Hermitian LCD 2-拟交换群码的渐近性研究

张光辉
（宿迁学院数理学院，江苏宿迁 223800）

摘 要： 利用有限域上群代数的性质构造了一类Hermitian LCD（Hermitian Linear Complementary Dual）2-拟交换群码. 基于有限域上群代数的结构定理精确计算出了此类码的个数. 通过探讨相对最小距离较小的此类码的计数问题，本文证明了有限域上的Hermitian LCD 2-拟交换群码是渐近好码.

关键词： 有限域；2-拟交换群码；Hermitian LCD 码；渐近好码
基金项目： 非线性分析及其应用教育部重点实验室（华中师范大学）开放课题；宿迁市科技计划（No.Z2023130）
中图分类号： TN914；O236.2 **文献标识码：** A **文章编号：** 0372-2112(2025)06-1923-09
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20240157

Asymptotically Good Hermitian LCD 2-Quasi-Abelian Codes

ZHANG Guang-hui
(*School of Mathematics and Physics*, *Suqian University*, *Suqian*, *Jiangsu* 223800, *China*)

Abstract: Utilizing properties of group algebras over finite fields, we construct a class of Hermitian linear complementary dual (LCD) 2-quasi-abelian codes. Employing the structure theorem for group algebras over finite fields, we explicitly determine the number of such codes. By investigating the enumeration of codes within this class that possess small relative minimum weights, we demonstrate that the class of Hermitian LCD 2-quasi-abelian codes over any finite field is asymptotically good.

Key words: finite fields; quasi-abelian codes of index 2; Hermitian LCD codes; asymptotically good codes
Foundation Item(s): Open Research Fund of Key Laboratory of Nonlinear Analysis & Applications (Central China Normal University), Ministry of Education, China; Suqian Science & Technology Program (No.Z2023130)

1 引言

设 F 是有限域，n 是正整数，F^n 是 F 上的 n 维向量空. 向量 $\boldsymbol{a}=(a_1, a_2, \cdots, a_n)$，定义 $\boldsymbol{a}$ 的汉明（Hamming）重量 $w(\boldsymbol{a})$ 为非零分量 a_i 的个数. 对于 $\boldsymbol{a}, \boldsymbol{b}\in F^n$，$\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的汉明（Hamming）距离 $d(\boldsymbol{a}, \boldsymbol{b})$ 定义为向量 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 不同分量的个数，即 $d(\boldsymbol{a}, \boldsymbol{b})=w(\boldsymbol{a}-\boldsymbol{b})$. F 上的线性码 C 是指向量空间 F^n 的一个线性子空间，C 中的向量称为码字. 线性码 C 的维数 k 是指它作为 F-向量空间的维数，C 的最小汉明重量 $w(C)$ 定义为 C 中所有非零码字汉明重量的最小值，C 的最小汉明距离 $d(C)$ 定义为 C 中任意两个不同码字之间汉明距离的最小值. 线性码 C 的最小汉明重量 $w(C)$ 等于最小汉明距离 $d(C)$[1,2]. 如果线性码 C 的维数为 k，最小汉明距离为 d，那么称线性码 C 是一个 $[n, k, d]$ 线性码，这里 n 称为线性码 C 的码长，k 表示码的信息位数，k/n 表示线性码 C 的码率（又称信息率），记作 $R(C)$；d 用于刻画线性码 C 的检错能力和纠错能力，d/n 表示线性码 C 的相对最小距离，记作 $\Delta(C)$.

信息论中著名的Shannon定理[3]指出，对于任意的 $\varepsilon>0$，总存在一个线性码，它的码率大于一个固定的正数，使得字差错率 $<\varepsilon$. 满足这些条件的码称为Shannon码. 具体构造出一列Shannon码是一个很困难的问题. 对于一个线性码，当码长和维数一定时，最小汉明距离越大，它的纠错和检错能力就越大. 因此对于一列 $[n_i, k_i, d_i]$ 线性码，如果 n_i 趋于无穷大，要保证纠错能力和检错能力，相对最小距离应该不趋于0. 在实际构造中，要达到Shannon定理的效果，就是要找到这样一列无穷多个 $[n_i, k_i, d_i]$ 线性码，使得码长趋于无穷大，同时它们的码率和相对最小距离都大于0. 这样一系列码称为渐近好码. 从实用上来讲，渐近好码可以在保持一定的信息率下，使得信息传输中字错率越来越小，故其实用价值是显然的. 从理论上来讲，构造渐近好码本身是

收稿日期：2024-02-17；修回日期：2024-12-09；责任编辑：李勇锋

一个构造性的数学问题,涉及诸多的数学分支,因而在通信系统中有重要的理论价值.

由于渐近好码的实用价值和理论价值,使得码的渐近性的研究成为编码理论中的重要研究课题. 构造可达到信道容量或者可逼近信道容量(Shannon限)的信道编码具体方法,及其可实用的(线性复杂度)有效译码算法一直是信道编码理论与技术研究的中心任务,也就是如何构造出能接近或达到Shannon限的码(渐近好码)是编码学者长期追求的目标. 目前已知有限域上的线性码是渐近好码[4,5],但是BCH码作为汉明(Hamming)码的推广,不是渐近好码[6,7];有限域上的重根循环码也不是渐近好码[8]. 至今,人们仍然不知道具有良好代数结构的一类线性码——循环码(单根的情形)是否是渐近好码[9],这是一个长期以来悬而未决的公开问题. 对于循环码的渐近性这一问题,人们知之甚少,关于它的任何进展都能引起人们的广泛兴趣.

