多输出布尔函数的特征值分析

高海英 杨义先 侍伟敏
(北京邮电大学信息安全中心 北京 100876)

摘 要: 为了研究自变量是独立而非均匀分布条件下的多输出布尔函数的密码学性质，文章定义了多输出布尔函数的“谱值”和“特征值”，给出了多输出函数的特征值的一般表达式和估计式，并且计算出了 n 阶布尔置换和“t-弹性函数”特征值的上界。

关键词: 特征值，无偏函数，t-弹性函数，布尔置换
中图分类号: TP918.4 文献标识码：A 文章编号：1009-5896(2005)09-1467-03

The Analysis of Eigenvalue of Multi-outputting Boolean Functions

Gao Hai-ying Yang Yi-xian Shi Wei-min
(*The Information Security Center, BUPT, Beijing* 100876, *China*)

Abstract In order to investigate the cryptographical properties of the Multi-outputting Boolean functions under non-uniformity of arguments, this paper defines the spectrum and eigenvalue, presents the general expression and estimation formula, and computes the upper bounds of agonic functions and t-resilient functions.

Key words Eigenvalue, Agonic function, t-resilient function, Boolean permutation

1 引言

在密码算法的设计中，布尔函数是一个重要的组成部分，布尔函数选取的好坏直接影响算法的安全性。目前该领域已经取得了相当多的研究成果。文献[1]对布尔函数的平衡性、非线性度、相关免疫性、扩散性等密码性质进行了深入的研究，文献[2]分析了布尔函数的非线性标准，但对于布尔函数的密码性质的研究都是基于自变量是均匀分布这个前提条件的，而在实际应用中，布尔函数的输入变量值来自反馈移位寄存器，因此输入变量 $x=(x_1,x_2,\cdots,x_n)$ 的每个分量序列 $\{x_i\}$ 并不是均匀分布的，而满足 $p\{x_i=1\}=0.5-\varepsilon_i$，因此有必要对相互独立而非均匀分布条件下的布尔函数的密码学性质进行研究。文献[3]首次定义了自变量是非均匀分布的布尔函数的“特征值”，并分析了 Bent 函数、相关免疫函数等的“特征值”，给出了一般表达式，但对于密码学中广泛使用的多输出布尔函数的特征值未作分析。本文为了填补这一空白，定义了多输出布尔函数的“谱值”和“特征值”，给出了多输出函数的特征值的一般表达式和估计式，并且计算出了 n 阶布尔置换和“t-弹性函数”特征值的上界。

2 基本概念和引理

定义 1[4] 设 $F(x)$ 是 $F_2^n\to F_2^m$ 的函数，若对任意的 $\beta\in F_2^m$，$F^{-1}(\beta)=\{x\mid F(x)=\beta\}$ 有相同个数的元素，即 $\#\{x\mid F(x)=\beta\}=2^{n-m}$ (#表示集合的基数)，则称 $F(x)$ 是无偏的。

定义 2[1] 若 $F(x)$ 是 $F_2^n\to F_2^n$ 的函数，并且 $F(x)$ 是一个单射，则称 $F(x)$ 是 n 阶置换。

定义 3[4] 设 $F(x)$ 是 $F_2^n\to F_2^m$ 的函数，$t\ge 0$，若 $\forall a=(a_1,\cdots,a_t)\in F_2^t$，$\{i_1,\cdots,i_t\}\subseteq\{1,2,\cdots,n\}$，$F(x\mid x_{i_1}=a_1,\cdots,x_{i_t}=a_t)$ 是 $F_2^{n-t}\to F_2^m$ 的无偏函数，则称 $F(\ )$ 是 $t-$弹性函数。

引理 1[4] 设 $F(x)$ 是 $F_2^n\to F_2^m$ 的函数，$F(x)$ 是无偏的 t 阶相关免疫函数 $\Leftrightarrow$ $F(x)$ 是 t-弹性函数。无偏函数就是 0-弹性函数。

引理 2[4] 设 $F(x)$ 是 $F_2^n\to F_2^m$ 的函数，对每个 $\beta\in F_2^m$ $B_\beta=\{x\in F_2^n\mid F(x)=\beta\}$，令 $F_\beta(x)=\begin{cases}0, & x\notin B_\beta\\ 1, & x\in B_\beta\end{cases}$，则 $F(x)$ 是 t 阶相关免疫的，当且仅当对任意的 $\beta\in F_2^m$，$F_\beta(x)$ 是 t 阶相关免疫的。

