k-阶旋转对称函数性质分析与轨道计数

李泉，高光普，刘文芬
(信息工程大学 信息工程学院，河南 郑州 450002)

摘 要：研究了 *k*-阶旋转对称函数的性质，证明了 *k*-阶旋转对称函数的 Walsh 谱和自相关函数都满足 *k*-阶的旋转对称。分析发现 *k*-阶旋转对称函数的很多性质都可以利用其轨道来刻画，并给出了 *k*-阶旋转对称函数的轨道中的长圈和短圈的计数公式。

关键词：布尔函数；旋转对称；Walsh 谱；计数
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2012)01-0114-06

Analysis of properties and counting of orbits for *k*-rotation symmetric Boolean functions

LI Quan, GAO Guang-pu, LIU Wen-fen
(Institute of Information Engineering, Information Engineering University, Zhengzhou 450002, China)

Abstract: The properties of *k*-rotation symmetric Boolean functions (*k*-RSBF) were analyzed. It was presented that the Walsh spectrum and auto-correlation value were invariant when the parameters of a *k*-rotation symmetric Boolean function were under *k*-circular translation of indices were presented. The analysis of the properties showed that many properties of *k*-RSBF could be described by their orbits, and the counting formulas of long cycles and short cycles on *k*-RSBF' orbits were given.

Key words: Boolean functions; rotation symmetry; Walsh spectrum; counting

1 引言

1999 年，密码学者 Pieprzyk[1]在研究散列算法的快速实现时提出了旋转对称函数的概念。随着文献[2~6]等对旋转对称函数的进一步分析与研究后，发现这一类结构特殊的布尔函数可以具有良好的密码学性质，并且搜索旋转对称函数要比穷尽搜索布尔函数空间的效率要高，所以一直以来不断地通过改良搜索旋转对称函数空间的方法寻找密码学性质优良的布尔函数。2006 年，密码学者 Kavut 和 Yücel[4]利用最速下降法在旋转对称函数空间上搜索到的非线性度为 241 的 9 元布尔函数，随后 Kavut 和 Yücel[7]又证明了 241 为 9 元旋转对称函数所能达到的最高非线性度。为了得到更好的结果，2008 年，Kavut 和 Yücel[8]推广了旋转对称函数的概念，提出了 k -阶旋转对称函数，初步搜索出了 9 元非线性度为 242 的 3-阶旋转对称函数，并且利用该结论证明了 9 元、11 元、13 元非线性度大于 $2^{n-1}-2^{\frac{n-1}{2}}$ 的布尔函数都是存在的，彻底解决了这个提出近 30 年的公开问题。k -阶旋转对称函数比旋转对称函数对布尔函数代数结构的约束更低，所以数量更多，并且已经寻找到了比旋转对称函数密码学性质更为优良的布尔函数。

本文在 Kavut 和 Yücel 的基础上研究了 k -阶旋

收稿日期：2010-05-24；修回日期：2011-03-15
基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（2012CB315905, 2012CB315901）
Foundation Item: The National Basic Research Program of China (973 Program) (2012CB315905, 2012CB315901)

转对称函数的性质。首先，证明了 k -阶旋转对称函数的 Walsh 谱和自相关函数都满足 k -阶的旋转对称。分析发现 k -阶旋转对称函数的很多性质都可以利用其轨道来刻画，并给出了 k -阶旋转对称函数的轨道中的长圈和短圈的计数公式。特别取 $k=1$ 时，利用本文所得计数公式与 Sarkar 和 Maitra 所得的计数公式进行比较，发现 Sarkar 和 Maitra 所得的计数公式在 $n=p_1^{a_1}\perp p_l^{a_l}, l=2$ 且存在 $a_i\geq 2$，或 $l\geq 3$ 的情况下是不成立的，并分析了原因。

2　基本概念介绍

记二元域 $\{0,1\}$ 为 GF(2)，定义 $\mathrm{GF}^n(2)$ 到 GF(2) 上的函数 $f(x)=f(x_1,x_2,\perp,x_n)$，$x=(x_1,x_2,\perp,x_n)\in \mathrm{GF}^n(2)$ 为 n 元布尔函数。

