一类广义布尔函数的相关函数分析

杨志耀[1],卓泽朋[1],崇金凤[1,2]
(1. 淮北师范大学数学科学学院,安徽淮北 235000;2. 淮北师范大学信息学院,安徽淮北 235000)

摘 要: 基于广义布尔函数的理论研究,利用广义 Walsh-Hadamard 变换、相关函数以及平方和指标,分析了一类广义布尔函数的相关函数关系,得到这类广义布尔函数互相关函数以及自相关函数的关系;基于所得结果,利用自相关函数证明了一类广义 Bent 函数与 Bent 函数之间的关系. 最后,给出一类广义布尔函数的平方和指标关系.

关键词: 广义布尔函数; 相关函数; Bent 函数; 平方和指标; 广义 Walsh-Hadamard 变换
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2019)12-2556-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.12.014

Analysis of Correlation Function of a Class of Generalized Boolean Functions

YANG Zhi-yao[1], ZHUO Ze-peng[1], CHONG Jin-feng[1,2]
(1. *School of Mathematical Sciences, Huaibei Normal University, Huaibei, Anhui* 235000, *China*;
2. *Information College, Huaibei Normal University, Huaibei, Anhui* 235000, *China*)

Abstract: Based on the theoretical study of the generalized Boolean functions. The correlation functions of a class of generalized Boolean functions are analyzed by using generalized Walsh-Hadamard transform, correlation functions and sum-of-squares and indicator, and the relationship between correlation functions and auto-correlation functions of such generalized Boolean functions are obtained. Based on the results obtained, the relationship between a class of generalized Bent functions and Bent functions is proved by using auto-correlation functions. Finally, the relationship between sum-of-squares and indicator of a class of generalized Boolean functions is given.

Key words: generalized Boolean functions; correlation functions; Bent functions; sum-of-squares and indicator; generalized Walsh-Hadamard transform

1 引言

布尔函数在密码学中有着重要的应用,而作为非线性度最高的布尔 Bent 函数在密码学领域也有着诸多研究与应用[1~3].

随着布尔函数的研究深入,布尔函数的推广形式也随之而来. 从 $Z_2^n \to Z_q$ 的这一类函数称为广义布尔函数,此推广由 Schmidt 率先提出. 文中 Schmidt 对广义布尔函数 $f: Z_2^n \to Z_q$,当 $q=4$ 时进行研究,给出三类构造方法[4]. 近年来,广义布尔函数成为许多学者研究的热点,例如,满足平衡性、非线性等优良密码学性质的广义布尔函数构造,之后,关于广义 Bent 函数的性质、构造等问题也是重要研究方向,取得较为丰硕的研究成果[5~9]. Solé 和 Tokareva 等同样在 $q=4$ 时进行研究,得到一类 Bent 函数与广义 Bent 函数之间的关系[10]. Pantelimon Stănică 等则利用相关函数以及广义 Walsh-Hadamard 变换等理论对 Solé 等人的部分研究成果进行了丰富,并对 $q=8$ 时的广义布尔函数 f 进行研究,得到其广义 Walsh-Hadamard 变换之间的关系,并给出三类广义 Bent 函数的构造方法,其本质是布尔 Bent 函数构造方法的推广[11]. 布尔函数的相关函数理论对于布尔函数的性质刻画具有重要的作用,但 Pantelimon Stănică 等在文中未对当 $q=8$ 时这类广义布尔函数的相关性进行说明,那么,此时广义布尔函数的相关函数是否也满足一定关系,对此进行分析研究.

本文在 Stănică 等人研究基础上,利用相关函数的

收稿日期:2018-12-14;修回日期:2019-03-11;责任编辑:梅志强
基金项目:国家自然科学基金(No. 60573026, No. 10101008);安徽省自然科学基金(No. 1608085MF143);安徽高校省级自然科学研究重点项目(No. KJ2018A0678);淮北师范大学研究生创新基金(No. ycx201901008)

有关理论得到定义在 $Z_2^n \to Z_8$ 上的这类广义布尔函数的互相关函数以及自相关函数关系. 其次,利用所得自相关函数结论对一类广义 Bent 函数与 Bent 函数之间关系进行证明,并给出其平方和指标关系. 最后,对文章的研究进行总结与展望. 所得结果,对于利用相关函数研究广义布尔函数 $f:Z_2^n \to Z_8$ 提供一定的理论支持.

2　符号说明与相关定义

2.1　符号说明

整数集、实数集和复数集分别用 Z、R 和 C 表示,模 q 的剩余类环表示为 Z_q. Z_2 上 n 维向量空间用 Z_2^n 表示,$+$ 为 Z、R 和 C 上数的加法运算和模 q 的加法运算,$\oplus$ 为 Z_2^n 上向量的加法运算和 Z_2 上加法运算.

