

广义西尔运算

王万树

(吉林工业大学, 长春 130025)

摘要 本文讨论了 $GF(2^m)$ 域无进位运算的逻辑特征及其逻辑网络,在此基础上定义了广义西尔运算。把这种运算应用于 $GF(2^m)$ 域的快速逻辑沃尔什变换,有利于西尔运算在序列理论中的进一步应用。

关键词 不进位运算;西尔运算;有限域

一、前言

H.F. 哈尔姆斯发展了 N.H. 西尔不进位运算的思想,用二进制数字对的真值表定义了不进位的加减运算,并称之为西尔运算^[1]。据此,文献[2]研究了西尔运算的逻辑特征,还给出了实现运算的逻辑网络。文献[3]则在 $GF(2)$ 域研究了西尔运算的矩阵表示,不用真值表可以直接简便地实现运算。本文是在 $GF(2^m)$ 域较为一般地研究了多位二进制数的不进位运算,揭示出不进位运算实质是有限域上的运算。根据有限域元素的线性运算定义了广义西尔运算,并指出文献[1]的西尔运算只不过是 $m=2$ 时广义西尔运算的特殊情况。最后举例说明 $GF(2^m)$ 域的逻辑变换。

二、 $GF(2^m)$ 域的元素

集合 $F_2 = (0, 1)$ 构成二元域 $GF(2)$,它是 $GF(2^m)$ 的子域。对 $m=4$,由本原多项式 $f(x) = 1 + x + x^4$ 生成的 $GF(2^4)$ 域的元素有表1所列的前三种表示方法^[4]。如果把 m 重表示看成二进制数,那么使用二进制数到十进制数转换的公式,可以把二进制数 $a = a_{m-1}a_{m-2}\cdots a_1a_0$, $a_i \in F_2$ 转换成 A_a 表示,即

$$A_a = a_{m-1}2^{m-1} + a_{m-2}2^{m-2} + \cdots + a_12^1 + a_02^0 \quad (1)$$

当 m 一定,二进制数共有 2^m 个可能,因而 A_a 也可以有 2^m 个不同的值对应 $GF(2^m)$ 域的 2^m 个元素。所以把 A_a 表示看成 $GF(2^m)$ 域元素的第四种表示方法。在 $m=4$ 的情况下,如果按大小排序, $GF(2^4)$ 的元素可集成 $F_{2^4} = (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15)$ 。

另一方面,为了今后运算的需要,还把 m 重用 $GF(2)$ 域的有限维列向量表示,即

1991.10.29 收到, 1992.04.09 定稿。

王万树 男, 1957 年生, 教授, 现从事电子学的教学和研究工作。

表 1

幂表示	多项式表示	4重表示 ($a_0a_1a_2a_3$)	A_s 表示
0	0	(0000)	$A_0 = 0$
1	1	(1000)	$A_1 = 1$
α^1	α	(0100)	$A_2 = 2$
α^2	α^2	(0010)	$A_4 = 4$
α^3	α^3	(0001)	$A_8 = 8$
α^4	$1 + \alpha$	(1100)	$A_3 = 3$
α^5	$\alpha + \alpha^2$	(0110)	$A_6 = 6$
α^6	$\alpha^2 + \alpha^3$	(0011)	$A_{12} = 12$
α^7	$1 + \alpha + \alpha^3$	(1101)	$A_{11} = 11$
α^8	$1 + \alpha^2$	(1010)	$A_5 = 5$
α^9	$\alpha + \alpha^3$	(0101)	$A_{10} = 10$
α^{10}	$1 + \alpha + \alpha^2$	(1110)	$A_7 = 7$
α^{11}	$\alpha + \alpha^2 + \alpha^3$	(0111)	$A_{14} = 14$
α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	(1111)	$A_{15} = 15$
α^{13}	$1 + \alpha^2 + \alpha^3$	(1011)	$A_{13} = 13$
α^{14}	$1 + \alpha^3$	(1001)	$A_9 = 9$

$\begin{bmatrix} a_{m-1} \\ a_{m-2} \\ \vdots \\ a_1 \\ a_0 \end{bmatrix}$. 当 $m = 4$, A_8, A_4, A_2, A_1 对应的列向量分别为 $\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$, 它

