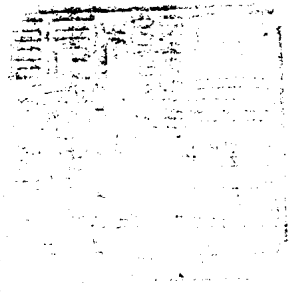
伪随机序列及其应用

肖国镇　梁传甲　王育民　编著

国防工业出版社

伪随机序列及其应用

肖国镇　梁传甲　王育民　编著



国防工业出版社

内 容 简 介

本书介绍伪随机序列的理论与应用。

本书共分六章。前三章介绍线性和非线性移位寄存器的基本理论。第四、五章讨论实际应用中最为关心的伪随机序列的相关函数特性。第六章介绍伪随机序列的各种应用：即在伪码测距、导航、伪码多址、数字数据加乱器、噪声产生器、数据保密系统中的应用举例。

本书所需用的数学知识尽量采用为工程技术人员容易接受的方式阐述。

伪随机序列的理论近几年来又发现了在一些新兴领域中的应用。多维伪随机序列的研究正在受到广泛的重视。

本书可作为通信、雷达、导航、遥控、遥测及计算机等有关专业的大学生、研究生和工程技术人员的参考书。

伪随机序列及其应用

肖国镇　梁传甲　王育民　编著

责任编辑：李　端

*

国防工业出版社出版

新华书店北京发行所发行　　各地新华书店经售

国防工业出版社印刷厂印装

*

850×1168 1/32　印张12 1/2　330千字

1985年3月第一版　1985年3月第一次印刷　印数：0,001— 4,600册

统一书号：15034·2727　　定价：2.40元

序

伪随机序列（或称伪噪声序列）的理论与应用，从产生到发展，算来已有二十几年的历史了。但是，这项新理论与新技术并不象某些其它所谓新思想那样，突然爆发出来，形成一阵热潮，尔后不久便逐渐消声匿迹乃至无人问津了。伪随机序列的理论在它形成的初期，便在通信、雷达、导航以及密码学等重要的技术领域中获得了广泛的应用。而在近年来的发展中，它的应用范围远远超出了上述领域之外，如自动控制、计算机、声学和光学测量、数字式跟踪和测距系统以及数字网络系统的故障检测等。正象它的丰富多采的应用吸引着许多工程技术工作者一样，它的优美奇妙的数学理论以及许多尚待解决的数学问题也引起了理论工作者的极大兴趣。为了进一步发展伪随机序列的理论与应用研究，我们认为在国内出版一本既有一定理论深度又注重这一新理论广泛应用的书是适宜的。这正是我们试图写作这一本书的主要目的。在这方面，我们特别感谢万哲先教授的鼓励与支持，他曾多次建议我们编写一套有关伪随机码与编码理论及其应用的书。

本书共分六章。前三章介绍线性和非线性移位寄存器的基本理论。这方面所需要的数学理论主要是伽罗瓦（Galois）域论。本书假定读者对这一理论已有一定程度的了解。对于不太熟悉这一理论的读者，可参看万哲先教授所著的《代数与编码》这本理论著作。本书的第四、五两章讨论实际应用中最为关心的伪随机序列的相关函数特性。第六章介绍伪随机序列的各种应用。伪随机序列在工程技术上有很多成功的应用，由于涉及的面很广而又多样化，本书不可能包罗万象。但是，我们试图对伪随机序列的几种典型应用作一较为清晰的介绍。自然，难免在题材的选取上受到了主观因素的影响。好在书末列入了有关的参考文献，以供读

者去深入研究更广泛的课题。

研究生何大可同志在本书的写作过程中帮了很大的忙。他在本书的某些部分做了整理加工以及抄写、绘图的工作，并为本书中所介绍的一些算法编制了计算程序。考虑到多元伪随机序列的理论与应用的新近发展，已将此项内容作为附录列入本书。书末有关的附表以及这一附录都是何大可同志编写的。

作者还感谢西北电讯工程学院资料室的同志在本书写作过程中所给予的支持和帮助。感谢编码讨论班同志们的鼓励、批评和建议。由于我们的水平有限，本书难免会有许多缺点及不当之处，诚恳地希望得到广大读者批评和指正。

