文章编号:1000－2367(2019)04－0001－15 DOI:10.16366/j.cnki.1000－2367.2019.04.001

有限域上分圆映射对合的构造、计数与分类

屈龙江,李康荃

(国防科技大学 文理学院,长沙 410073)

摘 要:由于有限域上多项式 $f(x)$ 可以唯一地写成 $x^rh(x^s)+f(0)$,2009 年王强等基于此表示提出多项式指标概念.这一概念自提出之后,在研究多项式值域、特征和、置换多项式等问题上起到了重要的作用.对合在分组密码构造中有十分重要的意义.近两年,有多位学者对对合进行研究,旨在为分组密码构造中 S 盒的设计提供更多选择.最近,郑大彬等对 F_q 上形如 $x^rh(x^s)$ 的对合进行研究,给出了该类多项式是对合的一个充要条件并提出了一种构造此类对合的方法.该方法需要对某方程组,即方程组(3),进行求解.

利用对称群中的共轭关系和分块矩阵的思想,首先对郑大彬等的方法进行深层次的分析,给出了方程组解的确切表达式,改进了该构造方法;其次,给出了有限域上任意固定指标、常数项为 0 的对合的个数;再次,根据指标的大小,对具有显性表达式的已有对合进行分类;最后,确定了几类对合,丰富了已有结果.具体地,针对低指标对合,给出了指标为 2 和 3 的较郑大彬等结果更具体的对合条件;针对非低指标对合,利用李康荃等得到的复合逆结果,给出了一类 F_{q^2} 上形如 $x^rh(x^{q-1})$ 的对合.

关键词:有限域;指标;对合;分类

中图分类号:TP918 **文献标志码**:A

1 介 绍

设 q 为素数幂,有限域 F_q 上的置换多项式是指能使映射 $f:F_q\to F_q$ 为双射的多项式 $f(x)$.给定 F_q 上的一个置换多项式 $f(x)$,显然存在 F_q 上的一个多项式 $f^{-1}(x)$ 使得

$$f(f^{-1}(x))\equiv f^{-1}(f(x))\equiv x\ (\mathrm{mod}\ x^q-x),$$

并且 $f^{-1}(x)(\mathrm{mod}\ x^q-x)$ 是被 $f(x)$ 唯一确定的,一般称之为 $f(x)$ 在 F_q 上的复合逆.特别地,如果置换 f 的复合逆恰为其本身,即有 $f(f(x))=x$,则称 f 为对合.

众所周知,有限域 F_q 上的任意次数小于等于 $q-1$ 的多项式 $f(x)$ 可以唯一地写成 $f(x)=a(x^rh(x^{(q-1)/\ell}))+b$,其中 $b=f(0)$,$\ell\mid q-1$.事实上,如果 $f(x)=a(x^d+a_{d-i_1}x^{d-i_1}+\cdots+a_{d-i_k}x^{d-i_k})+b$,其中 $a,a_{d-i_j}\neq 0,j=1,\cdots,k$.记 $d-i_k=r$.则 $f(x)=a(x^rh(x^{(q-1)/\ell}))+b$,其中 $h(x)=x^{e_0}+a_{d-i_j}x^{e_1}+\cdots+a_r$,$e_0=\dfrac{d-r}{s}$,对任意整数 $1\le j\le k-1$,$e_j=\dfrac{d-r-i_j}{s}$,$s=\gcd(d-r,d-r-i_1,\cdots,d-r-i_{k-1},q-1)$,$\ell=\dfrac{q-1}{s}$ 和 $\gcd(e_0,e_1,\cdots,e_{k-1},\ell)=1$.此时,称整数 $\ell=\dfrac{q-1}{s}$ 为多项式 $f(x)$ 的指标(index).从指标的定义可以看出其适用的多项式至少是二项式.指标这一概念是王强等[1]于 2009 年提出的.这一概念自提出后,在多项式值域[2]、特征和[3]、置换多项式[1]等众多研究方向上都有重要的应用.

假设有限域 F_q 上的多项式 $f(x)$ 满足首项系数为 1 且 $f(0)=0$,则 $f(x)$ 可以写成 $x^rh(x^s)$,其中 $s=$

收稿日期:2019-02-11;**修回日期**:2019-05-17.

基金项目:国家自然科学基金(61722213;61572026)

作者简介(通信作者):屈龙江(1980—),男,河南新县人,国防科技大学教授,博士生导师,国家优青,研究方向为编码密码及其应用,E-mail:ljqu_happy@hotmail.com.

$\frac{q-1}{\ell}$.事实上,这类多项式与 r 阶分圆映射有着紧密联系.设 γ 为有限域 F_q 的本原元,$q-1=\ell s$,$C_0:=\{\gamma^{\ell j}\mid j=0,1,\cdots,s-1\}$.则 $F_q^*:=F^q\backslash\{0\}$ 可以分解成若干个分圆陪集:$C_i=\gamma^i C_0$,$i=0,1,\cdots,\ell-1$.

对任意 $A_0,A_1,\cdots,A_{\ell-1}\in F_q$,分圆映射 $f_{A_0,A_1,\cdots,A_{\ell-1}}(x)$ 定义如下:

$$f_{A_0,A_1,\cdots,A_{\ell-1}}(x)=\begin{cases}0,\text{如果 } x=0,\\ A_i x,\text{如果 } x\in C_i,i=0,1,\cdots,\ell-1.\end{cases}$$

更一般地,r 阶分圆映射 $f^r_{A_0,A_1,\cdots,A_{\ell-1}}(x)$ 是指

$$f^r_{A_0,A_1,\cdots,A_{\ell-1}}(x)=\begin{cases}0,\text{如果 } x=0,\\ A_i x^r,\text{如果 } x\in C_i,i=0,1,\cdots,\ell-1.\end{cases}$$

可以证明,有限域 F_q 上形如 $f(x)=x^r h(x^s)$ 的多项式等价于 r 阶分圆映射.一方面,设 $f(x)=x^r h(x^s)$,令 $A_i=h(\gamma^{is})$,$i=0,1,\cdots,\ell-1$,则 $f^r_{A_0,A_1,\cdots,A_{\ell-1}}(x)=f(x)$;另一方面,对于 r 阶分圆映射 $f^r_{A_0,A_1,\cdots,A_{\ell-1}}(x)$,其多项式表示为 $f(x)=\frac{1}{\ell}\sum\limits_{j=0}^{\ell-1}\Big(\sum\limits_{i=0}^{\ell-1}a_i\zeta^{-ji}\Big)x^{js+r}$,其中 $\zeta=\gamma^s$ 是 ℓ 阶单位根.针对有限域 F_q 上 r 阶分圆映射或 $f(x)=x^r h(x^s)$ 置换性质的研究可以追溯到 Rogers 和 Dickson 的工作.1991 年,万大庆和 Lidl[4] 第一次系统地给出此类多项式的置换性质刻画.后续的研究可以参考侯向东[5] 关于置换多项式的综述论文和李念等[6] 关于 Niho 指数的综述论文以及其中的参考文献.

对合在实践和理论中皆有广泛和重要的应用.在实践应用上,对合是分组密码算法中 S 盒的理想选择;在理论应用上,对合在构造 Bent 函数中有着直接应用[7].关于 r 阶分圆映射或 $f(x)=x^r h(x^s)$ 的对合性质,2017 年王强[8] 给出了一类更具有一般性的多项式,即广义分圆映射的对合刻画.设 $R_0(x),R_1(x),\cdots,R_{\ell-1}(x)\in F_q[x]$,$F_q$ 上的广义分圆映射定义如下:

$$f^{R_0(x),R_1(x),\cdots,R_{\ell-1}(x)}_{A_0,A_1,\cdots,A_{\ell-1}}(x)=\begin{cases}0,\text{如果 } x=0,\\ A_i R_i(x),\text{如果 } x\in C_i,i=0,1,\cdots,\ell-1.\end{cases}$$

与 r 阶分圆映射类似,广义分圆映射的多项式表示为 $f(x)=\frac{1}{\ell}\sum\limits_{i=0}^{\ell-1}\sum\limits_{j=0}^{\ell-1}A_i\zeta^{-ji}R_i(x)x^{js}$,其中 $s=\frac{q-1}{\ell}$,$\zeta=\gamma^s$.最近,郑大彬等[9] 给出了 $f(x)=x^r h(x^s)$ 是对合的一个充要条件,本文将说明其充要条件可由王强的结果[8] 简单证明.在此基础上,他们提出了一个构造形如 $x^r h(x^s)$ 对合的方法,该方法需要对某类方程组,即方程组(3)进行求解.

本文主要对有限域上形如 $f(x)=x^r h(x^s)$ 的对合进行更深入的分析,根据指标对已有对合进行分类并构造几类新的对合.本文剩余部分的主要工作及组织结构安排如下:第二节在回顾王强和郑大彬等工作的基础上,对郑大彬等的方法进行深入的分析.利用对称群中的共轭关系和分块矩阵的思想,给出了方程组(3)解的确切表达式,改进了郑大彬等的方法;在此基础上,第三节给出了有限域上任意固定指标、常数为 0 的对合个数.第四节是根据指标大小对对合进行分类,其中包括已有结果和新结果.第五节是总结与进一步工作.因为本文涉及符号较多,为方便读者阅读,下面对本文常见符号进行说明.

符号说明:

q:素数幂;

γ:有限域 F_q 的本原元;

ℓ,s:皆为正整数,并且 $q-1=\ell s$;

$\zeta=\gamma^s$:ℓ 阶本原单位根;

$\mu_\ell:=\{x\in F_q\mid x^\ell=1\}$;

$\mathrm{ind}_\gamma(\alpha)$,其中 $\alpha\in F_q^*$:使得 $\alpha=\gamma^k$ 成立的最小的正整数 k;

$Z_\ell:=\{0,1,\cdots,\ell-1\}$;

S_ℓ:Z_ℓ 上的对称群;

$\mathrm{id}\in S_\ell$:Z_ℓ 上的恒等映射;

$\mathscr{R}_s:=\{1\le r\le s\mid r^2\equiv 1(\mathrm{mod}\ s)\}$;

$\mathscr{R}_{s,s_1}=\{1\le r\le s\mid r^2\equiv 1(\mathrm{mod}\ s_1)\}$,其中 $s\mid s_1$;

$\mathscr{F}_{\ell,\mathscr{R}_s}$:$F_q$ 上所有形如 $x^r h(x^s)$ 的对合组成的集合,其中 $1\le r\le s$;

$\mathscr{F}_{\ell_1,\mathscr{R}_s,s_1}$:$F_q$ 上所有形如 $x^r h(x^{s_1})$ 的对合组成的集合,其中 $1\le r\le s$.

$\mathscr{G}_{\ell_1,\mathscr{R}_s,s_1}$:$\mathscr{F}_{\ell,\mathscr{R}_s}$ 中指标为 ℓ_1 的对合,其中 $\ell_1\mid\ell$,$s_1=\frac{q-1}{\ell_1}$;

$\mathscr{G}_{\ell,\mathscr{R}_s}:=\mathscr{G}_{\ell,\mathscr{R}_{s,s}}$;

$\mathscr{M}_\ell$:$\mathscr{F}_{\ell,\mathscr{R}_s}$ 中的单项式对合;

$\mathscr{M}_{\ell,\ell_1}$:$\mathscr{M}_\ell$ 中形如 $x^r h(x^{s_1})$ 的单项式对合;

本文提到的所有“因子”皆为正因子.

2　分圆映射对合的构造

本节主要对分圆映射对合的构造进行研究.众所周知,有限域上多项式 $f(x)$ 可唯一地写成 $x^r h(x^s)+f(0)$ 的形式.基于此,王强等[1] 于 2009 年提出多项式指标概念.显然,当 $f(x)$ 各项次数皆小于等于 $q-1$ 时,由多项式指标的定义可知 $f(x)$ 指标是唯一的.然而,当允许 $f(x)$ 项的次数大于等于 q 时,r 的选择并不唯一,然而下述引理说明多项式指标不随 r 选择的不同而变化.