设G是一个有限交换群,FG是F上G的群代数. FG的任一个理想(FG-子模)称为有限域F上的一个交换群码. 当G是循环群时,交换群码即为循环码. 记

$$(FG)^2:=\{(a,b)|a,b\in FG\},$$

则$(FG)^2$的FG-子模C称为指数为2的拟交换群码. 当G是循环群时,称C为指数为2的拟循环码. 虽然人们还不知道循环码是否是渐近好码,但是人们很早就证明了指数为2的拟循环码是渐近好码. 具体地,利用随机码,Chen等人[10]证明了,如果2是无限多个素数的本原元(即Artin猜想),那么存在渐近好的二元拟循环码;Chepyzhov[11]和Kasami[12]分别从不同的角度,在不需要假设Artin猜想成立的前提下,证明了渐近好的二元拟循环码的存在性. 近期,Fan等人[13]定义了指数为$1\frac{1}{3}$的拟循环码,即首次引入了分数指数的拟循环码的概念,并证明了这样的拟循环码是渐近好码. 随后,Mi等人[14]的结果推广到任意分数指数的拟循环码上,证明了任意分数指数的拟循环码是渐近好码. 作为拟循环码的推广,拟交换群码的渐近性研究自然引起了人们的关注. Fan等人[15]利用概率的方法证明了存在渐近好的拟交换群码达到Gilbert-Varshamov界.

在拟交换群码上能够自然引入欧氏内积,所以可以研究自正交拟交换群码与自对偶拟交换群码的渐近性. Lin等人[16]证明了自正交拟交换群码是渐近好码;Ling等人[17]证明了存在二元自对偶拟循环码(I型或II型)达到Gilbert-Varshamov界;Martínez-Pérez等人[18]利用随机方法,证明了指数为2的二元自对偶的doubly-even拟循环码是渐近好码;Lin等人[16]证明了当-1是F中的平方元时,自对偶的拟交换群码是渐近好码.

LCD(Linear Complementary Dual)码是编码理论中一类重要的码,在数据存储、通信系统、量子信息以及密码学等方面都有广泛应用[19]. 最早是由Massey[20]为解决一类信息论的问题而引入的. LCD是渐近好码[20],能够达到Gilbert-Varshamov界[21]. 本文在前人结果的基础上,在拟交换群码上引入Hermitian内积,构造了一类HermitianLCD拟交换群码,并证明了存在渐近好的Hermitian LCD拟交换群码. 为此,我们首先探讨了拟交换群码是LCD码的一个充分条件,在此基础上我们构造了一类Hermitian LCD拟交换群码,并研究了它们的维数特征(定理1和定理2);然后利用群表示论方法(主要是群代数的本原幂等元)计算了此类码的个数,并确定了它的一个下界(定理3和定理4);最后通过对相对最小距离(即相对最小重量)较小的(即小于一个固定较小的正数δ)这类码个数的估值,主要确定了它的一个上界(定理5),依据概率的方法证明了任意有限域上的Hermitian LCD拟交换群码是渐近好码(定理6).

2 预备知识

本文总假设q是一个素数的幂,n是一个与q互素的奇数. F是一个q^2元有限域,F_q表示F的q元子域. 设G是一个n阶有限交换群. 用$|X|$表示集合X的元素个数. 设S_0和S是两个集合,且S_0是S的子集,用$S-S_0$表示集合$\{a|a\in S,a\notin S_0\}$. 如果V是有限域K上的线性空间,那么用$\dim_K V$表示线性空间V的维数.

2.1 交换群码及其 Hermitian 对偶码

设FG是域F上的有限交换群G的群代数,即$FG=\left\{\sum_{x\in G}a_x x\middle|a_x\in F\right\}$,则$FG$是有限域$F$上的线性空间,它同构于$F^n$. 因此$FG$的任一元素$a=\sum_{x\in G}a_x x$等同于$F^n$中的码字$(a_x)_{x\in G}$,进而$a$的汉明重量$w(a)$为

$$w(a)=\left|\{a_x\in F|a_x\neq 0,\ \forall x\in G\}\right|.$$

如果C是群代数FG的一个理想,那么我们称C为F上长为n的交换群码. 因为群代数FG自然附带一个Hermitian内积$\langle\cdot,\cdot\rangle_h$:

$$\left\langle\sum_{g\in G}a_g g,\sum_{g\in G}b_g g\right\rangle_h=\sum_{g\in G}a_g b_g^q\ \forall\sum_{g\in G}a_g g,\ \sum_{g\in G}b_g g\in FG.$$

所以可以定义交换群码C的Hermitian对偶码:

$$C^{\perp_h}=\left\{a\in FG\middle|<a,c>_h=0,\ \forall c\in C\right\}.$$

显然,$C^{\perp_h}$也是有限域F上长为n的交换群码. 如果$C=C^{\perp_h}$,那么称C为Hermitian自对偶交换群码;如果$C\subseteq C^{\perp_h}$,那么称C为Hermitian自正交交换群码;如果$C\cap C^{\perp_h}=\{0\}$,那么称C为Hermitian LCD交换群码.