目　录

第一章　反馈移位寄存器的基本概念

大家知道，一般控制系统大体上可分为动态系统与静态系统两大类。在所谓动态系统中，其系统特性是由含有时间参数的输出、输入变量的微分方程来描述。而在静态系统中，其系统特性可用没有时间参数的方程来描述。此时，系统在每一瞬间的输出仅由同一瞬间的输入来决定。近年来在数字设备中所考虑的，是一种特殊的静态系统，即所谓二元系统。这种系统中的变量只取两个值，简单地表示为“0”和“1”。描述这种二元系统的方程可由含有逻辑运算“与”、“或”、“非”的关系来表示。有时也把这种二元系统称作静态逻辑系统，它是电子工程实践中最为重要的静态系统。

在本书中我们所要讨论的是一种典型的二元系统，即所谓反馈移位寄存器。由于这种装置在无线电电子技术中具有广泛的应用，因而近年来特别引起人们的重视。

在本章中，我们将对反馈移位寄存器的基本结构及其有关概念做一大致的介绍。从本质上说，我们的论述可以在q元域$GF(q)$上进行。但是，考虑到目前具有实用价值的仍然是二元的情况，因此我们仅在二元域$GF(2)$中进行讨论。为简便，今后用$\boldsymbol{F}_q$与$\boldsymbol{F}_2$分别代表$GF(q)$与$GF(2)$。

§1.1　反馈移位寄存器

现在我们来考察一般反馈移位寄存器的基本结构。图1.1.1是这种反馈移位寄存器的框图。它由串联的n个二元移存器及一个开关网络构成。众所周知，每一个二元存储器即为一个双稳态触发器，它的两种状态分别记为“1”与“0”，每个触发器看作一级。因此，图1.1.1可以看作是一个r级反馈移位寄存器。图

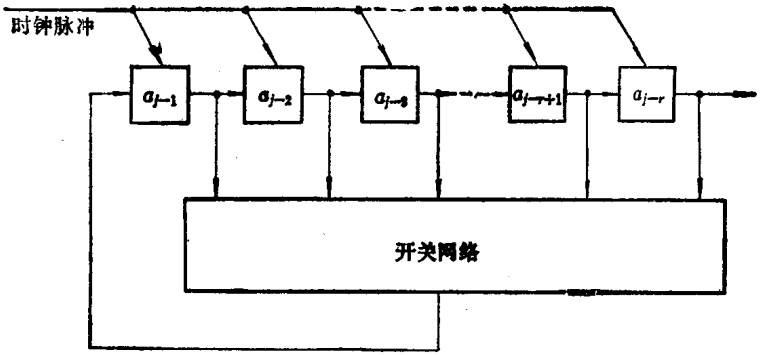


图1.1.1 一般反馈移位寄存器示意图

中上面一排小方框，自左至右，分别称为第1级、第2级、第3级、…、第 $r-1$ 级及第 r 级存储器。下面一个长方框内所示的开关网络可视为具有 r 个输入端及一个输出端的组合门电路。从理论上来说，这一组合门电路可由一个含有 r 个逻辑变元 $x_1, x_2, \cdots, x_r$ 的布尔（Boole）函数：

$$x_{r+1} = f(x_1, x_2, \cdots, x_r)$$

来标志。我们称这一函数为该组合门电路的反馈逻辑函数。

上述反馈移位寄存器的工作是受时钟脉冲控制的。假定在第 j 个时钟移位脉冲（第 j 拍）到来时，移位寄存器的状态是：

$$(a_{j-r}, a_{j-r+1}, \cdots, a_{j-2}, a_{j-1})。$$

于是，再来一个时钟脉冲使 j 增至 $j+1$ 时（第 $j+1$ 拍），最右面的一级在第 j 拍之状态 a_{j-r} 即为输出，并且每个存贮器在第 $j+1$ 拍之状态恰为邻接于它的左面的存贮器在第 j 拍之状态。同时，这 r 个寄存器在第 j 拍之状态输入至开关网络后，相应的输出为：

$$a_j = f(a_{j-r}, a_{j-r+1}, \cdots, a_{j-2}, a_{j-1}),$$

它反馈给最左面一级，作为第1级寄存器在第 $j+1$ 拍的状态。这样一来，从状态转移的角度来看，从第 j 拍过渡到第 $j+1$ 拍

后，就使移位寄存器的状态由 $(a_{j-r}, a_{j-r+1}, \cdots, a_{j-2}, a_{j-1})$ 变换到 $(a_{j-r+1}, a_{j-r+2}, \cdots, a_{j-1}, a_j)$，记作：

$$T_f:(a_{j-r}, a_{j-r+1}, \cdots, a_{j-2}, a_{j-1}) \to (a_{j-r+1}, a_{j-r+2}, \cdots, a_{j-1}, a_j),$$

