doi:10.3969/j.issn.1000-436x.2013.03.002

# 素数元旋转对称弹性布尔函数的构造与计数

杜皎[1,2]，温巧燕[1]，张劼[3]，庞善起[4]

（1. 北京邮电大学 网络与交换技术国家重点实验室，北京 100876；2. 新乡学院 数学与信息科学系，河南 新乡 453003；
3. 北京邮电大学 理学院，北京 100876；4. 河南师范大学 数学与信息科学学院，河南 新乡 453007）

**摘 要**：通过对素数元旋转对称弹性布尔函数特征矩阵的研究，给出了其特征矩阵的若干性质，得到了素数元旋转对称布尔函数为弹性函数的一个充要条件，由此完全决定了旋转对称弹性函数的构造以及这类函数的精确计数公式，最后还给出了所有的三元、五元、七元旋转对称弹性布尔函数的构造方案与精确计数。

**关键词**：布尔函数；特征矩阵；相关免疫；代数免疫

**中图分类号**：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2013)03-0006-08

# Construction and count of resilient rotation symmetric Boolean functions with prime number variables

DU Jiao[1,2], WEN Qiao-yan[1], ZHANG Jie[3], PANG Shan-qi[4]

(1. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Department of Mathematics and Information Science, Xinxiang University, Xinxiang 453003, China;
3. School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China;
4. College of Mathematics and Information Science, Henan Normal University, Xinxiang 453007, China)

**Abstract:** The characteristic matrix of the resilient rotation symmetric Boolean functions (RSBF) with prime number variables were explored. Some properties about character ic matrix of them were given. A necessary and sufficient condition on the construction of resilient RSBF with prime number variables was derived. So construction and count formula of all the resilient RSBF with prime number variables were determined by this way. At last, all the resilient RSBF with 3, 5 or 7 variables were given.

**Key words:** Boolean functions; characteristic matrix; correlation immune; algebraic immunity

## 1 引言

在流密码和分组密码的密码系统中，所选用的布尔函数必须满足各种不同的要求，以抵抗各种已有的攻击方法，如 1984 年 Siegenthaler 提出的相关攻击[1]，要求选用的布尔函数具有相关免疫性和平衡性[1,2]（弹性）。2003 年，法国的密码学家 Nicolas 和 Wilimeier 提出了基于线性反馈移位寄存器的代数攻击方法[3]，对密码学中使用的布尔函数提出了更高的要求。近年来，代数攻击引起了密码学家们的广泛关注[4~8]。为了衡量布尔函数抵抗代数攻击的能力，Meier 等人提出了代数免疫(AI, algebraic immunity)的概念[3]，由于代数免疫阶高的函数同时具有较高的代数次数和非线性度，因此，如何构造同时具有最优代数免疫性和弹性的布尔函数既是布尔函数研究领域的一个极具重要研究意义的课

收稿日期：2011-12-29；修回日期：2012-05-10
基金项目：国家自然科学基金资助项目(61272057, 61202434, 61170270, 61100203, 61003286, 61121061, 11171093)；中央高校基本科研业务费专项基金资助项目(BUPT2011YB01, BUPT2011RC0505, 2011PTB-00-29, 2011RCZJ15,2012RC0612)；河南省教育厅自然科学研究计划基金资助项目(2011B110010)；2010 年新乡学院科技创新基金资助项目
**Foundation Items:** The National Natural Science Foundation of China (61272057, 61202434, 61170270, 61100203, 61003286, 61121061, 11171093); The Fundamental Research Funds for the Central Universities (BUPT2011YB01, BUPT2011RC0505, 2011PTB-00-29, 2011RCZJ15, 2012RC0612); The Natural Science Research Program of the Education Department of Henan Province (2011B110010); The Science and Technology Innovat ion of Xinxiang University 2010

题，也是当前密码函数研究的热点问题。到目前为止，关于偶数元具有最优代数免疫阶的布尔函数的构造已经出现了很多研究成果[9,10]，然而关于同时具有弹性和最优代数免疫性的奇数元布尔函数的构造问题的结果至今仍然很少，一个重要的原因是到现在为止，还没有找到一个很有效的数学工具可以用来同时研究一个布尔函数的代数免疫性和弹性。

1999 年，Pieprzyk 和 Qu 将旋转对称函数（RSBF）用于某些密码算法如 MD4、MD5 和 HAVAL 的快速实现中[11]，RSBF 一经提出就引起了密码学界的广泛关注[12~16]，近年来，关于具有最优代数免疫性或其他性质的旋转对称函数的构造已经出现了许多有价值的结果[15~18]，它是一类较对称布尔函数更大的函数类，对称布尔函数可以看成是一类特殊的旋转对称布尔函数，人们运用计算机搜索的方法发现了 12 个同时具有 2 阶弹性和最优代数免疫性的七元旋转对称布尔函数[7]，这就启示笔者从旋转对称布尔函数类中去寻找同时具有弹性和最优代数免疫性的奇数元布尔函数，为了缩小搜索空间，笔者有 2 个思路：1）从已经得到的最优代数免疫的 RSBF 中去寻找弹性函数；2）从已经得到的具有弹性的 RSBF 类中去寻找最优代数免疫函数。如果从 1）的角度考虑去获得具有弹性的最优代数免疫函数，那么最优代数免疫的 RSBF 具有弹性时的性质刻画就尤为重要；如果从 2）的角度考虑去获得具有弹性的最优代数免疫函数，那么具有弹性的 RSBF 的构造与计数就是一个极有意义的研究课题，本文主要对素数元 RSBF 类具有弹性时其特征矩阵的性质进行了刻画，并且研究了素数元旋转对称的弹性布尔函数的构造与计数问题。关于 RSBF 的构造与计数已经有了一些结果[17,18]，但它们都不是弹性的，具有弹性的 RSBF 的构造与计数这一问题的解决将有效地缩小笔者搜索具有弹性最优代数免疫的 RSBF 空间范围。

