布尔函数与e-导数及其在密码学中的应用

王 卓 黄景廉 著

科学出版社

布尔函数与 e-导数及其在密码学中的应用

王 卓 黄景廉 著



科学出版社
北京

内 容 简 介

本书主要内容有：布尔函数的e-导数的概念和性质、布尔导数的概念和性质，方程和布尔积分的概念和解法，e-导数和导数在解布尔微分方程中的应用，e-导数和导数在解布尔方程和布尔方程组中的应用，e-导数在逻辑电路检测中的应用，向量布尔函数与偏导数、偏e-导数，e-导数和导数在函数2-分解中的应用，e-导数和导数的谱性质，布尔函数最低代数次数零化子与e-导数、导数的关系，利用e-导数和导数构造最优代数免疫函数，通过解微分方程求最低代数次数零化子，代数免疫性与非线性度的线性函数关系，Bent函数的2-分解性，变量的P变换与Bent函数的不变性，2n元最优代数免疫Bent函数的构造，变量的P变换与代数免疫阶的不变性，e-导数和导数与平衡H布尔函数的最高相关免疫阶，H布尔函数相关免疫阶的e-导数和导数判定公式，平衡H布尔函数的最大相关度和最小相关度的e-导数、导数求解，2-分解H布尔函数的代数免疫性，2次齐次完全旋转对称布尔函数的矩阵和相关免疫性，偶数元和奇数元2次齐次完全旋转对称布尔函数的重量与非线性度的不同关系及高次非线性度，偶数元和奇数元的一类2次齐次旋转对称布尔函数的重量与非线性度的关系与高次非线性度，内容中的很多问题都是用传统方法难以解决的重要问题，但通过e-导数、导数推演方法就能够顺利解决.

本书适合高等院校相关专业本科生、研究生用作教材或参考书，也适合高等院校有关专业教师、社会各界相关专业科研人员和科技工作者作参考书籍.

图书在版编目(CIP)数据

布尔函数与e-导数及其在密码学中的应用/王卓，黄景廉 著. —北京：科学出版社，2019.11

ISBN 978-7-03-062797-1

Ⅰ.①布… Ⅱ.①王… ②黄… Ⅲ.①布尔函数—应用—密码学—研究 ②导数—应用—密码学—研究 Ⅳ.①TN918.1

中国版本图书馆CIP数据核字（2019）第240285号

责任编辑：李 欣 李香叶/责任校对：彭珍珍

责任印制：吴兆东/封面设计：陈 敬

科学出版社 出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

北京中石油彩色印刷有限责任公司 印刷

科学出版社发行 各地新华书店经销

*

2019年11月第 一 版 开本：720×1000 1/16

2019年11月第一次印刷 印张：32 1/2

字数：650 000

定价：198.00 元

（如有印装质量问题，我社负责调换）

前　言

在布尔函数的理论和应用中, 从来都只有并不为人熟知的布尔函数的导数 (或称布尔差分) 的概念. 布尔函数密码安全性质研究中也几乎没有用到布尔导数. 但我们在研究布尔函数密码安全性质时发现, 布尔函数密码安全性质依赖于布尔函数自身的结构, 自然与布尔导数有一定的关联. 不过, 导数只能反映布尔函数的部分结构, 而不能反映布尔函数的另一部分结构, 这应该是导数不能在布尔函数密码安全性质研究中发挥作用并得到应用的根本原因, 也是导数在布尔函数理论和其他领域的应用中都得不到发展的原因. 我们定义了 e-导数来反映布尔函数的另一部分结构, 将 e-导数和导数结合以完整反映布尔函数的整体结构, 便能用于研究工作. e-导数的计算与差分的计算差异很大, 所以是不能称为 e-差分的, 只能称为 e-导数, 相应地, 也不可将导数称为差分, 只能因为 e-导数而使用导数这个名称.

