DOI:10.19789/j.1004-9398.2023.02.001
文献引用:崔萌,王维琼,许豪杰,等.两类多输出*k*-旋转对称布尔函数的构造[J].首都师范大学学报(自然科学版),2023,44(2):1-7. CUI M, WANG W Q, XU H J, et al. Construction of two classes of multi-output *k*-rotation symmetric Boolean functions[J]. Journal of Capital Normal University(Natural Science Edition),2023,44(2):1-7.

两类多输出*k*-旋转对称布尔函数的构造*

崔　萌，王维琼**，许豪杰，刘欢欢
（长安大学理学院，陕西 西安　710064）

摘要:具有良好性质的多输出*k*-旋转对称布尔函数在密码系统设计中发挥着重要作用。基于循环群在二元域上的*n*元向量空间上的作用,使用轨道划分及构造正交表的方法,分别研究了平衡及1阶弹性*n*元*m*输出*k*-旋转对称布尔函数存在的充分条件及其构造方法。当$\frac{n}{k}=p^r$(*p*为素数,$r\in\mathbf{Z}^+$)时,给出了平衡或1阶弹性的多输出*k*-旋转对称布尔函数存在时*m*的取值范围,并用Matlab对构造法进行了验证。

关键词:多输出布尔函数;旋转对称;平衡函数;弹性函数;正交表
中图分类号:O29　　**文献标识码**:A

Construction of two classes of multi-output *k*-rotation symmetric Boolean functions*

CUI Meng, WANG Weiqiong**, XU Haojie, LIU Huanhuan
(School of Science, Chang'an University, Xi'an Shaanxi　710064)

Abstract: Multi-output rotation symmetric Boolean functions with good properties play an important role in the design of cryptographic systems. Based on the action of cyclic group on the *n*-dimensional vector space over binary field, the sufficient conditions for the existence of multi-output *k*-rotation symmetric balanced and 1-resilient Boolean functions are studied by using the method of orbital partition and constructing orthogonal tables respectively. When $\frac{n}{k}=p^r$ (p is prime, $r\in\mathbf{Z}^+$), the range of values given for *m* when a balanced or 1-resilient multi-output rotational symmetric Boolean function exists. The concrete construction methods are provided and verified by Matlab.

Keywords: multi-output Boolean function; rotation symmetric; balanced function; resilient function; orthogonal table
CLC: O29　　**DC**: A

0　引　言

旋转对称函数(rotation symmetric function,RSF)最初也叫做幂等函数,由Filiol和Fontaine[1]首次提出。1999年,Pieprzyk与Qu[2]在研究Hash算法压缩函数的快速计算时,首次使用RSF。这类函数具有

收稿日期:2022-04-21
* 国家自然科学基金项目(11901049);陕西省自然科学基础研究计划项目(2020JQ-343);陕西省高校科协青年人才托举计划项目(20200505)
** 通信作者:wqwang@chd.edu.cn

运算速度快、结构简单等特点。此外,旋转对称布尔函数还具有一些优良的密码学性质[3-5]。2008年,Kavut和Yücel[6]将旋转对称布尔函数推广到k-旋转对称布尔函数,推广后的函数不仅具备旋转对称布尔函数的优良性质,而且数量更多。因此,构造具有特殊密码学性质的k-旋转对称布尔函数具有重要的理论意义。

近年来,许多学者对旋转对称布尔函数的平衡性、相关免疫性和弹性进行了深入的研究。Siegenthaler[7]首先提出m阶相关免疫函数,并证明了一个函数为m阶相关免疫函数的充分条件;Chor等[8]在计算机科学基础研讨会上提出弹性函数的概念;Stinson[9]给出了弹性函数(平衡的相关免疫函数)与正交表大集之间的关系;基于此,杜蛟课题组[10-15]分别研究了变元个数为p、pq、p^r、$4p$的1阶弹性单输出RSF的构造与计数问题;Pang等[16]同样利用弹性函数与正交表大集之间的关系,将构造1阶弹性旋转对称布尔函数的问题转化为求解方程组的问题,给出了任意变元的1阶弹性单输出旋转对称布尔函数的一般构造方法。

多输出布尔函数可以用来设计分组密码的S盒,是分组加密算法的重要部分,具有一些特殊密码学性质的多输出布尔函数在密码体制中发挥着重要作用。2009年,元彦斌和赵亚群[17]首次提出多输出RSF的概念,并研究了多输出RSF的广义Walsh谱和广义自相关函数的性质,以及函数满足平衡性、相关免疫性的充要条件;2017年,杜蛟等[18]讨论了当输入变元$n = 2^r (r \in \mathbf{Z}^+)$,多输出旋转对称布尔函数满足平衡和弹性的条件时,所对应的输出变量维数的取值范围,给出了8元多输出旋转对称1阶弹性函数的具体构造并对其计数;2018年,Du等[19]又通过解方程组的方法,当多输出旋转对称布尔函数满足平衡及1阶弹性条件时,给出了对于变元$n = p^r$(p为奇素数,$r \in \mathbf{Z}^+$),相应的输出变量维数的取值范围,并证明了其存在性;2020年,田晔晨等[20]对Du等[19]的结果进行推广,将结果推广到多输出k-旋转对称布尔函数,通过对轨道进行划分,证明了几类平衡多输出k-旋转对称布尔函数与1阶弹性多输出k-旋转对称布尔函数的存在性。