为了进一步刻画群代数FG中的Hermitian内积,下

面介绍群代数FG的一个自同构和一个线性函数. 群代数FG有如下的环自同构，记作“–”：

$$-:\quad FG\to FG,\ \sum_{g\in G}a_g g\mapsto \sum_{g\in G}a_g^q g^{-1},$$

即$\overline{\sum_{g\in G}a_g g}=\sum_{g\in G}a_g^q g^{-1}$.

另外，在FG上有一个如下的线性函数“σ”：

$$\sigma:\quad FG\to F,\ \sum_{g\in G}a_g g\mapsto a_{1_G},$$

即σ把FG中的元素$\sum_{g\in G}a_g g$映成G的单位元1_G的系数.

引理1　设$a,b\in FG$，则

$$<a,b>_h=\sigma(a\bar{b}).$$

证明　设$a=\sum_{g\in G}a_g g,\ b=\sum_{h\in G}b_h h\in FG$，则

$$\sigma(a\bar{b})=\sigma\left(\sum_{g\in G}a_g g\cdot\sum_{h\in G}b_h^q h^{-1}\right)=\sigma\left(\sum_{g\in G}\sum_{h\in G}(a_g b_h^q)gh^{-1}\right)$$
$$=\sum_{x\in G}a_x b_x^q=<a,b>_h.$$

证毕.

2.2　群代数FG的本原幂等元

根据Maschke定理[22]，由$\gcd(n,q)=1$可得FG是一个半单代数，从而它可以分解成极小理想$I_i(0\leqslant i\leqslant m)$的直和：

$$FG=I_0\oplus I_1\oplus\cdots\oplus I_m,$$

其中，m表示FG分解成极小理想的个数，它由FG唯一决定，与分解式无关，参考文献[23]的推论2.2.4. 故FG的单位元1有如下的本原幂等元分解：

$$1=e_0+e_1+\cdots+e_m,$$

其中，$e_i(i=0,1,\cdots,m)$满足

$$e_i e_j=\begin{cases}e_i, & i=j\\ 0, & i\neq j\end{cases},$$

并且$I_i=FGe_i(i=0,1,\cdots,m)$，这里$FGe_i$表示群代数$FG$的由$e_i$所生成的理想，故$I_i$就是由本原幂等元$e_i$所生成的理想. 特别地，

$$e_0=\frac{1}{n}\sum_{g\in G}g,$$

故$I_0=FGe_0=Fe_0$是一个1维的平凡FG-模.

令$E=\{e_0,e_1,\cdots,e_m\}$，即E是FG的全部本原幂等元构成的集合，则$1=\sum_{e\in E}e$. 对于任意的$i=0,1,\cdots,m$，FGe_i是有限域，并且可以将它们视作有限域F上的线性空间. 记

$$\mu_q(n)=\min\left\{\dim_F FGe\,\middle|\,e\in E-\{e_0\}\right\}\qquad(1)$$

关于$\mu_q(n)$的性质，见文献[16]引理II.2.

既然环自同构“–”置换E中的元素，则

$$E=\{e_0\}\cup\{e_1,e_2,\cdots,e_r\}\cup\{e_{r+1},\overline{e_{r+1}},\cdots,e_{r+s},\overline{e_{r+s}}\},$$

其中，$m=1+r+2s$；$\bar{e}_i=e_i,i=0,1,2,\cdots,r$；$\overline{e_{r+j}}\neq e_{r+j},j=1,2,\cdots,s$.

记　$e_{r+j}^*=e_{r+j}+\overline{e_{r+j}},j=1,2,\cdots,s$，　则　$e_{r+j}^*=\overline{e_{r+j}^*},j=1,2,\cdots,s$. 令

$$E^*=\left\{e_0,e_1,\cdots,e_r,e_{r+1}^*,\cdots,e_{r+s}^*\right\},$$

则

$$\bar{e}=e,\forall e\in E^*;\ 1=\sum_{e\in E^*}e;\ ee'=\begin{cases}e,e=e'\\ 0,e\neq e'\end{cases},\ \forall e,e'\in E^*.$$

并且FG有如下的直和分解：

$$FG=(\oplus_{i=0}^{r}FGe_i)\oplus(\oplus_{j=1}^{s}FGe_{r+j}^*)\qquad(2)$$

再令

$$E_0^*=E^*-\{e_0\}=\left\{e_1,\cdots,e_r,e_{r+1}^*,\cdots,e_{r+s}^*\right\},$$
$$k_e=\dim_F FGe,\quad\forall e\in E_0^*.$$
$$k_i=k_{e_i},\ i=1,2,\cdots,r;\ k_{r+j}=k_{e_{r+j}^*},\ j=1,2,\cdots,s.$$