## 2　基础知识

令 $\boldsymbol{F}_2^n$ 是二元域 $F_2$ 上的 $n$ 维向量空间，$B_n$ 表示所有的 $n$ 元布尔函数的集合，符号 $|A|$ 表示集合 $A$ 中元素的个数，$x=(x_1,x_2,\mathrm{L},x_n)\in \boldsymbol{F}_2^n$，定义旋转变换 $r_n^k\ (1\le k\le n)$ 如下。

$$r_n^k(x_1,x_2,\mathrm{L},x_n)=(r_n^k(x_1),r_n^k(x_2),\mathrm{L},r_n^k(x_n))$$

其中，$r_n^k(x_i)=\begin{cases}x_{i+k}, i+k\le n\\ x_{i+k-n}, i+k>n\end{cases}$。当 $i>n$ 时，约定 $x_i=x_{i_0}$，$i_0$ 满足 $i\equiv i_0(\mathrm{mod}\,n)$，$1\le i_0\le n$。对于 $x=(x_1,x_2,\mathrm{L},x_n)\in \boldsymbol{F}_2^n$，称 $G_n(x)=\{r_n^k(x)\,|1\le k\le n\}$ 为向量 $x$ 在变换 $r_n^k\ (1\le k\le n)$ 下生成的轨道，称 $|G_n(x)|$ 为轨道的长度。

任何布尔函数 $f(x)\in B_n$，都可以唯一地表示为如下的代数标准型（ANF）。

$$f(x_1,x_2,\cdots,x_n)=a_0+\sum_{i=1}^{n}a_ix_i+\sum_{1\le i<j\le n}a_{ij}x_ix_j+$$

$$\cdots+a_{12\cdots n}x_1x_2\cdots x_n$$

其中，系数 $a_0,a_1,\cdots,a_{12\cdots n}\in F_2$，代数标准型中最高次项的次数称为 $f(x)$ 的次数，记为 $\deg(f(x))$。

**定义 1**[11]　布尔函数 $f(x)$ 称为旋转对称布尔函数（RSBF），当且仅当对于任意的输入 $(x_1,x_2,\cdots,x_n)\in \boldsymbol{F}_2^n$，$f(r_n^k(x_1,x_2,\cdots,x_n))=f(x_1,x_2,\cdots,x_n)$ 对 $0\le k\le n-1$ 成立。

下文中，用 RSBF 表示旋转对称布尔函数的缩写，用 $G_n(x)$ 表示向量 $x$ 在变换 $r_n^k$ 下生成的轨道，即 $G_n(x)=\{r_n^k(x_1,x_2,\mathrm{L},x_n)|1\le k\le n\}$，$n$ 元 RSBF 的轨道个数为 $g_n=\frac{1}{n}\sum_{k|n}f(k)\cdot 2^{n/k}$，其中，$f$ 为欧拉函数，因而 $n$ 元 RSBF 的总个数为 $2^{g_n}$。将每个轨道 $G_n(x)$ 中的元素按照字典排列法排序，将排在第一位的所有向量按照重量大小以及字典排列法依次记为 $\boldsymbol{L}_{n,w}^i$，其中，$w$ 表示轨道中向量的重量，$i$ 表示重量为 $w$ 的轨道中的第 $i$ 个轨道，$g_{n,w}$ 表示重量为 $w$ 的轨道总数，则所有重量为 $w$ 的轨道可以表示为 $G_n(\boldsymbol{L}_{n,w}^i)$，$1\le i\le g_{n,w}$。注意到两元平衡的相关免疫旋转对称布尔函数只有 2 个，即 $f_1(x_1,x_2)=x_1+x_2$ 和 $f_2(x_1,x_2)=1+x_1+x_2$，下文中，只考虑当 $p$ 满足 $p\ge 3$ 的素数时的情形。

**定义 2**[19]　设 $f(x)$ 是一个 $n$ 元布尔函数，$x\in \boldsymbol{F}_2^n$，若 $f(x)=1$，则称 $x$ 为 $f(x)$ 的一个特征向量，记 $f(x)$ 的全体特征向量的集合为 $\boldsymbol{D}$，即：$\boldsymbol{D}=\{a\mid f(a)=1,a\in \boldsymbol{F}_2^n\}$，$|\boldsymbol{D}|=w$，其中，$w$ 表示函数 $f(x)$ 的 Hamming 重量，$\boldsymbol{D}$ 称为 $f(x)$ 的支撑集，将集合 $\boldsymbol{D}$ 中的向量按行排列，记第 $i$ 个向量 $\boldsymbol{w}_i=(c_{i1},c_{i2},\cdots,c_{in})$，$1\le i\le w$，则称如下的 0、1 矩阵

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

为 $f(x)$ 的特征矩阵，在不引起混淆的情况下简记为 $\boldsymbol{C}$。下文中不考虑特征矩阵的行置换。

布尔函数与特征矩阵是一一对应的，对布尔函数有关问题的研究等价于对布尔函数特征矩阵的研究，下文中把布尔函数的特征矩阵与该布尔函数均称为布尔函数。

**定义 3**[19] 设 $\boldsymbol{A}$ 是一个 $w$ 行 $n$ 列的矩阵，称 $\boldsymbol{A}$ 是一个 $(w,n,2,m)$ 正交矩阵是指 $\boldsymbol{A}$ 的任 $m$ 列构成矩阵的行向量中，$\boldsymbol{F}_2^m$ 中的每个向量都出现且出现的次数相同。

