从国外还写信提出宝贵意见. 本书第 1 版同时也得到同行的支持与好评，曾荣获教育部优秀教材二等奖. 本着与时俱进的精神，第 3 版将在保持原有特色的基础上，反映近世代数在科学技术中的最新应用，内容也更加完整，我们力求使它不仅是一本教材，而且是一本值得收藏的参考书.

修订情况

与第 1 版和第 2 版相比较，第 3 版主要作了以下修订.

第一，增加了一些新的应用实例. 比如，在 1.1 节中增加了保密通信问题；在 2.10 节中增加了有关 RSA 密码系统的加密和解密变换的内容；在 4.3 节中增加了在密码学中很有用的离散椭圆曲线和离散对数的介绍.

第二，新增了第 5 章方程根式求解问题简介. 在前两版中，虽然在第 1 章中都提及了这个著名的问题，但是并未作出完整回答. 在第 3 版中，我们用一章的篇幅简要介绍了这个问题是如何解决的.

第三，为了便于学习，每章新增了一个小结，对全章的内容进行梳理和总结.

此外，第 3 版也对前两版个别表述进行了修改，对部分章节的内容作了不同程度的补充和调整，还增加了个别结论，在此不一一列举.

学习指导

第 1 章预备知识，读者应通读一下，即使有些内容不熟悉，也不要过多纠缠. 第 2 章群论，是本书的核心内容，要仔细阅读和学习，并要注重掌握基本概念和基本的分析方法. 学好了群论，对后面的环与域可起到举一反三的作用. 第 3 章环论，在某种程度上可以说是群的推广，有许多类似的概念和定理，因此只需把注意力放在环和群的不同之处，可比较快地学完这一章. 第 4 章域论，虽然域是环的一种，不必再去讨论一般理论，但由于域的扩张和有限域理论在近代科学中有很多应用，所以这一章的内容反而比较丰富. 而第 5 章方程根式求解问题简介，在理论上不仅把群、环、域融合在一起，而且三者结合起来，解决了当初引发近世代数诞生的方程根式求解问题. 但是如果时间有限，可把第 5 章作为选学或自学内容.

每节后的习题不可不做，也不一定全做，这是加深印象和测试学习效果的

一个环节，先要独立思考，后面有提示可参考. 每章后的小结列出这一章的精华，不仅起到概括总结、强调重点的作用，而且可作为今后查阅之用，这是本书具有收藏价值的一个方面. 至于应用的例子，随个人的兴趣和专业可以有所舍取.

本书特点

把抽象的理论写得通俗有趣，但又不失数学的严格性，是本书写作过程中追求的目标及特点之一. 近世代数是我们已有的代数知识的自然发展. 从我们熟知的整数、有理数、实数出发，由此引出群、环、域的概念，起点是很初等的. 我们把一些应用问题作为“引子”提出，每章都以问题的解决作为结局，使抽象的理论体现出很强的应用背景和效力.

另一特点是使读者用较少的时间学到最基本的内容，为此，每一节围绕一个中心问题，突出一两个定理，而把其他的内容作为相关的结论或例子给出，使读者对所学内容留下简洁清晰的印象. 全书的主要内容适合 48～60 学时的教学要求.

第三个特点是“开放性”，传统的近世代数书比较强调自成系统，有的从整数的定义讲起，甚至连导数也要重新定义. 本书采用“拿来主义”，一切学过的知识都可拿来就用，导数就是微积分中的导数，涉及初等数论、组合数学、图论、密码学等内容都即兴介绍.

本书的参考文献列于书后，特别要指出，本书参考了著名代数学家、中国科学技术大学教授曾肯成先生 20 世纪 80 年代初在清华大学数学系的讲课笔记，特此再次表示感谢. 同时继续向所有关心、支持与提供宝贵意见的读者、同行和编辑表示衷心的感谢.