故对任意的$j=1,2,\cdots,s$，k_{r+j}是偶数，且$\dim_F FGe_{r+j}=\dim_F FG\overline{e_{r+j}}=\frac{1}{2}k_{r+j},j=1,2,\cdots,s$. 根据式(2)我们得到

$$n=1+\sum_{i=1}^{r}k_i+\sum_{j=1}^{s}k_{r+j}\qquad(3)$$

3　指数为2的Hermitian LCD拟交换群码

设$(FG)^2:=\{(a,b)|a,b\in FG\}$，则$(FG)^2$是一个$FG$-模. 我们称$(FG)^2$的任一个$FG$-模$C$为有限域$F$上的指数为2的拟交换群码，或者简称为有限域$F$上的2-拟交换群码. 若$G$是循环群，则称$C$为有限域$F$上的2-拟循环群码. 注意到，$(FG)^2$中的元素$(a,b)=(\sum_{g\in G}a_g g,\ \sum_{h\in G}b_h h)$等同于$F$上长为$2n$的码字$\left((a_g)_{g\in G},(b_h)_{h\in G}\right)$. 故有限域$F$上的2-拟交换群码$C$的码率为$\frac{\dim_F C}{2n}$，相对最小距离为$\frac{d(C)}{2n}$，即$R(C)=\frac{\dim_F C}{2n},\Delta(C)=\frac{d(C)}{2n}$.

自然地，我们可以通过扩充FG中的Hermitian内积来定义$(FG)^2$中的Hermitian内积. 因此我们可以进一步定义有限域F上Hermitian自对偶的2-拟交换群码、Hermitian自正交的2-拟交换群码以及Hermitian LCD 2-拟交换群码.

以后我们主要研究有限域F上的Hermitian LCD 2-拟交换群码的渐近性质. 为此，我们需要构造一类指数为2的Hermitian LCD拟交换群码.

假设$a\in FG$，定义$C_{1,a}$如下：

$$C_{1,a}=\left\{u(1,a)\,|\,u\in FG\right\}\qquad(4)$$

下面给出$C_{1,a}$是Hermitian LCD码的一个充分条件.

设$I\leqslant FG$是FG的一个理想，则把环I的乘法单位群记作$I^\times$.

定理 1 设 $a\in FG$, $C_{1,a}$ 如式(4)所示. 若 $1+a\bar{a}\in(FG)^{\times}$,则 $C_{1,a}$ 是一个指数为2的Hermitian LCD拟交换群码,即

$$C_{1,a}\cap C_{1,a}^{\perp_h}=\{0\}.$$

证明 任取 $u_0(1,a)\in C_{1,a}\cap C_{1,a}^{\perp_h}$, 即对任意的 $u\in FG$, $<(u_0,u_0a),(u,ua)>_h=0$. 下面我们证明 $u_0=0$,即可得到 $u_0(1,a)=0$.

根据引理1,得到

$$0=<(u_0,u_0a),(u,ua)>_h=<u_0,u>_h+<u_0a,ua>_h$$
$$=\sigma(u_0\bar{u})+\sigma(u_0a\overline{ua})=\sigma\left(u_0\bar{u}(1+a\bar{a})\right).$$

因为 $1+a\bar{a}\in(FG)^{\times}$, 所以对任意的 $u\in FG$, $\sigma(u_0\bar{u})=0$. 假设 $u_0\neq0$,令 $u_0=\sum_{g\in G}a_gg$,不妨设 $a_{g_0}\neq0$,这里 $g_0\in G$. 取 $u=g_0$,则

$$0=\sigma(u_0\bar{u})=\sigma\left(\sum_{g\in G}a_gg\cdot g_0^{-1}\right)=a_{g_0}\neq0.$$

由此得到一个矛盾,故 $u_0=0$,即得 $C_{1,a}\cap C_{1,a}^{\perp_h}=\{0\}$. 故 $C_{1,a}$ 是一个指数为2的Hermitian LCD拟交换群码. 证毕.

进一步,为了研究Hermitian LCD拟交换群码的渐近性,我们需要探讨 $F-$线性空间 $C_{1,a}$ 的维数.

定理 2 设 $a\in FG$, $C_{1,a}$ 如式(4)所示,则 $\dim_FC_{1,a}\geqslant n$,进而得 $C_{1,a}$ 的码率满足

$$R(C_{1,a})\geqslant\frac{1}{2}.$$

证明 定义映射 τ 如下:

$$\tau:\quad FG\to C_{1,a},\quad u\mapsto u(1,a),$$

则 τ 是 $FG\to C_{1,a}$ 的 $F-$ 单同态,从而 $\dim_FC_{1,a}\geqslant\dim_FFG=n$,进而得

$$R(C_{1,a})=\frac{\dim_FC_{1,a}}{2n}\geqslant\frac{n}{2n}=\frac{1}{2}.$$

证毕.

设 $\lambda\in(FG)^{\times}$, $a\in FG$, 满足 $a\bar{a}=\lambda-1$. 按照定理1, $C_{1,a}=\{u(1,a)\,|\,u\in FG\}$ 是一类指数为2的Hermitian LCD拟交换群码. 为了研究指数为2的Hermitian LCD拟交换群码的渐近性,我们需要探讨下面两个集合.

设 $\delta\in[0,1-q^{-2}]$, $\lambda\in(FG)^{\times}$,定义

$$D_\lambda=\left\{C_{1,a}\,\middle|\,a\bar{a}=\lambda-1,\ a\in FG\right\}\tag{5}$$

$$D_\lambda^{\leqslant\delta}=\left\{C_{1,a}\,\middle|\,C_{1,a}\in D_\lambda,\Delta(C_{1,a})\leqslant\delta\right\}\tag{6}$$

4 指数为2的Hermitian LCD拟交换群码的渐近性

为了研究指数为2的Hermitian LCD拟交换群码的渐近性,重要的是确定式(5)和式(6)中的两个集合 D_λ 和 $D_\lambda^{\leqslant\delta}$ 的基数. 首先我们计算集合 D_λ 的基数,即确定这类Hermitian LCD拟交换群码的个数. 根据 D_λ 的定义,问题转化为确定下列集合 D^λ 的基数:

设 $\lambda\in(FG)^{\times}$,有

$$D^\lambda=\left\{a\,\middle|\,a\bar{a}=\lambda-1,\ a\in FG\right\}\tag{7}$$

显然 $|D_\lambda|=|D^\lambda|$.