们正好是 4 维向量的一组基向量。把任意 A_s 所对应的列向量用 $\bar{A}_s$ 表示, 它与基向量的关系可表示为

$$\bar{A}_s = a_{m-1} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} + a_{m-2} \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{bmatrix} + \cdots + a_1 \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{bmatrix} + a_0 \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} \quad (2)$$

其中列向量是 m 维, $a_i \in F_2$, 加法运算是对应元素的模 2 相加, 自然是不进位运算。

根据表 1 不难验证 $GF(2^4)$ 域元素 A_s 满足表 2 的加法规则和表 3 的乘法规则。验证时注意应用 $GF(2^m) = GF(2^4)$ 域中 $\alpha^{2^m-1} = \alpha^{2^4-1} = \alpha^{15} = 1$, $\alpha^i + \alpha^i = 0$, $0 \leq i \leq 2^m - 1$ 。例如

$$3 + 7 \longleftrightarrow (1 + \alpha) + (1 + \alpha + \alpha^2) = \alpha^2 \longleftrightarrow 4 \quad (3)$$

$$12 \times 13 \longleftrightarrow \alpha^6 \cdot \alpha^{13} = \alpha^{19} = \alpha^{15} \cdot \alpha^4 = \alpha^4 \longleftrightarrow 3 \quad (4)$$

如果考虑到列向量的加法是对应元素的模 2 相加, 那么(3)式也可以如下来完成, 即

$$3 + 7 \longleftrightarrow \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \longleftrightarrow 4$$

表 2

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

表 3

×	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	2	4	6	8	10	12	14	3	1	7	5	11	9	15	13
3	0	3	6	5	12	15	10	9	11	8	13	14	7	4	1	2
4	0	4	8	12	3	7	11	15	6	2	14	10	5	1	13	9
5	0	5	10	15	7	2	13	8	14	11	4	1	9	12	3	6
6	0	6	12	10	11	13	7	1	5	3	9	15	14	8	2	4
7	0	7	14	9	15	8	1	6	13	10	3	4	2	5	12	11
8	0	8	3	11	6	14	5	13	12	4	15	7	10	2	9	1
9	0	9	1	8	2	11	3	10	4	13	5	12	6	15	7	14
10	0	10	7	13	14	4	9	3	15	5	8	2	1	11	6	12
11	0	11	5	14	10	1	15	4	7	12	2	9	13	6	8	3
12	0	12	11	7	5	9	14	2	10	6	1	13	15	3	4	8
13	0	13	9	4	1	12	8	5	2	15	11	6	3	14	10	7
14	0	14	15	1	13	3	2	12	9	7	6	8	4	10	11	5
15	0	15	13	2	9	6	4	11	1	14	12	3	8	7	5	10

下节讨论用 $\bar{A}_a$ 表示的乘法运算.

三、 A_a 运算的逻辑特征

给出 $GF(2^m)$ 域元素 A_a 的 m 重表示 $(a_0 a_1 \cdots a_{m-2} a_{m-1})$, 不难写出相应的(降幂)多项式表示

$$a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \dots + a_1\alpha^1 + a_0\alpha^0 = [\alpha^{m-1}\alpha^{m-2}\dots\alpha^1\alpha^0] \begin{bmatrix} a_{m-1} \\ a_{m-2} \\ \vdots \\ a_1 \\ a_0 \end{bmatrix}$$

如果注意到幂表示中的 $\alpha^{m-1}, \alpha^{m-2}, \dots, \alpha^1, \alpha^0$ 同 A_a 表示中的 $A_{2^{m-1}}, 2^{m-2}, \dots, 2^1, 2^0$ 相对应, 比如表 1 中 $\alpha^3, \alpha^2, \alpha^1, \alpha^0$ 分别对应 $2^3 = 8, 2^2 = 4, 2^1 = 2, 2^0 = 1$, 用 2^i 代替上面的 α^i , 不会改变 A_a 的值. 于是有

$$A_a = [2^{m-1} 2^{m-2} \dots 2^1 2^0] \begin{bmatrix} a_{m-1} \\ a_{m-2} \\ \vdots \\ a_1 \\ a_0 \end{bmatrix} \quad (5)$$

这实际上是(1)式的矩阵和向量表示. 将(5)式等号右边左乘的行矩阵元素

$$2^{i-1} = \underbrace{00\dots 10\dots\dots 00}_{\substack{\text{共 } i \text{ 位} \\ \text{共 } m \text{ 位}}}$$