编者

2006 年 1 月

第 2 版前言

为了满足数学与应用数学以及理工科专业学生和科技人员学习近世代数的需要，本书尽力做到联系实际，多举例子，使读者感到有趣想学. 在叙述方法上尽力做到连贯、前后呼应、合乎中文习惯. 对部分定理的证明采用提示式、部分论证式等方式给出，留有思考余地，读者若能边学边动手按提示完成证明或计算，会收到满意的效果. 每节后的习题均附有提示或答案，便于自学.

本书第 1 版出版后受到读者的欢迎，并得到同行的好评和支持，荣获国家教委第三届高校优秀教材二等奖. 本次再版时，根据读者和同行的意见与建议做了修改与补充. 在此，作者向所有给予本书关心、支持与提供宝贵意见的读者、同行和编辑表示衷心的感谢.

胡冠章

1999 年 1 月

目　录

第 1 章　引言和预备知识 …… 1
1.1　几类实际问题 …… 1
1. 一些计数问题 …… 1
2. 数字通信的可靠性问题与保密性问题 …… 5
3. 几何作图问题 …… 7
4. 代数方程根式求解问题 …… 8
习题 1.1 …… 8
1.2　集合与映射 …… 9
1. 集合的记号 …… 9
2. 子集与幂集 …… 9
3. 子集的运算 …… 10
4. 包含与排斥原理 …… 10
5. 映射的概念 …… 12
6. 映射的分类 …… 13
7. 映射的复合 …… 15
8. 映射的逆 …… 16
习题 1.2 …… 17
1.3　二元关系 …… 18
1. 二元运算与代数系统 …… 18
2. 二元关系 …… 19
3. 等价关系、等价类和商集 …… 19
4. 偏序和全序 …… 22
习题 1.3 …… 24
1.4　整数与同余方程 …… 24
1. 整数的运算 …… 25
2. 最大公因子和最小公倍数 …… 25
3. 互素 …… 29
4. 同余方程及孙子定理 …… 29
习题 1.4 …… 34

第 1 章小结 …… 35

第 2 章 群论 …… 37
2.1 基本概念 …… 37
1. 群和半群 …… 37
2. 关于单位元的性质 …… 39
3. 关于逆元的性质 …… 39
4. 群的几个等价性质 …… 40
习题 2.1 …… 45
2.2 子群 …… 45
1. 子群 …… 45
2. 元素的阶 …… 48
习题 2.2 …… 49
2.3 循环群和生成群,群的同构 …… 50
1. 循环群和生成群 …… 50
2. 群的同构 …… 51
3. 循环群的性质 …… 53
习题 2.3 …… 54
2.4 变换群和置换群,Cayley 定理 …… 55
1. 置换群 …… 56
2. Cayley 定理 …… 60
习题 2.4 …… 62
2.5 子群的陪集和 Lagrange 定理 …… 62
1. 子群的陪集 …… 62
2. 子群的指数和 Lagrange 定理 …… 64
习题 2.5 …… 66
2.6 正规子群和商群 …… 67
1. 正规子群的概念 …… 67
2. 正规子群的性质 …… 68
3. 商群 …… 69
4. 单群 …… 71
习题 2.6 …… 71
2.7 共轭元和共轭子群 …… 72
1. 中心和中心化子 …… 72

2. 共轭元和共轭类 …… 73
3. 共轭子群与正规化子 …… 74
4. 置换群的共轭类 …… 75
习题 2.7 …… 78
2.8 群的同态 …… 79
1. 群的同态 …… 79
2. 同态基本定理 …… 80
3. 有关同态的定理 …… 82
4. 自同态与自同构 …… 85
习题 2.8 …… 86
2.9 群对集合的作用,Burnside 引理 …… 87
1. 群对集合的作用 …… 87
2. 轨道与稳定子群 …… 88
3. Burnside 引理 …… 90
习题 2.9 …… 92
2.10 应用举例 …… 92
1. 项链问题 …… 93
2. 分子结构的计数问题 …… 96
3. 正多面体着色问题 …… 97
4. 开关线路的计数问题 …… 98
5. 图的计数问题 …… 99
6. RSA 密码系统的加密与解密变换 …… 101
7. 二次同余方程 …… 102
习题 2.10 …… 104
2.11 群的直积和有限可换群 …… 104
1. 群的直积 …… 104
2. 有限可换群的结构 …… 105
习题 2.11 …… 108
2.12 有限群的结构,Sylow 定理 …… 108
1. p-子群与 Sylow p-子群 …… 109
2. Sylow 定理 …… 109
习题 2.12 …… 112
第 2 章小结 …… 112

