基于拉丁方的 GF(p)上 q 元旋转对称弹性函数的新构造

杜 蛟[1,2],刘春红[3],张 恩[3],尚玉婧[1,2],董 乐[1,2]
(1. 河南师范大学数学与信息科学学院,河南新乡 453007;
2. 河南师范大学大数据统计分析与优化控制河南省工程实验室,河南新乡 453007;
3. 河南师范大学计算机与信息工程学院,河南新乡 453007)

摘 要: 在特征为 p 的有限域上,基于弹性函数与正交表大集间的等价关系,借助于一个具有最大圈结构的拉丁方,给出了一个构造 q 元旋转对称弹性函数的新方法. 此外,通过一个具体的实例说明了本文的方法能够构造出已有方法不能构造的 GF(p)上的 q 元旋转对称弹性函数.

关键词: 密码学; 旋转对称函数; 平衡函数; 弹性函数; l 值支撑矩阵
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2018)09-2173-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.09.018

New Constructions of q-Variable Rotation Symmetric Resilient Functions Based on Latin Square Over GF(p)

DU Jiao[1,2], LIU Chun-hong[3], ZHANG En[3], SHANG Yu-jing[1,2], DONG Le[1,2]
(1. *College of Mathematics and Information Science, Henan Normal University, Xinxiang, Henan* 453007, *China*;
2. *Henan Engineering Laboratory for Big Data Statistical Analysis and Optimal Control, Henan Normal University, Xinxiang, Henan* 453007, *China*;
3. *College of Computer and Information Engineering, Henan Normal University, Xinxiang, Henan* 453007, *China*)

Abstract: A novel method to construct rotation symmetric resilient functions with q variables is proposed over GF(p) by using a Latin square with maximum cycle structure. This method is based on the equivalence between resilient functions and Large sets of orthogonal arrays. Additionally, an example is given to demonstrate that some rotation symmetric resilient functions with q variables can be constructed by the method presented in this paper, while these functions cannot be determined according to the earlier constructions over the finite field GF(p).

Key words: cryptography; rotation symmetric functions; balanced functions; resilient functions; l-value support table

1 引言

近年来,旋转对称布尔函数因为其良好的密码学性质而受到极大的关注[1~5],计算机搜索结果表明,旋转对称布尔函数可以同时具有平衡性、高非线性度、相关免疫性、最优代数免疫性、高代数次数等密码学性质[2~4]. 因此,把旋转对称函数的有关概念和结果从特征为2的有限域上推广到特征为奇素数 p 的有限域上,进而研究有限域 GF(p)上具有某些密码学性质的旋转对称函数的构造就是一个有意义的工作. 特征为 p 的有限域上的旋转对称函数(RSFs)近来受到了较多的关注,对称函数是旋转对称函数的一个子类,Cusick 和 Li Yuan 等人首先研究了有限域 GF(p)上对称函数的线性结构[6],给出了 GF(p)上平衡对称函数的构造与计数下界[7],柯品惠等人进一步改进了它们的下界[8]. 与此同时,付绍静等人进一步证明了这类函数的构造问题等价于求解一个方程组,并根据方程组的解对所构造的函数个数进行计数[9].

文献[10]研究了平衡的旋转对称多项式的构造与计数问题,得到了一系列结果,文献[11,12]进一步深

收稿日期:2017-05-09;修回日期:2018-05-09;责任编辑:梅志强
基金项目:国家自然科学基金(No. U1404601, No. 11571094, No. 11501181, No. U1604156, No. 61402154);河南省科技攻关计划项目(No. 172102210045);河南师范大学博士科研启动基金资助项目(No. 5101019170133).

入研究了特殊的平衡的旋转对称函数的计数问题. 受到上述结果的启发,文献[13]给出了 GF(p)上 q(本文中均为不同于 p 的奇素数)元旋转对称弹性函数的等价刻画,文献[14,15]研究了 GF(p)上素数元旋转对称 1-弹性函数的构造问题,并分别给出了计数下界.

本文基于弹性函数与正交表大集间的等价关系,借助一个具有最大圈结构的拉丁方,给出了旋转对称轨道的所有的型的一个划分. 由这个划分将所有的长旋转对称轨道组成 $(p^{q-1}-1)/q$ 个不同的 OA($pq,q,p,1$),然后通过求解一个方程组,寻求 r 个特殊的 OA($pq,q,p,1$),使得这些正交表含有的旋转对称轨道与 p 个长度为 1 的短轨道一起重新构成 p 个不同的正交表 OA($rq+1,q,p,1$). 最后将这些正交表(看做行向量的集合)取相同的函数值,从而构造出新的 q 元旋转对称弹性函数,本文中 p 和 q 为不同的奇素数,最后通过一个具体的实例说明了本文的方法能够构造出文献[14]中已有方法不能构造出来的 GF(p)上的 q 元旋转对称弹性函数.

2 预备知识

设有限域 $\mathrm{GF}(p)=\{0,1,\cdots,p-1\}$,$\mathrm{GF}(p)^n$ 表示 GF(p)上的 n 维向量空间. 映射 $f:\mathrm{GF}(p)^n\to\mathrm{GF}(p)$ 表示一个 n 元广义的布尔函数,定义在 $\mathrm{GF}(p)^n$ 上的 n 元广义布尔函数的全体记为 $B_{n,p}$. $|S|$表示集合 S 中元素的个数;本文中若 S 表示一个维数相同的行向量构成的集合,那么 $\boldsymbol{S}$ 可以看成一个行向量属于 S 的矩阵;反过来,若一个矩阵 $\boldsymbol{S}$ 的行互不相同,则矩阵 $\boldsymbol{S}$ 可看作其行向量构成的集合.

定义 1[13] 设 $f(x)\in B_{n,p}$,记 $f^{-1}(l)=\{x\in\mathrm{GF}(p)^n\mid f(x)=l,l\in\mathrm{GF}(p)\}$ 若对任意的 $l\in\mathrm{GF}(p)$ 都有 $|f^{-1}(l)|=p^{n-1}$,则称 $f(x)$ 是一个平衡函数,$f^{-1}(l)$ 称为广义布尔函 $f(x)$ 的 l 值支撑集,集合 $f^{-1}(l)$ 中的向量称为 l 值支撑向量.

定义 2[16,17] 对于有限域 GF(p)上的 $w\times n$ 矩阵 $\boldsymbol{A}$,如果空间 $\mathrm{GF}(p)^d$ 中的每一个向量都在矩阵 $\boldsymbol{A}$ 的任意列中出现相同的次数,则称是一个正交表 OA(w,n,p,d).

定义 3[16] 对任意的 $0\le i,j\le p-1$,每一个 V_i 都是一个 OA(p^{n-1},n,p,d),且 $V_i\cap V_j=\varnothing,i\ne j$,而 $\bigcup_{i=0}^{p-1}V_i=\mathrm{GF}(p)^n$(把 V_i 看成集合),则称集合 $\{V_0,V_1,\cdots,V_{p-1}\}$ 为一个正交表大集,记为 LOA(p^{n-1},n,p,d).