4.1 确定 $|D_\lambda|$ 的一个下界

引理2 设 $\lambda\in(FG)^{\times}$, $a\in FG$,则 $a\bar{a}=\lambda-1$ 当且仅当 $a\bar{a}e=(\lambda-1)e$, $\forall e\in E^*$.

证明 由 $1=\sum_{e\in E^*}e$; $FG=\oplus_{e\in E^*}(FGe)$ 是一个直和分解,得 $a\bar{a}=\lambda-1$ 当且仅当 $\sum_{e\in E^*}a\bar{a}e=\sum_{e\in E^*}(\lambda-1)e$,当且仅当

$$a\bar{a}e=(\lambda-1)e,\ \forall e\in E^*.$$

证毕.

定义 $\forall e\in E^*$,有

$$I_e=\left\{a\in FGe\,\middle|\,a\bar{a}=(\lambda-1)e\right\}\tag{8}$$

引理3 符号 $D_\lambda,D^\lambda,I_e(e\in E^*)$ 的定义如式(5),式(7)和式(8)所示,则

$$|D_\lambda|=|D^\lambda|=\prod_{e\in E^*}|I_e|.$$

证明 既然 $|D_\lambda|=|D^\lambda|$,下面只需证明 $|D^\lambda|=\prod_{e\in E^*}|I_e|$即可. 构造 D^λ 和 $\oplus_{e\in E^*}I_e$ 之间的一个对应 η 如下:

$$\eta:D^\lambda\to\oplus_{e\in E^*}I_e,\ a\mapsto\sum_{e\in E^*}(ae).$$

下面证明 η 是一个双射.

设 $a\in D^\lambda$, 则 $a\bar{a}=\lambda-1$. 由引理2知 $a\bar{a}e=(\lambda-1)e$, $\forall e\in E^*$. 故

$$(ae)\overline{ae}=(\lambda-1)e,\ \forall e\in E^*,$$

即得 $ae\in I_e$. 因此 η 是一个映射.

设 $\eta(a)=\eta(b)$,这里 $a,b\in D^\lambda$,则 $\sum_{e\in E^*}(ae)=\sum_{e\in E^*}(be)$,即得 $a\sum_{e\in E^*}e=b\sum_{e\in E^*}e$,故 $a=b$. 因此 η 是一个单射.

任取 $c\in\oplus_{e\in E^*}I_e$, 不妨设 $c=\oplus_{e\in E^*}\alpha_e$, 这里 $\alpha_e\in I_e$,则

$$\eta(c)=\sum_{e'\in E^*}ce'=\sum_{e'\in E^*}\left(\sum_{e\in E^*}\alpha_e\right)e'$$
$$=\sum_{e'\in E^*}\sum_{e\in E^*}\alpha_ee'=\sum_{e\in E^*}\alpha_ee=\sum_{e\in E^*}\alpha_e=c,$$

故 η 是一个满射.

综上所述,η 是一个双射. 由此可得

$$|D_\lambda|=|D^\lambda|=\prod_{e\in E^*}|I_e|.$$

证毕.

以下总假设：$\lambda\in(FG)^{\times}$，并且$\lambda-1\in F_q^{\times}$. 这样的$\lambda$是存在的，例如$F^{\times}-F_q^{\times}$中的元素总满足这个条件.

根据引理3，我们把问题归结为计算I_e的基数，即计算$|I_e|, e\in E^*$.

引理4　若$e=e_0$，则$|I_e|=q+1$.

证明　根据I_e的定义我们有

$$\begin{aligned}I_e&=\{a\in FGe_0\mid a\bar{a}=(\lambda-1)e_0\}\\&=\{a\in Fe_0\mid a\bar{a}=(\lambda-1)e_0\}\\&=\{\mu e_0\mid \mu e_0\overline{\mu e_0}=(\lambda-1)e_0,\mu\in F\}\\&=\{\mu\in F\mid \mu\bar{\mu}=\lambda-1\}\\&=\{\mu\in F\mid \mu^{q+1}=\lambda-1\}.\end{aligned}$$

设$\mathrm{Norm}_1(x)=x^{q+1}$是$F^{\times}$到$F_q^{\times}$的范映射，则$I_e=\{\mu\in F\mid \mathrm{Norm}_1(\mu)=\lambda-1\}$. 既然$\lambda-1\in F_q^{\times}$，故有

$$|I_e|=\frac{q^2-1}{q-1}=q+1.$$

参看文献[24]，推论7.17(ii). 证毕.

引理5　若$e=e_i(1\leqslant i\leqslant r)$，则$|I_e|=q^{k_i}+1$.