用列向量表示, 把 A_a 记为 $\bar{A}_a$, 则有

$$\bar{A}_a = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix} \begin{bmatrix} a_{m-1} \\ a_{m-2} \\ \vdots \\ a_1 \\ a_0 \end{bmatrix} = \begin{bmatrix} a_{m-1} \\ a_{m-2} \\ \vdots \\ a_1 \\ a_0 \end{bmatrix} \quad (6)$$

(6)式右边的方阵是 $m \times m$ 的单位矩阵. 显然(5)式中 A_a 是在 F_2^m 中取值, (6)式则是将 $\bar{A}_a$ 用 F_2 中列向量表示. A_a 和 $\bar{A}_a$ 彼此对应, 但表示方法不同. 因此可以认为(5)式与(6)式在数值上等效对应.

为了明确, 令 $m = 4$. 给定两个 4 重列向量 $\begin{bmatrix} a_3 \\ a_2 \\ a_1 \\ a_0 \end{bmatrix}$ 和 $\begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix}$, $a_i, b_i \in F_2$, 它们分别对

应 F_2^4 中两个元素 A_a 和 A_b , 根据(5)式不难写出

$$A_a A_b = [2^3 2^2 2^1 2^0] \begin{bmatrix} a_3 \\ a_2 \\ a_1 \\ a_0 \end{bmatrix} [2^3 2^2 2^1 2^0] \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} \quad (7)$$

按照表 3 的乘法规则, 将(7)式前 3 个矩阵乘出来后

$$A_a A_b = [8A_a \ 4A_a \ 2A_a \ A_a] \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} \quad (8)$$

行矩阵中 $A_a = a_3 2^3 + a_2 2^2 + a_1 2^1 + a_0 2^0$, 它也是(8)式等号左边的 A_a . 给出

$$a = a_3 a_2 a_1 a_0$$

的 16 种可能取值, 按照表 2, 表 3 的规则算出 $A_a, 2A_a, 4A_a, 8A_a$, 再把它们换成相应

的列向量代入(8)式, 记 $\begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix}$ 为 $\bar{A}_b$, 则有下列 16 种 A_a 表示的乘积和矩阵向量积的对应

关系

$$A_0 \cdot A_b \Leftrightarrow \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_0 \cdot \bar{A}_b; \quad A_1 \cdot A_b \Leftrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_1 \cdot \bar{A}_b$$

$$A_2 \cdot A_b \Leftrightarrow \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_2 \cdot \bar{A}_b; \quad A_3 \cdot A_b \Leftrightarrow \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_3 \cdot \bar{A}_b$$

$$A_4 \cdot A_b \Leftrightarrow \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_4 \cdot \bar{A}_b; \quad A_5 \cdot A_b \Leftrightarrow \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_5 \cdot \bar{A}_b$$

$$A_6 \cdot A_b \Leftrightarrow \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_6 \cdot \bar{A}_b; \quad A_7 \cdot A_b \Leftrightarrow \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_7 \cdot \bar{A}_b$$

$$A_8 \cdot A_b \Leftrightarrow \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_8 \cdot \bar{A}_b; \quad A_9 \cdot A_b \Leftrightarrow \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_9 \cdot \bar{A}_b$$

$$A_{10} \cdot A_b \Leftrightarrow \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_{10} \cdot \bar{A}_b; \quad A_{11} \cdot A_b \Leftrightarrow \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_{11} \cdot \bar{A}_b$$

$$\begin{aligned}
 A_{12} \cdot A_b &\Leftrightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_{12} \cdot \bar{A}_b; & A_{13} \cdot A_b &\Leftrightarrow \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_{13} \cdot \bar{A}_b, \\
 A_{14} \cdot A_b &\Leftrightarrow \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_{14} \cdot \bar{A}_b; & A_{15} \cdot A_b &\Leftrightarrow \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = M_{15} \cdot \bar{A}_b,
 \end{aligned}$$

式中 M_a 是 m 阶方阵, 最后一列是 A_a 对应的列向量, 从右到左各列依次按表 3 乘法规则加倍。由此可归纳出一般的对应关系

$$A_a \cdot A_b \Leftrightarrow M_a \cdot \bar{A}_b \quad (9)$$

即 $GF(2^m)$ 域中的乘积 $A_a \cdot A_b$ 可以用 $GF(2)$ 域中的 m 阶方阵左乘列向量 $\bar{A}_b$ 来实现。反之亦然。例如 $GF(2^4)$ 域的 $9 \times 12 = 6$, 在 $GF(2)$ 域则为

$$M_9 \cdot \bar{A}_{12} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \Leftrightarrow 6$$