引理 1　设 $q-1=\ell s$ 且多项式 $f(x)=x^r h(x^s)\in F_q[x]$ 的指标为 ℓ.则 ℓ 不随着 r 选择的不同而变化.

证明　假设 $h(x)=x^{e_0}+b_1x^{e_1}+\cdots+b_{k-1}x^{e_{k-1}}+b_k$,其中 $e_0>e_1>\cdots>e_{k-1}$,则由多项式指标的定义可知 $\gcd(e_0,e_1,\cdots,e_{k-1},\ell)=1$. 并且 $f(x)=x^r(x^{e_0s}+b_1x^{e_1s}+\cdots+b_{k-1}x^{e_{k-1}s}+b_k)=x^{r+e_0s}+b_1x^{r+e_1s}+\cdots+b_{k-1}x^{r+e_{k-1}s}+b_kx^r$.

如果将 $f(x)$ 中的 x^{r+e_is} 项提出来,也就是说,$r\to r_i:=r+e_is$,则 $f(x)$ 可写成

$$x^{r_i}(x^{(e_0-e_i)s}+\cdots+b_{i-1}x^{(e_{i-1}-e_i)s}+b_i+b_{i+1}x^{(\ell+e_{i+1}-e_i)s}+\cdots+b_kx^{(\ell-e_i)s}).$$

下面只需证明 $\gcd(e_0-e_i,\cdots,e_{i-1}-e_i,\ell+e_{i+1}-e_i,\cdots,\ell-e_i,\ell)=1$.如若不然,假设 $\gcd(e_0-e_i,\cdots,e_{i-1}-e_i,\ell+e_{i+1}-e_i,\cdots,\ell-e_i,\ell)=d>1$,则 $d\mid\ell$,结合 $d\mid\ell-e_i$ 得到 $d\mid e_i$.进而 $d\mid e_j$,其中 $j=0,1,\cdots,k-1$.所以 $d\mid\gcd(e_0,e_1,\cdots,e_{k-1},\ell)=1$,这与 $d>1$ 矛盾.所以 $\gcd(e_0-e_i,\cdots,e_{i-1}-e_i,\ell+e_{i+1}-e_i,\cdots,\ell-e_i,\ell)=1$.也就是说 $f(x)=x^{r_i}h_i(x^s)$,其中 $h_i(x)=x^{e_0-e_i}+\cdots+b_{i-1}x^{e_{i-1}-e_i}+b_i+b_{i+1}x^{\ell+e_{i+1}-e_i}\cdots+b_kx^{\ell-e_i}$.所以 $f(x)$ 的指标 ℓ 是多项式 $f(x)$ 的固有性质,不随着 r 选择的不同而变化.

2017 年,王强[8]得到了广义分圆置换 $f^{x^{r_0},x^{r_1},\cdots,x^{r_{\ell-1}}}_{A_0,A_1,\cdots,A_{\ell-1}}(x)$ 的复合逆,进而完全刻画了广义分圆映射 $f^{x^{r_0},x^{r_1},\cdots,x^{r_{\ell-1}}}_{A_0,A_1,\cdots,A_{\ell-1}}(x)$ 的对合性质.

定理 1[8](定理2)　设 γ 为有限域 F_q 的本原元,$q-1=\ell s$,$\zeta=\gamma^s$.令 $A_0,A_1,\cdots,A_{\ell-1}\in F_q^*$,$r_0,r_1,\cdots,r_{\ell-1}$ 皆为正整数.则 $f(x)=\frac{1}{\ell}\sum_{i=0}^{\ell-1}\sum_{j=0}^{\ell-1}A_i\zeta^{-ji}x^{r_i+js}\in F_q[x]$ 是 F_q 上的对合当且仅当以下 4 个条件同时成立:

(1)对任意 $i=0,1,\cdots,\ell-1$,存在整数 g_i 和 t_i 使得 $r_ig_i+st_i=1$ 成立;

(2)$\{\varphi(i)=\mathrm{ind}_\gamma(A_i)+ir_i(\mathrm{mod}\ \ell)\mid i=0,1,\cdots,\ell-1\}=Z_\ell$;

(3)对任意 $i=0,1,\cdots,\ell-1$,$r_{\varphi(i)}\equiv r_i^{-1}\equiv g_i(\mathrm{mod}\ s)$;

(4)对任意 $i=0,1,\cdots,\ell-1$,$A_{\varphi(i)}=A_i^{-g_i}\zeta^{it_i}$.

最近,郑大彬等对有限域 F_q 上形如 $f(x)=x^r h(x^s)$ 多项式的对合性质进行研究,给出了如下的充要条件.

定理 2[9](定理2,2)　设 $q-1=\ell s$,$f(x)=x^r h(x^s)\in F_q[x]$ 和 $g(x)=x^r h(x)^s$.则 $f(x)$ 是 F_q 上的对合当且仅当(1) $r^2\equiv1(\mathrm{mod}\ s)$ 且(2) 对任意 $z\in\mu_\ell$,$\phi(z)=z^{\frac{r^2-1}{s}}(h\circ g)(z)h(z)^r=1$.

事实上,在定理 1 中令 $r_0=r_1=\cdots=r_{\ell-1}$,则 $f(x)$ 为 r 阶分圆映射,即等价于形如 $x^r h(x^s)$ 的多项式,进而有推论 1.

推论 1　设 $f(x)=x^r h(x^s)\in F_q[x]$,其中 $s=\frac{q-1}{\ell}$.则 $f(x)$ 是 F_q 上的对合当且仅当

(1) $r^2\equiv1(\mathrm{mod}\ s)$;

(2)$\{\varphi(i)=\mathrm{ind}_\gamma(h(\zeta^i))+ir(\mathrm{mod}\ \ell)\mid i=0,1,\cdots,\ell-1\}=Z_\ell$;

(3)对任意 $i=0,1,\cdots,\ell-1$,$h(\zeta^{\varphi(i)})=h(\zeta^i)^{-r}\gamma^{i(1-r^2)}$,其中 $\zeta=\gamma^s$.

证明　在定理 1 中,对 $\forall\, i=0,1,\cdots,\ell-1$,$A_i=h(\zeta^i)$,$r_i=r$.且由定理 1 中的(3) 可知 $r\equiv r^{-1}(\mathrm{mod}\ s)$,也就是说,$r^2\equiv1(\mathrm{mod}\ s)$.此外,由定理 1 中的(2) 可直接得到本推论的(2).最后,假设 $r^2+st=1$,即 $t_i=t$,

则 $\zeta^{it_i}=(\gamma^s)^{it}=\gamma^{i(1-r^2)}$.所以定理 1 中的(4) 等价于对任意 $i=0,1,\cdots,\ell-1,h(\zeta^{\varphi(i)})=h(\zeta^i)^{-r}\gamma^{i(1-r^2)}$.

对于定理 2 中的(2),记 $z=\zeta^i\in\mu_\ell$,则

$$\phi(z)=\phi(\zeta^i)=\gamma^{i(r^2-1)}(h\circ g)(\zeta^i)h(\zeta^i)^r=\gamma^{i(r^2-1)}h(\zeta^{ir}h(\zeta^i)^s)h(\zeta^i)^r=\gamma^{i(r^2-1)}h(\zeta^{\varphi(i)})h(\zeta^i)^r=1,$$

也就是推论 1 中的(3).此外,由推论 1 中的(3)不仅可以得到 $\{\varphi(i)=\mathrm{ind}_\gamma(h(\zeta^i))+ir(\mathrm{mod}\,\ell)\mid i=0,1,\cdots,\ell-1\}=Z_\ell$,而且可以推导出 $\varphi(i)=\mathrm{ind}_\gamma(h(\zeta^i))+ir(\mathrm{mod}\,\ell)$ 是 Z_ℓ 上的对合.由 $\varphi(i)=\mathrm{ind}_\gamma(h(\zeta^i))+ir(\mathrm{mod}\,\ell)$ 可知,存在整数 $1\le e_i\le s$ 使得

$$h(\zeta^i)=\gamma^{\ell e_i+\varphi(i)-ir}. \tag{1}$$

并且由推论 1 中的(3)可知 $h(\zeta^{\varphi(i)})=h(\zeta^i)^{-r}\gamma^{i(1-r^2)}=\gamma^{-\ell re_i-\varphi(i)r+i}$.此外,在等式(1) 中用 $\varphi(i)$ 代替 i 可得 $h(\zeta^{\varphi(i)})=\gamma^{\ell e_{\varphi(i)}+\varphi(\varphi(i))-\varphi(i)r}$.所以,对任意 $i=0,1,\cdots,\ell-1$ 有

$$\ell e_{\varphi(i)}+\ell re_i+\varphi(\varphi(i))-i\equiv 0\ (\mathrm{mod}\ q-1). \tag{2}$$

因为 $|\varphi(\varphi(i))-i|<\ell$ 和 $\ell\mid(\varphi(\varphi(i))-i)$,所以对任意 $i=0,1,\cdots,\ell-1,\varphi(\varphi(i))=i$.

命题 1 令 $f(x)=x^rh(x^s)$,其中 $s=\dfrac{q-1}{\ell}$.如果 $f(x)$ 是 F_q 上的对合,则 $\varphi(i)=\mathrm{ind}_\gamma(h(\zeta^i))+ir(\mathrm{mod}\,\ell)$ 是 Z_ℓ 上的对合.

进而,方程组(2)变为

$$e_{\varphi(i)}+re_i\equiv 0(\mathrm{mod}\ s) \tag{3}$$

其中 $i=0,1,\cdots,\ell-1$.

由文献[9]中定理 2.5 可知,假设 $r,\varphi(i),e_i$ 皆给定并且 $f(x)=x^rh(x^s)$ 是 F_q 上的对合,则 $h(x)=b_{\ell-1}x^{\ell-1}+b_{\ell-2}x^{\ell-2}+\cdots+b_1x+b_0$ 的系数可由以下方程组确定:

$$\begin{cases}h(1)=b_{\ell-1}+b_{\ell-2}+\cdots+b_1+b_0=\gamma^{\ell e_0+\varphi(0)},\\ h(\zeta)=b_{\ell-1}\zeta^{\ell-1}+b_{\ell-2}\zeta^{\ell-2}+\cdots+b_1\zeta+b_0=\gamma^{\ell e_1+\varphi(1)-r},\\ \qquad\vdots\\ h(\zeta^{l-1})=b_{\ell-1}\zeta^{(\ell-1)(\ell-1)}+b_{\ell-2}\zeta^{(\ell-1)(\ell-2)}+\cdots+b_1\zeta^{\ell-1}+b_0=\gamma^{\ell e_{\ell-1}+\varphi(\ell-1)-(\ell-1)r},\end{cases}$$

也就是,

$$\boldsymbol{AX}=\boldsymbol{R}, \tag{4}$$

其中

$$\boldsymbol{A}=\begin{pmatrix}1&1&\cdots&1&1\\ \zeta^{\ell-1}&\zeta^{\ell-2}&\cdots&\zeta&1\\ \vdots&\vdots&&\vdots&\vdots\\ \zeta^{(\ell-1)(\ell-1)}&\zeta^{(\ell-1)(\ell-2)}&\cdots&\zeta^{\ell-1}&1\end{pmatrix},\boldsymbol{X}=\begin{pmatrix}b_{\ell-1}\\ b_{\ell-2}\\ \vdots\\ b_1\\ b_0\end{pmatrix},\boldsymbol{R}=\begin{pmatrix}\gamma^{\ell e_0+\varphi(0)}\\ \gamma^{\ell e_1+\varphi(1)-r}\\ \vdots\\ \gamma^{\ell e_{\ell-1}+\varphi(\ell-1)-(\ell-1)r}\end{pmatrix}.$$

显然,$\boldsymbol{A}$ 是范德蒙德矩阵,是可逆的.即 $\boldsymbol{X}=\boldsymbol{A}^{-1}\boldsymbol{R}$ 是 $\boldsymbol{AX}=\boldsymbol{R}$ 的唯一解.所以,想要构造有限域 F_q 上形如 $x^rh(x^s)$ 的对合,只需确定 $r,\varphi(i),e_i$ 的值即可.首先不妨假设 $1\le r\le s$.其原因在于,如果 $r>s$,$r=r_1+s$,其中 $r_1\ge 1$,则 $f(x)=x^rh(x^s)=x^{r_1+s}(b_{\ell-1}x^{(\ell-1)s}+\cdots+b_1x^s+b_0)=x^{r_1}(b_{\ell-2}x^{(\ell-1)s}+\cdots+b_0x^s+b_{\ell-1})=x^{r_1}h_1(x^s)$.也就是说,$f(x)=x^rh(x^s)=x^{r_1}h_1(x^s)$.所以 r 满足 $1\le r\le s$,并且 $r^2\equiv 1(\mathrm{mod}\ s)$;其次 $\varphi(i)$ 是 Z_ℓ 上的对合;最后只需在 $r,\varphi(i)$ 给定的条件下,计算方程组(3) 的解即可.