证明　对任意的$i=1,2,\cdots,r$，FGe_i是有限域且$|FGe_i|=q^{2k_i}$. 令

$$\mathrm{Fix}(FGe_i)=\{a\in FGe_i\mid \bar{a}=a\},$$

则$\mathrm{Fix}(FGe_i)$是FGe_i的F_q-子空间. 由文献[25]，引理2.2可知

$$\dim_{F_q}\mathrm{Fix}(FGe_i)=\frac{1}{2}\dim_{F_q}(FGe_i).$$

设$G=\mathrm{Gal}(FGe_i\backslash F_q)$是$FGe_i$的所有$F_q-$自同构对于自同构的复合运算构成的伽罗华群，则映射“–”属于群G. 设H是映射“–”所生成的G的子群，则由伽罗华理论得

$$|H|=[FGe_i:\mathrm{Fix}(FGe_i)],$$

其中，$[FGe_i:\mathrm{Fix}(FGe_i)]$表示域扩张$FGe_i\backslash\mathrm{Fix}(FGe_i)$的次数. 因此

$$|FGe_i|=|\mathrm{Fix}(FGe_i)|^{|H|},$$

故$|H|=2$，即映射“–”是群G中的2阶元. 注意到$|G|=|\mathrm{Gal}(FGe_i\backslash F_q)|=[FGe_i:F_q]=2k_i$. 又$G=<\varphi>$，其中$\varphi(x)=x^q,\forall x\in FGe_i$，故$\bar{a}=\varphi^{k_i}(a)=a^{q^{k_i}},\ \forall a\in FGe_i$. 因此，

$$\begin{aligned}I_e&=\{a\in FGe\mid a\bar{a}=(\lambda-1)e\}\\&=\{a\in FGe\mid a^{q^{k_i}+1}=(\lambda-1)e\}.\end{aligned}$$

又$(FGe)^{\times}=F_{q^{2k_i}}^{\times}$到$F_{q^{k_i}}^{\times}$范映射$\mathrm{Norm}_2$定义如下：

$\mathrm{Norm}_2:(FGe)^{\times}=F_{q^{2k_i}}^{\times}\to F_{q^{k_i}}^{\times},\quad x\mapsto x^{q^{k_i}+1}$. 由此得到

$$I_e=\{a\in F_{q^{2k_i}}^{\times}\mid \mathrm{Norm}_2(a)=(\lambda-1)e\}.$$

根据文献[24]，推论7.17(ii)，我们得到

$$|I_e|=\frac{(q^{k_i})^2-1}{q^{k_i}-1}=q^{k_i}+1, i=1,2,\cdots,r.$$

证毕.

引理6　若$e=e_{r+j}^*(1\leqslant j\leqslant s)$，则

$$|I_e|=q^{k_{r+j}}-1.$$

证明　设$a=b+c\in I_e$，$b\in FGe_{r+j}$，$c\in FG\overline{e_{r+j}}$，则由$a\bar{a}=(\lambda-1)e$，得

$$(b+c)(\overline{b+c})=(\lambda-1)e,$$

从而$(b+c)(\bar{b}+\bar{c})=(\lambda-1)(e_{r+j}+\overline{e_{r+j}})$，故

$$b\bar{b}+b\bar{c}+c\bar{b}+c\bar{c}=(\lambda-1)e_{r+j}+(\lambda-1)\overline{e_{r+j}}.$$

注意到$b\bar{b}=c\bar{c}=0$，进而得到$b\bar{c}+c\bar{b}=(\lambda-1)e_{r+j}+(\lambda-1)\overline{e_{r+j}}$，即得$b\bar{c}=(\lambda-1)e_{r+j}$. 因此

$$\begin{aligned}I_e&=\{a\in FGe\mid a\bar{a}=(\lambda-1)e\}\\&=\{b+c\mid b\bar{c}=(\lambda-1)e_{r+j}, b\in(FGe_{r+j})^{\times}, c\in(FG\overline{e_{r+j}})^{\times}\}\\&=\{b+(\lambda-1)\overline{b^{-1}e_{r+j}}\mid b\in(FGe_{r+j})^{\times}\}.\end{aligned}$$

由此可得I_e由元素$b\in(FGe_{r+j})^{\times}$所唯一确定，从而

$$\begin{aligned}|I_e|&=|(FGe_{r+j})^{\times}|=|FGe_{r+j}|-1\\&=|F|^{\dim_F FGe_{r+j}}-1=(q^2)^{\frac{k_{r+j}}{2}}-1=q^{k_{r+j}}-1,\\&\qquad j=1,2,\cdots,s.\end{aligned}$$

证毕.

定理3　设D_λ如式(5)所示，则D_λ的基数

$$|D_\lambda|=(q+1)\cdot\prod_{i=1}^{r}(q^{k_i}+1)\cdot\prod_{j=1}^{s}(q^{k_{r+j}}-1).$$

证明　利用引理3~6可得. 证毕.

引理7[26]　设$q\geqslant 3$，t是正整数. 若$\kappa_1,\kappa_2,\cdots,\kappa_t$是正整数且满足$\kappa_i\geqslant\log_q t,\ i=1,2,\cdots,t$，则

$$(q^{\kappa_1}-1)(q^{\kappa_2}-1)\cdots(q^{\kappa_t}-1)\geqslant q^{\kappa_1+\kappa_2+\cdots+\kappa_t-2}.$$

定理4　设$\dfrac{\log_q n}{\mu_q(n)}\leqslant 1$，则$|D_\lambda|\geqslant q^{n-2}$.

