doi:10.3969/j.issn.1000-436x.2014.08.022

GF(*p*)上 *q* 元旋转对称弹性函数的一个等价刻画

杜皎[1]，庞善起[1]，温巧燕[2]，张劼[3]

（1. 河南师范大学 数学与信息科学学院，河南 新乡 453007；
2. 北京邮电大学 网络与交换技术国家重点实验室，北京 100876； 3. 北京邮电大学 理学院，北京 100876）

摘 要：基于旋转对称弹性函数 *l* 值支撑矩阵的性质，给出了 *GF*(*p*)上 *q* 变元旋转对称弹性函数的一个等价刻画，证明了 *GF*(*p*)上 *q* 变元旋转对称一阶弹性函数的构造问题等价于一个方程组的求解问题，并且利用方程组的所有解给出这类函数计数结果的一个表示。

关键词：旋转对称函数；*l* 值支撑矩阵；正交表；弹性函数

中图分类号：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2014)08-0179-05

Equivalent characterization of resilient rotation symmetric functions with *q* number of variables over *GF*(*p*)

DU Jiao[1], PANG Shan-qi[1], WEN Qiao-yan[2], ZHANG Jie[3]

(1. College of Mathematics and Information Science，Henan Normal University, Xinxiang 453007, China;
2. State Key Laboratory of Networking and Switching Technology，Beijing University of Posts and Telecommunications, Beijing 100876, China;
3. School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: Baesd on the property of the *l*-value support tables of the resilient rotation symmetric functions (RSF) with *q* number of variables, an equivalent characterization on the resilient RSF with *q* number of variables is derived. It is proved that construction of the resilient RSF with *q* number of variables are equivalent to solve an equation system. At last, the count of resilient RSF with *q* number of variables are represented by using all the solutions of the equation system.

Key words: rotation symmetric functions; *l*-value support table; orthogonal arrays; resilient functions

1 引言

近年来，旋转对称布尔函数受到了极大的关注，不仅是因为其在 MD4、MD5 以及 HAVAL 等散列算法的轮函数实现中派上了用场[1]，一个更为重要的原因是，在旋转对称布尔函数类中发现了一批具有多个密码学性质的的布尔函数[2~4]。人们自然想到将定义在有限域 $GF(2)^n$ 空间上的旋转对称布尔函数的有关结果推广到定义在有限域 $GF(p)^n$ 上的函数上。对称函数是旋转对称函数的一个子类，Cusick 和 Li 首先研究了 $GF(p)^n$ 空间上的对称函数的线性结构[5]，文献[6]研究了 *GF*(*p*)上对称函数的构造与计数问题。文献[6,7]在变元个数 *n* 和有限域特征 *p* 在比较宽松的条件下，研究了 *GF*(*p*)上平衡对称多项式的构造与计数下界问题。在此基础上，柯品惠进一步改进了这个计数下界，并且给出了对称的平衡函数的一个等价刻画[8]。付绍静等人在文献[9]中证明了 *GF*(*p*)上平衡对称函数的构造问题等价于一个线性方程组的求解问题；文献[10]研究了 *GF*(*p*)上旋转对称函数的计数问题；文献[11]研究了素数元旋转对称弹性布尔函数的构造与计数。受文献[9~11]的启发，本文主要研究 *GF*(*p*)上 *q* 变元旋转

收稿日期：2014-01-09；**修回日期**：2014-03-18

基金项目：国家自然科学基金资助项目(11171093, 61300181, 61272057, 61202434, 61170270, 61100203, 61121061)；中央高校基本科研业务费专项基金资助项目(BUPT2011YB01，2012RC0612)；河南省教育厅自然科学研究计划基金资助项目(2011B110010)

Foundation Items: The National Natural Science Foundation of China (11171093, 61300181, 61272057, 61202434, 61170270, 61100203, 61121061); The Fundamental Research Funds for the Central Universities (BUPT2011YB01, 2012RC0612); The Natural Science Research Program of the Education Department of Henan Province (2011B110010)