到目前为止,还没有文章给出任意变元的平衡与弹性多输出k-旋转对称布尔函数的存在性及构造方法。基于循环群在空间F_2^n上的作用,通过轨道划分以及构造正交表的方法,本文对田晔晨等[20]的结果进行推广,将输入变元n和旋转阶数k推广到任意正整数,给出了具有平衡及弹性的旋转对称布尔函数存在的充分条件以及具体的构造方法。

1 预备知识

记F_2^n为二元域F_2上的n维向量空间。定义映射$F: \mathrm{F}_2^n \mapsto \mathrm{F}_2^m$为$n$元$m$输出布尔函数,简记为$(n, m)$函数,即

$$F(\boldsymbol{X}) = (f_1(\boldsymbol{X}), f_2(\boldsymbol{X}), \cdots, f_m(\boldsymbol{X})),$$

式中$f_i: \mathrm{F}_2^n \mapsto \mathrm{F}_2 (1 \leqslant i \leqslant m)$为$n$元布尔函数[16]。若$n$元$m$输出布尔函数$F(\boldsymbol{X})$,对于$\forall \boldsymbol{Y} \in \mathrm{F}_2^m$,都有$|F^{-1}(\boldsymbol{Y})| = 2^{n-m}$,则称$F(\boldsymbol{X})$为平衡函数。特别地,当$m = 1$时,$F(\boldsymbol{X}) = f_1(\boldsymbol{X})$为单输出布尔函数。

考虑循环群$C_n^k = \{\rho_n^k | 1 \leqslant k \leqslant n\}$在$\mathrm{F}_2^n$上的作用。对于$\forall \boldsymbol{X} = (x_1, x_2, \cdots, x_n) \in \mathrm{F}_2^n, x_i \in \mathrm{F}_2$,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k-循环移位变换为

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

定义1[18] 设$F(\boldsymbol{X})$为F_2上的(n, m)函数,$1 \leqslant k \leqslant n$且$k|n$。若对于$\forall \boldsymbol{X} \in \mathrm{F}_2^n, U \in \mathrm{F}_2^m \backslash \{\boldsymbol{0}\}$,都有

$$U \cdot F(\rho_n^k(x_1, x_2, \cdots, x_n)) = U \cdot F(x_1, x_2, \cdots, x_n),$$

式中$\cdot$表示向量内积,则称$F(\boldsymbol{X})$为F_2上的n元m输出k-旋转对称布尔函数,记作$(n, m)k$-RSBF。

循环群C_n^k把F_2^n分为若干个大小不同的轨道。由$\boldsymbol{X} = (x_1, x_2, \cdots, x_n)$生成的轨道记为

$$G_{n,k}(\boldsymbol{X}) = \{\rho_n^i(x_1, x_2, \cdots, x_n) | i = k, 2k, \cdots, n\},$$

式中$k|n$。记$|G_{n,k}(\boldsymbol{X})|$为轨道$G_{n,k}(\boldsymbol{X})$的大小,易知$|G_{n,k}(\boldsymbol{X})|$为$\dfrac{n}{k}$的因子。因为

$$G_{n,k}(\boldsymbol{X}) = G_{n,k}(\rho_n^i(\boldsymbol{X})) \quad (i = k, 2k, \cdots, n),$$

所以对于$\forall \boldsymbol{Y} = (y_1, y_2, \cdots, y_n) \in \mathrm{F}_2^n$,有

$$G_{n,k}(\boldsymbol{X}) = G_{n,k}(\boldsymbol{Y}) \text{或} G_{n,k}(\boldsymbol{X}) \cap G_{n,k}(\boldsymbol{Y}) = \varnothing。$$

定义2[18] 若$|G_{n,k}(\boldsymbol{X})| = d$,记

$$\boldsymbol{M}_{G_{n,k}(\boldsymbol{X})} = \begin{pmatrix} \rho_n^k(\boldsymbol{X}) \\ \rho_n^{2\cdot k}(\boldsymbol{X}) \\ \vdots \\ \rho_n^{(d-1)\cdot k}(\boldsymbol{X}) \\ \rho_n^{d\cdot k}(\boldsymbol{X}) \end{pmatrix}_{d \times n},$$

则称$\boldsymbol{M}_{G_{n,k}(\boldsymbol{X})}$为$G_{n,k}(\boldsymbol{X})$对应的轨道矩阵。

设 $F(\boldsymbol{X})$ 是一个 $(n,m)k$-RSBF, $\forall \boldsymbol{Y} \in \mathrm{F}_2^m$, $F^{-1}(\boldsymbol{Y})$ 是由一定数量的轨道组成。由于 $F(\boldsymbol{X})$ 在同一轨道上的取值相等,因此轨道矩阵对分析 $F^{-1}(\boldsymbol{Y})$ 具有重要意义。