上述构造有限域 F_q 上形如 $x^rh(x^s)$ 对合的方法与文献[9] 中定理 2.5 类似.利用该方法,郑大彬等[9] 构造了 F_q 上 $x^rh(x^s)$ 的对合,其中 $3\mid q-1$ 和 $s=\dfrac{q-1}{3}$.本节对该方法进行改进,主要在于对方程组(3) 进行更深层次的分析.事实上,利用对称群中的共轭关系和分块矩阵的思想可以对方程组(3) 进行化简并求解,在此基础上,可以计算出有限域 F_q 上指标为 ℓ,常数为 0 的对合的个数.

首先回顾对称群与共轭关系的基本概念和结论[10].记 S_ℓ 为 Z_ℓ 上的对称群,若置换 $\sigma\in S_\ell$ 把 t 个不同元

素 $a_{i_1},a_{i_2},\cdots,a_{i_t}$ 分别映成 $a_{i_2},a_{i_3},\cdots,a_{i_t},a_{i_1}$,则称此为一个长为 t 的轮换,并且记为$(a_{i_1}a_{i_2}\cdots a_{i_t})$,特别地,长为 2 的轮换又称为对换.显然,每个置换均可写成一些轮换的乘积,并且不同轮换中没有公共元素.如果其中长为 r 的轮换共有 λ_r 个$(1\leq r\leq \ell)$,则称此置换的型为 $1^{\lambda_1}2^{\lambda_2}\cdots\ell^{\lambda_\ell}$,并且 S_ℓ 中型为 $1^{\lambda_1}2^{\lambda_2}\cdots\ell^{\lambda_\ell}$ 的置换共有 $\dfrac{\ell!}{\prod_{i=1}^{\ell}\lambda_i!\ i^{\lambda_i}}$ 个.记 $\mathscr{L}_\ell$ 为 Z_ℓ 上所有对合组成的集合.显然,对任意 $\varphi\in\mathscr{L}_\ell$,其型为 $1^{\lambda_1}2^{\lambda_2}$,其中 $\lambda_1+2\lambda_2=\ell$.设 σ 和σ'是S_ℓ 中的两个置换.如果存在 $\tau\in S_\ell$,使得 $\sigma'=\tau\sigma\tau^{-1}$,则称 σ 和σ'是共轭的,记为 $\sigma\sim\sigma'$.显然,共轭关系 $\sim$ 是 $\mathscr{L}_\ell$ 中的一个等价关系.

引理 2　设 $\widetilde{\mathscr{L}}_\ell=\mathscr{L}_\ell/\sim$.则 $|\widetilde{\mathscr{L}}_\ell|=\lfloor\dfrac{\ell}{2}\rfloor+1$,其中$\lfloor x\rfloor=\max\{n\in Z\mid n\leq x\}$.

证明　对任意 $\varphi\in\mathscr{L}_\ell$,假设 φ 的型为 $1^{\lambda_1}2^{\lambda_2}$,其中 $\lambda_1+2\lambda_2=\ell$.则 λ_2 有$(\lfloor\dfrac{\ell}{2}\rfloor+1)$ 种选择,即 0 到$\lfloor\dfrac{\ell}{2}\rfloor$.又因为任意两个置换 $\sigma,\sigma'\in Z_\ell$ 是共轭的当且仅当它们具有相同的型[10],所以,$|\widetilde{\mathscr{L}}_\ell|=\lfloor\dfrac{\ell}{2}\rfloor+1$.

对任意 $\varphi\in\mathscr{L}_\ell$,假设其型为 $1^{\lambda_1}2^{\lambda_2}$,其中 $\lambda_1+2\lambda_2=\ell$,则 φ 共轭等价于$\bar{\varphi}=(\lambda_1(\lambda_1+1))((\lambda_1+2)(\lambda_1+3))\cdots((\ell-2)(\ell-1))$,称 $\bar{\varphi}$ 是型为 $1^{\lambda_1}2^{\lambda_2}$ 的标准对合.所以 $\widetilde{\mathscr{L}}_\ell$ 可以看成 $\mathscr{L}_\ell$ 中所有标准对合组成的集合.将 $\bar{\varphi}$ 代入方程组(3),并将方程组写成矩阵形式,得到

$$\boldsymbol{M}\boldsymbol{X}=\boldsymbol{T},\tag{5}$$

其中

$$\boldsymbol{M}=\begin{pmatrix}(r+1)\boldsymbol{I}_{\lambda_1} & & & \\ & \boldsymbol{M}_{2,1} & & \\ & & \ddots & \\ & & & \boldsymbol{M}_{2,\lambda_2}\end{pmatrix},$$

$\boldsymbol{I}_{\lambda_1}$ 是 λ_1 阶单位矩阵,对任意 $1\leq i\leq\lambda_2$,

$$\boldsymbol{M}_{2,i}=\begin{pmatrix}r & 1\\ 1 & r\end{pmatrix},\boldsymbol{X}=\begin{pmatrix}\boldsymbol{X}_{\lambda_1}\\ \boldsymbol{X}_{2,1}\\ \vdots\\ \boldsymbol{X}_{2,\lambda_2}\end{pmatrix},\boldsymbol{T}=\begin{pmatrix}\boldsymbol{T}_{\lambda_1}\\ \boldsymbol{T}_{2,1}\\ \vdots\\ \boldsymbol{T}_{2,\lambda_2}\end{pmatrix},\boldsymbol{X}_{\lambda_1}=\begin{pmatrix}e_0\\ e_1\\ \vdots\\ e_{\lambda_1-1}\end{pmatrix},$$

$$\boldsymbol{X}_{2,i}=\begin{pmatrix}e_{\lambda_1+2i-2}\\ e_{\lambda_1+2i-1}\end{pmatrix},\boldsymbol{T}_{\lambda_1}=\begin{pmatrix}st_0\\ st_1\\ \vdots\\ st_{\lambda_1-1}\end{pmatrix},\boldsymbol{T}_{2,i}=\begin{pmatrix}st_{\lambda_1+2i-2}\\ st_{\lambda_1+2i-1}\end{pmatrix},$$

其中 $1\leq i\leq\lambda_2$,并且对任意 $0\leq j\leq\ell-1$,t_j 为整数,$1\leq e_j\leq s$.不妨记 $\boldsymbol{M}_{2,i}=M_2$,$\boldsymbol{X}_{2,i}=\boldsymbol{X}_2$ 和 $\boldsymbol{T}_{2,i}=\boldsymbol{T}_2$.

所以为计算方程组 $\boldsymbol{M}\boldsymbol{X}=\boldsymbol{T}$,只需计算两个子方程组$(r+1)\boldsymbol{I}_{\lambda_1}\boldsymbol{X}_{\lambda_1}=\boldsymbol{T}_{\lambda_1}$ 和 $\boldsymbol{M}_2\boldsymbol{X}_2=\boldsymbol{T}_2$.

对子方程组 $(r+1)\boldsymbol{I}_{\lambda_1}\boldsymbol{X}_{\lambda_1}=\boldsymbol{T}_{\lambda_1}$,因为 $1\leq r\leq s$,所以 $r+1\neq 0$,进而$(r+1)\boldsymbol{I}_{\lambda_1}\boldsymbol{X}_{\lambda_1}=\boldsymbol{T}_{\lambda_1}$ 的解为$(e_0,e_1,\cdots,e_{\lambda_1-1})=(\dfrac{st_0}{r+1},\dfrac{st_1}{r+1},\cdots,\dfrac{st_{\lambda_1-1}}{r+1})$,其中 $t_0,t_1,\cdots,t_{\lambda_1-1}$ 为整数.结合对任意 $0\leq i\leq\lambda_1-1$,$1\leq e_i\leq s$,可知 $1\leq t_i\leq r+1$.又因为 $e_i=\dfrac{st_i}{r+1}\in Z$,所以 $t_i=\dfrac{j_i(r+1)}{\gcd(s,r+1)}$,其中 $1\leq j_i\leq\gcd(s,r+1)$.进一步,对任意 $0\leq i\leq\lambda_1-1$,$e_i=\dfrac{j_is}{\gcd(s,r+1)}$,其中 $1\leq j_i\leq\gcd(s,r+1)$.所以$(r+1)\boldsymbol{I}_{\lambda_1}\boldsymbol{X}_{\lambda_1}=\boldsymbol{T}_{\lambda_1}$ 一共有 $\gcd(s,$

$r+1)^{\lambda_1}$ 个解,并且所有的解为$(e_0,e_1,\cdots,e_{\lambda_1-1})=(\frac{j_0 s}{\gcd(s,r+1)},\frac{j_1 s}{\gcd(s,r+1)},\cdots,\frac{j_{\lambda_1-1}s}{\gcd(s,r+1)})$,其中 $1\leq j_i\leq \gcd(s,r+1)$.

引理 3 方程组 $(1+r)e_i\equiv 0(\bmod s)$,其中 $i=0,1,\cdots,\lambda_1-1$,的解为$(e_0,e_1,\cdots,e_{\lambda_1-1})=(\frac{j_0 s}{\gcd(s,r+1)},\frac{j_1 s}{\gcd(s,r+1)},\cdots,\frac{j_{\lambda_1-1}s}{\gcd(s,r+1)})$,其中 $1\leq j_i\leq \gcd(s,r+1)$ 和 $0\leq i\leq \lambda_1-1$.

对于方程组 $\boldsymbol{M}_2\boldsymbol{X}_2=\boldsymbol{T}_2$,为方便起见,将该方程组记为

$$\boldsymbol{M}_2\boldsymbol{X}=\boldsymbol{T}, \tag{6}$$

其中 $\boldsymbol{M}_2=\begin{pmatrix}r & 1\\ 1 & r\end{pmatrix}$ 和 $\boldsymbol{X}=\begin{pmatrix}e_0\\ e_1\end{pmatrix}$,$\boldsymbol{T}=\begin{pmatrix}st_0\\ st_1\end{pmatrix}$,$t_0,t_1$ 为整数.

当 $r=1$ 时,$\boldsymbol{M}_2=\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}$.此时,方程组(6)有解当且仅当 $t_0=t_1$.并且当 $t_0=t_1$ 时,方程(6)的解为$(e_0,e_1)=(e_0,st_0-e_0)$.结合 $e_i\in Z$ 和 $1\leq e_0,e_1\leq s$,方程(6)的解是$(e_0,e_1)=(e_0,(s-e_0)(\bmod s))$,其中 $1\leq e_0\leq s$.需要注意的是,因为 $1\leq e_1\leq s$,所以本文令 $0(\bmod s)=s$.

当 $1<r\leq q-2$ 时,$\boldsymbol{M}_2^{-1}=\frac{1}{r^2-1}\begin{pmatrix}r & -1\\ -1 & r\end{pmatrix}$. 所以方程组(6)的解为$(e_0,e_1)=(\frac{s(rt_0-t_1)}{r^2-1},\frac{s(rt_1-t_0)}{r^2-1})$.又因为 $t_1=rt_0-\frac{r^2-1}{s}e_0\in Z$,所以 e_0 可以是 1 到 s 的任意整数.进一步可得,$e_1=st_0-re_0=-re_0(\bmod s)$.所以,方程组 $\boldsymbol{M}_2\boldsymbol{X}=\boldsymbol{T}$ 的解为$(e_0,e_1)=(e_0,-re_0(\bmod s))$,其中 $1\leq e_0\leq s$.

