文章编号: 1000−8152(2011)10−1513−11

从布尔代数到布尔微积分

程代展, 赵　寅, 徐相如

(中国科学院 数学与系统科学研究院 系统科学研究所, 北京 100190)

摘要: 布尔函数作为最简单的有限值函数具有特殊的重要性. 它在包括信息、控制等许多领域有着广泛的应用. 本文综合介绍有关布尔函数的理论基础. 包括从布尔代数到布尔微积分的主要理论结果, 它们在信息与控制中的一些重要应用, 以及其前沿动态与新进展. 介绍的一个重点是矩阵半张量积在这些领域的应用.

关键词: 布尔函数; 布尔代数; 布尔导数; 布尔积分; 矩阵半张量积

中图分类号: O153.2, O172　　**文献标识码:** A

From Boolean algebra to Boolean calculus

CHENG Dai-zhan, ZHAO Yin, XU Xiang-ru

(Institute of Systems Science, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China)

Abstract: Boolean functions are of special importance, though they are the simplest class of finite-valued functions. It is widely applied to many fields, including information, control and so on. The theoretical foundation of Boolean functions is introduced in this paper, involving some main results from Boolean algebra to Boolean Calculus, applications in information and control and some recent frontiers and developments. The semi-tensor product approach to these fields is introduced emphatically.

Key words: Boolean function; Boolean algebra; Boolean derivative; Boolean integral; semi-tensor product of matrices

1　引言(Introduction)

正如文[1]所指出, 通常说的“布尔代数”有两种不同而又相关的概念: 一是指Boole (1815年至1864年)在19世纪创造的一套基于二值的表示逻辑推理的符号系统. 记$\mathcal{D}=\{0,1\}$, 则$f:\mathcal{D}^n\to\mathcal{D}$通常称为一个$n$元布尔函数, 当$n\leqslant 2$时, 习惯上将它称为逻辑算子. 常用的一元逻辑算子是“非”, 记作“$\neg$”.

$$\neg x=1-x,\ x\in\mathcal{D}. \tag{1}$$

常见的二元逻辑算子有:“合取”记作“$\wedge$”; “析取”记作“$\vee$”; “蕴涵”记作“$\to$”; “等值”记作“$\leftrightarrow$”等, 它们的取值可由真值表表示(见表1). 本文只涉及命题逻辑, 命题逻辑的概念和基本性质可参见文[2].

表 1 真值表

Table 1 Truth table

p	q	$p\wedge q$	$p\vee q$	$p\to q$	$p\leftrightarrow q$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

布尔的第1本数理逻辑著作《逻辑的数学分析》发表于1847年, 它包括了布尔、德摩根(De Morgan)等人关于符号与推理的基本原理. 1854年, 布尔的另一本巨著《思维规则研究》问世, 它在现代数学和控制技术的影响下, 逐渐发展成今天的布尔代数. 布尔代数为古老的逻辑学提供了一个严格的数学描述, 它的助力促使古老的逻辑思辨发展成为一个严格的数学分支和重要的数学基础−数理逻辑[3].

布尔代数在之后的开关电路研究[4,5], 原胞自动机[6], 代数编码[7]等研究中得到广泛应用, 特别是计算机的诞生及计算机科学的发展, 大大促进了布尔代数的研究[8].

布尔代数的方法近年来有许多新发展. 多值逻辑是布尔逻辑的一个自然推广, 它在电路设计和计算机中都有许多应用[9,10], 特别是, 它更准确地刻划了离散值动态模型[11,12]. 虽然模糊逻辑可以取连续值, 但模糊控制本质上只用到有限值逻辑[13]. 最近, 本文作者在研究动态博弈时提出了混合值逻辑这一概念[14,15], 它实际上是最一般的有限集到有限集的映射, 称作有限值函数.

另一个概念是狭义的布尔代数(为区分, 本文将其记作Boole代数), 它是一个严格的代数结构, 近代的书多由“格”导入这一概念[16], 为方便计, 本文采

收稿日期: 2011−03−14.
基金项目: 国家自然科学基金资助项目(61074114, 60736022, 60821091).

如下初等定义.

定义 1[1] 在$\mathcal{D}$上定义3种运算: 一个一元算子$\neg:\mathcal{D}\to\mathcal{D}$; 两个二元算子$\wedge:\mathcal{D}\times\mathcal{D}\to\mathcal{D}$, $\vee:\mathcal{D}\times\mathcal{D}\to\mathcal{D}$. $\{\mathcal{D};\ \neg,\ \wedge,\ \vee\}$称为一个Boole 代数, 如果它满足:

i) 交换律:

$$\begin{cases}x\vee y=y\vee x,\\ x\wedge y=y\wedge x.\end{cases}\tag{2}$$

ii) 结合律:

$$\begin{cases}(x\vee y)\vee z=x\vee(y\vee z),\\ (x\wedge y)\wedge z=x\wedge(y\wedge z).\end{cases}\tag{3}$$

iii) 分配律:

$$\begin{cases}x\vee(y\wedge z)=(x\vee y)\wedge(x\vee z),\\ x\wedge(y\vee z)=(x\wedge y)\vee(x\wedge z).\end{cases}\tag{4}$$

iv) 零一律:

$$\begin{cases}x\vee 0=x,\\ x\wedge 1=x.\end{cases}\tag{5}$$

ii) 互补律:

$$\begin{cases}x\vee\neg x=1,\\ x\wedge\neg x=0.\end{cases}\tag{6}$$

定义1中的“$\neg$”, “$\wedge$”, “$\vee$”可以是任意算子(不必是前面定义的相应逻辑算子). 例如, 一个常用且后面将用到的Boole代数为二元域$GF(2)=\{\mathcal{D},\oplus,\odot\}$, 其中

$$\begin{cases}a\oplus b:=a+b(\text{mod }2),\\ a\odot b:=ab(\text{mod }2).\end{cases}\tag{7}$$

事实上, $\oplus$和$\odot$分别是逻辑算子$\veebar$和$\wedge$. 除特别声明的情况外, 本文将$a\oplus b$和$a\odot b$分别简记为$a+b$与ab.

布尔代数, 或更一般的有限值代数, 无论在控制、信息或计算机领域都起着越来越重要的作用. 研究报告[17]指出: “计算思维正$\cdots$利用计算机科学的基本概念来解决问题、设计系统和理解人类行为.” 而“计算机科学的概念和定理以一种离散的模式来应对动态变化.” 因此, 随着科学的发展和计算机能力的提高, 在未来的科学技术中, 有限值数学的重要性可能超过传统的连续值数学. (这里“有限值代数”指定义域与值域都是有限集合的映射的相关性质与计算.)

本文的目的是介绍有限值代数的基本概念和它的一些进展, 特别是矩阵半张量积在其中的应用. 希望能起到抛砖引玉的作用, 引起大家的注意和研究兴趣.

2 矩阵的半张量积与逻辑的矩阵表示 (Semi-tensor product of matrices and the matrix expression of logic)

利用矩阵半张量积, 布尔函数可以表示为一种矩阵积形式[18]. 这种方法被成功应用于布尔网络[19]的分析与控制, 初步形成了一套确定型布尔网络的控制理论体系[20]. 之后, 该方法又被进一步用于研究布尔函数及布尔微积分的一些性质[21~23], 这些内容将在第3, 4节中介绍. 本节首先介绍矩阵的半张量积与逻辑的矩阵表示. 为方便计, 本文首先介绍一些文中需要用到的记号:

1) $\mathcal{M}_{m\times n}$: $m\times n$维实矩阵集合, 当$m=n$简记为$\mathcal{M}_n$.

2) $\text{Col}(A)(\text{Row}(A))$: 矩阵$A$的列(行)集合, $\text{Col}_i(A)(\text{Row}_i(A))$为$A$的第$i$列(行).

3)

$$\text{diag}\{A_1,A_2,\cdots,A_k\}=\begin{bmatrix}A_1&0&\cdots&0\\0&A_2&\cdots&0\\\vdots&\vdots&\vdots&\vdots\\0&0&\cdots&A_k\end{bmatrix}.$$

4) $\mathcal{D}_k$: $\mathcal{D}_k=\{0,1,\cdots,k-1\}$, $\mathcal{D}:=\mathcal{D}_2$.

5) δ_n^i: 单位阵I_n的第i列.

6) Δ_n: $\Delta_n=\{\delta_n^i\,|\,i=1,2,\cdots,n\}$;

7) $L\in\mathcal{M}_{m\times r}$称为一个逻辑矩阵, 如果$\text{Col}(L)\subset\Delta_m$. $m\times r$维逻辑矩阵集合记作$\mathcal{L}_{m\times r}$.