我们将 e-导数和导数结合, 用来研究布尔函数的密码安全性质, 取得了很好的系列性成果. 将 e-导数和导数结合, 用到逻辑线路检测、布尔方程、布尔微分方程、布尔函数 2-分解等领域, 也得到很多有意义的成果. 将这些系列研究成果整理出来, 与 e-导数、导数研究方法一起, 汇集成本书.

e-导数的定义, 源自对布尔函数密码安全性质的研究, 自然, 本书就以布尔函数密码安全性质研究内容为主, 以布尔积分、布尔微分方程、布尔方程、逻辑线路检测、布尔函数 2-分解等领域的研究内容为辅写成. 通过导数、e-导数以求得布尔函数很多难以求得的密码安全性质, 这与实数域上连续函数微分方程稳定性理论和定性分析理论的分析很相似, 而布尔函数密码安全性质中的很多性质, 其实也是布尔函数理论中函数应该具有的性质, 如重量、代数次数、旋转对称、齐次函数、平衡性、与线性函数的关系、与布尔微分方程的关系等. 所以, 本书的内容, 大多既有实践的品格, 又有理论的品格, 而 e-导数和导数本身, 自然也既有实践的品格, 又有理论的品格.

全书共 11 章, 一个附录. 第 1 章布尔函数基本知识, 主要是要为后面 2-分解的例题服务, 第 2 章导数、e-导数的概念和性质, 既补充布尔函数理论中的不足, 又为后面各章提供工具, 其余 9 章对各研究领域中未解决的重要问题, 利用导数、e-导数给予解决, 如布尔方程的导数、e-导数求解算法, 解决了布尔方程难求解的问题; 又如布尔函数最低代数次数零化子的解微分方程的求解算法, 解决了迄今尚无求最低代数次数零化子的通用方法的问题; 又如用求导数和 e-导数的方

法, 解决了 2 次齐次的完全旋转对称、旋转对称布尔函数中偶数元和奇数元函数各自的重量与非线性度相等和不相等两种关系的问题, 并求得接近布尔函数非线性度最大值的非线性度等. 更多的这一类内容读者自会从书中看到, 这里不再一一赘述.

本书得到国家自然科学基金 (项目编号: 61262085) 资助, 谨表示感谢!

本书难免存在疏漏或不足之处, 切盼方家批评指正.

王　卓　黄景廉

2018 年 11 月

目　录

第一篇　布尔函数的导数、e-导数基础

第 1 章　布尔函数 **3**

1.1　$GF(2)$ 上的布尔函数 3

1.2　布尔函数的表示 4

1.2.1　真值表 (表示) 4

1.2.2　小项 (表示) 5

1.2.3　多项式 (表示) 5

1.3　布尔函数的距离和重量 6

第 2 章　布尔函数的导数和 e-导数 **8**

2.1　布尔函数的导数 8

2.1.1　布尔函数对单个变元的导数 8

2.1.2　布尔函数与变元的无关性和布尔函数的展开式 11

2.1.3　布尔函数对多个变元的导数 13

2.2　布尔函数的 e-导数 17

2.2.1　布尔函数的 e-导数的概念和性质 18

2.2.2　布尔函数的 e-导数和导数的基本关系 24

2.2.3　布尔函数的平衡性 27

第 3 章　布尔积分和布尔微分方程 **38**

3.1　布尔积分 38

3.2　e-导数在解布尔微分方程中的应用 43

3.3　与导数有关的布尔微分方程 46

3.4　导数、e-导数与布尔方程的解法 49

第 4 章　e-导数微分方程在逻辑电路检测中的应用 **66**

4.1　e-导数微分方程在逻辑电路检测中的应用 66

4.2　微分方程线路检测实例 68

4.3　e-导数与线路检测的说明 76

第 5 章　向量布尔函数、偏导数、偏 E-导数 …… 80
5.1　布尔向量和布尔矩阵 …… 80
5.2　布尔向量的广义求补运算和转置运算 …… 84
5.3　广义求补变换和转置变换下布尔函数一些性质的不变性 …… 89
5.4　向量布尔函数 …… 97
5.5　向量布尔函数的偏导数和偏 E-导数 …… 100
5.6　布尔函数的 2-分解 …… 106