或

$$T_f(a_{j-r}, a_{j-r+1}, \cdots, a_{j-2}, a_{j-1}) = (a_{j-r+1}, a_{j-r+2}, \cdots, a_{j-1}, a_j)。$$

称 T_f 为这一反馈移位寄存器的状态转移变换。

从上面的分析不难看出，对于反馈移位寄存器来说，起决定性作用的是那个组合门电路的反馈逻辑函数 $f(x_1, x_2, \cdots, x_r)$，它是由 r 个逻辑变元 $x_1, x_2, \cdots, x_r$ 通过“与”、“或”、“非”等逻辑运算联接起来的关系式。

下面，我们通过两个具体例子来说明反馈移位寄存器的功能。

例1.1.1 考虑如图1.1.2所示之三级反馈移位寄存器。这个

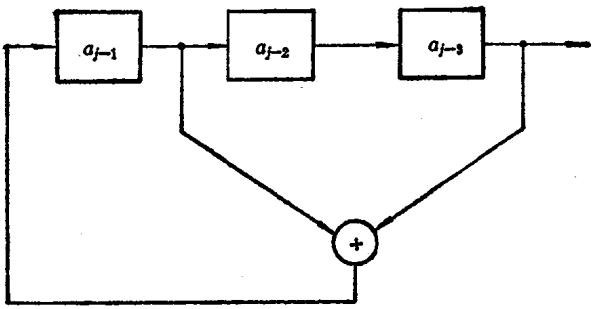


图1.1.2 三级反馈移位寄存器示意图

反馈移位寄存器的工作情况是：当第 j 拍处于状态 $(a_{j-3}, a_{j-2}, a_{j-1})$ 时，第 $j+1$ 拍便处于状态 (a_{j-2}, a_{j-1}, a_j)，其中 $a_j = a_{j-1} + a_{j-3}$。这里的符号“+”是指模2加法。显然，这个反馈移位寄存器的组合门电路就是简单的模2加法器。它所对应的反馈逻辑函数是 $f(x_1, x_2, x_3) = x_1 + x_3$。该反馈移位寄存器的状态转移情况如下表所示。

第 j 拍之状态			第 $j+1$ 拍之状态		
0	0	0	0	0	0
0	0	1	0	1	1
0	1	0	1	0	0
0	1	1	1	1	1
1	0	0	0	0	1
1	0	1	0	1	0
1	1	0	1	0	1
1	1	1	1	1	0

为了从直观上描述这一反馈移位寄存器的状态转移情况，可以使用一些方框及联接这些方框的箭头组成的图形，如图 1.1.3（a）所示。如果把方框内的状态所对应的二进位数字转化为十进制数，则这一反馈移位寄存器的状态转移情况可由图1.1.3（b）来表示。

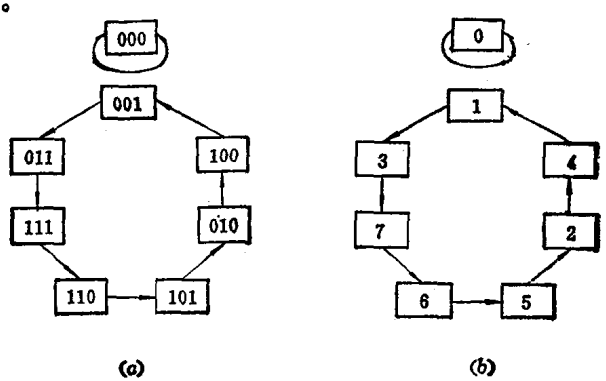


图1.1.3　状态转移图

（a）二进制表示；（b）十进制表示。

在数学上，把表示反馈移位寄存器功能的上述图形叫做状态转移图。

从这个反馈移位寄存器的输出端来看，以状态转移图 1.1.3 的任一状态作为初始状态，沿箭头所指示的路径依次取出第一个

分量，便得到八个相应的二元序列：

0 0 0 0 0 0 0 0 0 ……
0 0 1 1 1 0 1 0 0 ……
0 1 0 0 1 1 1 0 1 ……
0 1 1 1 0 1 0 0 1 ……
1 0 0 1 1 1 0 1 0 ……
1 0 1 0 0 1 1 1 0 ……
1 1 0 1 0 0 1 1 1 ……
1 1 1 0 1 0 0 1 1 ……