8) 设$L\in\mathcal{L}_{m\times r}$, 那么$L=[\delta_m^{i_1}\ \delta_m^{i_2}\ \cdots\ \delta_m^{i_r}]$. 为简洁起见, 将它记作

$$L=\delta_m[i_1\ i_2\ \cdots\ i_r].$$

9) $B\in\mathcal{M}_{m\times r}$称为一个布尔矩阵, 如果$B$的元素$b_{i,j}\in\mathcal{D}$, $m\times r$维布尔矩阵集合记作$\mathcal{B}_{m\times r}$.

10) $A=(a_{i,j}),B=(b_{i,j})\in\mathcal{B}_{m\times n}$是两个布尔矩阵. 定义作用在$A$和$B$的布尔算子为相应布尔函数作用在$A$和$B$对应的元上, 例如$\neg A=(\neg a_{i,j})$, $A\wedge B=(a_{i,j}\wedge b_{i,j})$等.

11) $\otimes$是矩阵间的 Kronecker 积, 令$A=(a_{ij})\in\mathcal{M}_{m\times n}$, $A\otimes B$定义为

$$A\otimes B=\begin{bmatrix}a_{11}B&\cdots&a_{1n}B\\\vdots&\vdots&\vdots\\a_{m1}B&\cdots&a_{mn}B\end{bmatrix}.$$

12) $W_{[n,m]}$是一个$mn\times mn$维的常数阵, 它的定义见[18]. 它的作用是将两个分别属于Δ_n与Δ_m的向量的乘积交换位置(见式(9)), 因此本文称之为交换矩阵.

矩阵的半张量积将需满足等维数关系的普通矩

阵乘法推广到任意两个矩阵之间的乘积.

定义 2[18]　设$A \in \mathcal{M}_{m\times n}$, $B \in \mathcal{M}_{p\times q}$, $c = \mathrm{lcm}(n,p)$是n和p的最小公倍数. 则A和B的半张量积(STP)$A \ltimes B$定义为

$$A \ltimes B = (A \otimes I_{\frac{c}{n}})(B \otimes I_{\frac{c}{p}}). \tag{8}$$

当$n = p$时, 很容易看出$A \ltimes B = A \times B$, 即半张量积退化为矩阵的普通乘法. 因此在本文中, 在不引起混淆的情况下本文不区分两者, 并将半张积记号$\ltimes$省略.

所有矩阵乘法的基本性质在半张量积下仍然成立. 下面一些性质是普通矩阵乘法所没有的, 而且这些性质将在下文中用到.

命题 1[20]

1) 设$x \in \mathbb{R}^m$, $y \in \mathbb{R}^n$为两个列向量. 则

$$W_{[m,n]}xy = yx. \tag{9}$$

2) 设$x \in \mathbb{R}^t$为一列向量, A为任一给定矩阵. 则

$$xA = (I_t \otimes A)x. \tag{10}$$

3) 令$x \in \Delta_n$, 则$x^2 = M_r^n x$, 其中

$$M_r^n := \mathrm{diag}\{\delta_n^1, \delta_n^2, \cdots, \delta_n^n\}$$

被称为以n为底的降阶矩阵.

对于布尔变量, 本文令$1 \sim \delta_2^1$, $0 \sim \delta_2^2$, 则$\mathcal{D} \sim \Delta$. 容易看出, 对任意$x \in \mathcal{D}$, 有

$$x \sim \begin{pmatrix} x \\ x+1 \end{pmatrix}.$$

对于$\mathcal{D}^n$中的布尔向量$X = (x_1, x_2, \cdots, x_n)$, 本文还可以用下面两种方法来表示:

1) 数值形式: 将$(x_1, x_2, \cdots, x_n)$看成一个二项制数, 将之转化为十进制

$$\chi = x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_n, \tag{11}$$

注意这里的“+”是实数域中的加法.

2) 向量形式: 将x_i视为Δ中变量, 并记

$$x := \ltimes_{i=1}^n x_i \in \Delta_{2^n}. \tag{12}$$

通过直接计算可验证如下数值形式和向量形式的转换. 因此这3种表达是等价的, 在不引起混淆的情况下, 本文将3者混用.

命题 2　考虑$X = (x_1, x_2, \cdots, x_n)$. 假设$\chi$是其数值形式, 则其向量形式$x \in \Delta_{2^n}$为

$$x = \delta_{2^n}^{2^n - \chi}. \tag{13}$$

另一方面, 如果其向量形式为$x = \delta_{2^n}^t$, 则其数值形式为

$$\chi = 2^n - t. \tag{14}$$

例 1　令$X = (0,0,1,1,0,0,1,1)$, 容易算出

$$\chi = 2^5 + 2^4 + 2 + 1 = 51,$$
$$x = \delta_2^2\delta_2^2\delta_2^1\delta_2^1\delta_2^2\delta_2^2\delta_2^1\delta_2^1 = \delta_{256}^{201}$$

满足式(13)和(14).

通过将布尔变量转化成向量形式, 一个布尔函数$f: \mathcal{D}^n \to \mathcal{D}$可转化为$f: \Delta_{2^n} \to \Delta$. 于是有了下面的结果[24].

定理 1　设$f(x_1, \cdots, x_n)$为一个布尔函数, 在向量形式下有$f: \Delta_{2^n} \to \Delta$. 并且存在唯一逻辑矩阵$M_{\mathrm{f}} \in \mathcal{L}_{2\times 2^n}$, 称为$f$的结构矩阵, 使得

$$f(x_1, \cdots, x_n) = M_{\mathrm{f}} \ltimes x, \tag{15}$$

这里$x = \ltimes_{i=1}^n x_i$.

表2是一些常用逻辑算子的结构矩阵.

表 2　逻辑算子的结构矩阵

Table 2　The structure matrix of logical operators

逻辑算子	结构矩阵
$\neg$	$M_\neg = \delta_2[2\ 1]$
$\wedge$	$M_\wedge = \delta_2[1\ 2\ 2\ 2]$
$\vee$	$M_\vee = \delta_2[1\ 1\ 1\ 2]$
$\to$	$M_\to = \delta_2[1\ 2\ 1\ 1]$
$\leftrightarrow$	$M_\leftrightarrow = \delta_2[1\ 2\ 2\ 1]$
$\bar{\vee}$(或$\oplus$)	$M_\oplus = \delta_2[2\ 1\ 1\ 2]$

3　布尔函数(Boolean function)

布尔函数的性质对其应用, 尤其是在开关电路设计及编码中十分重要. 比如在电路设计中, 线性布尔函数因其容易实现而被广泛应用, 并且希望函数是可以被分解为几个简单部分的. 但在密码系统中, 线性函数容易被攻击, 所以更喜欢用高度非线性布尔函数, 但非线性度最高的布尔函数却失去了平衡性、相关免疫性等在编码中必要的性质. 所以很有必要深入研究布尔函数的性质及其关系. 本节着重介绍半张量积方法在布尔函数的表示, 线性结构及分解中的作用. 更详细的内容可参见文[3,7,25].

3.1　布尔函数的表示(The expressions of Boolean function)

布尔函数已经有许多的表示方法, 不同的方法在布尔函数的分析或计算上有着各自的优势. 定理1给出了一种新的布尔函数的表示方法, 本小节着重介绍布尔函数的多项式表示及谱表示, 它们在对布尔函数的理论分析中十分有用. 然后, 利用定理1 给出的矩阵表示建立从布尔函数真值表到其多项式表示的转换. 其他常用表示, 包括一些图方法可参见文[7,26,27].

最直接的表示方法是将f的所有值排成一个向量, 也就是布尔函数的真值表:

$$[f(\delta_{2^n}^1)\ \ f(\delta_{2^n}^2)\ \ \cdots\ \ f(\delta_{2^n}^{2^n})]^{\mathrm{T}}. \tag{16}$$

注 1 因为f的结构矩阵M_{f}是一个2×2^n的逻辑矩阵, 它完全决定于其第1行

$$m_{\mathrm{f}}^{\mathrm{T}}=\mathrm{Row}_1(M_{\mathrm{f}}).$$

事实上, m_{f}就是f的真值表. 利用半张量积, 本文本质上是赋予了布尔函数的真值表与布尔变量之间, 以及真值表与真值表之间的一种运算关系.

为了得到布尔函数的多项式表示, 对$x\in\mathcal{D}$, 本文首先记$x^1=x$, $x^0=x+1$, 则对任意$c\in\mathcal{D}$, 显然

$$x^c=\begin{cases}1,\ x=c,\\ 0,\ x\neq c.\end{cases} \tag{17}$$

对$X=(x_1,x_2,\cdots,x_n)\in\mathcal{D}^n$和$C=(c_1,c_2,\cdots,c_n)\in\mathcal{D}^n$, 定义

$$X^C:=\prod_{i=1}^{n}x_i^{c_i}=\begin{cases}1,\ X=C,\\ 0,\ X\neq C,\end{cases} \tag{18}$$

那么显然有

$$f(X)=\sum_{C=0}^{2^n-1}f(C)X^C. \tag{19}$$

将式(19)中x^1和x^0用x和$x+1$代替, 则$f(x)$可以展开为$GF^n(2)$中的多项式:

$$f(x)=a_0+\sum_{k=1}^{n}\sum_{1\leqslant j_1<\cdots<j_k\leqslant n}a_{j_1\cdots j_k}x_{j_1}\cdots x_{j_k}. \tag{20}$$

式(20) 即为f的多项式表示.