2004-03-11 收到，2004-11-11 改回
国家“973”计划(G1999035804)和国家自然科学基金 (60372094, 90204017)资助课题

3 主要定义和定理

定义 4[3] 设 $f(x)$ 是 $F_2^n \to F_2$ 的布尔函数，$x=(x_1,x_2,\cdots,x_n)$，$P\{x_i=1\}=1/2-\varepsilon_i$，$i=1,\cdots,n$，设 $|\varepsilon_i|\le\varepsilon$，令

$$\Delta_f(\varepsilon)=\max_{|\varepsilon_i|\le\varepsilon,i=1,\cdots,n}\left|1/2-P\{f(x)=1\}\right|$$

为 $f(x)$ 的特征值。

定义 5 设 $F(x)$ 是 $F_2^n \to F_2^m$ 的函数，$x=(x_1,x_2,\cdots,x_n)$，$P\{x_i=1\}=1/2-\varepsilon_i$，$i=1,\cdots,n$，设 $|\varepsilon_i|\le\varepsilon$，令

$$\Delta_F(\varepsilon)=\max_{\substack{\beta\in F_2^m\\ |\varepsilon_i|\le\varepsilon,i=1,\cdots,n}}\left|1/2^m-P\{F(x)=\beta\}\right|$$

为 $F(x)$ 的特征值。

定义 4 是文献[3]定义的布尔函数的特征值，定义 5 是作者定义的多输出布尔函数的特征值，当 m=1 时，

$$\Delta_F(\varepsilon)=\max_{\substack{\beta\in F_2\\ |\varepsilon_i|\le\varepsilon,i=1,\cdots,n}}\left|1/2-P\{F(x)=\beta\}\right|\ge\Delta_f(\varepsilon)$$

定义 6 设 $F(x)$ 是 $F_2^n \to F_2^m$ 的函数，$\omega\in F_2^n$，$\beta\in F_2^m$，令

$$T_\beta(\omega)=1/2^n\sum_{\substack{F(x)=\beta\\ x\in F_2^n}}(-1)^{\omega\cdot x}$$

为 $F(x)$ 取 β 时在 ω 点的谱值，并且令 $T^*(\omega)=\max_{\beta\in F_2^m}\left|T_\beta(\omega)\right|$.

定理 1 设 $F(x)$是$F_2^n \to F_2^m$ 的函数，$\omega\in F_2^n$，$\beta\in F_2^m$，则

$$\Delta_F(\varepsilon)=\max_{\substack{\beta\in F_2^m\\ |\varepsilon_i|\le\varepsilon,i=1,\cdots,n}}\left|\frac{1}{2^m}-T_\beta(0)-\sum_{s=1}^{n}2^s\sum_{\substack{\omega\in F_2^n\\ W(\omega)=s}}T_\beta(\omega)\varepsilon_{1(\omega)}\cdots\varepsilon_{s(\omega)}\right|$$

其中 $W(\omega)$ 表示 ω 的重量。

证明

$$\begin{aligned}
\frac{1}{2^m}-p\{F(x)=\beta\}&=\frac{1}{2^m}-\sum_{a\in F_2^n,F(a)=\beta}P\{x_1=a_1,\cdots,x_n=a_n\}\\
&=\frac{1}{2^m}-\sum_{a\in F_2^n,F(a)=\beta}P\{x_1=a_1\}\cdots\{x_n=a_n\}\\
&=\frac{1}{2^m}-\sum_{a\in F_2^n,F(a)=\beta}\left(\frac{1}{2}+(-1)^{a_1}\varepsilon_1\right)\cdots\left(\frac{1}{2}+(-1)^{a_n}\varepsilon_n\right)\\
&=\frac{1}{2^m}-\sum_{a\in F_2^n,F(a)=\beta}\frac{1}{2^n}\\
&\quad-\sum_{a\in F_2^n,F(a)=\beta}\sum_{s=1}^{n}\frac{1}{2^{n-s}}\sum_{\omega\in F_2^n,W(\omega)=s}(-1)^{(a,\omega)}\varepsilon_{1(\omega)}\cdots\varepsilon_{s(\omega)}\\
&=\frac{1}{2^m}-T_\beta(0)\\
&\quad-\sum_{s=1}^{n}2^s\sum_{\omega\in F_2^n,W(\omega)=s}\frac{1}{2^n}\sum_{a\in F_2^n,F(a)=\beta}(-1)^{(a,\omega)}\varepsilon_{1(\omega)}\cdots\varepsilon_{s(\omega)}\\
&=\frac{1}{2^m}-T_\beta(0)-\sum_{s=1}^{n}2^s\sum_{\omega\in F_2^n,W(\omega)=s}T_\beta(\omega)\varepsilon_{1(\omega)}\cdots\varepsilon_{s(\omega)}
\end{aligned}$$