下面考虑循环群 $C_n=\{\rho_n^l\mid 0\le l\le n-1\}$ 在 $\mathrm{GF}(p)^n$ 上的作用,变换 ρ_n^l 定义为:

$$\begin{aligned}\rho_n^l(x_1,x_2,\cdots,x_n)&=(\rho_n^l(x_1),\rho_n^l(x_2),\cdots,\rho_n^l\{x_n\})\\&=(x_{l+1},x_{l+2},\cdots,x_n,x_1,\cdots,x_l),\end{aligned}$$

$x=(x_1,x_2,\cdots,x_n)\in\mathrm{GF}(p)^n$ 在群 $C_n=\{\rho_n^l\mid 0\le l\le n-1\}$ 的作用下形成的轨道记为 $\mathrm{RO}_n(x)=\{\rho_n^l(x)\mid 0\le l\le n-1\}$. 为了方便,本文中将 $\boldsymbol{RO}_n(x)$ 看作一个行向量来自于 $\mathrm{RO}_n(x)$ 的轨道矩阵. 称 $\mathrm{RO}_n(x)$ 为一个长旋转对称轨道,若 $|\mathrm{RO}_n(x)|=n$,否则称其是一个短旋转对称轨道.

定义 4[11] 设 $f(x)\in B_{n,p}$,若 $f(\rho_n^l(x_1,x_2,\cdots,x_n))=f(x_1,x_2,\cdots,x_n)$ 对任意的 $0\le l\le n-1$ 都成立,则称 $f(x)$ 是一个旋转对称函数,$\mathrm{GF}(p)^n$ 上旋转对称函数的全体记为 $\mathrm{RSF}_{n,p}$.

引理 1[10] 设 g_n 为所有的旋转对称轨道的个数,那么 GF(p)上所有的 n 元旋转对称函数的总数为 p^{g_n},这里

$$g_n=(1/n)\sum_{k\mid n}\varphi(k)\cdot p^{n/k},$$

其中 $\varphi(\cdot)$ 表示欧拉函数.

如果对称群 S_n 作用在 $x=(x_1,x_2,\cdots,x_n)\in\mathrm{GF}(p)^n$ 上,则形成一个如下的对称轨道 $O_x=\{(y_1,y_2,\cdots,y_n)\mid(y_1,y_2,\cdots,y_n)=(x_{\pi(1)},x_{\pi(2)},\cdots,x_{\pi(n)}),\pi\in S_n\}$.

定义 5[6,7] 设 $f(x)\in B_{n,p}$,如果 $f(x_{\pi(1)},x_{\pi(2)},\cdots,x_{\pi(n)})=f(x_1,x_2,\cdots,x_n)$ 对任意的 $\pi\in S_n$ 都成立,则称 $f(x)$ 是一个对称函数.

定义 6[13] 设 $x=(x_1,x_2,\cdots,x_n)\in\mathrm{GF}(p)^n$,称 $\boldsymbol{x}$ 是一个 $(i_0,i_1,\cdots,i_{p-1})$ 型的向量. 如果在 $\boldsymbol{x}$ 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,则称对称轨道 O_x 是 $(i_0,i_1,\cdots,i_{p-1})$ 型的;若其中的向量是 $(i_0,i_1,\cdots,i_{p-1})$ 型的,则称旋转对称轨道 $\mathrm{RO}_n(x)$ 是 $(i_0,i_1,\cdots,i_{p-1})$ 型的.

让 $\overline{x}=(\overline{x_1},\overline{x_2},\cdots,\overline{x_n})$ 为对称轨道 O_x 的代表元,这里 $\overline{x_1}\le\overline{x_2}\le\cdots\le\overline{x_n}$,本文中只考虑函数的变元个数 $n=q$ 的情况,不妨假设

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

这里 $i_0+i_1+\cdots+i_{p-1}=q$,并且对于任意的 $s\in\mathrm{GF}(p)$ 都有 $0\le i_s\le q$. 显然有如下的关系:

$$|O_x|=q!/(i_0!\,i_1!\cdots i_{p-1}!).$$

当函数的变元个数 $n=q$ 时,对称群 S_q 将空间 $\mathrm{GF}(p)^q$ 分成了 $C(p+q-1,q)$ 个不同的对称轨道,

因而不同的型的总数为 $C(p+q-1,q)$,其中所有的长对称轨道的型的总数为:

$$N=C(p+q-1,q)-p.$$

根据不同的型,将所有的长对称轨道被分成 N 个不同的类 $\Omega_1,\Omega_2,\cdots,\Omega_N$,其中集合 Ω_j 中对称轨道的型为 $(i_{j,0},i_{j,1},\cdots,i_{j,p-1})$,并且 Ω_j 中不同的旋转对称轨道的总数为:

$$n_j=(q-1)!\ /(i_{j,0}!\ i_{j,1}!\ \cdots i_{j,p-1}!).$$

引理 2[10]　当变元个数 n 为素数 q 时,旋转对称轨道的总数 g_q 和长旋转对称轨道的总数 $h_{q,p}$ 依次为:

$$g_q=(1/q)\sum_{t\mid q}\varphi(t)p^{q/t}=p\cdot[(p^{q-1}-1)/q]+p;$$

$$h_{q,p}=p\cdot[(p^{q-1}-1)/q]=\sum_{r=1}^{N}n_r.$$

为了方便,我们约定整数 $K=(p^{q-1}-1)/q$,行向量 $\boldsymbol{e}_{n,s}=(\underbrace{ss\cdots s}_{n})$. 为了构造有限域 GF($p$)上 q 元 1 阶旋转对称弹性函数,我们只需要将 GF $(p)^q$ 中的 p^q 个向量分成互不相交的,向量个数相等的 p 组,即 $V_0,V_1,\cdots,V_{P-1}$,满足 GF $(p)^q=\bigcup_{s=0}^{p-1}V_s$,使得每个旋转对称轨道中的所有向量在同一组中,且集合$\{V_0,V_1,\cdots,V_{P-1}\}$构成一个 LOA$(p^{q-1},q,p,1)$. 由于 $p^{q-1}-1$ 不是 p 的倍数,所以正如文献[11]中所证明的,集合$\{\boldsymbol{e}_{q,s}\mid 0\leq s\leq p-1\}$中的任意两个向量所取函数值不同,以保证函数 $f(x)$ 的平衡性,即每一个 V_s 中包含一个短旋转对称轨道,以及 K 个长旋转对称轨道.

