Spectrum Distribution Characteristics of *k*th-Order Generalized Quasi-*Bent* Functions over Ring Z_p

Teng Ji-hong, Huang Xiao-ying, Li Xin-ran, Zhang Xi-yong

PLA Information Engineering University, Zhengzhou 450002, China
Email address: *tengjihong@263.net*

Abstract: Nonlinearity criterion is one of the most important criteria of nonlinear combined functions in the design of Cryptographic system, and it is necessary to investigate the nonlinearity of *k*th-order generalized quasi-*Bent* functions over ring Z_p in order to study its application to Cryptography and coding theory. In this paper, the spectrum distribution characteristics of *k*th-order generalized quasi-*Bent* functions over ring Z_p is proposed by using the knowledge of algebraic number theory, followed by the coincide ratio of such functions with all affine functions. The results in the paper offer much reference in the further study of the application of *k*th-order generalized quasi-*Bent* functions over ring Z_p in the fields of Cryptography design and coding theory.

Keywords: *k*th-order generalized quasi-*Bent* functions; *Chrestenson* cyclic spectrum；nonlinearity criterion; algebraic integers;

环 Z_p 上 *k* 阶广义拟 *Bent* 函数的谱分布特性

滕吉红　黄晓英　李信然　张习勇

解放军信息工程大学　中国郑州　450002

【摘要】 在密码体制的设计中，非线性度是衡量非线性组合函数安全性的一个重要指标，环 Z_p 上的 *k* 阶广义拟 *Bent* 函数作为一类重要的逻辑函数，为研究它在密码和编码中的应用价值，就要考察其非线性度问题。本文利用代数数论的知识给出了环 Z_p 上 *k* 阶广义拟 *Bent* 函数的 *Chrestenson* 循环谱的取值分布特性，进一步考察了 *p* 值 *k* 阶广义拟 *Bent* 函数与所有仿射函数的符合率，由此说明了环 Z_p 上 *k* 阶广义拟 *Bent* 函数也是一类近似稳定的逻辑函数，为进一步研究它在密码和编码中的应用提供了理论基础。

【关键词】 *k* 阶广义拟 *Bent* 函数；*Chrestenson* 循环谱；非线性度；代数整数;

1. 引言

通信保密的实现方法之一是对需要发送的明文进行加密 ，其安全性在很大程度上取决于生成密钥流序列的非线性组合器的安全性。目前根据不同的攻击方法，判定非线性组合器安全性有一系列标准，如非线性组合函数必须有高的代数次数、高的非线性度、一定阶的相关免疫性和一定次数的扩散性等等[1]，依据上述准则，密码设计者设计了大量的非线性组合函数。但由于这些准则之间存在着一定的制约关系[2]，因此要设计出兼顾各种性质的非线性组合函数是有一定难度的。其中，*Bent* 函数[3]由于非线性度达到最大、稳定性强而备受关注。但这类函数不具有平衡性和相关免疫性，为弥补 *Bent* 函数的这一不足，C.Carlet 提出了部分 *Bent* 函数的概念[4]，这类函数可以具有平衡性、相关免疫性和一定次数的扩散性，但所有的非仿射的部分 *Bent* 函数都可以通过 *Bent* 函数来构造[5]，因此它的某些性质也收到了限制。

后来，文献[6]提出了 *k* 阶拟 *Bent* 函数的概念，这类函数是包含 *Bent* 函数、部分 Bent 函数的更大的函数类。随后的研究发现 *k* 阶拟 *Bent* 函数具有特殊的密码学性质[7]，因而在密码和通信领域具有广泛应用[8]；文献[9]、[10]又分别将拟 *Bent* 函数的概念推广到环 Z_p 上和有限域 F_q($q = p^l$, *p* 为素数)上，给出了 *k* 阶广义拟 *Bent* 函数的定义以及等价判别条件。由定义可知环 Z_p 上 *k* 阶广义拟 *Bent* 函数的 *Chrestenson* 循环谱的模的平方要
么为 0，要么是一非零常数。但是 *k* 阶广义拟 *Bent* 函数的 *Chrestenson* 循环谱取值的分布特性并不能从定义中直接看出，因此很难考察 *p* 值 *k* 阶广义拟 *Bent* 函数的非线性度，而非线性度是逻辑函数的一个非常重要的密码学性质。

