文章编号:1000－2367(2015)03－0001－04 **DOI**:10.16366/j.cnki.1000－2367.2015.03.001

两类具有特殊线性结构点的平衡旋转对称函数的计数

耿旭旭,赵先鹤

(河南师范大学 数学与信息科学学院,河南 新乡 453007)

摘 要:基于对旋转对称轨道的计算,分别给出了当变元个数为 p^k 和 pq(其中 p,q 均为奇素数,$k\leq 1$)时,旋转对称函数类中两类具有特殊线性结构点的平衡函数的计数.

关键词:旋转对称布尔函数;平衡函数;计数;线性结构

中图分类号:TN911.2 **文献标志码**:A

近年来,旋转对称布尔函数受到了越来越多的关注[1－10],最初是由 Pieprzyk 和 Qu 提出,由于它很好地迎合了 MD4,MD5 以及 HAVAL 这些 Hash 密码算法需要高效执行的客观要求,因此,它被应用于这些 Hash 算法的实现中[1],人们对其自身代数结构的性质产生了极大兴趣. 其中,线性结构是度量布尔函数安全性的一个重要指标. 众所周知,具有非零线性结构的布尔函数是密码学中的一类"弱函数",布尔函数的退化性可以归结为对布尔函数线性结构的研究[11]. 而布尔函数的平衡性反映一种安全性能指标,也是密码函数的设计准则之一. 因此,考察平衡的 RSBF 的线性结构特征既有理论意义又有应用价值.

文献[8]给出了 p^r(p 为素数)以及一般奇数元平衡旋转对称布尔函数的计数下界. 文献[9]给出了 1 阶相关免疫旋转对称布尔函数的计数,并且还推导了平衡的旋转对称布尔函数的计数公式,首次给出了十一变元和十三变元的 1 阶相关免疫旋转对称布尔函数的数目. 文献[12－13]分别构造了 $2p$ 元及素数元旋转对称弹性布尔函数,并给出了计数公式. 文献[14]给出了 pq 元的 1 阶弹性函数的构造与计数. 文献[15]给出了 p^r 元的所有 1 阶弹性旋转对称布尔函数的精确计数. 文献[10,16]构造了一类以 1 为不变线性结构点的相关免疫函数. 文献[17]证明了对于给定变量的 1 阶弹性旋转对称布尔函数的构造就相当于求解方程系统,其个数等价于方程系统的解的个数. 文献[18]告诉我们对于平衡的或趋于稳定的旋转对称函数如何进行分类.

本文在文献[2]的基础上,利用轨道计数公式给出了当变元个数为 p^k 和 pq(其中 $p<q$ 均为奇素数,$k\leq 1$)时,旋转对称函数类中两类以 1 为线性结构点的平衡函数的计数. 这更便于密码学工作者寻找具有良好密码学性质的旋转对称布尔函数.

1 预备知识

令 F_2^n 是二元域 $F_2=\{0,1\}$ 上的 n 维向量空间,B_n 为全体 n 元布尔函数 $f:F_2^n\to F_2$ 的集合. 定义 f 的支撑集为 $supp(f)=\{\boldsymbol{x}\in F_2^n \mid f(x)=1\}$,称支撑集所含元素的个数为 $f(\boldsymbol{x})$ 的汉明重量,记为 $wt(f)$. 对于任意一个集合 A,用 $|A|$ 表示集合 A 内元素的个数. 若 $wt(f)=|supp(f)|=2^{n-1}$,则称 $f(\boldsymbol{x})$ 是平衡函数.

定义 1 设 n 为正整数,对任意的 $(x_1,x_2,\cdots,x_n)\in F_2^n$ 和 $1\leq k\leq n$,定义 $\rho_n^k(x_1,x_2,\cdots,x_n)=(\rho_n^k(x_1),\rho_n^k(x_2),\cdots,\rho_n^k(x_n))$,其中 $\rho_n^k(x_i)=x_{(i+k)\bmod n}$.

如果对任意的 $(x_1,x_2,\cdots,x_n)\in F^{n^n}$ 都有 $f(\rho_n^k(x_1,x_2,\cdots,x_n))=f(x_1,x_2,\cdots,x_n)$,$1\leq k\leq n$,则称

收稿日期:2014-06-03;**修回日期**:2015-03-16.