结合上述两种情况,有以下结论.

引理 4 方程组

$$\begin{cases}e_0+re_1\equiv 0\ (\bmod s),\\ re_0+e_1\equiv 0\ (\bmod s)\end{cases} \tag{7}$$

的解为 $(e_0,e_1)=(e_0,-re_0(\bmod s))$,其中 $1\leq e_0\leq s$.

本节主要对文献[9]中提出的构造 F_q 上形如 $x^rh(x^s)$ 的对合方法进行更深层次的分析,主要贡献在于利用对称群中的共轭关系和分块矩阵的思想,对方程组(3)进行求解.最终得到了算法 1.算法 1 主要是针对 φ 是标准对合的情况.事实上,对于某个标准对合 $\bar{\varphi}$,$\mathscr{L}_\varphi:=\{\tau\bar{\varphi}\tau^{-1}\mid\tau\in\mathscr{L}_\ell\}$ 是所有与 $\bar{\varphi}$ 同型的对合.想要得到 F_q 上所有形如 $x^rh(x^s)$ 的对合,只需将 $\mathscr{L}_\varphi$ 输入到算法 1 中即可,其中 $\bar{\varphi}$ 跑遍 $\widetilde{\mathscr{L}}_\ell$.

算法 1 构造 F_q 上形如 $x^rh(x^s)$ 的对合

1:输入 q,F_q 的本原元 γ,$\ell\mid q-1$,$s=\frac{q-1}{s}$,$\zeta=\gamma^s$,$\mathscr{R}_s=\{1\leq r\leq s\mid r^2\equiv 1\ (\bmod s)\}$,$\widetilde{\mathscr{L}}_\ell$

2:for r in $\mathscr{R}_s$ do

3: $d:=\gcd(s,r+1)$

4: for φ in $\widetilde{\mathscr{L}}_\ell$ do

5: 记 λ 为 φ 中对换的个数

6: for j_0 in $[1..d]$ do

7: …

8: for $j_{\ell-2\lambda-1}$ in $[1..d]$ do

9: for $e_{\ell-2\lambda}$ in $[1..s]$ do

10: for $e_{\ell-2\lambda+2}$ in $[1..s]$ do

11: …

12: for $e_{\ell-2}$ in $[1..s]$ do

13: $(e_0,\cdots,e_{\ell-2\lambda-1},e_{\ell-2\lambda},e_{\ell-2\lambda+1},\cdots,e_{\ell-1})=$

$$(\frac{j_0 s}{d},\cdots,\frac{j_{\ell-2\lambda-1}s}{d},e_{\ell-2\lambda},(-re_{\ell-2\lambda})\pmod s,\cdots,(-re_{\ell-2})\pmod s)$$

14：
$$\begin{pmatrix}b_{\ell-1}\\b_{\ell-2}\\\vdots\\b_1\\b_0\end{pmatrix}=\frac{1}{n}\begin{pmatrix}1&\zeta&\cdots&\zeta^{\ell-2}&\zeta^{\ell-1}\\1&\zeta^2&\cdots&\zeta^{2(\ell-2)}&\zeta^{2(\ell-1)}\\\vdots&\vdots&&\vdots&\vdots\\1&\zeta^{\ell-1}&\cdots&\zeta^{(\ell-1)(\ell-2)}&\zeta^{(\ell-1)(\ell-1)}\\1&1&\cdots&1&1\end{pmatrix}\begin{pmatrix}\gamma^{\ell e_0+\varphi(0)}\\\gamma^{\ell e_1+\varphi(1)-r}\\\vdots\\\gamma^{\ell e_{\ell-1}+\varphi(\ell-1)-(\ell-1)r}\end{pmatrix}$$

15：　　输出 $f(x)=x^r(b_{\ell-1}x^{(\ell-1)s}+b_{\ell-2}x^{(\ell-2)s}+\cdots+b_1x^s+b_0)$

16：　　end for

17：　　…

18：　　end for

19：　　end for

20：　　end for

21：　　end for

22：　　end for

23：　　end for

24：end for

有限域 F_q 上对合 $f(x)$ 的不动点是指 F_q 中满足 $f(x)=x$ 的元素.对合的不动点数量多少决定对合的好坏,分组密码算法设计一般要求其中的对合只具有少量的不动点,甚至没有不动点.对于 F_q 上形如 $f(x)=x^rh(x^s)$ 的对合,显然 $x=0$ 是方程 $f(x)=x$ 的一个解;此外,对任意 $x\in F_q^*$,存在整数 i 使得 $x=\gamma^i$,此时方程 $f(x)=x$ 等价于 $\gamma^{ri}h(\zeta^i)=\gamma^i$,将等式(1),即 $h(\zeta^i)=\gamma^{\ell e_i+\varphi(i)-ir}$ 代入可得 $\ell e_i+\varphi(i)\equiv i\pmod{q-1}$.显然,当 $\varphi(i)\neq i$ 时,方程 $\ell e_i+\varphi(i)\equiv i\pmod{q-1}$ 没有解.也就是说,$f(x)$ 没有非零的不动点.所以,如果想利用算法 1 构造只具有少量不动点、形如 $x^rh(x^s)$ 的对合,应该选择 Z_ℓ 上不动点少的对合 φ 作为算法 1 的输入.

3　任意指标对合的计数

上一节在文献[9]的基础上,利用对称群中共轭关系和分块矩阵的思想,给出了一种构造 F_q 上形如 $x^rh(x^s)$ 对合更具体的方法,详见算法 1.本节利用算法 1,计算 F_q 上指标为 ℓ,常数为 0 的对合个数.首先给出 F_q 上形如 $x^rh(x^s)$ 的对合个数.

定理 3　设 $\ell\mid q-1$,$s=\dfrac{q-1}{\ell}$,$f(x)=x^rh(x^s)$,其中 $h(x)=b_{\ell-1}x^{\ell-1}+b_{\ell-2}x^{\ell-2}+\cdots+b_1x+b_0$,$\mathscr{R}_s:=\{1\le r\le s\mid r^2\equiv 1\pmod s\}$.则 F_q 上形如 $f(x)=x^rh(x^s)$ 的对合的个数为

$$N_{\ell,\mathscr{R}_s}=\sum_{r\in\mathscr{R}_s}\sum_{\lambda=0}^{\lfloor\frac{\ell}{2}\rfloor}\frac{\ell!}{(\ell-2\lambda)!\,\lambda!\,2^\lambda}\times\gcd(s,r+1)^{\ell-2\lambda}\times s^\lambda.\tag{8}$$

证明　由以上分析可知,$f(x)=x^rh(x^s)$ 是 F_q 上的对合当且仅当 $r\in\mathscr{R}_s$ 和 $(b_{\ell-1},b_{\ell-2},\cdots,b_1,b_0)$ 是方程组(4)的解.进一步由方程组(4)解的唯一性可知不同的 $(e_0,e_1,\cdots,e_{\ell-1})$ 和 φ(Z_ℓ 上的对合)可得到不同的 $(b_{\ell-1},b_{\ell-2},\cdots,b_1,b_0)$,所以 F_q 上形如 $f(x)$ 的对合个数等于 $(r,\varphi,e_0,\cdots,e_{\ell-1})$ 的个数.

下面假设 $r\in\mathscr{R}_s$ 给定,由引理 2 可知,相互不共轭的对合 $\varphi\in S_\ell$ 有 $\lfloor\dfrac{\ell}{2}\rfloor+1$ 种可能性,即它们的型为 $1^{\ell-2\lambda}2^\lambda$,其中 $\lambda=0,1,\cdots,\lfloor\dfrac{\ell}{2}\rfloor$.假设 λ 给定,则对每个型为 $1^{\ell-2\lambda}2^\lambda$ 的对合 φ,由引理 3 和引理 4 可知,方程组(5)解的个数是 $\gcd(s,r+1)^{\ell-2\lambda}\times s^\lambda$.另外,型为 $1^{\ell-2\lambda}2^\lambda$ 的对合一共有 $\dfrac{\ell!}{(\ell-2\lambda)!\,\lambda!\,2^\lambda}$ 个,所以 F_q 上形如

$f(x)$ 的对合的个数为

$$\sum_{r\in\mathcal{R}_s}\sum_{\lambda=0}^{\lfloor\frac{\ell}{2}\rfloor}\frac{\ell!}{(\ell-2\lambda)!\ \lambda!\ 2^{\lambda}}\times\gcd(s,r+1)^{\ell-2\lambda}\times s^{\lambda}.$$

证毕.

下面给出 F_q 上指标为 ℓ,形如 $f(x)=x^rh(x^s)$ 的对合个数,也就是 F_q 上指标为 ℓ,常数项为 0 的多项式对合的个数.由多项式指标的定义可知,形如 $f(x)=x^rh(x^s)$ 的多项式指标不一定为 $\ell=\frac{q-1}{s}$,但肯定是 ℓ 的因子.假设 $\mathcal{R}_s=\{1\le r\le s\mid r^2\equiv 1(\bmod s)\}$ 和 $\mathcal{R}_{s,s_1}=\{1\le r\le s\mid r^2\equiv 1(\bmod s_1)\}$,其中 $s\mid s_1$.显然 $\mathcal{R}_{s,s_1}\subseteq\mathcal{R}_{s_1}$,特别地,如果 $s_1=s$,则 $\mathcal{R}_{s,s_1}=\mathcal{R}_s$.再设 ℓ_1 为 ℓ 的任一因子,$s=\frac{q-1}{\ell}$ 和 $s_1=\frac{q-1}{\ell_1}$,令 $\mathcal{F}_{\ell,\mathcal{R}_s}$ 表示 F_q 上所有形如 $x^rh(x^s)$ 的对合组成的集合,$\mathcal{G}_{\ell_1,\mathcal{R}_{s,s_1}}$ 表示 $\mathcal{F}_{\ell,\mathcal{R}_s}$ 中指标为 ℓ_1 的对合,需要注意的是,$\mathcal{G}_{\ell_1,\mathcal{R}_{s,s_1}}$ 中不包含单项式.特别地,当 $\ell_1=\ell$,$\mathcal{G}_{\ell_1,\mathcal{R}_{s,s_1}}$ 简记为 $\mathcal{G}_{\ell,\mathcal{R}_s}$,并且最终需要计算的是 $|\mathcal{G}_{\ell,\mathcal{R}_s}|$.令 $\mathcal{M}_\ell$ 表示 $\mathcal{F}_{\ell,\mathcal{R}_s}$ 中的单项式对合,$\mathcal{M}_{\ell,\ell_1}$ 表示 $\mathcal{M}_\ell$ 中形如 $x^rh(x^{s_1})$ 的单项式对合.关于 $\mathcal{M}_\ell$ 和 $\mathcal{M}_{\ell,\ell_1}$,有以下结果.

命题 2 设 $q-1=\ell s,\ell_1\mid\ell,s_1=\frac{q-1}{\ell}$.则 $\mathcal{M}_\ell=\{bx^{r+is}\mid 0\le i\le\ell-1,1\le r\le s,b^{r+is+1}=1,(r+is)^2\equiv 1\ (\bmod q-1)\}$,$\mathcal{M}_{\ell,\ell_1}=\{bx^{r+is_1}\mid 0\le i\le\ell_1-1,1\le r\le s,b^{r+is_1+1}=1,(r+is_1)^2\equiv 1\ (\bmod q-1)\}$.记 $M_\ell=|\mathcal{M}_\ell|$ 和 $M_{\ell,\ell_1}=|\mathcal{M}_{\ell,\ell_1}|$,则

$$M_\ell=\sum_{(r,i)\in\mathcal{T}_s}\gcd(r+is+1,q-1),\tag{9}$$

$$M_{\ell,\ell_1}=\sum_{(r,i)\in\mathcal{T}_{s,s_1}}\gcd(r+is_1+1,q-1),\tag{10}$$

其中 $\mathcal{T}_s:=\{(r,i)\mid 1\le r\le s,0\le i\le\ell-1,(r+is)^2\equiv 1(\bmod q-1)\}$ 和 $\mathcal{T}_{s,s_1}:=\{(r,i)\mid 1\le r\le s,0\le i\le\ell_1-1,(r+is_1)^2\equiv 1(\bmod q-1)\}$.