对称弹性函数的等价刻画问题。文中，q 表示不同于 p 的奇素数。

2 基础知识

设 $GF(p)^n$ 表示有限域 $GF(p)=\{0,1,\cdots,p-1\}$ 上的 n 维向量空间，称映射 $f: GF(p)^n \to GF(p)$ 是一个 n 变元广义布尔函数。为避免混淆，当 $GF(p)^n$ 的特征为 $p=2$ 时，就称映射 f 为布尔函数，当素数 $p>2$ 时，就称映射 f 为 $GF(p)$ 上的广义布尔函数（或简称为函数）。将 $GF(p)$ 上所有的 n 元函数的全体记为 $B_{n,p}$。

定义 1[12] 若 $f(x)\in B_{n,p}$，$l\in\{0,1,\cdots,p-1\}$，记 $f^{-1}(l)=\{x\in GF(p)^n | f(x)=l\}$，$x\in f^{-1}(l)$ 称为 $f(x)$ 的 l 值支撑向量(support vector)，记为 ***l*-SV**，由所有的 ***l*-SV** 构成的矩阵称为是 $f(x)$ 的 l 值支撑矩阵(support table)，记为 ***l*-ST**。进一步，若 $|f^{-1}(l)|=p^{n-1}$ 对于任意的 l 都是成立的，则称函数 $f(x)$ 是平衡的。

为了避免混淆，不考虑特征矩阵的行向量的顺序，***l*-ST** 可以看作是所有的 ***l*-SV** 的集合。

定义 2[12] 对于有限域 $GF(p)$ 的 $w\times n$ 矩阵 $\boldsymbol{A}$，如果空间 $GF(p)^d$ 中的每一个向量都在矩阵 $\boldsymbol{A}$ 的任意 d 列中出现相同的次数，则称 $\boldsymbol{A}$ 是一个正交表 $OA(w, n, p, d)$。

定义 3[12] 假设 $f(x)\in B_{n,p}$，$f(x)$ 称为 t 阶相关免疫函数，如果其所有的 ***l*-ST** 都是 $OA(w_l, n, p, t)$。进一步，如果所有的 ***l*-ST** 都是 $OA(p^{n-1}, n, p, t)$，则称 $f(x)$ 为 t 阶弹性函数。

由定义 3 可知 $GF(p)$ 上 n 元一阶弹性函数的构造等价于 $GF(p)^n$ 空间的 1-正交分划(orthogonal partition)[13]的构造。令 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in GF(p)^n$，这里 $1\leqslant n\leqslant k$，定义 $\rho_n^k(x_i)=x_{i+k}$，这里下角标取 n 的模，特别地，若为 0，就改取 n。

定义 4[12] 如果对于每一个输入 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$ 和任意的 k 都有关系 $f(\rho_n^k(x_1,x_2,\cdots,x_n))=f(x_1,x_2,\cdots,x_n)$ 成立，则称 $f(x)\in B_{n,p}$ 是一个旋转对称函数。

本文中用 $\mathrm{RSF}_{n,p}$ 来表示 $GF(p)$ 上所有 n 元旋转对称函数构成的集合。

定义 5 设 S_n 表示集合 $\{1,2,\cdots,n\}$ 上的对称群，称 $f(x)$ 是一个对称函数，如果对于任意的 $\pi\in S_n$ 都有关系 $f(x_{\pi(1)},x_{\pi(2)},\cdots,x_{\pi(n)})=f(x_1,x_2,\cdots,x_n)$ 成立。

由定义 5，对于给定的输入 $x=(x_1,x_2,\cdots,x_n)$，让 S_n 作用在 x 上，则可以生成轨道 $O_n(x)=\{(y_1,y_2,\cdots,y_n)|(y_1,y_2,\cdots,y_n)=(x_{\pi(1)},x_{\pi(2)},\cdots,x_{\pi(n)}),\ \pi\in S_n\}$。如果 $f(x)$ 在一个轨道上所取的函数值相同，那么 $f(x)$ 就是一个对称函数。显然，对称函数是旋转对称函数的子类，由定义 4 可知 x 所在的旋转对称轨道记为 $RO_n(x)=\{\rho_n^k(x)|1\leqslant k\leqslant n\}$。$|RO_n(x)|$ 表示旋转对称轨道 $RO_n(x)$ 中的元素个数，称为轨道 $|RO_n(x)|$ 的长度，g_n 表示所有的旋转对称轨道的个数，$\phi(\cdot)$ 表示欧拉函数，根据伯恩赛德引理(Burnside)可得[7]