第二篇　导数、e-导数与布尔函数的密码安全性质

第 6 章　布尔函数的 Walsh 谱与布尔函数的导数、e-导数 …… 127
6.1　对称密码与布尔函数 …… 127
6.2　布尔函数的 Walsh 谱 …… 130
6.3　布尔函数的导数、e-导数与 Walsh 谱 …… 133
6.4　布尔函数的非线性性 …… 140
6.5　布尔函数的严格雪崩准则和扩散性的概念 …… 147
6.6　布尔函数的相关免疫性与 Walsh 谱 …… 153
第 7 章　布尔函数的代数免疫性 …… 156
7.1　代数攻击和布尔函数的代数免疫性 …… 156
7.2　最低代数次数零化子和导数、e-导数 …… 159
7.3　导数、e-导数与最优代数免疫函数 …… 190
第 8 章　几种密码学性质的相关联性与导数、e-导数 …… 201
8.1　最低代数次数零化子的微分方程解 …… 201
8.2　布尔函数的代数免疫性与非线性度 …… 210
第 9 章　Bent 函数与导数、e-导数 …… 233
9.1　Bent 函数的导数、e-导数 …… 233
9.2　Bent 函数的代数免疫性和最优代数免疫 Bent 函数 …… 251
第 10 章　H 布尔函数与其导数、e-导数 …… 289
10.1　H 布尔函数与导数、e-导数 …… 289
10.2　平衡 H 布尔函数与导数、e-导数 …… 308
10.3　H 布尔函数的相关免疫性 …… 317
10.4　平衡 H 布尔函数的 m 阶相关度 ε_m …… 348

10.5　H 布尔函数的代数免疫性……365
10.6　2-分解 H 布尔函数的代数免疫性……368
第 11 章　旋转对称布尔函数与其导数、e-导数……377
11.1　基本概念和基本定理……377
11.2　2 次齐次完全旋转对称布尔函数的矩阵表示和相关免疫性……383
11.3　完全旋转对称布尔函数的代数免疫性……411
11.4　二类齐次完全旋转对称布尔函数的非线性度……429
11.5　一类 2 次齐次旋转对称布尔函数……457
参考文献……494
附录　椭圆曲线和费马大定理……502

第一篇　布尔函数的导数、e-导数基础

$GF(2)$ 上的布尔函数在密码设计和安全性研究中有重要作用. 由布尔函数密码安全性质研究的需要, 产生了布尔函数的 e-导数这一数学概念. 将 e-导数和布尔函数基础理论中原来已有的导数一起作为研究工具, 对布尔函数密码安全性质的研究能起到有益的作用. 随着 e-导数这一新概念的产生, 自然也产生了一些和 e-导数有关的布尔函数基础理论和应用的相关知识, 如含 e-导数的布尔微分方程及其解法、逻辑电路 e-导数误差检测方法、e-导数和 2-分解等. 布尔函数的 e-导数和伴随它而产生的一些新的知识, 对布尔函数密码安全性质的研究是有用的, 在逻辑电路误差检测中是必须具备的, 在布尔函数的一些应用, 如解布尔方程中是需要的. 同时, 布尔函数的 e-导数及其新知识, 也充实了布尔函数基础理论的内容. 本篇将介绍 e-导数、导数及与之相关的布尔函数基本理论知识.