注意到对任意有m列的矩阵A, 有$A(I_m\otimes B)=A\otimes B$, 于是只考虑式(15)的第1行, 有

$$\begin{aligned}&f(x)=\\ &m_{\mathrm{f}}^{\mathrm{T}}\begin{pmatrix}x_1\\ x_1+1\end{pmatrix}\begin{pmatrix}x_2\\ x_2+1\end{pmatrix}\cdots\begin{pmatrix}x_n\\ x_n+1\end{pmatrix}=\\ &m_{\mathrm{f}}^{\mathrm{T}}\begin{bmatrix}0&1\\ 1&1\end{bmatrix}\begin{pmatrix}1\\ x_1\end{pmatrix}\cdots\begin{bmatrix}0&1\\ 1&1\end{bmatrix}\begin{pmatrix}1\\ x_n\end{pmatrix}=\\ &m_{\mathrm{f}}^{\mathrm{T}}\left(\underbrace{\begin{bmatrix}0&1\\ 1&1\end{bmatrix}\otimes\cdots\otimes\begin{bmatrix}0&1\\ 1&1\end{bmatrix}}_{n}\right)\otimes\\ &\begin{pmatrix}1\\ x_1\end{pmatrix}\begin{pmatrix}1\\ x_2\end{pmatrix}\cdots\begin{pmatrix}1\\ x_n\end{pmatrix}:=\\ &m_{\mathrm{f}}^{\mathrm{T}}P_n\xi_n,\end{aligned}$$

其中

$$P_n=\left(\underbrace{\begin{bmatrix}0&1\\ 1&1\end{bmatrix}\otimes\cdots\otimes\begin{bmatrix}0&1\\ 1&1\end{bmatrix}}_{n}\right), \tag{21}$$

而且

$$\begin{aligned}&\xi_n=\begin{pmatrix}1\\ x_1\end{pmatrix}\begin{pmatrix}1\\ x_2\end{pmatrix}\cdots\begin{pmatrix}1\\ x_n\end{pmatrix}=\\ &(1,x_n,x_{n-1},x_{n-1}x_n,x_{n-2},\cdots,x_1x_2\cdots x_n)^{\mathrm{T}}\end{aligned} \tag{22}$$

中的所有元素是$GF^n(2)$的一组基, 于是$m_{\mathrm{f}}^{\mathrm{T}}P_n\xi_n$已经是$f$的多项式表示. 真值表和多项式之间的转化是早已有的结论[7,28], 但利用半张量积方法, 这种转换非常自然而且方便.

如果要把$m_{\mathrm{f}}^{\mathrm{T}}P_n\xi_n$转化为标准多项式形式(20), 也就是要求$GF^n(2)$的基按脚标及升幂次序排列成

$$\begin{aligned}\eta_n=&(1,x_1,\cdots,x_n,x_1x_2,\cdots,x_{n-1}x_n,\cdots,\\ &x_1x_2,\cdots,x_n)^{\mathrm{T}}.\end{aligned}$$

本文只需引入一个正交矩阵来改变ξ_n中元素的位置. 可以证明如下定理:

定理 2 令

$$\Phi_n=\delta_{2^n}[1\ \ \phi_1\ \ \phi_2\ \ \cdots\ \ \phi_n], \tag{23}$$

其中

$$\begin{aligned}\phi_r=&(\mu_{1,2,\cdots,r},\mu_{2,\cdots,r+1},\cdots,\\ &\mu_{n-r+1,n-r+2,\cdots,n}),\\ &r=1,2,\cdots,n,\\ \mu_{i_1,i_2,\cdots,i_r}=&\sum_{j=1}^{r}2^{n-i_j}+1,\end{aligned}$$

这里的“+”是实数域中的加法.

则布尔函数f的真值表m_{f}, 与其多项式表示的系数向量β之间的转换如下:

$$\begin{cases}\beta=m_{\mathrm{f}}^{\mathrm{T}}P_n\Phi_n,\\ m_{\mathrm{f}}^{\mathrm{T}}=\beta\Phi_n^{\mathrm{T}}P_n^{-1}.\end{cases} \tag{24}$$

例 2 考虑布尔函数

$$f(x_1,x_2,x_3)=x_1\vee(\neg x_2\wedge x_3), \tag{25}$$

将其化为矩阵形式, 有

$$\begin{aligned}&f(x_1,x_2,x_3)=\\ &M_{\vee}x_1M_{\wedge}M_{\neg}x_2x_3=\\ &M_{\vee}(I_2\otimes M_{\wedge}M_{\neg})x_1x_2x_3=\\ &\delta_2[1\ 1\ 1\ 1\ 0\ 0\ 1\ 0]x_1x_2x_3=M_{\mathrm{f}}x.\end{aligned}$$

容易验证$M_{\rm f}$的第1行

$$m_{\rm f}^{\rm T}=[1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0]$$

确实是f的真值表. 所以其多项式表示为

$$f(x_1,x_2,x_3)=\sum_{C=0}^{7}f(C)X^C=$$
$$x_1^1x_2^1x_3^1+x_1^1x_2^1x_3^0+x_1^1x_2^0x_3^1+x_1^1x_2^0x_3^0+x_1^0x_2^0x_3^1=$$
$$x_1x_2x_3+x_1x_2(x_3+1)+x_1(x_2+1)x_3+$$
$$x_1(x_2+1)(x_3+1)+(x_1+1)(x_2+1)x_3=$$
$$x_1+x_3+x_1x_3+x_2x_3+x_1x_2x_3. \tag{26}$$

利用定理2,

$$P_3=\begin{bmatrix}0&1\\1&1\end{bmatrix}\otimes\begin{bmatrix}0&1\\1&1\end{bmatrix}\otimes\begin{bmatrix}0&1\\1&1\end{bmatrix}=$$
$$\begin{bmatrix}0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&1\\0&0&0&0&0&1&0&1\\0&0&0&0&1&1&1&1\\0&0&0&1&0&0&0&1\\0&0&1&1&0&0&1&1\\0&1&0&1&0&1&0&1\\1&1&1&1&1&1&1&1\end{bmatrix},$$

所以

$$f(x)=m_f^{\rm T}P_3\begin{pmatrix}1\\x_1\end{pmatrix}\begin{pmatrix}1\\x_2\end{pmatrix}\begin{pmatrix}1\\x_3\end{pmatrix}=$$
$$[0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1](1,x_3,x_2,x_2x_3,x_1,$$
$$x_1x_3,x_1x_2,x_1x_2x_3)^{\rm T}=$$
$$x_1+x_3+x_1x_3+x_2x_3+x_1x_2x_3.$$

与式(26) 一致.

为了介绍布尔函数的谱表式, 本文首先定义两个$\mathcal{D}^n$中的变量

$$X=(x_1,x_2,\cdots,x_n),\ \Omega=(\omega_1,\omega_2,\cdots,\omega_n)$$

的内积

$$X\cdot\Omega=x_1\omega_1+\cdots+x_n\omega_n\in\mathcal{D}, \tag{27}$$

并记$Q_\Omega(X)=(-1)^{\Omega\cdot X}$. 再定义第一类Walsh变换:

$$S_{\rm f}(\omega)=2^{-n}\sum_{x=0}^{2^n-1}f(x)Q_x(\omega), \tag{28}$$

称之为f的Walsh谱.

其逆变换为

$$f(x)=\sum_{\omega=0}^{2^n-1}S_{\rm f}(\omega)Q_\omega(x). \tag{29}$$

可以证明, 真值表与Walsh谱之间的关系为[7]

$$(f(0),f(1),\cdots,f(2^n-1))=$$
$$(S_{\rm f}(0),S_{\rm f}(1),\cdots,S_{\rm f}(2^n-1))H(n), \tag{30}$$

其中

$$H(n)=\underbrace{\begin{bmatrix}1&1\\1&-1\end{bmatrix}\otimes\cdots\otimes\begin{bmatrix}1&1\\1&-1\end{bmatrix}}_{n}.$$

布尔函数的谱表式在非线性, 平衡性等重要性质中都很关键. 这里本文不再赘述, 下面着重介绍矩阵表示在线性结构及2–分解中的应用.

3.2 布尔函数的线性结构(The linear structure of Boolean functions)

布尔函数可以被表示为多项式形式(20), 因此只含有一次项的布尔函数被称为线性布尔函数. 线性结构是推广的线性布尔函数.