图 1

特别是这种矩阵运算还可以通过图 1 所示的逻辑网络来实现。由图可见, $M_9 \cdot \bar{A}_{12}$ 的计算, 除了一位需要模 2 相加之外, 其余各位都是错位直接输出。一般来说, 这种逻辑网络只有位之间模 2 相加和错位输出, 非常简便。

由(9)式可见, 在有限域 $GF(2^m)$ 中 A_a 和 M_a 个数相同, 因此 A_a 和 M_a 同构, A_a 所满足的代数关系, M_a 也应满足。比如对 $m=4$ 来说, A_4 满足本原多项式 $f(x) = 1 + x + x^4$, 即

$$1 + A_4 + A_4^4 = 1 + 4 + 4^4 = 1 + 4 + 5 = 0$$

是按表 2, 表 3 加、乘规则运算的。 M_4 亦满足本原多项式, 即 $I + M_4 + M_4^4 = 0$, 具体写成

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}^4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

下面不加证明地列出几个 A_a 与 M_a 的对应关系, 对于 $m=4$, 可以用表 2 和表 3 加以验证。

$$(1) A_{a+b} = A_a + A_b;$$

$$(1') M_{a+b} = M_a + M_b$$

$$\begin{aligned}
 (2) A_{a \cdot b} &= A_a \cdot A_b = A_b \cdot A_a \\
 &= A_{b \cdot a};
 \end{aligned}$$

$$\begin{aligned}
 (2') M_{a \cdot b} &= M_a \cdot M_b = M_b \cdot M_a \\
 &= M_{b \cdot a}
 \end{aligned}$$

$$(3) A_{2^n} + A_{2^{n+1}} = 1;$$

$$(3') M_{2^n} + M_{2^{n+1}} = I$$

I 是 m 阶单位矩阵, $n = 0, 1, \dots, 2^{m-1} - 1$.

根据对应关系(1')和(2')我们有

$$\begin{aligned} M_a &= M_{a_{m-1} \cdot 2^{m-1} + a_{m-2} \cdot 2^{m-2} + \dots + a_1 2^1 + a_0 2^0} \\ &= a_{m-1} \cdot M_2^{m-1} + a_{m-2} M_2^{m-2} + \dots + a_1 M_2^1 + a_0 M_2^0 \end{aligned} \quad (10)$$

如果把 $M_2^i (i = 0, 1, 2, \dots, m-1)$, 比如 $M_2^3, M_2^2, M_2^1, M_2^0$ 看成是一些基矩阵, 则任意 M_a 均可用基矩阵的线性组合表示. 以 $m = 4$ 时的 $M_9 = M_{1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0}$ 为例, 因有 $a_3 = 1, a_2 = 0, a_1 = 0, a_0 = 1$, 所以

$$\begin{aligned} M_9 &= a_3 M_2^3 + a_2 M_2^2 + a_1 M_2^1 + a_0 M_2^0 = a_3 M_8 + a_2 M_4 + a_1 M_2 + a_0 M_1 \\ &= 1 \cdot \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} + 0 \cdot \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} + 0 \cdot \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} + 1 \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \end{aligned}$$