3　主要结果

3.1　有限域 GF $(p)^q$ 上旋转对称轨道的性质

下面,我们开始研究有限域 GF(p)上 q 元 1 阶旋转对称轨道的性质. 让长旋转对称轨道的 N 个不同的型按照一定的顺序构成如下的矩阵:

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

这里 $\boldsymbol{I}_j=(i_{j,0},i_{j,1},\cdots,i_{j,p-1})$ 表示矩阵 $\boldsymbol{I}$ 的第 j 个行向量,也就是集合 Ω_j 中旋转对称轨道的型,并且 $N=C(p+q-1,q)-p$.

若 $\tau\in S_p$,且$\{0,\tau(0),\cdots,\tau^{p-1}(0)\}=\mathrm{GF}(p)$,则下面的矩阵 $\boldsymbol{L}$ 是一个拉丁方:

$$\boldsymbol{L}=\begin{pmatrix}0&\cdots&p-1\\\tau(0)&\cdots&\tau(p-1)\\\vdots&\ddots&\vdots\\\tau^{p-1}(0)&\cdots&\tau^{p-1}(p-1)\end{pmatrix}$$

对于任意的 $1\leq j\leq N$,若 $\tau^k(i_{j,0},i_{j,1},\cdots,i_{j,p-1})=(i_{j,\tau^k(0)},i_{j,\tau^k(1)},\cdots,i_{j,\tau^k(p-1)})$,$0\leq k\leq p-1$,显然 τ 是一具有最大圈结构的置换,注意到$\{\tau^k\mid 0\leq k\leq p-1\}$是对称群 S_p 的一子群.

定义 7[15]　具有上述 $\boldsymbol{L}$ 这样最长圈结构的拉丁方称为具有最大圈结构的拉丁方.

下面考虑循环群$\{\tau^k\mid 0\leq k\leq p-1\}$在 $\boldsymbol{I}$ 上的作用,假设可以得到 m 个不同的轨道,按照一定的顺序分别记为 $\Delta_1,\Delta_2,\cdots,\Delta_m$. 将 Δ_l 中的向量按照一定的顺序排列,这里 $1\leq l\leq m$,将它们中排在第一位的向量作为该轨道的代表元,将这些代表元依次记 $J_1,J_2,\cdots,J_m$,即对于 $J_l=(i_{k_l,0},i_{k_l,1},\cdots,i_{k_l,p-1})\in\Delta_l$ 都有 $\tau^k(J_l)\in\Delta_l$,且 $1\leq k_1<k_2<\cdots<k_m\leq N$,$0\leq k\leq p-1$.

定理 1　符号如前所述,对任意的 $0\leq k\leq p-1$,有如下的结果成立:

(1)对任意的 $1\leq l\leq m$,都有 $|\Delta_l|=p$ 成立;

(2)对于任意的 J_l 和 $0\leq k\leq p-1$,都有 $\tau^k(J_l)=\tau^k(i_{k_l,0},i_{k_l,1},\cdots,i_{k_l,p-1})\in\Delta_l$,RSO$(\tau^k(J_l))$表示型为 $\tau^k(J_l)$的所有旋转对称轨道构成的集合,且型为 $\tau^k(J_l)$的旋转对称轨道的个数均为:$n_{k_l}=|\mathrm{RSO}(\tau^k(J_l))|=(q-1)!\ /(i_{k_l,0}!\ i_{k_l,1}!\ \cdots i_{k_l,p-1}!)$,其中 $1\leq l\leq m$.

证明

(1)采用反证法. 注意到 $J_l=(i_{k_l,0},i_{k_l,1},\cdots,i_{k_l,p-1})\in\Delta_l$,不妨设存在不同的 s 和 t,满足 $0\leq s<t\leq p-1$,且有如下的关系:

$$(i_{k_l,\tau^s(0)},i_{k_l,\tau^s(1)},\cdots,i_{k_l,\tau^s(p-1)})=(i_{k_l,\tau^t(0)},i_{k_l,\tau^t(1)},\cdots,i_{k_l,\tau^t(p-1)});$$

那么对任意的 $0\leq v\leq p-1$,都有 $i_{k_l,\tau^s(v)}=i_{k_l,\tau^t(v)}$,那么矩阵

$$\boldsymbol{L}=\begin{pmatrix}0&\cdots&p-1\\\tau(0)&\cdots&\tau(p-1)\\\vdots&\ddots&\vdots\\\tau^{p-1}(0)&\cdots&\tau^{p-1}(p-1)\end{pmatrix}$$

的第 $s+1$ 行与第 $t+1$ 行相等,即

$$(\tau^s(0),\tau^s(1),\cdots,\tau^s(p-1))=(\tau^t(0),\tau^t(1),\cdots,\tau^t(p-1)),$$

这就与前文中 $\boldsymbol{L}$ 是一个拉丁方的假设矛盾,从而上述的假设不成立,即对任意的 $0\leq s<t\leq p-1$,有:

$$(i_{k_l,\tau^s(0)},i_{k_l,\tau^s(1)},\cdots,i_{k_l,\tau^s(p-1)})\neq(i_{k_l,\tau^t(0)},i_{k_l,\tau^t(1)},\cdots,i_{k_l,\tau^t(p-1)}),$$

且对任意的 $0\leq k\leq p-1$,都有 $\tau^k(J_l)\in\Delta_l$,从而对任意的 $1\leq l\leq m$,都有 $|\Delta_l|=p$ 成立,(1)获证.

(2)若 $J_l=(i_{k_l,0},i_{k_l,1},\cdots,i_{k_l,p-1})\in\Delta_l$,则由集合 Δ_l 的定义可知,$\tau^k(J_l)$满足:

$$\tau^k(J_l)=(i_{k_l,\tau^k(0)},i_{k_l,\tau^k(1)},\cdots,i_{k_l,\tau^k(p-1)})\in\Delta_l,$$

其中 $0\leq k\leq p-1$. 注意到

$$i_{k_l,\tau^k(0)}+i_{k_l,\tau^k(1)}+\cdots+i_{k_l,\tau^k(p-1)}=q,$$

故型为 $\tau^k(J_l)$的旋转对称轨道的总数为:

$$|\mathrm{RSO}(\tau^k(J_l))|=(q-1)!\ /(i_{k_l,0}!\ i_{k_l,1}!\ \cdots i_{k_l,p-1}!)$$

而 $\tau^k(0),\tau^k(1),\cdots,\tau^k(p-1)$是 $0,1,\cdots,p-1$ 的一个排列,故有

$$\begin{aligned}n_{k_l}&=|\mathrm{RSO}(\tau^k(J_l))|\\&=(q-1)!\ /(i_{k_l,\tau^k(0)}!\ i_{k_l,\tau^k(1)}!\ \cdots i_{k_l,\tau^k(p-1)}!)\\&=(q-1)!\ /(i_{k_l,0}!\ i_{k_l,1}!\ \cdots i_{k_l,p-1}!)\end{aligned}$$

这就完成了(2)的证明.