定义 1[9]　n 元布尔函数 $f(x),\ x\in \mathrm{GF}^n(2)$ 的 Walsh 谱定义为

$$S_{(f)}(w)=\frac{1}{2^n}\sum_{x\in \mathrm{GF}^n(2)}(-1)^{f(x)+wx},\ w\in \mathrm{GF}^n(2)$$

定义 2[9]　设 $f(x),\ x\in \mathrm{GF}^n(2)$ 是 n 元布尔函数，对 $x=(x_1,x_2,\perp,x_n)\in \mathrm{GF}^n(2)$，$s=(s_1,s_2,\perp,s_n)\in \mathrm{GF}^n(2)$，称

$$r_f(s)=\frac{1}{2^n}\sum_{x\in \mathrm{GF}^n(2)}(-1)^{f(x+s)+f(x)},\ s\in \mathrm{GF}^n(2)$$

为 $f(x)$ 的自相关函数。

n 元布尔函数 f 的自相关函数 r_f 和 Walsh 谱 $S_{(f)}$ 有如下关系：

$$r_f(s)=\sum_{w\in \mathrm{GF}^n(2)}\left[S_{(f)}(w)\right]^2(-1)^{ws},\ s\in \mathrm{GF}^n(2)$$

定义 3[2]　对于任意给定的 $1\leq i\leq n, 1\leq k\leq n$，$x_i\in \mathrm{GF}(2)$ 定义

$$r_n^k(x_i)=\begin{cases}x_{i+k}, & i+k\leq n\\ x_{i+k-n}, & i+k>n\end{cases}$$

对于 $(x_1,x_2,\perp,x_n)\in \mathrm{GF}^n(2)$，定义

$$r_n^k(x_1,x_2,\perp,x_n)=(r_n^k(x_1),r_n^k(x_2),\perp,r_n^k(x_n))$$

可知，r_n^k 可视为 $(x_1,x_2,\perp,x_n)$ 的左循环移位算子。

定义 4[8]　对于给定的 $1\leq k\leq n, k\mid n$，n 元布尔函数 f 对任意输入的 $x=(x_1,x_2,\perp,x_n)\in \mathrm{GF}^n(2)$ 都满足：

$$f(r_n^k(x_1,\perp x_n))=f(x_1,\perp x_n)$$

则称 f 为 k -阶旋转对称函数(k -RSBF)。

注 $k=1$ 时 f 即为旋转对称函数。

定义 5[2]　对于给定的 $1\leq k\leq n, k\mid n$ 和 $(x_1,\perp x_n)\in \mathrm{GF}^n(2)$ 称

$$G_{n,k}(x_1,\perp x_n)=\{r_n^i(x_1,\perp x_n)\,|\,i=k,2k,\perp,n\}$$

为 k -阶旋转对称函数的轨道，简称为轨道。

由定义 4 可知，对任意的轨道 $G_{n,k}^j$，k -阶旋转对称函数限制在该轨道上取值为常数。将轨道个数记为 $g_{n,k}$。$G_{n,k}=\{r_n^i\,|\,i=k,2k,\perp,n\}$ 将 $\mathrm{GF}^n(2)$ 分成了 $g_{n,k}$ 个不相交的轨道 $G_{n,k}^j\ (0\leq j\leq g_{n,k})$。显然，$G_{n,k}^j$ 中元素的个数 $\left|G_{n,k}^j\right|\leq\frac{n}{k}$ 且都为 $\frac{n}{k}$ 的因子，称 $\left|G_{n,k}^j\right|=\frac{n}{k}$ 的轨道为长圈，其个数记为 $h_{n,k}$，称 $\left|G_{n,k}^j\right|=d\ \left(d<\frac{n}{k}, d\mid\frac{n}{k}\right)$ 的轨道为短圈，其个数记为 $s_{n,k}$。