**定义 4**[19] 如果一个布尔函数 $f(x)$ 的特征矩阵 $\boldsymbol{C}_f$ 是一个 $(w,n,2,m)$ 正交矩阵，则称 $f(x)$ 是一个 $m$（$m\geq 1$）阶相关免疫函数，简称 $f(x)$ 是相关免疫函数或 $f(x)$ 是 CI 函数。

**定义 5**[3] 设 $f(x)$，$g(x)\in B_n$，若 $f(x)g(x)=0$，称 $g(x)$ 是 $f(x)$ 的零化子，$f(x)$ 的零化子集合记为 $AN(f)$，$f(x)$ 的代数免疫阶 $AI(f)$ 定义为

$$AI(f)=\{\min(\deg(g(x)))\,|\,g(x)\in AN(f)\cup AN(1+f)\}$$

当 $AI(f)$ 取得最大值 $\lceil n/2\rceil$ 时，则称 $f(x)$ 为最优代数免疫函数或 MAI 函数[4]。

**定义 6** 设 $f(x)$ 是一个 $n$ 元布尔函数，它可能满足如下的性质。

1) 平衡性：$n$ 元布尔函数 $f(x)$ 是平衡函数，即它的输出中 0 和 1 各半。

2) 相关免疫性：$n$ 元布尔函数 $f(x)$ 是 CI 函数，即它的特征矩阵是 $(w,n,2,m)$ 正交矩阵。

3) 旋转对称性：$n$ 元布尔函数 $f(x)$ 是 RSBF。

4) 最优代数免疫性：$n$ 元布尔函数 $f(x)$ 是 MAI 函数。

笔者称 $n$ 元布尔函数 $f(x)$ 是一个 $P(i_1,i_2,\cdots,i_t)$ 函数是指 $f(x)$ 同时满足上述的性质 1)~4)，$P(1,2)$ 函数即为弹性函数，下文中主要研究 $p$（$p$ 为素数）元 $P(1,2,3)$函数的构造问题，如未特别说明，均假设 $p$ 为奇素数。

## 3 主要结果

### 3.1 对 $p$ 元 $P(3)$、$P(2,3)$、$P(1,2,3)$函数特征矩阵性质的刻画

当旋转对称布尔函数 $f(x)$ 的变元个数 $n$ 为不小于 3 的奇素数 $p$ 时，其特征矩阵有什么特征呢？下面的定理给出了回答。

**定理 1** $p$ 元 RSBF $f(x)$ 的特征矩阵总可以写成如下的 4 种形式。

$$\boldsymbol{C}_{f_1}=\begin{pmatrix} \boldsymbol{0}_p \\ A_1 \\ \vdots \\ A_{k_1} \end{pmatrix}$$

$$\boldsymbol{C}_{f_2}=\begin{pmatrix} \boldsymbol{1}_p \\ B_1 \\ \vdots \\ B_{k_2} \end{pmatrix}$$

$$\boldsymbol{C}_{f_3}=\begin{pmatrix} \boldsymbol{0}_p \\ \boldsymbol{1}_p \\ C_1 \\ \vdots \\ C_{k_3} \end{pmatrix}$$

$$\boldsymbol{C}_{f_4}=\begin{pmatrix} D_1 \\ D_2 \\ \vdots \\ D_{k_4} \end{pmatrix}$$

其中，$\boldsymbol{0}_p=\underbrace{00\cdots0}_{p}$，$\boldsymbol{1}_p=\underbrace{11\cdots1}_{p}$，$\boldsymbol{A}_i$、$\boldsymbol{B}_j$、$\boldsymbol{C}_k$ 和 $\boldsymbol{D}_l$ 都是对称的 $p\times p$ 方阵，其中，$1\leq i\leq k_1$，$1\leq j\leq k_2$，$1\leq k\leq k_3$，$1\leq l\leq k_4$。

**证明** 由于 $p$ 是素数，空间 $\boldsymbol{F}_2^p$ 被分成了 $2\times\dfrac{2^{p-1}-1}{p}+2$ 个轨道，其中，$\boldsymbol{0}_p=\underbrace{00\cdots0}_{p}$ 和 $\boldsymbol{1}_p=\underbrace{11\cdots1}_{p}$ 是 2 个单元素轨道，其他的 $2\times\dfrac{2^{p-1}-1}{p}$ 个轨道中都含有 $p$ 个点。而每个轨道构成的特征矩阵形式为 $\boldsymbol{M}_0=\begin{pmatrix} x \\ r_p^1(x) \\ \vdots \\ r_p^{p-1}(x) \end{pmatrix}$，对于任意的 $x\notin\{\boldsymbol{0}_p,\boldsymbol{1}_p\}$，下面证 $\boldsymbol{M}_0$ 是一个 $p\times p$ 对称矩阵。设 $x=(x_1,x_2,\cdots,x_p)$，$\boldsymbol{M}_0$ 的第 $i$ 行第 $j$ 列的元素为 $m_{ij}$，第 $j$ 行第 $i$ 列的元素为 $m_{ji}$，这里 $1\leq i,j\leq p$，根据旋转对称变换 $r_n^k$ 的意义，可知 $m_{ij}=x_{i+j-1(\bmod p)}$，$m_{ji}=x_{j+i-1(\bmod p)}$，这就是说 $m_{ij}=m_{ji}$，根据对称矩阵的定义可知 $\boldsymbol{M}_0$ 是对称

的。因而 $f(x)$ 的特征矩阵总可以写成如上的 4 种形式之一。

因此，由定理 1 很快可以判断文献[20]中给出构造得到的 $P(2,3)$函数都不是 $P(1)$函数，因为它们所得的函数具有 $\boldsymbol{C}_{f_3}$ 或者 $\boldsymbol{C}_{f_4}$ 的形式。笔者有如下的推论。