本文利用代数数论的相关知识，讨论了环 Z_p 上 *k* 阶广义拟 *Bent* 函数的 *Chrestenson* 循环谱的取值分布特性，进一步考察了 *p* 值 *k* 阶广义拟 *Bent* 函数与所有仿射函数的符合率。特殊地，当 *k*=0 时，所得结论即为广义 *Bent* 函数的 *Chrestenson* 循环谱的取值分布特性以及广义 *Bent* 函数与所有仿射函数的符合率，与文献[11]、[12]的结论相一致，从而为考察环 Z_p 上 *k* 阶

国家自然科学基金资助项目（批准号：60803154）

978-1-935068-01-3 © 2009 SciRes.

广义拟 *Bent* 函数的非线性度提供了理论基础。

2. 基本知识

定义 1[12] 设 $f(x)$，$x \in Z_p^n$ 为一个 n 元 p 值逻辑函数，称

$$S_{(f)}(w)=\frac{1}{p^n}\sum_{x\in Z_p^n} u^{f(x)-w\cdot x}\ ,\quad w\in Z_p^n$$

为 $f(x)$ 的 *Chrestenson* 循环谱，其中 u 为 p 次本原单位根。

定义 2[9] 称一个 p 值逻辑函数 $f(x)$，$x \in Z_p^n$ 为 n 元 k 阶广义拟 *Bent* 函数，如果其 *Chrestenson* 循环谱满足：$|S_{(f)}(w)|^2=0$ 或 $\frac{1}{p^{n-k}}$，$w \in Z_p^n$.

如果不强调 n 元 k 阶广义拟 *Bent* 函数的阶数，称其为广义拟 *Bent* 函数。k=0 时，即为广义 *Bent* 函数[11].

以下有关代数数论方面的知识见文献[13]:

记 $Q(u)$ 为由 u 生成的分圆域，其中 u 为 p 次本原单位根。记 G 为 $Gal(Q(u)/Q)$，σ^*，$\sigma_k \in G$，且 $\sigma_k(u)=u^k$，$\sigma^*(u)=u^{-1}$。又记 $Q(u)$ 上的代数整数环为 B，则 $B=Z[u]$，$B[p]$ 为 p 在 B 中生成的理想.

引理 1[13] 若 $\alpha \in Q(u)$ 为代数整数，则 $|\alpha|$=1 的充要条件是 α 为单位根.

引理 2[13] $B[p]=[1-u]^{p-1}$，其中 $[1-u]$ 为 $1-u$ 在 B 中生成的素理想. 记

$$G_p=\{\sigma\in G:\sigma([1-u])=[1-u]\},$$

则 $\sigma^* \in G_p$.

引理 3[13] (1)若 $p\equiv 1 \bmod 4$，则 $\sqrt{p}\in Q(u)$；

(2)若 $p\equiv 3 \bmod 4$，则 $\sqrt{p}\in Q(\delta)\setminus Q(\gamma)$.

其中，δ 为 $4p$ 次本原单位根，γ 为 $2p$ 次本原单位根.

定义 3[13] 设 K 为数域，若 $\gamma \in K$，且存在 $n\geq 1$，使得 $\gamma^n=1$，则称 γ 为数域 K 中的单位根，数域 K 中的单位根的全体 W_K 称为数域 K 的单位根群.

