# 基于模运算模为合数的多值逻辑函数的展开 [1]

王伶俐 徐新民 陈偕雄

(杭州大学电子工程系 杭州 310028)

**摘 要** 本文分析了模为素数的多值逻辑函数的展开，提出模相关的概念，然后提出了任意四值逻辑函数的展开.

**关键词** 多值逻辑，谱函数，模相关性

**中图号** TN791

## 1 引 言

众所周知模加、模乘运算是模代数理论中的两种基本运算，用它们实现的电路的体积、速度和可测试性方面都有很好的优越性，所以对它的研究一直都很重视 [1,2]。但是该模代数系统在模为合数时却不能象 Reed-Muller 展开式一样展开函数 [3]。虽然也提出多项式模代数来解决模为 $P^m$ 的函数展开问题，其中 $P$ 为任一质数，$m$ 为任一正整数，并且对此也有较多的研究，但在电路实现上却有明显的缺陷 [4,5]。近来又有定义多值“异或”运算，用神经元网络来实现的方法，但还不适合于合数场合 [6]。针对这个问题，本文提出基于模加，模乘运算适用于模为合数时的函数展开，以使模代数也能在模为合数时发挥更大的作用。

## 2 对普通代数和模代数中函数展开式的分析

### 2.1 基本定义

**定义 1** 本文所指的普通代数是指包含实数变量，实数常量以及联结它们的各种运算，如加、减、乘，指数，导数等所构成的代数系统，各运算的优先级都符合传统的规定。

**定义 2** 对一个整数变量 $i$ 的取模 $r$ 运算就是找到任一整数 $m$，使得 $i+mr=r'$ 成立，其中 $r'\in R, R=\{0,1,\cdots,r-1\}$。记作 $(i)_r=r'$，它是一元运算。由此可知，当 $i,r$ 确定时，$r'$ 是唯一确定的。

**定义 3** 二元模运算是指各变量的取值集合均为 $R$，各运算的函数值就是按普通代数中对应的运算的结果经取模 $r$ 运算后得到的值。表 1 列出 $r=2,4$ 时的模加 (用 $\oplus$ 表示)，模乘 (用 $\otimes$ 表示或省略) 运算的真值表。顺便说一下，当 $x=y=0$ 时 $x^y$ 运算在普通代数中可用极限逼近的方法知其为 1。在工程实现中也往往隐含了这一点。我们把函数 $x^y$ 也列于表 1 之中。

**定义 4** 模函数就是由各种变量，常量 (它们的取值都属于 $R$)，以及各种模运算联结成的表达式。

[1] 1996-07-23 收到，1997-03-31 定稿
国家自然科学基金资助项目

### 2.2 函数展开

**定义 5**　任一模 $r$ 函数的规范展开形式可表示为

$$f(x)=\sum_i a_i f_i(x), \tag{1}$$

其中 $x, a_i, i, \sum$ 分别为一变量矢量，模常量，自然数及模运算，$f_i(x)$ 不随 $f(x)$ 变化，且 $f(x)$ 与各 $a_i$ 之间有着一一对应的关系。

根据文献[3,7]，若一单变量函数能按 (1) 式展开，则任一多变量函数也可按 (1) 式展开。为简单起见，以下我们均讨论单变量函数。不失一般性，我们假设其中的 $\sum$ 运算为模加运算。

**表 1 模运算真值表**

(a) $r=2$

| $x$ | $y$ | $x\oplus y$ | $x\otimes y$ | $x^y$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 |

**表 2 模运算真值表**

(b) $r=4$

| $x$ | $y$ | $x\oplus y$ | $x\otimes y$ | $x^y$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 0 |
| 0 | 2 | 2 | 0 | 0 |
| 0 | 3 | 3 | 0 | 0 |
| 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 2 | 1 | 1 |
| 1 | 2 | 3 | 2 | 1 |
| 1 | 3 | 0 | 3 | 1 |
| 2 | 0 | 2 | 0 | 1 |
| 2 | 1 | 3 | 2 | 2 |
| 2 | 2 | 0 | 0 | 0 |
| 2 | 3 | 1 | 2 | 0 |
| 3 | 0 | 3 | 0 | 1 |
| 3 | 1 | 0 | 3 | 3 |
| 3 | 2 | 1 | 2 | 1 |
| 3 | 3 | 2 | 1 | 3 |