**推论 1**　设 $f(x)$ 是一个 $p$ 元 $P(3)$函数（$p\geq 3$），其特征矩阵为 $\boldsymbol{C}_f$，则 $\boldsymbol{C}_f$ 的任意 2 列中 0 和 1 的个数相同。

**证明**　由定理 1 可知，若 $f(x)$ 是一个 $p$ 元 $P(3)$函数（$p\geq 3$），那么特征矩阵为 $\boldsymbol{C}_f$ 一定可以写成上述的 $\boldsymbol{C}_{f_1}$、$\boldsymbol{C}_{f_2}$、$\boldsymbol{C}_{f_3}$ 或 $\boldsymbol{C}_{f_4}$ 的形式，由于 $\boldsymbol{A}_i$，$\boldsymbol{B}_j$，$\boldsymbol{C}_k$，$\boldsymbol{D}_l$ 都具有对称矩阵 $\boldsymbol{M}_0$ 的形式，因而其行向量和列向量都有相同的重量，并且都是对称的 $p\times p$ 方阵，因而无论 $\boldsymbol{C}_f$ 是哪种形式，$\boldsymbol{C}_f$ 的任意 2 列中 0 和 1 的个数均相同。

文献[20]通过计算也得到了与推论 1 相同的结论，推论 1 刻画了 $p$ 元 $P(3)$函数特征矩阵的一个简单性质，由此还可得如下的推论。

**推论 2**　$p(p\geq 3)$元 $P(3)$函数 $f(x)$是一阶 $P(2)$函数，当且仅当它的特征矩阵的第一列中 0 和 1 的个数相等。

**证明**　一方面，若 $f(x)$ 是 $P(2)$函数，由一阶相关免疫函数的定义可知，它的第一列中 0 和 1 的个数相等。

另一方面，对于 $P(3)$函数 $f(x)$，如果它的特征矩阵的第一列中 0 和 1 的个数相等，由推论 1 可知，$\boldsymbol{C}_f$ 的任意 2 列中 0 和 1 的个数相同，那么它所有的列中 0 和 1 的个数相等，因而它是一阶 $P(2)$函数。

文献[21]研究了 $P(2)$函数阶的判别方法，由上述的推论 2 可知，要判断一个 $P(3)$函数是否是一阶的 $P(2)$函数，只需要判断它的第一列中 0 和 1 的个数是否相等即可。当 $f(x)$ 是 $P(1)$函数时，其特征矩阵又有什么性质呢?下面的定理对这一问题做了回答。

**定理 2**　$p$ 元旋转对称布尔函数 $f(x)$ 是平衡函数，那么 $f(x)$ 特征矩阵的形式一定是定理 1 中的 $\boldsymbol{C}_{f_1}$ 或者 $\boldsymbol{C}_{f_2}$ 的形式，并且 $k_1=k_2=\dfrac{2^{p-1}-1}{p}$，向量 $\mathbf{0}_p$ 和 $\mathbf{1}_p$ 有且仅有一个在 $f(x)$ 的支撑集中。

**证明**　$p$ 元旋转对称布尔函数 $f(x)$ 是平衡函数，那么 $f(x)$ 的支撑集中一定含有长度为 $p$ 的轨道 $\dfrac{2^{p-1}-1}{p}$ 个，因而向量 $\mathbf{0}_p$ 和 $\mathbf{1}_p$ 有且仅有一个在 $f(x)$ 的支撑集中才能保证 $f(x)$ 是平衡函数。也就是说平衡函数 $f(x)$ 的特征矩阵只能是 $\boldsymbol{C}_{f_1}$ 或者 $\boldsymbol{C}_{f_2}$ 的形式。

上述的定理 1、定理 2、推论 1 和推论 2 从不同的角度刻画了 $p$ 元 $P(3)$函数 $f(x)$ 特征矩阵的性质。

### 3.2　对文献[14,20]构造方法的改进

当变元个数 $n$ 为奇素数 $p$ 时，文献[14,20]给出了一类 $P(2,3)$函数的构造方法如下。

1) 对于任意给定的 $1\leq w\leq (n-1)/2$，从重量为 $w$ 的轨道 $G_n(L^{\,i}_{n,w})$（$1\leq i\leq g_{n,w}$）中取出任意的 $k$ 个（$0\leq k\leq g_{n,w}$）轨道作为矩阵 $\boldsymbol{C}_f$ 的行向量。

2) 从重量为 $n-w$ 的轨道 $G_n(L^{\,i}_{n,n-w})$（$1\leq i\leq g_{n,n-w}$）中也取出任意的 $k$ 个轨道作为矩阵 $\boldsymbol{C}_f$ 的行向量。

文献[20]中还给出了上述方法构造得到的 $P(2,3)$函数的准确计数为

$$2\prod_{w=1}^{(n-1)/2}\left(\sum_{k=0}^{g_{n,w}}\binom{g_{n,w}}{k}\binom{g_{n,n-w}}{k}\right)=2\prod_{w=1}^{(n-1)/2}\left(\sum_{k=0}^{g_{n,w}}\binom{g_{n,w}}{k}^2\right)$$

其中，符号 $\binom{a}{b}$ 表示从 $a$ 个中任选 $b$ 个的组合数，下文同。由这个结果可得：当 $n$ 为奇素数 $p$ 时，$P(2,3)$函数的一个计数下界。下面笔者进一步给出一种新的 $p$ 元 $P(2,3)$函数的构造。

