第 20 卷 第 6 期 电 子 科 学 学 刊 Vol.20 No.6
1998 年 11 月 JOURNAL OF ELECTRONICS Nov. 1998

3-值逻辑函数的稳定性 [1]

李世取 赵亚群 俞嘉恩

(郑州信息工程学院应用数学系 郑州 450002)

摘 要 本文提出了 3-值逻辑函数稳定性的概念，考察了“稳定”的概率定义，给出了 3-值逻辑函数稳定的判别条件，提供了构造稳定的 3-值逻辑函数的典型方法，用本文的方法，也可考察一般 P-值逻辑函数的稳定性.

关键词 3-值逻辑函数，稳定性，Chrestenson 循环谱，概率空间

中图号 TN918.1

1 引 言

在密码学中，对布尔函数的两种重要特性——相关免疫性和稳定性的研究已经持续了一个时期 [1,2]. 近年来，人们对布尔函数 (2-值逻辑函数) 的稳定性和多值逻辑函数的相关免疫性及谱特征给予了更多的关注 [3-6]，但多值逻辑函数的稳定性问题尚未见公开讨论. 布尔函数的稳定性概念是丁存生博士等 1987 年提出的 [1]，后来发现稳定的布尔函数即 Rothaus 定义的 Bent 函数 [7]. Bent 函数是较为理想的非线性滤波和非线性组合函数，有密码学价值. 其原因之一是任一 n 元 Bent 函数 $f(x)$ 与任一仿射函数 $w\cdot x+i$ 的符合率，即概率 $P(f(X)=w\cdot X+i)$ 满足 $|P(f(X)=w\cdot X)-1/2|=1/2\times 2^{n/2}$，而这一特性与 $f(x)$ 的 Walsh 谱 $S_{(f)}(w)$ 满足 $|S_{(f)}(w)|=1/2^{n/2}$ 是等价的. 在 $P=3$ 时，我们通过研究 $|S_{(f)}(w)|=1/3^{n/2}$ 时 $S_{(f)}(w)$ 的取值，与研究布尔函数的稳定性一样，用谱和概率的特性完美地刻划了 3-值逻辑函数的稳定性. 我们的研究表明，稳定的 3-值逻辑函数也是有密码学价值的.

2 预备知识

2.1 Chrestenson 谱 [1] 的概率表示

设 Z 为整数环，记 Z_3 为整数模 3 的剩余类环 (域)，且记 $G(3)\triangleq Z_3$，Z_3^n 为 n 个环 Z_3 的直和 [8]. 简称定义在某一概率空间 (Ω,F,P)[9] 上且取值于 $G(3)$ 的随机变量 X_k 为 3-值随机变量. 若 $P(X_k=i)=1/3$，$i\in G(3)$，则称 X_k 具有对称分布. 规定 3-值随机变量及 $G(3)$ 中元素间的运算都在环 Z_3 中进行.

定义 1 称 Z_3^n 到 $G(3)$ 的任一映射 f 为 3-值逻辑函数. 记 $L(Z_3^n)=\{f(x), f(x)$ 为 3-值逻辑函数 $\}$.

定义 2 设 $\Omega=Z_3^n$，F 为 Ω 的全体子集构成的 σ 代数，(Ω,F) 上的概率测度 P 满足 $P((x_1,\cdots,x_n))=1/3^n$, $(x_1,\cdots,x_n)\in\Omega$, 则 (Ω,F,P) 是一概率空间. 在此概率空间上定义

$$X_k(x_1,\cdots,x_n)=x_k,\quad 1\le k\le n,\quad (x_1,\cdots,x_n)\in\Omega.$$

易知 $X_1,X_2,\cdots,X_n$ 是 (Ω,F,P) 上的相互独立且具有对称分布的 3-值随机变量. 若记 $w\in Z_3^n$ 在加法群 Z_3^n 中的负元为 w^*, $X=(X_1,\cdots,X_n)$, 则 $\forall f(x_1,\cdots,x_n)\in L(Z_3^n)$ 都有 [5]