故定理结论成立。 证毕

注：在定理 1 的证明中，若 $W(\omega)=s$，则分别用 $1(\omega),2(\omega),\cdots,s(\omega)$ 表示 ω 中的分量为 1 的位置。

引理 3 若 $F(x)$ 是 $F_2^n \to F_2^m$ 的无偏函数，则

$$T_\beta(0)=\frac{1}{2^m}$$

证明 由定义 1 和定义 6 直接可得。

定理 2 设 $F(x)$ 是 $F_2^n \to F_2^m$ 的无偏函数，则

$$\Delta_F(\varepsilon)\le\sum_{\omega\in F_2^n/\{0\}}T^*(\omega)(2\varepsilon)^{W(\omega)}$$

其中 $W(\omega)$ 表示 ω 的重量。

证明 由定理 1 和引理 3 可得

$$\Delta_F(\varepsilon)=\max_{\substack{\beta\in F_2^m\\ |\varepsilon_i|\le\varepsilon,i=1,\cdots,n}}\left|\sum_{s=1}^{n}2^s\sum_{\omega\in F_2^n,W(\omega)=s}T_\beta(\omega)\varepsilon_{1(\omega)}\cdots\varepsilon_{s(\omega)}\right|$$

当 β 取定值时，由 $\left|\sum_{s=1}^{n}2^s\sum_{\omega\in F_2^n,W(\omega)=s}T_\beta(\omega)\varepsilon_{1(\omega)}\cdots\varepsilon_{s(\omega)}\right|$ 可以看出，对于任意的 $i\in\{1,\cdots,n\}$，只有 $\varepsilon_i=\varepsilon$ 或 $-\varepsilon$ 时，才能达到最大值。因此

$$\Delta_F(\varepsilon)\le\max_{\substack{\beta\in F_2^m\\ |\varepsilon_i|=\varepsilon,i=1,\cdots,n}}\left|\sum_{s=1}^{n}2^s\sum_{\omega\in F_2^n,W(\omega)=s}T_\beta(\omega)\varepsilon_{1(\omega)}\cdots\varepsilon_{s(\omega)}\right|\qquad(1)$$

令 $\varepsilon_i=(-1)^{u_i}\varepsilon$，$i=1,\cdots,n$，$u_i\in F_2$，则存在 $u\in F_2^n$，使下式成立：

$$\varepsilon_{1(\omega)}\cdots\varepsilon_{s(\omega)}=(-1)^{u\omega}\varepsilon^s$$

因此,由式(1)得

$$\begin{aligned}
\Delta_F(\varepsilon)&\le\max_{u\in F_2^n,\beta\in F_2^m}\left|\sum_{\omega\in F_2^n/\{0\}}(-1)^{u\omega}T_\beta(\omega)(2\varepsilon)^{W(\omega)}\right|\\
&\le\max_{\beta\in F_2^m}\sum_{\omega\in F_2^n/\{0\}}\left|T_\beta(\omega)\right|(2\varepsilon)^{W(\omega)}\\
&=\sum_{\omega\in F_2^n/\{0\}}T^*(\omega)(2\varepsilon)^{W(\omega)}
\end{aligned}$$

故定理结论成立。 证毕

定理 3 若 $F(x)$ 是 n 阶布尔置换，则

$$\Delta_F(\varepsilon)\le\frac{1}{2^n}\sum_{s=1}^{n}\binom{n}{s}(2\varepsilon)^s$$