设 n 维空间向量

$$\boldsymbol{x} = (x_1, x_2, \cdots, x_n),$$

$$\boldsymbol{y} = (y_1, y_2, \cdots, y_n),$$

有

$$\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 \oplus x_2 y_2 \oplus \cdots \oplus x_n y_n.$$

设复数 $z = a + b\mathrm{i}$, $|z| = \sqrt{a^2 + b^2}$, z 的共轭复数记为 $\bar{z} = a - b\mathrm{i}$,其中 $a, b \in R$, $\mathrm{i}^2 = -1$.

设从 $Z_2^n \to Z_2$ 的函数 f 称为布尔函数,记 B_n 为 $Z_2^n \to Z_2$ 的全体函数,则 $f \in B_n$. 从 $Z_2^n \to Z_q$ 的函数 f 称为广义布尔函数,记 gB_n^q 为 $Z_2^n \to Z_q$ 的全体函数,则 $f \in gB_n^q$,其中 $q \geq 2$, $q \in Z$.

2.2　相关定义

定义 1　设 $f \in B_n$,那么函数 f 在任意点 $\boldsymbol{u} \in Z_2^n$ 的 Walsh-Hadamard 变换为

$$W_f(\boldsymbol{u}) = 2^{-n/2} \sum_{\boldsymbol{x} \in Z_2^n} (-1)^{f(\boldsymbol{x})} (-1)^{\boldsymbol{u} \cdot \boldsymbol{x}}.$$

定义 2　设 $f, g \in B_n$,那么函数 f 与 g 在任意点 $\boldsymbol{u} \in Z_2^n$ 的互相关函数为

$$C_{f,g}(\boldsymbol{u}) = \sum_{\boldsymbol{x} \in Z_2^n} (-1)^{f(\boldsymbol{x}) \oplus g(\boldsymbol{x} \oplus \boldsymbol{u})},$$

函数 f 在任意点 $\boldsymbol{u} \in Z_2^n$ 的自相关函数为 $C_{f,f}(\boldsymbol{u})$,记为 $C_f(\boldsymbol{u})$.

定义 3[11] 设 $f \in gB_n^q$, $\zeta = \mathrm{e}^{2\pi \mathrm{i}/q}$,那么函数 f 在任意点 $\boldsymbol{u} \in Z_2^n$ 的(广义)Walsh-Hadamard 变换为复值函数,有

$$H_f(\boldsymbol{u}) = 2^{-n/2} \sum_{\boldsymbol{x} \in Z_2^n} \zeta^{f(\boldsymbol{x})} (-1)^{\boldsymbol{u} \cdot \boldsymbol{x}}.$$

定义 4[12] 设 $f, g \in gB_n^q$,那么函数 f 与 g 在任意点 $\boldsymbol{u} \in Z_2^n$ 的互相关函数为

$$C_{f,g}(\boldsymbol{u}) = \sum_{\boldsymbol{x} \in Z_2^n} \zeta^{f(\boldsymbol{x}) - g(\boldsymbol{x} \oplus \boldsymbol{u})},$$

函数 f 在任意点 $\boldsymbol{u} \in Z_2^n$ 的自相关函数为 $C_{f,f}(\boldsymbol{u})$,记为 $C_f(\boldsymbol{u})$. 特别的,当 $q = 8$ 时,记

$$\zeta = \frac{\sqrt{2}}{2}(1 + \mathrm{i}).$$

定义 5[13] 设 $f \in gB_n^q$,那么函数 f 的广义平方和指标为

$$\sigma_f = \sum_{\boldsymbol{u} \in Z_2^n} |C_f(\boldsymbol{u})|^2.$$

关于广义布尔函数和 Bent 有着丰富的理论研究成果,为方便起见,总结如下,具体可参见[14~17].

命题 1　下列结果成立

(1) 若函数 $f, g \in gB_n^q$,则有

$$\zeta^{f(\boldsymbol{x})} = 2^{-n/2} \sum_{\boldsymbol{u} \in Z_2^n} H_f(\boldsymbol{u}) (-1)^{\boldsymbol{u} \cdot \boldsymbol{x}}.$$

(2)若函数 $f, g \in gB_n^q$,则有

$$\sum_{\boldsymbol{u} \in Z_2^n} C_{f,g}(\boldsymbol{u}) (-1)^{\boldsymbol{u} \cdot \boldsymbol{x}} = 2^n H_f(\boldsymbol{x}) \overline{H_g(\boldsymbol{x})},$$

$$C_{f,g}(\boldsymbol{u}) = \sum_{\boldsymbol{x} \in Z_2^n} H_f(\boldsymbol{x}) \overline{H_g(\boldsymbol{x})} (-1)^{\boldsymbol{u} \cdot \boldsymbol{x}},$$

这里对任意 $\boldsymbol{u} \in Z_2^n$,有 $C_{f,g}(\boldsymbol{u}) = \overline{C_{g,f}(\boldsymbol{u})}$,因此 $C_f(\boldsymbol{u})$ 是实值函数.