由上述的定理1可知此时矩阵 $\boldsymbol{I}$ 可以改写为如下的形式:

$$\boldsymbol{I}=\begin{pmatrix}\Delta_1\\ \Delta_2\\ \vdots\\ \Delta_m\end{pmatrix},m=\frac{N}{p},\Delta_l=\begin{pmatrix}J_l\\ \tau(J_l)\\ \vdots\\ \tau^{p-1}(J_l)\end{pmatrix},\text{其中 } 1\leq l\leq m.$$

且对于 Δ_l 中的 p 个不同的型 $\tau^k(J_l)$ 而言,对于任意的 $0\leq k\leq p-1$,型为 $\tau^k(J_l)$ 的旋转对称轨道的个数均为 n_{k_l}. 下面我们来研究型属于 Δ_l 的旋转对称轨道的性质,有如下的结果:

定理2 概念与符号如前所述,设 $\boldsymbol{M}_k$ 是循环群 $C_q=\{\rho_q^i\mid 0\leq i\leq q-1\}$ 作用在 $\mathrm{GF}(p)^q$ 上形成的一个 $\tau^k(J_l)=(i_{k_l,\tau^k(0)},i_{k_l,\tau^k(1)},\cdots,i_{k_l,\tau^k(p-1)})$ 型的长旋转对称轨道(矩阵),$0\leq k\leq p-1$,$1\leq k\leq m$,则如下的矩阵:

$$\boldsymbol{M}=\begin{pmatrix}\boldsymbol{M}_0\\ \boldsymbol{M}_1\\ \vdots\\ \boldsymbol{M}_{p-1}\end{pmatrix}=(\boldsymbol{m}_1,\boldsymbol{m}_2,\cdots,\boldsymbol{m}_q)$$

是一正交表 $\mathrm{OA}(pq,q,p,1)$,这里 $\boldsymbol{m}_1,\boldsymbol{m}_2,\cdots,\boldsymbol{m}_q$ 是矩阵 $\boldsymbol{M}$ 的 q 个列向量.

证明:要证 $\boldsymbol{M}$ 是一个正交表 $\mathrm{OA}(pq,q,p,1)$,只需证 m_1 是一个正交表 $\mathrm{OA}(pq,1,p,1)$ 即可.

首先考虑矩阵 $\boldsymbol{M}$ 的子矩阵 $\boldsymbol{M}_k$,其行向量实际上构成一个旋转对称轨道,这里 $0\leq k\leq p-1$,不妨设 $\boldsymbol{M}_k$ 是由 $\boldsymbol{x}=(x_1,x_2,\cdots,x_q)\in\mathrm{GF}(p)^q$ 在群 $C_q=\{\rho_q^i\mid 0\leq i\leq q-1\}$ 的作用下生成的旋转对称轨道,则可以将 $\boldsymbol{\tau}^k(J_l)$ 型的矩阵 $\boldsymbol{M}_k$ 表示为:

$$\boldsymbol{M}_k=\begin{pmatrix}x_1 & x_2 & \cdots & x_q\\ x_2 & x_3 & \cdots & x_1\\ \vdots & \vdots & \ddots & \vdots\\ x_q & x_1 & \cdots & x_{q-1}\end{pmatrix}=(\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_q)$$

注意到矩阵 $\boldsymbol{M}_k$ 是一个对称矩阵,其中 $\boldsymbol{a}_1$ 是它的第一列. 显然 $\boldsymbol{a}_1$ 能够为矩阵 $\boldsymbol{M}$ 的第一列 $\boldsymbol{m}_1$ 贡献 $i_{k_l,\tau^k(0)}$ 个 0,$i_{k_l,\tau^k(1)}$ 个 1,$\cdots$,$i_{k_l,\tau^k(p-1)}$ 个 $p-1$. 当 k 跑遍 $\mathrm{GF}(p)$ 时,在矩阵 $\boldsymbol{M}_0$ 的第一列中有 $i_{k_l,0}$ 个 0,在矩阵 $\boldsymbol{M}_1$ 的第一列中有 $i_{k_l,\tau(0)}$ 个 0,,矩阵 $\boldsymbol{M}_{p-1}$ 的第一列中有 $i_{k_l,\tau^{p-1}(0)}$ 个 0,从而在矩阵 $\boldsymbol{M}$ 的第一列 $\boldsymbol{m}_1$ 中 0 出现的总数为:$i_{k_l,0}+i_{k_l,\tau(0)}+\cdots+i_{k_l,\tau^{p-1}(0)}$,注意到 $\boldsymbol{L}$ 是一个拉丁方,故 $\{0,\tau(0),\tau^2(0),\cdots,\tau^{P-1}(0)\}=\mathrm{GF}(p)$,从而 $i_{k_l,0}+i_{k_l,\tau(0)}+\cdots+i_{k_l,\tau^{p-1}(0)}=i_{k_l,0}+i_{k_l,1}+\cdots+i_{k_l,p-1}=q$,这就意味着在矩阵 $\boldsymbol{M}$ 的第 1 列 $\boldsymbol{m}_1$ 中符号 0 出现的总数为 q.

类似地,对于任意的 $k\in\mathrm{GF}(p)$,在矩阵 $\boldsymbol{M}_0$ 的第 1 列中有 $i_{k_l,k}$ 个 k,在矩阵 $\boldsymbol{M}_1$ 的第一列中有 $i_{k_l,\tau(k)}$ 个 k,$\cdots$,矩阵 $\boldsymbol{M}_{p-1}$ 的第一列中有 $i_{k_l,\tau^{p-1}(k)}$ 个 k,从而在矩阵 $\boldsymbol{M}$ 的第一列 $\boldsymbol{m}_1$ 中符号 k 的出现的总数为 $i_{k_l,k}+i_{k_l,\tau(k)}+\cdots+i_{k_l,\tau^{p-1}(k)}$,注意到 $\{k,\tau(k),\cdots,\tau^{p-1}(k)\}=\mathrm{GF}(p)$,从而

$$\begin{aligned}&i_{k_l,k}+i_{k_l,\tau(k)}+\cdots+i_{k_l,\tau^{p-1}(k)}\\ =&i_{k_l,0}+i_{k_l,1}+\cdots+i_{k_l,p-1}\\ =&q.\end{aligned}$$

这就说明对于任意的 $k\in\mathrm{GF}(p)$,j 在矩阵 $\boldsymbol{M}$ 的第一列 $\boldsymbol{m}_1$ 中出现的总数均为 q,这就证明了 $\boldsymbol{m}_1$ 是一个 $\mathrm{OA}(pq,1,p,1)$,这就完成了证明.