$$g_n=\frac{1}{n}\sum_{k|n}\phi(k)p^{\frac{n}{k}} \tag{1}$$

$\overline{x}=(\overline{x}_1,\overline{x}_2,\cdots,\overline{x}_n)$ 为轨道 O_x 的代表元，这里 $\overline{x}_1\leqslant\overline{x}_2\leqslant\cdots\leqslant\overline{x}_n$，假设

$$\overline{x}=\left(\underbrace{0,0,\cdots,0}_{i_0},\underbrace{1,1,\cdots,1}_{i_1},\cdots,\underbrace{p-1,p-1,\cdots,p-1}_{i_{p-1}}\right) \tag{2}$$

其中，$i_0+i_1+\cdots+i_{p-1}=n$，$0\leqslant i_j\leqslant n$，$j=0,1,\cdots,p-1$。对称轨道 O_x 中向量的个数记为 $|O_x|$，等于多项式展开系数

$$C(n,i_0,i_1,\cdots,i_{p-2})=\frac{n!}{i_0!i_1!\cdots i_{p-1}!} \tag{3}$$

定义 6 设 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in GF(p)^n$，称 $\boldsymbol{x}$ 是一个 $(i_0,i_1,\cdots,i_{p-1})$-型的向量。在 $\boldsymbol{x}$ 的各分量坐标中，$k\in\{0,1,\cdots,p-1\}$ 出现的次数是 i_k。若其中的向量是 $(i_0,i_1,\cdots,i_{p-1})$-型的，O_x 则称为是一个 $(i_0,i_1,\cdots,i_{p-1})$-型的对称轨道；若其中的向量是 $(i_0,i_1,\cdots,i_{p-1})$-型的，RO_x 称为是一个 $(i_0,i_1,\cdots,i_{p-1})$-型的旋转对称轨道。

根据定义 6，当且仅当 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 在同一个对称轨道中，向量 $\boldsymbol{x}$ 和向量 $\boldsymbol{y}$ 的型相同，显然，$(i_0,i_1,\cdots,i_{p-1})$-型的向量的总数为 $C(n,i_0,i_1,\cdots,i_{p-2})$，注意到不同的对称轨道的个数为方程 $i_0+i_1+\cdots+i_{p-1}=n$，$0\leqslant i_j\leqslant n$，$j=0,1,\cdots,p-1$ 的解的个数，因而不同的型的总数为 $C(n+p-1,n)$，这里

$$C(n,k)=\frac{n!}{k!(n-k)!} \tag{4}$$

显然，对称轨道 O_x 可以被分解为若干个旋转对称轨道，不妨记为 $RO_n(x^1)$，$RO_n(x^2)$，$\cdots$，$RO_n(x^l)$，并且 $RO_n(x^2)\bigcup\cdots\bigcup RO_n(x^l)=O_x$。

引理 1[6] $GF(p)$ 上的 n 变元对称多项式的个数是 $p^{C(n+p-1,n)}$。

引理 2[7] 设 $h_{l,p}$ 为 *GF*(*p*)上的长为 *l* 的旋转对称轨道的个数，则

$$h_{l,p}=p,h_{q^k,p}=\frac{p^{q^k}-p^{q^k-1}}{q^k} \tag{5}$$

引理 3 设 $f(x)\in \mathrm{RSF}_{n,p}$，那么 *f*(*x*)是一阶相关免疫函数当且仅当 *f*(*x*)的任意一个 *l* 值支撑矩阵

$$l\text{-}\boldsymbol{ST}=\begin{pmatrix} i_1 & i_1\cdots & i_1 \\ i_2 & i_2\cdots & i_2 \\ & \cdots & \\ i_k & i_k\cdots & i_k \\ C_{RO_n(x^1)} & & \\ C_{RO_n(x^2)} & & \\ \cdots & & \\ C_{RO_n(x^m)} & & \end{pmatrix}=(\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_n) \tag{6}$$