证明 因为 $\mathcal{M}_\ell$ 是形如 $x^rh(x^s)$ 的单项式对合组成的集合,所以 $\mathcal{M}_\ell:=\{bx^{r+is}\mid 1\le r\le s,0\le i\le\ell$ 且 bx^{r+is} 是对合$\}$.又因为 bx^{r+is} 是 F_q 上的对合当且仅当 $b^{r+is+1}x^{(r+is)^2}=x$,也就是 $b^{r+is+1}=1$ 且 $(r+is)^2\equiv 1(\bmod q-1)$.所以 $\mathcal{M}_\ell=\{bx^{r+is}\mid 0\le i\le\ell-1,1\le r\le s,b^{r+is+1}=1,(r+is)^2\equiv 1(\bmod q-1)\}$,同理可得 $=\{bx^{r+is_1}\mid 0\le i\le\ell_1-1,1\le r\le s,b^{r+is_1+1}=1,(r+is_1)^2\equiv 1(\bmod q-1)\}$.由 $\mathcal{M}_\ell$ 和 $\mathcal{M}_{\ell,\ell_1}$ 的表达式易得 M_ℓ 和 M_{ℓ,ℓ_1}.

由 $\mathcal{F}_{\ell,\mathcal{R}_s}$,$\mathcal{M}_\ell$ 和 $\mathcal{G}_{\ell_1,\mathcal{R}_{s,s_1}}$ 的含义,易得

$$\mathcal{F}_{\ell,\mathcal{R}_s}=\mathcal{M}_\ell\bigcup_{\ell_1\text{跑遍}\ell\text{的因子}}\mathcal{G}_{\ell_1,\mathcal{R}_{s,s_1}}.\tag{11}$$

假设 $\mathcal{F}_{\ell_1,\mathcal{R}_{s,s_1}}$ 是 F_q 上所有形如 $x^rh(x^{s_1})$ 的对合组成的集合,其中 $1\le r\le s$.则由定理 3 可知,$|\mathcal{F}_{\ell,\mathcal{R}_s}|=N_{\ell,\mathcal{R}_s}$ 和 $|\mathcal{F}_{\ell_1,\mathcal{R}_{s,s_1}}|=N_{\ell_1,\mathcal{R}_{s,s_1}}$,其中

$$N_{\ell_1,\mathcal{R}_{s,s_1}}=\sum_{r\in\mathcal{R}_{s,s_1}}\sum_{\lambda=0}^{\lfloor\frac{\ell_1}{2}\rfloor}\frac{\ell_1!}{(\ell_1-2\lambda)!\ \lambda!\ 2^{\lambda}}\times\gcd(s_1,r+1)^{\ell_1-2\lambda}\times s_1^{\lambda}.\tag{12}$$

$\mathcal{F}_{\ell,\mathcal{R}_s}$ 和 $\mathcal{F}_{\ell_1,\mathcal{R}_{s,s_1}}$ 有以下性质.

命题 3 设 $\ell=\ell_1\ell_2,\overline{\ell}=\gcd(\ell_1,\ell_2),s=\frac{q-1}{\ell},s_1=\frac{q-1}{\ell_1},s_2=\frac{q-1}{\ell_2}$ 和 $\bar{s}=\frac{q-1}{\overline{\ell}}$.令 $\mathcal{F}_{\ell,\mathcal{R}_s}$,$\mathcal{F}_{\ell_1,\mathcal{R}_{s,s_1}}$ 定义如上.则(1)$\mathcal{F}_{\ell,\mathcal{R}_s}\cap\mathcal{F}_{\ell_1,\mathcal{R}_{s_1}}=\mathcal{F}_{\ell_1,\mathcal{R}_{s,s_1}}$;(2)$\mathcal{F}_{\ell,\mathcal{R}_s}\cap\mathcal{F}_{\ell_2,\mathcal{R}_{s_2}}=\mathcal{F}_{\ell_2,\mathcal{R}_{s,s_2}}$;(3)$\mathcal{F}_{\ell_1,\mathcal{R}_{s,s_1}}\cap\mathcal{F}_{\ell_2,\mathcal{R}_{s,s_2}}=\mathcal{F}_{\overline{\ell},\mathcal{R}_{s,\bar{s}}}$.

证明 对任意 $f_1(x)\in\mathcal{F}_{\ell,\mathcal{R}_s}\cap\mathcal{F}_{\ell_1,\mathcal{R}_{s_1}}$,由 $f_1(x)\in\mathcal{F}_{\ell_1,\mathcal{R}_{s_1}}$ 可知,存在 $1\le r_1\le s_1,{r_1}^2\equiv 1\ (\bmod s_1)$ 和

$b'_{\ell_1-1},\cdots,b'_1,b'_0\in F_q$ 使得 $f_1(x)=x^{r_1}(b'_{\ell_1-1}x^{(\ell_1-1)s_1}+b'_{\ell_1-2}x^{(\ell_1-2)s_1}+\cdots+b'_1x^{s_1}+b'_0)$. 又因 $f_1(x)\in\mathscr{F}_{\ell,\mathscr{R}_s}$,所以 $1\le r_1\le s$,并且

$$f_1(x)=x^{r_1}(b'_{\ell_1-1}x^{(\ell_1-1)\ell_2 s}+b'_{\ell_1-2}x^{(\ell_1-2)\ell_2 s}+\cdots+b'_1x^{\ell_2 s}+b'_0)\in\mathscr{F}_{\ell,\mathscr{R}_s}.$$

进而 $\mathscr{F}_{\ell,\mathscr{R}_s}\cap\mathscr{F}_{\ell_1,\mathscr{R}_{s_1}}=\mathscr{F}_{\ell_1,\mathscr{R}_{s,s_1}}$.类似地,可以证明 $\mathscr{F}_{\ell,\mathscr{R}_s}\cap\mathscr{F}_{\ell_2,\mathscr{R}_{s_2}}=\mathscr{F}_{\ell_2,\mathscr{R}_{s,s_2}}$.

下面说明 $\mathscr{F}_{\ell_1,\mathscr{R}_{s,s_1}}\cap\mathscr{F}_{\ell_2,\mathscr{R}_{s,s_2}}=\mathscr{F}_{\bar\ell,\mathscr{R}_{s,s}}$.一方面,由 $\bar\ell\mid\ell_1$ 和 $d\mid\ell_2$ 可知 $\mathscr{F}_{\bar\ell,\mathscr{R}_{s,s}}\subseteq\mathscr{F}_{\ell_1,\mathscr{R}_{s,s_1}}$ 和 $\mathscr{F}_{\bar\ell,\mathscr{R}_{s,s}}\subseteq\mathscr{F}_{\ell_2,\mathscr{R}_{s,s_2}}$,所以 $\mathscr{F}_{\bar\ell,\mathscr{R}_{s,s}}\subseteq\mathscr{F}_{\ell_1,\mathscr{R}_{s,s_1}}\cap\mathscr{F}_{\ell_2,\mathscr{R}_{s,s_2}}$.另一方面,令 $f(x)\in\mathscr{F}_{\ell_1,\mathscr{R}_{s,s_1}}\cap\mathscr{F}_{\ell_2,\mathscr{R}_{s,s_2}}$.则存在 $1\le r\le s$ 和 $b'_{\ell_1-1},\cdots,b'_1,b'_0,b''_{\ell_2-1},\cdots,b''_1,b''_0\in F_q$ 使得

$$f(x)=x^r(b'_{\ell_1-1}x^{(\ell_1-1)s_1}+b'_{\ell_1-2}x^{(\ell_1-2)s_1}+\cdots+b'_1x^{s_1}+b'_0)\in\mathscr{F}_{\ell_1,\mathscr{R}_{s,s_1}}$$

和

$$f(x)=x^r(b''_{\ell_2-1}x^{(\ell_2-1)s_2}+b''_{\ell_2-2}x^{(\ell_2-2)s_2}+\cdots+b''_1x^{s_2}+b''_0)\in\mathscr{F}_{\ell_2,\mathscr{R}_{s,s_2}}.$$

令 $\ell_1=\bar\ell\ell'_1$ 和 $\ell_2=\bar\ell\ell'_2$,则 $\gcd(\ell'_1,\ell'_2)=1$.进一步,$s_1=\dfrac{q-1}{\ell_1}=\dfrac{q-1}{\bar\ell\ell'_1}=\dfrac{\bar s}{\ell'_1}$ 和 $s_2=\dfrac{\bar s}{\ell'_2}$.通过比较 $f(x)$ 的系数可知,对于某些满足 $b'_{\ell_1-i}\ne0$ 的 i,存在 j 使得 $b''_{\ell_2-j}\ne0$ 并且满足 $(\ell_1-i)s_1=(\ell_2-j)s_2$. 也就是说,$(\ell_1-i)\ell'_2=(\ell_2-j)\ell'_1$.所以 $i\ell'_2=j\ell'_1$.因为 $\gcd(\ell'_1,\ell'_2)=1$,所以存在 ℓ' 使得 $i=\ell'_1\ell'$ 和 $j=\ell'_2\ell'$.所以,$f(x)$ 任意指数形如 $(\ell_1-\ell'_1\ell')s_1=(\bar\ell-\ell')\bar s$,也就是说,$f(x)\in\mathscr{F}_{\bar\ell,\mathscr{R}_{s,s}}$.

综上所述,$\mathscr{F}_{\ell_1,\mathscr{R}_{s,s_1}}\cap\mathscr{F}_{\ell_2,\mathscr{R}_{s,s_2}}=\mathscr{F}_{\bar\ell,\mathscr{R}_{s,s}}$.

由等式(11)可知,为计算 F_q 上指标为 ℓ,常数项为 0 的对合的个数,只需去掉 $\mathscr{F}_{\ell,\mathscr{R}_s}$ 中的单项式对合以及指标为 ℓ 的因子($\ne\ell$) 的对合即可.

定理 4　令 $\ell=p_1^{n_1}p_2^{n_2}\cdots p_m^{n_m}\mid q-1$,其中 $p_1,\cdots,p_m$ 是不同的素数,$n_1\ge n_2\ge\cdots\ge n_m$,$s=\dfrac{q-1}{\ell}$,对任意 $1\le i\le m$,$s_i=p_i^{n_i}s$.则 F_q 上指标为 ℓ,常数项为 0 的多项式对合的个数为

$$N_{\ell,\mathscr{R}_s}-M_\ell-\sum_{k=1}^{m}(-1)^{k+1}\Big(\sum_{1\le i_1<\cdots<i_k\le m}(N_{\bar\ell,\mathscr{R}_{s,s}}-M_{\ell,\bar\ell})\Big),$$

其中 $\bar\ell=\gcd\Big(\dfrac{\ell}{p_{i_1}},\cdots,\dfrac{\ell}{p_{i_k}}\Big)$,$\bar s=\dfrac{q-1}{\bar\ell}$,$N_{\ell,\mathscr{R}_s}$,$N_{\bar\ell,\mathscr{R}_{s,s}}$,$M_\ell$ 和 $M_{\ell,\bar\ell}$ 分别定义如(8)、(12)、(9) 和(10) 式.