在定理2中若变换 $\tau\in C_p=\{\rho_p^i\mid 0\leq i\leq p-1\}$,作用在 N 个不同的型构成的集合 $\boldsymbol{I}$ 上,那么我们有如下的推论:

推论1 概念与符号如前所述,设 $\boldsymbol{M}_k$ 是循环群 $C_q=\{\rho_q^i\mid 0\leq i\leq q-1\}$ 作用在 $\mathrm{GF}(p)^q$ 上形成的一个 $(i_k,i_{k+1},\cdots,i_{p-1},i_0,\cdots,i_{k-1})$ 型的长旋转对称轨道(矩阵),且 $0\leq k\leq p-1$,则如下的矩阵:

$$\boldsymbol{M}=\begin{pmatrix}\boldsymbol{M}_0\\ \boldsymbol{M}_1\\ \vdots\\ \boldsymbol{M}_{P-1}\end{pmatrix}=(\boldsymbol{m}_1,\boldsymbol{m}_2,\cdots,\boldsymbol{m}_q)$$

是一正交表 $\mathrm{OA}(pq,q,p,1)$,这里 $\boldsymbol{m}_1,\boldsymbol{m}_2,\cdots,\boldsymbol{m}_q$ 是矩阵 $\boldsymbol{M}$ 的 q 个列向量.

推论1实际上就是文献[14]中的定理1,由此可见,文献[14]中定理1是本文定理2的特殊情形.

对任意的 $1\leq l\leq m$,注意到

$$\Delta_l=\{J_l,\tau(J_l),\cdots,\tau^{p-1}(J_l)\}$$

其中 Δ_l 的代表元为 $J_l=(i_{k_l,0},i_{k_l,1},\cdots,i_{k_l,p-1})$.

由定理1的(2)可知型为 $\tau^k(J_l)$ 的旋转对称轨道的个数为

$$\begin{aligned}n_{k_l}&=|\mathrm{RSO}(\tau^k(J_l))|\\ &=(q-1)!/(i_{k_l,0}!\ i_{k_l,1}!\cdots i_{k_l,p-1}!).\end{aligned}$$

对于不同的 $0\leq k\leq p-1$,从集合 $\mathrm{RSO}(\tau^k(J_l))$ 中分别选出一个旋转对称轨道,根据上述的定理2可知,这 p 个旋转对称轨道构成一个正交表 $\mathrm{OA}(pq,q,p,1)$,这样可得到 n_{k_l} 个 $\mathrm{OA}(pq,q,p,1)$,将它们构成的集合记为 $\{\boldsymbol{M}_{k_l,1},\boldsymbol{M}_{k_l,2},\cdots,\boldsymbol{M}_{k_l,n_k}\}$,当 i 跑遍集合 $\{l\mid 1\leq l\leq m\}$ 时,则可以得到 K 个不同的 $\mathrm{OA}(pq,q,p,1)$,这时 $\mathrm{GF}(p)^q$ 就被分成了 K 个不同的 $\mathrm{OA}(pq,q,p,1)$ 以及 p 个短轨道 $\{\boldsymbol{e}_{q,k}\}$,这里 $0\leq k\leq p-1$.

3.2 GF(p)上基于拉丁方的 q 元1阶旋转对称弹性函数的构造

注意到 K 不是 p 的倍数,所以我们不能把上述 K 个不同的 $\mathrm{OA}(pq,q,p,1)$ 平均分成 p 组来构造 q 元旋转对称弹性函数. 为了解决这个问题,我们考虑寻找其中若

干个 OA(pq,q,p,1),不妨记这样的正交表的个数为 r,满足 $K=(p^{q-1}-1)/q=p\cdot g+r$,$1\le r\le p-1$,其中 $g\ge 0$.

不难证明满足上述条件的整数 r 是唯一的,那么我们有 $w=(r\cdot q+1)/p=p^{q-2}-q\cdot g$,现要从上述的 K 个 OA(pq,q,p,1)中找到 r 个特殊的正交表 OA(pq,q,p,1),然后把它们分成 rp 个不同的旋转对称轨道,接下来再将这 rp 个不同的旋转对称轨道重新分成 p 组,使得每一组中的旋转对称轨道与某个短轨道$\{\boldsymbol{e}_{q,k}\}$都能构成一个 OA($rq+1$,q,p,1). 如下的定理 3 给出了一个有效的方法.

定理 3　让 $\boldsymbol{e}_i=(\underbrace{0,0,\cdots,0}_{i-1},1,\underbrace{0,0,\cdots,0}_{p-i})$,如果下面的方程组:

$$(1)\begin{cases}\boldsymbol{e}_{r,1}\boldsymbol{X}=\boldsymbol{e}_{p,w}-\boldsymbol{e}_1\\ \boldsymbol{X}\boldsymbol{e}_{p,1}^{\mathrm{T}}=\boldsymbol{e}_{r,q}^{\mathrm{T}}\end{cases}$$

有一个解

$$\boldsymbol{X}=\begin{pmatrix}x_{1,0}&x_{1,1}&\cdots&x_{1,p-1}\\ x_{2,0}&x_{2,1}&\cdots&x_{2,p-1}\\ \vdots&\vdots&\ddots&\vdots\\ x_{r,0}&x_{r,1}&\cdots&x_{r,p-1}\end{pmatrix}=\begin{pmatrix}\boldsymbol{x}_1\\ \boldsymbol{x}_2\\ \vdots\\ \boldsymbol{x}_r\end{pmatrix},$$

满足下面的条件:

(1)$x_{u,v}\in\{0,1,\cdots,q-1\}$,$1\le u\le r$,$0\le v\le p-1$;

(2)$\boldsymbol{x}_i$ 是矩阵 $\boldsymbol{X}$ 的第 i 个行向量,并且有 $\bigcup_{i=1}^{l_1}\{x_i\}\subseteq\Delta_1$,$\bigcup_{i=l_1+1}^{l_1+l_2}\{\boldsymbol{x}_i\}\subseteq\Delta_2$,$\cdots$,$\bigcup_{i=r-l_m+1}^{r}\{\boldsymbol{x}_i\}\subseteq\Delta_m$,这里 $0\le l_1\le n_{k_1}$,$0\le l_2\le n_{k_2}$,$\cdots$,$0\le l_m\le n_{k_m}$,且 $l_1+l_2+\cdots+l_m=r$,那么存在 p 个不同的正交表 OA($rq+1$,q,p,1),记为 $\boldsymbol{B}_0,\boldsymbol{B}_1,\cdots,\boldsymbol{B}_{p-1}$,使得对任意的$\{s,t\}\subseteq$GF($p$),都有 $\boldsymbol{e}_{q,s}\in\boldsymbol{B}_s$,$\boldsymbol{e}_{q,t}\in\boldsymbol{B}_t$,$\boldsymbol{B}_s\cap\boldsymbol{B}_t=\varnothing$,且每一个 $\boldsymbol{B}_s$ 中都含有 r 个不同的旋转对称轨道.