设 $L_{(n,k),j}\in \mathrm{GF}^n(2)$ 表示 $G_{n,k}^j$ 中元素按字典序排列的第一个元素，称为轨道 $G_{n,k}^j$ 的代表元。k -阶旋转对称函数的输出序列可以由长为 $g_{n,k}$ 的比特序列

$$[f(L_{(n,k),1}),f(L_{(n,k),2}),\perp,f(L_{(n,k),g_{n,k}})]$$

给出，显然该序列包含着 k -阶旋转对称函数的全部信息。由该序列可知，变元个数为 n 的所有 k -阶旋转对称函数的个数为 $2^{g_{n,k}}$。

例 1　所有 4 元 2-阶旋转对称函数的轨道为

$G_{4,2}^0=G_{4,2}(L_{(4,2),0})=\{(0,0,0,0)\}$

$G_{4,2}^1=G_{4,2}(L_{(4,2),1})=\{(0,0,0,1),(0,1,0,0)\}$

$G_{4,2}^2=G_{4,2}(L_{(4,2),2})=\{(0,0,1,0),(1,0,0,0)\}$

$G_{4,2}^3=G_{4,2}(L_{(4,2),3})=\{(0,0,1,1),(1,1,0,0)\}$

$G_{4,2}^4=G_{4,2}(L_{(4,2),4})=\{(0,1,1,0),(1,0,0,1)\}$

$G_{4,2}^5=G_{4,2}(L_{(4,2),5})=\{(0,1,0,1)\}$

$G_{4,2}^6=G_{4,2}(L_{(4,2),6})=\{(1,0,1,0)\}$

$G_{4,2}^7=G_{4,2}(L_{(4,2),7})=\{(0,1,1,1),(1,1,0,1)\}$

$G_{4,2}^8=G_{4,2}(L_{(4,2),8})=\{(1,0,1,1),(1,1,1,0)\}$

$G_{4,2}^9=G_{4,2}(L_{(4,2),9})=\{(1,1,1,1)\}$

显然，$G_{4,2}^j$ 的全体代表元为

$L_{(4,2),0}=(0,0,0,0)$　　$L_{(4,2),1}=(0,0,0,1,$

$$L_{(4,2),2}=(0,0,1,0)\quad L_{(4,2),3}=(0,0,1,1)$$
$$L_{(4,2),4}=(0,1,1,0)\quad L_{(4,2),5}=(0,1,0,1)$$
$$L_{(4,2),6}=(1,0,1,0)\quad L_{(4,2),7}=(0,1,1,1)$$
$$L_{(4,2),8}=(1,0,1,1)\quad L_{(4,2),9}=(1,1,1,1)$$

3 k-阶旋转对称函数的性质分析

3.1 k-阶旋转对称函数的 Walsh 谱和自相关函数的性质

本节证明了 k-阶旋转对称函数的 Walsh 谱和自相关函数满足 k-阶旋转对称。

引理 1[3] 对任意给定 $1\le k\le n$、$w\in \mathrm{GF}^n(2)$ 和 $x\in \mathrm{GF}^n(2)$ 都有

$$wr_n^k(x)=r_n^{n-k}(w)x$$

即有 $wx=r_n^k(w)r_n^k(x)$。

定理 1 假设 $1\le k\le n,k\mid n$。则布尔函数 f 是 n 元 k-阶旋转对称函数的充要条件是其 Walsh 谱 $S_{(f)}(w)$ 满足：

$$S_{(f)}(w)=S_{(f)}(r_n^k(w)),w\in \mathrm{GF}^n(2)$$

证明 1) 必要性。因为布尔函数 f 是 k-阶旋转对称函数，则对于给定的 $1\le k\le n,k\mid n$ 有 $f(r_n^k(x))=f(x)$，则

$$\begin{aligned}S_{(f)}(w)&=\frac{1}{2^n}\sum_{x\in \mathrm{GF}^n(2)}(-1)^{f(x)+wx}\\&=\frac{1}{2^n}\sum_{i=1}^{g_{n,k}}\sum_{x\in G_{n,k}^i(L_{(n,k),i})}(-1)^{f(x)+wx}\\&=\frac{1}{2^n}\sum_{i=1}^{g_{n,k}}\sum_{x\in G_{n,k}^i(L_{(n,k),i})}(-1)^{f(r_n^k(x))+r_n^k(w)r_n^k(x)}\\&=S_{(f)}(r_n^k(w))\end{aligned}$$

