doi:10.11959/j.issn.1000-436x.2017140

8 元多输出旋转对称弹性函数的构造与计数

杜蛟[1]，尚玉婧[1]，赵金玲[1]，董乐[1]，张恩[2]
（1. 河南师范大学数学与信息科学学院，河南 新乡 453007；2. 河南师范大学计算机与信息工程学院，河南 新乡 453007）

摘 要：在 2^r 个变元的多输出旋转对称平衡函数和弹性函数存在的条件下，研究了输出变量维数的取值问题。根据输出变量的不同维数，基于弹性函数和正交表大集间的等价关系，给出了 8 元多输出平衡函数的计数结果，在此基础上进一步研究了 8 元多输出旋转对称 1-弹性函数的构造与计数方法，将这类函数的构造问题转化为方程组的求解问题。

关键词：密码学；旋转对称函数；平衡函数；弹性函数；支撑矩阵
中图分类号：TN918.1 **文献标识码**：A

Construction and count of multi-output rotation symmetric resilient functions with 8 input variables

DU Jiao[1], SHANG Yu-jing[1], ZHAO Jin-ling[1], DONG Le[1], ZHANG En[2]
(1. College of Mathematics and Information Science, Henan Normal University, Xinxiang 453007, China;
2. College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China)

Abstract: The value ranges of the number of output variables were determined respectively under the existence of multi-output rotation symmetric balanced functions and resilient functions with 2^r input variables. Based on the equivalence between the resilient functions and large sets of orthogonal arrays, some results on the construction and count of multi-output rotation symmetric balanced functions with 8 input variables were presented according to the different dimensions of output vectors, and construction and count of multi-output rotation symmetric 1-resilient functions with 8 input variables were also studied. Besides, constructions of multi-output rotation symmetric resilient functions are transformed into the problem of solving a system of equations.

Key words: cryptography, rotation symmetric function, balanced function, resilient function, support table

1 引言

Filiol 和 Fontaine[1]首先在特征为 2 的有限域上提出了“幂等元”的概念，Pieprzyk 和 Qu 在文献[2]中提出了旋转对称函数（RSBF, rotation symmetric function）的概念，文献[3]进一步指出了幂等元与旋转对称函数的关系，即旋转对称函数可以由幂等元在相应的有限域中通过适当地选择正规基变形而得到。事实上，自 1999 年以来，旋转对称函数就成为这类函数的标准术语[2]。RSBF 是一类在输入变量周期性旋转变化时，函数值保持不变的函数，这类函数不仅数量丰富，而且容易快速实现，因而被用于某些密码算法（如 MD4、MD5 和 HAVAL 等轮函数）的快速实现中[2]。近年来，人们在旋转对称函数类中得到了诸多令人满意的结果[4~7]。2006 年， Kavut 等[8]利用最速下降法在旋转对称函数类中找到了非线性度为 241 的 9 元旋转对称函数，随后他们又证明了这是 9 元旋转对称函数所能达到的最大非线性度，在此基础上进一步找到了非线性度为 242 的 9 元 3 阶旋转对称布尔函数，利用该结果，

收稿日期：2017-02-07；**修回日期**：2017-05-17
基金项目：国家自然科学基金资助项目（No.U1404601, No.11571094, No.61402154, No.U1604156）；河南师范大学博士科研启动基金资助项目（No.5101019170133）
Foundation Items: The National Natural Science Foundation of China (No.U1404601, No.11571094, No.61402154, No.U1604156), PhD Research Startup Foundation of Henan Normal University (No.5101019170133)

证明了9元、11元、13元非线性度大于$2^{n-1}-2^{\frac{n-1}{2}}$的布尔函数的存在性，彻底解决了30年来一个悬而未决的公开问题[7,8]。实验表明旋转对称布尔函数可以同时具有多个良好的密码学性质，如平衡性、最优代数免疫性、较高的代数次数、相关免疫性、较高的非线性度等[4,6,7]。因而构造具有特殊密码学性质的旋转对称函数就是一个具有重要理论意义的工作，也是当前密码学领域的一个热点问题，出现了一大批研究成果[4,6~17]。

对称布尔函数作为旋转对称布尔函数的一个子类，其平衡性、相关免疫性、弹性首先得到了深入的研究[11]。Stanica 等[3,4]研究了平衡以及相关免疫的旋转对称函数的构造问题，文献[12]进一步研究了这个问题。文献[13~17]基于弹性函数与正交表大集间的关系研究了单输出旋转对称弹性函数的构造与计数问题。文献[18]给出了多输出旋转对称函数的概念，研究了多输出旋转对称函数的平衡性、相关免疫性等密码学性质，给出了满足这些性质的充分必要条件。

由于在分组密码中的广泛应用，多输出布尔函数尤其是具有特殊性质的多输出布尔函数在密码体制中逐渐扮演着重要角色。旋转对称S盒具有良好的密码学性质，如低差分均匀度、高代数次数、高非线性度等[10,19,20]，这就启发本文从旋转对称S盒中寻找具有多个密码学性质的S盒。到目前为止，已有诸多文献研究旋转对称S盒的相关问题，文献[18~23]研究了旋转对称S盒的设计与某些密码学性质，但是关于给定参数的旋转对称弹性S盒的存在性、构造与计数等一系列问题的结果仍然很少，因而旋转对称弹性S盒的构造问题就是一个具有重要理论意义的公开问题。文献[17]研究了素数幂元的旋转对称单输出弹性函数的构造与计数问题，文献[20]从部分8元平衡的旋转对称函数中搜索到了5 382个非线性度为116的函数，本文首先研究了当$n=2^r$时，多输出旋转对称平衡函数的输出变元的维数m的取值范围，进一步研究了当变元个数$n=8$时，m取不同值时的多输出旋转对称平衡函数的计数问题，以及多输出旋转对称弹性函数的构造与计数方法。

2 基础知识

设F_2表示二元域{0,1}，对任一取定的正整数n，以F_2^n表示F_2上的n维向量空间，称$F_2^n\to F_2$的任一映射f为n变元布尔函数，即当$\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in F_2^n$，$f(\boldsymbol{x})=f(x_1,x_2,\cdots,x_n)\in F_2$时，若$f(\boldsymbol{x})=1$，则称$\boldsymbol{x}$为函数$f(\boldsymbol{x})$的支撑向量。设$f_i(\boldsymbol{x})$为$F_2^n\to F_2$上的布尔函数，称$F(\boldsymbol{x})=(f_1(\boldsymbol{x}),f_2(\boldsymbol{x}),\cdots,f_m(\boldsymbol{x}))$为$F_2^n\to F_2^m$上的$n$个变元$m$个输出的多输出布尔函数，简记为$(n,m)$函数，这里，$1\leqslant i\leqslant m\leqslant n$。多输出布尔函数也称为向量值布尔函数或S盒，其中，$f_i(\boldsymbol{x})$称为分量函数或坐标函数。