引理 1.1[20]　设 $h_{d,k}$ 为 C_n^k 作用在 F_2^n 上得到的长度为 d 的轨道的个数,则

$$h_{d,k}=\frac{1}{d}\sum_{t|d}\mu(t)\cdot 2^{\frac{kd}{t}},$$

式中 $\mu(\cdot)$ 为莫比乌斯函数。

记 $\overline{\boldsymbol{X}}=(x_1+1,x_2+1,\cdots,x_n+1)$,则由 $\overline{\boldsymbol{X}}$ 生成的轨道为

$$\overline{G_{n,k}(\boldsymbol{X})}=$$
$$\left\{\rho_n^i(x_1+1,x_2+1,\cdots,x_n+1)|i=k,2k,\cdots,n\right\},$$

且 $|G_{n,k}(\boldsymbol{X})|=|\overline{G_{n,k}(\boldsymbol{X})}|$。称 $\overline{G_{n,k}(\boldsymbol{X})}$ 为 $G_{n,k}(\boldsymbol{X})$ 的共轭轨道。若 $G_{n,k}(\boldsymbol{X})=\overline{G_{n,k}(\boldsymbol{X})}$,则称 $G_{n,k}(\boldsymbol{X})$ 为自共轭轨道。因为自共轭轨道的向量中的分量是0、1各半,因此当 n 为奇数时不存在自共轭轨道。同时,由于自共轭轨道中的向量均是成对出现的,因此自共轭轨道的大小 $|G_{n,k}(\boldsymbol{X})|$ 为偶数。

已有研究中,Dalai等[21]、高光谱和刘文芬[22]分别给出了 $k=1$ 时,自共轭轨道的计数公式。田晔晨等[20]对其进行推广,得到了 k 为 n 的任意因子时,自共轭轨道的计数公式。

引理 1.2[20]　设 $h'_{d,k}$ 为 C_n^k 作用在 F_2^n 上得到的长为 d 的自共轭轨道个数,则

$$h'_{d,k}=\frac{1}{d}\left(2^{\frac{kd}{2}}-\sum_{t<\frac{d}{2},t\nmid\frac{d}{2}}t\cdot h'_{t,k}\right)。$$

定义 3[23]　设 $\boldsymbol{A}=(a_{ij})_{\omega\times n}$ 为 F_2 上的矩阵,若 F_2^m 中的每个向量在由 $\boldsymbol{A}$ 的任意 $m(1\leqslant m\leqslant n)$ 列所构成的子矩阵中出现的次数相同,则称 $\boldsymbol{A}$ 是一个 $(\omega,n,2,m)$ 正交表,简记作 $\mathrm{OA}(\omega,n,2,m)$。

引理 1.3[24-25]　一个 (n,m) 函数是 d 阶相关免疫的当且仅当对于 $\forall \boldsymbol{Y}\in\mathrm{F}_2^m$, $F^{-1}(\boldsymbol{Y})$ 中向量构成的矩阵均为 $\mathrm{OA}(|F^{-1}(\boldsymbol{Y})|,n,2,d)$。一个 (n,m) 函数是 d 阶弹性的当且仅当对于 $\forall \boldsymbol{Y}\in\mathrm{F}_2^m$,由 $F^{-1}(\boldsymbol{Y})$ 中向量构成的矩阵为 $\mathrm{OA}(2^{n-m},n,2,d)$。

2　平衡 $(n,m)k$-RSBF 存在的充分条件

本节讨论对于任意的正整数 n,平衡 $(n,m)k$-RSBF存在的充分条件及其构造方法。

引理 2.1[20]　若平衡 $(n,m)k$-RSBF 存在,则平衡 $(n,m-1)k$-RSBF也存在。

定理 2.1　设 $n=p_1^{r_1}p_2^{r_2}\cdots p_t^{r_t}(\forall i<j,p_i<p_j$ 为素数,$r_i\in\mathbf{Z}^+)$,当 $\frac{n}{k}=p_i^{s_i}(p_i$ 为奇素数,$1\leqslant s_i\leqslant r_i)$时,对 $\forall 2\leqslant m\leqslant k$,平衡 $(n,m)k$-RSBF存在。

证明　由引理2.1知,只需要证明平衡 $(n,k)k$-RSBF存在。

设 $h_{d,k}$ 为 C_n^k 作用于 F_2^n 上所得长度为 d 的轨道个数,由引理1.1得轨道分布如下:

$$\begin{cases}h_{1,k}=2^k,\\ h_{p_i,k}=\dfrac{1}{p_i}(2^{p_i\cdot k}-2^k),\\ \cdots\\ h_{p_i^{s_i},k}=\dfrac{1}{p_i^{s_i}}(2^{p_i^{s_i}\cdot k}-2^{p_i^{s_i-1}\cdot k})。\end{cases}$$