假设重量依次为 $w_1$、$w_4$、$n-w_2$、$n-w_3$ 的轨道 $G_n(L^{\,i}_{n,w_1})$、$G_n(L^{\,j}_{n,w_4})$、$G_n(L^{\,s}_{n,n-w_2})$ 以及 $G_n(L^{\,t}_{n,n-w_3})$ 满足 $1\leq w_1<w_2<w_3<w_4\leq (n-1)/2$ 且 $w_1+w_4=w_2+w_3$，任取整数 $k$ 满足 $0\leq k\leq \min\{g_{n,w_1},g_{n,n-w_2},g_{n,n-w_3},g_{n,w_4}\}$，按照如下的方法构造函数。

1) 从轨道 $G_n(L^{\,i}_{n,w_1})$（$1\leq i\leq g_{n,w_1}$）中取出任意的 $k$ 个（$0\leq k\leq g_{n,w_1}$）重量为 $w_1$ 的轨道作为矩阵 $\boldsymbol{C}_f$ 的行向量。

2) 从轨道 $G_n(L^{\,j}_{n,w_4})$（$1\leq j\leq g_{n,w_4}$）中取出任意的 $k$ 个（$0\leq k\leq g_{n,w_4}$）重量为 $w_4$ 的轨道作为矩阵 $\boldsymbol{C}_f$ 的行向量。

3) 从轨道 $G_n(L^{\,s}_{n,n-w_2})$（$1\leq s\leq g_{n,n-w_2}$）中取出

任意的 $k$ 个（$0 \le k \le g_{n,n-w_2}$）重量为 $n-w_2$ 的轨道作为矩阵 $\boldsymbol{C}_f$ 的行向量。

4) 从轨道 $G_n(L^{\ t}_{n,n-w_3})$（$1 \le t \le g_{n,n-w_3}$）中取出任意的 $k$ 个（$0 \le k \le g_{n,n-w_3}$）重量为 $n-w_3$ 的轨道作为矩阵 $\boldsymbol{C}_f$ 的行向量。

5) 从轨道 $G_n(L^{\ u}_{n,w_0})$ 和 $G_n(L^{\ v}_{n,n-w_0})$（$1 \le u, v \le g_{n,w_0} = g_{n,n-w_0}$，$w_0 \notin \bigcup_{i=1}^{4}\{w_i, n-w_i\}$）中分别取出任意的 $l$ 个（$0 \le l \le g_{n,w_0}$）重量为 $w_0$ 和 $n-w_0$ 的轨道作为矩阵 $\boldsymbol{C}_f$ 的行向量。

对于任意的 $0 \le w \le n$，都有 $g_{n,w} = \begin{pmatrix} n \\ w \end{pmatrix} \Big/ n$，分别重复操作 1)~4）和 5)，以改变 $\boldsymbol{C}_f$ 行向量的个数，得到重量不同的函数。

**定理 3** 上述方法得到的函数是 $P(2,3)$函数。

**证明** 一方面，从 1)~5)可以看出，每次选出的都是整个轨道，因而上述方法构造的函数是 $P(3)$函数。

另一方面，考查上述的 1)~4)步选取的行向量构成的矩阵 $\boldsymbol{P}_1$，其行数为 $4kn$，其第一列中 1 的个数是 $kw_1 + kw_4 + k(n-w_2) + k(n-w_3) = 2kn$，考查 5)选取的行向量构成的矩阵 $\boldsymbol{Q}_1$，其行数为 $2ln$，其第一列中 1 的个数是 $lw_0 + l(n-w_0) = ln$，由推论 1 可知 $\boldsymbol{P}_1$ 和 $\boldsymbol{Q}_1$ 都是正交矩阵，若重复操作 1)~4)和 5)，分别得到若干个 $\boldsymbol{P}_i$ 和 $\boldsymbol{Q}_j$，类似地，它们都是正交矩阵，因而所有的 $\boldsymbol{P}_i$ 和 $\boldsymbol{Q}_j$（包括 $\boldsymbol{P}_1$ 和 $\boldsymbol{Q}_1$）一起构成的特征矩阵仍然是正交矩阵，由定义 4 可知，上述函数是 $P(2)$函数。

综上所述，上述方法得到的函数是 $P(2,3)$函数。

显然，当 1)~4)步得到的向量个数不为 0 时，上述方法构造得到的函数与文献[14,20]中构造的函数是不同的，当 1)~4)步得到的向量个数为 0 时，文献[14,20]的方法就是笔者方法的特例，实际上反复运用上述方法 1)~5)，笔者可以得到比文献[14,20]中方法更多的 $P(2,3)$函数。

### 3.3 $P(1,2,3)$函数的构造与精确计数

当 $P(3)$函数是 $P(2)$函数时，笔者对其特征矩阵的性质有了一个全面的认识，本节笔者讨论弹性的 RSBF 构造与计数问题。这一问题等价于从 $2\times\frac{2^{p-1}-1}{p}$ 个 $p$ 长轨道中选出 $\frac{2^{p-1}-1}{p}$ 个，加上向量 $\boldsymbol{0}_p$ 或 $\boldsymbol{1}_p$，构成一个 $2^{p-1}\cdot p$ 的矩阵，使得该矩阵的第一列中 0 和 1 的个数相等，下文中笔者都假设向量 $\boldsymbol{0}_p$ 在 $f(x)$ 的支撑集中，$\boldsymbol{1}_p$ 在 $1+f(x)$ 的支撑集中，下面笔者构造具有某些密码学性质的 $p$ 元 $P(3)$函数 $f(x)$，有如下的结果。

**定理 4** 设 $p$ 元 $P(3)$函数 $f(x)$ 的支撑集中重量为 $i$ 的轨道个数为 $n_i$ $(1 \le i \le p-1)$，那么 $f(x)$ 是 $P(1,2)$函数的充要条件是如下的方程组有解。

$$\begin{cases} \sum_{i=1}^{p-1} i n_i = 2^{p-2} \\ \sum_{i=1}^{p-1} n_i = (2^{p-1}-1)\Big/ p \end{cases} \tag{1}$$