定义1[3,4] 设$f(\boldsymbol{x})$为n元布尔函数，任取$\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in F_2^n$，令

$$\rho_n^k(x_i)=\begin{cases}x_{i+k}, & i+k\leqslant n\\ x_{i+k-n}, & i+k>n\end{cases},\ 1\leqslant i\leqslant n$$

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

若对$\forall(x_1,x_2,\cdots,x_n)\in F_2^n$均有

$$f(\rho_n^k(x_1,x_2,\cdots,x_n))=f(x_1,x_2,\cdots,x_n)$$

对$0\leqslant k\leqslant n-1$成立，则称$f(\boldsymbol{x})$为旋转对称函数。

RSBF_n表示所有n元旋转对称布尔函数构成的集合，循环群$\{\rho_n^k\mid 0\leqslant k\leqslant n-1\}$作用在$F_2^n$上，将$F_2^n$中的向量分为如下形式的轨道。

$$O_n(\boldsymbol{x})=\{\rho_n^k\mid 0\leqslant k\leqslant n-1,\boldsymbol{x}\in F_2^n\}$$

而旋转对称函数$f(\boldsymbol{x})$在每一个轨道上取相同的函数值，这里，$O_n(\boldsymbol{x})$是由x生成的轨道，并且轨道的总数g_n和长轨道的总数h_n分别为[4]

$$g_n=\frac{1}{n}\sum_{t\mid n}\varphi(t)2^{\frac{n}{t}},\ h_n=\frac{1}{n}\sum_{t\mid n}\mu(t)2^{\frac{n}{t}}$$

其中，$\varphi(t)$为欧拉函数，$\mu(t)$为莫比乌斯函数。

定义2[16,17,24] 设$f(\boldsymbol{x})=f(x_1,x_2,\cdots,x_n)$为$n$元布尔函数，$\boldsymbol{x}\in F_2^n$，若$f(\boldsymbol{x})=1$，则称$\boldsymbol{x}$为函数$f(\boldsymbol{x})$的支撑向量。$f(\boldsymbol{x})$的所有支撑向量按照一定的顺序排列的矩阵$\boldsymbol{C}_f$称为$f(\boldsymbol{x})$的支撑矩阵。

$$\boldsymbol{C}_f=\begin{pmatrix}c_{11}&c_{12}&\cdots&c_{1n}\\ c_{21}&c_{22}&\cdots&c_{2n}\\ \vdots&\vdots&\ddots&\vdots\\ c_{w1}&c_{w2}&\cdots&c_{wn}\end{pmatrix}=\begin{pmatrix}\boldsymbol{d}_1&\boldsymbol{d}_2&\cdots&\boldsymbol{d}_n\end{pmatrix}$$

其中，$\boldsymbol{d}_i$是$\boldsymbol{C}_f$的第i个列向量，$1\leqslant i\leqslant n$。

定义3[17] 设$f(\boldsymbol{x})\in\mathrm{RSBF}_n$且$|O_n(\boldsymbol{x})|=t$，轨道

$O_n(\boldsymbol{x})$ 中的所有向量按如下方式排列得到的矩阵被称为轨道矩阵。

$$\boldsymbol{C}_{O_n(\boldsymbol{x})}=\begin{pmatrix}\boldsymbol{x}\\ \rho_n(\boldsymbol{x})\\ \vdots\\ \rho_n^{t-1}(\boldsymbol{x})\end{pmatrix}=\begin{pmatrix}\boldsymbol{u}_1 & \boldsymbol{u}_2 & \cdots & \boldsymbol{u}_n\end{pmatrix}$$

其中，$\boldsymbol{u}_i$ 是轨道矩阵 $\boldsymbol{C}_{O_n(\boldsymbol{x})}$ 的第 i 列，$1\leqslant i\leqslant n$，$\omega t(\boldsymbol{u}_i)$ 为 $\boldsymbol{u}_i$ 的汉明重量。

$\boldsymbol{R}^{\mathrm{T}}$ 表示矩阵 $\boldsymbol{R}$ 的转置，$\boldsymbol{k}_r$ 表示 r 个 k 构成的列向量，如果 $\boldsymbol{A}=(a_{ij})_{n_1\times m_1}$，$\boldsymbol{B}=(a_{ij})_{n_2\times m_2}$，那么矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 的 Kronecker 积定义为 $\boldsymbol{A}\otimes\boldsymbol{B}=(a_{ij}\boldsymbol{B})_{n_1n_2\times m_1m_2}$，显然有 $\boldsymbol{C}_{O_n(\boldsymbol{x})}=\begin{pmatrix}\boldsymbol{u}_1 & \boldsymbol{u}_2 & \cdots & \boldsymbol{u}_n\end{pmatrix}=\boldsymbol{1}_s^{\mathrm{T}}\otimes\boldsymbol{M}$，其中，$\boldsymbol{M}=\begin{pmatrix}\boldsymbol{u}_1 & \boldsymbol{u}_2 & \cdots & \boldsymbol{u}_t\end{pmatrix}$ 为一个 $t\times t$ 的循环矩阵，并且 $n=st$，因此，有 $\omega t(\boldsymbol{u}_1)=\omega t(\boldsymbol{u}_2)=\cdots=\omega t(\boldsymbol{u}_n)$。$\boldsymbol{C}_f$ 是由若干个轨道矩阵构成的，若函数 $f(\boldsymbol{x})$ 是一个 RSBF，那么 $f(\boldsymbol{x})$ 在每一个轨道上的向量所取的函数值是相同的，因而旋转对称布尔函数的轨道矩阵在对其支撑矩阵(布尔函数的一个原像集)的分析中起着重要的作用。本文在不考虑向量顺序的情况下，将 $\boldsymbol{S}$ 看成一个行向量的矩阵。

本文需要一些定义和符号来表述结果。从 n 个元素中选取 k 个的方法数记为组合数 C_n^k。假设 $\boldsymbol{u}_i(1\leqslant i\leqslant n)$ 是 $\boldsymbol{C}_{O_n(\boldsymbol{x})}$ 的第 i 个列向量，$h_{l,\omega}$ 是 $O_{l,\omega}=\{O_n(\boldsymbol{x})\,|\,\omega t(\boldsymbol{u}_1)=\omega,|O_n(\boldsymbol{x})|=l\}$ 中不同轨道的总个数，那么

$$h_{l,\omega}=|O_n(\boldsymbol{x})|=\left|\{O_n(\boldsymbol{x})\,|\,\omega t(\boldsymbol{u}_1)=\omega,|O_n(\boldsymbol{x})|=l\}\right|$$