(3)特别的,当 $f = g$ 时,有

$$C_f(\boldsymbol{u}) = \sum_{\boldsymbol{x} \in Z_2^n} |H_f(\boldsymbol{x})|^2 (-1)^{\boldsymbol{u} \cdot \boldsymbol{x}}.$$

(4)若函数 f 为广义 Bent 函数,当且仅当

$$C_f(\boldsymbol{u}) = \begin{cases} 0, & \text{if } \boldsymbol{u} \neq 0, \\ 2^n, & \text{if } \boldsymbol{u} = 0. \end{cases}$$

3　主要结果

定理 1　设函数 f 和 g 为 $Z_2^n \to Z_8$ 上广义布尔函数,有

$$f(\boldsymbol{x}) = a_1(\boldsymbol{x}) + b_1(\boldsymbol{x})2 + c_1(\boldsymbol{x})2^2,$$

$$g(\boldsymbol{x}) = a_2(\boldsymbol{x}) + b_2(\boldsymbol{x})2 + c_2(\boldsymbol{x})2^2,$$

这里 $a_i, b_i, c_i (i = 1, 2)$ 为 $Z_2^n \to Z_2$ 上布尔函数,那么函数 f 和 g 在 $\boldsymbol{u} \in Z_2^n$ 上的互相关函数为

$$\begin{aligned} C_{f,g}(\boldsymbol{u}) = {} & \left(\frac{1}{4} + \frac{\sqrt{2}}{8}\right)[C_{c_1,c_2}(\boldsymbol{u}) + C_{b_1+c_1,b_2+c_2}(\boldsymbol{u}) \\ & + \mathrm{i}(C_{c_1,b_2+c_2}(\boldsymbol{u}) - C_{b_1+c_1,c_2}(\boldsymbol{u}))] \\ & + \left(\frac{1}{4} - \frac{\sqrt{2}}{8}\right)[C_{a_1+c_1,a_2+c_2}(\boldsymbol{u}) + C_{a_1+b_1+c_1,a_2+b_2+c_2}(\boldsymbol{u}) \\ & + \mathrm{i}(C_{a_1+c_1,a_2+b_2+c_2}(\boldsymbol{u}) - C_{a_1+b_1+c_1,a_2+c_2}(\boldsymbol{u}))] \\ & + \frac{\sqrt{2}}{8}[C_{b_1+c_1,a_2+c_2}(\boldsymbol{u}) + C_{a_1+c_1,b_2+c_2}(\boldsymbol{u}) \\ & - C_{c_1,a_2+b_2+c_2}(\boldsymbol{u}) - C_{a_1+b_1+c_1,c_2}(\boldsymbol{u}) \\ & + \mathrm{i}(C_{c_1,a_2+c_2}(\boldsymbol{u}) + C_{b_1+c_1,a_2+b_2+c_2}(\boldsymbol{u}) \\ & - C_{a_1+c_1,c_2}(\boldsymbol{u}) - C_{a_1+b_1+c_1,b_2+c_2}(\boldsymbol{u}))]. \end{aligned}$$

同时,设 f 为 $Z_2^n \to Z_8$ 上广义布尔函数,有

$$f(\boldsymbol{x}) = a(\boldsymbol{x}) + b(\boldsymbol{x})2 + c(\boldsymbol{x})2^2,$$

这里 a, b, c 为 $Z_2^n \to Z_2$ 上布尔函数,那么函数 f 在 $\boldsymbol{u} \in Z_2^n$ 上的自相关函数为

$$C_f(\boldsymbol{u}) = \left(\frac{1}{4} + \frac{\sqrt{2}}{8}\right)(C_c(\boldsymbol{u}) + C_{b+c}(\boldsymbol{u}))$$

$$+\left(\frac{1}{4}-\frac{\sqrt{2}}{8}\right)(C_{a+c}(\boldsymbol{u})+C_{a+b+c}(\boldsymbol{u}))$$
$$+\frac{\sqrt{2}}{4}(C_{a+c,b+c}(\boldsymbol{u})-C_{c,a+b+c}(\boldsymbol{u})).$$

证明 由定义4

$$C_{f,g}(\boldsymbol{u})=\sum_{x\in Z_2^n}\zeta^{f(x)-g(x\oplus\boldsymbol{u})}.$$

当 $q=8$ 时,$\zeta=\frac{\sqrt{2}}{2}(1+\mathrm{i})$,应用公式

$$\zeta^{a-b}=\frac{1+(-1)^{a+b}}{2}+\frac{\sqrt{2}}{2}\left(\frac{1-(-1)^{a+b}}{2}+\frac{(-1)^b-(-1)^a}{2}\mathrm{i}\right),$$