**定义 6**　当一模函数能按 (1) 式规范展开时，我们称 $f(x), f_i(x), a_i, i$ 分别为原函数，谱函数，谱系数及展开式的项数。

于是当 $r=2,3$ 时单变量函数 $f(x)$ 可展开为

$$f(x)=f(0)\oplus(f(0)\oplus f(1))x, \tag{2}$$

$$f(x)=f(0)\oplus[2f(1)\oplus f(2)]x\oplus[2f(0)\oplus 2f(1)\oplus 2f(2)]x^2, \tag{3}$$

其中 $f(x_i)=f(x)|_{x=x_i}$ 。

在普通代数中也有类似的展开式，即麦克劳林展开式：

$$f(x)=f(0)+f'(0)x+\frac{f''(0)}{2!}x^2+\cdots+\frac{f^{(n)}(0)}{n!}x^n+\cdots, \tag{4}$$

但对于连续取值的实函数，只有当项数为无穷大时才能精确表达，否则会带来截断误差。这也是离散取值的模代数优越于普通代数之处。

**定义 7**　对于任意两个模函数 $f_1(x)$ 和 $f_2(x)$，若存在模常量 $a_0, a_1$，使得

$$a_0 f_1(x)=a_1 f_2(x), \tag{5}$$

则称 $f_1(x)$ 和 $f_2(x)$ 模相关；否则，为模无关。可见当 $r=2,3$ 时各 $x^i$ 之间是模无关的。而当 $r=4$ 时，因为 $2\otimes x^2=2\otimes x^3$，所以称 $x^2$ 和 $x^3$ 为模相关。

**定理 1** 在模函数的规范展开中，各谱函数 $f_i(x)$ 之间必须模无关。

**证明** 不失一般性可假设函数为单变量 $x$ 的函数，设在 $f(x)$ 的展开式中，

$$f(x)=a_0f_0(x)\oplus\cdots\oplus a_jf_j(x)\oplus\cdots\oplus a_kf_k(x)\oplus\cdots\oplus a_{r-1}f_{r-1}(x) \tag{7}$$

有 $f_j(x)$ 和 $f_k(x)$ 模相关，其中 $0\le j,k\le r-1, j\ne k$, 且 $a_j, a_k\ne 0$，即有

$$b_0f_j(x)=b_1f_k(x), \tag{8}$$

式中 $b_0, b_1\ne 0$。将 (7) 式 $\otimes b_0$ 得

$$\begin{aligned}b_0f(x)=&(a_0b_0)_rf_0(x)\oplus\cdots\oplus(a_jb_0)_rf_j(x)\oplus\cdots\oplus(a_kb_0)_rf_k(x)\\&\oplus\cdots\oplus(a_{r-1}b_0)_rf_{r-1}(x).\end{aligned} \tag{9}$$

为简单起见，可省略取模运算符号 $(\ )_r$。这在计算机中是很易实现的，即进位 (借位) 可以自然丢失，而不必再施加取模运算。

将 (8) 式 $\oplus a_j$ 代入 (9) 得

$$b_0f(x)=a_0b_0f_0(x)\oplus\cdots\oplus(a_jb_1\oplus a_kb_0)f_k(x)\oplus\cdots\oplus a_{r-1}b_0f_{r-1}(x). \tag{10}$$

比较 (9)、(10) 式，可知对于同一函数 $b_0f(x)$，有 2 组谱系数和它对应，这样就违反了定义 5 中关于规范性，即函数与谱系数一一对应性的要求，即 (7) 式中的谱函数不能构成规范展开式。 证毕

根据定理 1 可知当 $r=4$ 时由于 $x^2$ 与 $x^3$ 相关，所以它们不能构成谱函数，这与文献 [3] 的结论是一致的。而当 $r=2,3$ 时各 $x^i$ 能构成谱函数，其中常数项可视为 $x^0$ 的谱系数。