第 3 章 环论 …… 116
3.1 环的定义和基本性质 …… 116
1. 环的定义 …… 116
2. 环内一些特殊元素和性质 …… 118
3. 环的分类 …… 120
习题 3.1 …… 121
3.2 子环、理想和商环 …… 123
1. 子环 …… 123
2. 生成子环和生成理想 …… 126
3. 商环 …… 126
习题 3.2 …… 128
3.3 环的同构与同态 …… 129
1. 同构与同态 …… 129
2. 有关同态的一些定理 …… 130
3. 分式域 …… 132
习题 3.3 …… 133
3.4 整环中的因子分解 …… 134
1. 一些基本概念 …… 134
2. 既约元和素元 …… 135
3. 最大公因子 …… 135
习题 3.4 …… 137
3.5 惟一分解整环 …… 137
1. 惟一分解整环及其性质 …… 137
2. 主理想整环 …… 139
3. 欧氏整环 …… 141
习题 3.5 …… 142
3.6 多项式分解问题 …… 143
1. 本原多项式及其性质 …… 143
2. $D[x]$的分解性质 …… 144
3. 多项式的可约性判断 …… 146
习题 3.6 …… 148
3.7 应用举例 …… 148
1. 编码问题 …… 148
2. 多项式编码方法及其实现 …… 149

习题 3.7 …… 153
第 3 章小结 …… 153

第 4 章　域论 …… 155
4.1　域和域的扩张，几何作图问题 …… 155
1. 域的特征和素域 …… 155
2. 扩张次数，代数元和超越元 …… 157
3. 添加元素的扩张 …… 158
4. 代数扩张与有限扩张 …… 159
5. 几何作图问题 …… 160
习题 4.1 …… 163
4.2　分裂域，代数基本定理 …… 164
1. 分裂域 …… 164
2. 代数基本定理 …… 168
习题 4.2 …… 169
4.3　有限域，有限几何 …… 170
1. 有限域的构造及惟一性 …… 170
2. 有限域的元素的性质 …… 172
3. $Z_p[x]$中多项式的根 …… 174
4. 有限域的子域 …… 175
5. 有限域的自同构群 …… 175
6. 有限域上的元素和多项式的性质 …… 176
7. 有限几何 …… 177
习题 4.3 …… 180
4.4　单位根，分圆问题 …… 181
1. 单位根 …… 181
2. 分圆问题 …… 182
习题 4.4 …… 185
第 4 章小结 …… 185

第 5 章　方程根式求解问题简介 …… 188
5.1　多项式的 Galois 群 …… 189
1. 域和多项式的 Galois 群 …… 189
2. 多项式的 Galois 群的置换表示 …… 190

3. 多项式的 Galois 群的阶 …… 191
4. 多项式的 Galois 群的计算 …… 192
习题 5.1 …… 194
5.2 群的可解性和代数方程的根式求解问题 …… 194
1. 群的可解性 …… 194
2. 可解群的性质 …… 196
3. 代数方程的根式可解性 …… 197
习题 5.2 …… 198
第 5 章小结 …… 198

附录 其他代数系简介 …… 199
1. 格与布尔代数 …… 199
2. 模的概念及例 …… 201
3. 代数 …… 201
习题 …… 202

习题提示与答案 …… 203

符号索引 …… 218

名词索引 …… 220

参考文献 …… 223

第 1 章　引言和预备知识

第 1 章作为开场白，首先介绍近世代数的一些实际应用问题，并且以这些问题为线索展开全书的内容，所以读者对这些问题应大致有个印象.