引理 4[13] 设 ξ_n 为 n 次本原单位根，$K=Q(\xi_n)$，W_K 为数域 K 的单位根群，则

1) 当 $n=1 \bmod 2$ 时，

$$W_K=\{\xi_{2n}^k : 0\leq k\leq 2n-1\};$$

2) 当 $n=0 \bmod 2$ 时，

$$W_K=\{\xi_n^k : 0\leq k\leq n-1\}.$$

由引理 4 不难得到下面的结论：

引理 5 设 u 为 p 次本原单位根，γ 为 $2p$ 次本原单位根，δ 为 $4p$ 次本原单位根，则，

1) $Q(u)$ 中的单位根群

$$W_1=\{\gamma^l : 0\leq l\leq 2p-1\};$$

2) $Q(\gamma)$ 中的单位根群

$$W_2=\{\gamma^l : 0\leq l\leq 2p-1\};$$

3) $Q(\delta)$ 中的单位根群

$$W_3=\{\delta^l : 0\leq l\leq 4p-1\}.$$

引理 6[13] 设 u 是 p 次本原单位根，记 $G(p)=\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)u^j$，则

$$G(p)=\begin{cases}\sqrt{p}, & \text{若} p\equiv 1 \bmod 4;\\ i\sqrt{p}, & \text{若} p\equiv 3 \bmod 4.\end{cases}$$

3 主要结果

由定义 2 可知，p 值 k 阶广义拟 *Bent* 函数的 *Chrestenson* 循环谱的模的平方要么为 0，要么为一非零常数，但是其循环谱取值的分布特性并不能从定义中直接看出，这为我们考察 p 值 k 阶广义拟 *Bent* 函数的非线性度带来困难。下面我们利用代数数论的知识，讨论 p 值 k 阶广义拟 *Bent* 函数的循环谱分布特性.

定理 1 设 $f(x)$，$x \in Z_p^n$ 为 n 元 p 值逻辑函数，则 $f(x)$ 是 k 阶广义拟 *Bent* 函数的充分必要条件是 $f(x)$ 的 *Chrestenson* 循环谱满足：对任意的 $w \in Z_p^n$，

1) 若 $n-k$ 为偶数，则

$$S_{(f)}(w)\in\{0,\pm\frac{1}{p^{\frac{n-k}{2}}},\ \pm\frac{u}{p^{\frac{n-k}{2}}}\cdots\cdots,\ \pm\frac{u^{p-1}}{p^{\frac{n-k}{2}}}\};$$

2) 若 $n-k$ 为奇数且 $p\equiv 1 \bmod 4$，则

$$S_{(f)}(w)\in\{0,\pm\frac{1}{p^{\frac{n-k}{2}}},\ \pm\frac{u}{p^{\frac{n-k}{2}}}\cdots\cdots,\ \pm\frac{u^{p-1}}{p^{\frac{n-k}{2}}}\};$$

3) 若 $n-k$ 为奇数且 $p\equiv 3 \bmod 4$，则

$$S_{(f)}(w)\in\{0,\pm\frac{i}{p^{\frac{n-k}{2}}},\ \pm\frac{iu}{p^{\frac{n-k}{2}}}\cdots\cdots,\ \pm\frac{iu^{p-1}}{p^{\frac{n-k}{2}}}\}.$$

证明 充分性显然；下面证明必要性：

若 $S_{(f)}(w)=0$，显然；

否则，记 $S(w)=\sum_{x\in Z_p^n} u^{f(x)-w\cdot x}$，则

$$S(w)=p^n\ S_{(f)}(w),$$

显然 $S(w)\in Z[u]$ 是 $Q(u)$ 上的代数整数，由 k 阶广义拟 *Bent* 函数的定义知

$$S(w)\ \overline{S(w)}=p^{n+k},$$

即 $$S(w)\ \sigma^*(S(w))=p^{n+k},$$

而 $S(w)$ 和 $\sigma^*(S(w))$ 生成同一理想，因此 $[S^2(w)]=[p^{n+k}]$，所以 $S^2(w)/p^{n+k}$ 为一单位，即