这八个序列统称为反馈移位寄存器序列。第一个是全0序列。后七个序列取自状态转移图 1.1.3 所构成的同一个圈上，它们的周期都是 7。我们把这七个序列称作是移位等价的。这个名称的来历是由于将这七个序列之一经过适当的移位可以得到其余任何一个序列。比如，将第二个序列：

0 0 1 1 1 0 1 0 0 1 1 1 0 1 ……

相继左移 5 位以后便得第三个序列：

0 1 0 0 1 1 1 0 1 ……。

有关反馈移位寄存器的这些概念与性质的更详尽与更确切的讨论，留待以后进行。

例1.1.2 考察图1.1.4所示之反馈移位寄存器。它的反馈关

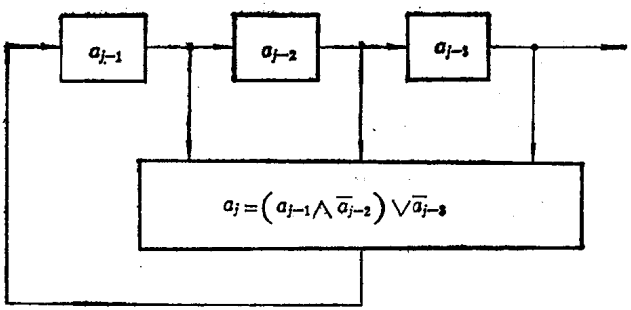


图1.1.4 三级反馈移位寄存器实例

系可列表于下：

a_{j-3}	a_{j-2}	a_{j-1}	$a_j=(a_{j-1}\wedge\overline{a}_{j-2})\vee\overline{a}_{j-3}$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

此处符号“$\wedge$”、“$\vee$”、“$-$”分别代表逻辑运算“与”、“或”、“非”。由此不难写出状态转移表：

第 j 拍之状态			第 $j+1$ 拍之状态		
0	0	0	0	0	1
0	0	1	0	1	1
0	1	0	1	0	1
0	1	1	1	1	1
1	0	0	0	0	0
1	0	1	0	1	1
1	1	0	1	0	0
1	1	1	1	1	0

图1.1.5是这个反馈移位寄存器之状态转移图。读者不难自己写出由这个反馈移位寄存器所产生的序列。

从上面的两个例子可以看出，反馈移位寄存器的功能主要取决于它所对应的开关网络，也就是说，取决于相应的反馈逻辑函数。

在前面的讨论中，我们是以 $(a_{-r}, a_{-r+1}, \cdots, a_{-1})$ 作为初始状态。有时，为了方便，也以 $(a_0, a_1, \cdots, a_{r-1})$ 作为初始状态。

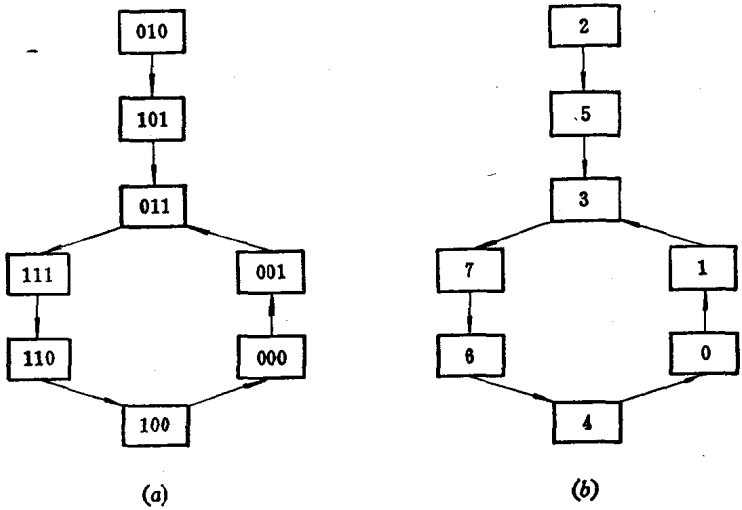


图1.1.5 状态转移图

（a）二进制表示；（b）十进制表示。

§1.2 反馈逻辑函数

从上一节我们已经看到，一个反馈移位寄存器的功能完全由它所对应的反馈逻辑函数来决定。

n 级反馈移位寄存器由一个 n 元反馈逻辑函数 $f(x_1, x_2, \cdots, x_n)$ 来决定，其中变元 $x_1, x_2, \cdots, x_n$ 之间由“与”、“或”、“非”等逻辑运算来联系。我们称这种函数为 n 元布尔函数。这种函数实质上是定义于 F_2^n 上且在 F_2 上取值的函数。