这样，要寻找模为合数时函数的规范展开式，就须寻找互为模无关的谱函数。虽然我们还没判断模相关性的等价条件，但有以下定理帮助判断。

**定理 2** 一组模函数为模无关的必要条件是这些函数所构成的行列式的值 (按普通代数中的求法) 取模运算后不为 0。

**证明** 由于模函数中的取值只是普通代数中的一个子集，所以它们完全可以返回到普通代数中运算而不会冲突。

根据文献 [8] 关于普通代数与模代数的关系，即普通代数中的运算相当于有限位长的模代数中的拓位的情形，可知若一行列式的值在截取有限位后 (即取模运算) 的值为 0，则表示构成行列式的这些函数在截取有限位后对应的模代数中相关，或者说存在不为 0 的常数 $a_0, a_1$ 使得 (5) 式成立。 证毕

例如考察 $r=4$ 时由 $x^0,x^1,x^2,x^3$ 构成的行列式的值，其中 $|\ |_r$ 表示对行列式的值再进行取模 $r$ 运算。

$$\begin{vmatrix}x^0&x^1&x^2&x^3\\1&0&0&0\\1&1&1&1\\1&2&0&0\\1&3&1&3\end{vmatrix}_4=(2-6)_4=0,$$

所以这些函数模相关，即它们之中至少存在 2 个模相关的函数。

但考察 $r=4$ 时由 $x^0,x^1,x^2,x^x$ 构成的行列式

$$\begin{vmatrix} x^0 & x^1 & x^2 & x^x \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 0 & 0 \\ 1 & 3 & 1 & 3 \end{vmatrix}_4 = 2 \neq 0,$$

可它们却是模相关的，因为 $2 \otimes x^1 = 2 \otimes x^2$ .

### 2.3 以模运算展开模为 4 时的多值逻辑函数

由于模为 4 是一个较为经济的代数系统 [9]，本文就讨论 $r=4$ 的情形.

首先寻找互为模无关的谱函数. 考察由 $x^0,(x\oplus 1),x^x,(x\oplus 1)^{x\oplus 1}$ 构成的行列式的值：

$$\begin{vmatrix} x^0 & x\oplus 1 & x^x & (x\oplus 1)^{x\oplus 1} \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 0 & 3 \\ 1 & 0 & 3 & 1 \end{vmatrix}_4 = 1.$$

根据定理 3 可知这些函数有可能构成谱函数.

为进一步考察，我们可列方程组来判断. 假设任一模为 4 的函数均可按以上谱函数展开得

$$f(x) = a_0 \oplus a_1(x\oplus 1) \oplus a_2 x^x \oplus a_3(x\oplus 1)^{x\oplus 1}, \tag{11}$$

取 $x=0,1,2,3$ 得

$$\left.\begin{aligned} f(0) &= a_0 \oplus a_1 \oplus a_2 \oplus a_3, \\ f(1) &= a_0 \oplus 2a_1 \oplus a_2, \\ f(2) &= a_0 \oplus 3a_1 \oplus 3a_3, \\ f(3) &= a_0 \oplus 3a_2 \oplus a_3. \end{aligned}\right\} \tag{12}$$

解以上方程组得

$$\left.\begin{aligned} a_0 &= 3f(0) \oplus 3f(1) \oplus f(2) \oplus 2f(3), \\ a_1 &= 3f(0) \oplus 2f(2) \oplus 3f(3), \\ a_2 &= 3f(0) \oplus 2f(1) \oplus 3f(2), \\ a_3 &= 3f(1) \oplus 2f(2) \oplus 3f(3). \end{aligned}\right\} \tag{13}$$

把 (13) 式代入 (11) 式得模为 4 的多值逻辑函数的展开式为

$$\begin{aligned} f(x) = {} & 2f(0) \oplus 3f(1) \oplus 3f(2) \oplus f(3) \oplus [3f(0) \oplus 2f(2) \oplus 3f(3)]x \\ & \oplus [3f(0) \oplus 2f(1) \oplus 3f(2)]x^x \oplus [3f(1) \oplus 2f(2) \oplus 3f(3)](x\oplus 1)^{x\oplus 1}. \end{aligned} \tag{14}$$

由于 (12) 式可解，说明以上四个函数互为模无关. 读者可从各方面来验证 (14) 式的正确性.