基金项目:国家自然科学基金(10771172;11271301;U1204101);河南省教育厅重点项目(13B110085);河南师范大学骨干教师资助计划项目.

作者简介:耿旭旭(1988—),女,河南安阳人,河南师范大学硕士研究生,研究方向:有限群及其应用.

通信作者:赵先鹤(1978—),女,河南南阳人,河南师范大学副教授,博士,E-mail:zhaoxianhe989@163.com.

$f(x)$ 为旋转对称布尔函数(简称 RSBF).

设 $\boldsymbol{x}=(x_1,\cdots,x_n)\in F^{nn}$,令 $G_n(\boldsymbol{x})=\{\rho_n^k(\boldsymbol{x})\mid 1\leq k\leq n\}$ 表示由向量 $\boldsymbol{x}$ 生成的轨道,由于 $G_n(\boldsymbol{x})$ 中每个向量的汉明重量都相等,定义轨道的重量为该轨道中向量的汉明重量.n 元 RSBF 的轨道个数为 $g_n=\frac{1}{n}\sum\limits_{k\mid n}\phi(k)\cdot 2^{n/k}$,其中,$\phi(\cdot)$ 为欧拉函数[13].当 n 为奇数时,令 h_d 为所有含 d 个向量的轨道对数,显然 d 是 n 的因子,且有 $\sum\limits_{d\mid n}2h_d=g_n$.

定义 2 设 $f\in B_n$,向量 $\boldsymbol{\alpha}\in F_2^n$ 称为布尔函数 f 的 0-类线性结构点当且仅当 $f(\boldsymbol{x}+\boldsymbol{\alpha})+f(\boldsymbol{x})$ 为常值.

若 $f(\boldsymbol{x}+\boldsymbol{\alpha})+f(\boldsymbol{x})=0$,则称 $\boldsymbol{\alpha}$ 为 f 的 0-类线性结构点;若 $f(\boldsymbol{x}+\boldsymbol{\alpha})+f(\boldsymbol{x})=1$,则称 $\boldsymbol{\alpha}$ 为 f 的 1-类线性结构点;记 $R_n(0)=\{f\in B_n\mid f(\boldsymbol{x})+f(\boldsymbol{x}+1)=0\}$;$R_n(1)=\{f\in B_n\mid f(\boldsymbol{x})+f(\boldsymbol{x}+1)=1\}$.

为方便读者,我们约定以下记号:$F_n^0=\{f_n^0\mid f_n^0\in R_n(0)$ 且 $wt(f_n^0)=2^{n-1}\}$;$F_n^1=\{f_n^1\mid f_n^1\in R_n(1)$ 且 $wt(f_n^1)=2^{n-1}\}$.

2 主要结论

定理 1 当 $n=p^k$ 时(p 为奇素数且 $k\geq 1$),则(1) $|F_n^0|=\sum\limits_{j=1}^{t}\left(\prod\limits_{i=1}^{k}C_{h_{p^i}}^{y_i^j}\right)$,(2) $|F_n^1|=2^{g_n/2}$.

证明 (1) 首先证明 $|F_n^0|=\sum\limits_{j=1}^{t}\left(\prod\limits_{i=1}^{k}C_{h_{p^i}}^{y_i^j}\right)$.

因为 p 为奇素数,则对任意的 $\boldsymbol{x}\in F_2^n$,有 $G_n(\boldsymbol{x})\cap G_n(\boldsymbol{x}+1)=\varnothing$,即 $G_n(\boldsymbol{x})$ 与 $G_n(\boldsymbol{x}+1)$ 总成对出现.那么对任意的 $f_n^0\in R_n(0)$,有 $f_n^0(\boldsymbol{x})$ 和 $f_n^0(\boldsymbol{x}+1)$ 同时为 0 或者同时为 1.