$\frac{S(w)}{\sqrt{p^{n+k}}}$ 为代数整数，且$|\frac{S(w)}{\sqrt{p^{n+k}}}|=1$，

再由引理 1 知$\frac{S(w)}{\sqrt{p^{n+k}}}$ 为单位根，而由引理 3 及引理 5 知

1) 若 $n-k$ 为偶数，则存在 l，使得

$$\frac{S(w)}{\sqrt{p^{n+k}}}=\gamma^{l},$$

其中 γ 为 $2p$ 次本原单位根，因此

$$S_{(f)}(w)=\frac{\gamma^{l}}{\sqrt{p^{n-k}}}。$$

若 l 为偶数，即 $l=2l_1$，则 $S_{(f)}(w)=\frac{u^{l_1}}{\sqrt{p^{n-k}}}$，

若 $l=2l_1+1$，则

$$S_{(f)}(w)=\frac{\gamma^{2l_1+1}}{\sqrt{p^{n-k}}}=-\frac{\gamma^{p+2l_1+1}}{\sqrt{p^{n-k}}}=-\frac{u^{\frac{p+2l_1+1}{2}}}{\sqrt{p^{n-k}}}$$

2) 若 $n-k$ 为奇数，且 $p\equiv 1 \bmod 4$，则由引理 3 及引理 5 同上； 若 $n-k$ 为奇数，且 $p\equiv 3 \bmod 4$，则由引理 3 及引理 5 知

$$\frac{S(w)}{\sqrt{p^{n+k}}}=\delta^{2l+1},$$

所以由 $\delta^{p}=i$ 可知

$$S_{(f)}(w)=\frac{\delta^{2l+1}}{\sqrt{p^{n-k}}}=\frac{-i\delta^{p+2l+1}}{\sqrt{p^{n-k}}}=\frac{-i\gamma^{\frac{p+2l+1}{2}}}{\sqrt{p^{n-k}}}$$

$$=\begin{cases}\dfrac{-iu^{\frac{p+2l+1}{4}}}{\sqrt{p^{n-k}}}\hat{=}\dfrac{-iu^{l_1}}{\sqrt{p^{n-k}}} & \text{若}l\text{为偶数;}\\ \dfrac{iu^{\frac{p+2l+1+2p}{4}}}{\sqrt{p^{n-k}}}\hat{=}\dfrac{iu^{l_2}}{\sqrt{p^{n-k}}} & \text{若}l\text{为奇数.}\end{cases}$$

定理得证. #

逻辑函数的一个非常重要的密码学性质是其非线性度，它与逻辑函数循环谱的分布有着不可分割的关系。而环 Z_p 上逻辑函数的非线性度实质上是考察逻辑函数与所有仿射函数距离的远近，因此考察 p 值 k 阶广义拟 *Bent* 函数与所有仿射函数的符合率实质上就是考察 p 值 k 阶广义拟 *Bent* 函数的非线性度.

定理 2 设 $f(x)$， $x\in Z_p^n$ 为 n 元 p 值逻辑函数，则

1) 当 $n-k$ 为偶数， $f(x)$ 是 k 阶广义拟 *Bent* 函数的充分必要条件是对任意的 $w\in Z_p^n$，下列条件必有一个成立：

I. 对任意 $j\in Z_p$，有

$$P\{f(X)=w\cdot X+j\}=\frac{1}{p};$$

II. 存在唯一的 $j_0\in Z_p$，使得

$$P\{f(X)=w\cdot X+j_0\}=\frac{1}{p}\pm\frac{p-1}{p\cdot p^{\frac{n-k}{2}}},$$

而当 $j\in Z_p\setminus\{j_0\}$ 时，有

$$P\{f(X)=w\cdot X+j\}=\frac{1}{p}\mp\frac{1}{p\cdot p^{\frac{n-k}{2}}};$$

2) 当 $n-k$ 为奇数时， $f(x)$ 是 k 阶广义拟 *Bent* 函数的充分必要条件是对任意的 $w\in Z_p^n$，下列条件必有一个成立：

I. 对任意的 $j\in Z_p$，有

$$P\{f(X)=w\cdot X+j\}=\frac{1}{p},$$

II. 存在唯一的 $j_0\in Z_p$，使得

$$P\{f(X)=w\cdot X+j_0\}=\frac{1}{p},$$

而当 $j\in Z_p\setminus\{j_0\}$ 时，有

$$P\{f(X)=w\cdot X+j\}=\frac{1}{p}\pm\left(\frac{j-j_0}{p}\right)\cdot\frac{1}{p^{\frac{n-k+1}{2}}},$$

其中$\left(\frac{j-j_0}{p}\right)$为 *Legendre* 符号.