定义 3　$f:\mathcal{D}^n\to\mathcal{D}$是布尔函数.

1) $a\in\mathcal{D}^n$被称为f的不变线性结构, 如果

$$f(x+a)+f(x)=0.$$

2) $a\in\mathcal{D}^n$被称为f的变线性结构, 如果

$$f(x+a)+f(x)=1.$$

3) 记

$$\begin{cases}E_0:=\{a\in\mathcal{D}^n\mid f(x+a)+f(x)=0\},\\E_1:=\{a\in\mathcal{D}^n\mid f(x+a)+f(x)=1\},\\E:=E_0\cup E_1,\end{cases} \tag{31}$$

则E称为f的线性结构子空间.

4) 如果$E\neq\{\mathbf{0}\}$, f称为有线性结构的布尔函数. 对一个有线性结构的布尔函数, 如果$E_0\neq\{\mathbf{0}\}$, 则称f有第一类线性结构, 否则称f有第二类线性结构.

利用布尔函数的矩阵表示及半张量积的基本性质, 可以得到计算线性结构的公式. 令$f(x_1,x_2,\cdots,x_n)$为一布尔函数, 其结构矩阵为$M_{\rm f}$. $a=(a_1,a_2,\cdots,a_n)\in E_0$, 当且仅当

$$M_{\rm f}M_\oplus a_1x_1M_\oplus a_2x_2\cdots M_\oplus a_nx_n=$$
$$M_{\rm f}x_1x_2\cdots x_n. \tag{32}$$

记$a=\ltimes_{i=1}^n a_i$, $x=\ltimes_{i=1}^n x_i$. 于是有

$$M_{\rm f}M_\oplus\ltimes_{i=1}^{n-1}(I_{2^{2^i}}\otimes M_\oplus)\ltimes_{i=1}^{n-1}(I_{2^i}\otimes W_{[2,2^i]})ax=$$
$$M_{\rm f}x. \tag{33}$$

定义

$$\Psi_{\rm f}:=M_{\rm f}M_\oplus\ltimes_{i=1}^{n-1}(I_{2^{2^i}}\otimes M_\oplus)\ltimes_{i=1}^{n-1}\left(I_{2^i}\otimes W_{[2,2^i]}\right),$$

对给定的n, 除$M_{\rm f}$外, 其他部分是已知的常数阵. 将$\Psi_{\rm f}$分成2^n块$\Psi_{\rm f}=[\Psi_1\ \Psi_2\ \cdots\ \Psi_{2^n}]$, 则有:

命题 3　令$\alpha=\ltimes_{i=1}^n a_i=\delta_{2^n}^i$. $(a_1,\cdots,a_n)\in E_0$, 当且仅当$\Psi_i=M_{\rm f}$. $(a_1,\cdots,a_n)\in E_1$, 当且仅当$\psi_i=M_\neg M_{\rm f}$.

例 3 在例2中,

$$f(x_1,x_2,x_3)=x_1+x_3+x_1x_3+x_2x_3+x_1x_2x_3,$$

显然不是线性布尔函数. 本文来验证其有没有线性结构, 直接计算可得

$$\begin{aligned}\Psi_{\rm f}=\delta_2[&2\ 1\ 2\ 2\ 1\ 1\ 1\ 1\ \ 1\ 2\ 2\ 2\ 1\ 1\ 1\ 1\\ &2\ 2\ 2\ 1\ 1\ 1\ 1\ 1\ \ 2\ 2\ 1\ 2\ 1\ 1\ 1\ 1\\ &1\ 1\ 1\ 1\ 2\ 1\ 2\ 2\ \ 1\ 1\ 1\ 1\ 1\ 2\ 2\ 2\\ &1\ 1\ 1\ 1\ 2\ 2\ 2\ 1\ \ 1\ 1\ 1\ 1\ 2\ 2\ 1\ 2].\end{aligned}$$

只有$\psi_8=M_{\rm f}$, 所以$E_0=\{\mathbf{0}\}$, $E_1=\varnothing$, f无线性结构.

3.3 布尔函数的2–分解(Bi-decomposition of Boolean functions)

逻辑电路可以由逻辑函数来表示, 如果逻辑函数可以被分解, 则会显著改善原有电路的性能. 逻辑函数的分解已有大量研究结果[4,5], 本文从半张量积的角度给出出逻辑函数的2–分解的一般方法.

定义 4 $f:\mathcal{D}^n\to\mathcal{D}$是一个布尔函数, $\Gamma\cup\Lambda$是$\{1,2,\cdots,n\}$的一个划分. f是关于Γ和Λ可2–分解的, 如果存在3个布尔函数$F:\mathcal{D}^2\to\mathcal{D}$, $\phi:\{x_\gamma|\gamma\in\Gamma\}\to\mathcal{D}$, $\psi:\{x_\lambda|\lambda\in\Lambda\}\to\mathcal{D}$, 使得

$$f(x_1,\cdots,x_n)=F(\phi(x_\gamma|\gamma\in\Gamma),\psi(x_\lambda|\lambda\in\Lambda)). \tag{34}$$

首先假设

$$\Gamma=\{1,2,\cdots,k\},\ \Lambda=\{k+1,k+2,\cdots,n\}. \tag{35}$$

利用半张量积方法和结构矩阵分析, 可以得到如下判别方法.

定理 3 f是关于形如(35)的划分Γ和Λ可2–分解的, 当且仅当f的结构矩阵可以表示为下述形式

$$M_{\rm f}=[\mu_1M_\psi\ \ \mu_2M_\psi\ \ \cdots\ \ \mu_{2^k}M_\psi], \tag{36}$$

其中$M_\psi\in\mathcal{L}_{2\times2^{n-k}}$; $\mu_i\in S$, $\forall i$, S可以是下列几个类型之一:

类型 1 $S=S_1=\{\delta_2[1\ \ 1],\ \delta_2[2\ \ 2]\}$;

类型 2 $S=S_2=\{\delta_2[1\ \ 1],\ \delta_2[1\ \ 2]\}$或$S=S_2=\{\delta_2[2\ \ 2],\delta_2[1\ \ 2]\}$;

类型 3 $S=S_3=\{\delta_2[1\ 2]\}$, 或 $\{\delta_2[2\ 1]\}$;

类型 4 $S=S_4=\{\delta_2[1\ 2],\ \delta_2[2\ 1]\}$.

如果经验证一个布尔函数是关于Γ和Λ可2–分解的, 则可以通过以下方法来构造分解.

推论 1 假设布尔函数f的结构矩阵$M_{\rm f}$满足定理 3 的条件, 那么F, ϕ, 和ψ的结构矩阵可以通过以下方法构造:

1) 如果集合$\{\mu_1,\cdots,\mu_{2^k}\}$只包含一个元素$\delta_2[p,q]$, 那么

$$M_{\rm F}=[\delta_2[p,q]\ \ \delta_2[p,q]]; \tag{37}$$

否则包含两个元素$\delta_2[p_1,q_1]$, $\delta_2[p_2,q_2]$, 那么

$$M_{\rm F}=[\delta_2[p_1,q_1]\ \ \delta_2[p_2,q_2]]. \tag{38}$$

2) 如果

$$\mu_i=M_{\rm F}\delta_2^{t_i},\ i=1,\cdots,2^k,$$

那么

$$M_\phi=\delta_2[t_1\ \ t_2\ \ \cdots\ \ t_{2^k}]. \tag{39}$$

3) M_ψ取为式(36)中的M_ψ.

定理3要求划分满足(35), 对一般情况, 本文只能逐次交换变量位置去验证是否满足条件. 本文给一个简单的例子来说明.

例 4 仍然考虑例2中的例子

$$f(x_1,x_2,x_3)=x_1\vee(\neg x_2\wedge x_3),$$

显然其已经是分解状态了. 笔者来验证其是否满足定理3的条件. $M_{\rm f}=\delta_2[1\ \ 1\ \ 1\ \ 1\ \ 2\ \ 2\ \ 1\ \ 2]$. 显然$M_\psi=\delta_2[2\ \ 2\ \ 1\ \ 2]$, $\mu_1=\delta_2[1\ \ 1]$, $\mu_2=\delta_2[1\ \ 2]$具有类型2. 所以$M_{\rm F}=\delta_2[1\ \ 1\ \ 1\ \ 2]$, $M_\phi=\delta_2[1\ \ 2]$. 构造出来的结果与原函数一样.