则有

$$\begin{cases}\dfrac{h_{1,k}}{2^k}=1,\\ \dfrac{h_{p_i,k}}{2^k}=\dfrac{1}{p_i}(2^{p_i\cdot k-k}-1),\\ \cdots\\ \dfrac{h_{p_i^{s_i},k}}{2^k}=\dfrac{1}{p_i^{s_i}}(2^{p_i^{s_i}\cdot k-k}-2^{p_i^{s_i-1}\cdot k-k})。\end{cases}$$

其中,

$$\begin{aligned}\frac{h_{p_i^s,k}}{2^k}&=\frac{1}{p_i^s}(2^{p_i^s\cdot k-k}-2^{p_i^{s-1}\cdot k-k})=\\ &\frac{2^{p_i^{s-1}\cdot k-k}}{p_i^s}((2^{p_i^s-p_i^{s-1}})^k-1)=\\ &\frac{2^{p_i^{s-1}\cdot k-k}}{p_i^s}(2^{p_i^s-p_i^{s-1}}-1)((2^{p_i^s-p_i^{s-1}})^{k-1}+\cdots+\\ &2^{p_i^s-p_i^{s-1}}+1),\quad(0\leqslant s\leqslant s_i)。\end{aligned}$$

由于2与 p 互素,由欧拉定理知 $p_i^s|(2^{p_i^s-p_i^{s-1}}-1)$,因此 $\frac{h_{1,k}}{2^k},\frac{h_{p_i,k}}{2^k},\cdots,\frac{h_{p_i^{s_i},k}}{2^k}$ 均为整数。将每 $\frac{h_{p_i^s,k}}{2^k}$ 个轨道合并,则长为 $p_i^s(0\leqslant s\leqslant s_i)$ 的 $h_{p_i^s,k}$ 个轨道被划分为 2^k 个集合,记这 2^k 个集合为 $V_1^s,V_2^s,\cdots,V_{2^k}^s$,且 $|V_j^s|=\frac{p_i^s h_{p_i^s,k}}{2^k},(1\leqslant j\leqslant 2^k)$。

将所有不同长度的轨道按照如上方式划分,令 $V_j=V_j^0\cup V_j^1\cup\cdots\cup V_j^{s_i}$,则

$$|V_j|=\sum_{s=0}^{s_i}p^s\frac{h_{p^s,k}}{2^k}=\frac{1}{2^k}\sum_{s=0}^{s_i}p^s h_{p^s,k}=2^{n-k},(1\leqslant j\leqslant 2^k),$$

即所有输入向量按照轨道被分为了 2^k 个集合。

令一个集合作为同一输出向量的原像集合,即构造1个F_2^n上的n元k输出的函数$F(\boldsymbol{X})$,其中,

$$F^{-1}(\boldsymbol{Y}_i)=V_i,\ \boldsymbol{Y}_i\in\mathrm{F}_2^k,\ 1\leqslant i\leqslant 2^k,$$

即得到平衡$(n,k)k$-RSBF。由引理2.1,对$\forall 2\leqslant m\leqslant k$,平衡$(n,m)k$-RSBF均存在。

注　对于任意长为d的所有$h_{d,k}$个轨道,若满足$2^m|h_{d,k}$且最短轨道至少可以划分为2^m个集合(即$\frac{n}{k}$为奇素数方幂且$m\leqslant k$),那么平衡$(n,m)k$-RSBF存在。

定理2.1给出了对于任意正整数n,当$\frac{n}{k}$为奇素数方幂时,平衡$(n,m)k$-RSBF存在的充分条件。下面考虑当$\frac{n}{k}$的值为2的方幂时,平衡$(n,m)k$-RSBF的存在情况。

定理2.2　设n为偶数,当$\frac{n}{k}=2^r(r\in\mathbf{Z}^+)$时,对$\forall 2\leqslant m\leqslant n-r$,平衡$(n,m)k$-RSBF存在。

证明　只需证明平衡$(n,n-r)k$-RSBF存在。

设$h_{d,k}$为C_n^k作用在F_2^n上得到的长度为d的轨道个数,由轨道计数公式可得轨道分布为

$$\begin{cases}h_{1,k}=2^k,\\ h_{2,k}=\dfrac{1}{2}(2^{2\cdot k}-2^k),\\ \cdots\\ h_{2^r,k}=\dfrac{1}{2^r}(2^{2^r\cdot k}-2^{2^{r-1}\cdot k})。\end{cases}$$

对上述轨道进行如下划分:

(1)将大小为1的轨道两两任意合并,得到$a_0=\frac{h_{1,k}}{2}$个大小为2的集合,至此共得到$a_0+h_{2,k}$个大小为2的集合;

(2)将(1)中得到的大小为2的集合两两任意合并后得到$a_1=\frac{a_0+h_{2,k}}{2}$个大小为4的集合,至此共得到$a_1+h_{2^2,k}$个大小为4的集合;