这里 $a,b\in\{0,1\}$,可得

$$\begin{aligned}C_{f,g}(\boldsymbol{u})&=\sum_{x\in Z_2^n}\zeta^{f(x)-g(x\oplus\boldsymbol{u})}\\&=\sum_{x\in Z_2^n}\zeta^{a_1(x)-a_2(x\oplus\boldsymbol{u})}(\mathrm{i})^{b_1(x)-b_2(x\oplus\boldsymbol{u})}(-1)^{c_1(x)\oplus c_2(x\oplus\boldsymbol{u})}\\&=\sum_{x\in Z_2^n}\left[\frac{1+(-1)^{a_1(x)+a_2(x\oplus\boldsymbol{u})}}{2}+\frac{\sqrt{2}}{2}\cdot\left(\frac{1-(-1)^{a_1(x)+a_2(x\oplus\boldsymbol{u})}}{2}+\frac{(-1)^{a_2(x\oplus\boldsymbol{u})}-(-1)^{a_1(x)}}{2}\mathrm{i}\right)\right]\\&\quad\cdot(\mathrm{i})^{b_1(x)-b_2(x\oplus\boldsymbol{u})}(-1)^{c_1(x)\oplus c_2(x\oplus\boldsymbol{u})}.\end{aligned}$$

为方便起见,以下推导过程用 $a_1(\boldsymbol{x})=a_1$,$a_2(\boldsymbol{x}\oplus\boldsymbol{u})=a_2$,替代($b,c$ 类似),有

$$\begin{aligned}C_{f,g}(\boldsymbol{u})&=\sum_{x\in Z_2^n}\Big[\frac{1}{2}(\mathrm{i})^{b_1-b_2}(-1)^{c_1\oplus c_2}+\frac{1}{2}(\mathrm{i})^{b_1-b_2}(-1)^{a_1+c_1\oplus c_2+a_2}\\&\quad+\frac{\sqrt{2}}{4}(\mathrm{i})^{b_1-b_2}(-1)^{c_1\oplus c_2}-\frac{\sqrt{2}}{4}(\mathrm{i})^{b_1-b_2}(-1)^{a_1+c_1\oplus c_2+a_2}\\&\quad+\frac{\sqrt{2}\mathrm{i}}{4}(\mathrm{i})^{b_1-b_2}(-1)^{c_1\oplus c_2+a_2}-\frac{\sqrt{2}\mathrm{i}}{4}(\mathrm{i})^{b_1-b_2}(-1)^{a_1+c_1\oplus c_2},\end{aligned}$$