第 1 章　布尔函数

1.1　$GF(2)$ 上的布尔函数

布尔函数是布尔代数 $\langle S, \oplus, \otimes, -, 0, 1\rangle$ 上的常量、变量由运算“$\oplus$”(或运算)、“$\otimes$”(与运算)、“$-$”(非运算) 连接起来的布尔表达式. 布尔代数上的运算“$\oplus$”“$\otimes$”“$-$”和 $GF(2)$ 上的运算“$+$”“$\cdot$”有如下关系：

$$x_1 \otimes x_2 = x_1 \cdot x_2 \text{ (在不会引起混淆的情况下, } x_1 \cdot x_2 \text{ 可写为 } x_1x_2), \tag{1.1.1}$$

$$x_1 \oplus x_2 = x_1 + x_2 + x_1x_2, \tag{1.1.2}$$

$$\overline{x}_1 = 1 + x_1. \tag{1.1.3}$$

由于有 $\overline{x}_1 = 1 + x_2$ 这样的运算关系, 所以在 $GF(2)$ 上的布尔函数的运算中, 有时为方便表示, 也可以使用“$\overline{x_1}$”这样的非运算表示.

布尔函数是布尔代数中的布尔表达式, 而布尔代数中的运算“$\oplus$”“$\otimes$”“$-$”, 可以用 $GF(2)$ 上的表达式 (1.1.1)、(1.1.2)、(1.1.3) 表示, 所以可在 $GF(2)$ 上定义布尔函数.

布尔代数中, 常用基于数学归纳法的定义方法来定义函数. 方法是：先规定某些初始项, 然后给出从已知的值求后续值的规则. 这样的定义称为递归定义或归纳定义. 定义 1.1.1 给出递归定义的具体描述.

定义 1.1.1　令 $R : N \times D \to D$, 对 $n \in N$, $c \in D$, 若 $f : N \to D$ 满足：

(1) $f(0) = c$;

(2) $f(n+1) = R(n, f(n))(n \geqslant 0)$,

则称 f 是由 (1), (2) 规则定义的函数. 称 (1) 为定义的基础步, (2) 步为递归 (或归纳) 步.

有了递归定义的概念, 现在可以用递归定义方法来定义 $GF(2)$ 上的布尔函数.

定义 1.1.2　令 $x_1, x_2, \cdots, x_n$ 是 $GF(2)$ 上的布尔变量, c 是 $GF(2)$ 上的布尔常量. 映射 $f(x_1, x_2, \cdots, x_n) : GF(2)^n \to GF(2)$ 若按下述递归定义构成, 则为 $GF(2)$ 上的布尔函数：

1. (基础步):

$f(x_1, x_2, \cdots, x_n) = c$ 是布尔函数, 称为常函数；$f(x_1, x_2, \cdots, x_n) = x_i (i = 1, 2, \cdots, n)$ 是布尔函数, 称为投影函数.

2. (归纳步):

若 $f(x_1,x_2,\cdots,x_n)$ 是布尔函数, 则 $1+f(x_1,x_2,\cdots,x_n)$(也可以记为补的形式 $\overline{f(x_1,x_2,\cdots,x_n)}$) 也是布尔函数; 若 $f_1(x_1,x_2,\cdots,x_n)$ 和 $f_2(x_1,x_2,\cdots,x_n)$ 是布尔函数, 则 $f_1(x_1,x_2,\cdots,x_n)+f_2(x_1,x_2,\cdots,x_n)$ 和 $f_1(x_1,x_2,\cdots,x_n)\cdot f_2(x_1,x_2,\cdots,x_n)$ 也都是布尔函数.

对 $GF(2)$ 上的 n 维布尔函数 f, 自然也可以记为 $f\in GF(2)^{GF(2)^n}$. 为方便起见, 也常将 $(x_1,x_2,\cdots,x_n)$ 记为 x, 将 $f(x_1,x_2,\cdots,x_n)$ 记为 $f(x)$.