设 $h_l=\sum_{\omega=1}^{l-1}h_{l,\omega}$ 表示集合 $\bigcup_{\omega=1}^{l-1}O_{l,\omega}=\{O_n(\boldsymbol{x})\,|\,\omega t(\boldsymbol{u}_i)=\omega,|O_n(\boldsymbol{x})|=l,\ 1\leqslant\omega\leqslant l-1\}$ 中不同轨道的总数。

定义 4[18]　设 $F(\boldsymbol{x})=(f_1(\boldsymbol{x}),f_2(\boldsymbol{x}),\cdots,f_m(\boldsymbol{x}))$ 为 $F_2^n\to F_2^m$ 上的 n 元 m 输出布尔函数，$2^m\leqslant g_n$，如果对于任意的 $(x_1,x_2,\cdots,x_n)\in F_2^n$，$\boldsymbol{u}\in F_2^m\setminus\{\overline{\boldsymbol{0}}\}$ 均有 $\boldsymbol{u}F(\rho_n^k(x_1,x_2,\cdots,x_n))=\boldsymbol{u}F(x_1,x_2,\cdots,x_n),0\leqslant k\leqslant n-1$，则称该函数为多输出旋转对称函数，记为 (n,m)-RSBF。

由于 (n,m)-RSBF 最多有 2^m 种输出，又因为 ρ_n^k 可将 F_2^n 中的元素分为 g_n 个轨道，从而 $2^m\leqslant g_n$，这个要求显然限制了多输出旋转对称函数的数量。

由定义 4 可知，若 $f(\boldsymbol{x})$ 是一个 (n,m)-RSBF，则其坐标函数的任意非零线性组合都是 RSBF，具体的 (n,m)-RSBF 的例子可参考文献[18]。

定义 5[24,25]　如果 $\boldsymbol{A}$ 的任意 m 列构成的矩阵的行向量中，F_2^m 中的每个向量都出现相同的次数，则 $\boldsymbol{A}$ 是一个 ω 行 n 列的矩阵，称 $\boldsymbol{A}$ 是一个正交表 $\boldsymbol{OA}(\omega,n,2,m)$。

定义 6[24,25]　如果一个布尔函数 $f(\boldsymbol{x})$ 的支撑矩阵是一个 $\boldsymbol{OA}(\omega,n,2,m)$，则称 $f(\boldsymbol{x})$ 是一个 m 阶相关免疫函数，简称为相关免疫函数或 CI 函数。

定义 7[26~28]　设 $f(\boldsymbol{x}):F_2^n\to F_2^m$ 是一个 (n,m) 函数，则 $f(\boldsymbol{x})$ 是平衡函数，当且仅当对 $\forall\boldsymbol{\alpha}\in F_2^m$ 都有 $\left|f^{-1}(\boldsymbol{\alpha})\right|=2^{n-m}$，$f(\boldsymbol{x})$ 是 m-弹性函数（简称弹性函数）；当且仅当对 $\forall\boldsymbol{\alpha}\in F_2^m$，原像集 $f^{-1}(\boldsymbol{\alpha})$ 中的向量构成的矩阵都是 $\boldsymbol{OA}(2^{n-m},n,2,m)$。

平衡的相关免疫函数实际上就是弹性函数，通常把平衡函数看作弹性阶为 0 的弹性函数，文献[25]给出了弹性函数与正交表 ($\boldsymbol{OA}$) 大集间的等价关系，文献[29]研究了 2 种特殊的平衡旋转对称函数的计数问题。

引理 1[20]　F_2^8 的所有轨道中轨道长度为 8 的有 30 个，轨道长度为 4 的有 3 个，轨道长度为 2 的有 1 个，轨道长度为 1 的有 2 个。

3　主要结果

3.1　$n=2^r(r\in N^+)$ 的多输出旋转对称函数 $f:F_2^n\to F_2^m$ 满足平衡、弹性条件时 m 的取值问题

当多输出旋转对称函数的变元个数为 $n=2^r$ 时，定理 1 给出了它对应 m 的取值。

定理 1　若 2^r 元多输出旋转对称函数 $f:F_2^{2^r}\to F_2^m$ 是平衡的，其中，m 和 r 为正整数，则

$$2\leqslant m\leqslant 2^r-r$$

证明　首先，因为函数 $f:F_2^{2^r}\to F_2^m$ 是多输出函数，所以 $m\geqslant 2$；其次，由于 $f:F_2^{2^r}\to F_2^m$ 是平衡函数，且 $F_2^{2^r}$ 中向量的总数为 2^{2^r}，F_2^m 中向量个数为 2^m，所以对 $\forall\boldsymbol{\alpha}\in F_2^m$ 都有 $\left|f^{-1}(\boldsymbol{\alpha})\right|=2^{2^r-m}$。

另一方面，由于 $f:F_2^{2^r}\to F_2^m$ 是旋转对称函数，故对 $\forall\boldsymbol{\alpha}\in F_2^m$，$f^{-1}(\boldsymbol{\alpha})$ 中的元素都是由一个或几个完整的轨道中的所有向量组成，并且向量个数都是

相等的；又因为 $F_2^{2^r}$ 长轨道的长度为 2^r，所以 F_2^m 中每个向量的原像中至少有一个轨道，故必有 F_2^m 中的某个向量 $\boldsymbol{\beta}\in F_2^m$ 的原像中含有长度为 2^r 的轨道，即 $\left|f^{-1}(\boldsymbol{\beta})\right|\geqslant 2^r$，从而 $2^{2^r-m}\geqslant 2^r$，即 $m\leqslant 2^r-r$。

综上，$2\leqslant m\leqslant 2^r-r$ 成立。

推论 1　若 2^r 元多输出旋转对称函数 $f:F_2^{2^r}\to F_2^m$ 是弹性函数，其中，m 和 r 为正整数，则

$$2\leqslant m\leqslant 2^r-r-1$$

证明　由于多输出旋转对称弹性函数一定是平衡函数，故由定理 1 可知 $2\leqslant m\leqslant 2^r-r$；注意 $f:F_2^{2^r}\to F_2^m$ 是多输出相关免疫函数，$F_2^{2^r}$ 中元素个数为 2^{2^r}，F_2^m 中向量个数为 2^m。