证明　由定理3得

$$\begin{aligned}|D_\lambda|&=(q+1)\cdot\prod_{i=1}^{r}(q^{k_i}+1)\cdot\prod_{j=1}^{s}(q^{k_{r+j}}-1)\\&\geqslant q\cdot\prod_{i=1}^{r}(q^{k_i}-1)\cdot\prod_{j=1}^{s}(q^{k_{r+j}}-1).\end{aligned}$$

根据引理7，我们需要证明：

$$k_i\geqslant\log_q(r+s),\ i=1,2,\cdots,r+s.$$

由$\mu_q(n)\geqslant\log_q n$，$n=1+k_1+\cdots+k_{r+s}$以及$k_i\geqslant\mu_q(n)\geqslant 1(\forall 1\leqslant i\leqslant r+s)$，即得

$q^{\mu_q(n)}\geqslant n=1+k_1+\cdots+k_{r+s}\geqslant 1+\mu_q(n)(r+s)\geqslant r+s$，即得$\mu_q(n)\geqslant\log_q(r+s)$，故根据式(1)中$\mu_q(n)$的定义有

$$k_i\geqslant\mu_q(n)\geqslant\log_q(r+s).$$

因此由引理7得

$$\left|D_\lambda\right|\geqslant q\cdot q^{k_1+k_2+\cdots+k_{r+s}-2}=q^{k_1+k_2+\cdots+k_{r+s}-1}.$$

再利用$n=1+k_1+k_2+\cdots+k_{r+s}$得$\left|D_\lambda\right|\geqslant q^{n-2}$. 证毕.

4.2 确定$\left|D_\lambda^{\leqslant\delta}\right|$的一个上界

先引入下面的符号. 设$a\in FG$，定义

$$\begin{cases}E_a^*=\left\{e\middle|e\in E^*,ea\neq 0\right\}\\ E_{0,\,a}^*=\left\{e\middle|e\in E_0^*,ea\neq 0\right\}\end{cases}\tag{9}$$

$$I_a=\oplus_{e\in E_{0,\,a}^*}FGe,k_a=\dim_F I_a\tag{10}$$

故$k_a=\sum\limits_{e\in E_{0,\,a}^*}\dim_F FGe=\sum\limits_{e\in E_{0,\,a}^*}k_e$.

引理8[16] 设$q\geqslant 3$，t是正整数. 若$\kappa_1,\kappa_2,\cdots,\kappa_t$是正整数且满足$\kappa_i\geqslant\log_q t,i=1,2,\cdots,t$，则

$$(q^{\kappa_1}+1)(q^{\kappa_2}+1)\cdots(q^{\kappa_t}+1)\leqslant q^{\kappa_1+\kappa_2+\cdots+\kappa_t+2}.$$

引理9 设$(b,c)\in(FG)^2$，定义

$$D_{(b,\,c)}=\left\{C_{1,\,a}\middle|(b,\,c)\in C_{1,\,a},C_{1,\,a}\in D_\lambda\right\}.$$

(1)若$D_{(b,\,c)}\neq\varnothing$，则$E_b^*=E_c^*$.

(2)若$\dfrac{\log_q n}{\mu_q(n)}\leqslant 1$，则$\left|D_{(b,\,c)}\right|\leqslant q^{n+3-k_b}$.

证明 既然$D_{(b,\,c)}\neq\varnothing$，设$C_{1,\,a}\in D_{(b,\,c)}$，则$C_{1,\,a}\in D_\lambda$，且$(b,c)\in C_{1,\,a}$，从而存在$u\in FG$使得$(b,c)=u(1,a)$，即得$c=ab$.

令$a=\sum\limits_{e\in E^*}a_e$，这里$a_e\in FGe(e\in E^*)$，则由$c=ab$得$ec=eab=eba_e,\ \forall e\in E^*$.

又由$C_{1,\,a}\in D_\lambda$得$a\overline{a}=\lambda-1$，即$\left(\sum\limits_{e\in E^*}a_e\right)\left(\sum\limits_{e\in E^*}\overline{a_e}\right)=\lambda-1$，从而

$$\sum_{e\in E^*}a_e\overline{a_e}=\lambda-1=(\lambda-1)\sum_{e\in E^*}e,$$

故$a_e\overline{a_e}=(\lambda-1)e,\forall e\in E^*$.

因此$C_{1,\,a}\in D_{(b,\,c)}$当且仅当下面两个条件成立：

(i)$ec=eab=eba_e,\forall e\in E^*$；

(ii)$a_e\overline{a_e}=(\lambda-1)e,\forall e\in E^*$.

(1)由条件(ii)知，$a_e\in(FGe)^\times$，再由条件(i)知$E_b^*=E_c^*$.