满足 *GF*(*p*)中的 *p* 个符号在 *l*-***ST*** 的第一列中出现的次数相同，即 $\boldsymbol{c}_1$ 是一个 *OA*(*nm*+*k*,1,*p*,1)。

3　主要结果

假设 *n*=*q*，由引理 1 可知，空间 $GF(p)^q$ 共有 $C(q+p-1,q)$个不同的对称轨道，其中，长轨道的个数为 $N=C(q+p-1,q)-p$，并且每一个长轨道可以分成一些互不相交的长旋转对称轨道。令型相同的长旋转对称轨道构成一个集合，型不同的长旋转对称轨道在不同的集合中，把这些集合按照一定的顺序依次排列为 $\boldsymbol{\Omega}_1$，$\boldsymbol{\Omega}_2$，…，$\boldsymbol{\Omega}_N$。显然 $\boldsymbol{\Omega}_j$ 中元素的个数（旋转对称轨道的个数）与其中的旋转对称轨道的型有关。而长旋转对称轨道的型对应着方程 $i_{j,0}+i_{j,1}+\cdots+i_{j,p-1}=q$ 的一组解（$1\leqslant j\leqslant N$），令

$$\boldsymbol{I}=\begin{pmatrix} i_{1,0} & i_{1,1} & \cdots & i_{1,p-1} \\ i_{2,0} & i_{2,1} & \cdots & i_{2,p-1} \\ \vdots & \vdots & \cdots & \vdots \\ i_{N,0} & i_{N,1} & \cdots & i_{N,p-1} \end{pmatrix}=\begin{pmatrix} \boldsymbol{I}_1 \\ \boldsymbol{I}_2 \\ \vdots \\ \boldsymbol{I}_N \end{pmatrix} \tag{7}$$

其中，$\boldsymbol{I}_u$（$1\leqslant u\leqslant N$）是 $\boldsymbol{I}$ 的第 *u* 个行向量，也是集合 $\boldsymbol{\Omega}_u$ 中的旋转对称轨道的型。

假设下面矩阵的所有的元素 $x_{u,v}$ ($1\leqslant u\leqslant N$, $0\leqslant v\leqslant p-1$)都是非负整数，令

$$\boldsymbol{X}=\begin{pmatrix} x_{1,0} & x_{2,1} & \cdots & x_{N,0} \\ x_{1,1} & x_{2,1} & \cdots & x_{N,1} \\ \vdots & \vdots & \cdots & \vdots \\ x_{1,p-1} & x_{2,p-1} & \cdots & x_{N,p-1} \end{pmatrix}=(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_N)$$

这里 $\boldsymbol{x}_u$ 为矩阵 $\boldsymbol{X}$ 的第 $u(1\leqslant u\leqslant N)$个列向量，向量 $\mathbf{x}_u$ 表示型为 $(i_{u,0},i_{u,1},\cdots,i_{u,p-1})$ 的旋转对称轨道的一个划分，集合 $\boldsymbol{\Omega}_u$ 和向量 $\boldsymbol{I}_u$ 存在一一对应的关系，事实上向量 $\boldsymbol{I}_u$ 是集合 $\boldsymbol{\Omega}_u$ 中旋转对称轨道的型。$\boldsymbol{x}_u^{\mathrm{T}}$ 给出了集合 $\boldsymbol{\Omega}_u$ 中旋转对称轨道的划分，矩阵 $\boldsymbol{X}$ 给出了整个空间 $GF(p)^q$ 的划分。

下文中用 $\boldsymbol{I}_p$ 表示 *p* 个 1 构成的列向量，$\boldsymbol{I}_p^{\mathrm{T}}$ 表示 $\boldsymbol{I}_p$ 的转置，$\boldsymbol{A}\otimes\boldsymbol{B}$ 表示矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 的张量积，由引理 2 可知长旋转对称轨道的个数为

$$\frac{p^q-p}{q}=p\frac{p^{q-1}-1}{q} \tag{8}$$

由费尔马定理可知，它是 *p* 的倍数，而短旋转对称轨道的个数为 *p*，所以函数 *f*(*x*)的每一个 *l*-***ST*** 中需要一个短轨道以保证 *f*(*x*)的平衡性。因而，有如下结果。