故必要性成立。

2) 充分性。假设布尔函数 f 的 Walsh 谱 $S_{(f)}(w)$ 对任意给定的 $1\le k\le n,k\mid n$，$x\in \mathrm{GF}^n(2)$ 和 $w\in \mathrm{GF}^n(2)$ 满足 $S_{(f)}(w)=S_{(f)}(r_n^k(w))$，由引理 1 可知 $wx=r_n^k(w)r_n^k(x)$。

由反演公式知

$$\begin{aligned}(-1)^{f(x)}&=\sum_{w\in \mathrm{GF}^n(2)}S_{(f)}(w)(-1)^{wx}\\&=\sum_{w\in \mathrm{GF}^n(2)}S_{(f)}(r_n^k(w))(-1)^{wx}\\&=\sum_{w\in \mathrm{GF}^n(2)}S_{(f)}(r_n^k(w))(-1)^{r_n^k(w)r_n^k(x)}\\&=(-1)^{f(r_n^k(x))}\end{aligned}$$

则 $f(r_n^k(x))=f(x),x\in \mathrm{GF}^n(2)$。即布尔函数 $f(x_1,\cdots,x_n)$，$(x_1,\cdots,x_n)\in \mathrm{GF}^n(2)$ 是 k-阶旋转对称的。故充分性成立。

综合 1)、2)可知定理 1 成立。

定理 1 说明 n 元 k-阶旋转对称函数 Walsh 谱 $S_{(f)}(w)$ 的取值个数不超过 $g_{n,k}$ 个，约是 n 元旋转对称函数 Walsh 谱取值个数的 k 倍。所以它可以具有比 n 元旋转对称函数更为均匀的谱值分布，即更高的非线性度。

定理 2 假设 $1\le k\le n,k\mid n$，布尔函数 f 是 n 元 k-阶旋转对称函数，则其自相关函数 $r_f(s)$ 满足

$$r_f(s)=r_f(r_n^k(s)),s\in \mathrm{GF}^n(2)$$

证明 由布尔函数 Walsh 谱和自相关函数的关系可知

$$r_f(s)=\sum_{w\in \mathrm{GF}^n(2)}\left[S_{(f)}(w)\right]^2(-1)^{ws}$$

又由定理 1 的结论知

$$\begin{aligned}r_f(s)&=\sum_{w\in \mathrm{GF}^n(2)}\left[S_{(f)}(r_n^k(w))\right]^2(-1)^{r_n^k(w)r_n^k(s)}\\&=r_f(r_n^k(s))\end{aligned}$$

定理 2 的逆命题是不成立的（Bent 函数的自相关函数在所有非零点都是零，但 Bent 函数显然不全是 k-阶旋转对称函数）。所以定理 2 不能作为 k-阶旋转对称函数的等价判别条件。

3.2 k-阶旋转对称函数轨道中的长圈与短圈计数

由前述可知，k-阶旋转对称函数的输出序列、Walsh 谱和自相关函数等都可以通过其轨道进行分类，所以有关 k-阶旋转对称函数的轨道的计数和性质的研究是有意义的。本节利用组合论的知识分别给出了 k-阶旋转对称函数的轨道中的长圈和短圈的计数公式。首先介绍几个基本概念。

引理 2[2] (Burnside 引理) 假设 G 为一个作用在集合 S 上的置换群，则 G 作用在 S 上得到的轨道数量为 $\frac{1}{|G|}\sum_{p\in G}|fix_S(p)|$，其中 $fix_S(p)=\{x\in S\mid p(x)=x\}$。

引理 3[10]　(**容斥原理**) 设 $A_1, A_2, \cdots, A_n$ 是有限集合，则

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n}|A_i| + (-1)\sum_{1\le i<j\le n}\left|A_i \cap A_j\right| + \cdots + (-1)^{s-1}\cdot$$

$$\sum_{1\le j_1<j_2<\cdots<j_s\le n}\left|A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_s}\right| + \cdots +$$

$$(-1)^{n-1}\left|A_1 \cap A_2 \cap \cdots \cap A_n\right|$$

文献[8]根据引理 2 给出了下面结论。

定理 3[8]　$g_{n,k}$ 表示 n 元 k -阶旋转对称函数的轨道的个数，则

$$g_{n,k} = \frac{k}{n}\sum_{t\left|\frac{n}{k}\right.} f(t)2^{\frac{n}{t}} \approx k\times\frac{2^n}{n}，\ f(t) \text{ 为欧拉函数}$$