显然，$F_2^{2^r}$ 的长旋转对称轨道的长度为 2^r，因而存在 $\boldsymbol{\beta}\in F_2^m$，使 $f^{-1}(\boldsymbol{\beta})$ 中至少包含一个长旋转对称轨道。而 F_2^m 中每个向量的原像中至少有一个旋转对称轨道，由 f 的平衡性可知，对 $\forall\boldsymbol{\alpha}\in F_2^m$ 都有 $\left|f^{-1}(\boldsymbol{\alpha})\right|=2^{2^r-m}$，且 $f^{-1}(\boldsymbol{\alpha})$ 所有的向量构成的矩阵均为正交表，即该矩阵的每个列向量中 0 和 1 的个数应该是相等的。若 $f^{-1}(\boldsymbol{\beta})$ 中包含一个长旋转对称轨道，并且当该轨道中的所有向量构成矩阵的列向量的汉明重量为 k 时，$f^{-1}(\boldsymbol{\beta})$ 中一定还包含其他旋转对称轨道，且其中的向量个数至少为 2^r，此时这些向量构成的矩阵的列向量的汉明重量至少为 2^r-k，即 F_2^m 中每个向量的原像中向量的个数至少为 $2\times 2^r=2^{r+1}$，所以 $2^{2^r-m}\geqslant 2^{r+1}$，即 $2^r-m\geqslant r+1$，故有 $m\leqslant 2^r-r-1$。

综上，$2\leqslant m\leqslant 2^r-r-1$ 成立。

3.2　*n*=8 时多输出旋转对称 0-弹性函数的构造与计数问题

定理 2　对于多输出旋转对称函数 $f:F_2^n\to F_2^m$，若 $n=8$，则 m 输出旋转对称平衡函数（0-弹性函数）的个数 N_m 为

1) $N_5=\mathrm{C}_3^1\times 32!$

2) $N_4=91\times\dfrac{30!}{2^{11}}$

3) $N_3=116\times\dfrac{30!}{(4!)^7}$

4) $N_2=316\times\dfrac{30!}{7!(8!)^3}$

证明　由引理 1 知 $h_8=30$、$h_4=3$、$h_2=1$、$h_1=2$，即长度为 8 的轨道有 30 个，长度为 4 的轨道有 3 个，长度为 2 的轨道有 1 个，长度为 1 的轨道有 2 个。

当 $n=8$ 时，由定理 1 知 m 的取值范围为 $2\leqslant m\leqslant 5$。根据 m 的取值分以下几种情况讨论。

情形 1　当 $m=5$ 时，F_2^m 中有 32 个向量，故可将 F_2^8 中所有轨道分为 32 组，每组含 8 个向量。其中必有一组是由 2 个长度为 4 的轨道组成，一组是由 1 个长度为 2 的轨道、2 个长度为 1 的轨道和一个长度为 4 的轨道组成，而其余 30 组分别由一个长轨道中的 8 个向量组成。因此，将 F_2^8 中的 256 个向量分成 32 组，有 C_3^1 种不同分法，因而共可以构造出 $N_5=\mathrm{C}_3^1\times 32!$ 种不同的 (8,5) 旋转对称平衡函数。

情形 2　当 $m=4$ 时，F_2^m 中有 16 个向量，故可将 F_2^8 中所有轨道分为 16 组，每组含 16 个向量，此时可分为以下 2 种情况。

1) 当所有的短轨道被分到同一组中，那么只需将 30 个长轨道分成 15 组即可，这是一个平均分组问题，因而共有 $\dfrac{1}{15!}\mathrm{C}_{30}^2\mathrm{C}_{28}^2\cdots\mathrm{C}_4^2\mathrm{C}_2^2$ 种不同的分法，按这些不同的分法可以构造不同的 (8,4) 旋转对称平衡函数的个数为

$$N_{4,1}=16!\frac{1}{15!}\mathrm{C}_{30}^2\mathrm{C}_{28}^2\cdots\mathrm{C}_4^2\mathrm{C}_2^2=\frac{30!}{2^{11}}$$

2) 当有一个长度为 4 的轨道、2 个长度为 1 的轨道、一个长度为 2 的轨道与一个长度为 8 的轨道构成一组，2 个长度为 4 的轨道和一个长度为 8 的轨道构成一组时，即短轨道被分到 2 个不同的组中，其余长度为 8 的 28 个轨道平均分成 14 组，那么将 F_2^8 中所有轨道就分成了 16 组，因而共有 $\mathrm{C}_3^1\mathrm{C}_{30}^1\mathrm{C}_{29}^1\mathrm{C}_{28}^2\mathrm{C}_{26}^2\cdots\mathrm{C}_4^2\mathrm{C}_2^2\dfrac{1}{14!}$ 种不同的分法，所以可构造出不同的 (8,4) 旋转对称平衡函数的个数为

$$N_{4,2}=16!\mathrm{C}_3^1\mathrm{C}_{30}^1\mathrm{C}_{29}^1\mathrm{C}_{28}^2\mathrm{C}_{26}^2\cdots\mathrm{C}_4^2\mathrm{C}_2^2\frac{1}{14!}=90N_{4,1}$$

显然，1)和 2)所构造的函数是不同的，因而所得到的 (8,4) 旋转对称平衡函数的个数为

$$N_4=N_{4,1}+N_{4,2}=91N_{4,1}=1\,456\times\frac{30!}{2^{15}}=91\times\frac{30!}{2^{11}}$$

情形 3　当 $m=3$ 时，F_2^m 中有 8 个向量，故可

将 F_2^8 中所有轨道分为 8 组，每组含 32 个向量，此时可分为以下 2 种情况。

1) 当所有的短轨道被分到同一组中，那么只需要从 30 个长轨道中选出 2 个，将其他 28 个长轨道平均分成 7 组即可，这是一个平均分组问题，因而共有 $\mathrm{C}_{30}^2\mathrm{C}_{28}^4\mathrm{C}_{24}^4\cdots\mathrm{C}_4^4\dfrac{1}{7!}$ 种不同的分法，所以可构造出不同的 (8,3) 旋转对称平衡函数的个数为

$$N_{3,1}=\mathrm{C}_{30}^2\mathrm{C}_{28}^4\mathrm{C}_{24}^4\cdots\mathrm{C}_4^4\frac{1}{7!}8!=4\times\frac{30!}{(4!)^7}$$

