文章编号: 1001- 2486(2008) 03- 0086- 04

布尔函数的 Walsh 谱绝对值分布及其性质研究*

屈龙江[1], 李　强[1], 李　超[1,2]
(1. 国防科技大学 理学院, 湖南 长沙　410073;
2. 福建师范大学 网络安全与密码技术重点实验室, 福建 福州　350007)

摘　要: 提出并研究了布尔函数的 Walsh 谱绝对值分布。指出布尔函数 Walsh 谱绝对值分布在仿射变换下的不变性, 计算了 $n(n \leqslant 5)$ 元布尔函数的 Walsh 谱绝对值分布, 研究了 Walsh 谱绝对值分布与 Walsh 谱支撑和 Walsh 谱中非零取值个数以及其他一些密码学难题的联系, 最后研究了布尔函数的 Walsh 谱绝对值分布的大小。

关键词: 布尔函数; Walsh 谱绝对值分布; 仿射等价类; Walsh 谱支撑; Walsh 谱非零取值个数
中图分类号:TN918. 1　　文献标识码: A

On the Absolute Values Distribution of the Walsh Spectrums of Boolean Functions and Their Properties

QU Long-jiang[1], LI Qiang[1], LI Chao[1,2]
(1. College of Science, National Univ. of Defense Technology, Changsha 410073, China;
2. Key Lab of Network Security and Cryptology, Fujian Normal Univ., Fuzhou 350007, China)

Abstract: The absolute value distribution of the Walsh spectrums of Boolean functions is presented and studied. The absolute value distribution of the Walsh spectrum is invariant under affine transformations. Then Walsh spectrums' absolute value distributions of all n-variable Boolean functions are obtained for. The relationships of the absolute value distributions of the Walsh spectrums and the support of the Walsh spectrums and the number of nonzero values of the Walsh spectrums and other problems are studied. Finally, the size of the absolute value distribution of the Walsh spectrum of Boolean functions is studied.

Key words: Boolean function; the absolute value distribution of Walsh spectrum; affine equivalent class; Walsh support; number of the nonzero values of Walsh spectrum

布尔函数在 Hash 函数, 流密码和分组密码的设计和分析中都有极其重要的作用[1-2]。在密码学中使用的布尔函数需要满足许多密码学准则, 如平衡、高非线性度、高相关免疫、高传播特征、无线性结构、高代数免疫度等。研究布尔函数密码学性质最重要的数学工具是 Walsh 谱[3], 即特征 2 情形下的离散 Fourier 变换。由一个布尔函数 Walsh 谱可以唯一确定这个函数。平衡、非线性度、相关免疫等密码学性质直接与布尔函数 Walsh 谱有很深刻的联系, 所以研究布尔函数 Walsh 谱有十分深刻的意义。文献[4]中研究了布尔函数 Walsh 谱支撑, 文献[5]中研究了布尔函数 Walsh 谱中非零取值个数, 本文提出并研究了布尔函数的 Walsh 谱绝对值分布。

1　Walsh 谱绝对值分布及其仿射不变性

一个 n 元布尔函数 $f(x) = f(x_1, x_2, \cdots, x_n)$ 为 F_2^n 到 F_2 上的映射, 其重量为 $wt(f) = \#\{x \in F_2^n \mid f(x) = 1\}$。记 B_n 为 n 元布尔函数全体, 设 $f(x) \in B_n$, 则 $f(x)$ 的 Walsh 谱是 $\{0,1\}^n$ 上的一个实值函数, 定义 $W_f(\omega) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus x \cdot \omega}$, 这里"$\cdot$" 表示两个向量的点乘, 即 $x \cdot \omega = \bigoplus_{i=1}^{n} x_i \omega_i$, 其中, $x = (x_1, x_2,$

* 收稿日期: 2007- 11- 10
基金项目: 国家自然科学基金资助项目(60573028); 国防科技大学校预研基金资助项目(JC07- 02- 03); 福建师范大学网络安全与密码技术重点实验室开放课题资助项目(07A0003)
作者简介: 屈龙江(1980—), 男, 博士生。

$\cdots, x_n)$, $\omega = (\omega_1, \omega_2, \cdots, \omega_n)$。其逆变换为$(-1)^{f(x)} = \frac{1}{2^n}\sum_{\omega\in\{0,1\}^n} W_f(\omega)(-1)^{x\cdot\omega}$。Walsh 谱有很多性质。