证明　由等式(11)可知,只需从 $\mathscr{F}_{\ell,R_s}$ 中去掉单项式对合以及所有指标为 ℓ_1 的对合即可,其中 $\ell_1\ne\ell$ 跑遍 ℓ 的因子.而所有指标为 ℓ_1 的对合即为所有形如 $x^rh(x^{s_1})$ 的非单项式对合,其中 $s_1=\dfrac{q-1}{\ell_1}$.显然,ℓ 所有非 ℓ 的因子可以是 $\tilde\ell$ 的全部因子,其中 $\tilde\ell\in\Big\{\dfrac{\ell}{p_1},\dfrac{\ell}{p_2},\cdots,\dfrac{\ell}{p_m}\Big\}$.令 $A_i=\mathscr{F}_{\frac{\ell}{p_i},\mathscr{R}_{s,p_i^s}}\setminus\mathscr{M}_{\ell,\frac{\ell}{p_i}}$,$1\le i\le m$.则 $\mathscr{F}_{\ell,R_s}$ 中所有形如 $x^rh(x^{s_1})$ 的非单项式对合为 $\bigcup_{i=1}^m A_i$,其中 $s_1=\dfrac{q-1}{\ell_1}$,$\ell_1\ne\ell$ 跑遍 ℓ 的因子.由容斥原理可知,对有限集合 $A_1,\cdots,A_m$,有 $\Big|\bigcup_{i=1}^m A_i\Big|=\sum_{k=1}^{m}(-1)^{k+1}\Big(\sum_{1\le i_1<\cdots<i_k\le m}|A_{i_1}\cap\cdots\cap A_{i_k}|\Big)$.

由命题 3 可知,对任意 $1\le i_1<i_2<\cdots<i_k\le m$,

$$|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}|=|\mathscr{F}_{\bar\ell,\mathscr{R}_{s,s}}|-|\mathscr{M}_{\ell,\bar\ell}|,$$

其中 $\bar\ell=\gcd\Big(\dfrac{\ell}{p_{i_1}},\cdots,\dfrac{\ell}{p_{i_k}}\Big)$ 和 $\bar s=\dfrac{q-1}{\bar\ell}$.

所以,F_q 上指标为 ℓ,常数项为 0 的多项式对合的个数是

$$|\mathscr{F}_{\ell,\mathscr{R}_s}|-|\mathscr{M}_\ell|-\Big|\bigcup_{i=1}^m A_i\Big|=|\mathscr{F}_{\ell,\mathscr{R}_s}|-M_\ell-\sum_{k=1}^{m}(-1)^{k+1}\Big(\sum_{1\le i_1<\cdots<i_k\le m}(|\mathscr{F}_{\bar\ell,\mathscr{R}_{s,s}}|-M_{\ell,\bar\ell})\Big)=$$

$$N_{\ell,\mathcal{R}_s}-M_\ell-\sum_{k=1}^{m}(-1)^{k+1}\Big(\sum_{1\le i_1<\cdots<i_k\le m}(N_{\overline{\ell},\mathcal{R}_{s,s}}-M_{\ell,\overline{\ell}})\Big).$$

例 1 为检验定理 4 的正确性,首先利用 Magma 直接搜索得到 F_{25} 上指标为 2,3,4,6 对合的个数,发现与定理 4 计算得到的理论值一致.其次,利用定理 4 可以计算出 F_{25} 上指标为 8,12 对合的个数.详见表 1.在表 1 中,利用 Magma 直接搜索 F_{25} 上指标为 8,12 对合的个数分别需要至少穷尽 $25^8\approx 2^{37}$ 和 $25^{12}\approx 2^{56}$ 个循环,所以表 1 没有列出其实验值.

4 分圆映射对合的分类

上一节结合算法 1 和容斥原理,给出了有限域 F_q 上任意指标、常数为 0 的对合个数.考虑到对合构造目前已有较多结果,根据指标对其进行分类显得尤为重要.这不仅可以对已有结果进行梳理,避免后来研究者重复构造;而且便于考虑不同指标对合的密码学性质,为进一步应用提供有效指导.本节根据指标大小,对分圆映射对合进行分类,其中包括已有结果,以及利用算法 1 和对合定义得到的新结果.

表 1 F_{25} 中任意指标对合的个数

Tab.1 The number of involutions with any fixed index over F_{25}

q	ℓ	$\lvert\mathcal{G}_{\ell,\mathcal{R}_s}\rvert$	
		理论值	实验值
25	2	184	184
25	3	912	912
25	4	2 856	2 856
25	6	36 532	36 532
25	8	352 956	—
25	12	30 705 312	—

4.1 低指标对合

本节主要利用算法 1 给出低指标对合($\ell=2$ 和 3)的完全刻画.事实上,郑大彬等[9]利用定理 2,给出了 $x^rh(x^{\frac{q-1}{2}})$ 对合性质的完全刻画.此时因为 $\ell=2$ 是素数,所以此类对合也是 F_q 上指标为 2,常数项为 0 对合的完全刻画.

定理 5[9](命题3.1) 设 q 是奇素数幂,$a,b\in F_q$ 且 $a\neq b$,$f(x)=\frac{a-b}{2}x^{\frac{q-1}{2}+r}+\frac{a+b}{2}x^r$.则 $f(x)$ 是 F_q 上的对合当且仅当

(1) $r^2\equiv 1 \bmod \frac{q-1}{2}$;

(2) $\frac{a-b}{2}a^{\frac{q-1}{2}+r}+\frac{a+b}{2}a^r=1$ 和 $(-1)^r\frac{a-b}{2}b^{\frac{q-1}{2}+r}+\frac{a+b}{2}b^r=(-1)^{\frac{2(r2-1)}{q-1}}$.

下面利用算法 1,给出更具体的刻画.

定理 6 设 $2\mid q-1$,$f(x)=x^rh(x^s)$,其中 $s=\frac{q-1}{2}$ 和 $h(x)=b_1x+b_0\in F_q[x]$.则 $f(x)$ 是 F_q 上的对合当且仅当

$$\begin{cases}b_1=\frac{1}{2}(\gamma^{2e_0+\varphi(0)}-\gamma^{2e_1+\varphi(1)-r}),\\ b_0=\frac{1}{2}(\gamma^{2e_0+\varphi(0)}+\gamma^{2e_1+\varphi(1)-r}),\end{cases}$$

其中 $r^2\equiv 1(\bmod s)$,φ,(e_0,e_1) 满足下述条件之一:

(1)当 $\varphi=\mathrm{id}$ 时,$(e_0,e_1)=(\frac{j_0s}{\gcd(s,r+1)},\frac{j_1s}{\gcd(s,r+1)})$,其中 $1\le j_0,j_1\le\gcd(s,r+1)$.

(2)当 $\varphi=(01)$ 时,$(e_0,e_1)=(e_0,-re_0(\bmod s))$,其中 $1\le e_0\le s$.

证明 假定 φ 已经给定并且已经计算得到 e_i,则由方程(4)可得 $\boldsymbol{AX}=\boldsymbol{R}$,其中

$$\boldsymbol{A}=\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix},\boldsymbol{X}=\begin{pmatrix}b_1\\ b_0\end{pmatrix}\text{和}\boldsymbol{R}=\begin{pmatrix}\gamma^{2e_0+\varphi(0)}\\ \gamma^{2e_1+\varphi(1)-r}\end{pmatrix},\text{显然}\boldsymbol{A}^{-1}=\frac{1}{2}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}.$$

进一步,

$$\boldsymbol{X}=\begin{pmatrix}b_1\\ b_0\end{pmatrix}=\boldsymbol{A}^{-1}\boldsymbol{R}=\frac{1}{2}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}\begin{pmatrix}\gamma^{2e_0+\varphi(0)}\\ \gamma^{2e_1+\varphi(1)-r}\end{pmatrix}=\frac{1}{2}\begin{pmatrix}\gamma^{2e_0+\varphi(0)}-\gamma^{2e_1+\varphi(1)-r}\\ \gamma^{2e_0+\varphi(0)}+\gamma^{2e_1+\varphi(1)-r}\end{pmatrix}.$$

下面主要考虑 φ 和(e_0,e_1).

情况(1)　$\varphi=\mathrm{id}$. 此时,方程组(2)变为

$$\begin{cases}e_0+re_0\equiv 0\ (\mathrm{mod}\ s),\\ e_1+re_1\equiv 0\ (\mathrm{mod}\ s),\end{cases}\tag{13}$$

由引理 3 可知,方程(13)的解为 $(e_0,e_1)=(\dfrac{j_0 s}{\gcd(s,r+1)},\dfrac{j_1 s}{\gcd(s,r+1)})$,其中 $1\le j_i\le\gcd(s,r+1)$.

情况(2)　$\varphi=(01)$. 此时,方程组(2)变为

$$\begin{cases}e_0+re_1\equiv 0\ (\mathrm{mod}\ s),\\ re_0+e_1\equiv 0\ (\mathrm{mod}\ s),\end{cases}\tag{14}$$

由引理 4 可知,方程(14)的解为 $(e_0,e_1)=(e_0,-re_0(\mathrm{mod}\ s))$,其中 $1\le e_0\le s$.

综上所述,此定理成立.

对于指标为 3,常数项为 0 的对合,文献[9]也给出了相应的充分必要条件.但因为文献[9]没有得到方程组(3)解的具体表达式,所以利用本文的算法 1 可以得到更加确切的结果.

定理 7　设 $3\mid q-1$,$f(x)=x^r h(x^s)$,其中 $s=\dfrac{q-1}{3}$ 和 $h(x)=b_2x^2+b_1x+b_0\in F_q[x]$.则 $f(x)$ 是 F_q 上的对合当且仅当

$$\begin{cases}b_2=\dfrac{1}{3}(\gamma^{3e_0+\varphi(0)}+\gamma^{3e_1+\varphi(1)-r+s}+\gamma^{3e_2+\varphi(2)-2r+2s}),\\ b_1=\dfrac{1}{3}(\gamma^{3e_0+\varphi(0)}+\gamma^{3e_1+\varphi(1)-r+2s}+\gamma^{3e_2+\varphi(2)-2r+s}),\\ b_0=\dfrac{1}{3}(\gamma^{3e_0+\varphi(0)}+\gamma^{3e_1+\varphi(1)-r}+\gamma^{3e_2+\varphi(2)-2r}),\end{cases}$$

其中 $r^2\equiv 1(\mathrm{mod}\ s)$,$\varphi$,$(e_0,e_1,e_2)$ 满足下述条件之一:

(1)当 $\varphi=\mathrm{id}$ 时,$(e_0,e_1,e_2)=\left(\dfrac{j_0 s}{\gcd(s,r+1)},\dfrac{j_1 s}{\gcd(s,r+1)},\dfrac{j_2 s}{\gcd(s,r+1)}\right)$,其中 $1\le j_0,j_1,j_2\le\gcd(s,r+1)$.

(2)当 $\varphi=(12)$ 时,$(e_0,e_1,e_2)=\left(\dfrac{j_0 s}{\gcd(s,r+1)},e_1,-re_1(\mathrm{mod}\ s)\right)$,其中 $1\le j_0\le\gcd(s,r+1)$ 和 $1\le e_1\le s$.

(3)当 $\varphi=(01)$ 时,$(e_0,e_1,e_2)=\left(e_0,-re_0(\mathrm{mod}\ s),\dfrac{j_2 s}{\gcd(s,r+1)}\right)$,其中 $1\le j_2\le\gcd(s,r+1)$ 和 $1\le e_0\le s$.

(4)当 $\varphi=(02)$ 时,$(e_0,e_1,e_2)=\left(e_0,\dfrac{j_1 s}{\gcd(s,r+1)},-re_0(\mathrm{mod}\ s)\right)$,其中 $1\le j_1\le\gcd(s,r+1)$ 和 $1\le e_0\le s$.