其中，$0 \le n_i \le N_i = \begin{pmatrix} p \\ i \end{pmatrix} \Big/ p$，（$n_i$、$N_i \in N$）。

**证明** 先证必要性。

首先，若 $f(x)$ 是 $P(1)$函数，且 $\boldsymbol{0}_p$ 在 $f(x)$ 的支撑集中，而每个轨道都有 $p$ 个点，因而 $f(x)$ 的支撑集中还需要 $(2^{p-1}-1)\Big/ p$ 个 $p$ 长轨道，因而 $\sum_{i=1}^{p-1} n_i = (2^{p-1}-1)/p$ 成立；其次，要保证 $f(x)$ 是 $P(2)$函数，则由推论 1 可知它的第一列中 0 和 1 的个数相等，从而由定理 2 可知 $f(x)$ 的特征矩阵一定具有定理 2 中 $\boldsymbol{C}_{f_1}$ 的形式，并且对应的 $k_1 = \sum_{i=1}^{p-1} n_i$，因而它的第一列中 1 的总个数必为 $\sum_{i=1}^{p-1} i n_i = 2^{p-2}$，所以如果 $f(x)$ 是 $P(1,2)$函数，那么如下的方程组

$$\begin{cases} \sum_{i=1}^{p-1} i n_i = 2^{p-2} \\ \sum_{i=1}^{p-1} n_i = (2^{p-1}-1)\Big/ p \end{cases}$$

必然有解，其中，$0 \le n_i \le N_i = \begin{pmatrix} p \\ i \end{pmatrix} \Big/ p$，（$n_i$、$N_i \in N$）

再证充分性。

若方程组（1）成立，$\sum_{i=1}^{p-1} n_i = (2^{p-1}-1)\Big/ p$ 保证了函数 $f(x)$ 是 $P(1)$函数，条件 $\sum_{i=1}^{p-1} i n_i = 2^{p-2}$ 保证了 $f(x)$ 的特征矩阵的第一列中 1 的个数为 $2^{p-2}$，与 0

的个数相等，由推论 2 可知 $f(x)$ 是 $P(2)$函数，所以 $f(x)$ 是 $P(1,2)$函数。

**定理 5**　如果上述方程组(1)有 $q$ 组不同的解 $n_{1i}, n_{2i}, \cdots, n_{qi}$ $(1 \le i \le p-1)$，对于上述方程组的一组解 $n_{ji}$ （$1 \le i \le p-1$，$1 \le j \le q$），可以得到不同的 $p$ 元 $P(1,2,3)$函数 $f(x)$ 的个数为 $2T_j$，其中，$T_j = \prod_{i=1}^{p-1} \binom{N_i}{n_{ji}}$ 由 $q$ 组解得到不同的 $p$ 元 $P(1,2,3)$函数的总个数 $2T = 2\sum_{j=1}^{q} T_j$。

**证明**　一方面，对于方程组（1）的一组解 $n_{ji}$ $(1 \le i \le 6$，$1 \le j \le q)$，由于 $f(x)$ 是 $P(1,2)$函数，$n_{ji}$ 是指 $f(x)$ 的支撑集中重量为 $i$ 的轨道个数，而重量为 $i$ 的轨道总个数为 $N_i = \binom{p}{i} \Big/ p$，因而选择 $n_{ji}$ 个重量为 $i$ 的轨道（可以看成向量的集合）放入 $f(x)$ 的支撑集中的方法有 $\binom{N_i}{n_{ji}}$ 种，所以对于方程组（1）的一组解 $n_{ji}$ $(1 \le i \le 6$，$1 \le j \le q)$，可以得到的函数个数为 $T_j = \prod_{i=1}^{p-1} \binom{N_i}{n_{ji}}$ 个，这些函数的支撑集中都含有向量 $\mathbf{0}_p$，得到的这 $T_j$ 个函数是互不相同的，注意到当 $f(x)$ 是 $P(1,2,3)$函数，那么 $1+f(x)$ 也是 $P(1,2,3)$函数，因此得到的互不相同的 $P(1,2,3)$ 函数的总个数为 $2T_j$ $(1 \le j \le q)$。

另一方面，2 组不同的解 $n_{ji}$ 和 $n_{ki}$，这里 $1 \le j,k \le q$，$j \ne k$，至少存在某个 $i$ 满足 $n_{ji} \ne n_{ki}$，根据方程组（1）解的含义可知，在由解 $n_{ji}$ 和 $n_{ki}$ 所得到的函数的支撑集中，重量为 $i$ 的轨道数是不等的，因而由解 $n_{ji}$ 和 $n_{ki}$ 所得到的函数一定是不同的，所以由 $q$ 组解得到不同的 $p$ 元 $P(1,2,3)$函数的总个数为 $2T = 2\sum_{j=1}^{q} T_j$。

下面笔者给出几个通过求解方程组（1）来构造 $P(1,2,3)$函数的实例。

**推论 3**　有且仅有 2 个三元 $P(1,2,3)$函数。

**证明**　在方程组（1）中，令 $p$ =3，上述的方程组(1)简化为 $\begin{cases} 1n_1 + 2n_2 = 2 \\ n_1 + n_2 = 1 \end{cases}$，这里 $0 \le n_1, n_2 \le 1$，解这个方程组可得 $\begin{cases} n_1 = 0 \\ n_2 = 1 \end{cases}$，再由定理 5 可得：一共可得到 2 个三元 $P(1,2,3)$函数。