由于 F_2^n 一共有 2^n 个元素，在 F_2^n 的每一元素 $(x_1, x_2, \cdots, x_n)$ 上取 0 或 1 为值均能得到一个相应的布尔函数，故 n 元布尔函数一共有：

$$\underbrace{2 \cdot 2 \cdot \cdots \cdot 2}_{2^n\text{个}} = 2^{2^n}$$

个。显然，以不同的 n 元布尔函数作为反馈函数的 n 级反馈移位

寄存器的状态转移变换亦不同。因此，一共有 2^{2^n} 个功能各不相同的 n 级反馈移位寄存器。

以下，我们来讨论布尔函数的解析表示问题。为了简单起见，我们就三元布尔函数加以研究。我们首先给出：

定理1.2.1 每一个布尔函数 $f(x_1, x_2, x_3)$ 恒可唯一地表示成如下形式：

$$\begin{aligned} f(x_1, x_2, x_3) &= \bigvee_{(c_1,c_2,c_3)=(0,0,0)}^{(1,1,1)} f(c_1, c_2, c_3) x_1^{c_1} x_2^{c_2} x_3^{c_3} \\ &= f(0,0,0) x_1^0 x_2^0 x_3^0 \vee f(0,0,1) x_1^0 x_2^0 x_3^1 \\ &\vee f(0,1,0) x_1^0 x_2^1 x_3^0 \vee f(0,1,1) x_1^0 x_2^1 x_3^1 \\ &\vee f(1,0,0) x_1^1 x_2^0 x_3^0 \vee f(1,0,1) x_1^1 x_2^0 x_3^1 \\ &\vee f(1,1,0) x_1^1 x_2^1 x_3^0 \vee f(1,1,1) x_1^1 x_2^1 x_3^1 \end{aligned} \tag{1.2.1}$$

其中定义：

$$x_i^0 = \bar{x}_i, \quad x_i^1 = x_i \quad (i = 1, 2, 3)$$

并且 $x_1^{c_1} x_2^{c_2} x_3^{c_3}$ 代表 $x_1^{c_1} \wedge x_2^{c_2} \wedge x_3^{c_3}$。

证明 首先注意上面引进的符号具有“正交性”：

$$x_i^c = \begin{cases} 0, & x_i \neq c, \\ 1, & x_i = c。 \end{cases}$$

因此，进一步便有下面的“正交关系”：

$$x_1^{c_1} x_2^{c_2} x_3^{c_3} = \begin{cases} 0, & (x_1, x_2, x_3) \neq (c_1, c_2, c_3), \\ 1, & (x_1, x_2, x_3) = (c_1, c_2, c_3)。 \end{cases}$$

要证明 (1.2.1) 式成立，只须就 (x_1, x_2, x_3) 的全部八种状态，证明其中任一状态之下，等式两端的取值均相等。现假定 (x_1, x_2, x_3) 取值 (y_1, y_2, y_3)，于是 (1.2.1) 式左端取值为 $f(y_1, y_2, y_3)$。又，式右端之 (c_1, c_2, c_3) 经历由 (0, 0, 0) 到 (1, 1, 1) 的全部八种状态，故 (c_1, c_2, c_3) 必取 (y_1, y_2, y_3) 一次且仅一次。因此，根据上述“正交关系”，在和式，

$$\bigvee_{(c_1,\ c_2,\ c_3)=(0,\ 0,\ 0)}^{(1,\ 1,\ 1)} f(c_1,\ c_2,\ c_3)y_1^{c_1}y_2^{c_2}y_3^{c_3}$$

中，仅当 $(c_1,\ c_2,\ c_3)=(y_1,\ y_2,\ y_3)$ 时才有：

$$y_1^{c_1}y_2^{c_2}y_3^{c_3}=1,$$

其余各项均为 0。这表明上述和式仅保留一项，即

$$f(y_1,\ y_2,\ y_3)y_1^{y_1}y_2^{y_2}y_3^{y_3}=f(y_1,\ y_2,\ y_3)。$$

由此可见，当把 $(y_1,\ y_2,\ y_3)$ 分别代入 (1.2.1) 式之两端时，取值均为 $f(y_1,\ y_2,\ y_3)$。这就证明了等式 (1.2.1) 的正确性。

其次证明唯一性。假设 $f(x_1,\ x_2,\ x_3)$ 可表示为：

$$f(x_1,\ x_2,\ x_3)=\bigvee_{(c_1,\ c_2,\ c_3)=(0,\ 0,\ 0)}^{(1,\ 1,\ 1)} a_{c_1,c_2,c_3}x_1^{c_1}x_2^{c_2}x_3^{c_3},$$

