新世纪信息安全系列教材

移位寄存器序列应用教程

YIWEI JICUNQI XULIE YINGYONG JIAOCHENG

李正朝　王　伟　李新国　编著

河南大学出版社

YIWEI JICUNQI XULIE YINGYONG JIAOCHENG

移位寄存器序列应用教程

李正朝　王　伟　李新国　编著

河南大学出版社
·开封·

图书在版编目(CIP)数据

移位寄存器序列应用教程/李正朝，王伟，李新国编著. —开封：河南大学出版社，2009.6

ISBN 978-7-81091-020-0

Ⅰ.移… Ⅱ.①李…②王…③李… Ⅲ.移位寄存器序列—教材 Ⅳ.017

中国版本图书馆 CIP 数据核字(2009)第 023089 号

责任编辑 梁宏伟
责任校对 梁宏伟
封面设计 王四朋

出版发行 河南大学出版社
地址：河南省开封市明伦街 85 号　　邮编：475001
电话：0378-2825001(营销部)　　网址：www.hupress.com
排　版 郑州市今日文教印制有限公司
印　刷 河南新华印刷集团有限公司
版　次 2009 年 6 月第 1 版　　**印　次** 2009 年 6 月第 1 次印刷
开　本 787mm×1092mm　1/16　　**印　张** 8.75
字　数 202 千字　　**印　数** 1—1000 册
定　价 22.00 元

前　言

当前，人类社会已经进入高度的信息化阶段，发达国家把信息化作为强国、富民、振兴经济、抢占新世纪制高点的国策. 网络化、数字化的特点使信息空间跨越国界，有别于传统的运作模式，信息安全成为数字化安全生存的基础和信息革命成败的关键.

“信息就是财富，安全才有价值”. 我们知道，密码技术是信息安全技术中的核心技术，而序列密码一直是作为军事和外交场合使用的主要密码技术，它的主要原理是：通过有限状态机产生性能优良的伪随机序列，使用该序列加密信息流得到密文序列. 所以，序列密码算法的安全强度完全决定于它所产生的伪随机序列的好坏. 产生好的序列密码的主要途径之一是利用移位寄存器产生伪随机序列，典型方法有：

1) 采用 n 阶非线性反馈函数产生大周期的非线性序列(如 M 序列).

2) 利用线性反馈移位寄存器加非线性前馈函数，产生前馈序列.

3) 利用一个寄存器序列作为时钟控制另一个寄存器序列(或自己控制自己)来产生钟控序列.

4) 通过组合运用以上方法，产生更复杂的网络，来实现复杂的序列.

5) 利用混沌理论、细胞自动机等方法产生伪随机序列.

当然，伪随机序列在其他方面有着广泛的应用，如通信、雷达、导航、自动控制、计算机、声学和光学测量、数字式跟踪、距离测量系统、数字网络系统的故障检测等等. 反馈移位寄存器优美奇妙的数学理论以及许多尚未解决的数学问题也引起了许多理论工作者的极大兴趣. 为了适应伪随机序列理论的不断发展和研究以及现实教学的需要，作者结合多年的教学实践，参考相关教材和大量资料，编写了这本教材.

本书是适用于信息安全、网络安全、应用数学、密码学及其他相关专业本科生的伪随机序列课程的教材，共分 11 章. 第 1～4 章由李正朝编写，第 5～8 章由王伟编写，第 9～11 章由李新国编写. 本书约有 200 道练习题，主要集中在线性移位寄存器部分，由于非线性部分的理论还不十分成熟，因此练习题就相对少一些. 为了充分理解教材内容，应该尽量解答大量的习题，否则就不可能有很大的进步. 许多习题都是例行的练习，当然部分习题也有一定的难度，但也不是深不可测的.

本书语言简练，通俗易懂，适合于有一定代数基础的大学高年级学生作为教材或教学

参考书.

在本书的编写过程中，得到了领导和数学教研室同行们的大力支持，在此一并表示感谢！由于编者水平有限，书中难免会有许多缺点和不当之处，敬请广大读者批评指正，我们将不胜感激！

编　者

2008 年 3 月于洛阳

目　录

第1章 预备知识

本章给出高等代数、近世代数、有限域等课程中的相关重要结论，只对少数结论给出证明过程，对这部分内容不熟悉的读者可参看相关教材.

1.1 线性变换

设集合 V_n 是数域 F 上的 n 维线性空间，$\underline{A}$ 是 V_n 上的线性变换. $\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n$ 是 V_n 的一组基，$\underline{A}$ 在某组基下的表示是一个 n 阶方矩阵 $\boldsymbol{A}$. V_n 上的所有线性变换组成的集合 K 构成一个线性空间，它与所有 n 阶方矩阵构成的 n^2 维线性空间同构. 称 n 次多项式 $f(x)=|x\boldsymbol{E}-\boldsymbol{A}|$ 为矩阵 $\boldsymbol{A}$ 的特征多项式，由哈密顿－凯莱定理知 $f(\boldsymbol{A})=0$.

1.1.1 线性变换的极小多项式

由于集合 K 是一个 n^2 维线性空间，因此 n^2+1 个线性变换 $\underline{\boldsymbol{E}},\underline{\boldsymbol{A}},\underline{\boldsymbol{A}}^2,\cdots,\underline{\boldsymbol{A}}^{n^2}$ 是线性相关的，即存在不全为 0 的数 $c_0,c_1,\cdots,c_{n^2}$ 使得 $c_0\underline{\boldsymbol{E}}+c_1\underline{\boldsymbol{A}}+\cdots+c_{n^2}\underline{\boldsymbol{A}}^{n^2}=0$ 成立. 就是说，存在次数不超过 n^2 的非零多项式 $f(x)$ 使得 $f(\underline{\boldsymbol{A}})=0$（$f(x)$ 叫 $\underline{\boldsymbol{A}}$ 的零化多项式）.