表 1 给出当 $n = 4, 6, \cdots, 15$ 时，$g_{n,k}$ 的取值。

表 1　　n=4,6,…,15 时 $g_{n,k}$ 的取值

n	$g_{n,k}$	k						
		1	2	3	4	5	6	7
4	$g_{4,k}$	6	10					
6	$g_{6,k}$	14	24	36				
8	$g_{8,k}$	36	70		136			
9	$g_{9,k}$	60		176				
10	$g_{10,k}$	108	208			528		
12	$g_{12,k}$	352	700	1 044	1 376		2 080	
14	$g_{14,k}$	1 182	2 344					8 256
15	$g_{15,k}$	2 192		6 560		10 944		

通过表 1 可以看出，k -阶旋转对称函数的轨道个数约是旋转对称函数的轨道个数的 k 倍。

推论 1　对于素数 p，若 $n = p^a$，显然 $k = p^b$ 且 $0 \le b \le a$，则

$$g_{p^a,p^b} = p^{b-a}\left(2^{p^a} + \sum_{i=1}^{a-b}(p^i - p^{i-1})2^{p^{a-i}}\right)$$

证明　因为 $n = p^a, k = p^b$，其中，$0 \le b \le a$。则可用 $p^i, 0 \le i \le a-b$ 表示所有 $\frac{n}{k}$ 的因子，又因为 $f(t)$ 为欧拉函数，则由欧拉函数的性质得 $f(t) = f(p^i) = p^i - p^{i-1}$。由定理 1 可知：

$$g_{n,k} = g_{p^a,p^b} = p^{b-a}\left(2^{p^a} + \sum_{i=1}^{a-b}(p^i - p^{i-1})2^{p^{a-i}}\right)$$

定理 4　$h_{n,k}$ 表示 n 元 k -阶旋转对称函数的轨道所有长圈的个数，则

$$h_{n,k} = \frac{k}{n}\sum_{d\left|\frac{n}{k}\right.} m(d)2^{\frac{n}{d}}，\ m(d) \text{ 为默比乌斯函数}$$

证明　首先对于给定的 $1 \le k \le n, k \mid n$，令 $G = \{r_n^i \mid i = k, 2k, \cdots, n\}$，易知 G 是循环群，对任意的 $p \in G$，p 可以分解成两两不相交且长度相同的轮换之积。令 $G(x) = \{r_n^i(x) \mid i = k, 2k, \cdots, n\}$，表示在 G 作用下由向量 x 生成的轨道，定义轨道的重量为向量 x 的汉明重量。

1) 当 $k = 1$ 时，$G = \{r_n^1, r_n^2, \cdots, r_n^n\}$。对任意的 $x \in \mathrm{GF}^n(2)$，若 $G(x)$ 是短圈 $\Leftrightarrow$ 存在 $d \mid n\ (d < n)$，使得 $r^d(x) = x$。

令 $n = p_1^{a_1} \cdots p_l^{a_l}$ 为 n 的标准分解式，定义 $A_i = \{x \in \mathrm{GF}^n(2) : r^{\frac{n}{p_i}}(x) = x\}, 1 \le i \le l$，表示所有在 $r^{\frac{n}{p_i}}$ 作用下不动点的集合。因为轮换 $(1,2,\cdots,n)$ 在 $r^{\frac{n}{p_i}}$ 作用下可以分解成 $\frac{n}{p_i}$ 个长度为 p_i 的两两不相交的轮换之积。由于 p_i 为素数，则对任意的 $x \in \mathrm{GF}^n(2)$，若 $|G(x)| < n$，一定存在某个 i，$(1 \le i \le l)$ 使得 $x \in A_i$。若 $x \in A_i$，则 $r^{\frac{n}{p_i}}(x)$ 的每个长为 p_i 的轮换取值全为 0 或 1。因此，$|A_i| = 2^{\frac{n}{p_i}}$。又对任意的 $\{p_{j_1}, p_{j_2}, \cdots p_{j_s}\} \subseteq \{p_1, p_2, \cdots p_l\}$，可知 $lcm(p_{j_1}, p_{j_2}, \cdots, p_{j_s}) = p_{j_1} p_{j_2} \cdots p_{j_s}$，所以 $\left|A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_s}\right| = 2^{\frac{n}{p_{j_1}p_{j_2}\cdots p_{j_s}}}$。由引理 3 可知：