本章的另一个内容是明确我们讨论问题的基础、平台，整理、罗列读者应该预先具备的数学知识，主要是有关集合、映射和整数运算方面的知识. 这些内容大部分是读者已经学过的，但也有一些可能是新的，例如孙子定理等. 关于本章内容读者只要通读即可，不必花费太多时间.

需要特别指出的是本章给出了“代数系统”的概念，这是近世代数的研究对象，是群、环、域等具体的模型的一般化，对今后的学习有指导意义.

1.1　几类实际问题

初等代数、高等代数和线性代数都称为**经典代数**(classical algebra)，它的研究对象主要是代数方程和线性方程组. **近世代数**(modern algebra)又称为**抽象代数**(abstract algebra)，它的研究对象是代数系. 所谓代数系，是由一个集合和定义在这个集合中的一种或若干种运算所构成的一个系统. 例如，整数集合$\mathbb{Z}$和普通的整数加法“+”构成一个代数系，记作$(\mathbb{Z},+)$. $\mathbb{Z}$和普通加法“+”以及普通乘法“·”两种运算也构成一个代数系，记作$(\mathbb{Z},+,\cdot)$.

由于近世代数在近代物理、近代化学、计算机科学、数字通信、系统工程等许多领域都有重要应用，因而它是现代科学技术的数学基础之一，许多科技人员都希望掌握它的基本内容与方法. 本书将以一些实际问题为背景，在初等代数和线性代数的基础上，由浅入深地介绍它的基本内容，使读者感到通俗易懂，饶有兴趣. 下面介绍几类与近世代数的应用有关的实际问题.

1. 一些计数问题

(1) 项链问题

这个问题的提法是，用 n 种颜色的珠子做成有 m 颗珠子的项链，问可做成多少种不同类型的项链？

首先需要对此问题作数学上的确切描述. 设由 m 颗珠子做成一个项链，可用一个正 m 边形来代表它，每个顶点代表一颗珠子. 从任意一个顶点开始，

沿逆时针方向，依次给每个顶点标以号码 $1,2,\cdots,m$. 这样的一个项链称为有标号的项链. 由于每一颗珠子的颜色有 n 种选择，因而由乘法原理可知，这些有标号的项链共有 n^m 种. 但是其中有一些项链可通过旋转一个角度或翻转 180°使它们完全重合. 对于这些项链，称它们本质上是相同的. 对那些无论怎样旋转或翻转都不能使它们重合的项链，称为本质上不同的项链，即为问题所提的不同类型的项链. 当 n 与 m 较小时，不难用枚举法求得问题的解答，读者不妨自行解决以下例子.

例 1.1.1　用黑、白两种颜色的珠子做成有 5 颗珠子的项链，问可以做成多少种不同类型的项链？

随着 n 与 m 的增加，用枚举法越来越困难，因而必须寻找更加有效的可解决一般的任意正整数 n 与 m 的方法. 采用群论方法可完全解决此问题，且至今尚未发现其他更为简单和有效的方法.

(2) 分子结构的计数问题

在化学中研究由某几种元素可合成多少种不同物质的问题，由此可以指导人们在大自然中寻找或人工合成这些物质.

例 1.1.2　在一个苯环上结合 H 原子或 CH_3 原子团，问可能形成多少种不同的化合物(图 1.1(a))？

如果假定苯环上相邻 C 原子之间的键都是互相等价的，则此问题就是两种颜色 6 颗珠子的项链问题.

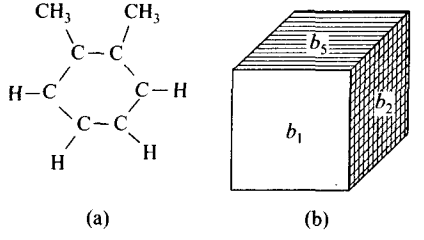

图　1.1

(3) 正多面体着色问题

对一个正多面体的顶点或面用 n 种颜色进行着色，问有多少种不同的着色方法？

下面以正六面体为例说明此问题的数学描述.

