第4卷 第4期 光学 精密工程 Vol. 4, No. 4
1996年8月 OPTICS AND PRECISION ENGINEERING August, 1996

异或逻辑性质及伽罗华域算术运算的逻辑实现

王世昌
(烟台大学数学与信息科学系,烟台 264005)

摘要 讨论了异或逻辑的性质,并以信息论的熵函数论述了异或逻辑的效率。给出了组合设计的异或化方法,然后讨论了伽罗华域算术运算中的异或逻辑。

关键词:异或逻辑;完备集;效率;伽罗华域

1 引 言

模2运算在数学、逻辑学、计算机科学、密码学及人工神经网络等方面都有重要的应用,而用线路实现模2运算恰是"异或逻辑元件"。本文讨论了异或逻辑的逻辑、正文、效率等方面的特性,给出了组合逻辑设计的"异或"化方法。并讨论了伽罗华域算术运算线路实现中的异或逻辑,从而看到"异或逻辑"的重要性及用该逻辑元件可得到高效而经济的组合逻辑电路的可行性。

2 异或逻辑性质

2.1 K值逻辑

设 E_K 是一个 K 元集合,$K>2$,函数 $f(x_1,\cdots,x_n)$ 定义在 E_K 上而其函数值仍属于 E_K,如果对任意值组 $(a_1,a_2,\cdots,a_n)$ $(a_i\in E_k, i=1,2,\cdots,n)$,$f(a_1,a_2,\cdots,a_n)$ 皆有定义,则称 $f(x_1,x_2,\cdots,x_n)$ 为完全K值逻辑函数,否则称 $f(x_1,x_2,\cdots,x_n)$ 为非完全K值逻辑函数。所有完全K值逻辑函数作成之集合记为 P_K

定义1 设 A 是 P_K 中的一个非空子集,函数 $f(t_1,\cdots,t_m)\in A$;函数 $g_i(x_1,\cdots,x_n)$ $(i=1,\cdots,m)$ 或属于 A 或为自变量 x_i。于是,函数 $f(g_1(x_1,\cdots,x_n),\cdots,g_m(x_1,\cdots,x_n)$ 称由 A 中的函数复合出来的函数。所有由 A 复合出来的函数作成之集合为 A'。

定义2 设 $A\subseteq P_K$ 非空,称 A 为封闭的,如果 $A'=A$。

定义3 设 A 是 P_K 的一个非空子集,包含 A 的所有封闭集之交集称为 A 的封化集,记为 $\mathrm{GEN}(A)$。$\mathrm{GEN}(A)$ 中的函数称为 A 的叠合函数,实际上它们都是由 A 中的函数经过有限次复合后产生出来的函数。

定义4 设 A 是 P_K 的一个非空子集。A 说是完备集,如果 $\mathrm{GEN}(A)=P_K$。

收稿日期:1996年3月20日

2.2 二值逻辑

当 K=2 时，$E_2=\{0,1\}$是一个布尔代数。

定义 5 $A(\subseteq P_2)$说是 P_2 的一个底，如果 A 完备且 A 的任意真子集都不是完备的。

定理 P_2 中，底中的元素不超过 3 个。

证明 设 A 是 P_2 是由 2 元函数做成的底，即 $GEN(A)=P_2$。由 A 的定义有 $f_1\in A$，使 $f_1(0,0)=1$。若 $f_1(1,1)=0$，则 f_1 不保 0，不保 1 且非单调。这样我们取 $f_2(x_1,x_2)\in A$ 且非自对偶，再取 $f_3(x_1,x_2)\in A$ 且非线性。这样 f_1,f_2,f_3 就是一完备集。

若 $f_1(1,1)=1$，因 f_1 不保 0 且非自对偶，则必有 $f_2\in A$ 且 $f_2(1,1)=0$。因 f_2 为二元函数，则 $f_2\neq 0$。从而必有一值组$(a_1,a_2)<(1,1)$且 $f_2(a_1,a_2)>f_2(1,1)$。则 f_2 非单调而不保 1。再取 $f_3\in A$ 且非线性，则 f_1,f_2,f_3 就构成一完备集，定理得证。

由定理不难证得$\{x\oplus y,xy,1\}$是 P_2 的一个底。

可见，异或逻辑在 2 值逻辑中的重要地位。

2.3 正交性

因 $$x\oplus y=\begin{cases}0,\text{当 } x=y \text{ 时}\\ \text{不为 } 0,\text{当 } x\neq y \text{ 时}\end{cases}$$