证明　与定理 6 的证明类似,首先假定 φ 已经给定并且已经计算得到 e_i,则由方程(4)可得 $\boldsymbol{AX}=\boldsymbol{R}$,其中

$$\boldsymbol{A}=\begin{pmatrix}1 & 1 & 1\\ \zeta^2 & \zeta & 1\\ \zeta & \zeta^2 & 1\end{pmatrix},\boldsymbol{X}=\begin{pmatrix}b_2\\ b_1\\ b_0\end{pmatrix},\boldsymbol{R}=\begin{pmatrix}\gamma^{3e_0+\varphi(0)}\\ \gamma^{3e_1+\varphi(1)-r}\\ \gamma^{3e_2+\varphi(2)-2r}\end{pmatrix},\text{显然,}\boldsymbol{A}^{-1}=\frac{1}{3}\begin{pmatrix}1 & \zeta & \zeta^2\\ 1 & \zeta^2 & \zeta\\ 1 & 1 & 1\end{pmatrix}.$$

进一步,

$$\boldsymbol{X}=\begin{pmatrix}b_2\\b_1\\b_0\end{pmatrix}=\boldsymbol{A}^{-1}\boldsymbol{R}=\frac{1}{3}\begin{pmatrix}1&\zeta&\zeta^2\\1&\zeta^2&\zeta\\1&1&1\end{pmatrix}\begin{pmatrix}\gamma^{3e_0+\varphi(0)}\\\gamma^{3e_1+\varphi(1)-r}\\\gamma^{3e_2+\varphi(2)-2r}\end{pmatrix}=\frac{1}{3}\begin{pmatrix}\gamma^{3e_0+\varphi(0)}+\gamma^{3e_1+\varphi(1)-r+s}+\gamma^{3e_2+\varphi(2)-2r+2s}\\\gamma^{3e_0+\varphi(0)}+\gamma^{3e_1+\varphi(1)-r+2s}+\gamma^{3e_2+\varphi(2)-2r+s}\\\gamma^{3e_0+\varphi(0)}+\gamma^{3e_1+\varphi(1)-r}+\gamma^{3e_2+\varphi(2)-2r}\end{pmatrix}.$$

下面考虑 φ 和(e_0,e_1,e_2).由引理 2,只需考虑$\lfloor\frac{\ell}{2}\rfloor+1=2$ 种情况,也就是,$\varphi=\mathrm{id}$ 和 $\varphi=(12)$.事实上,情况 $\varphi=(01)$ 和 $\varphi=(02)$ 皆与 $\varphi=(12)$ 共轭.

情况(1) $\varphi=\mathrm{id}$. 此时,方程组(2)变为

$$\begin{cases}e_0+re_0\equiv 0\ (\mathrm{mod}\ s),\\e_1+re_1\equiv 0\ (\mathrm{mod}\ s),\\e_2+re_2\equiv 0\ (\mathrm{mod}\ s),\end{cases}\tag{15}$$

由引理 3 可知,方程组(15)的解为

$$(e_0,e_1,e_2)=\left(\frac{j_0 s}{\gcd(s,r+1)},\frac{j_1 s}{\gcd(s,r+1)},\frac{j_2 s}{\gcd(s,r+1)}\right),$$

其中 $1\le j_i\le\gcd(s,r+1)$.

情况(2) $\varphi=(12)$. 此时,方程组(2)变为

$$\begin{cases}e_0+re_0\equiv 0\ (\mathrm{mod}\ s),\\re_1+e_2\equiv 0\ (\mathrm{mod}\ s),\\e_1+re_2\equiv 0\ (\mathrm{mod}\ s),\end{cases}\tag{16}$$

也就是,

$$\boldsymbol{M}\boldsymbol{X}=\boldsymbol{T},\tag{17}$$

其中 $\boldsymbol{M}=\begin{pmatrix}r+1&0&0\\0&r&1\\0&1&r\end{pmatrix},\boldsymbol{X}=\begin{pmatrix}e_0\\e_1\\e_2\end{pmatrix},\boldsymbol{T}=\begin{pmatrix}st_0\\st_1\\st_2\end{pmatrix}$.

由引理 3 和引理 4 可知,方程组(17)的解是 $(e_0,e_1,e_2)=(\frac{j_0 s}{\gcd(s,r+1)},e_1,-re_1(\mathrm{mod}\ s))$,其中 $1\le j_0\le\gcd(s,r+1)$ 和 $1\le e_1\le s$.

至于情况 $\varphi=(01)$ 和 $\varphi=(02)$,可以参考情况(2) 直接写出结果.当 $\varphi=(01)$ 时,

$$(e_0,e_1,e_2)=(e_0,-re_0(\mathrm{mod}\ s),\frac{j_2 s}{\gcd(s,r+1)}),$$

其中 $1\le j_2\le\gcd(s,r+1)$ 和 $1\le e_0\le s$.当 $\varphi=(02)$ 时,

$$(e_0,e_1,e_2)=(e_0,\frac{j_1 s}{\gcd(s,r+1)},-re_0(\mathrm{mod}\ s)),$$

其中 $1\le j_1\le\gcd(s,r+1)$ 和 $1\le e_0\le s$.

综上所述,此定理成立.

4.2 其他指标对合

上一节利用算法 1 给出了 F_q 上形如$x^rh(x^{\frac{q-1}{2}})$ 和 $x^rh(x^{\frac{q-1}{3}})$ 对合性质的完全刻画.显然,利用算法 1 可以高效地刻画出指标较小的对合.对于其他指标情形,需要考虑利用其他方法构造对合.下面首先对已有结果进行总结.

设 $q-1=\ell s$,$f(x)=x^rh(x^s)\in F_q[x]$ 和 $g(x)=x^rh(x)^s$.郑大彬等在文献[9]推论 2.3 中证明如果 $f(x)$ 是 F_q 上的对合,则 $g(x)$ 是 μ_ℓ 上的对合.反过来,从 μ_ℓ 上的对合出发,结合定理 2,可以构造 F_q 上形如 $x^rh(x^s)$ 的对合.在文献[9]中,郑大彬等从 μ_ℓ 上的对合单项式 $g(x)=x^r$,$g(x)=x^{-1}$ 和 $g(x)=x$ 出发构造三类 F_q 上形如 $x^rh(x^s)$ 的对合.具体构造如下.

(1)令 $r\equiv -1(\bmod q-1)$,$h(x)\in F_{q^2}[x]$ 满足对任意 $\beta\in\mu_{q+1}$,有 $\beta^{\frac{r^2-1}{q-1}}h(\beta^r)=h(\beta)\in F_q$ 并且 $h(\beta)\neq 0$,则 $f(x)=x^rh(x^{q-1})$ 是 F_{q^2} 上的对合[9](定理4.1).此时,$g(x)=x^rh(x)^{q-1}=x^r$.

(2)令 $\ell\mid \gcd(q-1,m)$,$s=\dfrac{q^m-1}{\ell}$,$r\equiv -1(\bmod s)$,$e\equiv\dfrac{r^2-1}{s}(\bmod \ell)$ 且 $0\leq e\leq d-1$.令 $h(x)=\sum_{0\leq i\leq \ell}h_ix^i\in F_q[x]$ 满足对任意 $0\leq i\leq e$,$h_{e-i}=h_i$ 和对任意 $e+1\leq i\leq \ell-1$,$h_{\ell+e-i}=h_i$.并且 $h(x)$ 在 μ_ℓ 上无根,则 $f(x)=x^rh(x^s)$ 是 F_{q^m} 上的对合[9](定理4.4).此时,$g(x)=x^rh(x)^s=x^{-1}$.

(3)令 $r\equiv -1(\bmod q-1)$,$d\equiv r-1(\bmod q+1)$,$h(x)\in F_{q^2}[x]$ 满足 $\deg h(x)=d$,$h(0)\neq 0$ 并且对 $\forall x\in F_{q^2}^*$,$(x^dh(x^{-1}))^q=h(x^q)$,则 $f(x)=x^rh(x^{q-1})$ 是 F_{q^2} 上的对合.此时,$g(x)=x^rh(x)^{q-1}=x$.

此外,Charpin 等学者[11]对 F_{2^n} 上线性化多项式和 Dickson 多项式的对合性质进行研究.这两类多项式对合性质的研究主要依赖于对合的定义,即对合的复合逆等于自身或者自身与自身的复合等于恒等映射.并且,利用引理 1 可以计算发现这些对合的指标属于非低指标情形.具体的构造性结果如下.

(1)令 $f(x)=x^{2^i}(bx^{2^i(2^m-1)}+a)\in F_{2^{2m}}[x]$,其中 $i=0$ 且 $a^2+b^{2^m+1}=1$ 或 $m=2i$,$ab^{2^i}+a^{2^{3i}}b=1$ 且 $a^{2^i+1}+b^{2^{3i}+1}=0$,则 $f(x)$ 是 $F_{2^{2m}}$ 上的对合[11](命题3.11).此时 $f(x)$ 的指标是 2^m+1.

(2)令 $f(x)=x+ax^{2^m}+ax^{2^{3m}}$,其中 $a\in F_{2^m}^*$,则 $f(x)$ 是 $F_{2^{4m}}$ 上的对合[11](命题3.14(iii)).此时 $f(x)$ 的指标是 $2^{3m}+2^{2m}+2^m+1$.

(3)令 $f(x)=x+\gamma \mathrm{Tr}_{km/m}(x)$,其中 $\mathrm{Tr}_{km/m}(\gamma)=0$,$\mathrm{Tr}_{km/m}(\cdot)$ 是 $F_{2^{km}}$ 到 F_{2^m} 的相对迹函数,则 $f(x)$ 是 $F_{2^{km}}$ 上的对合[11](推论4.7).此时 $f(x)$ 的指标是 $\sum_{i=0}^{k-1}2^{im}$.

(4)令 $D_k=\sum_{i=0}^{\lfloor k/2\rfloor}\dfrac{k}{k-i}\binom{k-i}{i}x^{k-2i}\in F_2[x]$,$S:=\{u\mid 1\leq u\leq 2^n-2,u^2\equiv 1\ (\bmod\ 2^n-1)\}$,则 D_k 是 F_{2^m} 上的对合当且仅当(i) 若 m 是奇数,则 $k\in S$;(ii) 若 m 是偶数,则 $k\in S\cup 2^{m/2}S$[11](定理3.5).此时 $f(x)$ 的指标是 2^m-1.

2017 年,Xu 等[12]利用 Charpin 等[11]提出的"piece by piece"构造法,给出了一类 4 差分对合;同年,Fu 等[13]总结了已有 4 差分置换是对合的可能性,主要研究方法是对合的定义.由引理 1 以及这些分段函数的多项式表达形式可知这些对合都是高指标对合,详见表 2.

表 2　部分高指标对合已有结果

Tab.2　Some known results of involutions with high index

对合	多项式表示	所在域	指标	出处
$x^{-1}+\mathbf{1}_U(x),U=\{0,1\}$	$x^{-1}+(x^2+x)^{2^n-1}+1$	F_{2^n}	2^n-1	[13](表 1)
$x^{-1}+\mathbf{1}_U(x),U=\{\omega,\omega^2\}$	$x^{-1}+(x^2+x+1)^{2^n-1}+1$	F_{2^n}	2^n-1	[13](表 1)
$x^{-1}+\mathbf{1}_U(x),U=\{0,1,\omega,\omega^2\}$	$x^{-1}+(x^4+x)^{2^n-1}+1$	F_{2^n}	2^n-1	[13](表 1)
$\begin{cases}\beta(x+1)^{-1}+\alpha,\text{如果 } x\in F_{2^d}\\ x^{-1},\text{如果 } x\in F_{2^n}\backslash F_{2^d}\end{cases}$	$x^{-1}(x^{2^d}+x)^{2^n-1}+$ $(\beta(x+1)^{-1}+\alpha)((x^{2^d}+x)^{2^n-1}+1)$	F_{2^n}	2^n-1	[13](表 1)
$\begin{cases}\beta x^{-1}+\alpha,\text{如果 } x\in F_{2^d}\\ x^{-1},\text{如果 } x\in F_{2^n}\backslash F_{2^d}\end{cases}$	$x^{-1}(x^{2^d}+x)^{2^n-1}+$ $(\beta x^{-1}+\alpha)((x^{2^d}+x)^{2^n-1}+1)$	F_{2^n}	2^n-1	[13](表 1)
$\begin{cases}(\gamma x)^{-1},\text{如果 } x\in U\\ x^{-1},\text{如果 } x\in F_{2^n}\backslash U\end{cases}$	$x^{-1}(\prod_{a\in U}(x-a))^{2^n-1}+$ $(\gamma x)^{-1}((\prod_{a\in U}(x-a))^{2^n-1}+1)$	F_{2^n}	2^n-1	[13](表 1)
$\begin{cases}(x+1)^{-1}+1,\text{如果 } x\in U\\ x^{-1},\text{如果 } x\in F_{2^n}\backslash U\end{cases}$	$x^{-1}(\prod_{a\in U}(x-a))^{2^n-1}+$ $((x+1)^{-1}+1)((\prod_{a\in U}(x-a))^{2^n-1}+1)$	F_{2^n}	2^n-1	[12](构造 1)

上面总结了到目前为止已有的非低指标对合的构造结果.由表 1 可知,给定指标对合的个数随着指标大

小的增加而增大,也就是说,还存在大量非低指标对合还未发现.下面利用一个置换多项式复合逆结果,得到一类 F_{q^2} 上形如 $x^rh(x^{q-1})$ 的对合.由对合的定义可知,对于置换多项式 $f(x)\in F_q[x]$,如果 $f^{-1}(x)=f(x)$,则 $f(x)$ 是对合.2018 年,文献[14] 中提出一种计算 F_q 上形如 $x^rh(x^s)$ 的置换多项式复合逆的新方法,并给出了下述结果.