应用公式

$$\mathrm{i}^{a-b}=\frac{1+(-1)^{a+b}}{2}+\frac{(-1)^b-(-1)^a}{2}\mathrm{i},$$

这里 $a,b\in\{0,1\}$,可得

$$\begin{aligned}&C_{f,g}(\boldsymbol{u})\\&=\frac{1}{2}\sum_{x\in Z_2^n}\left[\frac{1+(-1)^{b_1+b_2}}{2}+\frac{(-1)^{b_2}-(-1)^{b_1}}{2}\mathrm{i}\right](-1)^{c_1\oplus c_2}\\&\quad+\frac{1}{2}\sum_{x\in Z_2^n}\left[\frac{1+(-1)^{b_1+b_2}}{2}+\frac{(-1)^{b_2}-(-1)^{b_1}}{2}\mathrm{i}\right](-1)^{a_1+c_1\oplus c_2+a_2}\\&\quad+\frac{\sqrt{2}}{4}\sum_{x\in Z_2^n}\left[\frac{1+(-1)^{b_1+b_2}}{2}+\frac{(-1)^{b_2}-(-1)^{b_1}}{2}\mathrm{i}\right](-1)^{c_1\oplus c_2}\\&\quad-\frac{\sqrt{2}}{4}\sum_{x\in Z_2^n}\left[\frac{1+(-1)^{b_1+b_2}}{2}+\frac{(-1)^{b_2}-(-1)^{b_1}}{2}\mathrm{i}\right](-1)^{a_1+c_1\oplus c_2+a_2}\\&\quad+\frac{\sqrt{2}\mathrm{i}}{4}\sum_{x\in Z_2^n}\left[\frac{1+(-1)^{b_1+b_2}}{2}+\frac{(-1)^{b_2}-(-1)^{b_1}}{2}\mathrm{i}\right](-1)^{c_1\oplus c_2+a_2}\\&\quad-\frac{\sqrt{2}\mathrm{i}}{4}\sum_{x\in Z_2^n}\left[\frac{1+(-1)^{b_1+b_2}}{2}+\frac{(-1)^{b_2}-(-1)^{b_1}}{2}\mathrm{i}\right](-1)^{a_1+c_1\oplus c_2}\\&=\frac{1}{2}\sum_{x\in Z_2^n}\Big[\frac{1}{2}\cdot(-1)^{c_1\oplus c_2}+\frac{1}{2}\cdot(-1)^{b_1+c_1\oplus c_2+b_2}+\frac{\mathrm{i}}{2}(-1)^{c_1\oplus c_2+b_2}-\frac{\mathrm{i}}{2}(-1)^{b_1+c_1\oplus c_2}\Big]\\&\quad+\frac{1}{2}\sum_{x\in Z_2^n}\Big[\frac{1}{2}\cdot(-1)^{a_1+c_1\oplus c_2+a_2}+\frac{1}{2}\cdot(-1)^{a_1+b_1+c_1\oplus c_2+a_2+b_2}+\frac{\mathrm{i}}{2}(-1)^{a_1+c_1\oplus c_2+a_2+b_2}-\frac{\mathrm{i}}{2}(-1)^{a_1+b_1+c_1\oplus c_2+a_2}\Big]\\&\quad+\frac{\sqrt{2}}{4}\sum_{x\in Z_2^n}\Big[\frac{1}{2}\cdot(-1)^{c_1\oplus c_2}+\frac{1}{2}\cdot(-1)^{b_1+c_1\oplus c_2+b_2}+\frac{\mathrm{i}}{2}(-1)^{c_1\oplus c_2+b_2}-\frac{\mathrm{i}}{2}(-1)^{b_1+c_1\oplus c_2}\Big]\\&\quad-\frac{\sqrt{2}}{4}\sum_{x\in Z_2^n}\Big[\frac{1}{2}\cdot(-1)^{a_1+c_1\oplus c_2+a_2}+\frac{1}{2}\cdot(-1)^{a_1+b_1+c_1\oplus c_2+a_2+b_2}+\frac{\mathrm{i}}{2}(-1)^{a_1+c_1\oplus c_2+a_2+b_2}-\frac{\mathrm{i}}{2}(-1)^{a_1+b_1+c_1\oplus c_2+a_2}\Big]\\&\quad+\frac{\sqrt{2}\mathrm{i}}{4}\sum_{x\in Z_2^n}\Big[\frac{1}{2}\cdot(-1)^{c_1\oplus c_2+a_2}+\frac{1}{2}\cdot(-1)^{b_1+c_1\oplus c_2+a_2+b_2}+\frac{\mathrm{i}}{2}(-1)^{c_1\oplus c_2+a_2+b_2}-\frac{\mathrm{i}}{2}(-1)^{b_1+c_1\oplus c_2+a_2}\Big]\\&\quad-\frac{\sqrt{2}\mathrm{i}}{4}\sum_{x\in Z_2^n}\Big[\frac{1}{2}\cdot(-1)^{a_1+c_1\oplus c_2}+\frac{1}{2}\cdot(-1)^{a_1+b_1+c_1\oplus c_2+b_2}+\frac{\mathrm{i}}{2}(-1)^{a_1+c_1\oplus c_2+b_2}-\frac{\mathrm{i}}{2}(-1)^{a_1+b_1+c_1\oplus c_2}\Big]\\&=\frac{1}{4}C_{c_1,c_2}(\boldsymbol{u})+\frac{1}{4}C_{b_1+c_1,c_2+b_2}(\boldsymbol{u})+\frac{\mathrm{i}}{4}C_{c_1,c_2+b_2}(\boldsymbol{u})-\frac{\mathrm{i}}{4}C_{b_1+c_1,c_2}(\boldsymbol{u})+\frac{1}{4}C_{a_1+c_1,c_2+a_2}(\boldsymbol{u})\\&\quad+\frac{1}{4}C_{b_1+a_1+c_1,c_2+a_2+b_2}(\boldsymbol{u})+\frac{\mathrm{i}}{4}C_{a_1+c_1,c_2+a_2+b_2}(\boldsymbol{u})-\frac{\mathrm{i}}{4}C_{b_1+a_1+c_1,c_2+a_2}(\boldsymbol{u})+\frac{\sqrt{2}}{8}C_{c_1,c_2}(\boldsymbol{u})\\&\quad+\frac{\sqrt{2}}{8}C_{b_1+c_1,c_2+b_2}(\boldsymbol{u})+\frac{\sqrt{2}\mathrm{i}}{8}C_{c_1,c_2+b_2}(\boldsymbol{u})-\frac{\sqrt{2}\mathrm{i}}{8}C_{b_1+c_1,c_2}(\boldsymbol{u})-\frac{\sqrt{2}}{8}C_{a_1+c_1,c_2+a_2}(\boldsymbol{u})\\&\quad-\frac{\sqrt{2}}{8}C_{b_1+a_1+c_1,c_2+a_2+b_2}(\boldsymbol{u})-\frac{\sqrt{2}\mathrm{i}}{8}C_{a_1+c_1,c_2+a_2+b_2}(\boldsymbol{u})+\frac{\sqrt{2}\mathrm{i}}{8}C_{b_1+a_1+c_1,c_2+a_2}(\boldsymbol{u})+\frac{\sqrt{2}\mathrm{i}}{8}C_{c_1,c_2+a_2}(\boldsymbol{u})\end{aligned}$$