定理 1 若 $f(x)\in \mathrm{RSF}_{q,p}$，$\boldsymbol{I}_p$ 为 *p* 阶单位矩阵，那么 *f*(*x*)是一阶弹性函数当且仅当如下的方程组至少有一个解。

$$\boldsymbol{\Phi}_{q,p}=\begin{cases} \boldsymbol{XI}=p^{q-2}(\boldsymbol{I}_p\otimes\boldsymbol{I}_p^{\mathrm{T}})-\boldsymbol{I}_p \\ \sum_{k=0}^{p-1}x_{j,k}=\dfrac{(q-1)!}{i_{j,0}!i_{j,1}!\cdots i_{j,p-1}!}, \\ 0\leqslant k\leqslant p-1 \\ 1\leqslant j\leqslant C(p+q-1,q)-p \end{cases} \tag{9}$$

证明　令 $e_i=(\underbrace{0,0,\cdots,0}_{i-1},1,\underbrace{0,0,\cdots,0}_{p-i})$，将空间 $GF(p)^n$ 中的旋转对称轨道中的向量分成 *p* 组，每一组中的向量构成一个正交表 $OA(p^{q-1},q,p,1)$。

先证充分性，假设矩阵 $\boldsymbol{X}$ 是方程组 $\boldsymbol{\Phi}_{q,p}$ 的一组解，可以根据如下的步骤构造空间 $GF(p)^n$ 中的旋转对称轨道中的一个划分 $\boldsymbol{A}_0,\boldsymbol{A}_1,\cdots,\boldsymbol{A}_{p-1}$。

第一步，从集合 $\boldsymbol{\Omega}_1$ 中选取 $x_{1,0}$ 个 $(i_{1,0},i_{1,1},\cdots,i_{1,p-1})$ 型的旋转对称轨道，从集合 $\boldsymbol{\Omega}_2$ 中选取 $x_{2,0}$ 个 $(i_{1,0},i_{1,1},\cdots,i_{1,p-1})$ 型的旋转对称轨道，…，从集合 $\boldsymbol{\Omega}_N$ 中选取 $x_{N,0}$ 个 $(i_{N,0},i_{N,1},\cdots,i_{N,p-1})$ 型的旋转对称轨道，将这些轨道中的向放入 $\boldsymbol{A}_0$ 中，由方程组 $\boldsymbol{XI}=p^{q-2}(\boldsymbol{I}_p\otimes\boldsymbol{I}_p^{\mathrm{T}})-\boldsymbol{I}_p$，有关系

$$(x_{1,0},x_{2,0},\cdots,x_{N,0})\boldsymbol{I}=p^{q-2}\boldsymbol{I}_p^{\mathrm{T}}-e_1 \tag{10}$$

把向量 $\boldsymbol{0}_p^{\mathrm{T}}$ 放入 $\boldsymbol{A}_0$ 中，这就使 $\boldsymbol{A}_0$ 中的向量构成一个 $OA(p^{q-1},q,p,1)$。

第二步，从集合 $\boldsymbol{\Omega}_1$ 中选取 $x_{1,1}$ 个 $(i_{1,0},i_{1,1},\cdots,i_{1,p-1})$ 型的旋转对称轨道，从集合 $\boldsymbol{\Omega}_2$ 中选取 $x_{2,1}$ 个 $(i_{1,0},i_{1,1},\cdots,i_{1,p-1})$ 型的旋转对称轨道，…，从集合 $\boldsymbol{\Omega}_N$ 中选取 $x_{N,1}$ 个 $(i_{N,0},i_{N,1},\cdots,i_{N,p-1})$ 型的旋转对称轨道，将这些轨道中的向放入 $\boldsymbol{A}_1$ 中，由方程组 $\boldsymbol{XI}=p^{q-2}(\boldsymbol{I}_p\otimes\boldsymbol{I}_p^{\mathrm{T}})-\boldsymbol{I}_p$，有

$$(x_{1,1},x_{2,1},\cdots,x_{N,1})\boldsymbol{I}=p^{q-2}\boldsymbol{I}_p^{\mathrm{T}}-e_2 \tag{11}$$