当 $n=p^k$ 时,由轨道长计数公式有:

$$h_1=1,h_p=\frac{g_p-2}{2}=\frac{\left(\frac{1}{p}\sum\limits_{k\mid p}\phi(k)\cdot 2^{p/k}\right)-2}{2}=\frac{2^p-1-1}{p},$$

$$h_{p^2}=\frac{g_{p^2}-(g_p-2)-2}{2}=\frac{g_{p^2}-g_p}{2}=\frac{\frac{1}{p^2}\sum\limits_{k\mid p^2}\phi(k)\cdot 2^{p^2/k}-\frac{1}{p}\sum\limits_{k\mid p}\phi(k)\cdot 2^{p/k}}{2}=\frac{2^{p^2-1}-2^{p-1}}{p^2},\cdots,$$

$$h_{p^k}=\frac{g_{p^k}-(g_{p^{k-1}}-2)-2}{2}=\frac{g_{p^k}-g_{p^{k-1}}}{2}=\frac{2^{p^{k-1}}-2^{p^{k-1}}-1}{p^k}.$$

因为 f_n^0 为平衡函数,从长为 $1,p,p^2,\cdots,p^k$ 的轨道中分别选 y_0 对,y_1 对,y_2 对,$\cdots$,y_k 对,使得:

$$\begin{cases}\sum\limits_{i=0}^{k}2p^iy_i=2^{(p^k-1)};\\ 0\leq y_i\leq h_p^i,(0\leq i\leq k).\end{cases}$$

设上述方程有 t 组不同的解,其中第 j 组解为 $(y_0^j,y_1^j,\cdots,y_k^j)$,这里 $1\leq j\leq t$.

由此可知:$|F_n^0|=\sum\limits_{j=1}^{t}\left(\prod\limits_{i=1}^{k}C_{h_{p^i}}^{y_i^j}\right)$.

(2) 下面证明 $|F_n^1|=2^{g_n/2}$.

对任意的 $f_n^1\in R_n(1)$,则 $G_n(\boldsymbol{x})$ 与 $G_n(\boldsymbol{x}+1)$ 恰有一个属于 f_n^1 的支撑集.又 $G_n(\boldsymbol{x})$ 与 $G_n(\boldsymbol{x}+1)$ 总成对出现,且 f_n^1 为平衡函数,因此,只需令每对轨道中的任一条属于 f_n^1 的支撑集即可,那么对于每对轨道有两种选择,共有 $g_n/2$ 对轨道,所以共有 $2^{g_n/2}$ 种.因此,$|F_n^1|=2^{g_n/2}$.

由以上讨论可知:当 $n=p^k$(p 为奇素数且 $k\geq 1$) 时,有 $|F_n^0|=\sum\limits_{j=1}^{t}\left(\prod\limits_{i=1}^{k}C_{h_{p^i}}^{y_i^j}\right)$,$|F_n^1|=2^{g_n/2}$.

例 1 以 $p=5^2=25$ 为例,计算 $|F_{25}^0|$ 和 $|F_{25}^1|$.

首先计算 $|F_{25}^0|$.

当 $n=25$ 时,则有 $h_1=1,h_5=3,h_{25}=671\,088$.从中分别取出 y 对,z 对,r 对,由定理 1 可得方程:

$2y+2\times5z+2\times25r=2^{25-1}$，其中 $0\leq y\leq1;0\leq z\leq3;0\leq r\leq671\ 088$.

上述方程等价于：$y+5z+25r=2^{23}$. 由 y,z 的取值范围可知 $0\leq y+5z\leq16$，也即 $0\leq2^{23}-25r\leq16$. 因为 r 为正整数，解得 $r=335\ 544$，此时 $y+5z=8$，又由 y,z 取值范围，显然可知，此方程组无解. 即不存在 y,z,r 使得 $2y+2\times5z+2\times25r=2^{25-1}$，所以 $|F_{25}^0|=0$.

下面计算 $|F_{25}^1|$.

因为 f_{25}^1 为平衡函数，此时 $G_{25}(\boldsymbol{x})$ 与 $G_{25}(\boldsymbol{x}+1)$ 恰有一个属于 f_{25}^1 的支撑集，因此，只需令每对轨道中的任一条属于 f_{25}^1 的支撑集即可. 由轨道计算公式：$g_{25}=\frac{1}{25}(\phi(1)\cdot2^{25}+\phi(5)\cdot2^5+\phi(25)\cdot2)=1\ 342\ 184$，所以当 $n=25$ 时，有 671 092 对轨道，对轨道有 2 种选择，从而 $|F_{25}^1|=2^{g_{25}/2}=2^{671\ 092}$.

定理 2　当 $n=pq$（p,q 为互异的奇素数）时，则(1) $|F_n^1|=2^{g_n/2}$，(2) $|F_n^0|=\sum_{i=1}^{t}C_{h_p}^{b_i}C_{h_q}^{c_i}C_{h_{pq}}^{d_i}$.