$$+\frac{\sqrt{2}\mathrm{i}}{8}C_{b_1+c_1,c_2+a_2+b_2}(\boldsymbol{u})-\frac{\sqrt{2}}{8}C_{c_1,c_2+a_2+b_2}(\boldsymbol{u})$$
$$+\frac{\sqrt{2}}{8}C_{b_1+c_1,c_2+a_2}(\boldsymbol{u})-\frac{\sqrt{2}\mathrm{i}}{8}C_{a_1+c_1,c_2}(\boldsymbol{u})$$
$$-\frac{\sqrt{2}\mathrm{i}}{8}C_{b_1+a_1+c_1,c_2+b_2}(\boldsymbol{u})+\frac{\sqrt{2}}{8}C_{a_1+c_1,c_2+b_2}(\boldsymbol{u})$$
$$-\frac{\sqrt{2}}{8}C_{b_1+a_1+c_1,c_2}(\boldsymbol{u})$$
$$=\left(\frac{1}{4}+\frac{\sqrt{2}}{8}\right)[C_{c_1,c_2}(\boldsymbol{u})+C_{b_1+c_1,b_2+c_2}(\boldsymbol{u})$$
$$+\mathrm{i}(C_{c_1,b_2+c_2}(\boldsymbol{u})-C_{b_1+c_1,c_2}(\boldsymbol{u}))]$$
$$+\left(\frac{1}{4}-\frac{\sqrt{2}}{8}\right)[C_{a_1+c_1,a_2+c_2}(\boldsymbol{u})+C_{a_1+b_1+c_1,a_2+b_2+c_2}(\boldsymbol{u})$$
$$+\mathrm{i}(C_{a_1+c_1,a_2+b_2+c_2}(\boldsymbol{u})-C_{a_1+b_1+c_1,a_2+c_2}(\boldsymbol{u}))]$$
$$+\frac{\sqrt{2}}{8}[C_{b_1+c_1,a_2+c_2}(\boldsymbol{u})+C_{a_1+c_1,b_2+c_2}(\boldsymbol{u})$$
$$-C_{c_1,a_2+b_2+c_2}(\boldsymbol{u})-C_{a_1+b_1+c_1,c_2}(\boldsymbol{u})$$
$$+\mathrm{i}(C_{c_1,a_2+c_2}(\boldsymbol{u})+C_{b_1+c_1,a_2+b_2+c_2}(\boldsymbol{u})$$
$$-C_{a_1+c_1,c_2}(\boldsymbol{u})-C_{a_1+b_1+c_1,b_2+c_2}(\boldsymbol{u}))].$$

当 $f=g$ 时,可得函数 f 的自相关函数为

$$C_f(\boldsymbol{u})=\left(\frac{1}{4}+\frac{\sqrt{2}}{8}\right)(C_c(\boldsymbol{u})+C_{b+c}(\boldsymbol{u}))$$
$$+\left(\frac{1}{4}-\frac{\sqrt{2}}{8}\right)(C_{a+c}(\boldsymbol{u})+C_{a+b+c}(\boldsymbol{u}))$$
$$+\frac{\sqrt{2}}{4}(C_{a+c,b+c}(\boldsymbol{u})-C_{c,a+b+c}(\boldsymbol{u})).$$

通过上述自相关函数关系,这里给出函数 f 为广义布尔 Bent 函数的两个充分条件:当 n 为偶数时,对任意的 $\boldsymbol{u}\in Z_2^n$

条件 1:若函数 $c,a+c,b+c,a+b+c$ 为布尔 Bent 函数,且 $C_{b+c,a+c}(\boldsymbol{u})=C_{c,a+b+c}(\boldsymbol{u})$,那么函数 f 为广义布尔 Bent 函数;

条件 2:若函数 $c,b+c$ 为布尔 Bent 函数且 $a=b$,那么函数 f 为广义布尔 Bent 函数.

设 $n=2k$,构造 F_{2^k} 和 F_2^k 间的一个同构,并将置换多项式 m_F 表示为从 $F_2^k\to F_2^k$ 的映射,对任意的 $\boldsymbol{x},\boldsymbol{y}\in F_2^k$,定义

$$a(\boldsymbol{x},\boldsymbol{y})=b(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{x}\cdot\boldsymbol{y},$$
$$c(\boldsymbol{x},\boldsymbol{y})=m_F(\boldsymbol{x})\cdot\boldsymbol{y},$$

这里满足充分条件 2,置换多项式 m_F 是与 Maiorana-McFarland 类布尔 Bent 函数 $c,a+c,b+c,a+b+c$ 存在关联的完全映射多项式. 即对任意 $\boldsymbol{u},\boldsymbol{v}\in F_2^k$,有

$$C_{a+c}(\boldsymbol{u},\boldsymbol{v})=C_{b+c}(\boldsymbol{u},\boldsymbol{v}),C_{a+c}(\boldsymbol{u},\boldsymbol{v})=0.$$
$$C_c(\boldsymbol{u},\boldsymbol{v})=C_{a+b+c}(\boldsymbol{u},\boldsymbol{v}),C_{c,a+b+c}(\boldsymbol{u},\boldsymbol{v})=0.$$

具体可参见文献[11]中例 21.