2) 当有一个长度为 4 的轨道、2 个长度为 1 的轨道、一个长度为 2 的轨道与 3 个长度为 8 的轨道构成一组，2 个长度为 4 的轨道和 3 个长度为 8 的轨道构成一组时，其他长度为 8 的 24 个轨道平均分成 6 组，那么将 F_2^8 中所有轨道就分成了 8 组，因而共有 $\mathrm{C}_3^1\mathrm{C}_{30}^3\mathrm{C}_{27}^3\mathrm{C}_{24}^4\mathrm{C}_{20}^4\cdots\mathrm{C}_4^4\dfrac{1}{6!}$ 种不同的分法，所以可构造出不同的 (8,3) 旋转对称平衡函数的个数为

$$N_{3,2}=\mathrm{C}_3^1\mathrm{C}_{30}^3\mathrm{C}_{27}^3\mathrm{C}_{24}^4\mathrm{C}_{20}^4\cdots\mathrm{C}_4^4\frac{1}{6!}8!=\frac{14\times30!}{3\times(4!)^6}$$

显然，1)和 2)所构造的函数是不同的，因而所得到的 (8,3) 旋转对称平衡函数的个数为

$$N_3=N_{3,1}+N_{3,2}=29N_{3,1}=116\times\frac{30!}{(4!)^7}$$

情形 4　当 $m=2$ 时，F_2^m 中有 4 个向量，故可将 F_2^8 中所有轨道分为 4 组，每组含 64 个向量，此时可分为以下 2 种情况。

1) 当所有的短轨道被分到同一组中，那么只需要从 30 个长轨道中选出 6 个，将其他 24 个长轨道平均分成 3 组即可，这是一个平均分组问题，因而共有 $\mathrm{C}_{30}^6\mathrm{C}_{24}^8\mathrm{C}_{16}^8\mathrm{C}_8^8\dfrac{1}{3!}$ 种不同的分法，按这种分法可以构造出不同的 (8,2) 旋转对称平衡函数的个数为

$$N_{2,1}=\mathrm{C}_{30}^6\mathrm{C}_{24}^8\mathrm{C}_{16}^8\mathrm{C}_8^8\frac{1}{3!}4!=28\times\frac{30!}{7!(8!)^3}$$

2) 当有一个长度为 4 的轨道、2 个长度为 1 的轨道、一个长度为 2 的轨道与 7 个长度为 8 的轨道构成一组，2 个长度为 4 的轨道和 7 个长度为 8 的轨道构成一组时，其他长度为 8 的 16 个轨道平均分成 2 组，那么将 F_2^8 中所有轨道分成了 4 组，因而共有 $\mathrm{C}_3^1\mathrm{C}_{30}^7\mathrm{C}_{23}^7\mathrm{C}_{16}^8\mathrm{C}_8^8\dfrac{1}{2!}$ 种不同的分法，所以可以构造出不同的 (8,2) 旋转对称平衡函数的个数为

$$N_{2,2}=\mathrm{C}_3^1\mathrm{C}_{30}^7\mathrm{C}_{23}^7\mathrm{C}_{16}^8\mathrm{C}_8^8\frac{1}{2!}4!=288\times\frac{30!}{7!(8!)^3}$$

显然，1)和 2)所构造的函数是不同的，因而所得到的 (8,2) 旋转对称函数的个数为

$$N_2=N_{2,1}+N_{2,1}=316\times\frac{30!}{7!(8!)^3}$$

3.3　*n*=8 时多输出旋转对称 1-弹性函数的构造与计数问题探讨

由推论 1 可知，当 $n=8$ 时，多输出旋转对称弹性函数 $f:F_2^n\to F_2^m$ 中 m 的取值范围为 $2\leqslant m\leqslant 4$。下面考虑 $2\leqslant m\leqslant 4$ 时具体的多输出旋转对称弹性函数的构造与计数问题。根据多输出旋转对称函数和弹性函数的定义可知：旋转对称弹性函数的构造等价于正交表大集 $\left\{\boldsymbol{A}_0,\boldsymbol{A}_1,\cdots,\boldsymbol{A}_{2^m-1}\right\}$ 的构造，其中，每个 $\boldsymbol{A}_i$ 都是由若干个轨道矩阵构成，并且都是 $\boldsymbol{OA}(2^{n-m},n,2,1)$。为了方便和简单，需要约定一些符号。

设 $\boldsymbol{u}_i(1\leqslant i\leqslant n)$ 为矩阵 $\boldsymbol{C}_{O_n(x)}$ 的第 i 个列向量，记旋转对称轨道的集合 $O_{l,\omega}=\{O_n(\boldsymbol{x})\,|\,\omega t(\boldsymbol{u}_1)=\omega,|O_n(\boldsymbol{x})|=l\}$，$O_{l,\omega}$ 中轨道的个数 $h_{l,\omega}$，即 $h_{l,\omega}=\left|O_{l,\omega}\right|$。集合 $O_l=\bigcup_{\omega=1}^{l-1}O_{l,\omega}=\{O_n(\boldsymbol{x})\,|\,\omega t(\boldsymbol{u}_i)=\omega,\ |O_n(\boldsymbol{x})|=l,\ 1\leqslant\omega\leqslant l-1\}$ 中不同的旋转对称轨道的总数是 $h_l=|O_l|=\sum_{\omega=1}^{l-1}h_{l,\omega}$。

考虑循环群 $\left\{\rho_8^k\,|\,0\leqslant k\leqslant 7\right\}$ 在 F_2^8 上作用所形成的轨道，按照定义 3 写成轨道矩阵的形式，对于 6 个短轨道形成的轨道矩阵，以及 30 个长轨道形成的轨道矩阵分别按列向量的汉明重量分类计算可知：$h_{1,0}=h_{1,1}=1$，$h_{2,1}=1$，$h_{4,1}=h_{4,2}=h_{4,3}=1$，$h_{8,1}=h_{8,7}=1$，$h_{8,2}=h_{8,6}=3$，$h_{8,3}=h_{8,5}=7$，$h_{8,4}=8$。

由于要构造平衡函数，故 2 个长度为 1 的短轨道以及一个长度为 2 的短轨道必须分在同一组，将这 3 个短轨道“捆绑起来”，看成一个长度为 4、第 1 列的汉明重量为 2 的短轨道矩阵，即 $h_{4,1}=h_{4,3}=1$，$h_{4,2}=2$，$h_{8,1}=h_{8,7}=1$，$h_{8,2}=h_{8,6}=3$，$h_{8,3}=h_{8,5}=7$，$h_{8,4}=8$。

为了简化问题，本文可以采取以下 2 种简化方式。

方式 1 把 2 个行数为 4、列向量重量为 2 的轨道矩阵以及另外 2 个长度为 4 的轨道矩阵分别“捆绑”成 2 个长度为 8、列向量重量为 4 的轨道矩阵，本文有 $h_{8,1}=h_{8,7}=1$， $h_{8,2}=h_{8,6}=3$， $h_{8,3}=h_{8,5}=7$， $h_{8,4}=10$。