定义 1.1 设 $\underline{\boldsymbol{A}}$ 是 V_n 上的线性变换，在所有适合 $f(\underline{\boldsymbol{A}})=0$ 的非零多项式 $f(x)$ 中次数最低的首一多项式，称为 $\underline{\boldsymbol{A}}$ 的极小多项式.

结论 1.1 $\underline{\boldsymbol{A}}$ 的极小多项式是唯一的.

结论 1.2 设线性变换 $\underline{\boldsymbol{A}}$ 的极小多项式是 $m(x)$，$f(x)$ 是 $F[x]$ 中任意的多项式，则 $f(\underline{\boldsymbol{A}})=0$ 当且仅当 $m(x)\mid f(x)$，即 $\underline{\boldsymbol{A}}$ 的零化多项式 $f(x)$ 都是极小多项式 $m(x)$ 的倍式.

1.1.2 线性空间中元素的极小多项式

设 $\underline{\boldsymbol{A}}$ 的极小多项式是 $m(x)$，由于 $m(\underline{\boldsymbol{A}})=0$，因此，对于 V_n 中任意元素 $\boldsymbol{\alpha}$ 都有 $m(\underline{\boldsymbol{A}})\boldsymbol{\alpha}=0$. 但是对于某个固定的元素 $\boldsymbol{\alpha}$，在适合 $f(\underline{\boldsymbol{A}})\boldsymbol{\alpha}=0$ 的多项式 $f(x)$ 中，$m(x)$ 就不一定是次数最低的.

定义 1.2 设 $\underline{\boldsymbol{A}}$ 是 V_n 上的线性变换，$\boldsymbol{\alpha}$ 是 V_n 中一个固定的元素，在所有适合 $f(\underline{\boldsymbol{A}})\boldsymbol{\alpha}=0$ 的非零多项式 $f(x)$ 中次数最低的首一多项式，称为 $\boldsymbol{\alpha}$ 相对于 $\underline{\boldsymbol{A}}$ 的极小多项式，记作 $m_{\alpha}(x)$.

结论 1.3 上述定义中的 $m_\alpha(x)$ 是唯一的.

结论 1.4 设 $\underline{A}$ 是 V_n 上的线性变换，$\boldsymbol{\alpha}$ 是 V_n 中一个固定的元素，$\boldsymbol{\alpha}$ 相对于 $\underline{A}$ 的极小多项式是 $m_\alpha(x)$，$f(x)$ 是 $F[x]$ 中任意的多项式，则 $f(\underline{A})\boldsymbol{\alpha}=0$ 当且仅当 $m_\alpha(x)\mid f(x)$.

证明 必要性 设 $f(\underline{A})\boldsymbol{\alpha}=0$. 作带余除法

$$f(x)=m_\alpha(x)\cdot q(x)+r(x),$$

其中，$\partial^0 r(x)<\partial^0 m_\alpha(x)$ 或 $r(x)=0$，则 $r(\underline{A})\boldsymbol{\alpha}=f(\underline{A})\boldsymbol{\alpha}-m_\alpha(\underline{A})\cdot q(\underline{A})\boldsymbol{\alpha}=0$. 由 $m_\alpha(x)$ 的极小性可知，$r(x)=0$. 所以 $f(x)=m_\alpha(x)\cdot q(x)$，即 $m_\alpha(x)\mid f(x)$.

充分性 设 $m_\alpha(x)\mid f(x)$，则 $f(x)=m_\alpha(x)\cdot q(x)$，所以

$$f(\underline{A})\boldsymbol{\alpha}=m_\alpha(\underline{A})\cdot q(\underline{A})\boldsymbol{\alpha}=q(\underline{A})[m_\alpha(\underline{A})\boldsymbol{\alpha}]=q(\underline{A})[0]=0.$$

即 $\boldsymbol{\alpha}$ 相对于 $\underline{A}$ 的极小多项式 $m_\alpha(x)$ 一定是 $\underline{A}$ 的极小多项式 $m(x)$ 的因式.

设 $\boldsymbol{\alpha}$ 相对于 $\underline{A}$ 的极小多项式是 $m_\alpha(x)=x^m+c_{m-1}x^{m-1}+\cdots+c_1x+c_0$，由 $m_\alpha(\underline{A})\boldsymbol{\alpha}=0$ 得 $(\underline{A}^m+c_{m-1}\underline{A}^{m-1}+\cdots+c_1\underline{A}+c_0\underline{E})\boldsymbol{\alpha}=\underline{A}^m\boldsymbol{\alpha}+c_{m-1}\underline{A}^{m-1}\boldsymbol{\alpha}+\cdots+c_1\underline{A}\boldsymbol{\alpha}+c_0\underline{E}\boldsymbol{\alpha}=0$. 由此可知，向量组 $\underline{A}^m\boldsymbol{\alpha},\underline{A}^{m-1}\boldsymbol{\alpha},\cdots,\underline{A}\boldsymbol{\alpha},\underline{E}\boldsymbol{\alpha}$ 线性相关. $m_\alpha(x)$ 的极小性就表示向量组 $\underline{A}^{m-1}\boldsymbol{\alpha},\cdots,\underline{A}\boldsymbol{\alpha},\underline{E}\boldsymbol{\alpha}$ 必然线性无关.

把 $m_\alpha(\underline{A})\boldsymbol{\alpha}=0$ 写成

$$\underline{A}^m\boldsymbol{\alpha}=-c_{m-1}\underline{A}^{m-1}\boldsymbol{\alpha}-\cdots-c_1\underline{A}\boldsymbol{\alpha}-c_0\underline{E}\boldsymbol{\alpha},$$

则 $\underline{A}^m\boldsymbol{\alpha}$ 表示成 $\underline{A}^{m-1}\boldsymbol{\alpha},\cdots,\underline{A}\boldsymbol{\alpha},\underline{E}\boldsymbol{\alpha}$ 的线性组合. 当 $k>m$ 时，反复利用上式，向量 $\underline{A}^k\boldsymbol{\alpha}$ 都可以表示成 $\underline{A}^{m-1}\boldsymbol{\alpha},\cdots,\underline{A}\boldsymbol{\alpha},\underline{E}\boldsymbol{\alpha}$ 的线性组合.