可见异或逻辑是正交的，其任何输入的变化，都会使输出产生一一对应的变化。他不同于布尔电路需要特殊的输入信号组合才能使输出端较灵敏地变化。

2.4 效率

我们用二进制函数的熵来讨论这一问题。具体如下：

$f_1=x\cdot y$ 的熵，

$$H(f_1)=1/4(\log 4+3\log 4)=0.8113 \tag{1}$$

$f_2=x+y$ 的熵，

$$H(f_2)=0.8113 \tag{2}$$

$f_3=\bar{x}$ 的熵

$$H(f_3)=0.5 \tag{3}$$

$f_4=x\oplus y$ 的熵

$$H(f_4)=1/2[\log 2+\log 2]=1 \tag{4}$$

而
$$x\oplus y=\overline{xy}\cdot(x+y) \tag{5}$$

由(1)、(2)、(3)、(4)得用(5)式的右端的三种逻辑运算去实现 $x\oplus y$，其效率为 0.34，可见“异或逻辑”的效率及经济效益。

3 组合逻辑的异或化

以一实例来讨论这一问题

例：

对 $$f(A,B,C,D,E,F)=\sum\nolimits_m(2,20,21,23,34,52,53,55,58,60,61,63)=1 \tag{6}$$
进行逻辑设计。

对(6)式用卡诺图简化后得：

$$f=ABDF+ABD\bar{E}+B\bar{C}DF+B\bar{C}D\bar{E}+\bar{B}\bar{C}D\bar{E}\bar{F}+AB\bar{C}D\bar{E}\bar{F} \tag{7}$$

由(7)式得

$$\bar{f}=\bar{A}C+\bar{B}C+D\bar{B}+DE\bar{F}+B\bar{C}\bar{D}+\bar{D}\bar{E}+\bar{D}F=0 \tag{8}$$

由(8)式得：

$$\bar{f}=AC\cdot\overline{\bar{B}C}+\overline{\bar{A}C}\cdot BC+BDE\cdot\overline{BDEF}+\overline{BD\bar{E}}\cdot BDEF+B\cdot\overline{(C+D)}+\bar{B}\cdot(C+D)+\bar{D}\cdot\overline{DEF}+D\cdot\overline{\bar{D}EF}=0 \tag{9}$$

显然对(6)式 $f=1$ 的逻辑设计可转化为(9)式 $\bar{f}=0$ 的逻辑设计。

由(9)式得如下异或算式

$$AC\oplus BC=0 \tag{10}$$

$$BDE\oplus BDEF=0 \tag{11}$$

$$B\oplus(C+D)=0 \tag{12}$$

$$D\oplus(\overline{DEF})=0 \tag{13}$$

由(13)得：

$$D=\bar{E}+F \tag{14}$$

由(10)及(11)得：

$$A=A+C \tag{15}$$

则由(15)、(12)、(14)得：

$$A=A+C \tag{16}$$

$$B=C+D \tag{17}$$

$$D=\bar{E}+F \tag{18}$$

显然实现了(16)－(18)式即实现了(6)。从而用“异或逻辑”实现了线路简化。

4　伽罗华域算术运算中的异或逻辑

伽罗华域的算术运算在编码及密码学等方面都要经常用到，下面给出 GF(2^4)中的几种算术运算。

1)相加

相加可用图 1 逻辑电路实现，将相加的两个元素分别存入寄存器 A，寄存器 B，当给出加法脉冲后，相加之和就进入寄存器 A。

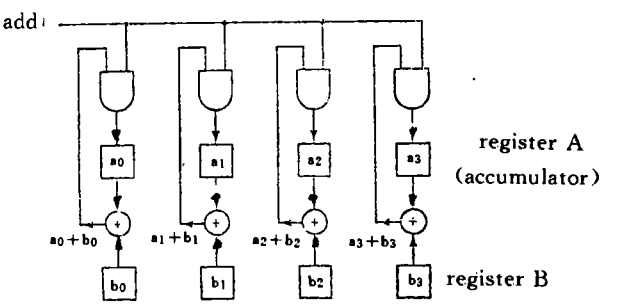

图 1　伽罗华域相加器

Fig. 1　The Galois field adder

2)相乘

(1)GF(2^4)中的本原元素 a 乘以域元素 b，b 可表成如下 a 的多项式：

$$b=b_0+b_1a+b_2a^2+b_3a^3 \tag{19}$$

因为 $a^4=1+a$，则得

$$ab=b_3+(b_0+b_3)a+b_1a^2+b_2a^3$$

(20)式可用图 2 的逻辑电路实现。

(2)元素 a^3 乘 GF(2^4)中任意元素 b。

将 a^3 乘(19)式两端有：

$$a^3b=b_0a^3+b_1a^4+b_2a^5+b_3a^6$$
$$=b_0a^3+b_1(1+a)+b_2(a+a^3)+b_3(a^2+a^3)$$
$$=b_1+(b_1+b_2)a+(b_2+b_3)a^2+(b_0+b_3)a_3 \quad (21)$$

(21)式可用图3逻辑电路实现。

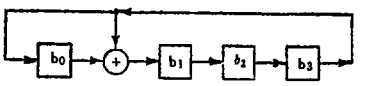

图2 a与GF(2⁴)中任一元素相乘电路

Fig. 2 The logic circuit of the a multiplied by any element in GF(2⁴)