[1] 1997-02-04 收到，1998-03-23 定稿

$$S_f(w)=\sum_{i=0}^{2}\sum_{j=0}^{2}iu^jP(f(X)=i,w^*\cdot X=j), \tag{1}$$

$$S_{(f)}(w)=\sum_{k=0}^{2}u^kP(f(X)+w^*\cdot X=k), \tag{2}$$

$$=\sum_{i=0}^{2}\sum_{j=0}^{2}u^{i+j}P(f(X)=i,w^*\cdot X=j). \tag{3}$$

2.2 两个引理

引理 1　设 α,β 为有理数，$\alpha=k/3^n$, $\beta=l/3^m$, k,l,m,n 为整数 $m,n\geq 0$, 且 $\alpha^2+\beta^2-\alpha\beta=1$ 则 α、β 取值必为下述四种情况之一：$\alpha=\pm1,\beta=0$; $\alpha=0,\beta=\pm1$; $\alpha=\beta=1$; $\alpha=\beta=-1$;

证明　由数论知识即可得证.

引理 2　设 n 是任一正偶数，$f(x)\in L(Z_3^n)$，则 $|S_{(f)}(w)|=1/3^{n/2}$ 的充要条件是 $S_{(f)}(w)\in\{\pm1/3^{n/2},\pm u/3^{n/2},\pm u^2/3^{n/2}\}$

证明　由 $|u|=|u^2|=1$，充分性显然. 必要性由 (2) 式和引理 1 即得.

3　3-值逻辑函数稳定性的定义及概率判别条件

以下总设 n 是正偶数.

定义 3　设 $f(x)\in L(Z_3^n)$，若对任一 $w\in Z_3^n$，都有 $|S_{(f)}(w)|=1/3^{n/2}$，则称 $f(x)$ 是稳定的.

由文献 [1] 可知，布尔函数稳定的充要条件是 $|P(f(X)=w\cdot X)-1/2|=(1/2)\times(1/2^{n/2})$ 对任一 $w\in GF^n(2)$.

对于 3-值逻辑函数，我们也有如下相应的判别条件.

定理 1　设 $f(x)\in L(Z_3^n)$，$X=(X_1,\cdots,X_n)$ 定义如前，则 $f(x)$ 稳定的充要条件是对任一 $w\in Z_3^n$，概率 $P(f(X)=w\cdot X)$、$P(f(X)=w\cdot X+1)$、$P(f(X)=w\cdot X+2)$ 中有且仅有一个为 $1/3\pm(1/3)\times(2/3^{n/2})$，其余两个皆为 $1/3\mp(1/3)\times(1/3^{n/2})$.

证明　*充分性*　由 (2) 式并注意 $1+u+u^2=0$ 即得.

必要性　设 $f(x)$ 是稳定的，则对任一 $w\in Z_3^n$，都有 $|S_{(f)}(w)|=1/3^{n/2}$，据引理 2 知必有 $S_{(f)}(w)\in\{\pm1/3^{n/2},\pm u/3^{n/2},\pm u^2/3^{n/2}\}$.

若有

$$\pm1/3^{n/2}=S_{(f)}(w)=P(f(X)=w\cdot X)+P(f(X)=w\cdot X+1)u+P(f(X)=w\cdot X+2)u^2,$$

则据文献 [6] 中引理 2 及概率性质可知

$$P(f(X)=w\cdot X)\mp1/3^{n/2}=P(f(X)=w\cdot X+1)=P(f(X)=w\cdot X+2),$$
$$P(f(X)=w\cdot X)=1/3\pm1/3\times2/3^{n/2},P(f(X)=w\cdot X+i)=1/3\mp1/3\times1/3^{n/2},i=1,2.$$

$S_{(f)}(w)=\pm u/3^{n/2}$ 及 $S_{(f)}(w)=\pm u^2/3^{n/2}$ 的相应结论同理可证.

下述定理 2 给出的概率判别条件对应文献 [1] 中定理 6.4.2 给出的布尔函数稳定的判别条件，但是，由于 3-值函数与布尔函数的差异，两个定理的证明方法也有较大不同.