假设一个5元布尔函数$f(x_1,x_2,x_3,x_4,x_5)$的结构矩阵是

$$\begin{aligned}M_{\rm f}=\delta_2[&1\ \ 1\ \ 2\ \ 2\ \ \ 1\ \ 2\ \ 2\ \ 1\ \ \ 1\ \ 1\ \ 2\ \ 2\ \ \ 1\ \ 1\ \ 2\ \ 2\\ &2\ \ 2\ \ 1\ \ 1\ \ \ 2\ \ 1\ \ 1\ \ 2\ \ \ 2\ \ 2\ \ 1\ \ 1\ \ \ 2\ \ 2\ \ 1\ \ 1].\end{aligned}$$

可以验证$M_{\rm f}$并不满足定理3.

通过试错法, 当$\Lambda=\{x_1,x_4\}$时, 将x_2,x_3,x_5调换到x_1之前, 得到新的结构矩阵

$$\begin{aligned}\tilde{M}_{\rm f}=&M_{\rm f}W_{[2,2^3]}W_{[2,2]}W_{[2^3,2^2]}=\\ &\delta_2[1\ \ 2\ \ 2\ \ 1\ \ \ 1\ \ 2\ \ 2\ \ 1\ \ \ 1\ \ 2\ \ 2\ \ 1\ \ \ 2\ \ 1\ \ 1\ \ 2\\ &\ \ 1\ \ 2\ \ 2\ \ 1\ \ \ 1\ \ 2\ \ 2\ \ 1\ \ \ 1\ \ 2\ \ 2\ \ 1\ \ \ 1\ \ 2\ \ 2\ \ 1].\end{aligned}$$

显然它具有类型4,

$$\begin{aligned}M_\psi&=M_{\rm F}=\delta_2[1\ \ 2\ \ 2\ \ 1],\\ M_\phi&=\delta_2[1\ \ 1\ \ 1\ \ 2\ \ 1\ \ 1\ \ 1\ \ 1].\end{aligned}$$

所以$f(x)$可被分解为

$$f(x)=\{[x_2\wedge(x_3\vee x_5)]\vee\neg x_2\}\leftrightarrow\{x_1\leftrightarrow x_4\}.$$

上面讨论的情况假定Γ和Λ不相交. 当分解允许变量分为两个相交的部分时, 称作相交2–分解.

定义 5 $f:\mathcal{D}^n\to\mathcal{D}$是一个布尔函数, $\Gamma\cup\Theta\cup\Lambda$是$\{1,2,\cdots,n\}$的一个划分. f是关于$\Gamma\cup\Theta$和$\Theta\cup\Lambda$可相交2–分解的, 如果存在3个布尔函数$F:\mathcal{D}^2\to\mathcal{D}$, $\phi:\{x_\gamma|\gamma\in\Gamma\cup\Theta\}\to\mathcal{D}$, $\psi:\{x_\lambda|\lambda\in\Lambda\cup\Theta\}\to$

$\mathcal{D}$, 使得

$$f(x_1,\cdots,x_n)=$$
$$F(\phi(x_\gamma|\gamma\in\Gamma\cup\Theta),\psi(x_\lambda|\lambda\in\Theta\cup\Lambda)). \tag{40}$$

仍然首先假设

$$\begin{cases} X^1=\{x_1^1,\cdots,x_{k_1}^1\}=\{x_i|i\in\Gamma\},\\ X^2=\{x_1^2,\cdots,x_{k_2}^2\}=\{x_i|i\in\Theta\},\\ X^3=\{x_1^3,\cdots,x_{k_3}^3\}=\{x_i|i\in\Lambda\}. \end{cases} \tag{41}$$

利用类似定理3的方法, 可以得到

定理 4　令$f:\mathcal{D}^n\to\mathcal{D}$为一布尔函数, $M_{\rm f}$是其结构矩阵. f可以被分解成形如式(40), 当且仅当它的结构矩阵可以表示为

$$\begin{aligned} M_{\rm f}=[&\mu_{1,1}M_\psi^1\ \ \mu_{1,2}M_\psi^2\ \ \cdots\ \ \mu_{1,2^{k_2}}M_\psi^{2^{k_2}}\\ &\mu_{2,1}M_\psi^1\ \ \mu_{2,2}M_\psi^2\ \ \cdots\ \ \mu_{2,2^{k_2}}M_\psi^{2^{k_2}}\\ &\quad\vdots\\ &\mu_{2^{k_1},1}M_\psi^1\ \ \mu_{2^{k_1},2}M_\psi^2\ \ \cdots\ \ \mu_{2^{k_1},2^{k_2}}M_\psi^{2^{k_2}}], \end{aligned} \tag{42}$$

其中:

$$M_\psi^s\in\mathcal{L}_{2\times2^{k_3}},\ s=1,\cdots,2^{k_2};$$
$$\mu_{i,j}\in S,\ i=1,\cdots,2^{k_1},\ j=1,\cdots,2^{k_2}.$$

S是注3中定义的S_1, S_2, S_3, S_4之一.

在上述框架下, 可以继续讨论多值逻辑函数函数, 混合值逻辑函数的2–分解以及它们的应用[22].

4　布尔微积分(Boolean calculus)

4.1　布尔导数(Boolean derivative)

Reed在研究纠错码的性质时首先提出布尔差分的概念[29], 其很多后续研究[30~32]提出了布尔微分及各种衍生概念. 文[33]是介绍布尔差分(微分)较全面的参考书, 在文[8]中相应章节对相应概念也有较详细的论述.

布尔差分(微分)在组合以及时序电路的故障检测, 设计, 分析, 测试与综合中得到了广泛的研究和应用[31,34]. 文[35]指出“布尔差分(微分) 是组合逻辑电路的理论基础”, 但是计算布尔差分(微分)“要处理大量文字符号的计算”. 半张量积方法正是把逻辑转换成数字运算, 它可以很好的解决这个问题. 除此以外, 布尔差分(微分) 在布尔函数的分解[22,36,37], 布尔网络的控制[38], 离散事件动态系统[39], 元胞自动机及有限自动机理论[40,41], 图像边界检测[42], 滤波理论[43]等理论中都有着广泛的应用.

布尔差分(微分)从不同角度有多种定义, 本文从布尔导数的角度对其进行探讨[44].

定义 6　设$f(x_1,\cdots,x_n):\mathcal{D}^n\to\mathcal{D}$是布尔函数.

1)　f关于x_i的布尔导数定义为

$$\frac{\partial f}{\partial x_i}=f(x_1,\cdots,x_i,\cdots,x_n)\oplus f(x_1,\cdots,\neg x_i,\cdots,x_n). \tag{43}$$

2)　f关于$x_{i_1},\cdots,x_{i_k}$的高阶布尔导数定义为

$$\frac{\partial^k f}{\partial x_{i_1}\cdots\partial x_{i_k}}=\frac{\partial}{\partial x_{i_1}}(\frac{\partial}{\partial x_{i_2}}(\cdots(\frac{\partial f}{\partial x_{i_k}}))). \tag{44}$$

布尔导数有一些常见的性质:

命 题 4[45]　$\dfrac{\partial f}{\partial x_i}$是与$x_i$无关的布尔函数, 因此$\dfrac{\partial^2 f}{\partial^2 x_i}=0$.

$$\frac{\partial^2 f}{\partial x_i\partial x_j}=\frac{\partial^2 f}{\partial x_j\partial x_i}, \tag{45}$$
$$\frac{\partial(f_1\oplus f_2)}{\partial x_i}=\frac{\partial f_1}{\partial x_i}\oplus\frac{\partial f_2}{\partial x_i}, \tag{46}$$
$$\frac{\partial(f_1f_2)}{\partial x_i}=\frac{\partial f_1}{\partial x_i}f_2\oplus f_1\frac{\partial f_2}{\partial x_i}\oplus\frac{\partial f_1}{\partial x_i}\frac{\partial f_2}{\partial x_i}. \tag{47}$$

记$\bar f:=\neg f$, 以及$\bar x:=\neg x$, 那么

$$\frac{\partial\bar f}{\partial x_i}=\frac{\partial f}{\partial x_i},\ \frac{\partial f}{\partial\bar x_i}=\frac{\partial f}{\partial x_i}. \tag{48}$$

设布尔函数$f(x_1,\cdots,x_n)$的结构矩阵是$M_{\rm f}$, 布尔导数算子$\dfrac{\partial}{\partial x_i}$的矩阵表示是$M_{\partial_i f}$. 记$x:=\ltimes_{i=1}^n x_i$, 那么

$$\frac{\partial f}{\partial x_i}=M_{\partial_i f}x=M_{\rm f}x\oplus M_{\rm f}x_1\cdots\bar x_i\cdots x_n. \tag{49}$$

利用半张量积的性质, $M_{\partial_i f}$可以计算为

$$M_{\partial_i f}=M_\oplus M_{\rm f}[I_{2^n}\otimes M_{\rm f}(I_{2^{i-1}}\otimes M_\neg)]M_r^{2^n}, \tag{50}$$

f的高阶布尔导数可以利用上式递归地得到. 本文可以进一步得到$\dfrac{\partial f}{\partial x_i}$显式的结构矩阵形式. 为此, 先给出如下命题.