证明　(1) 不妨设 $p<q$. 首先证明 $|F_n^1|=2^{g_n/2}$.

因为 p,q 均为奇素数，此时 n 仍为奇数，所以 $G_n(\boldsymbol{x})$ 与 $G_n(\boldsymbol{x}+1)$ 成对出现，那么对于 $f_n^1\in R_n(1)$ 为平衡函数，由定理 1(2) 讨论可知 $|F_n^1|=2^{g_n/2}$.

(2) 下面证明 $|F_n^0|=\sum_{i=1}^{t}C_{h_p}^{b_i}C_{h_q}^{c_i}C_{h_{pq}}^{d_i}$.

当 $n=pq$ 时，其轨道长只可能为 $1,p,q,pq$. 由轨道长计数公式有：

$h_1=1,h_p=\frac{g_p-2}{2}=\frac{2^{p-1}-1}{p},h_q=\frac{g_q-2}{2}=\frac{2^{q-1}-1}{q},h_{pq}=\frac{g_n-g_p-g_q+2}{2}=\frac{2^{pq-1}-2^{p-1}-2^{q-1}+1}{pq}$. f_n^0 为平衡函数，在长为 $1,p,q,pq$ 轨道中分别取 y 对，z 对，r 对，w 对，使得：

$$2y+2pz+2qr+2pqw=2^{pq-1}，其中$$

$$0\leq y\leq1;0\leq z\leq\frac{2^{p-1}-1}{p};0\leq r\leq\frac{2^{q-1}-1}{q};0\leq w\leq\frac{2^{pq-1}-2^{p-1}-2^{q-1}+1}{pq}.$$

设上述方程有 t 组不同的解，其中第 $i(1\leq i\leq t)$ 组解为：

$$y_i=a_i;z_i=b_i;r_i=c_i;w_i=d_i.$$

从而可知：$|F_n^0|=\sum_{i=1}^{t}C_{h_p}^{b_i}C_{h_q}^{c_i}C_{h_{pq}}^{d_i}$.

由以上讨论可知，当 $n=pq$（$p<q$ 为互异的奇素数）时，则有 $|F_n^0|=\sum_{i=1}^{t}C_{h_p}^{b_i}C_{h_q}^{c_i}C_{h_{pq}}^{d_i}$，$|F_n^1|=2^{g_n/2}$.

例 2　以 $n=15$ 为例，计算 $|F_{15}^0|$ 和 $|F_{15}^1|$.

首先计算 $|F_{15}^1|$. 因为 15 为奇数，所以 $G_{15}(\boldsymbol{x})$ 与 $G_{15}(\boldsymbol{x}+1)$ 成对出现，又 $f_{15}^1\in R_{15}(1)$ 为平衡函数，那么我们只需令每对轨道中的其中任意一条属于 f_{15}^1 的支撑集即可，一共有 $\frac{g_{15}}{2}=1\ 096$ 对轨道，以 $|F_{15}^1|=2^{1\ 096}$.

下面计算 $|F_{15}^0|$.

当 $n=15$ 时，从长为 1,3,5,15 的轨道中分别取出 y 对，z 对，r 对，w 对，由定理 2 可得方程：

$$2y+2\times3z+2\times5r+2\times15w=2^{15-1}，其中$$

$$0\leq y\leq1;0\leq z\leq1;0\leq r\leq3;0\leq w\leq1\ 091.$$

上述方程等价于：$y+3z+5r=2^{13}-15w$. 由 y,z,r 的取值范围可知 $0\leq y+3z+5r\leq19$，所以 $0\leq2^{13}-15w\leq19$，又 w 为正整数，可得 $w\in\left[\frac{8\ 173}{15},\frac{8\ 192}{15}\right]=[545,546]$.

(1) $w=545$ 时，$y+3z+5r=2^{13}-15w=17$，又由 y,z,r 的取值范围，显然此方程组无解；

(2) 当 $w=546$ 时，$y+3z+5r=2^{13}-15w=2$，又由 y,z,r 的取值范围，显然此方程组仍无解.

也就是说，不存在 y,z,r,w，使得：$2y+2\times3z+2\times5r+2\times15w=2^{15-1}$，所以 $|F_{15}^0|=0$.