证明:不失一般性,我们通过构造 p 个不同的满足条件的 OA($rq+1$,q,p,1)来证明定理正确性,也就是 $\boldsymbol{B}_0,\boldsymbol{B}_1,\cdots,\boldsymbol{B}_{p-1}$,满足对任何$\{s,t\}\subseteq$GF($p$)都有 $\boldsymbol{e}_{q,s}\in\boldsymbol{B}_s$,$\boldsymbol{e}_{q,t}\in\boldsymbol{B}_t$,$\boldsymbol{B}_s\cap\boldsymbol{B}_t=\varnothing$,且每一个 $\boldsymbol{B}_s$ 中都含有 r 个不同的长旋转对称轨道,这里的构造方法完全类似于参考文献[14]中的定理 2,也可参考文献[15]中的 Construction 1 和定理 3.

注意到变换 $\tau\in S_p$,$\{0,\tau(0),\cdots,\tau^{p-1}(0)\}=$GF($p$)如果 $\boldsymbol{X}=(X_0,X_1,\cdots,X_{p-1})$是如下的方程组

$$(1)\begin{cases}\boldsymbol{e}_{r,1}\boldsymbol{X}=\boldsymbol{e}_{p,w}-\boldsymbol{e}_1\\ \mathrm{Xe}_{p,1}^{\mathrm{T}}=\boldsymbol{e}_{r,q}^{\mathrm{T}}\end{cases}$$

的一组解,则 $\boldsymbol{X}=(X_0,X_{\tau(0)},\cdots,X_{\tau^{p-1}(0)})$也是(1)的一组解,那么 $\boldsymbol{X}=(X_{\tau(0)},X_{\tau(1)},\cdots,X_{\tau(p-1)})$就是如下的方程组:

$$(i)\begin{cases}\boldsymbol{e}_{r,1}\boldsymbol{X}=\boldsymbol{e}_{p,w}-\boldsymbol{e}_{1+\tau^{p-1}(0)}\\ \boldsymbol{X}\boldsymbol{e}_{p,1}^{\mathrm{T}}=\boldsymbol{e}_{r,q}^{\mathrm{T}}\end{cases}$$

的一个解,反之亦然.

事实上,定理 3 启发我们通过方程组(1)和方程组(i)的解去寻找 r 个特殊的 OA(pq,q,p,1),然后再把这 r 个特殊的正交表 OA($rq+1$,q,p,1)分成 rp 个不同的旋转对称轨道,再从中选出 r 个不同的长旋转对称轨道与一个短旋转对称轨道一起构成一个 OA($rq+1$,q,p,1). 由定理 3,我们可以构造出 p 个不同的 OA($rq+1$,q,p,1),每一个 OA($rq+1$,q,p,1),包含一个短旋转对称轨道轨道.

下面我们再把余下的 $K-r$ 个不同的 OA(pq,q,p,1)平均分成 p 组 $A_0,A_1,\cdots,A_{p-1}$. 使得每一组中都有 g 个正交表 OA(pq,q,p,1),最后将每一组都与某个 $\boldsymbol{B}_k$ 组合在一起,取相同的函数值,不同的组合取不同的函数值,这样我们就构造出一个 GF(p)上的 q 元 1 阶旋转对称弹性函数.

4　说明性的例子

在这一部分,我们以构造 GF(5)上的 3 元旋转对称弹性函数为例,来说明本文中所给出的构造方法,通过对结果的比较说明,我们可以构造出文献[14]不能构造的旋转对称弹性函数.

假设 $q=3$,$p=5$,那么有限域 GF$(5)^3$ 中所含有的向量的个数为 125,其中 5 个短轨道为$\{\boldsymbol{e}_{3,0}\}$,$\{\boldsymbol{e}_{3,1}\}$,$\{\boldsymbol{e}_{3,2}\}$,$\{\boldsymbol{e}_{3,3}\}$,$\{\boldsymbol{e}_{3,4}\}$,通过解如下的方程组 $i_0+i_1+i_2+i_3+i_4=3$,可以得到非负整数解的个数为 $C_{p+q-1}^{q}=35$,这些解对应着旋转对称轨道的型. 定义一个具有最大圈结构的变换 $\tau\in S_5$ 如下:$0\to\tau(0)=2\to\tau(2)=\tau^2(0)=3\to\tau(3)=\tau^3(0)=1\to\tau(1)=\tau^4(0)=4$.

显然$\{0,\tau(0),\tau^2(0),\tau^3(0),\tau^4(0)\}=$GF($p$)=GF(5),则循环群$\{\tau^k\mid 0\le k\le p-1\}$在上述方程组的解构成的集合上作用形成的其中一个轨道为:

$$\Delta_0=\{(3,0,0,0,0),(0,3,0,0,0),(0,0,3,0,0),(0,0,0,3,0),(0,0,0,0,3)\},$$

其中的向量依次对应着短轨道$\{\boldsymbol{e}_{3,0}\}$,$\{\boldsymbol{e}_{3,1}\}$,$\{\boldsymbol{e}_{3,2}\}$,$\{\boldsymbol{e}_{3,3}\}$,$\{\boldsymbol{e}_{3,4}\}$. 下面我们只考虑上述方程的那些可以作为 3 元长旋转对称轨道的型的解,解的总个数为 $C_{p+q-1}^{q}-p=30$ 个,它们在循环群$\{\tau^k\mid 0\le k\le p-1\}$作用下形成的轨道分别为:

$$\Delta_1=\{(0,0,1,1,1),(1,1,1,0,0),(1,0,0,1,1),(0,1,1,0,1),(1,1,0,1,0)\};$$

$$\Delta_2=\{(0,1,1,1,0),(1,0,1,1,0),(1,0,1,0,1),(1,1,0,0,1),(0,1,0,1,1)\};$$

$$\Delta_3=\{(0,0,0,2,1),(0,1,2,0,0),(2,0,0,1,0),$$

$$(0,0,1,0,2),(1,2,0,0,0,)\};$$
$$\Delta_4=\{(0,0,2,1,0),(2,0,1,0,0),(1,0,0,0,2),$$
$$(0,2,0,0,1),(0,1,0,2,0)\};$$
$$\Delta_5=\{(0,2,1,0,0),(1,0,0,2,0),(0,0,2,0,1),$$
$$(2,1,0,0,0),(0,0,0,1,2)\};$$
$$\Delta_6=\{(0,2,0,1,0),(0,0,1,2,0),(1,0,2,0,0),$$
$$(2,0,0,0,1),(0,1,0,0,2)\}.$$

由定理2,注意到以 Δ_1 中的向量作为型的旋转对称轨道的个数为 $n_{k_1}=(3-1)!/(0!\ 0!\ 1!\ 1!\ 1!)=2$,故对于轨道 Δ_1 中的每一个型(向量),分别选一个其中的型(向量)对应的旋转对称轨道,由定理2可知,所选出的这5个旋转对称轨道刚好构成一个正交表OA(15,3,5,1),重复上面的做法直到 Δ_1 中所有的向量对应的旋转对称轨道都组合成正交表OA(15,3,5,1),这样共可以得到 $n_{k_1}=2$ 个,分别记为 $\boldsymbol{M}_{1,1}$ 和 $\boldsymbol{M}_{1,2}$;