命 题 5　设$f(x_1,\cdots,x_n)$和$g(x_1,\cdots,x_n)$的真值表分别为$m_{\rm f},m_{\rm g}\in\mathcal{B}_{2^n}$. 设$\sigma$是一个二元逻辑算子, 那么

$$m_{f\sigma g}=m_{\rm f}\sigma m_g. \tag{51}$$

根据命题5, 可以得到

$$m_{\partial_i f}^{\rm T}=m_{\rm f}^{\rm T}\oplus m_{\rm f}^{\rm T}(I_{2^{i-1}}\otimes M_\neg). \tag{52}$$

利用异或算子的分配律性质得: $m_{\partial_i f}^{\rm T}=m_{\rm f}^{\rm T}\ltimes_{\mathcal{B}}(I_{2^{i-1}}\otimes\mathbf{1}_{2\times2})$, 其中$\ltimes_{\mathcal{B}}$是指用$GF(2)$中的加法与乘法代替半张量积定义中元素之间的运算. 综上, 有以下定理:

定理 5　设布尔函数$f(x_1,\cdots,x_n)$的结构矩阵

是$M_{\rm f}$, 那么$\dfrac{\partial f}{\partial x_i}$的结构矩阵$M_{\partial_i f}$是

$$M_{\partial_i f}=\begin{bmatrix}\mathrm{Row}_1(M_{\rm f})\ltimes_{\tilde B}\Xi_n^i\\ \neg\mathrm{Row}_1(M_{\rm f})\ltimes_{\tilde B}\Xi_n^i\end{bmatrix},\tag{53}$$

这里$\Xi_n^i=I_{2^{i-1}}\otimes\mathbf{1}_{2\times 2}$.

因此, 在向量形式下$\dfrac{\partial f}{\partial x_i}=M_{\partial_i f}x$, 同时布尔函数$\partial_i f$的真值表$m_{\partial_i f}=[\Xi_n^i]^{\rm T}m_{\rm f}$.

但是函数$\dfrac{\partial f}{\partial x_i}$与$x_i$无关, 本文可以进一步得到$\dfrac{\partial f}{\partial x_i}$与$x_i$无关的结构矩阵形式:

$$\frac{\partial f}{\partial x_i}=M_{\partial_{[i]}\rm f}x_1\ \cdots\ x_{i-1}\ \hat{x}_i x_{i+1}\ \cdots\ x_n,\tag{54}$$

其中记号$\hat{x}_i$是指x_i在此不出现. 为此, 把$M_{\partial_i f}$等分成2^i个矩阵块$M_{\partial_i f}=[C_1\ C_2\ \cdots\ C_{2^i}]$. 么$M_{\partial_{[i]}\rm f}$就是$M_{\partial_i f}$所有奇数矩阵块组成的矩阵(或者所有偶数矩阵块组成的矩阵), 这可以通过右乘以下矩阵得到:

$$\left(I_{2^{i-1}}\otimes\begin{bmatrix}I_{2^{n-i}}\\ \mathbf{0}_{2^{n-i}\times 2^{n-i}}\end{bmatrix}\right),$$

于是

$$M_{\partial_{[i]}\rm f}=\begin{bmatrix}\mathrm{Row}_1(M_{\rm f})\ltimes_{\tilde B}[\Psi_n^i]^{\rm T}\\ \neg\mathrm{Row}_1(M_{\rm f})\ltimes_{\tilde B}[\Psi_n^i]^{\rm T}\end{bmatrix},\tag{55}$$

这里

$$\Psi_n^i=$$

$$(I_{2^{i-1}}\otimes\begin{bmatrix}I_{2^{n-i}}\ \mathbf{0}_{2^{n-i}\times 2^{n-i}}\end{bmatrix})\ltimes_{\tilde B}(I_{2^{i-1}}\otimes\mathbf{1}_{2\times 2})=$$

$$I_{i-1}\otimes\mathbf{1}_2^{\rm T}\otimes I_{n-i}.$$

推论 2 设布尔函数$f(x_1,\cdots,x_n)$真值表为$m_{\rm f}$, 那么布尔函数

$$\frac{\partial f}{\partial x_i}(x_1,\cdots,x_{i-1},\hat{x}_i,x_{i+1},\cdots,x_n)$$

的真值表为

$$m_{\partial_{[i]}\rm f}=\Psi_n^i m_{\rm f}.\tag{56}$$

这与文[42]的结果是一致的.

推论 3 把$m_{\rm f}^{\rm T}$等分为2^i个矩阵块

$$m_{\rm f}^{\rm T}=(c_{1,1}\ c_{1,2}\ c_{2,1}\ c_{2,2}\ \cdots\ c_{2^{i-1},1}\ c_{2^{i-1},2}),$$

那么$m_{\partial_{[i]}\rm f}^{\rm T}$可以直接通过以下公式计算:

$$m_{\partial_{[i]}\rm f}^{\rm T}=$$

$$(c_{1,1}\oplus c_{1,2}\ c_{2,1}\oplus c_{2,2}\ \cdots\ c_{2^{i-1},1}\oplus c_{2^{i-1},2}).\tag{57}$$

推论 4 $\dfrac{\partial^k f}{\partial x_{i_1}\cdots\partial x_{i_k}}$的真值表为(设$i_1>i_2>\cdots>i_k$):

$$m_{\partial_{[i_k,\cdots,i_1]}\rm f}=\Psi_{n-k+1}^{i_k}\Psi_{n-k+2}^{i_{k-1}}\cdots\Psi_n^{i_1}m_{\rm f}.\tag{58}$$

这两个推论可以用于涉及布尔导数的数值计算. 例如, 如下涉及布尔函数$f(x_1,\cdots,x_n)$及其相关布尔导数的方程组的一类问题可以通过半张量积方法和以上引理方便地得到解决:

$$\begin{cases}G_j(x_i,f,\dfrac{\partial f}{\partial x_i},\cdots,\dfrac{\partial^k f}{\partial x_{i_1}\cdots\partial x_{i_k}})=c_j,\\ j=1,\cdots,s,\ i=1,\cdots,n.\end{cases}\tag{59}$$

组合电路的故障检测问题就是以上问题的典型例子: 设$f(x_1,\cdots,x_n)$是描述一个组合电路的布尔函数. 那么stuck-at-faults $x_i(s-a-\alpha)$, $x_j(s-a-\beta)$的测试矢量集是以下方程的解:

$$\bar{x}_i^\alpha x_j^\beta\frac{\partial f}{\partial x_i}\oplus x_i^\alpha\bar{x}_j^\beta\frac{\partial f}{\partial x_j}\oplus\bar{x}_i^\alpha\bar{x}_j^\beta\frac{\partial^2 f}{\partial x_i\partial x_j}=1,\tag{60}$$

这里$\alpha,\beta\in\mathcal{D}$, 而$x^1:=x$, $x^0:=\bar{x}$.

下面给出上述方法在解布尔微分方程中应用的例子.

例 5 考虑如下布尔微分方程, 边界条件$F(\mathbf{0})=0$:

$$\begin{cases}\dfrac{\partial F}{\partial x_3}=\neg x_1\wedge\neg x_4,\\ \dfrac{\partial^2 F}{\partial x_1\partial x_4}=\neg(x_2\vee x_3)\vee(x_2\wedge x_3),\\ \dfrac{\partial^2 F}{\partial x_2\partial x_4}=\neg x_1,\\ \dfrac{\partial^2 F}{\partial x_1\partial x_3}\vee\dfrac{\partial^2 F}{\partial x_1\partial x_2}=1.\end{cases}\tag{61}$$

将上述逻辑方程组转换为向量形式:

$$\begin{cases}M_{\partial_{[3]}F}=\delta_2[2\ 2\ 2\ 2\ 2\ 1\ 2\ 1],\\ M_{\partial_{[1,4]}F}=\delta_2[1\ 2\ 2\ 1],\\ M_{\partial_{[2,4]}F}=\delta_2[2\ 2\ 1\ 1],\\ \mathrm{Col}(M_\vee M_{\partial_{[1,3]}F}(I_4\otimes M_{\partial_{[1,2]}F})(I_2\otimes W_{[2]})\times\\ (I_4\otimes M_r^2))=\{\delta_2^1\}.\end{cases}$$