$$\left|\bigcup_{i=1}^{l} A_i\right| = \sum_{i=1}^{l}|A_i| + (-1)\sum_{1\le i<j\le l}\left|A_i \cap A_j\right| + \cdots + (-1)^{s-1}\cdot$$

$$\sum_{1\le j_1<j_2<\cdots<j_s\le l}\left|A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_s}\right| + \cdots +$$

$$(-1)^{l-1}\left|A_1 \cap A_2 \cap \cdots \cap A_l\right|$$

$$= \sum_{j=1}^{l} 2^{\frac{n}{p_j}} - \sum_{1\le i<j\le l} 2^{\frac{n}{p_i p_j}} + \cdots + (-1)^{s-1}\cdot$$

$$\sum_{1\le j_1<j_2<\cdots<j_s\le l} 2^{\frac{n}{p_{j_1}p_{j_2}\cdots p_{j_s}}} + \cdots (-1)^{l-1} 2^{\frac{n}{p_1 p_2 \cdots p_l}}$$

又因为每个长圈的元素个数都为 n 个，所以有：

$$h_{n,1} = \frac{1}{n}\left[2^n - \left|\bigcup_{i=1}^{l} A_i\right|\right]$$

$$= \frac{1}{n}\left[2^n - \sum_{j=1}^{l} 2^{\frac{n}{p_j}} + \cdots + (-1)^s\right.$$

$$\left.\sum_{1\le j_1<j_2<\cdots<j_s\le l} 2^{\frac{n}{p_{j_1}p_{j_2}\cdots p_{j_s}}}+\cdots+(-1)^l 2^{\frac{n}{p_1p_2\cdots p_l}}\right]$$

$$=\frac{1}{n}\sum_{d\mid n}m(d)2^{\frac{n}{d}}$$

2) 当 $k>1$ 时，则 $G=\{r_n^k, r_n^{2k}, \cdots, r_n^{mk}\}$。令 $m=\frac{n}{k}=q_1^{c_1}\cdots q_r^{c_r}$。对任意的 $x\in \mathrm{GF}^n(2)$，若 $|G(x)|<m$，则存在 $i\mid m\ (i<m)$，使得 $r^{ik}(x)=x$。又因为：

$$r_n^k=(1,k+1,\cdots,(m-1)k+1)(2,k+2,\cdots,$$
$$(m-1)k+2)\cdots(k,2k,\cdots,n)$$

为 k 个两两不相交的轮换之积，且每个轮换的长度为 m。用 fix 来表示 $\mathrm{GF}^n(2)$ 在 $G\setminus\{r_n^n\}$ 下保持不动的点，由 1)的结论可知：

$$|fix|=\sum_{j=1}^{r}(2^{\frac{m}{q_j}})^k-\sum_{1\le i<j\le r}(2^{\frac{m}{q_iq_j}})^k+\cdots+(-1)^{s-1}\cdot$$
$$\sum_{1\le j_1<j_2<\cdots<j_s\le r}(2^{\frac{m}{q_{j_1}q_{j_2}\cdots q_{j_s}}})^k+\cdots+(-1)^{r-1}(2^{\frac{m}{q_1q_2\cdots q_r}})^k$$