方式 2 把 2 个行数为 4、列向量重量为 2 的的轨道矩阵分别与另外 2 个长度为 4 的轨道矩阵组合“捆绑”成一个长度为 8、列向量重量为 3 和一个长度为 8、列向量重量为 5 的轨道矩阵，显然有 2 种“捆绑”方式，本文有 $h_{8,1}=h_{8,7}=1$，$h_{8,2}=h_{8,6}=3$，$h_{8,3}=h_{8,5}=8$， $h_{8,4}=8$。

1) 当 $m=4$ 时， F_2^m 中共有 16 个向量，此时 (8,4) 旋转对称 1-弹性函数的构造等价于把上述的 32 个行数都是 8 的矩阵分成 16 组，每组 2 个轨道矩阵，并且每组中的 2 个矩阵构成一个强度为 1 的正交表，根据这些短轨道的分组情况分以下几种情形。

① 所有短轨道中的 16 个向量被安排在一组，余下的 30 个长轨道分成 15 组，则有 $3!7!\mathrm{C}_8^2\mathrm{C}_6^2\mathrm{C}_4^2\mathrm{C}_2^2\frac{1}{4!}=\frac{(7!)^2}{8}$ 种不同的分法，从而可以构造的 (8,4) 旋转对称 1-弹性函数的个数为

$$N_a=3!7!\mathrm{C}_8^2\mathrm{C}_6^2\mathrm{C}_4^2\mathrm{C}_2^2\frac{1}{4!}16!=2\times(7!)^2\times15!$$

② 如果按照方式 1 的做法，当所得到的 2 个长度为 8、列向量重量为 4 的轨道矩阵分到不同组时，有 $3!7!\mathrm{C}_8^1\mathrm{C}_7^1\mathrm{C}_6^2\mathrm{C}_4^2\mathrm{C}_2^2\frac{1}{3!}=(7!)^2$ 种不同的分法，从而可以构造的 (8,4) 旋转对称 1-弹性函数的个数为

$$N_b=3!7!\mathrm{C}_8^1\mathrm{C}_7^1\mathrm{C}_6^2\mathrm{C}_4^2\mathrm{C}_2^2\frac{1}{3!}16!=(7!)^2\times16!$$

③ 如果按照方式 2 的做法，由于这有 2 种不同的“捆绑”方法，那么将所得到的 2 个长度为 8、列向量重量分别为 3 和 5 的轨道矩阵分到不同组中时，有 $2\cdot3!\mathrm{C}_7^1 7!\mathrm{C}_8^2\mathrm{C}_6^2\mathrm{C}_4^2\mathrm{C}_2^2\frac{1}{4!}$ 种不同的分法，从而可以构造的 (8,4) 旋转对称 1-弹性函数的个数为

$$N_c=2\cdot3!\mathrm{C}_7^1 7!\mathrm{C}_8^2\mathrm{C}_6^2\mathrm{C}_4^2\mathrm{C}_2^2\frac{1}{4!}16!=28\times(7!)^2\times15!$$

显然，根据①~③的情况构造的 (8,4) 旋转对称 1-弹性函数都不相同，因而本文有以下定理。

定理 3 当 $m=4$ 时，不同的 (8,4) 旋转对称 1-弹性函数的总数为 $46\times(7!)^2\times15!$。

证明 只需计算出 $N_a+N_b+N_c$ 的值即可。这里， N_a、 N_b 和 N_c 的表达式如上所述。

2) 当 $m=3$ 时， F_2^m 中共有 8 个向量，本文需要把上述的 32 个行数为 8 的矩阵（无论方式 1 还是方式 2）分成 8 组，使每组中含有 4 个轨道矩阵，并且它们构成一个强度为 1 的正交表。不妨记矩阵

$$\boldsymbol{X}=\begin{pmatrix}x_{1,1}&x_{1,2}&\cdots&x_{1,7}\\x_{2,1}&x_{2,2}&\cdots&x_{2,7}\\\vdots&\vdots&\ddots&\vdots\\x_{8,1}&x_{8,2}&\cdots&x_{8,7}\end{pmatrix}$$

其中，非负整数 $x_{i,j}$ 的含义为组 $\boldsymbol{A}_{i-1}$ 中所含有的轨道矩阵中列向量的重量为 j 的轨道个数，并且矩阵 $\boldsymbol{X}$ 在不考虑行向量顺序的情况下都看作是相同的，本文有以下的结果。

定理 4 按照方式 1 的做法，若以下方程组

$$\begin{cases}\boldsymbol{X}^{\mathrm{T}}\boldsymbol{1}_8=(1\quad3\quad7\quad10\quad7\quad3\quad1)^{\mathrm{T}}\\\boldsymbol{X}\boldsymbol{1}_7=4_8\\\boldsymbol{X}(1\quad2\quad3\quad4\quad5\quad6\quad7)^{\mathrm{T}}=16_8\end{cases}$$

有 λ 个不同的解

$$\boldsymbol{X}_s=\begin{pmatrix}x_{1,1}^s&x_{1,2}^s&\cdots&x_{1,7}^s\\x_{2,1}^s&x_{2,2}^s&\cdots&x_{2,7}^s\\\vdots&\vdots&\ddots&\vdots\\x_{8,1}^s&x_{8,2}^s&\cdots&x_{8,7}^s\end{pmatrix},\quad1\leqslant s\leqslant\lambda$$

那么按照方式 1，可以构造的 (8,3) 旋转对称 1-弹性函数的个数为

$$Num_1=8!\sum_{s=1}^{\lambda}\frac{3!7!10!7!3!}{\prod_{j=2}^{6}(\prod_{i=1}^{8}x_{i,j}^s!)}$$

其中，2 个解不同是指不存在任何置换矩阵 $\boldsymbol{P}$ 使

$$\boldsymbol{X}_{s_1}=\boldsymbol{P}\boldsymbol{X}_{s_2},\quad1\leqslant s_1\leqslant s_2\leqslant\lambda$$

证明 若 $\boldsymbol{X}$ 是上述方程组的一组解，本文按照矩阵来分组，根据 $\boldsymbol{X}$ 的第 i 行，本文分别挑选 $x_{i,n}$ 个列重量为 n 的轨道矩阵，$1\leqslant n\leqslant7$，把这些轨道矩阵中的行向量作为第 i 组，记为 $\boldsymbol{A}_{i-1}$，这样，就可以得到线性空间 F_2^8 的一个划分 $\{\boldsymbol{A}_0,\boldsymbol{A}_1,\cdots,\boldsymbol{A}_7\}$，由于每一组中的向量所取的函数值相同，不同组中的向量