引理 5[14](定理3.2) 设 $s\mid(q-1)$,$h(x)\in F_q[x]$ 满足对任意 $\zeta\in\mu_{(q-1)/s}$,$h(\zeta)^s=\zeta^n$ 成立.假设 $\gcd(r+n,(q-1)/s)=\gcd(r,q-1)=1$ 且 r',r'' 满足 $(r+n)r'\equiv 1\pmod{(q-1)/s}$ 和 $rr''\equiv 1\pmod{(q-1)}$.则 $f(x)=x^rh(x^s)$ 置换 F_q,并且 $f(x)$ 在 F_q 上的复合逆为 $f^{-1}(x)=(x^{q-s}h(x^{sr'})^{s-1})^{r''}x^{sr'}$.

由上述引理,可以得到一类 F_{q^2} 上形如 $x^rh(x^{q-1})$ 的对合.

定理 8 设 $q-1=s\ell$,$h(x)\in F_q[x]$ 满足对任意 $\zeta\in\mu_\ell$,$h(\zeta)^s=\zeta^2$.则 $f(x)=x^{q-2}h(x^s)$ 是 F_q 上的对合.

证明 在引理 5 中,$r=-1$,$n=2$.则 $r'=1$ 和 $r''=-1$.所以,

$$f^{-1}(x)=(x^{q-s}h(x^s)^{s-1})^{-1}x^s=x^{2s-1}h(x^s)x^{-2s}=x^{-1}h(x^s)=f(x).$$

下面给出定理 8 中对合的一些具体例子.令 $f(x)=x^{q^2-2}h(x^{q-1})\in F_{q^2}[x]$,其中 $h(x)=b_qx^q+b_{q-1}x^{q-1}+\cdots+b_1x+b_0$.首先确定 $b_i(0\le i\le q)$ 使得 $h(x)$ 满足对任意 $\zeta\in\mu_{q+1}$,$h(\zeta)^{q-1}=\zeta^n$ 成立.由 $h(\zeta)^{q-1}=\zeta^n$ 可知 $(b_q\zeta^q+b_{q-1}\zeta^{q-1}+\cdots+b_1\zeta+b_0)^q=\zeta^n(b_q\zeta^q+b_{q-1}\zeta^{q-1}+\cdots+b_1\zeta+b_0)$.进一步 $b_q^q\zeta+b_{q-1}^q\zeta^2+\cdots+b_1^q\zeta^q+b_0^q=b_{q-n}\zeta^q+b_{q-n-1}\zeta^{q-1}+\cdots+b_{q+2-n}\zeta+b_{q+1-n}$.所以,

$$(b_1^q-b_{q-n})\zeta^q+(b_2^q-b_{q-n-1})\zeta^{q-1}+\cdots+(b_q^q-b_{q+2-n})\zeta+b_0^q-b_{q+1-n}=0. \tag{18}$$

因为上述方程对任意 $\zeta\in\mu_{q+1}$ 皆成立,所以对任意 $0\le i,j\le q$,$i+j\equiv -n\pmod{q+1}$,有

$$b_i^q=b_j.$$

引理 6 设 $h(x)=b_qx^q+b_{q-1}x^{q-1}+\cdots+b_1x+b_0\in F_{q^2}[x]$.则对任意 $\zeta\in\mu_{q+1}$,$h(\zeta)^{q-1}=\zeta^n$ 成立当且仅当 $b_i^q=b_j$,其中 $0\le i,j\le q$,$i+j\equiv -n\pmod{q+1}$ 并且对任意 $\zeta\in\mu_{q+1}$,$h(\zeta)\ne 0$.

结合引理 6 和定理 8 可得

定理 9 令 $f(x)=x^{q^2-2}h(x^{q-1})\in F_{q^2}[x]$,其中 $h(x)=b_qx^q+b_{q-1}x^{q-1}+\cdots+b_1x+b_0$.并且对任意 $\zeta\in\mu_{q+1}$,$h(\zeta)\ne 0$.此外,$b_i^q=b_j$ 成立,其中 $0\le i,j\le q$ 和 $i+j\equiv -2\pmod{q+1}$.则 $f(x)$ 是 F_{q^2} 上的对合.

5 总结以及进一步工作

本文主要分析了有限域上形如 $f(x)=x^rh(x^s)$ 的对合,并根据指标对已有对合进行了分类并且构造几类新的对合.首先对郑大彬等[9]的方法进行深入分析.利用对称群中共轭关系和分块矩阵的思想,给出了方程组(3)解的确切表达式,改进了郑大彬等的方法;在此基础上,给出有限域上任意固定指标、常数为 0 的对合个数.此外,考虑到目前为止已经得到的对合数量之多,根据指标对已有对合进行分类就显得尤为重要,不仅可以对已有结果进行梳理,避免后来研究者重复构造,而且可以考虑不同指标对合的密码学性质,为进一步的应用提供有效指导.所以,本文根据指标大小对对合结果进行分类,其中包括已有结果和新结果.

除此之外,想要将对合应用到分组密码的设计中,还应当考虑对合的其他密码学性质,比如差分均匀度和非线性度.所以考虑指标与差分均匀度和非线性度的关系是下一步研究的重点.

参 考 文 献

[1] Akbary A,Ghioca D,Wang Q. On permutation polynomials of prescribed shape[J].Finite Fields and Their Applications,2009,15(2):195-206.

[2] Gao Z,Wang Q.A probabilistic approach to value sets of polynomials over finite fields[J].Finite Fields and Their Applications,2015,33:160-174.

[3] Wan D,Wang Q.Index bounds for character sums of polynomials over finite fields[J].Designs,Codes and Cryptography,2016,81(3):459-468.

[4] Wan D,Lidl R.Permutation polynomials of the form $x^rf(x^{(q-1)/d})$ and their group structure[J].Monatshefte für Mathematik,1991,112(2):149-163.

[5] Hou X.Permutation polynomials over finite fields—a survey of recent advances[J].Finite Fields and Their Applications，2015，32：82-119.
[6] Li N，Zeng X.A survey on the applications of Niho exponents[J].Cryptography and Communications，2019，11(3)：509-548.
[7] Coulter R S，Mesnager S.Bent Functions From Involutions Over F_{2^n} [J].IEEE Transactions on Information Theory，2018，64(4)：2979-2986.
[8] Wang Q.A note on inverses of cyclotomic mapping permutation polynomials over finite fields[J].Finite Fields and Their Applications，2017，45：422-427.
[9] Zheng D，Yuan M，Li N，et al.Constructions of involutions over finite fields[J/OL].[2019-01-16].http://xueshu.baidu.com/usercenter/paper/show? paperid=1h1u0ap04y3t0020180g0ap05y620190&site=xueshu_se.
[10] 冯克勤，李尚志，章璞.近世代数引论[M].3 版.合肥：中国科技大学出版社，2009：25-30.
[11] Charpin P，Mesnager S，Sarkar S.Involutions Over the Galois Field F_{2^n} [J].IEEE Transactions on Information Theory，2016，62(4)：2266-2276.
[12] Xu Y，Li Y，Wu C，et al.On the construction of differentially 4-uniform involutions[J].Finite Fields and Their Applications，2017，47：309-329.
[13] Fu S，Feng X.Involutory differentially 4-uniform permutations from known constructions[J].Designs，Codes and Cryptography，2019，87(1)：31-56.
[14] Li K，Qu L，Wang Q.Compositional inverses of permutation polynomials of the form $x^rh(x^s)$ over finite fields[J].Cryptography and Communications，2019，11(2)：279-298.

Constructions，counts and classifications of cyclotomic involutions over finite fields

Qu Longjiang，Li Kangquan

(College of Liberal Arts and Sicences，National University of Defense Technology，Changsha 410073，China)

Abstract：Since any polynomials $f(x)$ over finite fields can be written uniquely as $x^rh(x^s)+f(0)$，based on this form，Wang et al. presented a new concept called the index of polynomials in 2009. Since it was proposed，this parameter has turned out to be very useful in studying value set size of polynomials，character sum，permutation polynomials，among others. Involutions play very important roles in the design of block ciphers. For the past two years，in order to provide more S-boxes for block ciphers，several scholars did some research about involutions. Recently Zheng et al. studied involutions of the form $x^rh(x^s)$ over F_q providing a necessary and sufficient condition of this polynomials to be involutary and presenting a method to construct involutions with this form. However，the method needs to solve one equation system，i.e.，(3).

In this paper，we firstly improve the method of Zheng et al.，obtaining the explicit solutions of the equation system using the conjugacy relation over symmetric group and the idea of block matrices secondly we give the number of involutions with any fixed index and constant term 0. Thirdly according to the index，known involutions with explicit expression are classified. Finally，we determine several classes of involutions，enriching the known results. Specifically，aiming at the involutions of low indexes，more specific involutary conditions of index 2 and 3 are given than the results of Zheng et al. For involutions with high indexes，using the compositional results obtained by us before，we give a class of involutions of the form $x^rh(x^{q-1})$ over F_{q^2}.

Keywords：finite fields；index；involutions；classification

[责任编校　陈留院　赵晓华]

本 期 专 家 介 绍

屈龙江，国防科技大学数学系教授，博士，博士生导师.2017 年获得国家自然科学基金优秀青年基金，主持国家自然科学基金优秀青年基金等 10 余项项目，主要从事编码密码理论及其应用研究工作，在密码函数的安全性指标分析、对称密码算法安全性分析等方面取得一系列研究成果，在 *IEEE Trans on Inform Theory*，*SIAM J Dis Math* 等国内外著名学术期刊和 CRYPTO，FSE 等国内外高水平学术会议上发表学术论文 70 余篇，其中 SCI 论文 40 余篇，在科学出版社出版专著和教材各 1 部.入选教育部新世纪优秀人才计划和国防科技大学首届青年拔尖人才计划.获中国密码学会优秀青年奖，获国家教学成果二等奖和湖南省自然科学二等奖各 1 项.

杨震宇，南昌大学化学学院教授，博士，博士生导师.主要从事新能源材料及生物质材料高效利用等相关研究工作，对新能源材料的制备、生物质高效利用方法与思路以及高附加值化都有一定认识和经验.学习经历：河南师范大学化学学院本科、硕士（1995－2002）；中国科学院理化技术研究所博士（2002－2005）；北京大学访问学者，美国伦斯勒理工学院博士后及新加坡理工大学访问学者.工作经历：2005 年加入南昌大学，2011 年晋升教授职称；先后入选江西省中青年学科带头人、赣江特聘教授.主持完成 10 余项自然科学研究项目（包括 4 项国家自然科学基金，1 项江西省锂电重大专项项目）.在国内外学术刊物 *Energy Storage Materials*，*Carbon*，*J Power Sources*，*J Phys Chem*，*Nano Energy*，*Chemelectrochem* 等发表论文 100 余篇，其中 SCI 论文 69 篇，申请专利 10 余件.

我刊微信公众号已开通您可搜索“河南师范大学学报自然科学版”或扫描二维码关注.感谢您的关注！欢迎向我刊投稿.