结论 1.5 设 $\boldsymbol{\alpha}$ 相对于 $\underline{A}$ 的极小多项式 $m_\alpha(x)=x^m+c_{m-1}x^{m-1}+\cdots+c_1x+c_0$ 是 m 次的，那么向量组 $\underline{A}^{m-1}\boldsymbol{\alpha},\cdots,\underline{A}\boldsymbol{\alpha},\underline{E}\boldsymbol{\alpha}$ 必然线性无关. 而 m 维子空间 $L(\underline{A}^{m-1}\boldsymbol{\alpha},\cdots,\underline{A}\boldsymbol{\alpha},\underline{E}\boldsymbol{\alpha})$ 是 $\underline{A}$ 的一个不变子空间，所以 $m\leqslant n$，即 $\boldsymbol{\alpha}$ 相对于 $\underline{A}$ 的极小多项式 $m_\alpha(x)$ 的次数小于等于空间 V_n 的维数.

结论 1.6 设 $\underline{A}$ 是 V_n 上的线性变换，极小多项式为 $m(x)$. 若空间 V_n 由向量 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_t$ 生成，即 $V_n=L(\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_t)$，那么 $m(x)$ 等于 $m_{\alpha_1}(x),\cdots,m_{\alpha_t}(x)$ 的最小公倍式.

结论 1.7 设 $\underline{A}$ 是 V_n 上的线性变换，$\underline{A}$ 的极小多项式为 $m(x)$，那么在 V_n 中一定有一个向量 $\boldsymbol{\alpha}$，它相对于 $\underline{A}$ 的极小多项式 $m_\alpha(x)=m(x)$. 从而 $\underline{A}$ 的极小多项式 $m(x)$ 的次数小于等于空间 V_n 的维数.

结论 1.8 设 $\underline{A}$ 是 V_n 上的线性变换，$\boldsymbol{\alpha}\in V_n$，$g(x)\in F[x]$，如果 $\boldsymbol{\alpha}$ 相对于 $\underline{A}$ 的极小多项式为 $m_\alpha(x)$，则向量 $\boldsymbol{\beta}=g(\underline{A})\boldsymbol{\alpha}$ 相对于 $\underline{A}$ 的极小多项式 $m_\beta(x)=\dfrac{m_\alpha(x)}{(m_\alpha(x),g(x))}$. 从而 $m_\beta(x)$ 总是 $m_\alpha(x)$ 的因子，且 $m_\beta(x)=m_\alpha(x)$ 的充分必要条件是 $(m_\alpha(x),g(x))=1$.

1.1.3 循环子空间

设 $\underline{A}$ 是 V_n 上的线性变换，$L(\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_t)$ 是由向量 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_t$ 的所有线性组合构成的 V_n 的子空间，又称作由向量 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_t$ 所生成的子空间，它是包含 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_t$ 的最小子空间，但它不一定是 $\underline{A}$ 的不变子空间.

设 W 是包含 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_t$ 的最小 $\underline{A}$ 不变子空间，由 $\boldsymbol{\alpha}_1\in W$ 可知，$\underline{A}\boldsymbol{\alpha}_1\in W$，$\underline{A}^2\boldsymbol{\alpha}_1\in W$，$\underline{A}^3\boldsymbol{\alpha}_1\in W$，$\cdots$，即对于任意 $f(x)\in F[x]$，都有 $f(\underline{A})\boldsymbol{\alpha}_1\in W$. 对于 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_t$ 都有相

同的结论. 因此，如果 $\underline{A}$ 不变子空间 W 包含 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_t$，那么 W 就一定包含所有形为

$$f_1(\underline{A})\boldsymbol{\alpha}_1+f_2(\underline{A})\boldsymbol{\alpha}_2+\cdots+f_t(\underline{A})\boldsymbol{\alpha}_t$$

的向量，其中 $f_i(x)$ 是任意多项式. 显然，所有具有以上形式的向量构成一个 $\underline{A}$ 不变子空间，它就是包含 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_t$ 的最小 $\underline{A}$ 不变子空间，故称为由 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_t$ 生成的 $\underline{A}$ 不变子空间，而 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_t$ 称为这个不变子空间的一组生成元.

定义 1.3 设 $\underline{A}$ 是 V_n 上的线性变换，由一个向量生成的不变子空间称作循环子空间.

设循环子空间 W 是由 $\boldsymbol{\alpha}$ 生成的，$\boldsymbol{\alpha}$ 相对于 $\underline{A}$ 的极小多项式是 m 次的，因此向量组 $\underline{A}^{m-1}\boldsymbol{\alpha},\cdots,\underline{A}\boldsymbol{\alpha},\boldsymbol{\alpha}$ 必然线性无关. 当 $k>m$ 时，向量 $\underline{A}^k\boldsymbol{\alpha}$ 都可以表示成 $\underline{A}^{m-1}\boldsymbol{\alpha},\cdots,\underline{A}\boldsymbol{\alpha},\boldsymbol{\alpha}$ 的线性组合，而 $L(\underline{A}^{m-1}\boldsymbol{\alpha},\cdots,\underline{A}\boldsymbol{\alpha},\boldsymbol{\alpha})$ 是 $\underline{A}$ 的一个不变子空间，因此，由循环子空间的定义即有 $W=L(\underline{A}^{m-1}\boldsymbol{\alpha},\cdots,\underline{A}\boldsymbol{\alpha},\boldsymbol{\alpha})$，其中 $\underline{A}^{m-1}\boldsymbol{\alpha},\cdots,\underline{A}\boldsymbol{\alpha},\boldsymbol{\alpha}$ 是 W 的一组基.

结论 1.9 由 $\boldsymbol{\alpha}$ 生成的循环子空间的维数等于 $\boldsymbol{\alpha}$ 相对于 $\underline{A}$ 的极小多项式的次数.