类似地,按照定理2的方法,注意到以 Δ_2 中的向量作为型的旋转对称轨道的个数为:

$$n_{k_2}=(3-1)!/(0!\ 1!\ 1!\ 1!\ 0!)=2$$

故对于轨道 Δ_2 中的每一个型(向量),分别选一个其中的型(向量)对应的旋转对称轨道,由定理2可知,所选出的这5个旋转对称轨道刚好构成一个正交表OA(15,3,5,1),重复上面的做法直到 Δ_2 中所有向量对应的旋转对称轨道都组合成正交表OA(15,3,5,1),这样共可以得到 $n_{k_2}=2$ 个,分别记为 $\boldsymbol{M}_{2,1}$ 和 $\boldsymbol{M}_{2,2}$;

类似地,对于 $\Delta_3,\Delta_4,\Delta_5$ 和 Δ_6,按照上述相同的方法可得 $n_{k_3}=n_{k_4}=n_{k_5}=n_{k_6}=1$,即分别可以得到一个正交表OA(15,3,5,1),依次记为 $\boldsymbol{M}_3,\boldsymbol{M}_4,\boldsymbol{M}_5$ 和 $\boldsymbol{M}_6$,这样我们一共得到了8个OA(15,3,5,1).

下面要从上面得到的8个OA(15,3,5,1)中寻找 r 个OA(15,3,5,1),将它们中的旋转对称轨道按照定理3的方法构造出5个OA(10,3,5,1),r 满足:

$$K=(p^{q-1}-1)/q=p\cdot g+r,1\leq r\leq p-1,g\geq 0,$$

将 $p=5,q=3$ 代入上式计算可得 $r=3,g=1$,这个结果意味着需从上面得到的8个正交表OA(15,3,5,1)中寻找3个正交表OA(15,3,5,1),使得这3个正交表中所含有的旋转对称轨道中的型满足定理3中的方程组.首先可计算

$$w=(r\cdot q+1)/p=p^{q-2}-q\cdot g=2$$

从而在本例中,定理3对应的方程组具体为:

$$(1)\begin{cases}(1,1,1)\begin{pmatrix}x_{1,0}&x_{1,1}&x_{1,2}&x_{1,3}&x_{1,4}\\x_{2,0}&x_{2,1}&x_{2,2}&x_{2,3}&x_{2,4}\\x_{3,0}&x_{3,1}&x_{3,2}&x_{3,3}&x_{3,4}\end{pmatrix}=(1,2,2,2,2)\\ \begin{pmatrix}x_{1,0}&x_{1,1}&x_{1,2}&x_{1,3}&x_{1,4}\\x_{2,0}&x_{2,1}&x_{2,2}&x_{2,3}&x_{2,4}\\x_{3,0}&x_{3,1}&x_{3,2}&x_{3,3}&x_{3,4}\end{pmatrix}\begin{pmatrix}1\\1\\1\\1\\1\end{pmatrix}=\begin{pmatrix}3\\3\\3\end{pmatrix}\end{cases}$$

容易得到上述方程组的一个解为:

$$\begin{pmatrix}x_{1,0}&x_{1,1}&x_{1,2}&x_{1,3}&x_{1,4}\\x_{2,0}&x_{2,1}&x_{2,2}&x_{2,3}&x_{2,4}\\x_{3,0}&x_{3,1}&x_{3,2}&x_{3,3}&x_{3,4}\end{pmatrix}=\begin{pmatrix}0&0&1&1&1\\1&0&0&1&1\\0&2&1&0&0\end{pmatrix}.$$

注意到 $(0,0,1,1,1)\in\Delta_1,(1,0,0,1,1)\in\Delta_1,(0,2,1,0,0)\in\Delta_5$,这个结果表明我们需要选出 $\boldsymbol{M}_{1,1}$ 和 $\boldsymbol{M}_{1,2}$,以及 $\boldsymbol{M}_5$ 这三个正交表OA(15,3,5,1),将它们重新拆成单个的旋转对称轨道,然后按照定理3证明中的构造方法可得5个OA(10,3,5,1)如下:

$$\boldsymbol{B}_0=\begin{pmatrix}0&0&0\\2&3&4\\3&4&2\\4&2&3\\0&3&4\\3&4&0\\4&0&3\\1&1&2\\1&2&1\\2&1&1\end{pmatrix},\boldsymbol{B}_1=\begin{pmatrix}1&1&1\\0&4&3\\4&3&0\\3&0&4\\0&1&3\\1&3&0\\3&0&1\\2&2&4\\2&4&2\\4&2&2\end{pmatrix},\boldsymbol{B}_2=\begin{pmatrix}2&2&2\\0&3&1\\3&1&0\\1&0&3\\2&1&0\\1&0&2\\0&2&1\\3&4&4\\4&4&3\\4&3&4\end{pmatrix},$$

$$\boldsymbol{B}_3=\begin{pmatrix}3&3&3\\2&1&4\\1&4&2\\4&2&1\\3&2&4\\2&4&3\\4&3&2\\0&0&1\\0&1&0\\1&0&0\end{pmatrix},\boldsymbol{B}_4=\begin{pmatrix}4&4&4\\0&1&2\\1&2&0\\2&0&1\\1&2&4\\2&4&1\\4&1&2\\0&3&3\\3&3&0\\3&0&3\end{pmatrix}.$$

构造函数 $f(x)$:GF(5)$^3\to$GF(5)如下:$f^{-1}(0)=\boldsymbol{M}_{2,1}\cup\boldsymbol{B}_0,f^{-1}(1)=\boldsymbol{M}_{2,2}\cup\boldsymbol{B}_1,f^{-1}(2)=\boldsymbol{M}_3\cup\boldsymbol{B}_2,f^{-1}(3)=\boldsymbol{M}_4\cup\boldsymbol{B}_3,f^{-1}(4)=\boldsymbol{M}_6\cup\boldsymbol{B}_4$. 显然,$\{f^{-1}(0),f^{-1}(1),f^{-1}(2),f^{-1}(3),f^{-1}(4)\}$ 构成GF(5)^3 的一个分划,且 $f^{-1}(0),f^{-1}(1),f^{-1}(2),f^{-1}(3)$ 以及 $f^{-1}(4)$ 均为OA(25,3,5,1),从而 $\{f^{-1}(0),f^{-1}(1),f^{-1}(2),f^{-1}(3),f^{-1}(4)\}$ 构成了一个强度为1的正交表大集,因而 $f(x)$ 是一个GF(5)上的3元旋转对称1-弹性函数.

下面我们说明上述的函数 $f(x)$,是不能由文献[14]中的方法构造出来的.