把向量 $\boldsymbol{I}_p^{\mathrm{T}}$ 放入 $\boldsymbol{A}_1$ 中，这就使 $\boldsymbol{A}_1$ 中的向量构成一个 $OA(p^{q-1},q,p,1)$。

…

第 $p-1$ 步，从集合 $\boldsymbol{\Omega}_1$ 中选取 $x_{1,p-2}$ 个 $(i_{1,0},i_{1,1},\cdots,i_{1,p-1})$ 型的旋转对称轨道，从集合 $\boldsymbol{\Omega}_2$ 中选取 $x_{2,p-2}$ 个 $(i_{1,0},i_{1,1},\cdots,i_{1,p-1})$ 型的旋转对称轨道，…，从集合 $\boldsymbol{\Omega}_N$ 中选取 $x_{N,p-2}$ 个 $(i_{N,0},i_{N,1},\cdots,i_{N,p-1})$ 型的旋转对称轨道，将这些轨道中的向放入 $\boldsymbol{A}_{p-2}$ 中，由方程组 $\boldsymbol{XI}=p^{q-2}(\boldsymbol{I}_p\otimes\boldsymbol{I}_p^{\mathrm{T}})-\boldsymbol{I}_p$，有

$$(x_{1,p-2},x_{2,p-2},\cdots,x_{N,p-2})\boldsymbol{I}=p^{q-2}\boldsymbol{I}_p^{\mathrm{T}}-e_{p-1} \tag{12}$$

把向量 $(p-2)\boldsymbol{I}_p^{\mathrm{T}}$ 放入 $\boldsymbol{A}_{p-2}$ 中，这就使 $\boldsymbol{A}_{p-2}$ 中的向量构成一个 $OA(p^{q-1},q,p,1)$。

第 p 步，最后集合 $\boldsymbol{\Omega}_1$ 中剩下 $x_{1,p-1}$ 个 $(i_{1,0},i_{1,1},\cdots,i_{1,p-1})$ 型的旋转对称轨道，集合 $\boldsymbol{\Omega}_2$ 中剩下 $x_{2,p-1}$ 个 $(i_{1,0},i_{1,1},\cdots,i_{1,p-1})$ 型的旋转对称轨道，…，集合 $\boldsymbol{\Omega}_N$ 中剩下 $x_{N,p-1}$ 个 $(i_{N,0},i_{N,1},\cdots,i_{N,p-1})$ 型的旋转对称轨道，将这些轨道中的向放入 A_{p-1} 中，由方程组 $\boldsymbol{XI}=p^{q-2}(\boldsymbol{I}_p\otimes\boldsymbol{I}_p^{\mathrm{T}})-\boldsymbol{I}_p$，有

$$(x_{1,p-1},x_{2,p-1},\cdots,x_{N,p-1})\boldsymbol{I}=p^{q-2}(\boldsymbol{I}_p\otimes\boldsymbol{I}_p^{\mathrm{T}})-e_p \tag{13}$$

把向量 $(p-1)\boldsymbol{I}_p^{\mathrm{T}}$ 放入 $\boldsymbol{A}_{p-1}$ 中，这就使 $\boldsymbol{A}_{p-1}$ 中的向量构成一个 OA$(p^{q-1},q,p,1)$。

另外一方面，如果

$$\sum_{k=0}^{p-1}x_{j,k}=\frac{(q-1)!}{i_{j,0}!i_{j,1}!\cdots i_{j,p-1}!} \tag{14}$$

其中，$0\leqslant k\leqslant p-1$，以及 $1\leqslant j\leqslant C(q+p-1,q)-p$，方程成立。那么 $\boldsymbol{A}_0,\boldsymbol{A}_1,\cdots,\boldsymbol{A}_{p-1}$ 是空间 $GF(p)^n$ 的一个 1-正交分划。综上所述，函数 $f(x)$是一个一阶弹性函数。