结论 1.10 $\underline{A}$ 限制在循环子空间 W 上的极小多项式等于 W 的生成元 $\boldsymbol{\alpha}$ 相对于 $\underline{A}$ 的极小多项式(因为 $\underline{A}^k\boldsymbol{\alpha}$ 的极小多项式一定是 $\boldsymbol{\alpha}$ 的极小多项式的因式).

结论 1.11 $\underline{A}$ 限制在循环子空间 W 上，在一组适当基下的矩阵是有理块，其特征多项式等于极小多项式.

证明 设 $W=L(\underline{A}^{m-1}\boldsymbol{\alpha},\cdots,\underline{A}\boldsymbol{\alpha},\boldsymbol{\alpha})$，$W$ 的生成元 $\boldsymbol{\alpha}$ 相对于 $\underline{A}$ 的极小多项式为

$$m_\alpha(x)=x^m+c_{m-1}x^{m-1}+\cdots+c_1x+c_0.$$

令 $\varepsilon_1=\boldsymbol{\alpha},\varepsilon_2=\underline{A}\boldsymbol{\alpha},\varepsilon_3=\underline{A}^2\boldsymbol{\alpha},\cdots,\varepsilon_m=\underline{A}^{m-1}\boldsymbol{\alpha}$ 是 W 的一组基. 由关系

$$\underline{A}\varepsilon_1=\underline{A}\boldsymbol{\alpha}=\varepsilon_2,\underline{A}\varepsilon_2=\underline{A}^2\boldsymbol{\alpha}=\varepsilon_3,\cdots,\underline{A}\varepsilon_{m-1}=\underline{A}^{m-1}\boldsymbol{\alpha}=\varepsilon_m,$$

$$\underline{A}\varepsilon_m=\underline{A}^m\boldsymbol{\alpha}=-c_0\varepsilon_1-c_1\varepsilon_2-\cdots-c_{m-1}\varepsilon_m$$

可知，$\underline{A}$ 在这组基下的矩阵为

$$A=\begin{bmatrix}0&0&0&\cdots&0&-c_0\\1&0&0&\cdots&0&-c_1\\0&1&0&\cdots&0&-c_2\\\vdots&\vdots&\vdots&&\vdots&\vdots\\0&0&0&\cdots&0&-c_{m-2}\\0&0&0&\cdots&1&-c_{m-1}\end{bmatrix}.$$

显然，$\underline{A}$ 的特征多项式等于极小多项式.

结论 1.12 设 $\underline{A}$ 是 n 维线性空间 V_n 上的线性变换，则空间 V_n 是由一个向量生成当且仅当 $\underline{A}$ 的极小多项式的次数是 n，或者说 $\underline{A}$ 的极小多项式等于它的特征多项式.

1.2 模素数的有限域

把一个能够在其中进行某种意义下的加法“⊕”(包括减法)和乘法“⊗”(包括除法)两种运算的元素集合称为“域”，记作 F. 当然，域有其严格的数学公理化定义，从其公理出发，可以知道域对于加法和乘法运算是封闭的，域的零元素、负元素、单位元素、逆元素都

是唯一确定的.

域 F 中元素的个数称为 F 的阶. 如果 F 的阶是无限的,就把 F 称为无限域;如果 F 的阶是有限的,就把 F 称为有限域或伽罗瓦(Galois)域. 所有的有理数组成的集合,所有的实数组成的集合,所有的复数组成的集合,对于普通的加法和乘法来说都是域,而且都是无限域. 由 0 和 1 组成的二元集对于模 2 加法和乘法来说也是域,它是有限域的例子.

在伪随机序列的理论分析中,常常用到有限域这个数学工具. 下面是另一个有限域的例子.

设 p 是一个给定的素数,令 F_p 表示所有小于 p 的非负整数组成的集合,即

$$F_p=\{0,1,2,3,\cdots,p-1\}.$$

显然,对于普通的加法和乘法来说,F_p 不封闭,所以它不是域. 但是对于模 p 加法和乘法

$$(a\oplus b)=(a+b)\bmod p,(a\otimes b)=(a\times b)\bmod p$$

来说,F_p 是域. 它正好包含 p 个元素,是一个 p 元有限域. 当 $p=2$ 时,就是二元有限域 $F_2=\{0,1\}$. 应该指出,当 m 不是素数时,F_m 对于模 m 的加法和乘法来说不是域.

1.3 模不可约多项式的有限域

设 F 是一个给定的域,把系数 $a_i(i=0,1,2,\cdots,n)$ 属于 F,含有文字 x 的多项式 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ 称为系数属于 F 的多项式. $f(x)$ 中的每一项 a_ix^i 称为一个单项式,$f(x)$ 的次数记作 $\partial^0 f(x)$. 把 F 上的所有 x 的多项式组成的集合记作 $F[x]$. $F[x]$ 中的加法和乘法的运算规则如下:

设 $f(x)=\sum_{i=0}^{n}a_ix^i$,$g(x)=\sum_{i=0}^{m}b_ix^i$ 是 $F[x]$ 中的任意两个元素,假定 $n\geqslant m$,则规定它们的和为

$$f(x)+g(x)=\sum_{i=0}^{n}(a_i+b_i)x^i,$$

其中 $b_{m+1}=b_{m+2}=\cdots=b_n=0$;规定它们的积为

$$f(x)\cdot g(x)=\sum_{i=0}^{m+n}\left(\sum_{j=0}^{i}a_jb_{i-j}\right)x^i.$$

由于 $F[x]$ 含不具有逆元素的非零元素(例如 x 就没有倒元素),故在 $F[x]$ 中不能进行除法运算,但在 $F[x]$ 中还是可以进行带余除法. 设 $a(x)$ 和 $b(x)$ 是 $F[x]$ 中的两个多项式,而且 $b(x)\neq 0$,那么 $F[x]$ 中总能找到一对多项式 $q(x)$(称为商)和 $r(x)$(称为余式),使得 $a(x)=q(x)b(x)+r(x)$,$\partial^0 r(x)<\partial^0 b(x)$,这个式子就称作带余除法算式. 用符号 $r(x)=(a(x))_{b(x)}$ 来表示用 $b(x)$ 去除 $a(x)$ 所得的余式.