……

(r)将(r-1)中大小为2^{r-1}的集合两两任意合并后得到$a_{r-1}=\frac{a_{r-2}+h_{2^{r-1},k}}{2}$个大小为$2^r$的集合,至此共得到$a_{r-1}+h_{2^r,k}=2^{n-r}$个大小为$2^r$的集合。

记第(r)步中得到的2^{n-r}个集合为

$$V_1,V_2,\cdots,V_{2^{n-r}},|V_i|=2^r,\quad(1\leqslant i\leqslant 2^{n-r})。$$

从而可以构造出F_2上n元$n-r$输出的函数$F(\boldsymbol{X})$,其中,

$$F^{-1}(\boldsymbol{Y}_i)=V_i,\ \boldsymbol{Y}_i\in\mathrm{F}_2^{n-r},\ 1\leqslant i\leqslant 2^{n-r}。$$

则$F(\boldsymbol{X})$为平衡$(n,n-r)k$-RSBF。由引理2.1知,对$\forall 2\leqslant m\leqslant n-r$,平衡$(n,m)k$-RSBF存在。

注　当$\frac{n}{k}=2^r$时,如果最长轨道的长度最大为2^{n-m},即此时满足$m\leqslant n-r$,那么就可通过递归的方法对轨道进行划分,逐步将2^n个输入向量划分为2^m个大小为2^{n-m}的集合。令同一集合的向量对应同一函数值,即构造出平衡$(n,m)k$-RSBF。

3　1阶弹性$(n,m)k$-RSBF存在的充分条件

本节讨论对任意正整数n,1阶弹性$(n,m)k$-RSBF存在的充分条件及其构造性证明。

引理3.1[20]　若1阶弹性$(n,m)k$-RSBF存在,则1阶弹性$(n,m-1)k$-RSBF也存在。

定理3.1　设$n=p_1^{r_1}p_2^{r_2}\cdots p_t^{r_t}$(对$\forall i<j,p_i<p_j$是素数,$r_i\in\mathbf{Z}^+$),当$\frac{n}{k}=p_i^{s_i}$($p_i$为奇素数,$1\leqslant s_i\leqslant r_i$)时,对于$\forall 2\leqslant m\leqslant k-1$,1阶弹性$(n,m)k$-RSBF存在。

证明　由引理3.1,只需要证明1阶弹性$(n,k-1)k$-RSBF存在。

设$h_{d,k}$为C_n^k作用于F_2^n上得到的长度为d的轨道个数,由轨道计数公式,计算得函数的轨道分布为

$$\begin{cases}h_{1,k}=2^k,\\ h_{p_i,k}=\dfrac{1}{p_i}(2^{p_i\cdot k}-2^k),\\ \cdots\\ h_{p_i^{s_i},k}=\dfrac{1}{p_i^{s_i}}(2^{p_i^{s_i}\cdot k}-2^{p_i^{s_i-1}\cdot k})。\end{cases}$$

由定理2.1证明可知,$\frac{h_{1,k}}{2^k},\frac{h_{p_i,k}}{2^k},\cdots,\frac{h_{p_i^{s_i},k}}{2^k}$均为整数。设长为$p_i^s(0\leqslant s\leqslant s_i)$的$h_{p_i^s,k}$个轨道为$G_1,G_2,\cdots,G_{h_{p_i^s,k}}$。由于$p_i^s$为奇数,因此不存在自共轭轨道。令

$$U=\left\{\begin{pmatrix}M_{G_l}\\ M_{G_{l'}}\end{pmatrix}|\overline{G_l}=G_{l'},1\leqslant l,l'\leqslant h_{p_i^s,k}\right\}。$$

由正交表定义知,U中的元素均为正交表$\mathrm{OA}(2p_i^s,n,2,1)$,且$|U|=\frac{h_{p_i^s,k}}{2}$。从而长为$p_i^s$的$h_{p_i^s,k}$个

轨道被分为了$\frac{h_{p_i^s,k}}{2}$个大小为$2p_i^s$的集合,且集合中的向量构成正交表OA$(2p_i^s, n, 2, 1)$。将上述$\frac{h_{p_i^s,k}}{2}$个集合每$\frac{\frac{h_{p_i^s,k}}{2}}{2^{k-1}}$个合并,则长为$p_i^s$的$h_{p_i^s,k}$个轨道被划分为$2^{k-1}$个集合,并且集合中的向量构成正交表OA$(p_i^s\frac{h_{p_i^s,k}}{2^{k-1}}, n, 2, 1)$。记这$2^{k-1}$个集合为

$$V_1^s, V_2^s, \cdots, V_{2^{k-1}}^s, |V_j^s| = \frac{p_i^s h_{p_i^s,k}}{2^{k-1}}, (1 \leqslant j \leqslant 2^{k-1})。$$