同时,对于广义布尔函数 $f\in gB_n^8$ 的自相关函数关系进行研究得到以下结果,当 $a(\boldsymbol{x})=0$ 时,有

$$C_f(\boldsymbol{u})=\left(\frac{1}{4}+\frac{\sqrt{2}}{8}\right)(C_c(\boldsymbol{u})+C_{b+c}(\boldsymbol{u}))$$
$$+\left(\frac{1}{4}-\frac{\sqrt{2}}{8}\right)(C_c(\boldsymbol{u})+C_{b+c}(\boldsymbol{u}))$$
$$+\frac{\sqrt{2}}{4}(C_{c,b+c}(\boldsymbol{u})-C_{c,b+c}(\boldsymbol{u})),$$

即

$$C_f(\boldsymbol{u})=\frac{1}{2}(C_c(\boldsymbol{u})+C_{b+c}(\boldsymbol{u})).$$

利用上述自相关函数关系,可得以下结论.

定理 2　若 n 是任意正偶数,设 f 为 $Z_2^n\to Z_8$ 上广义布尔函数,a,b,c 为 $Z_2^n\to Z_2$ 上的布尔函数,当 $a(\boldsymbol{x})=0$ 时,对任意的 $\boldsymbol{x}\in Z_2^n,\boldsymbol{u}\in Z_2^n$,有

$$f(\boldsymbol{x})=b(\boldsymbol{x})2+c(\boldsymbol{x})2^2,$$

则下列结果等价

(1) 广义布尔函数是 f 广义 Bent 函数;

(2)两个 n 变元的布尔函数 c 和 $b+c$ 都是 Bent 函数.

证明　设 f 为 $Z_2^n\to Z_8$ 上广义布尔函数,若 f 是广义 Bent 函数,由命题 1(4)

$$C_f(\boldsymbol{u})=\begin{cases}0, & \text{if } \boldsymbol{u}\neq 0,\\ 2^n, & \text{if } \boldsymbol{u}=0.\end{cases}$$

当 $\boldsymbol{u}\neq 0$ 时,得函数 c 与 $b+c$ 的自相关函数关系

$$\frac{1}{2}(C_c(\boldsymbol{u})+C_{c+b}(\boldsymbol{u}))=0,$$

所以,c 与 $c+b$ 是 Bent 函数. 反之,若 c 与 $c+b$ 都是 Bent 函数,则 f 是广义 Bent 函数,结论得证.

同时,平方和指标的研究在布尔函数中也是较为重要的. 因此,通过广义布尔函数自相关函数与平方和指标间的相互关系,可以得到下面结论.

定理 3　设函数 f 为 $Z_2^n\to Z_8$ 上广义布尔函数,a,b,c 为 $Z_2^n\to Z_2$ 上的布尔函数,当 $a(\boldsymbol{x})=0$ 时,对任意的 $\boldsymbol{x}\in Z_2^n,\boldsymbol{u}\in Z_2^n$,有

$$f(\boldsymbol{x})=b(\boldsymbol{x})2+c(\boldsymbol{x})2^2,$$

则函数 f 的平方和指标为

$$\sigma_f=\frac{1}{4}\sigma_c(\boldsymbol{u})+\frac{1}{4}\sigma_{c+b}(\boldsymbol{u})+\frac{1}{2}\sum_{\boldsymbol{u}\in Z_2^n}C_b(\boldsymbol{u})C_{c+b}(\boldsymbol{u}).$$

推论 1　若函数 c 与 $c+b$ 都为布尔 Bent 函数,那么 f 是广义 Bent 函数.

证明　由定义 5

$$\sigma_f=\sum_{\boldsymbol{u}\in Z_2^n}|C_f(\boldsymbol{u})|^2,$$

则

$$\sigma_f=\frac{1}{4}\sigma_c(\boldsymbol{u})+\frac{1}{4}\sigma_{c+b}(\boldsymbol{u})+\frac{1}{2}\sum_{\boldsymbol{u}\in Z_2^n}C_b(\boldsymbol{u})C_{c+b}(\boldsymbol{u}).$$

当 c 与 $c+b$ 为布尔 Bent 函数时,其平方和指标为

$$\sigma_c(\boldsymbol{u}) = \sigma_{c+b}(\boldsymbol{u}) = 2^{2n},$$

所以

$$\sigma_f = 2^{2n},$$

因此,函数 f 是广义 Bent 函数,结论得证.