设 $f(x)$ 是 $F[x]$ 中的一个多项式,a 是 F 中的一个元素,用 $(x-a)$ 去除 $f(x)$,得到 $f(x)=q(x)(x-a)+c$. 如令 $x=a$,则得 $f(a)=c$. 这说明,用 $(x-a)$ 去除 $f(x)$ 所得的余式 c 就是 $x=a$ 时 $f(x)$ 的值 $f(a)$. 如果 $f(a)=0$,就说 a 是 $f(x)$ 的根. 显然,a 是 $f(x)$ 的根当且仅当 $(x-a)$ 能除尽 $f(x)$,即 $(x-a)\mid f(x)$. 设 $\partial^0 f(x)=n$,则 $f(x)$ 最多有 n 个不同

的根.

仿照模 n 运算的规定,也可以规定出模 $n(x)$ 运算规则.

设 $n(x)\in F[x]$,$\partial^0 n(x)=n$. 用 $F[x]_{n(x)}$ 表示 $F[x]$ 中所有次数小于 n 的多项式的集合,即 $F[x]_{n(x)}=\{a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}\}$,其中 $a_i(i=0,1,2,\cdots,n-1)$ 属于 F. 设 $a(x)$ 和 $b(x)$ 是 $F[x]_{n(x)}$ 中的两个元素. 规定它们的和与积如下:

$$a(x)\oplus b(x)=(a(x)+b(x))_{n(x)},a(x)\otimes b(x)=(a(x)\cdot b(x))_{n(x)},$$

把这样规定的加法和乘法称为模 $n(x)$ 加法和乘法.

如上所述,如果给定一个素数 p 后,便可以构造出一个包含 p 个元素的有限域 F_p. 类似地,如果给定一个 n 次不可约多项式 $p(x)$ 后,也可以构造出一个对于模 $p(x)$ 加法和乘法来说是有限域的集合

$$F[x]/(p(x))=\{a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}\},$$

其中 $a_i(i=0,1,2,\cdots,n-1)$ 属于 F. 如果 F 是由 p 个元素组成的有限域 F_p,而 a_i 可以取 p 个元素之一,则 $F[x]/(p(x))$ 就是一个包含 p^n 个元素的有限域.

用一个素数 p 构造出一个 p 阶有限域 F_p 和用一个 n 次不可约多项式 $p(x)$ 构造出一个 p^n 阶有限域 $F[x]/(p(x))$ 是两个具有代表性的有限域. 这是因为所有阶数相同的有限域都是同构的. 所谓同构关系,通俗地说就是一一对应关系. 设有两个域 F 和 F',如果在它们的元素之间可以建立起一个一一对应关系,即 F 中的 a 对应于 F' 中的 $\sigma(a)$,表示成:$a\to\sigma(a)$,而且有 $a+b\to\sigma(a)+\sigma(b)$,$a\cdot b\to\sigma(a)\cdot\sigma(b)$,就称 F 与 F' 同构.

1.4 交换群

设在一个域中可以进行所谓的加法和乘法两种运算. 如果在一个集合 G 中只能进行加法或乘法运算,且符合某些公理,就把集合 G 称为加法群或乘法群. 如果群中的运算满足交换律,就称这个群为交换群. 如果交换群 G 中元素个数有无限个,就称为无限交换群;如果交换群 G 中元素个数是有限个,就称为有限交换群. 显然,域 F 对于加法来说是一个交换群,而域 F 中所有非零元素组成的集合 F^*,对于乘法来说也是一个交换群.

设任意 $a\in G$,G 是一个交换群,如果对于任意正整数 n,都有 $a^n\neq1$,就把 a 称为无限阶元素;如果有正整数 n,使得 $a^n=1$,就把 a 称为有限阶元素,而使 $a^n=1$ 的最小正整数 n 称为 a 的阶. 如果 a 是一个 n 阶元素,那么 n 个元素 $a^0=1,a,a^2,\cdots,a^{n-1}$ 是 G 中 n 个不同的元素. 因此,有限交换群中所有的元素都是有限阶的.

设 G 是一个 n 阶乘法交换群,如果 G 中有一个 n 阶元素 a 存在,则 G 中 n 个不同的元素都可以表示成 a 的方幂,这时 $G=\{a^0=1,a,a^2,\cdots,a^{n-1}\}$ 称作一个 n 阶循环群,而 a 称作 G 的一个生成元,且 $a^n=1$.

可以证明:任一个有限域 F 中所有非零元素组成的集合 F^* 都是循环群,F^* 中一定有生成元存在,而有限域的交换乘法群的生成元称为该有限域的本原元.

1.5 本原多项式

设 $f(x)$是 $F_2[x]$中的次数等于 n 的多项式，常数项不等于 0，使得 $f(x)|(x^l-1)$的最小正整数 l 称作 $f(x)$的周期，记作 $p(f)$.

结论 1.13 设 $f(x)$是 $F_2[x]$中的次数等于 n 的多项式，且其常数项不为 0，如果 $f(x)|(x^l-1)$，则 $p(f)|l$.

结论 1.14 设 $f(x)$是 $F_2[x]$中的次数等于 n 的不可约多项式，且其常数项不等于 0，则 $p(f)|(2^n-1)$.

定义 1.4 设 $f(x)$是 $F_2[x]$中的次数等于 n 的不可约多项式，且其常数项不等于 0，若 $p(f)=2^n-1$，则称 $f(x)$是本原多项式.

结论 1.15 $F_2[x]$中的所有 r 大于一次不可约多项式必然能除尽 $x^{2^r-1}+1$.