由文献[22]可知，这些函数都不是最优代数免疫函数，即不存在三元的 $P(1,2,3,4)$函数。

**推论 4**　有且仅有 10 个五元 $P(1,2,3)$函数。

**证明**　在方程组（1）中，令 $p$ =5，上述的方程组（1）简化为

$$\begin{cases} \sum_{i=1}^{4} i n_i = 8 \\ \sum_{i=1}^{4} n_i = 3 \end{cases}, \quad 0 \le n_1, n_4 \le 1, \quad 0 \le n_2, n_3 \le 2$$

解这个方程组可得如下的几组解：1) $n_1$ =0，$n_2$ =1，$n_3$ =2，$n_4$ =0；2) $n_1$ =0，$n_2$ =2，$n_3$ =0，$n_4$ =1；3) $n_1$ =1，$n_2$ =0，$n_3$ =1，$n_4$ =1。

再根据定理 5，对于第 1 组解可得函数 4 个，对于第 2 组解可得函数 2 个，对于第 3 组解可得函数 4 个，因而一共可以得到 10 个五元平衡的相关免疫旋转对称布尔函数。

**推论 5**　有且仅有 13 394 个七元 $P(1,2,3)$函数。

**证明**　类似地，对于七元平衡的相关免疫旋转对称布尔函数，可以按照如下的方式获得：在方程组（1）中，令 $p$ =7，方程组（1）简化为

$$\begin{cases} \sum_{i=1}^{6} i n_i = 32 \\ \sum_{i=1}^{6} n_i = 9 \end{cases}, \quad \begin{matrix} 0 \le n_1, n_6 \le 1, 0 \le n_2, n_5 \le 3, \\ 0 \le n_3, n_4 \le 5 \end{matrix}$$

解这个方程组可得如表 1 的 34 组不同的解，根据定理 5 计算得到的函数总数为 13 394 个，所得到的函数个数情况（函数个数共计 6 697）如表 1 所示。

可以证明存在 8 个五元弹性阶为 1 的 $P(1,2,3,4)$函数，计算机搜索实验表明[7]：在七元 $P(1,2,3)$函数中，存在 12 个代数次数为 4，弹性阶为 2，非线性度为 56 的 $P(1,2,3,4)$函数，文献[22]的研究结果表明：$n$（$n$ 为奇数）元最优代数免疫函数的弹性阶最大为 $(n-3)/2$，笔者比较关注达到弹性阶上界的这类最优代数免疫函数，实际上它们的代数次数就等于它的代数免疫阶，因而有如下的猜想。

**猜想**　对于奇素数 $n$ $(n \ge 5)$，弹性阶为 $(n-3)/2$ 的 $P(1,2,3,4)$ 函数存在。进一步地，$n$ $(n \ge 5)$ 为奇数时，弹性阶为 $(n-3)/2$ 的 $P(1,2,3,4)$ 函数存在。

表 1 34 组解以及每组解所得到的 $P(1,2,3)$函数的个数

| 组号 | $n_1$ | $n_2$ | $n_3$ | $n_4$ | $n_5$ | $n_6$ | 函数个数 $T_j$ |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 4 | 5 | 0 | 0 | 5 |
| 2 | 0 | 0 | 5 | 3 | 1 | 0 | 30 |
| 3 | 0 | 1 | 3 | 4 | 1 | 0 | 450 |
| 4 | 0 | 1 | 4 | 2 | 2 | 0 | 450 |
| 5 | 0 | 1 | 4 | 3 | 0 | 1 | 150 |
| 6 | 0 | 1 | 5 | 0 | 3 | 0 | 3 |
| 7 | 0 | 1 | 5 | 1 | 1 | 1 | 45 |
| 8 | 0 | 2 | 1 | 5 | 1 | 0 | 45 |
| 9 | 0 | 2 | 2 | 3 | 2 | 0 | 900 |
| 10 | 0 | 2 | 2 | 4 | 0 | 1 | 150 |
| 11 | 0 | 2 | 3 | 1 | 3 | 0 | 150 |
| 12 | 0 | 2 | 3 | 2 | 1 | 1 | 900 |
| 13 | 0 | 2 | 4 | 0 | 2 | 1 | 45 |
| 14 | 0 | 3 | 0 | 4 | 2 | 0 | 15 |
| 15 | 0 | 3 | 0 | 5 | 0 | 1 | 1 |
| 16 | 0 | 3 | 1 | 2 | 3 | 0 | 50 |
| 17 | 0 | 3 | 1 | 3 | 1 | 1 | 150 |
| 18 | 0 | 3 | 2 | 1 | 2 | 1 | 150 |
| 19 | 1 | 0 | 2 | 5 | 1 | 0 | 30 |
| 20 | 1 | 0 | 3 | 3 | 2 | 0 | 300 |
| 21 | 1 | 0 | 3 | 4 | 0 | 1 | 50 |
| 22 | 1 | 0 | 4 | 1 | 3 | 0 | 25 |
| 23 | 1 | 0 | 4 | 2 | 1 | 1 | 150 |
| 24 | 1 | 0 | 5 | 0 | 2 | 1 | 3 |
| 25 | 1 | 1 | 1 | 4 | 2 | 0 | 225 |
| 26 | 1 | 1 | 1 | 5 | 0 | 1 | 15 |
| 27 | 1 | 1 | 2 | 2 | 3 | 0 | 300 |
| 28 | 1 | 1 | 2 | 3 | 1 | 1 | 900 |
| 29 | 1 | 1 | 3 | 1 | 2 | 1 | 450 |
| 30 | 1 | 2 | 0 | 3 | 3 | 0 | 30 |
| 31 | 1 | 2 | 0 | 4 | 1 | 1 | 45 |
| 32 | 1 | 2 | 1 | 2 | 2 | 1 | 450 |
| 33 | 1 | 2 | 2 | 0 | 3 | 1 | 30 |
| 34 | 1 | 3 | 0 | 1 | 3 | 1 | 5 |