注意到 $f^{-1}(4)=\boldsymbol{M}_6\cup\boldsymbol{B}_4$,我们可以给出 $f^{-1}(4)$ 中所含有的长旋转对称轨道的型构成的集合为 $\Delta_6\cup\{(0,0,1,1,1),(1,0,0,1,1),(0,2,1,0,0)\}$,稍加检验就可知它不包含它其中的任意一个向量在循环群 $\{\boldsymbol{\rho}_5^i\mid 0\leq i\leq 4\}$ 作用下形成的整个轨道.

而另外一方面,如果按照文献[14]中的方法构造

GF(5)^3→GF(5)的旋转对称弹性函 $g(x)$,对于循环群$\{\rho_3^i \mid 0 \le i \le 2\}$在 GF(5)^3 上作用形成的旋转对称轨道,$g(x)$在每一个旋转对称轨道上所取的函数值相等. 将循环群$\{\rho_5^l \mid 0 \le l \le 4\}$作用在方程 $i_0+i_1+i_2+i_3+i_4=3$ 的非负整数解构成的集合上得到7个轨道,显然对于任意的 $g^{-1}(l)$,这里 $0 \le l \le 4$,都有某一个型(i_0,i_1,i_2. i_3,i_4)存在,使得 $g^{-1}(l)$中同时含有型分别为 $\rho_5^l(i_0,i_1,i_2.i_3,i_4)$的5个旋转对称轨道,它们刚好构成一个 OA(15,3,5,1),以上分析比较可知本文方法能构造出新函数.

5　结论

本文中说明性的例子中由于 $\boldsymbol{M}_{2,1}$,$\boldsymbol{M}_{2,2}$,$\boldsymbol{M}_3$,$\boldsymbol{M}_4$ 以及 $\boldsymbol{M}_6$ 在构造弹性函数时的作用相同,但是它们分别取不同的函数值. 类似地,$\boldsymbol{B}_0$,$\boldsymbol{B}_1$,$\boldsymbol{B}_2$,$\boldsymbol{B}_3$,$\boldsymbol{B}_4$ 所取的函数值也分别不同,因而本文的方法可以构造出文献[14]中不能构造出来的函数,实际上由推论1可知,本文方法是文献[14]中方法的进一步推广,并且本文中的方法能构造出更多的旋转对称弹性函数. 但是,如何对构造出的新函数个数进行计数是一个有意义的工作,这也是我们未来工作的方向.

参考文献

[1] Du Jiao, Wen Qiaoyan, Zhang Jie, Pang Shanqi. Constructions of resilient rotation symmetric Boolean functions on given number of variables[J]. IET Information Security, 2014,8(5):265 – 272.

[2] Du Jiao, Pang Shanqi, Wen Qiaoyan, Liao Xin. Construction and count of 1-resilient rotation symmetric Boolean functions on p^r variables[J]. Chinese Journal of Electronics, 2014,23(4):816 – 820.

[3] Pang Shanqi, Xu Wenju, Du Jiao, Wang Ying. Construction and count of 1-resilient rotation symmetric Boolean functions on $4p$ variables[J]. Chinese Journal of Electronics, 2017,26(6):1276 – 1283.

[4] 张卫国,李路阳. 流密码中的布尔函数设计研究进展[J]. 河南师范大学学报(自然科学版),2017,45(3):24 – 33.
Zhang Weiguo, Li Luyang. Constructions of cryptographic Boolean functions in stream ciphers[J]. Journal of Henan Normal University(Natural Science Edition),2017,45(3):24 – 33. (in Chinese)

[5] Stanica, P, Maitra, S. A constructive count of rotation symmetric functions[J]. Information Processing Letters, 2003, 88:299 – 304.

[6] Li Yuan, Cusick T W. Linear structures of symmetric functions over finite fields[J]. Information Processing Letters, 2006,97:124 – 127.

[7] Cusick T W, Li Yuan, Stanica P. Balanced symmetric functions over GF(p)[J]. IEEE Transactions on Information Theory, 2008,54(3):1304 – 1307.

[8] Ke Pinhui, Huang Liuling, Zhang Shenyuan. Improved lower bound on the number of balanced symmetric functions over GF(p)[J]. Information Sciences, 2009, 179: 682 – 687.

[9] Fu Shaojing, LI Chao, QU Longjiang, et al. Enumeration of balanced symmetric functions over GF(p)[J]. Information Processing Letters, 2010,110:544 – 548.

[10] Li Yuan. Results on rotation symmetric polynomials over GF(p)[J]. Information Science, 2008,178:280 – 286.

[11] Fu Shaojing, Li Chao, Qu Longjiang, Dong Deshuai. On the number of rotation symmetric functions over GF(p)[J]. Mathematical and Computer Modelling, 2012,55(1 – 2):142 – 150.

[12] 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 Xuxu, Zhao Xianhe. 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. (in Chinese)

[13] 杜蛟,庞善起,温巧燕,张劼. GF(p)上 q 元旋转对称弹性函数的一个等价刻画[J]. 通信学报,2014,35(8):179 – 183.
Du Jiao, Pang Shanqi, Wen Qiaoyan, Zhang Jie. Euivalent characterization of resilient rotation symmetric functions with q number of variables over GF(p)[J]. Journal on Communications, 2014,35(8):179 – 183. (in Chinese)

[14] Du Jiao, Fu Shaojing, Qu Longjiang, Li Chao, Pang Shanqi. New constructions of q-variable 1-resilient rotation symmetric functions over F_p[J]. Science China Information Science, 2016,59(7),079102:1 – 3.

[15] Du Jiao, Li Chao, Fu Shaojing, Pang Shanqi. Constructions of p-variable 1-resilient rotation symmetric functions over GF(p)[J]. Security and Communication Networks, 2016, 9,(18):5651 – 5658.

[16] Gopalakrishnan K, Stinson D R. Three characterizations of non-binary correlation-immune and resilient functions[J]. Designs, Codes and Cryptography, 1995,5:241 – 251.

[17] 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.

作者简介

杜 蛟 男,1978 年生于湖北省英山县,河南师范大学数学与信息科学学院讲师,博士,研究方向为对称密码学.
E-mail:jiaodudj@126.com.

刘春红 女,1969 年生于河南省新乡市,河南师范大学计算机与信息工程学院副教授,硕士生导师,研究方向为云计算安全、云计算与虚拟化技术、机器学习.
E-mail:lch@htu.edu.cn

张 恩 男,1974 年生于河南省新乡市,河南师范大学计算机与信息工程学院副教授,硕士生导师,研究方向为密码协议与云计算安全.

尚玉婧 女,1993 年生于河南省卫辉市,河南师范大学数学与信息科学学院硕士研究生,主要研究方向为密码学.

董 乐 男,1980 年生于河南省封丘县,河南师范大学数学与信息科学学院副教授,硕士生导师,主要研究方向为对称密码的设计与分析.
E-mail:dongle127@163.com