不仅如此, 图 1 所示 M_9 的网络也可以由基矩阵对应的网络组成, 如图 2. 图中 a_i 为

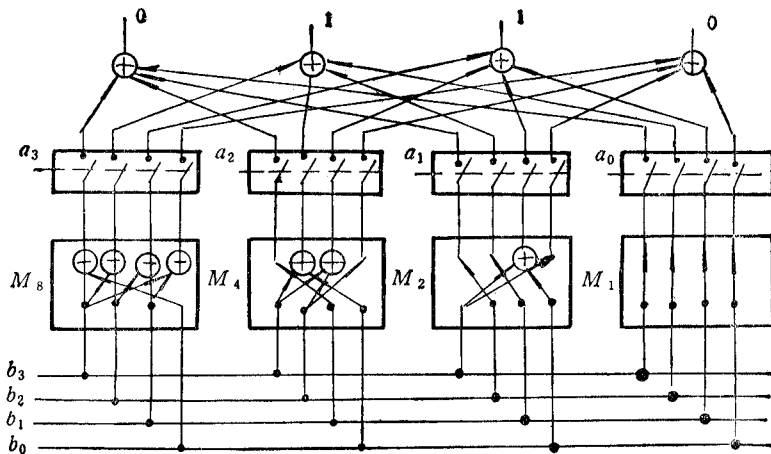


图 2

控制开关. 当 $a_i = 1$ 时, 相应的 4 个开关接通; 当 $a_i = 0$ 时, 相应的 4 个开关断开. b_3, b_2, b_1, b_0 为输入列向量, 在相应的 a_3, a_2, a_1, a_0 控制下, 输出则为 $M_9 \bar{A}_b \Leftrightarrow A_a \cdot A_b$, 图 2 比图 1 要复杂, 但却更加规范. 因为 2^m 个 M_a 所对应的网络只需用 m 个基网络的组合代替. 当 $m = 2$ 时, 网络数不多, 可以使用 M_a 所对应的网络, 不必采用基网络组合.

四、广义西尔运算

设 a, b 是需要不进位加减的两个数, 它们对应的二进制数分别有 i 位和 j 位, 即

$$a = a_{i-1}a_{i-2}\cdots a_1a_0; b = b_{j-1}b_{j-2}\cdots b_1b_0$$

$a_i, b_i \in F_2$, 且 $i \neq j$. 在最高位前添零, 把它们都变成 k 位, 而且要求 $k = ml$, m 为 $GF(2^m)$ 中的 m , 而 $l = 1, 2, \dots$, 是正整数. 然后将 k 位二进制数分成 l 段, 每段 m 位, 写成如下形式

$$\bar{a} = \begin{bmatrix} a_{k-1} & a_{k-m-1} \cdots a_{m-1} \\ a_{k-2} & a_{k-m-2} \cdots a_{m-2} \\ \vdots & \vdots \\ a_{k-m} & a_{k-2m} \cdots a_0 \end{bmatrix} \quad (11)$$

$$\bar{b} = \begin{bmatrix} b_{k-1} & b_{k-m-1} \cdots b_{m-1} \\ b_{k-2} & b_{k-m-2} \cdots b_{m-2} \\ \vdots & \vdots \\ b_{k-m} & b_{k-2m} \cdots b_0 \end{bmatrix} \quad (12)$$

当然, 如果已知(11)式和(12)式表示的 $\bar{a}$ 和 $\bar{b}$, 按照前面的说明不难恢复 a 和 b . 称 $\bar{a}$ 和 $\bar{b}$ 分别为 a 和 b 的向量. 若 I 是 m 阶单位矩阵, M_a 为 m 阶方阵, 仿照文献[3]可以把

$$I\bar{a} + I\bar{b} = \bar{c} \quad (13)$$

$$M_{2n+1}\bar{a} + M_{2n}\bar{b} = \bar{d}, \quad n = 1, 2, \dots, 2^{m-1} - 1 \quad (14)$$

分别定为 $a \oplus b$ 和 $a \odot b$ 的矩阵形式. 根据前述 A_a 与 M_a 的对应关系(3') $M_{2n+1} + M_{2n} = I$, 为确定起见, 可取 $n = 2$, 于是, $M_{2n+1} = M_5$, $M_{2n} = M_4$.

再把(13)式和(14)式合并成分块矩阵形式, 有

$$\begin{bmatrix} I & I \\ M_5 & M_4 \end{bmatrix} \begin{bmatrix} \bar{a} \\ \bar{b} \end{bmatrix} = \begin{bmatrix} \bar{c} \\ \bar{d} \end{bmatrix} \quad (15)$$

如果注意到

$$\begin{bmatrix} M_4 & I \\ M_5 & I \end{bmatrix} \begin{bmatrix} I & I \\ M_5 & M_4 \end{bmatrix} = \begin{bmatrix} M_4 + M_5 & M_4 + M_4 \\ M_5 + M_5 & M_5 + M_4 \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}$$

就得到

$$\begin{bmatrix} M_4 & I \\ M_5 & I \end{bmatrix} = \begin{bmatrix} I & I \\ M_5 & M_4 \end{bmatrix}^{-1} \quad (16)$$

利用(16)式的逆矩阵关系, 解(15)式得到

$$\begin{bmatrix} M_4 & I \\ M_5 & I \end{bmatrix} \begin{bmatrix} \bar{c} \\ \bar{d} \end{bmatrix} = \begin{bmatrix} \bar{a} \\ \bar{b} \end{bmatrix} \quad (17)$$

或者

$$M_4\bar{c} + I\bar{d} = \bar{a} \quad (18)$$

$$M_5\bar{c} + I\bar{d} = \bar{b} \quad (19)$$

(18)式和(19)式可以分别定义 $c \oplus_i d$ 和 $c \odot_i d$ 的矩阵形式.