将所有不同长度的轨道按照上述方式划分,令$V_j = V_j^0 \cup V_j^1 \cup \cdots \cup V_j^{s_i}$, 则

$$|V_j| = \sum_{s=0}^{r-1} p^s \frac{h_{p^s,k}}{2^{k-1}} = 2^{k-1}\sum_{s=0}^{r-1} p^s h_{p^s,k} = 2^{n-k+1}。$$

所有输入向量按照轨道被分为了2^{k-1}个集合:

$$V_1, V_2, \cdots, V_{2^{k-1}}, |V_j| = 2^{n-k+1}。$$

令一个集合作为输出向量的原像集,即构造1个F_2^n上的n元$k-1$输出的函数$F(\boldsymbol{X})$,其中

$$F^{-1}(\boldsymbol{Y}_i) = V_i, \boldsymbol{Y}_i \in F_2^{k-1}, 1 \leqslant i \leqslant 2^{k-1}。$$

则$F(\boldsymbol{X})$为1阶弹性$(n, k-1)k$-RSBF. 由引理3.1,对$\forall 2 \leqslant m \leqslant k-1$, 1阶弹性$(n, m)k$-RSBF存在。

例3.1　设$n = 2^2 \cdot 3, k = 4$, $\forall 2 \leqslant m \leqslant 3$, 则1阶弹性$(n, m)k$-RSBF存在。

只需要说明1阶弹性(12, 3)4-RSBF存在。其构造方法如下:

将$2^n = 2^{12}$ =4 096个输入向量通过循环群C_n^k作用后划分为若干轨道,由轨道计数公式得

$$\begin{cases} h_{1,4} = 16, \\ h_{3,4} = 1360。 \end{cases}$$

将长为1的16个轨道中互为共轭的轨道两两任意合并,得到8组正交表OA(2, 6, 2, 1);将长为3的1 360个轨道中互为共轭的轨道两两任意合并,得到680组正交表OA(6, 6, 2, 1);再将这680组正交表任意每85组合并得到8组OA(512, 6, 2, 1)。

至此所有4 096个输入向量被划分为8组正交表OA(512, 6, 2, 1)。记为$V_1, V_2, \cdots, V_8$。

从而可以构造出12元3输出函数$F = (f_1, f_2, f_3)$,其中

$$F^{-1}(\boldsymbol{Y}_i) = V_i, \boldsymbol{Y}_i \in F_2^3, 1 \leqslant i \leqslant 8。$$

由于篇幅限制,函数的真值表省略。

通过Matlab进行仿真测试,可以验证$F(\boldsymbol{X})$为1阶弹性(12, 3)4-RSBF。通过MATLAB计算,上述方式构造出来的1阶弹性(12, 3)4-RSBF的非线性度为1 868。

注　对于任意长为d的所有$h_{d,k}$个轨道,若满足$2^m | \frac{h_{d,k}}{2}$且最短轨道可以划分为2^m个OA$(2, n, 2, 1)$(即$\frac{n}{k}$的值为奇素数方幂且$m \leqslant k-1$),那么1阶弹性$(n, m)k$-RSBF存在。

定理3.1利用共轭轨道的性质以及弹性函数与正交表之间的关系,通过构造出正交表,给出了对于任意正整数n,当$\frac{n}{k}$的值为奇素数的方幂时,1阶弹性$(n, m)k$-RSBF存在的充分条件。下面考虑当$\frac{n}{k}$为2的方幂时,1阶弹性$(n, m)k$-RSBF存在的充分条件。

定理3.2　设n为偶数,当$\frac{n}{k} = 2^r (r \in \mathbf{Z}^+)$时,对$\forall 2 \leqslant m \leqslant n-r-1$, 1阶弹性$(n, m)k$-RSBF存在。

证明　由引理3.1知,只需证明1阶弹性$(n, n-r-1)k$-RSBF存在。

用循环群C_n^k作用于空间F_2^n上,将F_2^n划分为若干轨道,设$h_{d,k}$为长度为d的轨道个数,由轨道计数公式,计算不同轨道长度个数如

$$\begin{cases} h_{1,k} = 2^k, \\ h_{2,k} = \frac{1}{2}\left(2^{2\cdot k} - 2^k\right), \\ \cdots \\ h_{2^r,k} = \frac{1}{2^r}\left(2^{2^r\cdot k} - 2^{2^{r-1}\cdot k}\right)。 \end{cases}$$

设长为$2^s (0 \leqslant s \leqslant r)$的$h_{2^s,k}$个轨道为$G_1^s, G_2^s, \cdots, G_{h_{2^s,k}}^s$。令

$$U^s = \left\{G_l^s \cup G_{l'}^s | \overline{G_l^s} = G_{l'}^s, 1 \leqslant l, l' \leqslant h_{2^s,k}\right\},$$

$$V^s = \left\{G_l^s | \overline{G_l^s} = G_l^s, 1 \leqslant l \leqslant h_{2^s,k}\right\}。$$

对上述轨道按照如下方式划分:

(1) $s = 0$, U^0中均为可构成OA$(2, n, 2, 1)$的元素,且$|V^0| = 0$,则长为$2^0 = 1$的$h_{1,k}$个轨道被分为了$a_0 = \frac{h_{1,k}}{2}$个集合,每个集合中的元素均构成OA$(2, n, 2, 1)$。再把a_0个集合两两任意合并为$\frac{a_0}{2}$个集合,则集合中的元素均可构成正交表OA$(4, n, 2, 1)$。

(2) $s=1$, U^1中均为可构成OA$(4,n,2,1)$的元素, V^1的大小为偶数,将V^1中的轨道两两任意合并,则长为2^1的$h_{2,k}$个轨道被分为了$\frac{h_{2,k}}{2}$个集合,每个集合均可构成OA$(4,n,2,1)$,至此共得到$a_1=\frac{h_{2,k}+a_0}{2}$个可构成OA$(4,n,2,1)$的集合,再两两任意合并,得到$\frac{a_1}{2}$个其元素可构成OA$(8,n,2,1)$的集合。

……

(r+1) $s=r$, U^r中元素均为OA$(2\cdot 2^r,n,2,1)$, V^r的大小为偶数,将V^r中的轨道两两任意合并,则长度为2^r的$h_{2^r,k}$个轨道被分为了$\frac{h_{2^r,k}}{2}$个集合,集合中的元素均构成OA$(2^{r+1},n,2,1)$。至此,所有的输入向量集合被划分为了$a_r=\frac{h_{2^r,k}+a_{r-1}}{2}=2^{n-r-1}$个可构成OA$(2^{r+1},n,2,1)$的集合。

记第(r+1)步得到的2^{n-r-1}个集合为

$V_1,V_2,\cdots,V_{2^{n-r-1}}$,且$|V_i|=2^{r+1}(1\leqslant i\leqslant 2^{n-r-1})$。

从而可以构造出F_2^n上n元$n-r-1$输出的函数,其中

$$F^{-1}(\boldsymbol{Y}_i)=V_i,\ \boldsymbol{Y}_i\in\mathrm{F}_2^{n-r-1},\ 1\leqslant i\leqslant 2^{n-r-1},$$

则$F(\boldsymbol{X})$为1阶弹性$(n,n-r-1)k$-RSBF。由引理3.1知, $\forall 2\leqslant m\leqslant n-r-1$, 1阶弹性$(n,m)k$-RSBF存在。

例 3.2 设$n=2\cdot 3$, $k=3$, $\forall 2\leqslant m\leqslant 4$,则1阶弹性$(n,m)k$-RSBF存在。

只需说明1阶弹性$(6,4)3$-RSBF存在。其具体构造方法如下:

将$2^n=2^6=64$个输入向量空间用循环群作用划分为若干轨道,由轨道计数公式,得

$$\begin{cases}h_{1,3}=8,\\ h_{2,3}=28。\end{cases}$$

将长1的8个轨道,互为共轭的轨道两两合并为4组正交表OA$(2,6,2,1)$,再两两任意合并为2组正交表OA$(4,6,2,1)$;将长为2的28个轨道中自共轭轨道两两任意合并,互为共轭的轨道两两合并,得到14组正交表OA$(4,6,2,1)$。至此所有64个输入向量被划分为16组正交表OA$(4,6,2,1)$。记这16个集合为$V_1,V_2,\cdots,V_{16}$。

从而可以构造出6元4输出的函数$G=(g_1,g_2,g_3,g_4)$,其中

$$G^{-1}(\boldsymbol{Y}_i)=V_i,\ \boldsymbol{Y}_i\in\mathrm{F}_2^4,\ 1\leqslant i\leqslant 16。$$

函数$G(\boldsymbol{X})$的真值表(十六进制表示)为

g_1: 013E5E6E767A7C80,

g_2: 1F031DADB5B8C0F8,

g_3: 678F870A50E1F1E6,

g_4: 2A15AE5DBA75A854。

通过Matlab进行仿真测试,可以验证$G(\boldsymbol{X})$为1阶弹性$(6,4)3$-RSBF。通过Matlab计算,上述方式构造出来的1阶弹性$(6,4)3$-RSBF的非线性度为8。

注 当$\frac{n}{k}=2^r$时,如果最长轨道至多可以划分为1个OA$(2^{n-m},n,2,1)$,那么就可以通过递归,逐步将2^n个输入向量划分为2^m组,使得每组均为OA$(2^{n-m},n,2,1)$,将同一组中向量赋予同一输出值,即构造出1阶弹性$(n,m)k$-RSBF。

4 结束语

本文基于循环群C_n^k在空间F_2^n上的作用,利用轨道划分及构造正交表的方法,分别给出了对于任意正整数n,当$\frac{n}{k}$为奇素数方幂和2的方幂时,满足平衡性和1阶弹性的多输出旋转对称布尔函数存在的充分条件及其构造性证明。推广了田晔晨等[20]结果,得到了对一般的n和k, n维m输出k-RSBF存在的充分条件,并且对所构造出来的函数进行了仿真测试。通过研究这一类特殊的多输出布尔函数,进而去寻找密码学性质优良的多输出布尔函数,不论是在理论上,还是在实践上都具有重要意义。目前有关多输出k-旋转对称函数构造的研究相对较少,对于具有良好密码学性质的多输出旋转对称布尔函数,比如代数免疫度、非线性度和相关免疫性方面,还有许多工作要做。对于这些特性的研究将是今后工作的一个课题。

参 考 文 献

[1] FILIOL E, FONTAINE C. Highly nonlinear balanced boolean functions with a good correlation-immunity[C]// NYBERG K. Advances in Cryptology-Eurocrypt'98: international conference on the theory and application of cryptographic techniques. Lecture Notes in Computer Science, vol 1403. Heidelberg: Springer, 1998: 475-488.