(3)GF(2⁴)中两个元素相乘

设两个元素 b,d 分别为:

$$b=b_0+b_1a+b_2a^2+b_3a^3 \quad (22)$$

$$d=c_0+c_1a+c_2a^2+c_3a^3 \quad (23)$$

由(22)、(23)式得

$$bd=(((c_3b)a+c_2b)a+c_1b)a+c_0b \quad (24)$$

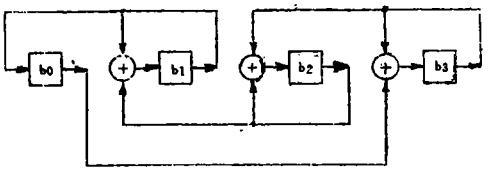

图3 a^3 乘 GF(2⁴)中任意元素的逻辑电路图

Fig. 3 The logic circuit of the a^3 multiplied by any element in GF(2⁴)

我们知道用图2电路可实现乘 a,用图4逻辑电路可实现(24)式。在图4的电路工作时,开始反馈移位寄存器 A 为全"0"(即初始状态为0),将 b 存入寄存器 B,d 存入 C 寄存器。然后寄存器 A、C 均右移四次。

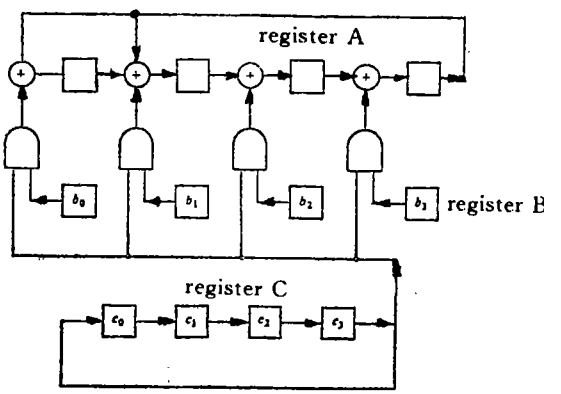

图4 GF(2⁴)两个元素相乘电路

Fig. 4 The multiplying circuit of the two elements in GF(2⁴)

第一次移位完毕后,寄存器 A 中含有 c_3b

第二次移位完毕后,寄存器 A 中含有 $(c_3b)a+c_2b$

第三次移位完毕后,寄存器 A 中含有 $((c_3b)a+c_2b)a+c_1b$

第四次移位完毕后,寄存器 A 中含有 bd(即(24)式)。

3)多项式的计算

$$令\ y(a)=b_0+b_1a+b_2a^2+\cdots+b_{14}a^{14} \quad (25)$$

由(25)式得:

$$y(a)=(\cdots((b_{14})a+b_{13})a+b_{12})a+\cdots)a+b_0 \quad (26)$$

可见在实现 a 乘域元素的图2中加一个输入,就可实现(25)式,其逻辑电路为图5。

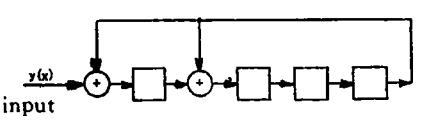

图5 计算y(a)的逻辑电路

Fig. 5 The logic circuit of the computing y(a)

此电路计算中,寄存器初始状态为全"0"。系数矢量 $(b_0,b_1,\cdots,b_{14})$ 一次移一位地移入该电路。第一次移位完毕后,寄存器为 $(b_{14},0,0,0)$,第二次移位完毕后,寄存器为 $(b_{14}a+b_{13})$,当最后一个数据 b_0 移入后,寄存器为 $y(a)$(即

(26)式)。从上讨论可见"异或逻辑"是伽罗华域算术运算线路实现的核心元件。

5 结 束 语

从本文的讨论可知，"异或逻辑"具有一些很好的特性，其应用十分广泛。文中只以简化组合逻辑设计及伽罗华域算术运算中的应用进行了讨论，从中可看出它在实际应用中的一些方法与技术。

参 考 文 献

〔1〕罗铸楷等，多值逻辑的理论及应用．北京：科学出版社，1992

〔2〕Shu Lin，Daniel J. Costello，JR.，Error Control Coding，Fundamentals and Applications. Prentice-Hill，1983

Properties of Exclusive OR Logic and Logic Realization of the Galois Feild Arithmetic Operation

Wang Shichang

(*Department of Mathematics and Information Science，Yantai University，Yantai* 264005)

Abstract

In this paper，the properties of Exclusive OR logic is discussed. The efficiency of the Exclusive OR logic is expounded by the entropy function of information theory. The Exclusive OR method of combinational logic design is given. Then the Exclusive OR logic of Galois field arithmetic operation is discussed.

Key words：Exclusive OR logic，Complete set，Efficiency，Galois field

王世昌　男，生于1940年11月。1964年毕业于吉林大学计算数学专业控制论专门化，主要研究方向是：自动机理论及其应用、数字逻辑、信息保密技术。取得的主要鉴定成果有：薄膜测量光谱仪，30kW 氙灯电源。发表论文20余篇，主要有：基于自动机的分析与综合因素神经网络的自动实现、流密码中 Bent 函数与有限状态机组合器、一个基于布尔方程的简化组合逻辑设计的分解方法、字符串匹配的自动机方法、S 盒随机化与随机化 DES 链式结构、$4t(t\geqslant 2)$阶规范化 HADAMARD 矩阵算法等。