故

$$h_{n,k}=\frac{1}{m}\left[2^n-|fix|\right]$$
$$=\frac{1}{m}\left[2^n-\sum_{j=1}^{r}2^{\frac{n}{q_j}}+\cdots+(-1)^s\cdot\right.$$
$$\left.\sum_{1\le j_1<j_2<\cdots<j_s\le r}2^{\frac{n}{q_{j_1}q_{j_2}\cdots q_{j_s}}}+\cdots+(-1)^r 2^{\frac{n}{q_1q_2\cdots q_r}}\right]$$
$$=\frac{k}{n}\sum_{d\mid\frac{n}{k}}m(d)2^{\frac{n}{d}}$$

综上所述，定理 4 的结论是成立的。

表 2 给出当 $n=4,6,\cdots,15$ 时 $h_{n,k}$ 的取值。

表 2 $n=4,6,\cdots,15$ 时 $h_{n,k}$ 的取值

n	$h_{n,k}$	k						
		1	2	3	4	5	6	7
4	$h_{4,k}$	3	6					
6	$h_{6,k}$	9	20	28				
8	$h_{8,k}$	30	60		120			
9	$h_{9,k}$	56		168				
10	$h_{10,k}$	99	204			496		
12	$h_{12,k}$	335	670	1 008	1 360		2 016	
14	$h_{14,k}$	1 161	2 340					8 128
15	$h_{15,k}$	2 182		6 552		10 912		

对比表 1 可以发现，在 k-阶旋转对称函数的轨道中长圈占大多数。

推论 2 假设 $s_{n,k}$ 表示 n 元 k-阶旋转对称函数的轨道中所有短圈的个数，则

$$s_{n,k}=\frac{k}{n}\sum_{d\mid\frac{n}{k}}(f(d)-m(d))2^{\frac{n}{d}}$$

证明 因为 $s_{n,k}=g_{n,k}-h_{n,k}$，所以结论是显然的。

前述结论在 $k=1$ 时即为旋转对称函数的轨道计数的结论，其相应的结论 Sarkar 和 Maitra 在文献[2]中已有详细的描述。值得注意的是，文献[3]所给出的旋转对称函数的轨道中的长圈的计数公式在 $n=p_1^{a_1}\cdots p_l^{a_l}$ 为 n 的标准分解式时为

$$h_n=\frac{1}{n}\sum_{d\mid n}f(d)2^{\frac{n}{d}}-\sum_{i=1}^{l}\sum_{j=1}^{a_i}\frac{2^{p_i^j}-2^{p_i^{j-1}}}{p_i^j}-2$$

而本文定理 4 在 $k=1$ 时为

$$h_{n,1}=\frac{1}{n}\sum_{d\mid n}m(d)2^{\frac{n}{d}}$$

经计算在 $n=12=2^2\times3$ 时文献[2]的结论为 $h_{12}=344$，而定理 4 的结论为 $h_{12,1}=335$。经验证 12 元旋转对称函数的轨道中长圈个数为 335 个，说明文献[2]的结论在 $n=12$ 时是不成立的。

具体原因是，Sarkar 和 Maitra 得出的 n 元旋转对称函数的轨道中所有短圈的数量为

$$s_n=\sum_{i=1}^{l}\sum_{j=1}^{a_i}\frac{2^{p_i^j}-2^{p_i^{j-1}}}{p_i^j}+2$$

之后将轨道总数减所有短圈的数量，所得即为 n 元旋转对称函数的轨道中所有长圈的数量。但是，s_n 只计算了所有在 r_n^1 和 $r_n^{p_j^{b_j}}$ $(1\le b_j\le a_j)$ 作用下不动的短圈数量，而没有计算所有在 r_n^d 作用下不动的短圈数量，其中 $d=\prod_{1<j\le m}p_j^{b_j}$ $(d<n,\ 1<m\le l, 1\le b_j\le a_j)$。

所以 Sarkar 和 Maitra 给出的旋转对称函数轨道中的长圈和短圈的计数公式在 $n=p_1^{a_1}\cdots p_l^{a_l}, l=2$ 且存在 $a_i\ge 2$ $(i=1,2)$ 或 $l\ge 3$ 时都是不正确的。