本书描述和讨论的函数, 都是 $GF(2)$ 上的函数. 所讨论的 e-导数、导数等, 都是对 $GF(2)$ 上的布尔函数的 e-导数、导数等进行的, 所以运用的运算 "+" "·", 自然是 $GF(2)$ 上的运算. 但书中也常常会碰到实数域上的 "+" "·" 运算, 如常常要对布尔函数的汉明 (Hamming) 重量这一实数值进行运算. 由于对 $GF(2)$ 上布尔函数的运算和在实数域上的运算, 运算对象和运算意义完全不同, 对这两种运算的相同运算符的不同意义容易区分. 因此, 书中将不加说明地对两种运算的相应 "加" "乘" 运算一律使用相同的运算符 "+" "·".

1.2　布尔函数的表示

$GF(2)$ 上的布尔函数有多种不同的表示方式. 在布尔函数的理论分析和应用上, 不同的表示方式有各自的使用方便之处和优点. 本节先介绍真值表 (表示)、小项 (表示)、多项式 (表示) 等最基本的表示方式.

1.2.1　真值表 (表示)

在 $GF(2)$ 上的布尔函数 $f(x)$, $\mathrm{dom}(f)=GF(2)^n$ 和 $\mathrm{ran}(f)=GF(2)$ 都是有限集, 因而可以用列表法表示.

将 $GF(2)^n$ 上的向量 $(x_1,x_2,\cdots,x_n)$ 看成 n 位的二进制数, 按从小到大的顺序排列, 并相应地与 $0\sim 2^n-1$ 这 2^n 个整数一一对应转换, 则依次表示出函数值 $f(0),f(1),f(2),\cdots,f(2^n-1)$. 将这些函数值依次作为 2^n 维向量的 2^n 个分量, 所得向量

$$(f(0),\ f(1),\ f(2),\ \cdots,\ f(2^n-1))^{\mathrm{T}} \tag{1.2.1}$$

称为 $f(x)$ 的真值 (表), 记为 $\vec{f}$. 将 $\vec{f}$ 列成表, 即得真值表. 对分量取布尔值 0, 1 的布尔向量 α, 称 α 中分量 "1" 的个数为 α 的 Hamming 重量 (简称重量), 记为 $w_t(\alpha)$. 将布尔向量 $\vec{f}$ 的 Hamming 重量称为布尔函数 $f(x)$ 的 Hamming 重量 (简称重量), 记为 $w_t(f(x))$ 或 $w_t(f)$. 所以也有 $w_t(f(x))=|\{x\,|x\in GF(2)^n, f(x)=1\}|$.

若 $w_t(f(x))=2^{n-1}$, 则称 $f(x)$ 是平衡布尔函数.

有了布尔函数的真值表, 就一定能得出布尔函数的解析表达式. 该表达式对研究、分析布尔函数的性质是重要的.

1.2.2 小项 (表示)

对 $x_i, c_i \in GF(2)(i=1,2,\cdots,n)$, 规定

$$x_i^1 = x_i, \quad x_i^0 = 1 + x_i.$$

于是

$$x_i^{c_i} = \begin{cases} 1, & x_i = c_i, \\ 0, & x_i \neq c_i. \end{cases}$$

对 $x=(x_1,x_2,\cdots,x_n) \in GF(2)^n$ 和 $c=(c_1,c_2,\cdots,c_n) \in GF(2)^n$, 定义

$$x_i^c = \prod_{i=1}^{n} x_i^{c_i} = \begin{cases} 1, & x = c, \\ 0, & x \neq c. \end{cases}$$

于是

$$f(x) = \sum_{c=0}^{2^n-1} f(c)x^c, \tag{1.2.2}$$

称布尔表达式 x^c 为小项, (1.2.2) 式为 $f(x)$ 的小项表示. (1.2.2) 式中的符号 "$\sum$" 表示 $GF(2)$ 上的 "和". 要说明的是, 书中以后要用到实数域上的连和时, 也仍用符号 "$\sum$" 来表示. 二者是容易区分的.