设F的真值表为$[a_1\ a_2\ \cdots\ a_{16}]$, 那么

$$\begin{aligned}&a_1\oplus a_3=0,\ a_2\oplus a_4=0,\\ &a_5\oplus a_7=0,\ a_6\oplus a_8=0,\\ &a_9\oplus a_{11}=0,\ a_{10}\oplus a_{12}=1,\\ &a_{13}\oplus a_{15}=0,\ a_{14}\oplus a_{16}=1\\ &a_1\oplus a_2\oplus a_9\oplus a_{10}=1,\\ &a_3\oplus a_4\oplus a_{11}\oplus a_{12}=0,\\ &a_5\oplus a_6\oplus a_{13}\oplus a_{14}=0,\\ &a_7\oplus a_8\oplus a_{15}\oplus a_{16}=1,\\ &a_1\oplus a_2\oplus a_5\oplus a_6=0,\end{aligned}$$

$$a_3 \oplus a_4 \oplus a_7 \oplus a_8 = 0,$$
$$a_9 \oplus a_{10} \oplus a_{13} \oplus a_{14} = 1,$$
$$a_{11} \oplus a_{12} \oplus a_{15} \oplus a_{16} = 1$$
$$a_3 \oplus a_7 \oplus a_{11} \oplus a_{15} = 1,$$
$$a_4 \oplus a_8 \oplus a_{12} \oplus a_{16} = 0.$$

边界条件$F(\mathbf{0}) = 0$表明$a_{16} = 0$, 可以得到方程的一般解如下:

$$m_{\mathrm{F}}^{\mathrm{T}} = \mathrm{Row}_1(M_{\mathrm{F}}) =$$
$$[a\ \ b\ \ a\ \ b\ \ c\ \ a \oplus \neg b \oplus \neg c$$
$$c\ \ a \oplus \neg b \oplus \neg c\ \ \neg b \oplus \neg c\ \ a \oplus \neg c$$
$$\neg b \oplus \neg c\ \ a \oplus c\ \ a \oplus \neg b\ \ 1\ \ a \oplus \neg b\ \ 0].$$

这里a, b和c可以是任意的布尔值.

4.2 布尔积分(Boolean integral)

直观的说, 本文可以定义上述布尔微分的逆映射作为布尔积分. 首先给出原函数的定义:

定义 7　给定布尔函数$f(x_1, \cdots, x_n)$. 如果存在$F(x_1, \cdots, x_{i-1}, z, x_i, \cdots, x_n)$, 使得

$$\frac{\partial F}{\partial z} = f(x_1, \cdots, x_n), \tag{62}$$

则称F为$f(x)$的第i次原函数, 记作

$$\int f(x_1, \cdots, x_n)\mathrm{d}[i] =$$
$$F(x_1, \cdots, x_{i-1}, z, x_i, \cdots, x_n). \tag{63}$$

由式(56), 求解原函数的问题即是求解以下方程:

$$\Psi_{n+1}^i m_{\mathrm{F}} = m_{\mathrm{f}}. \tag{64}$$

布尔函数$F(x_1, \cdots, x_n)$的微分形式$\mathrm{d}F$记作

$$\mathrm{d}F := \frac{\partial F}{\partial x_1}\mathrm{d}x_1 + \cdots + \frac{\partial F}{\partial x_n}\mathrm{d}x_n.$$

注意, 这里符号“+”只是形式记号. 本文可以给出下面布尔函数不定积分的概念.

定义 8　给定一组布尔函数

$$f_i(x_1, \cdots, x_{i-1}, \hat{x}_i, x_{i+1} \cdots, x_n),\ i = 1, \cdots, n.$$

如果存在$F(x_1, \cdots, x_n)$, 使得

$$\frac{\partial F}{\partial x_i} = f_i,\ i = 1, \cdots, n. \tag{65}$$

那么函数F称作微分形式

$$\mathrm{d}h = f_1\mathrm{d}x_1 + f_2\mathrm{d}x_2 + \cdots + f_n\mathrm{d}x_n$$

的不定积分, $\mathrm{d}h$被称为可积的.

显然如果F是$\mathrm{d}h$的不定积分, 那么$\bar{F}$也是$\mathrm{d}h$ 的不定积分. 本文称F跟$\bar{F}$为互反的.

以下定理给出布尔函数不定积分存在性的充要条件.

定理 6　设微分形式

$$\mathrm{d}h = f_1\mathrm{d}x_1 + f_2\mathrm{d}x_2 + \cdots + f_n\mathrm{d}x_n,$$

那么$\mathrm{d}h$存在一对互反的不定积分$F, \bar{F}$当且仅当

$$\frac{\partial f_i}{\partial x_j} = \frac{\partial f_j}{\partial x_i},\ 1 \leqslant i < j \leqslant n. \tag{66}$$

如果$\mathrm{d}h$是可积的, 记$\mathrm{d}h$的不定积分为

$$\int \mathrm{d}h = F(x) + C(C \in \mathcal{D}).$$

定理6表明, F在互反等价的意义下是唯一的. 记

$$\int \mathrm{d}h = F(x),\ F(\mathbf{0}) = 0;$$
$$\int \bar{\mathrm{d}}h = \bar{F}(x),\ \bar{F}(\mathbf{0}) = 1.$$

那么布尔函数$F(x)$可以通过下面的定理得到:

定理 7　微分形式$\mathrm{d}h = f_1\mathrm{d}x_1 + \cdots + f_n\mathrm{d}x_n$的不定积分如果存在, 该不定积分的真值表等于如下代数方程的解z(如果方程解存在, 则z, $\bar{z}$都是以下方程的解. 不失一般性, 假设$z_{2^n} = 0$):

$$\Psi_n \ltimes_{\mathcal{B}} z = b, \tag{67}$$

这里

$$\Psi_n = \begin{bmatrix} \Psi_n^1 \\ \Psi_n^2 \\ \vdots \\ \Psi_n^n \end{bmatrix} \in \mathcal{B}_{n\cdot 2^{n-1} \times 2^n},\ \text{且}\ b = \begin{bmatrix} m_{f_{[1]}}^{\mathrm{T}} \\ m_{f_{[2]}}^{\mathrm{T}} \\ \vdots \\ m_{f_{[n]}}^{\mathrm{T}} \end{bmatrix} \in \mathcal{B}_{n\cdot 2^{n-1}}.$$

例 6　设微分形式$\mathrm{d}h = x_2\mathrm{d}x_1 + \neg x_1\mathrm{d}x_2$, 那么

$$m_{\partial_{[1]}f} = [1\ \ 0]^{\mathrm{T}},\ m_{\partial_{[2]}f} = [0\ \ 1]^{\mathrm{T}}.$$

方程(67)即为

$$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \ltimes_{\mathcal{B}} \begin{bmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

由$F(\mathbf{0}) = 0$得$z_4 = 0$. 因此上述方程的解为

$$z_1 = 0,\ z_2 = 0,\ z_3 = 1,\ z_4 = 0,$$

即$m_{\mathrm{F}} = [0\ \ 0\ \ 1\ \ 0]^{\mathrm{T}}$. 因此,

$$\int x_2\mathrm{d}x_1 + \neg x_1\mathrm{d}x_2 = (\neg x_1) \wedge x_2, \tag{68}$$

或

$$\int x_2\bar{\mathrm{d}}x_1 + \neg x_1\bar{\mathrm{d}}x_2 = (\neg x_1) \wedge x_2 \oplus 1. \tag{69}$$

5 结论(Conclusion)

布尔代数和以它为代表的有限值代数在计算机、信息、编码及控制理论中起着越来越重要的作用. 本文对布尔代数及布尔微积分作了一个梗概的介绍, 同时展示了矩阵半张量积在其中的许多有成

效的应用. 过去, 人们更多地关心连续性数学, 寻找各种问题的闭形式的解. 但实际上, 正如数学家格拉哈姆所说: “背离传统的证明的潮流或许是不可避免的. 单靠人的思维无法证明的东西是一片汪洋大海, 与这片大海相比, 你能够证明的东西或许只是些孤零零的小岛, 一些例外情况而已.” [46]在纯粹数学逐渐退化成少数人的游戏的同时, 基于计算机的有限值数学却越来越成为解决实际工程问题甚至许多理论问题的有力工具. 有人说: “微积分在数学当中一贯处于领袖地位, 可以预期, 有朝一日这种地位将被离散数学夺走.” [46] 本文的目的之一就是希望引起读者对有限值代数的重视.

参考文献(References):

[1] ROSS K A, WRIGHT C R B. *Discrete Math*[M]. New York: Prentice Hall Inc, 2003.

[2] HAMILTON A G. *Logic for Mathematicians*[M]. Revised Ed. Cambridge: Press of University Cambridge, 1988.

[3] 杨炳儒. 布尔代数及其泛化结构[M]. 北京: 科学出版社, 2008.
(YANG Bingru. *Boolean Algebra and Its Generalization Structure*[M]. Beijing: Science Press, 2008.)

[4] ASHENHURST R L. The decomposition of switching functionis[C] //*Proceedings of an International Symposium on the Theory of Switching*. Cambridge: Harvard University Press, 1957: 74 – 116.

[5] CURTIS H A. *A New Approach to The Design of Switching Circuits*[M]. Princeton, N.J.: Van Nostrand, 1962.