下面证明定理的必要性。假设 $f(x)$是一个一阶弹性函数，根据定义 3 可知，$f(x)$的 l 值支撑矩阵 $\boldsymbol{A}_l$ 是一个 $OA(p^{q-1},q,p,1)$，这里 $0\leqslant l\leqslant p-1$，并且所有的 l 值支撑矩阵 $\boldsymbol{A}_l$ 构成空间 $GF(p)^n$ 的一个 1-正交分划，根据强度为 1 的正交表的定义可知，有方程组 $\boldsymbol{\Phi}_{q,p}$ 成立，证毕

注：假设 $\boldsymbol{\theta}_n$ 为如下的齐次线性方程组

$$\boldsymbol{\theta}_n:\begin{cases}\boldsymbol{XI}=0_{p\times p}\\ \boldsymbol{I}_p^{\mathrm{T}}\boldsymbol{X}=0_N\end{cases}$$

如果 $\boldsymbol{\theta}_n$ 是方程组 $\boldsymbol{\Phi}_{q,p}$ 所对应的齐次线性方程组，那么可以得到 $\boldsymbol{\theta}_n$ 的全部解和 $\boldsymbol{\Phi}_{q,p}$ 的一个特解，不妨设 $\boldsymbol{X}_{q,p}^0$ 为 $\boldsymbol{\theta}_n$ 的一个解，$\boldsymbol{X}_{q,p}$ 是 $\boldsymbol{\Phi}_{q,p}$ 的特解，如果矩阵 $\boldsymbol{X}_{q,p}^0+\boldsymbol{X}_{q,p}$ 中的元素都是非负整数，那么 $\boldsymbol{X}_{q,p}^0+\boldsymbol{X}_{q,p}$ 也是 $\boldsymbol{\Phi}_{q,p}$ 的一个解。

定理 2 符号如前面所定义的，假设方程组 $\boldsymbol{\Phi}_{q,p}$ 有如下的 m 个不同的解。

$$\boldsymbol{X}_t=\begin{pmatrix}x_{1,0}^t & x_{2,0}^t & \cdots & x_{N,0}^t\\ x_{1,1}^t & x_{2,1}^t & \cdots & x_{N,1}^t\\ \vdots & \vdots & \vdots & \vdots\\ x_{1,p-1}^t & x_{2,p-1}^t & \cdots & x_{N,p-1}^t\end{pmatrix}=(\boldsymbol{x}_1^t,\boldsymbol{x}_2^t,\cdots,\boldsymbol{x}_N^t) \tag{15}$$

这里，$n_i=\boldsymbol{I}_p^{\mathrm{T}}\boldsymbol{x}_i^t=\left|\boldsymbol{\Omega}_i\right|$，$1\leqslant t\leqslant m$，$i=1,2,\cdots,n$。令 R_q 为 $GF(p)$上 q 元旋转对称一阶弹性函数的总数，那么

$$R_q=\sum_{t=1}^{m}\left(p!\prod_{i=1}^{N}\frac{n_i!}{\prod_{j=0}^{p-1}x_{i,j}^t!}\right) \tag{16}$$

证明 对于方程组 $\boldsymbol{\Phi}_{q,p}$ 的一个固定的解 $\boldsymbol{X}_t=(\boldsymbol{x}_1^t,\boldsymbol{x}_2^t,\cdots,\boldsymbol{x}_N^t)$，根据定理 1 的证明可知，$GF(p)$上的 q 元一阶弹性函数的个数一定是 $p!$乘以选取分划 $\boldsymbol{A}_0,\boldsymbol{A}_1,\cdots,\boldsymbol{A}_{p-1}$ 的种数，也就是

$$p!\prod_{i=1}^{N}\frac{n_i!}{\prod_{j=0}^{p-1}x_{i,j}^t!} \tag{17}$$

另外一方面，对于方程组 $\boldsymbol{\Phi}_{q,p}$ 的 2 个不同的解 $\boldsymbol{X}_1$ 和 $\boldsymbol{X}_2$，它们对应于空间 $GF(p)^n$ 的不同的分划，即使是同一个解，不同的轨道选取方法，所得到的函数也是不同的，因此，上述的定理 1 构造所得到的一阶弹性函数的总的个数为

$$R_q=\sum_{t=1}^{m}\left(p!\prod_{i=1}^{N}\frac{n_i!}{\prod_{j=0}^{p-1}x_{i,j}^t!}\right) \tag{18}$$