既然任一单变量函数在 $r=4$ 时可按 (14) 式展开，所以它也可以表示任一多变量函数. 也就是说，模运算只在模为质数时才构成完备集的结论已不再成立.

### 2.4 讨论

以上从谱的观点引出模相关的概念，推导出模为 4 时的基于模运算的单变量函数的展开式。当模为其他合数时，还可推导出更一般的展开式使之与麦克劳林展开更好地对应。此外，当 $r=3$ 时除了 (3) 式以外还有以下两式成立，它们对应于泰勒级数展开：

$$f(x)=f(1)\oplus[f(0)\oplus 2f(2)](x\oplus 2)\oplus[2f(0)\oplus 2f(1)\oplus 2f(2)](x\oplus 2)^2, \tag{15}$$

$$f(x)=f(2)\oplus[f(1)\oplus 2f(0)](x\oplus 1)\oplus[2f(0)\oplus 2f(1)\oplus 2f(2)](x\oplus 1)^2. \tag{16}$$

也可讨论模为合数时的泰勒级数展开，并且可以相应地给出模代数中导数的一般定义及其物理意义 [5]。或许其中还同模代数的除法运算有关。

注意到普通代数中线性相关性和矩阵的秩有关，我们也可推导模秩的求法，使其与模相关性对应。最后，关于利用这些展开式实现的电路的可测试性仍需探讨及比较，以使模代数系统发挥更大的作用。

## 参 考 文 献


[1] Kodandapani K L, Setlur R. Reed-Muller canonical forms in multivalued-logic. IEEE Trans. on Computers, 1975, C-24: 628–636.

[2] Mckenzie L, Almaini A E A, Miller J F, Thompson P. Optimization of Reed-Muller logic functions. Int. J. of Electron., 1993, 75(3): 451–466.

[3] 赵小杰，吴训威. 模代数在多值逻辑系统中的适应范围. 科学通报, 1991, 36(18): 1431–1433.

[4] Fakowski B J, Rahardja S. Efficient computation of quarternary fixed polarity Reed-Muller expansions. IEE Proc. Comput. Digit. Tech, 1995, 142(5): 345–352.

[5] Stankvonic R S. Some remarks on Fourier transforms and differential operators for digital functions. Proc. IEEE 22nd ISMVL, Sendai, Japan: 1992, 365–370.

[6] Hozumi T, Kamiura N, Hata Y, Yamato K. Multiple-valued logic design using multiple-valued EXOR. Proc. IEEE 25th ISMVL, Bloomington, Indiana: 1995, 290–295.

[7] 吴训威著，陈偕雄校. 多值逻辑电路设计原理. 杭州：杭州大学出版社, 1994, 20–25.

[8] 王伶俐，陈偕雄. 模代数与普通代数的关系. 杭州大学学报 (自然科学版), 1997, 24(1): 40–44.

[9] Zilic Z, Vranesic Z. Current-mode CMOS Galois field circuits. Proc. IEEE 23rd ISMVL, Sacramento, California: 1993, 245–250.


## EXPANSIONS OF MVL FUNCTIONS IN COMPOSITE FIELD BASED ON MODULO OPERATIONS


Wang Lingli Xu Xinmin Chen Xiexiong

(*Department of Electronic Engineering, Hangzhou University, Hangzhou* 310028)



**Abstract** The expansions of MVL functions in prime field based on Modulo operations are analysed and the concept of modulo relativity is proposed. Then the canonical expansions of any quarternary logic function are presented.



**Key words** Multivalued logic, Spectral function, Modulo relativity



王伶俐： 男， 1971 年生，博士生，从事数字电子学专业.

徐新民： 男， 1966 年生，讲师，从事数字电子学专业.

陈偕雄： 男， 1941 年生，教授，博士生导师，从事数字电子学专业.