定理 2 设 $f(x)\in L(Z_3^n)$，$X=(X_1,\cdots,X_n)$，定义如前，则 $f(x)$ 稳定的充要条件是对任一 $w^*\in Z_3^n$，$w^*\neq 0$ 都有

$$P(f(X))=f(X\oplus w^*)+j)=1/3,\quad j=0,1,2. \tag{7}$$

证明 记 $y=x\oplus w^*$, $g(x)=f(x\oplus w^*)$，则

$$S_{(2g)}(2w)=\frac{1}{3^n}\sum_{x\in Z_3^n}u^{2f(x\oplus w^*)-2w\cdot x}=u^{2w\cdot w^*}\overline{S_{(f)}(w)}. \tag{8}$$

必要性 若 $f(x)$ 是稳定的，则对任一 $w^*\in Z_3^n$，$w^*\neq 0$，据卷积公式 [1] 及 (8) 式知

$$S_{(f+2g)}(0)=\sum_{x\in Z_3^n}S_{(f)}(w)S_{(2g)}(2w)=\frac{1}{3^n}\overline{\sum_{x\in Z_3^n}u^{w\cdot w^*}}=0. \tag{9}$$

注意到

$$P(f(X)+2g(X)=0)+P(f(X)+2g(X)=1)u+P(f(X)+2g(X)=2)u^2=S_{(f+2g)}(0),$$

由 (9) 式，据文献 [6] 即知 $P(f(x)=f(X\oplus w^*)+j)=P(f(X)+2g(X)=j)=1/3, j=0,1,2.$

充分性 若对任一 $w^*\in Z_3^n$，$w^*\neq 0$ 都有 (7) 式成立，则必有

$$S_{(f+2g)}(0)=0.$$

再由卷积公式及 (8) 式即知

$$\sum_{w\in Z_3^n}|S_{(f)}(w)|^2\cdot u^{2w\cdot w^*}=0,\quad w^*\in Z_3^n,\quad w^*\neq 0. \tag{10}$$

注意到守恒定理 [1]：$\sum_{w\in Z_3^n}|S_{(f)}(w)|^2=1$, 由 (10) 式又有

$$1=\sum_{w^*\in Z_3^n}\sum_{w\in Z_3^n}|S_{(f)}(w)|^2\cdot u^{2w\cdot w^*}=3^n|S_{(f)}(0)|^2. \tag{11}$$

而对任一 $\nu\in Z_3^n$，$\nu\neq 0$，由 (10) 式还知，

$$\sum_{w\in Z_3^n}|S_{(f)}(w)|^2\cdot u^{2(w\oplus 2\nu)\cdot w^*}=0,\quad w^*\in Z_3^n,\quad w^*\neq 0,$$

故仍有

$$1=\sum_{w^*\in Z_3^n}\sum_{w\in Z_3^n}|S_{(f)}(w)|^2\cdot u^{2(w\oplus 2\nu)\cdot w^*}=3^n|S_{(f)}(\nu)|^2. \tag{12}$$

由 (11)、(12) 式可见，总有 $|S_{(f)}(\nu)|=1/3^{n/2}$, $\nu\in Z_3^n$, 因而 $f(x)$ 是稳定的.

4 稳定 3-值逻辑函数的存在性及构造

引理 3 设 $f(x)\in L(Z_3^n)$，则 $f(x)$ 稳定的充要条件是对任一 $w^*\in Z_3^n$，$f(x)+w^*\cdot x$ 都是稳定的.

证明 由 $P(f(X)+w^*\cdot X=w\cdot X)=P(f(X)=(2w^*\oplus w)\cdot X)$, 据定理 1 即得.

(1) 变元个数 $n=2$ 时，由定理 1 和定理 2 都容易验证 x_1x_2、$x_1^2+x_2^2$、$x_1^2+x_1x_2$ 都是稳定的，由引理 3 知 $x_1x_2+a_1x_1+a_2x_2$，$x_1^2+x_2^2+a_1x_1+a_2x_2$，$x_1^2+x_1x_2+a_1x_1+a_2x_2$ 都是稳定的，其中 $a_1,a_2\in G(3)$.

(2) 变元个数 $n\geq 4$ 时，根据 $n=2$ 时存在性的保证，下述定理保证了稳定的 3-值逻辑函数的存在性并提供了构造方法.