表 3 给出当 $n=1,2,\cdots,30$ 时 h_n 与 $h_{n,1}$ 的取值对比。

表 3　n=1,2,…,30 时 h_n 与 $h_{n,1}$ 的取值对比

n	h_n	$h_{n,1}$	n	h_n	$h_{n,1}$
1	2	2	16	4 080	4 080
2	1	1	17	7 710	7 710
3	2	2	18	14 541	14 532
4	3	3	19	27 594	27 594
5	6	6	20	52 476	52 377
6	9	9	21	99 858	99 858
7	18	18	22	190 557	190 557
8	30	30	23	364 722	364 722
9	56	56	24	699 241	698 870
10	99	99	25	1 342 176	1 342 176
11	186	186	26	2 580 795	2 580 795
12	344	335	27	4 971 008	4 971 008
13	630	630	28	9 587 556	9 586 395
14	1 161	1 161	29	18 512 790	18 512 790
15	2 182	2 182	30	35 792 557	35 790 267

通过研究 k -阶旋转对称函数的轨道以及轨道中的长圈和短圈的计数，可以了解 k -阶旋转对称函数的轨道的性质，从而为更为深入地研究 k -阶旋转对称函数的密码学性质提供帮助。

4　结束语

本文分析了 k -阶旋转对称函数的性质，证明了 k -阶旋转对称函数的 Walsh 谱和自相关函数满足 k -阶的旋转对称。经分析发现 k -阶旋转对称函数的很多性质都可以利用其轨道来刻画，并利用组合论的知识给出了 n 元 k -阶旋转对称函数轨道中的长圈和短圈的计数公式。目前，对于 k -阶旋转对称函数的研究工作才刚刚开始，通过深入研究这一类特殊的布尔函数函数从而寻找到密码学性质优良的布尔函数，在理论和实践上都具有重要的意义。

参考文献：

[1] PIEPRZYK J, QU C X. Fast hashing and rotation-symmetric functions[J]. Journal of Universal Computer Science, 1999, 5(1): 20-31.

[2] SARKAR P, MAITRA S. Rotation symmetric Boolean functions-count and cryptographic properties[J]. Discrete Applied Mathematics, 2008, 156: 1567-1580.

[3] SARKAR P, MAITRA S, CLARK J. Results on rotation symmetric bent and correlation immune boolean functions[A]. Fast Software EncryptionFSE' 2004[C]. Berlin, 2004. 161-177.

[4] KAVUT S, YÜCEL M D. Search for boolean functions with excellent profiles in the rotation symmetric class[J]. IEEE Transactions on Information Theory, 2007, IT-53(5): 1743-1751.

[5] MAXIMOV A, HELL M, MAITRA S. Plateaued rotation symmetric boolean functions on odd number of variables[EB/OL]. http://eprint.iacr.org/2004/144.pdf.

[6] MAXIMOV A. Classes of plateaued rotation symmetric Boolean functions under transformation of Walsh spectra[EB/OL]. http:// eprint.iacr.org/2004/354.pdf.

[7] KAVUT S, SARKAR P, MAITRA S, *et al*. Enumeration of 9-variable rotation symmetric boolean function having nonlinearity>240[A]. Cryptology-INDOCRYPT' 2006[C]. Berlin, 2006.266-279.

[8] KAVUT S, YÜCEL M D. Generalized rotation symmetric and dihedral symmetric Boolean functions-9 variable Boolean functions with nonlinearity 242[EB/OL]. http://eprint.iacr.org/2007/308.pdf.

[9] 李世取，曾本胜，刘文芬. 密码学中的逻辑函数[M].北京：北京中软电子出版社，2003.
LI S Q,ZENG B S,LIU W F. Logic Functions in Cryptography[M]. Beijing: Zhongruan Electric Publishing Company,2003.

[10] 卢开澄，卢华明. 组合数学（第三版）[M]. 北京: 清华大学出版社, 2002.
LU K C,LU H M. Combinatorial Mathematics (Third Edition)[M]. Beijing: Tsinghua University Press,2002.

作者简介：

李泉（1983-），男，吉林长春人，信息工程大学硕士生，主要研究方向为密码学。

高光普（1984-），男，天津人，信息工程大学博士生，主要研究方向为密码学。

刘文芬（1965-），女，湖北安陆人，博士，信息工程大学博士生导师，主要研究方向为信息安全、密码学。