1.2.3 多项式 (表示)

由 $x_i^1 = x_i$, $x_i^0 = 1 + x_i$, 在 (1.2.2) 式中以 x_i 代 x_i^1, $1+x_i$ 代 x_i^0, 则 $f(x)$ 可展开得到 $GF(2)^n$ 上的多项式

$$\begin{aligned} f(x) &= a_0 + a_1x_1 + a_2x_2 + \cdots + a_nx_n + a_{12}x_1x_2 + \cdots \\ &\quad + a_{n-1,n}x_{n-1}x_n + \cdots + a_{12\cdots n}x_1x_2\cdots x_n \\ &= a_0 + \sum_{k=1}^{n} \sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n} a_{i_1i_2\cdots i_k}x_{i_1}x_{i_2}\cdots x_{i_k}, \end{aligned} \tag{1.2.3}$$

(1.2.3) 式称为 $f(x)$ 的代数标准形或正规形.

从 $f(x)$ 的代数标准形 (1.2.3) 式和 $f(x)$ 的小项表示 (1.2.2) 式可以看出, 从 $f(x)$ 的小项表示 (1.2.2) 式转化为 $f(x)$ 的代数标准形, 可以用以下可编程的算法实现.

令 $f_0 = f(0,0,\cdots,0)$, $f_{i_1 i_2 \cdots i_k} = f(0,\cdots,\underset{\substack{\downarrow \\ i_1\text{位}}}{1},\cdots,\underset{\substack{\downarrow \\ i_k\text{位}}}{1},\cdots,0)$.

(1) 令 $a_0 \leftarrow f_0$;

(2) 令 $k \leftarrow 1$;

(3) 对所有 $1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n$, 令

$$a_{i_1 i_2 \cdots i_k} \leftarrow f_0 + \sum_{l=1}^{k} \sum_{1 \leqslant j_1 < j_2 < \cdots < j_l \leqslant k} f_{i_{j_1}} x_{i_{j_2}} \cdots x_{i_{j_l}};$$

(4) 若 $k = n \to \Omega$;

(5) 令 $k \leftarrow k+1$, 转 (3).

由已知的 (1.2.2) 式按算法求出 (1.2.3) 式的所有系数 $a_0, a_1, a_2, \cdots, a_{12\cdots n}$, 便得到代数标准形 (1.2.3). 自然, 这个算法可以用归纳法来证明, 这里不再赘述.

根据代数标准形 (1.2.3), 定义布尔函数的代数次数为 $\max\{k \,|\, a_{i_1 i_2 \cdots i_k} \neq 0\}$, 记为 $\deg(f)$. 若 $f(x) = c$ (常数), 则定义 $\deg(f) = 0$. 若 $\deg(f) = 1$, 则称 $f(x)$ 为仿射函数. 当 $a_0 = 0$, $\deg(f) = 1$ 时, 称 $f(x)$ 为线性函数. 也常常不严格区分地将仿射函数称为线性函数. 当 $\deg(f) \geqslant 2$ 时, 称 $f(x)$ 为非线性函数.

1.3　布尔函数的距离和重量

在 1.2.1 节中已定义了布尔函数的重量. 对两个布尔函数 $f(x) = f(x_1, x_2, \cdots, x_n)$ 和 $g(x) = g(x_1, x_2, \cdots, x_n)$, 记 $f(x)$ 和 $g(x)$ 的距离为 $d(f,g)$, 并定义为

$$d(f,g) = w_t(f(x) + g(x)). \tag{1.3.1}$$

两个函数 $f(x)$, $g(x)$ 之和的重量有关系:

$$w_t(f(x) + g(x)) = w_t(f(x)) + w_t(g(x)) - 2w_t(f(x)g(x)). \tag{1.3.2}$$

用归纳法可以证明, 任意 m 个函数 $f_1(x)$, $f_2(x)$, $\cdots$, $f_m(x)$ 的和的重量有关系:

$$w_t\left(\sum_{i=1}^{m} f_i(x)\right) = \sum_{k=1}^{m} \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant m} (-2)^{k-1} w_t(f_{i_1} f_{i_2} \cdots f_{i_k}). \tag{1.3.3}$$

n 维布尔向量 $\omega = (\omega_1, \omega_2, \cdots, \omega_n) \in GF(2)^n$, 有如下性质.