证明 任意给定一个 $F_2[x]$中 r 大于一次不可约多项式 $f(x)$，便可以构造出一个对于模 $f(x)$加法和乘法来说是有限域的集合

$$F_2[x]/(f(x))=\{a_0+a_1x+a_2x^2+\cdots+a_{r-1}x^{r-1}\},$$

其中 $a_i(i=0,1,2,\cdots,n-1)$属于 F_2. $F_2[x]/(f(x))$中共有 2^r 个不同元素，因此，$F_2[x]_{f(x)}$的阶为 2^r. 由于任一个有限域中所有非零元素组成的集合都构成乘法循环群，故它的生成元为该有限域的本原元. 这就是说，$F_2[x]/(f(x))$中必有本原元存在. 设 a 是 $F_2[x]/(f(x))$中的一个本原元，则 $F_2[x]/(f(x))$中所有非零元素都可以表示成 a 的幂，即

$$F_2[x]/(f(x))=\{0,a^0,a,a^2,\cdots,a^{2^r-2}\}.$$

因为 a 是 $F_2[x]/(f(x))$中的一个本原元，因而 $a^{2^r-1}=1$. 于是对于任意元素 a^k，有 $(a^k)^{2^r-1}=(a^{2^r-1})^k=1$，这就是说，$F_2[x]/(f(x))$中所有非零元素都满足条件 $a^{2^r-1}=1$ 或 $a^{2^r-1}+1=0$，而 x 显然是 $F_2[x]/(f(x))$中的一个非零元素，因此它必然满足上式，即 $x^{2^r-1}+1=0$. 因为 $F_2[x]/(f(x))$是模 $f(x)$运算的有限域，所以上式的含义就是

$$(x^{2^r-1}+1)_{f(x)}=0.$$

即是说，任意 n 次不可约多项式 $f(x)$必然能除尽 $x^{2^r-1}+1$.

结论 1.16 有限域上元素的极小多项式都是不可约的. 当然，任何域上的极小多项式在自身上都是不可约的(关键在于域中无零因子).

结论 1.17 任意给定一个 $F_2[x]$中 r 大于一次不可约式 $f(x)$，则 $f(x)$的 r 个根全在 $F_2[x]/(f(x))$中.

结论 1.18 r 大于一次不可约多项式的个数 $I_r=\dfrac{1}{r}\sum\limits_{d|r}2^d\mu\left(\dfrac{r}{d}\right)$，其中 $\mu(\cdot)$为墨比乌斯(Möbius)函数.

由于并非所有的不可约多项式都是本原多项式，那么，在所有的 r 大于一次不可约多项式中究竟有多少个本原多项式呢?

设有限域 F_{2^r} 的阶是 2^r，即 F_{2^r} 中包含 2^r 个元素，a 是 F_{2^r} 的一个本原元，则 a 的阶为 $p=2^r-1$，即 $a^p=1$，于是 $F_{2^r}^*$ 中的所有 $p=2^r-1$ 个元素都可以表示成 a 的幂

$$F_{2^r}^*=\{a^0=1,a,a^2,\cdots,a^{p-1}\}.$$

结论 1.19 设 a 是 F^* 的一个 n 阶元，k 是任意正整数，则 a^k 的阶 m 满足 $m=\frac{n}{(k,n)}$，其中(k,n)表示 k 和 n 的最大公因子.

证明 由于$(a^k)^{\frac{n}{(n,k)}}=a^{\frac{kn}{(n,k)}}=(a^n)^{\frac{k}{(n,k)}}=1$，所以 $m\left|\frac{n}{(n,k)}\right.$. 又由于$(a^k)^m=a^{km}=1$，根据 a 是 n 阶元，即 $a^n=1$，故 $n|km$. 将 n,k 写成 $n=\frac{n}{(n,k)}\cdot(n,k)$，$k=\frac{k}{(n,k)}\cdot(n,k)$，则由 $n|km$，可得 $\frac{n}{(n,k)}\left|\frac{k}{(n,k)}\cdot m\right.$，但 $\left(\frac{n}{(n,k)},\frac{k}{(n,k)}\right)=1$，所以 $\frac{n}{(n,k)}\left|m\right.$，从而有 $m=\frac{n}{(k,n)}$.

显然，当$(k,n)=1$ 时，a 与 a^k 都是 n 阶元素，于是有下面结论.

结论 1.20 设 F_{2^r} 是 $p+1=2^r$ 阶的有限域，则 $F_{2^r}^*$ 是 p 阶循环群. 设 a 是 F_{2^r} 的本原元，则 a^k 也是 F_{2^r} 的本原元当且仅当$(k,p)=1$.

在 F_{2^r} 中共有 $p=2^r-1$ 个非零元素，它们是 $a^0=1,a,a^2,\cdots,a^{p-1}$，用函数 $\varphi(p)$表示小于 p 并且与 p 互素的正整数的个数，于是可得到下面结论.

结论 1.21 设 F_{2^r} 是 $p+1=2^r$ 阶的有限域，则 F_{2^r} 中共有 $\varphi(p)$个本原元.

如果 a 是 F_{2^r} 的本原元，则 $a^p=1$，因而$(a^k)^p=(a^p)^k=1(k=0,1,\cdots,p-1)$. 这就是说，$F_{2^r}^*$ 中的任一元素都是 $x^p-1=0$ 的根. 而 $x^p-1=0$ 最多只有 p 个不同的根，因此 $x^p-1=0$ 就以 $F_{2^r}^*$ 中 p 个元素为它的所有根. 正因为这样，把 a 称为 $x^p-1=0$ 的本原根.

结论 1.22 设 x^p-1 是 F_2 上的多项式，则 x^p-1 在 F_2 中有 $\varphi(p)$个本原根.

结论 1.23 多项式 x^m-1 能除尽 x^n-1 的充分必要条件是 $m|n$.

证明 充分性 设 $n=dm$，则由 $x^m=1$ 可得$(x^m)^d=x^n=1$，因此 x^m-1 的所有根都是 x^n-1 的根，所以$(x^m-1)|(x^n-1)$.

必要性 设 $n=dm+c,0\leqslant c<m$，并且$(x^m-1)|(x^n-1)$，根据 $x^m=1$ 可得 $x^{md+c}=(x^m)^dx^c=x^c=1$，因此，$(x^m-1)|(x^c-1)$，所以 $c=0$，即 $m|n$.