命题 1[1-2] $W_f(w) = 2^n - 2wt(f+\omega\cdot x)$。

命题 2[1-2] (Parseval 等式) $\sum_{\omega\in F_2^n} W_f^2(\omega) = 2^{2n}$。

命题 3 设$f\in B_n$, 记f 的重量为$wt(f)$, 若 $wt(f)$ 为偶数, 则 $W_f(\omega)\equiv 0 \pmod 4$, $\forall\ \omega\in F_2^n$; 若 $wt(f)$ 为奇数, 则 $W_f(\omega)\equiv 2 \pmod 4$, $\forall\ \omega\in F_2^n$。

证明 设 $S_1=\{x\in F_2^n | f(x)=1, \omega\cdot x=0\}$, $S_2=\{x\in F_2^n | f(x)=1, \omega\cdot x=1\}$, $S_3=\{x\in F_2^n | f(x)=0, \omega\cdot x=0\}$, $S_4=\{x\in F_2^n | f(x)=0, \omega\cdot x=1\}$, 记 $d_i=\#\ S_i (1\leqslant i\leqslant 4)$, 则 $d_2=wt(f)-d_1$, $d_3=2^{n-1}-d_1$, $d_4=2^n-d_1-d_2-d_3=d_1+2^{n-1}-wt(f)$, 从而有 $W_f(\omega)=d_2+d_3-d_1-d_4=2wt(f)-4d_1\equiv 2wt(f) \pmod 4$。由此易知命题成立。 □

定义 1 设$f\in B_n$, $W_f(\omega)$ 为 f 在 ω 处的 Walsh 谱值, 定义 f 的 Walsh 谱绝对值分布二元组为 $(w, \#\{\omega\in F_2^n | |W_f(\omega)| = w\})$, 定义$f$ 的 Walsh 谱绝对值分布为 $T_f=\{(w_1, N_1), (w_2, N_2), \cdots, (w_t, N_t)\}$, 其中, $1\leqslant i\leqslant t$, (w_i, N_i) 为f 的Walsh 谱绝对值分布二元组, $N_i\geqslant 1$, $0\leqslant w_1<w_2<\cdots<w_t$。称 t 为f 的Walsh 谱绝对值分布 T_f 的大小。定义 $T_n=\{T_f | f\in B_n\}$。

由Walsh 谱定义和 Parseval 等式易知有:

定理 1 设 $T_f=\{(w_1, N_1), (w_2, N_2), \cdots, (w_t, N_t)\}\in T_n$, 则有 $\sum_{i=1}^{t} N_i = 2^n$ 且 $\sum_{i=1}^{t} N_i\cdot W_i^2 = 2^{2n}$。

定义 2[5] 设$f_1, f_2\in B_n$, 若存在 F_2 上的 n 阶可逆矩阵$\boldsymbol{A}$, 向量 $\overline{a}, \overline{b}\in F_2^n$, 常数 $c\in F_2$, 使得$f_1(\overline{x}) = f_2(\overline{x}\boldsymbol{A}+\overline{a})+\overline{x}\cdot\overline{b}+c$, 则称$f_1, f_2$ 仿射等价。显然, 仿射等价关系满足自反性、对称性、传递性, 是一个等价关系。B_n 在该等价关系下的分类称为n 元布尔函数的仿射等价类。

定理 2 T_f 为仿射变换下的不变量。

证明 设$f_1, f_2\in B_n$, 若存在 F_2 上的 n 阶可逆矩阵$\boldsymbol{A}$, 向量 $\overline{a}, \overline{b}\in F_2^n$, 常数 $c\in F_2$, 使得$f_1(\overline{x}) = f_2(\overline{x}\boldsymbol{A}+\overline{a})+\overline{x}\cdot\overline{b}+c$, 则

$$
\begin{aligned}
W_{f_1}(\overline{\omega}) &= \sum_{\overline{x}\in F_2^n}(-1)^{f_1(\overline{x})+\overline{\omega}\cdot\overline{x}} = \sum_{\overline{x}\in F_2^n}(-1)^{f_2(\overline{x}\boldsymbol{A}+\overline{a})+\overline{x}\cdot\overline{b}+c+\overline{\omega}\cdot\overline{x}} = (-1)^c\sum_{\overline{x}\in F_2^n}(-1)^{f_2(\overline{x}\boldsymbol{A}+\overline{a})+\overline{x}\cdot(\overline{b}+\overline{\omega})}\\
&= (-1)^c\sum_{\overline{y}\in F_2^n}(-1)^{f_2(\overline{y})+(\overline{y}+\overline{a})\boldsymbol{A}^{-1}\cdot(\overline{b}+\overline{\omega})} = (-1)^{(\overline{a}\boldsymbol{A}^{-1})\cdot(\overline{b}+\overline{\omega})+c}\sum_{\overline{y}\in F_2^n}(-1)^{f_2(\overline{y})+\overline{y}\cdot[(\overline{b}+\overline{\omega})(\boldsymbol{A}^{-1})^t]}\\
&= (-1)^{(\overline{a}\boldsymbol{A}^{-1})\cdot(\overline{b}+\overline{\omega})+c} W_{f_2}[(\overline{b}+\overline{\omega})(\boldsymbol{A}^{-1})^t]
\end{aligned}
$$

由此可以看出, 必有 $T_{f_1}=T_{f_2}$, 从而 T_f 为仿射变换下的不变量。 □

2 T_n, $n\leqslant 5$

利用已有的布尔函数仿射等价类分类结果, 可以得到这些函数的 Walsh 谱绝对值分布。如利用文献[6]中的 $n(n\leqslant 5)$ 元布尔函数等价类的结果, 可以得到 $T_n(n\leqslant 5)$ 中的所有元素。

当 $n=1$ 时, $T_1=\{\{(0,1),(2,1)\}\}$;

当 $n=2$ 时, $T_2=\{\{(0,3),(4,1)\},\{(2,4)\}\}$;

当 $n=3$ 时, $T_3=\{\{(0,7),(8,1)\},\{(2,7),(6,1)\},\{(0,4),(4,4)\}\}$;

当 $n=4$ 时, $T_4=\{\{(0,15),(16,1)\},\{(0,12),(8,4)\},\{(0,8),(4,7),(12,1)\},\{(0,6),(4,8),(8,2)\},\{(4,16)\},\{(2,15),(14,1)\},\{(2,12),(6,3),(10,1)\},\{(2,10),(6,6)\}\}$

当 $n=5$ 时, T_5 中的全部元素如表 1 所示。

表1 T_5 中的全部元素

Tab.1 All elements of T_5

{(0,31),(32,1)}	{(0,28),(16,4)}	{(0,24),(8,7),(24,1)}	{(0,22),(8,8),(16,2)}
{(0,19),(8,12),(16,1)}	{(0,16),(4,15),(28,1)}	{(0,16),(4,12),(12,3),(20,1)	{(0,16),(4,10),(12,6)}}
{(0,16),(8,16)}	{(0,14),(4,14),(12,2),(16,2)}	{(0,12),(4,16),(8,3),(24,1)}	{(0,12),(4,14),(8,4),(12,1),(20,1)}
{(0,12),(4,12),(8,4),(12,4)}	{(0,11),(4,14),(8,4),(12,2),(16,1)}	{(0,10),(4,16),(8,4),(16,2)}	{(0,10),(4,15),(8,6),(20,1)}
{(0,10),(4,13),(8,6),(12,3)}	{(0,9),(4,15),(8,6),(12,1),(16,1)}	{(0,8),(4,14),(8,8),(12,2)}	{(0,7),(4,16),(8,8),(16,1)}
{(0,6),(4,15),(8,10),(12,1)}	{(0,4),(4,16),(8,12)}	{(4,30),(12,1),(20,1)}	{(4,28),(12,4)}
{(2,31),(30,1)}	{(2,28),(14,3),(18,1)}	{(2,24),(6,7),(26,1)}	{(2,24),(6,4),(10,3),(22,1)}
{(2,22),(6,6),(10,2),(14,1),(18,1)}	{(2,22),(6,4),(10,4),(14,2)}	{(2,21),(6,7),(10,1),(14,3)}	{(2,20),(6,10),(10,1),(22,1)}
{(2,19),(6,9),(10,3),(18,1)}	{(2,19),(6,7),(10,5),(14,1)}	{(2,18),(6,12),(14,1),(18,1)}	{(2,18),(6,10),(10,2),(14,2)}
{(2,16),(6,10),(10,6)}	{(2,15),(6,15),(10,1),(18,1)}	{(2,15),(6,13),(10,3),(14,1)}	{(2,12),(6,16),(10,4)}

3 T_f 与 Walsh 谱支撑, Walsh 谱非零取值个数的联系

定义3[4] 布尔函数$f(x)$的Walsh谱支撑为 $S_f=\{\omega\in F_2^n \mid W_f(\omega)\neq 0\}$。

定义4[5] 称$\#S_f$为布尔函数$f(x)$的Walsh谱的非零取值个数, 记 $S_n=\{\#S_f, f\in B_n\}$, $S=\bigcup_{n\geqslant 1}S_n$。

定理3[5] $2,3,5,6,7,9,11\notin S$。

设$f\in B_n$, $T_f=\{(w_1,N_1),(w_2,N_2),\cdots,(w_t,N_t)\}$为$f$的Walsh谱的绝对值分布, 若$w_1\neq 0$, 则 $S_f=F_2^n$, $\#S_f=2^n$; 若$w_1=0$, 则$\#S_f=2^n-N_1$, 从而有如下定理:

定理4 设$f\in B_n$, $T_f=\{(w_1,N_1),(w_2,N_2),\cdots,(w_t,N_t)\}$为$f$的Walsh谱绝对值分布, 若$w_1=0$, 则

$$N_1\notin\{2^n-2,2^n-3,2^n-5,2^n-6,2^n-7,2^n-9,2^n-11\}$$

由上面的分析, 我们知道布尔函数的Walsh谱绝对值分布包含着Walsh谱非零取值个数的全部信息, 包含着Walsh支撑的部分信息, 对于它的研究将是很有意义的。相同等价类的布尔函数必然有相同的Walsh谱绝对值分布, 不同等价类的布尔函数也可能有相同的Walsh谱绝对值分布。如当n为偶数时存在n元Bent函数, Bent函数的等价类划分问题直到现在仍未解决, 但是所有n元Bent函数的Walsh谱绝对值分布都是相同的。因此, 布尔函数Walsh谱绝对值分布是比仿射变换等价类更广义的概念, 对于它的研究将有助于理解以及解决一些现有难题。如: 众所周知, 当且仅当n为偶数时存在n元Bent函数达到最大非线性度$2^{n-1}-2^{\frac{n}{2}-1}$, 但是Bent函数不平衡, 一个$n(n\geqslant 8)$元平衡布尔函数的最大非线性度是多少, 这是一个长达30多年的公开问题[1]。当$n=8$时, 问题具体为:

问题1[1] 是否存在非线性度为118的8元平衡布尔函数?

命题4 非线性度为118的8元平衡布尔函数存在, 当且仅当T_8中包含如下形式的元素:

$$\{(0,N_1),(4,N_2),(8,N_3),(12,N_4),(16,N_5),(20,N_6)\},\quad N_1\geqslant 1$$

证明 设f为非线性度为118的8元平衡布尔函数, 则 $W_f(0)=0$, $\max_{\omega\in F_2^8}|W_f(\omega)|=20$, $|W_f(\omega)|\equiv 0 \pmod 4$, $\forall\omega\in F_2^n$, 从而T_f必形如$\{(0,N_1),(4,N_2),(8,N_3),(12,N_4),(16,N_5),(20,N_6)\}$, $N_1\geqslant 1$。

设T_8中有形如$\{(0,N_1),(4,N_2),(8,N_3),(12,N_4),(16,N_5),(20,N_6)\}$, $N_1\geqslant 1$的元素, 记之为T_f, 由$N_1\geqslant 1$, 知存在α, 使得$W_f(\alpha)=0$, 取$g=f\oplus\alpha\cdot x$, 则g为一个平衡函数, 且$T_g=T_f$。若$N_6=0$, 则$\max_{\omega\in F_2^8}|W_g(\omega)|=16$, g为Bent函数, 这与g平衡矛盾。从而, $N_6\geqslant 1$, $\max_{\omega\in F_2^8}|W_g(\omega)|=20$, $N_g=118$, 所以g

为非线性度为 118 的 8 元平衡布尔函数。命题由此得证。 □

4 T_f 的大小

设 $f\in B_n$, $T_f=\{(w_1,N_1),(w_2,N_2),\cdots,(w_t,N_t)\}$ 为 f 的 Walsh 谱绝对值分布,讨论 t 的值。当 $t=1$ 时,由 Parseval 等式, $T_f=\{(2^{\frac{n}{2}},2^n)\}$,从而 n 必为偶数且 f 为 Bent 函数。当 $t=2$ 时,若 $w_1=0$,则 $w_2N_2^2=2^{2n}$,于是存在整数 $\frac{n}{2}<k\leqslant n$,使得 $w_2=2^k$,从而有 $N_2=2^{n-k}$, $N_1=2^n-N_2$,这即是高原函数[1]。

定理 5 当 $n>2$ 时, $t\leqslant\lfloor\frac{1}{2}+\sqrt[3]{3\cdot2^{2n-4}+\frac{1}{2}\sqrt[3]{3\cdot2^{2n-4}}}\rfloor$。

证明 设 $f\in B_n$, $T_f=\{(w_1,N_1),(w_2,N_2),\cdots,(w_t,N_t)\}$,若 $wt(f)$ 为偶数,则 $w_i\equiv0(\mathrm{mod}\,4)$,从而有 $2^{2n}=\sum_{i=1}^{t}N_iw_i^2\geqslant4^2+8^2+\cdots+(4t-4)^2=\frac{16}{6}t(t-1)(2t-1)$。解此不等式,再由 $t\geqslant1$,可得 $t\leqslant\lfloor\frac{1}{2}+\sqrt[3]{3\cdot2^{2n-4}+\frac{1}{2}\sqrt[3]{3\cdot2^{2n-4}}}\rfloor$。若 $wt(f)$ 为奇数,则 $w_i\equiv2(\mathrm{mod}\,4)$,从而有 $2^{2n}=\sum_{i=1}^{t}N_iw_i^2\geqslant2^2[2^n-(t-1)]+6^2+10^2+\cdots+(4t-2)^2=\frac{2}{3}(8t^3-8t+6\cdot2^n+6)$。解此不等式,再由 $t\geqslant1$,设 $q=3\cdot(2^{2n-4}-2^{n-2}-\frac{1}{4})$,同理可得 $t\leqslant\lfloor\sqrt[3]{q+\frac{1}{3}+\sqrt[3]{q}}\rfloor$。容易证明,当 $n>2$ 时,总有 $\sqrt[3]{q+\frac{1}{3}+\sqrt[3]{q}}\leqslant\frac{1}{2}+\sqrt[3]{3\cdot2^{2n-4}+\frac{1}{2}\sqrt[3]{3\cdot2^{2n-4}}}$,从而 $t\leqslant\max\{\lfloor\sqrt[3]{q+\frac{1}{3}+\sqrt[3]{q}}\rfloor,\lfloor\frac{1}{2}+\sqrt[3]{3\cdot2^{2n-4}+\frac{1}{2}\sqrt[3]{3\cdot2^{2n-4}}}\rfloor\}=\lfloor\frac{1}{2}+\sqrt[3]{3\cdot2^{2n-4}+\frac{1}{2}\sqrt[3]{3\cdot2^{2n-4}}}\rfloor$。 □

由上述定理,可以得到关于 t 的一个上界如表 2 所示。

表 2 T_f 大小的一个上界

Tab. 2 An upper bound of the size of T_f

n	3	4	5	6	7	8	9	10
t 的上界	2	4	6	9	15	23	37	58

5 结束语

本文提出并研究了布尔函数的 Walsh 谱绝对值分布,指出其在仿射变换下的不变性,给出了一个集合为一个布尔函数 Walsh 谱绝对值分布的必要条件,计算了 $n(n\leqslant5)$ 元布尔函数的 Walsh 谱绝对值分布,研究了 Walsh 谱绝对值分布与 Walsh 谱支撑和 Walsh 谱中非零取值个数以及其他一些密码学难题的联系,最后研究了布尔函数 Walsh 谱绝对值分布的大小。布尔函数 Walsh 谱绝对值分布是比 Walsh 谱支撑, Walsh 谱非零取值个数意义更丰富的一个概念,对于它的深入研究必然能加深我们对布尔函数的认识,这对密码学中的很多问题都将是很有意义的。

参 考 文 献:

[1] Carlet C. Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the Monography Boolean Methods and Models[M]. Cambridge University Press, 2007.

[2] 温巧燕, 等. 现代密码学中的布尔函数[M]. 北京: 科学出版社, 2000.

[3] 冯登国. 频谱理论及其在密码学中的应用[M]. 北京: 科学出版社, 2000.

[4] Carlet C, et al. On the Supports of the Walsh Transforms of Boolean Functions[EB/OL]. http://eprint.iacr.org/2004/256, 2004.

[5] 冯克勤, 等. 布尔函数 Walsh 谱的非零取值个数[J]. 应用数学学报, 2004, 27(3): 500-514.

[6] Berlekamp E R, et al. Weight Distribution of the Cosets of the (32; 6) Reed-muller Code[J]. IEEE Trans. on Information Theory, 1972, 18(1): 203-207.