例 1.1.3　用 n 种颜色对正六面体的面着色，问有多少种不同的着色方法(图 1.1(b))？

首先建立此问题的数学模型，将问题中的一些概念进行量化.

设 n 种颜色的集合为

$$A=\{a_1,a_2,\cdots,a_n\},$$

正六面体的面集合为

$$B=\{b_1,b_2,b_3,b_4,b_5,b_6\},$$

则每一种着色法对应一个映射

$$f:B\to A,$$

反之，每一个映射 $f:B\to A$ 对应一种着色法. 由于每一个面的颜色有 n 种选择，所以全部着色法的总数为 n^6，但这样的着色法与面的编号有关，其中有些着色法可适当旋转正六面体使它们完全重合，对这些着色法，称它们本质上是相同的. 我们的问题是求本质上不同的着色法的数目.

当 n 很小时不难用枚举法求得结果，例如，当 $n=2$ 时，读者可以自己算出本质上不同的着色法数为 10，对于一般的情况则必须用群论方法才能解决.

(4) 图的构造与计数问题

首先介绍一下**图论**(graph theory)的一些基本概念.

设 $V=\{v_1,v_2,\cdots,v_n\}$，称为**顶点**集合(vertex set)，E 是由 V 的一些 2 元子集构成的集合，称为**边集**(edge set)，则称有序对 (V,E) 为一个**图**(graph)，记作 $G=(V,E)$.

例如，设 $V=\{1,2,\cdots,10\}$，$E=\{e_1,e_2,\cdots,e_{15}\}$，其中 $e_1=\{1,2\}$，$e_2=\{2,3\}$，$e_3=\{3,4\}$，$e_4=\{4,5\}$，$e_5=\{1,5\}$，$e_6=\{1,6\}$，$e_7=\{2,7\}$，$e_8=\{3,8\}$，$e_9=\{4,9\}$，$e_{10}=\{5,10\}$，$e_{11}=\{6,8\}$，$e_{12}=\{7,9\}$，$e_{13}=\{8,10\}$，$e_{14}=\{6,9\}$，$e_{15}=\{7,10\}$. 图 $G=(V,E)$ 可用图 1.2 来表示. 此图是图论中有名的 Petersen 图. 每一个顶点用圆圈表示，对边集 E 中的每一个元素 $\{i,j\}\in E$，用一条直线或曲线连接顶点 i 与 j. 顶点的位置及边的长短，形状均无关紧要.

一个图可以代表一个电路、水网络、通信网络、交通网络、地图等有形的结构，也可以代表一些抽象关系. 例如可用一个图表示一群人之间的关系，点代表人，凡有边相连的两个点表示他们互相认识，否则表示不认识，则这个图就表示出了这群人之间的关系. 图论中有许多有趣的问题，有兴趣的读者可阅读有关参考书.

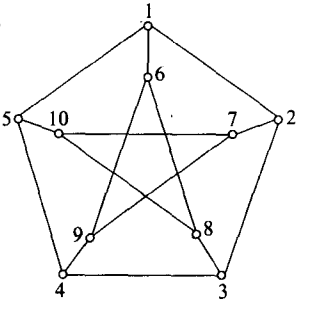

图 1.2

图论中自然会提出某类图有多少个的问题.

例 1.1.4 画出所有点数为 3 的图.

此问题可以这样来解决：首先画出 3 个顶点 1,2,3，在每两个点之间有

“无边”和“有边”两种情况，因而全部有 $2\times2\times2=2^3=8$ 种情况，每一种情况对应一个图(图 1.3).