所取的函数值不同，对于一个划分可以构造的函数个数为 8!个。而不同的轨道选取方法可以得到不同的划分，按照 $\boldsymbol{X}$ 可以得到的不同划分的方法数为

$$\frac{1!3!7!10!7!3!1!}{\prod_{j=1}^{7}(\prod_{i=1}^{8}x_{i,j}!)}=\frac{3!7!10!7!3!}{\prod_{j=2}^{7}(\prod_{i=1}^{8}x_{i,j}!)}$$

根据不同的划分方法得到的函数是不同的，因而，根据这个解可以构造不同的(8, 3)旋转对称 1-弹性函数的个数为

$$8!\frac{3!7!10!7!3!}{\prod_{j=2}^{6}(\sum_{i=1}^{8}x_{i,j}!)}$$

注意到对于不同的解 $\boldsymbol{X}$，所构造的(8, 3)旋转对称 1-弹性函数是不同的，那么根据所得到的 λ 个解可以构造出不同的 (8,3) 旋转对称 1-弹性函数的个数为

$$Num_1=8!\sum_{s=1}^{\lambda}\frac{3!7!10!7!3!}{\prod_{j=2}^{6}(\sum_{i=1}^{8}x_{i,j}^{s}!)}$$

定理 5　按照简化方式 2 的做法，若以下方程组

$$\begin{cases}\boldsymbol{X}^{\mathrm{T}}1_8=\begin{pmatrix}1&3&8&8&8&3&1\end{pmatrix}^{\mathrm{T}}\\ \boldsymbol{X}1_7=4_8\\ \boldsymbol{X}\begin{pmatrix}1&2&3&4&5&6&7\end{pmatrix}^{\mathrm{T}}=16_8\end{cases}$$

有 λ 个不同的解

$$\boldsymbol{X}_s=\begin{pmatrix}x_{1,1}^{s}&x_{1,2}^{s}&\cdots&x_{1,7}^{s}\\ x_{2,1}^{s}&x_{2,2}^{s}&\cdots&x_{2,7}^{s}\\ \vdots&\vdots&\ddots&\vdots\\ x_{8,1}^{s}&x_{8,2}^{s}&\cdots&x_{8,7}^{s}\end{pmatrix},1\leqslant s\leqslant\lambda$$

那么按照方式 2，可以构造的(8, 3)旋转对称 1-弹性函数的个数为

$$Num_2=8!\sum_{s=1}^{\lambda}\frac{3!8!8!8!3!}{\prod_{j=2}^{6}(\sum_{i=1}^{8}x_{i,j}^{s}!)}$$

其中，2 个解不同是指不存在任何置换矩阵 $\boldsymbol{P}$ 使

$$\boldsymbol{X}_{s_1}=\boldsymbol{P}\boldsymbol{X}_{s_2},1\leqslant s_1\leqslant s_2\leqslant\lambda$$

证明　类似于定理 4。

定理 4 和定理 5 实际上给出了一个构造(8, 3)旋转对称 1-弹性函数的有效方法，由定理 4 和定理 5 中的方程组得到的函数可能是相同的。

3) 当 $m=2$ 时，F_2^m 中共有 4 个向量，本文需要把上述的 32 个行数都是 8 的矩阵分成 4 组 $\boldsymbol{A}_0$、$\boldsymbol{A}_1$、$\boldsymbol{A}_2$、$\boldsymbol{A}_3$，每组 8 个轨道矩阵，并且每组中的 8 个矩阵构成一个强度为 1 的正交表，记矩阵

$$\boldsymbol{X}=\begin{pmatrix}x_{1,1}&x_{1,2}&\cdots&x_{1,7}\\ x_{2,1}&x_{2,2}&\cdots&x_{2,7}\\ x_{3,1}&x_{3,2}&\cdots&x_{3,7}\\ x_{4,1}&x_{4,2}&\cdots&x_{4,7}\end{pmatrix}$$

其中，非负整数 $x_{i,j}$ 的含义为组 $\boldsymbol{A}_{i-1}$ 中所含有的轨道矩阵中列向量的重量为 j 的轨道个数。

定理 6　按照简化方式 1 的做法，若如下的方程组

$$\begin{cases}\boldsymbol{X}^{\mathrm{T}}1_4=\begin{pmatrix}1&3&7&10&7&3&1\end{pmatrix}^{\mathrm{T}}\\ \boldsymbol{X}1_7=8_4\\ \boldsymbol{X}\begin{pmatrix}1&2&3&4&5&6&7\end{pmatrix}^{\mathrm{T}}=32_4\end{cases}$$

有 λ 个不同的解

$$\boldsymbol{X}_s=\begin{pmatrix}x_{1,1}^{s}&x_{1,2}^{s}&\cdots&x_{1,7}^{s}\\ x_{2,1}^{s}&x_{2,2}^{s}&\cdots&x_{2,7}^{s}\\ x_{3,1}^{s}&x_{3,2}^{s}&\cdots&x_{3,7}^{s}\\ x_{4,1}^{s}&x_{4,2}^{s}&\cdots&x_{4,7}^{s}\end{pmatrix},\ 1\leqslant s\leqslant\lambda$$

那么按照方式 1，可以构造的 (8,2) 旋转对称 1-弹性函数的个数为

$$Num_3=4!\sum_{s=1}^{\lambda}\frac{3!7!10!7!3!}{\prod_{j=2}^{6}(\sum_{i=1}^{4}x_{i,j}^{s}!)}$$

其中，2 个解不同是指不存在任何置换矩阵 $\boldsymbol{P}$ 使

$$\boldsymbol{X}_{s_1}=\boldsymbol{P}\boldsymbol{X}_{s_2},1\leqslant s_1\leqslant s_2\leqslant\lambda$$

证明　类似于定理 4。

定理 7　按照方式 2 的做法，若以下方程组

$$\begin{cases}\boldsymbol{X}^{\mathrm{T}}\boldsymbol{1}_4=\begin{pmatrix}1&3&8&8&8&3&1\end{pmatrix}^{\mathrm{T}}\\ \boldsymbol{X}\boldsymbol{1}_7=8_4\\ \boldsymbol{X}\begin{pmatrix}1&2&3&4&5&6&7\end{pmatrix}^{\mathrm{T}}=32_4\end{cases}$$

有 λ 个不同的解

$$\boldsymbol{X}_s=\begin{pmatrix}x_{1,1}^{s}&x_{1,2}^{s}&\cdots&x_{1,7}^{s}\\ x_{2,1}^{s}&x_{2,2}^{s}&\cdots&x_{2,7}^{s}\\ x_{3,1}^{s}&x_{3,2}^{s}&\cdots&x_{3,7}^{s}\\ x_{4,1}^{s}&x_{4,2}^{s}&\cdots&x_{4,7}^{s}\end{pmatrix},\ 1\leqslant s\leqslant\lambda$$