定理 3 设 $f_1(x)\in L(Z_3^n)$，$f_2(y)\in L(Z_3^n)$, 则 $f_1(x)+f_2(y)$ 是稳定的充要条件为 $f_1(x)$、$f_2(y)$ 都是稳定的.

证明 易知 $\forall w^{(1)}\in Z_3^n$，$w^{(2)}\in Z_3^m$ 都有

$$S_{(f_1+f_2)}(w^{(1)},w^{(2)})=S_{(f_1)}(w^{(1)})S_{(f_2)}(w^{(2)}) \tag{13}$$

由此立即证得充分性. 再据 (13) 式及守恒定理 [1] 又可得必要性.

注 用归纳法容易将上述定理 3 的结论推广至任意有限个 3-值逻辑函数的情形.

定理 4 设 $(x_1,\cdots,x_m,y_1,\cdots,y_m)\in Z_3^{2m}$，则 $\forall g(y_1,\cdots,y_m)\in L(Z_3^m)$，$f(x_1,\cdots,x_m,y_1,\cdots,y_m)=\sum_{i=1}^m a_ix_iy_i+g(y_1,\cdots,y_m)$ 都是稳定的，其中 a_i=1 或 2, $i=1,\cdots,m$.

证明 用定理 2 的判别条件即得.

还可用其它的方法来构造稳定的 3-值逻辑函数. 我们的研究表明，稳定的 3-值逻辑函数也是大量存在的. 有关结果不再赘述.

5 结束语

我们发现，研究一般 P-值逻辑函数稳定性的困难之处关键在于考察本文引理 2 在 P 取一般值时是否成立，若对一般素数 P, 引理 2 都成立，则易知本文的其它结论也都成立，这将是很有意义的结果. 对 P 是合数的情形，我们尚未深入研究，估计问题的难度更大.

致谢 感谢曾本胜副教授对本文工作的帮助.

参 考 文 献

[1] 丁存生，肖国镇. 流密码学及其应用. 北京：国防工业出版社，1994, 前言.

[2] 杨义先，等. 编码密码学. 北京：人民邮电出版社，1992, 589–627.

[3] 武传坤，王新梅. Bent 函数在流密码中的应用. 通信学报，1993, 14(4): 23–27.

[4] 张木想，肖国镇. 关于 Bent 函数与其变元的非线性组合之间的相关性. 科学通报，1994，39(19)：1738–1741.

[5] 李世取，曾本胜. 多值逻辑函数相关免疫的充要条件. 密码学进展 —CHINA CRYPT'94, 西安：科学出版社，1994, 257–264.

[6] 张木想，肖国镇. 多值逻辑函数相关免疫的谱特征. 科学通报，1994. 39(9): 772–773.

[7] O.S. Rothaus. On bent functions. Journal of Combinatorial Theory (Ser. A), 1976, 20: 300–305.

[8] 聂灵沼，丁石孙. 代数学引论. 北京：高等教育出版社，1988, 123–124.

[9] 严士健, 等. 概率论基础. 北京: 科学出版社, 1982, 135.

STABILITY OF 3-VALUED LOGICAL FUNCTIONS

Li Shiqu Zhao Yaqun Yu Jiaen

(*Dept. of Applied Mathematics, Zhengzhou Information Eng. Institute, Zhengzhou* 450002)

Abstract This paper introduces the concept of stability of 3-valued logical functions and examines probability characterization of "stability". Criterion of stability of 3-valued logical functions is given and a typical method of constructing stable 3-valued logical funtions is presented. With the approach in this paper, the stability of P-valued logical functions may be investigated.

Key words 3-valued logical function, Stability, Chrestenson spectrum, Probability space

李世取: 男, 1945 年生, 教授, 博士生导师, 长期从事于概率统计方面的教学和研究. 近年来, 主要从事于概率统计在密码学中的应用方面的研究. 曾先后发表论文多篇.

赵亚群: 女, 讲师, 博士生, 主要研究方向为概率统计在密码学中的应用.

俞嘉恩: 男, 1945 年生, 副教授, 专业为代数及其应用. 目前主要从事组合论方面的研究.