[6] WOLFRAM S. *Theory and Applications of Cellular Automata*[M]. Singapore: World Scientific, 1986.

[7] 温巧燕, 钮心忻, 杨义先. 现代密码学中的布尔函数[M]. 北京: 科学出版社, 2000.
(WEN Qiaoyan, NIU Xinxin, YANG Yixian. *Boolean Functions in Modern Cryptographies*[M]. Beijing: Science Press, 2000.)

[8] POSTHOFF C, STEINBACK B. *Logic Functions and Equations – Bimary Models for Computer Science*[M]. Dordrecht: Springer, 2004.

[9] 陈书开. 多值逻辑电路与神经网络和模糊计算机[M]. 北京: 国防工业出版社, 2002.
(CHEN Shukai. *Multi-Valued Logic Circuits, Neural Networks and Fuzzy Computer*[M]. Beijing: National Defence Industry Press, 2002.)

[10] SASAO T. *Switching Theory for Logic Synthesis*[M]. Norwell: Kluwer Academic Publishers, 1999.

[11] ADAMATZKY A. On dynamically non-trivial three-valued logics: oscillatory and bifurcatory species[J]. *Chaos Solitons & Fractals*, 2003, 18(5): 917 – 936.

[12] LI Z, CHENG D. Algebbraic approach to dynamics of multi-valued networks[J]. *Intternational Journal of Bifurcation and Chaos*, 2010, 20(2): 561 – 582.

[13] VERBRUGGEN H B, BABUSKA R (Eds.). *Fuzzy Logic Control Advances in Applications*[M]. Singapore: World Scientific Publishing Company, 1999.

[14] CHENG D, ZHAO Y, MU Y. Strategy optimization with its application to dynamic games[C] //*Proceedings of the 49th IEEE Conference on Decision an Control*. New York: IEEE, 2010: 5822 – 5827.

[15] ZHAO Y, LI Z, CHENG D. Optimal control of logical control networks[J]. *IEEE Transactions on Automatic Control*, Doi:10.1109/TAC.2010.2092290. (to appear, early access: http://ieeexplore.ieee.org/xpls/abs_all.jsp? arnumber=5635323& tag=1)

[16] BURRIS S, SANKAPPANAVAR H H. *A Course in Universal Algebra*[M]. New York: Springer-Verlag, 1981.

[17] EMMOTT S(Editor-in-Chief). *Towards 2020 Science*[M]. Cambridge: Microsoft Prsearch Ltd, 2006.

[18] CHENG D. Semi-tensor product of matrices and its applications: A survey[C] //*Proceedings of International Congress of Chinese Mathematicians*. Beijing: International Press, 2007, 3: 641 – 668.

[19] KAUFFMAN S A. Metabolic stability and epigenesis in randomly constructed genetic nets[J]. *Journal of Theoretical Biology*, 1969, 22(3): 437 – 467.

[20] CHENG D, QI H, LI Z. *Analysis and Control of Boolean Networks: A Semi-tensor Product Approach*[M]. London: Springer, 2011.

[21] CHENG D, ZHAO Y, XU X. Matrix approach to Boolean calculus[J]. to appear. Preprint: http://lsc.amss.ac.cn/ dcheng/preprint/DerBool_cdc11.pdf.

[22] CHENG D, XU X. Bi-decomposition of logical mappings via semi-tensor product of matrices[J]. to appear. Preprint: http://lsc.amss.ac.cn/dcheng/preprint/FAC11.pdf.

[23] ZHAO Y, GAO X, CHENG D. Some applications of the matrix expression of Boolean function via semi-tensor product[J]. to appear. Preprint: http://lsc.amss.ac.cn/dcheng/preprint/bf01.pdf.

[24] 程代展, 齐洪胜. 矩阵的半张量积──理论与应用[M]. 北京: 科学出版社, 2007.
(CHENG Daizhan, QI Hongsheng. *Semi-Tensor Product of Matrices: Theory and Application*[M]. Beijing: Science Press, 2007.)

[25] KIM K H. *Boolean Matrix Theory and Applications*[M]. New York: Marcel Dekker, 1982.

[26] AKERS S B. Binary decision diagrams[J]. *IEEE Transactions on Computer*, 1978, 27(6): 509 – 516.

[27] WACHTER M, HAENNI R. Propositional DAGs: a New Graph-Based Language for Representing Boolean Functions[C] //*Proceedings of KR'06, 10th International Conference on Principles of Knowledge Representation and Reasoning*. Lake District, UK: AAAI, 2006, 6: 275 – 285.

[28] CARLET C. Boolean functions for cryptography and error-correcting codes[C] //CRAMA C Y, HAMMER P. *Boolean Methods and Models in Mathematics, Computer Science, and Engineering*. Cambridge: Cambridge University Press, 2010.

[29] REED I S. A class of multiple error-correctiong and the decoding schene[J]. *IRE Transactions on Information Theory*, 1954, 4(4): 38 – 49.

[30] AKERS S B. On a theory of Boolean functions[J]. *Journal of the Society for Industrial and Applied Mathematics*, 1959, 7(4): 487 – 498.

[31] HSIAO M Y, CHIA D K. Boolean difference for fault detection in asynchronous sequential machines[J]. *IEEE Transactions on Computers*, 1971, 20(11): 1356 – 1361.

[32] TUCKER J H, TAPIA M A, BENNETT A W. Boolean integral calculus[J]. *Applied Mathematics and Computation*, 1988, 26(3): 201 – 236.

[33] THAYSE A. *Boolean Calculus of Differentces*[M]. Berlin: Springer-Verlag, 1981.

[34] SMITH J R, ROTH C H. Analysis and synthesis of asynchronous sequential networks using edge-sensitive flip-flops[J]. *IEEE Transactions on Computers*, 1971, 20(8): 847 – 855.

[35] 杨士元. 数字系统的故障诊断与可靠性设计[M]. 北京: 清华大学出版社, 2000.
(YANG Shiyuan. *Fault Diagnosis and Reliability Design of Digital Systems*[M]. Beijing: Tsinghua University Press, 2000.)

[36] SASAO T, BUTLER J T. On Bi-decompositions of logic functions[C] //*Proceedings of International Worksop on Logic Synthesis*. New York: IEEE, 1997: 1 – 6.

[37] SHEN V Y S, MCKELLAR A C, WEINER P. A fast algorithm for the disjunctive decomposition of switching functions[J]. *IEEE Transactions on Computers*, 1971, 20(3): 304 – 309.

[38] LUQUE B, SOLE R V. Lyapunov exponents in random Boolean networks[J]. *Physica A*, 2000, 284(1/4): 33 – 45.

[39] SCHEURING R, WEHLAN H. On the design of discrete event dynamic systems bu means of the Boolean diff erential calculus[C] //*First IFAC Symposium on Design Methods of Control Systems*. Pergamon: IFAC, 1991, 2: 723 – 728.

[40] PABITRA P C, SAHOO S, CHAKRABORTY M, et al. Investigation of the globak dynamics of cellular automata using Boolean derivatives[J]. *Computers & Mathematics with Applications*, 2009, 57(8): 1337 – 1351.

[41] VANDERMEULEN E, DONEGAN H A, LARNAC M, et al. The Temporal Boolean derivative applied to verification of extended finite state machines[J]. *Computers & Mathematics with Applications*, 1995, 30(2): 27 – 36.

[42] AGAIAN S S, PANETTA K A, NERCESSIAN S C, et al. Boolean derivatives with application to edge detection for imaging systems[J]. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 2010, 40(2): 371 – 382.

[43] EGIAZARIAN K, KUOSMANEN P, ASTOLA J. Boolean derivatives, weighted chow parpmeters, and selection probabilities of stack filters[J]. *IEEE Transactions on Signal Processing*, 1996, 44(7): 1341 – 1634.

[44] BOCHMANN D. *Boolean Differential Calculus*[M]. Karl Marx Stadt: German Democratic Pepublic, 1978.

[45] VICHNIAC G Y. Boolean derivatives on cellular automata[J]. *Physica D*, 1990, 45(1/3): 63 – 74.

[46] 王树和. 数学聊斋[M]. 北京: 科学出版社, 2008.
(WANG Shuhe. *Mathematics Stories*[M]. Beijing: Science Press, 2008.)

作者简介:

程代展　(1946—), 男, 研究员, 博士生导师, 主要研究方向为非线性控制系统、切换系统、Hamiltonian系统、逻辑动态系统以及控制设计的数值实现, E-mail: dcheng@iss.ac.cn;

赵　寅　(1986—-), 男, 博士研究生, 主要研究方向为复杂系统、逻辑动态系统及博弈论, E-mail: zhaoyin@amss.ac.cn;

徐相如　(1987—), 男, 博士研究生, 主要研究方向为逻辑动态系统、多智能体, E-mail: xuxiangru@amss.ac.cn.