证明 由于 $F(x)$ 是 n 阶布尔置换，故对任意的 $\beta\in F_2^n$，和式：

$$\begin{aligned}
&\sum_{\substack{a=(a_1,\cdots,a_n)\\ F(a)=\beta}}P\{x_1=a_1,\cdots,x_n=a_n\}\\
&\quad=P\{x_1=a_1\}\cdots P\{x_n=a_n\}\\
&\quad=\left([1+(-1)^{a_1}2\varepsilon_1]\cdots[1+(-1)^{a_n}2\varepsilon_n]\right)/2^n
\end{aligned}$$

对于任意的 $(a_1,a_2,\cdots,a_n)\in F_2^n$，都有

$$\frac{[1-2\varepsilon]^n}{2^n}\le P\{x_1=a_1,\cdots,x_n=a_n\}\le\frac{[1+2\varepsilon]^n}{2^n}$$

故对任意 $\beta\in F_2^n$，都有

$$\frac{1}{2^n}\sum_{s=1}^{n}(-1)^s\binom{n}{s}(2\varepsilon)^s$$

$$\le P\{x_1=a_1,\cdots,x_n=a_n\}-\frac{1}{2^n}\le\frac{1}{2^n}\sum_{s=1}^{n}\binom{n}{s}(2\varepsilon)^s$$

因此

$$\Delta_F(\varepsilon)=\max_{\substack{\beta\in F_2^m\\ |\varepsilon_i|\le\varepsilon,i=1,\ldots,n}}\left|\frac{1}{2^n}-p\{F(x)=\beta\}\right|\le\frac{1}{2^n}\sum_{s=1}^{n}\binom{n}{s}(2\varepsilon)^s$$

证毕

引理 4　设 $F(x)$ 是 $F_2^n\to F_2^m$ 的 t -弹性函数，$\omega\in F_2^n$，$\beta\in F_2^m$，若 $1\le W(\omega)\le t$，则 $T_\beta(\omega)=0$。

证明　已知 $F(x)$ 是 t -弹性函数，由引理 1 和引理 2 可知 $F_\beta(x)$ 是 t 阶相关免疫函数，即对于任意 $\omega\in F_2^n$ $(1\le W(\omega)\le t)$，有

$$\sum_{x\in F_2^n}(-1)^{F_\beta(x)+\omega\cdot x}=\sum_{x\in B_\beta}(-1)^{\omega\cdot x+1}+\sum_{x\notin B_\beta}(-1)^{\omega\cdot x}=0$$

又由于

$$\sum_{x\in F_2^n}(-1)^{\omega\cdot x}=\sum_{x\in B_\beta}(-1)^{\omega\cdot x}+\sum_{x\notin B_\beta}(-1)^{\omega\cdot x}=0$$

故

$$\sum_{x\in B_\beta}(-1)^{\omega\cdot x}=0\text{ 即 }T_\beta(\omega)=0$$　　证毕

定理 4　设 $F(x)$ 是 $F_2^n\to F_2^m$ 的 t -弹性函数，则

$$\Delta_F(\varepsilon)\le\sum_{\omega\in F_2^n\text{且}W(\omega)>t}T^*(\omega)(2\varepsilon)^{W(\omega)}$$

证明　由引理 4 和定理 2 直接可得。

4　结束语

本文在假设自变量的概率分布与均匀分布的偏差不超过 ε 的条件下，给出了多输出布尔函数的特征值的定义。本文又给出了特征值的计算公式，而且研究了密码设计中经常用到的无偏函数和 t -弹性函数的特征值的上界。在实际应用中，特征值随 ε 的变化情况在设计具有好的密码性质的多输出布尔函数的过程中是个值得考虑的因素。

参 考 文 献

[1] 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: 174.

[2] Meier W, Staffelbach O. Nonlinearity criteria for cryptographic functions. Advances in Cryptology-Eurocrypt'89, Proceedings[C]. Springer-Verlag, 1989: 549 – 562.

[3] Kanstantsin, Miranovich. Spectral analysis of Boolean functions under non-uniformity of arguments. http://eprint.iacr.org 2002.

[4] 王育民，王新梅，李大兴.密码学进展. CHINACRYPT'2002[M], 威海, 2002. 北京：电子工业出版社, 2002: 259 – 260.

高海英：女，1978 年生，博士生，研究方向为现代密码学、信息隐藏.

杨义先：男，1961 年生，教授，博士生导师，研究方向为现代密码学、信息安全.

侍伟敏：女，1978 年生，博士生，研究方向为现代密码学、网络安全.