结论 1.24 设 F_{2^r} 是 $p+1=2^r$ 阶的有限域，则 p 阶循环群 $F_{2^r}^*$ 中任意元素的阶一定是 p 的因子.

结论 1.25 一个 r 大于一次不可约多项式 $f(x)$是本原多项式的充分必要条件是它的根是 $x^{2^r-1}-1$ 的本原根，即是 2^r 阶有限域 F_{2^r} 的本原元.

结论 1.26 r 大于一次本原多项式的个数为$\frac{\varphi(2^r-1)}{r}$.

证明 设 J_r 表示 r 次本原多项式的个数. 由结论 1.25 知，这 J_r 个 r 次本原多项式的所有 rJ_r 个根都是 $x^{2^r-1}-1$ 的本原根，而且这 rJ_r 个根都是 $x^{2^r-1}-1$ 的所有本原根. 由结论 1.22 知，$x^{2^r-1}-1$ 总共有 $\varphi(2^r-1)$个本原根，因此，r 次本原多项式的个数

$$J_r=\frac{\varphi(2^r-1)}{r}.$$

第 2 章　LFSR 的数学描述

LFSR(Linear Feedback Shift Register)即线性反馈移位寄存器. 本章主要讨论用于刻画线性反馈寄存器特性的几个数学工具,包括状态转移矩阵、特征多项式、生成函数等. 线性反馈寄存器相对于非线性反馈寄存器来说,在结构上比较简单,研究方法上有比较满意的数学工具,因而目前已经有了相当完备的理论结果,并在实践中获得了广泛的应用. 为了简单和实用起见,讨论只限于二元有限域 F_2 的情形.

2.1　LFSR 的定义

一般 n 级反馈移位寄存器的基本结构如图 2.1 所示. 它由串联的 n 个二元寄存器及一个开关网络构成. 每个寄存器看作一级,从右至左,分别为该反馈移位寄存器的第 1 级,第 2 级,…,第 n 级. 图中的 $a_0, a_1, \cdots, a_{n-1}$ 是各级寄存器所处的状态,取值 0 或者 1,可视为有限域 F_2 中的元素. 向量 $\boldsymbol{\alpha}^0 = (a_0, a_1, \cdots, a_{n-1})$ 称为移位寄存器第 0 时刻的状态,也称为反馈移位寄存器的初始状态(简称初态),第 i 时刻的状态记为

$$\boldsymbol{\alpha}^i = (a_i, a_{i+1}, \cdots, a_{i+n-1}).$$

显然,n 级反馈移位寄存器共有 2^n 个可能的不同状态.

图中下方的方框表示一个开关网络,可视为具有 n 个输入端及一个输出端的组合门电路. 这一电路可由一个含有 n 个变元 $x_0, x_1, \cdots, x_{n-1}$ 的布尔函数 $f(x_0, x_1, \cdots, x_{n-1})$ 来表示,称该布尔函数为反馈移位寄存器的反馈函数(或反馈逻辑).

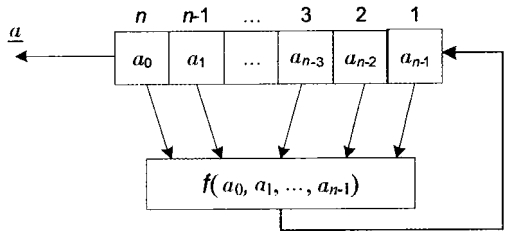

图 2.1

反馈移位寄存器是受时钟脉冲驱动的. 假定在第 i 个时钟脉冲到来时,移位寄存器的状态是 $\boldsymbol{\alpha}^i = (a_i, a_{i+1}, \cdots, a_{i+n-1})$,则在下一个时钟脉冲到来时,移位寄存器的状态变为

$$\boldsymbol{\alpha}^{i+1}=(a_{i+1},\cdots,a_{i+n-1},a_{i+n}),$$

其中 $a_{i+n}=f(a_i,a_{i+1},\cdots,a_{i+n-1})$. 即是说,反馈移位寄存器在一个时钟周期内完成了移位、输出和反馈操作. 移位操作将每一级寄存器的内容顺序左移,输出操作将第 n 级寄存器的内容 a_i 输出,反馈操作将开关网络的输出值 a_{i+n} 置为反馈移位寄存器第 1 级的内容.

不间断地对上述反馈移位寄存器施加时钟脉冲,则该反馈移位寄存器就可以输出一个 0,1 序列:$a_0,a_1,\cdots,a_{n-1},a_n,a_{n+1},\cdots$,记为$\underline{a}=(a_0,a_1,\cdots,a_{n-1},a_n,a_{n+1},\cdots)$. 显然,输出什么样的序列完全由反馈移位寄存器的初态 $\boldsymbol{\alpha}^0$ 和反馈函数 $f(x_0,x_1,\cdots,x_{n-1})$决定.

定义 2.1 若 n 级反馈移位寄存器的反馈函数是线性齐次函数

$$f(x_0,x_1,\cdots,x_{n-1})=\sum_{i=0}^{n-1}c_ix_i,c_i\in F_2,i=0,1,2,\cdots,n-1. \tag{1}$$

则称得到的反馈移位寄存器为线性反馈移位寄存器,简称线性移存器.

等价地,可以将定义 2.1 中的式(1)改为形式

$$f(x_0,x_1,\cdots,x_{n-1})=\sum_{i=0}^{n-1}c_{n-i}x_i,c_i\in F_2,i=1,2,3,\cdots,n. \tag{2}$$

则图 2.1 可以具体化为图 2.2 所示的 n 级线性反馈移位寄存器.

可以看到,图 2.2 中的开关网络由 $c_1,c_2,\cdots,c_n$ 这 n 个开关和一个加法器构成. 实际上,$c_1,c_2,\cdots,c_n$ 表示各级是否抽头参与反馈:若第 i 级抽头,则 $c_i=1$;若第 i 级不抽头,则 $c_i=0$. 本书中所讨论的线性反馈移存器都是基于图 2.2 的,并且讨论的重点放在第 n 级一定抽头,即 $c_n=1$ 的情况,称之为 n 级非退化的线性反馈移位寄存器.