4　结束语

本文利用旋转对称函数的 l 值支撑矩阵的性质给出了 *GF*(*p*)上 *q* 变元一阶弹性旋转对称函数的一个等价刻画，即 *GF*(*p*)上 *q* 变元一阶弹性旋转对称函数的构造等价于一个线性方程组的解，其计数可以通过次方程组的所有解表示出来，进一步推广了文献[11]给出的结果。为了构造 *GF*(*p*)上 *q* 元一阶弹性旋转对称函数，可以通过解方程组 $\boldsymbol{\Phi}_{q,p}$ 来获得，对于比较小的具体的不同素数 p 和 q，可以写出 $\boldsymbol{\Phi}_{q,p}$ 的具体形式，借助于计算机，通过求解 $\boldsymbol{\Phi}_{q,p}$，给出 *GF*(*p*)上 *q* 变元一阶弹性旋转对称函数的构造方案和这类函数的计数结果，对于比较大的素数 p 和 q，求出 $\boldsymbol{\Phi}_{q,p}$ 的所有解是比较困难的。对于具体的素数 p 和 q，如何更有效地求解方程组 $\boldsymbol{\Phi}_{q,p}$，将是下一步要研究的工作。事实上，上述的方程组 $\boldsymbol{\Phi}_{q,p}$ 是一个典型的背包问题，众所周知，背包问题是一个 NP 完全问题。特别需要提出的是，本文的思想方法对于任意的变元 n 也是可行的，只是如果 n 的素因子越多，对应的方程组的规模一般会越大，对应的求解问题会越复杂。

参考文献：

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

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

[3] STANICA P, MAITRA S, CLARK J. Results on rotation symmetric bent and correlation immune Boolean functions[A]. Fast software encryption workshop (FSE 2004)[C]. New Delhi Springer Verlag, 2004. 161-177.

[4] CARLET C, DALAI D K, GUPTA K C, *et al*. Algebraic immunity for cryptographically significant Boolean functions: analysis and construction[J]. IEEE Transaction on Information Theory, 2006, 52(7):3105-3121.

[5] LI Y, CUSICK T W. Linear structures of symmetric functions over finite fields[J]. Information Processing Letters, 2006,97:124-127.

[6] CUSICK T W, LI Y, STANICA P. Balanced symmetric functions over *GF*(*p*)[J]. IEEE Transactions on Information Theory, 2008, 54(3): 1304-1307.

[7] LI Y. Results on rotation symmetric polynomials over *GF*(*p*)[J]. Information Science, 2008, 178:280-286.

[8] KE P H, HUANG L L, ZHANG S Y. Improved lower bound on the number of balanced symmetric functions over *GF*(*p*)[J]. Information Sciences, 2009,179:682-687.

[9] FU S J, LI C, QU L J, *et al*. Enumeration of balanced symmetric functions over *GF*(*p*)[J]. Information Processing Letters, 2010,110:544-548.

[10] FU S J, LI C, QU L J, *et al*. On the number of rotation symmetric functions over *GF*(*p*)[J]. Mathematical and Computer Modelling, 2012, 55:142-150.

[11] 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.

[12] 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.

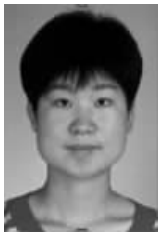
[13] DU J, WEN Q Y, ZHANG J, *et al*. New construction of symmetric orthogonal arrays of strength *t*[J]. IEICE Trans Fundamentals, 2013, 96(9):1901-1904.

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。

庞善起[通信作者]（1965-），男，河南卫辉人，博士，河南师范大学教授、硕士生导师，主要研究方向为试验设计与组合设计。E-mail:shanqipang@126.com。

温巧燕（1959-），女，陕西西安人，北京邮电大学教授、博士生导师，主要研究方向为信息安全、密码学、应用数学。



张劼（1970-），女，河北保定人，博士，北京邮电大学副教授，主要研究方向为密码学。