如表 1 所示，第一列表示解的序号，$n_i$ $(1 \le i \le 6)$所在的列表示的是$n_i$的取值；“函数个数”所在的列表示的是根据这一组解得到的支撑集中含有$\mathbf{0}_p = 0\underbrace{0\cdots0}_{p}$ ( $p=7$ )的函数个数，例如：在表 1 的第一行中，组号 1 表示的是第一组解，1 右边 $n_i$ $(1 \le i \le 6)$ 下边的数值就是第一组解 $n_1$ =0，$n_2$ =0，$n_3$ =4，$n_4$ =5，$n_5$ =0，$n_6$ =0；在这组解中：$n_1$ =0 的意义是重量为 1 的轨道选取 0 个，$n_2$ =0 的意义是重量为 2 的轨道选取 0 个，$n_3$ =4 的意义是重量为 3 的轨道选取 4 个（重量为 3 的轨道一共有 5 个），$n_4$ =5 的意义是重量为 4 的轨道选取 5 个（重量为 4 的轨道一共有 5 个），$n_5$ =0 的意义是重量为 5 的轨道选取 0 个，$n_6$ =0 的意义是重量为 6 的轨道选取 0 个，函数的个数“5”是这组解根据定理 5 的方法计算出的支撑集中含有$\mathbf{0}_p = 0\underbrace{0\cdots0}_{p}$ ( $p=7$ ) 的函数个数$T_j = \prod_{i=1}^{p-1}\binom{N_i}{n_{ji}}$，下面的类似。

## 4 结束语

本文首先改进了文献[20]中关于奇素数元 $P(2,3)$ 函数的构造方法，提出了一种更一般的构造；然后通过对具有某些密码学性质的旋转对称布尔函数特征矩阵性质的研究，给出了满足多个密码学性质 RSBF 的构造与计数；通过解定理 4 中的方程组（1）的整数解完全确定了素数元 $P(1,2,3)$函数的构造方案以及这类函数的精确计数问题；其次给出了三元、五元、七元 $P(1,2,3)$函数的构造与计数；最后笔者还给出了一个猜想。

## 参考文献：


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

[2] FILIOL E, FONTAINE C. Highly nonlinear balanced Boolean functions with good correlation immunity[A]. Advances in Cryptology-EUROCRYPT'98[C]. Espoo, Finland, 1998. 475-488.

[3] COURTOIS N, MEIER W. Algebraic attacks on stream ciphers with linear feedback[A]. Biham Eed Advances in Cryptology- EUROCRYPT 2003[C]. Warsaw, Poland, 2003.346-359.

[4] CANTEAUT A. Open problems related to algebraic attacks on stream ciphers[A]. WCC2005[C]. Bergen, Norway, 2006.120-134.

[5] DALAI D, MAITRA S, SARKAR S. Basic theory in construction of Boolean functions with maximum possible annihilator immunity[J]. Des Code Crypt, 2006, 40(1):41-58.

[6] BRAEKEN A, PRENEEL B. On the algebraic immunity of symmetric Boolean functions[A]. IndoCRYPT[C]. Bangalore, India, 2005. 35-48 .

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

[8] DALAI D K, MAITRA S. Reducing the number of homogeneous linear equations in finding annihilators[EB/OL]. http://eprint.iacr.org/2006/032.

[9] TU Z, DENG Y. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebra immunity[J]. Designs, Codes and Cryptography, 60(2011):1-14.

[10] TU Z, DENG Y. Boolean functions optimizing most of the cryptographic criteria[J]. Discrete Applied Mathematics(2011), 2011, 160(4-5): 427-435.

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

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

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

[14] 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, India, 2004. 161-177.

[15] SARKAR S, MAITRA S. Construction of rotation symmetric Boolean functions with maximum algebraic immunity on odd number of variables[A]. AAECC 2007[C]. Bangalore, India, 2007. 271-280.

[16] FU S J, LI C, MATSUURA K, *et al*. Construction of rotation symmetric Boolean functions with maximum algebraic immunity[A]. CANS 2009[C]. Kanazawa, Japan, 2009. 402-419.

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

[18] FU S J, LI C, QU L, *et al*. On the number of rotation symmetric functions over GF(*p*)[J]. Mathematical and Computer Modelling, 2012, 55(1-2): 142-150.

[19] **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.

[20] **王永娟,韩文报,李世取**. **满足** CI **的** RotS **函数的构造与计数**[J]. **通信学报**, 2007, 28(11A):6-9.
WANG Y J, HAN W B, LI S Q. Construction and numeration of correlation immunity RotS Boolean function[J]. Journal on Communications, 2007, 28(11A):6-9.

[21] **庞善起，杜蛟，席金彦**. **相关免疫函数阶的判别方法**[J]. **应用数学学报，** 2009, 32(3):445-453.
PANG S Q, DU J, XI J Y. Some methods for judging the order of correlation-immune functions[J]. Acta Mathematicae Applicacatae Si ica, 2009, 32(3):445-453.

[22] **杜蛟，温巧燕，张劼等**. **五元** 1 **阶弹性函数的代数免疫阶**[J]. **通信学报**, 2011, 32(4):17-24.
DU J, WEN Q Y, ZHANG J, *et al*. On the algebraic immunity for 1st-resilience Boolean functions with five pvariables[J]. Journal on Communications, 2011, 32(4):17-24.

**作者简介：**

**杜蛟（**1978-**），男，湖北英山人，北京邮电大学博士生，新乡学院助教，主要研究方向为密码学与应用数学。**

**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。**

**庞善起（**1965-**），男，河南卫辉人，博士，河南师范大学教授、硕士生导师，主要研究方向为实验设计与组合设计。**