其中系数 a_{c_1,c_2,c_3} 仍取 0、1 二值之一。于是，根据“正交关系”立即可得：

$$f(c_1,\ c_2,\ c_3)=a_{c_1,c_2,c_3}。$$

这就证明了表达式 (1.2.1) 之唯一性。证毕。

这一定理表明，每一个布尔函数均可唯一地表示成其基本逻辑变元 x_i（或其非 $\bar{x}_i=x_i^0$）之积的逻辑和。

对于 n 元布尔函数，不难给出 (1.2.1) 式之一般形式：

$$f(x_1,\ x_2,\cdots,\ x_n)=\bigvee_{(c_1,\ c_2\cdots,\ c_n)=(0,\ 0,\ \cdots,\ 0)}^{(1,\ 1,\ \cdots,\ 1)} f(c_1,\ c_2,\cdots,\ c_n)x_1^{c_1}x_2^{c_2}\cdots x_n^{c_n} \tag{1.2.2}$$

例1.2.1 写出下述布尔函数之解析表示式：

$$f(x_1,\ x_2)=\begin{cases}1,\ x_1,\ x_2\text{中有一个且只有一个为}1,\\ 0,\ \text{其它。}\end{cases}$$

根据上述定理，不难看出：

$$f(x_1,\ x_2)=x_1^0x_2^1\vee x_1^1x_2^0=\bar{x}_1x_2\vee x_1\bar{x}_2。$$

这正是电子计算机中设计半加器之逻辑关系。

例1.2.2 写出下述布尔函数之逻辑表达式：

$$f_1(x_1,\ x_2,\ x_3)=\begin{cases}1,\ x_1,x_2,x_3\text{中只有一个为}1\text{或三个全为}1,\\ 0,\ \text{其它。}\end{cases}$$

$$f_2(x_1,\ x_2,\ x_3)=\begin{cases}1,\ x_1,\ x_2,\ x_3\text{中至少有两个为}1,\\ 0,\ \text{其它。}\end{cases}$$

第一个布尔函数的解析表达式为：

$$\begin{aligned}f_1(x_1,\ x_2,\ x_3)&=x_1^1x_2^0x_3^0\vee x_1^0x_2^1x_3^0\vee x_1^0x_2^0x_3^1\vee x_1^1x_2^1x_3^1\\&=x_1\bar{x}_2\bar{x}_3\vee\bar{x}_1x_2\bar{x}_3\vee\bar{x}_1\bar{x}_2x_3\vee x_1x_2x_3。\end{aligned}$$

第二个布尔函数的解析表达式为：

$$\begin{aligned}f_2(x_1,\ x_2,\ x_3)&=x_1^1x_2^1x_3^0\vee x_1^0x_2^1x_3^1\vee x_1^1x_2^0x_3^1\vee x_1^1x_2^1x_3^1\\&=x_1x_2\bar{x}_3\vee\bar{x}_1x_2x_3\vee x_1\bar{x}_2x_3\vee x_1x_2x_3。\end{aligned}$$

这两个解析表达式就是电子计算机中设计全加器之逻辑关系。

我们知道，布尔代数运算比起伽罗瓦（Galois）域F_2上的算术运算来说，有许多不便之处。因此，从理论上探讨反馈函数，应当将其转化为F_2上算术运算。

我们先来讨论布尔代数运算与伽罗瓦域上的算术运算之间的相互转化关系。

首先，下述关系可将布尔代数运算转化为F_2上的算术运算：

$$\bar{x}=1+x;\tag{1.2.3}$$

$$x\wedge y=x\cdot y;\tag{1.2.4}$$

$$\begin{aligned}x\vee y&=\overline{\overline{x\vee y}}=\overline{\bar{x}\cdot\bar{y}}=\overline{(1+x)(1+y)}\\&=(1+x)(1+y)+1\\&=xy+x+y;\end{aligned}\tag{1.2.5}$$

特别，当x、y中至多有一个为1时，

$$x\vee y=x+y。\tag{1.2.6}$$

反过来，F_2上的算术运算也可通过下述关系转化为布尔代数运算：

$$x+y=(x\wedge\bar{y})\vee(\bar{x}\wedge y)=x\bar{y}\vee\bar{x}y;\tag{1.2.7}$$

$$x\cdot y=x\wedge y。\tag{1.2.8}$$

由此不难看出，布尔代数运算“$\wedge$”与F_2上的乘法运算“$\cdot$”是