由于(13)式、(14)式和(18)式、(19)式的矩阵 M_4, M_5 不一定是二阶的, 向量 $\bar{a}, \bar{b}$ 的各列向量不一定是数字对(因为 m 可以为奇数), 因此它们所定义的西尔运算比文献[1, 3]更为广义. 除此之外, 由于 n 有多种取值, 所以 M_{2n} 和 M_{2n+1} 亦有多种, (14)式, (18)式和(19)式的定义不是唯一的. 但只要 n 一定, (16)式的矩阵求逆就一定, 正反西尔运算就是唯一的.

将(11)式和(12)式向量 $\bar{a}, \bar{b}$ 中的每个列向量分别用 $\text{GF}(2^m)$ 中相应的元素 A_i 表示, 还可记为

$$a = (A_{a_1} A_{a_2} \cdots A_{a_l}) \quad (20)$$

$$b = (A_{b_1} A_{b_2} \cdots A_{b_l}) \quad (21)$$

$A_{a_i}, A_{b_i} \in F_{2^m}, A_{a_i}, A_{b_i}$ 分别是 $\bar{a}$ 和 $\bar{b}$ 中第 i 列向量所对应的 A_i . 使用 A_i 和 M_i 的同构关系, (13)、(14)式和(18)、(19)式还可记为

$$a + b = c \quad (22)$$

$$A_3 a + A_4 b = d \quad (23)$$

$$A_4 c + d = a \quad (24)$$

$$A_5 c + d = b \quad (25)$$

这就是说, 把任意数 a 和 b 按照(20)和(21)式定义后, 可以在 $\text{GF}(2^m)$ 域进行线性运算——不进位运算. (22)和(23)式是正向运算, (24)和(25)式是逆向运算, 我们分别称之为广义的西尔正向运算和广义的西尔逆向运算.

例如

$$a = (54)_+ = (00110110)_- = (3, 6)_{\text{GF}(2^4)}$$

$$b = (33)_+ = (00100001)_- = (2, 1)_{\text{GF}(2^4)}$$

正向运算为

$$\begin{aligned} c = a + b &= (3, 6)_{\text{GF}(2^4)} + (2, 1)_{\text{GF}(2^4)} = (1, 7)_{\text{GF}(2^4)} \\ &= (00010111)_- = (23)_+ \end{aligned}$$

$$\begin{aligned} d = A_3 a + A_4 b &= 5 \cdot (3, 6)_{\text{GF}(2^4)} + 4 \cdot (2, 1)_{\text{GF}(2^4)} \\ &= (15, 13)_{\text{GF}(2^4)} + (8, 4)_{\text{GF}(2^4)} \\ &= (7, 9)_{\text{GF}(2^4)} = (01111100)_- = (124)_+ \end{aligned}$$

逆向运算恢复 a, b

$$\begin{aligned} a &= A_4 c + d = 4 \cdot (1, 7)_{\text{GF}(2^4)} + (7, 9)_{\text{GF}(2^4)} \\ &= (3, 6)_{\text{GF}(2^4)} = (00110110)_- = (54)_+ \\ b &= A_5 c + d = 5 \cdot (1, 7)_{\text{GF}(2^4)} + (7, 9)_{\text{GF}(2^4)} \\ &= (2, 1)_{\text{GF}(2^4)} = (00100001)_- = (33)_+ \end{aligned}$$