定理 1.3.1 对 n 维布尔向量 $\omega=(\omega_1,\omega_2,\cdots,\omega_n)\in GF(2)^n$, 有

$$\sum_{x\in GF(2)^n}(-1)^{\sum\limits_{i=1}^{n}\omega_i x_i}=\begin{cases}2^n, & \omega=0,\\ 0, & \omega\neq 0\end{cases}\quad (\text{其中 } x=(x_1,x_2,\cdots,x_n)\in GF(2)^n).$$

定理 1.3.1 是易证的. 因为 $\omega\neq 0$ 时, $x\in GF(2)^n$ 共取 2^n 个值, 故 $\sum\limits_{i=1}^{n}\omega_i x_i=0$ 和 $\sum\limits_{i=1}^{n}\omega_i x_i=1$ 各有 2^{n-1} 个, 故性质成立. 而 $\omega=0$ 时, 是显然的.

对 $GF(2)$ 上的两个布尔函数 $f(x)$, $g(x)$ 的和, 还有如下的定理.

定理 1.3.2 对 $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$, $g(x)=g(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$, 有

$$(1)\ f(x)+g(x)=f(x)\overline{g(x)}+\overline{f(x)}g(x); \tag{1.3.4}$$

$$(2)\ w_t(f(x)+g(x))=w_t(f(x)\overline{g(x)})+w_t(\overline{f(x)}g(x)). \tag{1.3.5}$$

分 $f(x)=g(x)$ 和 $f(x)\neq g(x)$ 两种情况来讨论, 则 (1.3.4) 式显然成立. 由 (1.3.4) 式和 (1.3.2) 式, 显然 (1.3.5) 式也成立.

第 2 章　布尔函数的导数和 e-导数

2.1　布尔函数的导数

2.1.1　布尔函数对单个变元的导数

布尔函数对单个变元的导数和布尔函数对 2 个以上变元的导数, 可以按对多个变元的导数一起给出定义. 但因实际使用时各有用途, 这里分开定义. 首先定义布尔函数对单个变元的导数.

定义 2.1.1　设 $f \in GF(2)^{GF(2)^n}$.

(1) $f(x) = f(x_1, x_2, \cdots, x_n)$ 关于任意变元 x_i 的导数定义为

$$\begin{aligned}\frac{df(x)}{dx_i} &= f(x_1, x_2, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots, x_n) \\ &\quad + f(x_1, x_2, \cdots, x_{i-1}, \overline{x_i}, x_{i+1}, \cdots, x_n) \quad (i = 1, 2, \cdots, n),\end{aligned} \tag{2.1.1}$$

$\dfrac{df(x)}{dx_i}$ 称为 $f(x)$ 关于 $x_i (i = 1, 2, \cdots, n)$ 的导数.

为书写方便, (2.1.1) 式可写为 $df(x)/dx_i$. 但为清晰起见, 还是以正规书写方式 $\dfrac{df(x)}{dx_i}$ 为好.

(2) $f(x_1, x_2, \cdots, x_n)$ 关于 $x_{i_1}, x_{i_2}, \cdots, x_{i_k}$ 的高阶布尔导数定义为

$$\begin{aligned}\frac{d^k f(x)}{dx_{i_1} dx_{i_2} \cdots dx_{i_k}} &= \frac{d}{dx_{i_1}} \left(\frac{d}{dx_{i_2}} \left(\cdots \left(\frac{df(x)}{dx_{i_k}} \right) \right) \right) \\ &\quad (i_1, i_2, \cdots, \ i_k \in \{1, 2, \cdots, n\}, \ i_1 \neq i_2 \neq \cdots \neq i_k).\end{aligned} \tag{2.1.2}$$

下面讨论 $f(x_1, x_2, \cdots, x_n)$ 的导数的性质.