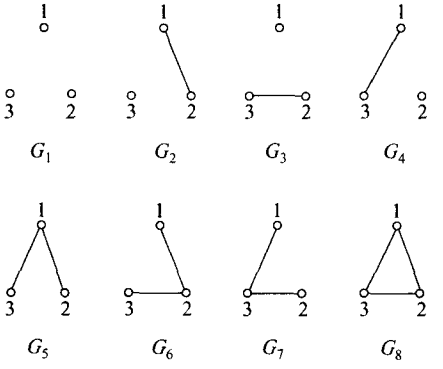

图　1.3

当点数为 n 时，共可形成 $\binom{n}{2}$ 个 2 元子集，每一个 2 元子集可以有对应图中的边或不对应图中的边两种情况，故可形成 $2^{\binom{n}{2}}$ 个图. 但是，我们观察一下图 1.3 中的 8 个图，可以发现有些图的构造是完全相同的，如果不考虑它们的点号，可以完全重合，称这样的图是同构的. 例如图 1.3 中的 G_2，G_3 与 G_4. 可以看出图 1.3 中的图，共有 4 个互不同构. 那么，对一般情况，n 个点的图中互不同构的图有多少个呢？这个问题也不能用初等方法来解决.

(5) 开关线路的构造与计数问题

一个有两种状态的电子元件称为一个开关，例如普通的电灯开关、二极管等. 由一些开关组成的二端网络称为开关线路. 一个开关线路的两端也只有两种状态：通与不通. 我们的问题是，用 n 个开关可以构造出多少种不同的开关线路？

首先必须对此问题建立一个数学模型，然后用适当的数学工具来解决它.

用 n 个变量 $x_1,x_2,\cdots,x_n$ 代表 n 个开关，每一个变量 x_i 的取值只能是 0 或 1，代表开关的两个状态. 开关线路的状态也用一个变量 f 来表示，f 的取值也是 0 或 1，代表开关线路的两个状态. f 是 $x_1,x_2,\cdots,x_n$ 的函数，称 f 为开关函数，记作

$$f(x_1,x_2,\cdots,x_n).$$

令 $A=\{0,1\}$，则 f 是 $\underbrace{A\times A\times\cdots\times A}_{n个}$ 到 A 的一个映射(函数)，反之，每一个

函数

$$f:A\times A\times\cdots\times A\to A$$

对应一个开关线路. 因此,开关线路的数目就是开关函数的数目. 下面来计算这个数目.

由于 f 的定义域的点数为 $|A|^n=2^n$,f 在定义域的每一个点上的取值有两种可能,所以全部开关函数的数目为 2^{2^n},这也就是 n 个开关的开关线路的数目.

但是上面考虑的开关线路中的开关是有标号的,有一些开关线路结构完全相同,只是标号不同,我们称这些开关线路本质上是相同的. 参见 2.10 节图 2.8的(a)与(b). 要进一步解决本质上不同的开关线路的数目问题,必须用群论方法.

2. 数字通信的可靠性问题与保密性问题

(1) 数字通信的可靠性问题

现代通信中用数字代表信息,用电子设备进行发送、传递和接收,并用计算机加以处理. 由于信息量大,在通信过程中难免出现错误. 为了减少错误,除了改进设备外,还可以从信息的表示方法上想办法. 用数字表示信息的方法称为编码. 编码学就是一门研究高效编码方法的学科. 下面用两个简单的例子来说明检错码与纠错码的概念.

例 1.1.5 简单检错码——奇偶性检错码.

设用 6 位二进制码来表示 26 个英文字母,其中前 5 位顺序表示字母,第 6 位作检错用,当前 5 位的数码中 1 的个数为奇数时,第 6 位取 1,否则第 6 位是 0. 这样编出的码中 1 的个数始终是偶数. 例如,

$$A:000011\qquad B:000101\qquad C:000110$$
$$D:001001\qquad \cdots$$

用这种码传递信息时可检查错误. 当接收一方收到的码中含有奇数个 1 时,则可断定该信息是错的,可要求发送者重发. 因而,同样的设备,用这种编码方法可提高通信的准确度.

但是,人们并不满足仅仅发现错误,能否不通过重发的办法,仅从信息本身来纠正其错误呢? 这在一定的程度上也可用编码方法解决.

例 1.1.6 简单纠错码——重复码.

设用 3 位二进制重复码表示 A,B 两个字母如下:

$$A:000\qquad B:111$$

则接收的一方对收到的信息码不管其中是否有错,均可译码如下: