Plateaued 函数的对偶性

王维琼[1,2] 肖国镇[2]

(长安大学理学院 西安 710064)[1] (西安电子科技大学 ISN 国家重点实验室 西安 710071)[2]

摘 要 研究了 Plateaued 函数的对偶性;基于 Plateaued 函数对偶性的定义及函数限制的理论,得到了 Plateaued 函数与其对偶函数在子空间上的限制及正规性上的对应关系;利用 Plateaued 的对偶这一工具,得到了两个 Plateaued 函数的互相关平方和指标的界。

关键词 Plateaued 函数,对偶,正规,Bent 函数

中图法分类号 TN918.1 **文献标识码** A

Dulity of Plateaued Functions

WANG Wei-qiong[1,2] XIAO Guo-zhen[2]

(School of Science, Chang'an University, Xi'an 710064, China)[1]

(National Key Laboratory of Integrated Service Network, Xidian University, Xi'an 710071, China)[2]

Abstract The dulity of Plateaued functions was analyzed. Based on the definition and the restriction of Plateaued functions on some affine subspaces, we proved that there are strong relationships between a Plateaued function and its dulity, especially on the restriction on flats. We also derived the bound of the sum-of-squares indicator of the cross-correlation between any two Plateaued functions by using the tool of dulity.

Keywords Plateaued functions, Dulity, Normality, Bent functions

1 引言

布尔函数在密码学尤其是对称密码学中发挥着重要的作用。为满足 Shannon 提出的混淆及扩散准则,一个好的密码函数必须足够复杂。为了精确刻画布尔函数的复杂性,密码学研究者从不同的角度给出了一系列复杂度指标,如非线性度、代数厚度、代数次数、正规性、相关免疫、弹性、代数免疫等。其中非线性度是重要的指标之一,具有最大非线性度的偶数元布尔函数被称为 Bent 函数。这类函数能有效地抵抗线性攻击和最佳仿射逼近攻击,从而引起了国内外密码学研究者的广泛关注。1974 年 Dillon 提出了 Bent 函数的对偶性[1],并用 Walsh 谱的特征函数予以刻画。Dillon 指出:Bent 函数的对偶仍为 Bent 函数。这一结论表明不仅 Bent 函数的非线性度很高,其对偶函数的非线性度也很高。研究发现,对偶是研究 Bent 函数的一个非常有用的工具。Canteaut 等人[2]在研究 Bent 函数的分解时,讨论了 Bent 函数在子空间上限制的 Walsh 谱与它的对偶函数之间的关系,得到了一些结论。文献[3]中讨论了两个 Bent 函数的导数与它们的对偶函数在 Walsh 谱方面的关系。

尽管 Bent 函数具有最高的非线性度,但它是不平衡的,不具有任一阶的相关免疫性,且变元的个数只能为偶数,这些缺陷都限制了 Bent 函数在密码学中的直接应用。为弥补这些缺陷,相继出现了部分 Bent 函数[4]及 Plateaued 函数[5]的概念,其中 Plateaued 函数是 Bent 函数和部分 Bent 函数的推广,它提供了一些能达到多个密码学指标折中的函数,且不具有非零的线性结构,因而对这一类函数性质的研究也是非常必要的。Gong 等人[6]于 2003 年提出了 Plateaued 函数的对偶性这一概念,并用 Walsh 谱的特征函数予以刻画。本文从 Walsh 谱的角度研究 Plateaued 函数的对偶性,分析了 Plateaued函数与其对偶在子空间上限制的 Walsh 谱及正规性方面的关系,并用对偶这一工具得到了两个 Plateaued 函数的互相关平方和指标的界。

2 预备知识

n 元布尔函数 $f(x)$ 定义为映射:$f: F_2^n \to F_2$,其中 $x=(x_1,x_2,\cdots,x_n)\in F_2^n$,并记 B_n 为 F_2^n 上所有 n 元布尔函数的集合。

定义 1 n 元布尔函数 $f(x)\in B_n$ 在 $\alpha\in F_2^n$ 处的 Walsh 谱变换定义为

$$F(f+\varphi_\alpha)=\sum_{x\in F_2^n}(-1)^{f(x)+\varphi_\alpha(x)}$$

当 $F(f)=0$ 时,称 $f(x)$ 为平衡函数。其中 $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in F_2^n$,$x=(x_1,x_2,\cdots,x_n)\in F_2^n$,$\varphi_\alpha(x)=\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_nx_n$。

定义 2 设 $\tilde{S}=\{\alpha\mid F(f+\varphi_\alpha)\neq 0,\alpha\in F_2^n\}$,其中 $f(x)\in B_n$。若存在某一偶数 $r(0\leqslant r\leqslant n)$,使 $\#\tilde{S}=2^r$,且对任意 $\alpha\in F_2^n$,都有 $F(f+\varphi_\alpha)\in\{0,\pm 2^\lambda\}$,其中 $\lambda=n-r/2$,则称 $f(x)$ 为

到稿日期:2013-01-08 返修日期:2013-02-27 本文受国家自然科学基金青年基金项目(61202437),中央高校基本科研业务基金(CHD 2010JC101)资助。

王维琼 女,博士,讲师,主要研究方向为密码学及信息安全,E-mail:wqwang@chd.edu.cn。

n 元 r 阶 Plateaued 函数。

特别地，若 $\lambda=\begin{cases}\frac{n+1}{2}, & \text{当 } n \text{ 为奇数时}\\ \frac{n+2}{2}, & \text{当 } n \text{ 为偶数时}\end{cases}$，则称 $f(x)$ 为三值几乎最优函数。在所有的 Plateaued 函数中，这类函数因具有最高的非线性度而特别引人关注。

设 $f(x)\in B_n$，V 为 F_2^n 上的一个 k 维线性子空间，称 $f\phi_V$ 为 $f(x)$ 在 V 上的限制，其中 $\phi_V(x)=\begin{cases}1, & x\in V\\ 0, & x\notin V\end{cases}$。显然，$f\phi_V(x)=1$ 当且仅当 $f(x)=1$ 且 $x\in V$。若 $f(x)$ 在某一 k 维的仿射子空间 $a+V$ 上的限制为常数，则称 $f(x)$ 为 k 正规布尔函数，或称 $f(x)$ 关于 $a+V$ 为 k 正规的。

定义 3[6] 设 $f(x)$ 为 Plateaued 函数，则 $f(x)$ 的对偶 $\tilde{f}(v)$ 定义为

$$\tilde{f}(v)=\begin{cases}0, & \text{当 } F(f+\varphi_v)=0 \text{ 时}\\ 1, & \text{当 } F(f+\varphi_v)\neq 0 \text{ 时}\end{cases}$$

定义 4[7] 设 $f(x),g(x)\in B_n$，$f(x)$ 与 $g(x)$ 的互相关平方和指标定义为

$$\sigma_{f,g}=\sum_{a\in F_2^n}\Delta_{f,g}^2(\alpha)$$

式中，$\Delta_{f,g}(\alpha)=\sum_{a\in F_2^n}(-1)^{D_{f,g}(\alpha)}$，而 $D_{f,g}(\alpha)=f(x)+g(x+\alpha)$。

3 主要结论

Gong 等人[6]已经证明，若平衡三值几乎最优函数的对偶函数仍为三值几乎最优函数，则 $f(x)$ 具有几个优良的密码学性质，如一阶弹性、高非线性性、有最优的自相关值等。因而要使 Plateaued 函数具有良好的密码学性质，其对偶函数也需具有较强的密码学性质。

引理 1[8] 设 $f(x)\in B_n$，V,W 分别为 F_2^n 上的 $k,n-k$ 维子空间，$V\times W=F_2^n$。并设 $f(x)$ 关于 V 的分解序列为 $\{f\phi_{b+V}\mid b\in W\}$，简记为 $\{f_b\mid b\in W\}$，则

$$\sum_{v\in V^\perp}F^2(f+\varphi_v)=2^{n-k}\sum_{b\in W}F^2(f_b)$$

基于 Plateaued 函数对偶性的定义及引理 1，可以得到 Plateaued 函数与其对偶在子空间上限制的 Walsh 谱之间的关系。

定理 1 设 $f(x)\in B_n$ 为 Plateaued 函数，其 Walsh 变换取值于 $\{0,\pm 2^i\}$，并设 V,W 分别为 F_2^n 上的 $k,n-k$ 维子空间，$V\times W=F_2^n$，则

$$F(\tilde{f}\phi_{V^\perp})=2^{n-k}-2^{n-k-2i+1}\sum_{a\in W}F^2(f\phi_{a+V})$$

特别地，若 $f(x)\in B_n$ 为三值几乎最优函数，则

$$F(\tilde{f}\phi_{V^\perp})=2^{n-k}-2^{-k}\sum_{a\in W}F^2(f\phi_{a+V})$$

证明：由 Plateaued 函数对偶的定义知，$F^2(f+\varphi_v)=2^{2i}\tilde{f}(v)=2^{2i-1}[1-(-1)^{\tilde{f}(v)}]$。同时由引理 1 可知：

$$\sum_{v\in V^\perp}F^2(f+\varphi_v)=2^{n-k}\sum_{a\in W}F^2(f\phi_{a+V})$$

而

$$\sum_{v\in V^\perp}F^2(f+\varphi_v)=2^{2i-1}\sum_{v\in V^\perp}[1-(-1)^{\tilde{f}(v)}]$$
$$=2^{2i-1}[2^{n-k}-F(\tilde{f}\phi_{V^\perp})]$$

从而

$$F(\tilde{f}\phi_{V^\perp})=2^{n-k}-2^{n-k-2i+1}\sum_{a\in W}F^2(f\phi_{a+V})$$

特别地，当 $f(x)$ 为三值几乎最优函数时，

$$F(\tilde{f}\phi_{V^\perp})=2^{n-k}-2^{-k}\sum_{a\in W}F^2(f\phi_{a+V})$$

推论 1 设 $f(x)$ 为 n(n 为奇数)元三值几乎最优函数，$\tilde{f}(v)$ 为 $f(x)$ 的对偶函数，V 为 F_2^n 上的一个 $\frac{n+1}{2}$ 维子空间。若 $f(x)$ 关于仿射子空间 $a_0+V(a\in F_2^n)$ 正规，则 $\tilde{f}(v)$ 也关于 $V^\perp$ 正规。

证明：因 $f(x)$ 为三值几乎最优函数，且正规，则存在一 $\frac{n+1}{2}$ 维的仿射子空间 $a_0+V(V\times W=F_2^n,a_0\in W)$，使得 $f\phi_{a_0+V}=\varepsilon(\varepsilon=0 \text{ 或 } 1)$。另一方面，由 Plateaued 函数的正规性[9]可知，$f\phi_{a+V}(a\neq a_0\in W)$ 为平衡函数，即对任意 $a\neq a_0\in W$，有 $F^2(f\phi_{a+V})=0$。将这些结论代入定理 1 中，便有

$$F(\tilde{f}\phi_{V^\perp})=2^{n-\frac{n+1}{2}}-2^{-\frac{n+1}{2}}2^{2\cdot\frac{n+1}{2}}$$
$$=2^{n-\frac{n+1}{2}}-2^{\frac{n+1}{2}}=-2^{n-\frac{n+1}{2}}=-2^{\frac{n-1}{2}}$$

即 $\tilde{f}(v)$ 关于 $V^\perp$ 正规。

该推论表明三值几乎最优函数与其对偶函数在正规性上也存在很强的对应关系。在文献[4]中，Carlet 证明了 Fourier 变换的如下性质。

引理 2[4] 设 $f(x)\in B_n$，V 为 F_2^n 上的一个 k 维子空间，则对 $\forall\beta\in F_2^n$，有

$$\sum_{a\in V}F^2(f+\varphi_{a+\beta})=2^k\sum_{e\in V^\perp}(-1)^{\beta\cdot e}F(D_ef)$$

其中，$D_ef(x)=f(x)+f(x+e)$ 表示 $f(x)$ 在 e 处的差分。

定理 2 设 $f(x)\in B_n$(n 为奇数)为三值几乎最优函数，V 为 F_2^n 上的一个 k 维线性子空间，$\beta\in F_2^n$。若对任意 $e\in V^\perp\setminus\{0\}$，$D_ef$ 为平衡函数，则 $\tilde{f}\phi_{\beta+V}$ 也为平衡函数。

证明：因为 $f(x)$ 为三值几乎最优函数，则 $F^2(f+\varphi_v)=2^n[1-(-1)^{\tilde{f}(v)}]$。由引理 2 可知函数 $f(x)$ 与其导数的 Walsh 变换之间存在如下关系：

$$\sum_{a\in V}F^2(f+\varphi_{a+\beta})=2^k\sum_{e\in V^\perp}(-1)^{\beta\cdot e}F(D_ef)$$

又由于对任意 $e\in V^\perp\setminus\{0\}$，$D_ef$ 为平衡函数，即 $F(D_ef)=0$，因此上式变为

$$\sum_{a\in V}F^2(f+\varphi_{a+\beta})=2^n\sum_{a\in V}\lfloor 1-(-1)^{\tilde{f}(\alpha+\beta)}\rfloor=2^k2^n$$，即 $2^k-\sum_{a\in V}(-1)^{\tilde{f}(\alpha+\beta)}=2^k$，从而推出 $\sum_{a\in V}(-1)^{\tilde{f}(\alpha+\beta)}=0$，也即 $\tilde{f}\phi_{\beta+V}$ 也为平衡函数。

在文献[7]中，作者提出了用于衡量两个不同布尔函数相关程度的指标，即互相关函数的全局雪崩准则，它用互相关函数的平方和指标加以刻画。借助于 Plateaued 函数的对偶性，不难证明两个 Plateaued 函数的互相关函数平方和指标的界。

定理 3 设 $f(x),g(x)\in B_n$ 为 Plateaued 函数，Walsh 变换取值于 $\{0,\pm 2^i\}$，则

$$0\leqslant\sigma_{f,g}\leqslant 2^{n+2i}$$

证明：$\sigma_{f,g}=\sum_{a\in F_2^n}\Delta_{f,g}^2(\alpha)=\frac{1}{2^n}\sum_{a\in F_2^n}F^2(f+\varphi_a)F^2(g+\varphi_a)$

$$=\frac{1}{2^n}\sum_{a\in F_2^n}2^{2i}\tilde{f}(\alpha)2^{2i}\tilde{g}(\alpha)$$

又因为

$$\#\{\alpha\mid\tilde{f}(\alpha)=1\}=2^{2n-2i}=\#\{\alpha\mid\tilde{g}(\alpha)=1\}$$

所以

（下转第 50 页）

D_1，从而

$$D_1 \wedge x \wedge C_1 \wedge \cdots \wedge C_m = x \wedge C_1 \wedge \cdots \wedge C_m$$

即 D_1 是 S' 中冗余子句。

定理 5 与定理 6 给出了子句集中某子句中的某个文字是冗余文字的等价刻画，可用于命题逻辑公式的化简。

注：设 S, D 如定义 5，若 D 是 S 中的冗余子句，D 中的文字并不一定是 D 中关于 S 的冗余文字。例如，令 $S=\{x_1, x_1 \vee x_2\}$，显然 $D=x_1 \vee x_2$ 是子句集 S 中的冗余子句，当 $\nu(x_1)=1, \nu(x_2)=0$ 时，有 $x_1 \wedge x_2 \neq x_1 \wedge (x_1 \vee x_2)$，所以 x_1 不是 D 中关于 S 的冗余文字。

3 公式的可满足性判定

徐扬在文献[6]中针对析取范式讨论了命题逻辑公式中文字与小项的可消性，给出了文字及小项可消去的等价条件。在此基础上，本节讨论子句冗余性与可满足性的关系。

对于子句 A, B，以下用 $\underline{A}$ 表示 A 中出现的文字构成的集合，且 $A-B=\bigvee_{x \in \underline{A}-\underline{B}} x$。

定理 7 设 $S=\{C_1, \cdots, C_m, D\}$ 是命题逻辑中子句集，且 D 中不含互补文字。D 是 S 中的冗余子句当且仅当子句集 $S'=\{C_1-D, C_2-D, \cdots, C_m-D\}$ 不可满足。

证明：(充分性)若 D 不是 S 中的冗余子句，则

$$C_1 \wedge C_2 \wedge \cdots \wedge C_m \neq C_1 \wedge \cdots \wedge C_m \wedge D$$

于是存在赋值 v 使得 $v(C_1 \wedge C_2 \wedge \cdots \wedge C_m)=1$ 且 $v(C_1 \wedge \cdots \wedge C_m \wedge D)=0$，从而有 $v(D)=0$。故对于任意文字 $y \in \underline{D}$，有 $v(y)=0$。对于任意的 $i, 1 \leqslant i \leqslant m$，有 $v(C_i)=1$，从而存在 $x_i \in \underline{C_i}$ 使 $v(x_i)=1$。显然 $x_i \notin \underline{D}$，即 $x_i \in \underline{C_i}-\underline{D}$，故有 $v(C_i-D)=1$。由 i 的任意性可得 S' 是可满足的，矛盾。

(必要性)假设 S' 是可满足的。由于

$$(C_1-D) \wedge (C_2-D) \wedge \cdots \wedge (C_m-D) = \bigvee_{(x_1, \cdots, x_m) \in \underline{C_1}-\underline{D} \times \cdots \times \underline{C_m}-\underline{D}} x_1 \wedge \cdots \wedge x_m$$

故存在赋值 v 及 $(x_1, \cdots, x_m) \in \underline{C_1}-\underline{D} \times \cdots \times \underline{C_m}-\underline{D}$ 使得 $v(x_1)=v(x_2)=\cdots=v(x_m)=1$。

由于 $\{x_1, \cdots, x_m\} \cap \underline{D}=\emptyset$，且 D 中不含互补文字，可设对于任意 $y \in \underline{D}, v(y)=0$，于是有 $v(D)=0$。对于任意 $C_i, 1 \leqslant i \leqslant m$，注意到 $x_i \in C_i$ 且 $v(x_i)=1$，故 $v(C_i)=1$。于是可得

$$v(C_1 \wedge C_2 \wedge \cdots \wedge C_m)=v(C_1) \wedge \cdots \wedge v(C_m)=1$$

$$v(C_1 \wedge C_2 \wedge \cdots \wedge C_m \wedge D)=v(C_1) \wedge \cdots \wedge v(C_m) \wedge v(D)=0$$

故 $C_1 \wedge \cdots \wedge C_m \neq C_1 \wedge \cdots \wedge C_m \wedge D$，此与 D 是 S 中冗余子句矛盾。

由定理 6、定理 7 可得如下推论：

推论 设 S, x, D 如定义 5，则 x 是 D 中关于 S 的冗余文字当且仅当子句集 $\{x, C_1-D_1, \cdots, C_m-D_1\}$ 不可满足。

参 考 文 献

[1] 张健. 逻辑公式的可满足性判定-方法、工具及应用[M]. 北京：科学出版社，2000

[2] 秦永彬，张秋菊. 基于关键文字的求解 SAT 问题的启发式算法[J]. 计算机与数字工程，2010，38：1-4

[3] Liberatore P. Redundancy in logic I：CNF propositional formulae [J]. Artificial Intelligence，2005，163(30)：203-232

[4] Liberatore P. Redundancy in logic Ⅱ：2CNF and Horn propositional formulae [J]. Artificial Intelligence，2008，172(35)：265-299

[5] Gottlob G，Fermüller C G. Removing redundancy from a clause [J]. Artificial Intelligence，1993，61(27)：263-289

[6] 徐扬，邹开其. 布尔逻辑公式中文字和小项的可消性[J]. 西南交通大学学报，1990，1：107-112

[7] Ostrowski R，Mazure B，Saïs L，et al. Eliminating redundancies in SAT search trees [C]// Proceedings of the 15th IEEE International Conference on Tools with Artificial Intelligence (ICTA' 2003). Sacramento，2003，5：100-104

[8] 王国俊. 数理逻辑引论与归结原理[M]. 北京：科学出版社，2006

(上接第 20 页)

$$0 \leqslant \sigma_{f,g} \leqslant 2^{4i-n+2n-2i}=2^{n+2i}$$

且 $\sigma_{f,g}=0$ 当且仅当 $\tilde{f} \cdot \tilde{g}=0$；当 $f=g$ 时，有 $\sigma_f=2^{n+2i}$。

本文借助于 Plateaued 函数的定义及函数分解理论得到了任一 Plateaued 函数与其对偶函数之间的一些关系，并运用 Plateaued 函数的对偶这一工具得到了任意两个 Plateaued 函数的互相关函数平方和指标的界。

参 考 文 献

[1] Dillon J F. Elementary Hadamard Difference sets [D]. University of Maryland，1974

[2] Canteaut A，Charpin P. Decomposing bent functions[J]. IEEE Transactions on Information Theory，2003，49(8)：2004-2019

[3] 卓泽朋，崇金凤，高胜，等. Bent 函数的对偶性[J]. 武汉大学学报：理学版，2012，58(1)：086-088

[4] Carlet C. Partially-bent functions[C]// Advances in Cryptology-CRYPTO' 92，Lecture Notes in Computer Science. Springer-Verlag，1993，740：280-291

[5] Zheng Y，Zhang X M. Plateaued functions[C]// Heidelberg，ed. Advances in Cryptology-ICICS' 99，Lecture Notes in Computer Science. Springer-Verlag，1999，1726：284-300

[6] Gong G，Khoo K. Additive Autocorrelation of Resilient Boolean Functions[C]// Selected Areas in Cryptography 2003，Lecture Notes in Computer Science. Springer-Verlag，2003，3006：275-290

[7] Zhou Yu，Xie Min，Xiao Guo-zhen. On the global avalanche characteristics of two Boolean functions and the higher order nonlinearity[J]. Information Sciences，2010，180：256-265

[8] Canteaut A，Carlet C，Charpin P，et al. On cryptographic properties of the cosets of R(1，m)[J]. IEEE Transactions on Information Theory，2001，47(4)：1494-1513

[9] Wang Wei-qiong，Xiao Guo-zhen. Decomposition and Construction of Plateaued Functions[J]. Chinese Journal of Electronics，2009，18(4)：686-688