那么按照方式 1，可以构造的 (8,2) 旋转对称 1-弹性函数的个数为

$$Num_4 = 4!\sum_{s=1}^{\lambda}\frac{3!8!8!8!3!}{\prod_{j=2}^{6}(\sum_{i=1}^{4}x_{i,j}^{s}!)}$$

其中，2 个解不同是指不存在任何置换矩阵 $\boldsymbol{P}$ 使

$$\boldsymbol{X}_{s_1} = \boldsymbol{P}\boldsymbol{X}_{s_2}, 1 \leqslant s_1 \leqslant s_2 \leqslant \lambda$$

证明 类似于定理 4。

定理 6 和定理 7 实际上给出了一个构造 (8,2) 旋转对称 1-弹性函数的有效方法，由定理 6 和定理 7 中的方程组得到的函数可能是相同的。

4 结束语

本文利用旋转对称函数的轨道与支撑矩阵的特征给出了 8 元多输出旋转对称 0-弹性函数的构造与计数，所得的函数个数可以根据轨道矩阵的性质运用分类讨论的思想，基于组合数学中的加法原理与乘法原理进行计算，而 8 元多输出旋转对称 1-弹性函数的构造等价于一个线性方程组的解。定理 4~定理 7 中线性方程组的所有不同的解实际上就是不同的轨道分配方案，可借助于计算机计算。

参考文献：

[1] FILIOL E, FONTAINE C. Highly nonlinear balanced Boolean functions with good correlation immunity[C]//Advances in Cryptology-EUROCRYPT'98, in Lecture Notes in Computer Science. 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] STANICA P, MAITRA S, CLARK J. Results on rotation symmetric bent and correlation immune Boolean functions[C]//Fast software encryption workshop (FSE 2004), in Lecture Notes in Computer Science. 2004: 161-177.

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

[5] CUSICK T W, STANICA P. Fast evaluation, weight and nonlinearity of rotation-symmetric functions[J]. Discrete Mathematics, 2002, 258(1-3): 289-301.

[6] CARLET C, DALAI D K, GUPTA K C. Algebraic immunity for cryptographically significant boolean functions: analysis and construction[J]. IEEE Transactions on Information Theory, 2006, 52(7): 3105-3121.

[7] KAVUT S, MAITRA S, YUCEL M D. Search for Boolean functions with excellent profiles in the rotation symmetric class[J]. IEEE Trans Inf Theory, 2007, 53(5): 1743-1751.

[8] KAVUT S, MAITRA S, SARKAR S, et al. Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity>240[C]// INDOCRYPT 2006, 2006: 266-279.

[9] STANICA P, MAITRA S. A constructive count of rotation symmetric functions[J]. Information Processing Letters, 2003, 88(6):299-304.

[10] CARLET C, GAO G, LIU W. Results on constructions of rotation symmetric bent and semibent functions[C]//SETA 2014. 2014: 21-33.

[11] SARKAR P, MAUTRA S. Balancedness and correlation immunity of symmetric Boolean functions[J]. Discrete Mathematics, 2003, 307(19): 2351-2358.

[12] 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.

[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.
DU J, WEN Q Y, ZHANG J, et al. Construction and count of resilient rotation symmetric Boolean functions with prime number variables[J]. Journal on Communications, 2013, 34(3):6-13.

[14] 杜蛟, 温巧燕, 张劼, 等. 2*p* 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.
DU J, WEN Q Y, ZHANG J, et al. Construction and count of resilient 2-rotation symmetric Boolean functions with 2*p* variables[J]. Journal of Beijing University of Posts and Telecommunications, 2012, 35(5): 36-40.

[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 of Electronics, Communications and Computer Sciences, E96-A, 2013, 7: 1653-1656.

[16] DU J, WEN Q Y, 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.

[17] 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.

[18] 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.
YUAN Y B, ZHAO Y Q. Cryptological properties of multi-output rotation symmetric functions[J]. Journal on Communications, 2009, 30(11A): 1-7.

[19] MAZUMDAR B, MUKHOPADHYAY D, SENGUPTA I. Design and implementation of rotation symmetric S-boxes with high nonlinearity and high DPA resiliency[C]//IEEE International Symposium on Hardware-Oriented Security and Trust(HOST). 2013: 87-92.

[20] MAZUMDAR B, MUKHOPADHYAY D. Construction of rotation symmetric S-boxes with high nonlinearity and improved DPA resistivity[J]. IEEE Trans on Computers, 2017, 66(1): 59-72.

[21] GAO G, CUSICK T W, LIU W. Families of rotation symmetric functions with useful cryptographic properties[J]. IET Information Security, 2014, 8(6): 297-302.

[22] RIJMEN V, BARRETO P, FILHO D L G. Rotation symmetry in algebraically generated cryptographic substitution tables[J]. Information Processing Letters, 2008, 106: 246-250.

[23] KAVUT S. Results on rotation symmetric S-boxes[J]. Information Science, 2012: 93-113.

[24] 温巧燕, 钮心忻, 杨义先. 现代密码学中的布尔函数[M]. 北京: 科学出版社, 2000.
WEN Q Y, NIU X X, YANG Y X. The Boolean functions in modern cryptology[M]. Beijing: Science Press, 2000.

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

[26] 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: 121-149.

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

[28] 鞠桂枝. 多输出布尔函数若干性质的研究[D]. 郑州: 信息工程大学, 2005.
JU G Z. Study on properties of multi-output functions[D]. Zhengzhou: PLA Information Engineering University, 2005.

[29] 耿旭旭, 赵先鹤. 两类具有特殊线性结构点的平衡旋转对称函数的计数[J]. 河南师范大学学报(自然科学版), 2015,43(3):1-4.
GENG X X, ZHAO X H. The count of balanced rotation symmetric Boolean functions with two special linear structure[J]. Journal of Henan Normal University (Natural Science Edition), 2015, 43(3): 1-4.

作者简介：

杜蛟（1978-），男，湖北英山人，博士，河南师范大学讲师，主要研究方向为密码学与应用数学。

尚玉婧（1993-），女，河南卫辉人，河南师范大学硕士生，主要研究方向为应用数学。

赵金玲（1994-），女，河南商丘人，河南师范大学硕士生，主要研究方向为应用数学。

董乐（1980-），男，河南封丘人，博士，河南师范大学副教授，主要研究方向为分组密码的设计与分析。

张恩（1974-），男，河南新乡人，博士，河南师范大学副教授，主要研究方向为密码协议与云计算安全。