下面利用定理 2，给出部分 pq 元的 $|F_n^0|$ 和 $|F_n^1|$，见表 1.

表 1 $n=15,21,33,35$ 时,$|F_n^0|$ 和 $|F_n^1|$ 的取值

n	h_1	h_p	h_q	h_{pq}	$g_n/2$	$\lvert F_n^0\rvert$	$\lvert F_n^1\rvert$
15	1	1	3	1 091	1 096	0	$2^{1\,096}$
21	1	1	9	49 929	49 940	0	$2^{49\,940}$
33	1	1	93	130 150 493	130 150 588	0	$2^{130\,150\,588}$
35	1	3	9	490 853 403	490 853 416	$186C_{490\,853\,403}^{245\,426\,701}$	$2^{490\,853\,416}$

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] 高光普,刘文芬. 关于旋转对称布尔函数线性结构的几点注记[J]. 电子与信息学报,34(9):2273-2276.

[3] 赵亚群,李 旭. 旋转对称布尔函数线性结构的 2 个公开问题[J]. 通信学报,34(3):171-174.

[4] 李 泉,高光普,刘文芬. k-阶旋转对称函数性质分析与轨道计数[J]. 通信学报,33(1):114-119.

[5] Esam E. On The Linear Structures of Cryptographic Rotation Symmetric Boolean Functions[C]. The 9th International Conference for Young Computer Scientists, ICYCS 2008, Zhangjiajie, 2008.

[6] 孟 强,陈鲁生,符方伟. 一类代数免疫度达到最优的布尔函数的构造[J]. 软件学报,2010,21(7):1758-1767.

[7] Fu S J, Li C, Kanta M, et al. Balanced 2p-variable rotation symmetric Boolean functions with maximum algebraic immunity[J]. Applied Mathematics Letters, 2011, 24(12): 2093-2096.

[8] 张 鹏,付绍静,屈龙江,等. 平衡旋转对称布尔函数的计数[J]. 应用科学学报,2013,30(1):45-51.

[9] Fu S J, Li C, Qu L J. On the number of rotation symmetric Boolean functions[J]. Science China Information Sciences, 2010, 53(3): 537-545.

[10] Stanica P, Maitra S, Clark J. Results on rotation symmetric bent and correlation immune Boolean functions[C]. Fast Software Encryption Workshop (FSE 2004), New Delhi India, 2004.

[11] 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.

[12] 杜 蛟,温巧燕,张 劼,等. $2p$ 元-2 阶旋转对称弹性布尔函数的构造与计数[J]. 北京邮电大学学报,2012,35(5):36-40.

[13] 杜 蛟,温巧燕,张 劼,等. 素数元旋转对称弹性布尔函数的构造与计数[J]. 通信学报,2013,34(3):6-13.

[14] Du J, Pang S Q, Wen Q Y, et al. Construction and count of 1-resilient rotation symmetric Boolean functions on p^r variables[J]. Chinese Journal of Electronics, 2014, 23(4): 816-820.

[15] Du J, Wen Q Y, Zhang J, et al. Construction and counting of 1-resilient rotation symmetric Boolean functions on pq variables[J]. IEICE. Trans. on Fundamentals, 2013(7): 1653-1656.

[16] 王永娟,韩文报,李世取. 满足 CI 的 Rots 函数的构造与计数[J]. 通信学报,2007,28(11A):6-9.

[17] Du J, Wen Q Y, Zhang J, et al. Construction of resilient rotation symmetric Boolean functions on given number of variables[J]. IET Information Security, 2014, 8(5): 265-272.

[18] Gao G P, Thomas W, Liu W F. Families of rotation symmetric functions with useful cryptographic properties[J]. IET Information Security, 2014, 8(6): 297-302.

The Count of Balanced Rotation Symmetirc Boolean Functions with Two Specion Linear Structure

GENG Xuxu, ZHAO Xianhe

(College of Mathematics and Information Science, Henan Normal University, Xinxiang 453007, China)

Abstract: Based on the calculation of rotation symmetric orbits, we count the balanced p^k-variable and pq-variable rotation symmetric Boolean functions which have two special linear structures, where p, q are primes and $k\leq 1$.

Keywords: rotation symmetric Boolean functions(RSBF); balanced functions; counting; linear