广义西尔运算也适用快速逻辑沃尔什变换, 给定数据序列 $A, B, C, \dots, G, H$, 它们的每一个都可能是十进制数. 把每一个都按(20)式的形式变换到 $\text{GF}(2^m)$ 域, 分别记为 $A(0), A(1), \dots, A(6), A(7)$, 按格雷码定序的不进位沃尔什-傅里叶正变换表^[1], 不难写出三次迭代变换的矩阵关系如下

$$\begin{bmatrix} a(0) \\ a(1) \\ a(3) \\ a(2) \\ a(7) \\ a(6) \\ a(4) \\ a(5) \end{bmatrix} = \begin{bmatrix} 1 & 1 & & & & & & \\ & 5 & 4 & & & & & \\ & & & 1 & 1 & & & \\ & & & 5 & 4 & & & \\ & & & & & 1 & 1 & \\ & & & & & 5 & 4 & \\ & & & & & & 1 & 1 \\ & & & & & & & 5 & 4 \end{bmatrix} \begin{bmatrix} 1 & 1 & & & & & & \\ & & 1 & 1 & & & & \\ & & 5 & 4 & & & & \\ & & & & 1 & 1 & & \\ & & & & 5 & 4 & & \\ & & & & & & 1 & 1 \\ & & & & & & 5 & 4 \\ & & & & & & & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & & & & & & \\ & & 1 & 1 & & & & \\ & & & & 1 & 1 & & \\ & & & & & & 1 & 1 \\ & & & & & & 5 & 4 \\ & & & & & & & 5 & 4 \\ & & & & & & & & 1 & 1 \\ & & & & & & & & 5 & 4 \end{bmatrix} \begin{bmatrix} A(0) \\ A(1) \\ A(2) \\ A(3) \\ A(4) \\ A(5) \\ A(6) \\ A(7) \end{bmatrix} \quad (26)$$

逆变换矩阵的迭代关系则为

$$\begin{bmatrix} A(0) \\ A(1) \\ A(2) \\ A(3) \\ A(4) \\ A(5) \\ A(6) \\ A(7) \end{bmatrix} = \begin{bmatrix} 4 & 1 & & & & & & \\ & 5 & 1 & & & & & \\ & & 4 & 1 & & & & \\ & & & 5 & 1 & & & \\ & & & & 4 & 1 & & \\ & & & & & 5 & 1 & \\ & & & & & & 4 & 1 \\ & & & & & & & 5 & 1 \end{bmatrix} \begin{bmatrix} 4 & 1 & & & & & & \\ & 4 & 1 & & & & & \\ & & 5 & 1 & & & & \\ & & & 5 & 1 & & & \\ & & & & 4 & 1 & & \\ & & & & & 4 & 1 & \\ & & & & & & 5 & 1 \\ & & & & & & & 5 & 1 \end{bmatrix} \begin{bmatrix} 4 & 1 & & & & & & \\ & 4 & 1 & & & & & \\ & & 4 & 1 & & & & \\ & & & 4 & 1 & & & \\ & & & & 5 & 1 & & \\ & & & & & 5 & 1 & \\ & & & & & & 5 & 1 \\ & & & & & & & 5 & 1 \end{bmatrix} \begin{bmatrix} a(0) \\ a(1) \\ a(3) \\ a(2) \\ a(7) \\ a(6) \\ a(4) \\ a(5) \end{bmatrix} \quad (27)$$

(26)式和(27)式与文献[3]的(6)式和(8)式相似。

五、结 语

本文研究了 $GF(2^m)$ 有限域的元素和其元素间某些运算形式,指出这些运算实质就是不进位运算,进而把二进制数字对的西尔运算推广到 $GF(2^m)$ 域元素的线性运算,定义为广义的西尔运算。快速逻辑变换不仅是广义西尔运算的一个应用,也是有限域代数的一个应用实例。

参 考 文 献

- [1] H. F. Harmuth 著,张其善等译,序率理论基础与应用,人民邮电出版社,北京,1980年,第一章,第71—77页,第89—94页。
- [2] 马华孝,电子学报,12(1984)2,1—8。
- [3] 王万树,电子学报,15(1987)3,99—104。
- [4] 林舒等著,王育民等译,差错控制编码基础和应用,人民邮电出版社,北京,1986年,第二章,第41页。

GENERALIZED SEARLE OPERATIONS

Wang Wanshu

(Jilin University of Technology, Changchun 130025)

Abstract The logical feature of no-carry operations over $GF(2^m)$ and their logical network are discussed, on which generalized Searle operations are defined. The operations are applied to logical fast Walsh transformation over $GF(2^m)$, which facilitates further applications of Searle operations in sequence theory.

Key words No-carry operation; Searle operation; Finite field