证明 记

$$n_i=|\{x:x\in Z_p^n,\ f(x)=w\cdot x+i\}|,$$

则由环 Z_p 上逻辑函数的 *Chrestenson* 循环谱的概率表示式可知：

$$S_{(f)}(w)=\frac{1}{p^n}(n_0+n_1u+\cdots+n_{p-1}u^{p-1}).$$

1) 当 $n-k$ 为偶数时，由定理 1 的(1)可知，

$$S_{(f)}(w)\in\{0,\pm\frac{1}{p^{\frac{n-k}{2}}},\ \pm\frac{u}{p^{\frac{n-k}{2}}}\cdots\cdots,\ \pm\frac{u^{p-1}}{p^{\frac{n-k}{2}}}\}$$

即或者

$$(n_0+n_1u+\cdots+n_{p-1}u^{p-1})=0$$

$$\Leftrightarrow n_0=n_1=\cdots=n_{p-1},$$

或者存在 $j\in Z_p$，使得

$$(n_0+n_1u+\cdots+n_{p-1}u^{p-1})=\pm p^{\frac{n+k}{2}}u^{j},$$

所以

$$n_0+n_1u+\cdots+n_{j-1}u^{j-1}+(n_j\mp p^{\frac{n+k}{2}})u^{j}+$$

978-1-935068-01-3 © 2009 SciRes.

$$+n_{j+1}u^{j+1}\cdots+n_{p-1}u^{p-1}=0$$

上式成立的充分必要条件是

$$n_0=\cdots=n_{j-1}=(n_j\mp p^{\frac{n+k}{2}})=n_{j+1}=\cdots=n_{p-1}$$

再由 $n_0+n_1+\cdots+n_{p-1}=p^n$ 即得结论.

2)当 $n-k$ 为奇数时，若 $p\equiv 1 \bmod 4$，则由定理 1 的 2) 可知或者

$$(n_0+n_1u+\cdots+n_{p-1}u^{p-1})=0$$

$$\Leftrightarrow n_0=n_1=\cdots=n_{p-1},$$

或存在 $j\in Z_p$，使得

$$(n_0+n_1u+\cdots+n_{p-1}u^{p-1})$$

$$=\pm p^{\frac{n+k}{2}}u^j=\pm p^{\frac{n+k-1}{2}}\sqrt{p}u^j,$$

再由引理 6 可知

$$(n_0+n_1u+\cdots+n_{p-1}u^{p-1})$$

$$=\pm p^{\frac{n+k-1}{2}}\sum_{l=1}^{p-1}\left(\frac{l}{p}\right)u^{l+j},$$

将上式合并同类项，所以

$$n_j+\sum_{l=1}^{p-1}[\mp p^{\frac{n+k-1}{2}}\left(\frac{l}{p}\right)+n_{l\oplus j}]u^{l+j}=0$$

($\oplus$ 是环 Z_p 中的运算)

而上式成立的充分必要条件是对任意的 $1\le l\le p-1$，有

$$n_j=\mp p^{\frac{n+k-1}{2}}\left(\frac{l}{p}\right)+n_{l\oplus j},$$

再由 $n_0+n_1+\cdots+n_{p-1}=p^n$ 即得结论;

当 $n-k$ 为奇数时，若 $p\equiv 3 \bmod 4$，同上面的方法，利用定理 1 和引理 6 可得结论. #

特别地，当 $k=0$ 时，p 值 k 阶广义拟 *Bent* 函数就是 p 值广义 *Bent* 函数，定理 1 和定理 2 的结论和文献[11]所给出的关于广义 *Bent* 函数与仿射函数符合率的结论是一致的.