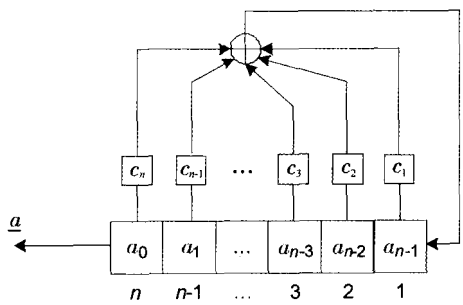

图 2.2

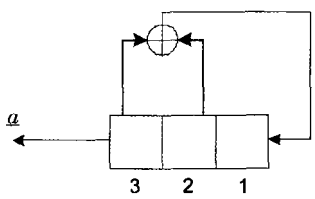

图 2.3

显然,在式(2)的约定下,图 2.2 所示线性反馈移位寄存器所输出的序列

$$\underline{a}=(a_0,a_1,\cdots,a_{n-1},a_n,a_{n+1},\cdots)$$

满足关系式

$$\begin{aligned}a_{n+i}&=c_1a_{n-1+i}+c_2a_{n-2+i}+\cdots+c_na_i\\&=\sum_{j=1}^{n}c_ja_{n-j+i},c_i\in F_2,\quad i=1,2,3,\cdots,n.\end{aligned} \tag{3}$$

称该输出序列为线性移位寄存器序列,称 $a_n,a_{n+1},\cdots,a_{n+i}$分别为线性移存器第 0 时刻,第 1 时刻,…,第 i 时刻的反馈符号. 式(3)说明,图 2.2 所示的线性移存器在第 i 时刻的反馈符号可以表示成第 i 时刻状态 $\boldsymbol{\alpha}^i=(a_i,a_{i+1},\cdots,a_{i+n-1})$中符号的线性组合. 式(3)完全刻画了一个线性移存器的功能,习惯上,也将该式称为线性移存器的反馈函数.

例 2.1 图 2.3 给出了一个 3 级非退化线性移存器. 据图可知，$c_3=c_2=1, c_1=0$，所以该 LFSR 的反馈函数为

$$a_{3+i}=\sum_{j=1}^{3}c_j a_{3-j+i}=a_i+a_{1+i},\ i=0,1,2,\cdots.$$

若预置初态为 $\boldsymbol{\alpha}^0=(0,1,1)$，即 $a_0=0, a_1=1, a_2=1$，则有

$$a_3=a_0+a_1=1, a_4=a_1+a_2=0, a_5=a_2+a_3=0, a_6=a_3+a_4=1,$$
$$a_7=a_4+a_5=0, a_8=a_5+a_6=1, a_9=a_6+a_7=1,\cdots.$$

继续下去，得到该线性移存器的输出序列 $\underline{a}=(0111001011\cdots)$. 同时，得到

$$\boldsymbol{\alpha}^1=(1,1,1), \boldsymbol{\alpha}^2=(1,1,0), \boldsymbol{\alpha}^3=(1,0,0), \boldsymbol{\alpha}^4=(0,0,1),$$
$$\boldsymbol{\alpha}^5=(0,1,0), \boldsymbol{\alpha}^6=(1,0,1), \boldsymbol{\alpha}^7=(0,1,1),\cdots.$$

显然，由输出序列 $\underline{a}$ 就可以直接写出状态序列 $\boldsymbol{\alpha}^0, \boldsymbol{\alpha}^1, \boldsymbol{\alpha}^2, \boldsymbol{\alpha}^3, \boldsymbol{\alpha}^4, \cdots$；反之亦然.

定义 2.2 相对定义 2.1，如果 n 级反馈移位寄存器的反馈函数不是线性齐次函数，则称此移存器为非线性反馈移位寄存器.

第 7,8,9,10 章将介绍非线性反馈移位寄存器的基本研究方法和一些基本结论.

定义 2.3 无限序列 $\underline{a}=(a_0, a_1, \cdots, a_{n-1}, a_n, a_{n+1}, \cdots)$ 称为一个线性递推序列，如果序列中的每个符号适合一个线性递推关系式

$$a_{n+i}=\sum_{j=1}^{n}c_j a_{n-j+i}, i=1,2,\cdots.$$

其中，$c_j\in F_2, j=1,2,3,\cdots,n$.

例 2.1 中线性移存器的输出序列 $\underline{a}=(0111001011\cdots)$ 适合关系式

$$a_{3+i}=a_i+a_{1+i},\ i=0,1,2,\cdots.$$

所以 $\underline{a}$ 是一个线性递推序列.

显然，线性递推序列不过是线性反馈移位寄存器序列的一个数学说法，而线性反馈移位寄存器序列是线性递推序列的物理实现.

2.2 LFSR 的状态转移变换

2.2.1 状态转移变换和状态转移矩阵

若将 n 级线性移存器每一时刻的内部状态看成是 F_2 上的一个 n 维向量，则移存器的全部 2^n 个可能状态就构成了 F_2 上的 n 维向量空间，记作 $V_n(F_2)$.

定义 2.4 移存器由一个时刻的状态变到下一时刻状态，可以看作是线性空间 $V_n(F_2)$ 的一个变换，称为状态转移变换，记为 $\underline{\boldsymbol{A}}$.

显然，若 n 级线性移存器第 $i(i=0,1,2,\cdots)$ 时刻的状态为 $\boldsymbol{\alpha}^i=(a_i, a_{i+1}, \cdots, a_{i+n-1})$，则第 $i+1$ 时刻的状态为

$$\boldsymbol{\alpha}^{i+1}=\underline{\boldsymbol{A}}(\boldsymbol{\alpha}^i)=(a_{i+1}, a_{i+2}, \cdots, a_{i+n-1}, \sum_{j=1}^{n}c_j a_{n-j+i}).$$