[2] PIEPRZYK J, QU C X. Fast hashing and rotation-symmetric functions[J]. Journal of Universal Computer

Science,1999,5(1):20-31.

[3] KAVUT S, MAITRA S, SARKAR S, et al. Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity>240 [C]//BARUA R, LANGE T. Progress in Crytology-INDOCRYPT 2006. Lecture Notes in Computer Science, vol 4329. Heidelberg: Springer,2006:266-279.

[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, 53(5):1743-1751.

[5] STĂNICĂ P, MAITRA S. Rotation symmetric Boolean functions-count and cryptographic properties [J]. Discrete Applied Mathematics, 2008, 156(10): 1567-1580.

[6] KAVUT S, YÜCEL M D. Generalized rotation symmetric and dihedral symmetric Boolean functions-9 variable boolean functions with nonlinearity 242 [C]// BOZTAS, LU H F. Applied algebra, algebraic algorithms and error-correcting codes: 17th international symposium. Lecture Notes in Computer Science, vol 4851. Heidelberg: Springer, 2007: 321-329.

[7] SIEGENTHALER T. Correlation-immunity of nonlinear combining functions for cryptographic applications [J]. IEEE Transactions on Information Theory, 1984, 30(5): 776-780.

[8] CHOR B, GOLDREICH O, HASTED J, et al. The bit extraction problem or t-resilient functions [C]//26th Annual Symposium on Foundations of Computer Science. SFCS 1985. Portland: IEEE, 1985: 396-407.

[9] STINSON D R. Resilient functions and large sets of orthogonal arrays [J]. Congressus Numerantium, 1993, 92:105-110.

[10] 杜蛟,温巧燕,张勐,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.

[11] DU J, WEN Q, ZHANG J, et al. Construction and counting of 1-resilient rotation symmetric Boolean functions on pq variables [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013, 96A(7):1653-1656.

[12] DU J, PANG S, WEN Q, 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.

[13] DU J, WEN Q, ZHANG J, et al. Constructions of resilient rotation symmetric Boolean functions on given number of variables [J]. IET Information Security, 2014, 8(5):265-272.

[14] DU J, FU S, QU L, et al. New constructions of q-variable 1-resilient rotation symmetric functions over F_p [J]. Science China Information Science, 2016, 59(079102):1-3.

[15] PANG S, XU W, DU J, et al. Construction and count of 1-resilient rotation symmetric Boolean functions on $4p$ variables [J]. Chinese Journal of Electronics, 2017, 26(6):1276-1283.

[16] PANG S, WANG X, WANG J, et al. Construction and count of 1-resilient rotation symmetric Boolean functions [J]. Information Sciences, 2018, 450:336-342.

[17] 元彦斌,赵亚群.多输出旋转对称函数的密码学性质[J].通信学报,2009,30(11A):1-7.

[18] 杜蛟,尚玉婧,赵金玲,等.8元多输出旋转对称弹性函数的构造与计数[J].通信学报,2017,38(7):47-55.

[19] DU J, FU S J, QU L J, et al. The existence of a class of balanced multi-output rotation symmetric Boolean functions [J]. Chinese Journal of Electronics, 2018, 27(5):995-1001.

[20] 田晔晨,孙玉娟,李路阳.多输出弹性k-旋转对称布尔函数的存在性与构造[J].密码学报,2020,8(1):96-109.

[21] DALAI D K, MAITRA S, SARKAR S. Results on rotation symmetric bent functions [J]. Discrete Mathematics, 2009, 309(8):2398-2409.

[22] 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,2012,34(9):2273-2276.

[23] CAMION P, CARLET C, CHARPIN P, et al. On correlation-immune functions [C]//FEIGENBAUM J. Advances in Cryptology-CRYPTO'91. Lecture Notes in Computer Science, vol 576. Heidelbery: Springer, 1991: 86-100.

[24] CAMION P, CANTEAUT A. Correlation-immune and resilient functions over a finite alphabet and their applications in cryptography [J]. Designs, Codes and Cryptography, 1999, 16(2):121-149.

[25] GOPALAKRISHNAN K, STINSON D R. Three characterizations of non-binary correlation-immune and resilient functions [J]. Designs, Codes and Cryptography, 1995, 5(3):241-251.

(责任编辑:马田田)