性质 1　$\dfrac{dc}{dx_i} = 0 (c = \text{const})$.

性质 2　当 $f(x)$ 的最高次项含有变元 x_i 时, 有

$$\deg \left(\frac{df(x)}{dx_i} \right) = \deg(f(x)) - 1.$$

这一性质由导数的定义即可证明, 或由 (2.1.10) 式, 可看出显然成立.

性质 3　$\dfrac{dx_i}{dx_i} = 1$.

性质 4 $\dfrac{d(cf(x))}{dx_i} = c\dfrac{d(f(x))}{dx_i}$ $(c = \text{const})$.

性质 5 $\dfrac{d\overline{f(x)}}{dx_i} = \dfrac{df(x)}{dx_i}$.

证明

$$\begin{aligned}\frac{d\overline{f(x)}}{dx_i} &= \overline{f(x_1, x_2, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots, x_n)} + \overline{f(x_1, x_2, \cdots, x_{i-1}, \overline{x_i}, x_{i+1}, \cdots, x_n)} \\ &= (1 + f(x_1, x_2, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots, x_n)) \\ &\quad + (1 + f(x_1, x_2, \cdots, x_{i-1}, \overline{x_i}, x_{i+1}, \cdots, x_n)) \\ &= \frac{df(x)}{dx_i}.\end{aligned}$$

性质 6 $\dfrac{d\overline{x_i}}{dx_i} = 1$.

性质 7 $\dfrac{dx_i}{d\overline{x_i}} = 1$.

利用性质 5, 有 $\dfrac{dx_i}{d\overline{x_i}} = \dfrac{d\overline{x_i}}{d\overline{x_i}} = 1$.

性质 8 $\dfrac{d}{dx_i}\left(\dfrac{df(x)}{dx_j}\right) = \dfrac{d}{dx_j}\left(\dfrac{df(x)}{dx_i}\right)$, 即 $\dfrac{d^2 f(x)}{dx_i dx_j} = \dfrac{d^2 f(x)}{dx_j dx_i}$.

性质 8 按导数的定义直接展开计算即可证明.

性质 9 $\dfrac{d(f(x)g(x))}{dx_i} = f(x)\dfrac{dg(x)}{dx_i} + g(x)\dfrac{df(x)}{dx_i} + \dfrac{df(x)}{dx_i}\dfrac{dg(x)}{dx_i}$.

证明

$$\begin{aligned}&\frac{d(f(x)g(x))}{dx_i} \\ &= f(x_1, x_2, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots, x_n)g(x_1, x_2, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots, x_n) \\ &\quad + f(x_1, x_2, \cdots, x_{i-1}, \overline{x_i}, x_{i+1}, \cdots, x_n)g(x_1, x_2, \cdots, x_{i-1}, \overline{x_i}, x_{i+1}, \cdots, x_n) \\ &= f(x_1, x_2, \cdots, x_{i-1}, \overline{x_i}, x_{i+1}, \cdots, x_n)g(x_1, x_2, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots, x_n) \\ &\quad + f(x_1, x_2, \cdots, x_{i-1}, \overline{x_i}, x_{i+1}, \cdots, x_n)g(x_1, x_2, \cdots, x_{i-1}, \overline{x_i}, x_{i+1}, \cdots, x_n) \\ &\quad + g(x_1, x_2, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots, x_n)f(x_1, x_2, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots, x_n) \\ &\quad + g(x_1, x_2, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots, x_n)f(x_1, x_2, \cdots, x_{i-1}, \overline{x_i}, x_{i+1}, \cdots, x_n)\end{aligned}$$