4 结论

本文利用广义 Walsh-Hadamard 变换、相关函数以及平方和指标的相关定义,得到一类在 $Z_2^n \to Z_8$ 上的广义布尔函数的互相关函数和自相关函数关系. 利用所得结论,证明一类广义 Bent 函数与 Bent 函数之间的关系及其平方和指标关系. 所得结论对利用相关函数研究 $Z_2^n \to Z_8$ 上广义布尔函数起到一定的作用. 与此同时,广义布尔函数 f 在 $Z_2^n \to Z_q$ 上的更多性质仍有待研究,布尔函数的特殊构造也是当前学者研究的热点,例如具有优良的密码学性质的布尔函数构造、Bent 函数的构造等具有非常重要的研究意义.

参考文献

[1] CUSICK T W, STANICA P. Cryptographic Boolean Functions and Applications [M]. USA: Elsevier Academic Press, 2009. 86 – 100.

[2] Chen L, Liu J. On nonlinearity of S-Boxes and their related binary codes [J]. Chinese Journal of Electronics, 2016, 25(1): 167 – 173.

[3] SCHMIDT K. Quaternary constant-amplitude codes for multi-code CDMA [J]. IEEE Transactions on Information Theory, 2009, 55(4): 1824 – 1832.

[4] SCHMIDT K. Z4-valued quadratic forms and quaternary sequence families [J]. IEEE Transactions on Information Theory 2009, 55(12): 5803 – 5810.

[5] 张卫国,肖国镇. 具有偶数个变元的高非线性度平衡布尔函数的构造[J]. 电子学报,2011,39(03):727 – 728.
ZHANG W G, XIAO G Z. Construction of highly nonlinear balanced boolean functions with even number of Arguments [J]. Acta Electronica Sinica, 2011, 39(03): 727 – 728. (in Chinese)

[6] 杨小龙,胡红钢. Bent 函数的构造方法研究[J]. 密码学报,2015,2(5):404 – 438.
YANG X L, HU H G. A survey of constructions on Bent functions [J]. Journal of Cryptologic Research, 2015, 2(5): 404 – 438. (in Chinese)

[7] TOKAREVA N N. Generalizations of Bent functions A surver [J]. Journal of Applied and Industrial Mathematics, 2011, 5(1): 110 – 129.

[8] STANICA P, GANGOPADHYAY S, SINGH B K. Some results concerning generalized bent functions [EB/OL]. http://eprint. iacr. org/2011/290, 2019-03-02.

[9] Zhuo Z P, Chong J F, Wei S M. Some properties correlation functions on generalized Boolean functions [J]. Chinese Journal of Electronics, 2015, 24(1): 166 – 169.

[10] SOLE P, TOKAREVA N. Connections between quaternary and binary Bent functions [EB/OL]. http://eprint. icar. org/2009 /544, 2019-03-04.

[11] STANICA P, MARTINSEN T, GANGOPADHYAY S, et al. Bent and generalized Bent Boolean functions [J]. Designs Codes and Cryptography, 2013, 69(1): 77 – 94.

[12] Zhuo Z P. On cross correlation properties of boolean functions [J]. International Journal of Computer Mathematics, 2011, 88(10): 2035 – 2014.

[13] Zhou Y. Characterization of a balanced Boolean function with the minimum of the sum-of-square indicator [J]. Journal of Cryptologic Research, 2015, 2(1): 17 – 26.

[14] Zhang F R, Xia S X, STANICA P, Zhou Y. Further results on constructions of generalized bent Boolean functions [J]. Science China Information Sciences, 2016, 59(5): 1 – 3.

[15] Zhang F R, PASALIC E, Wei Y Z. Construction Bent functions outside the Maiorana-McFarland class using a general form of rothaus [J]. IEEE Transactions on Information Theory, 2017, 63(8): 5336 – 5349.

[16] SINGH B K. Secondary constructions on generalized Bent functions [EB/OL]. Available at http://eprint. icar. org/2012/017, 2019-03-09.

[17] Zhang F R, PASALIC E, Wei Y Z. Large sets of disjoint spectra plateaued functions inequivalent to partially linear functions [J]. IEEE Transactions on Information Theory, 2018, 64(4): 2987 – 2999.

作者简介

杨志耀 男,1995 年 6 月出生,安徽淮南人. 现为淮北师范大学数学科学学院硕士生,研究方向为密码学、信息安全.
E-mail:1782884933@qq.com

卓泽朋(通信作者) 男,1978 年 10 月出生,安徽灵璧人. 现为淮北师范大学教授. 研究领域为密码学、信息安全.
E-mail:zzp781021@sohu.com

崇金凤 女,1979 年 10 月出生,安徽天长人,现为淮北师范大学副教授,研究方向为密码学、信息安全.