4. 结束语

本文利用代数数论的相关知识给出了 p 值 k 阶广义拟 *Bent* 函数的循环谱分布特性以及这类函数与所有仿射函数的符合率。结果表明 p 值 k 阶广义拟 *Bent* 函数当 k 很小时是一类近似稳定的逻辑函数，下一步我们将进一步考察 p 值 k 阶广义拟 *Bent* 函数的非线性度以及这类函数在密码和编码领域的应用。

References (参考文献)

[1] W. Meier, O. Staffelbach. Nonlinearity Criteria for Cryptographic Functions[C], *Advances in Cryptology-EUROCRYPT'89*, pringer-Verlag, 1990, 434, 549−562.

[2] J. Seberry, X. M. Zhang, Y. Zheng. Relationships among Nonlinearity Criteria [C]. *Advances in Cryptology-EUROCRYPT'94*, Springer-Verlag, 1994, 950,376−388.

[3] O. S. Rothaus. on *Bent* Functions [J]. Journal of Combinatorial Theory, 1976, Ser. A 20, 300−305.

[4] C. Carlet. Partially-*Bent* Functions. *Advances in Cryptology-CRYPT'92*, Springer-Verlag, 1993, 740,280−291.

[5] Zhao Ya-qun, The Properties and Constructions of Partially Bent Functions and Generalized Partially Bent Functions [D]. Doctorate Thesis. Information Engineering University, 2000.
赵亚群，部分 *Bent* 函数和广义部分 *Bent* 函数的性质及构造[D],博士论文，解放军信息工程大学，2000.

[6] Liu Wen-fen, Li Shi-qu，Teng Ji-hong, The Properties of kth order quasi-Bent Functions and its Applications [C], The 7th Youth Communication Conference of China, Nanjing, 2001, 939−943.
刘文芬，李世取，滕吉红，*k* 阶拟 Bent 函数的性质和应用[C]，第七届全国青年通信学术会议，2001，939−943.

[7] Teng Ji-hong, Zhang Wen-ying, Li Shi-qu, The Matrix Characteristics of the Cryptographic Properties,of a Special Kind of kth-order quasi-Bent Functions[J], Journal of China Institute of Computer, 2004.
滕吉红，张文英，李世取，一类 *k* 阶拟 Bent 函数密码性质的矩阵特征[J]，计算机学报,2004.

[8] Teng Ji-hong,, Li Shi-qu, Liu Wen-fen, The Application of kth-order quasi-Bent Functions in Cryptology and Communication Fields[J], Journal of China Institute of Communications, 2004，24(12), ,58−66.
滕吉红，李世取，刘文芬，*k* 阶拟 Bent 函数在密码设计和通信中的应用[J]，通信学报，2004，24(12),58−66.

[9] TengJi-hong, Li Shi-qu, Huang Xiao-ying, The *k*th order quasi-Generalized *Bent* Functions over Ring Z_p[C], First SKLOIS Conference, Information Security and Cryptology, 2005, Beijing, LNCS 3822, 189−200.

[10] Huang Xiao-ying, Du Yi-bin, Teng Ji-hong, etc, On *k*th-order quasi-Generalized *Bent* Functions over F_q[J], Journal of Information Engineering University,2008, 9(8), 14−17.
黄晓英、杜宜宾、滕吉红，有限域 F_q 上的 *k* 阶广义拟 Bent 函数。信息工程大学学报，2008, 9(8), 14−17.

[11] P. V. Kumar, R. A. Scholtz, L. R. Welch, Generalized Bent functions and their Properties[J], Journal of Combinatorial Theory, 1985, 40 , 90−107.

[12] Li Shi-qu, Zeng Ben-sheng, Lian Yu-zhong, Logical Functions in Cryptology[M], Beijing, Publishing Company of Software and Eletronic Industry,2003.
李世取，曾本胜，廉玉忠等，密码学中的逻辑函数[M]，北京，中软电子出版社，2003.

[13] Feng Ke-qin, The Algebraic Number Theory[M], Beijing,
冯克勤，代数数论[M]，北京，科学出版社, 2000.