(2)若$D_{(b,\,c)}=\varnothing$，则结论显然成立. 下设$D_{(b,\,c)}\neq\varnothing$. 由条件(i)和(ii)可知，我们只需考虑

$$D_{(b,\,c)}^*=\left\{a=\sum_{e\in E^*}a_e\middle|ec=eba_e,a_e\overline{a_e}=(\lambda-1)e,\forall e\in E^*\right\}$$
$$=\oplus_{e\in E^*}\left\{a_e\middle|ec=eba_e,a_e\overline{a_e}=(\lambda-1)e,\forall e\in E^*\right\}.$$

记$J_e=\left\{a_e\middle|ec=eba_e,a_e\overline{a_e}=(\lambda-1)e,\forall e\in E^*\right\}$，则

$$D_{(b,\,c)}=\left|D_{(b,\,c)}^*\right|=\prod_{e\in E^*}\left|J_e\right|$$
$$=\left|J_{e_0}\right|\cdot\prod_{e\in E_{0,\,b}^*}\left|J_e\right|\cdot\prod_{e\in E_0^*-E_{0,\,b}^*}\left|J_e\right|,$$

先计算$\left|J_{e_0}\right|$. 若$e=e_0$，则$a_e\in FGe_0=Fe_0$.

令$a_e=xe_0(x\in F)$，则由$a_e\overline{a_e}=(\lambda-1)e$得$xe_0\overline{xe_0}=(\lambda-1)e_0$，即得$x^{q+1}=\lambda-1$. 故由引理4及其证明可知

$$\left|J_{e_0}\right|\leqslant\left|\left\{x\middle|x^{q+1}=\lambda-1,x\in F\right\}\right|=q+1.$$

再计算$\prod\limits_{e\in E_{0,\,b}^*}\left|J_e\right|$. 若$e\in E_{0,\,b}^*$，即$e\in E_0^*$且$eb\neq 0$. 又由(1)知$E_b^*=E_c^*$，故$ec\neq 0$.

若$e\in\left\{e_1,e_2,\cdots,e_r\right\}$，此时$FGe$是一个有限域，则由$ec=eba_e$，得$a_e=(ec)(eb)^{-1}$，即$a_e$被唯一确定. 故此时的$J_e$满足$\left|J_e\right|\leqslant 1$.

若$e\in\left\{e_{r+1}^*,e_{r+2}^*,\cdots,e_{r+s}^*\right\}$，不妨假设$e=e_{r+j}^*=e_{r+j}+\overline{e_{r+j}}(1\leqslant j\leqslant s)$. 既然$a_e\in FGe_{r+j}^*=FGe_{r+j}+FG\overline{e_{r+j}}$，可令$a_e=u_e+v_e$，这里$u_e\in FGe_{r+j},v_e\in FG\overline{e_{r+j}}$. 由$ec=eba_e$得$(e_{r+j}+\overline{e_{r+j}})c=(e_{r+j}+\overline{e_{r+j}})b(u_e+v_e)$，即$ce_{r+j}+c\overline{e_{r+j}}=b(u_ee_{r+j}+v_e\overline{e_{r+j}}+u_e\overline{e_{r+j}}+v_ee_{r+j})$. 注意到$u_e\overline{e_{r+j}}=v_ee_{r+j}=0$，我们就得到$ce_{r+j}+c\overline{e_{r+j}}=bu_ee_{r+j}+bv_e\overline{e_{r+j}}$. 即得$ce_{r+j}=bu_ee_{r+j},c\overline{e_{r+j}}=bv_e\overline{e_{r+j}}$. 注意到$eb\neq 0$，即$(e_{r+j}+\overline{e_{r+j}})b\neq 0$，故$e_{r+j}b\neq 0$或$b\overline{e_{r+j}}\neq 0$，从而$u_e=ce_{r+j}(be_{r+j})^{-1}$或$v_e=c\overline{e_{r+j}}(b\overline{e_{r+j}})^{-1}$，表明$u_e$或$v_e$被唯一确定. 因此，此时的$J_e$满足$\left|J_e\right|\leqslant 1$. 总之，对任意的$e\in E_{0,\,b}^*$，均有$\left|J_e\right|\leqslant 1$.

最后计算$\prod\limits_{e\in E_0^*-E_{0,\,b}^*}\left|J_e\right|$. 若$e\in E_0^*-E_{0,\,b}^*$，则$eb=ec=0$. 故条件(i)显然成立，从而

$$J_e=\left\{a_e\in FGe\middle|a_e\overline{a_e}=(\lambda-1)e\right\}=I_e.$$

由引理5和引理6可得

$$J_e=\begin{cases}q^{k_i}+1=q^{k_e}+1,&e=e_i(1\leqslant i\leqslant r)\\ q^{k_{r+j}}-1=q^{k_e}-1,&e=e_{r+j}^*(1\leqslant j\leqslant s)\end{cases}.$$

因此，我们有

$$\prod_{e\in E_0^*-E_{0,\,b}^*}\left|J_e\right|\leqslant\prod_{e\in E_0^*-E_{0,\,b}^*}(q^{k_e}+1).$$

综上所述，对于$\left|D_{(b,\,c)}\right|$的估值，我们得到

$$\left|D_{(b,\,c)}\right|\leqslant(q+1)\cdot\prod_{e\in E_0^*-E_{0,\,b}^*}(q^{k_e}+1).$$

再注意到

$$1+\sum_{e\in E_{0,\,b}^*}k_e+\sum_{e\in E_0^*-E_{0,\,b}^*}k_e=n,$$

就得到

$$\sum_{e\in E_0^*-E_{0,b}^*}k_e=n-1-k_b,$$

进而由引理8得到

$$\left|D_{(b,c)}\right|\leqslant(q+1)\cdot q^{\sum\limits_{e\in E_0^*-E_{0,b}^*}k_e+2}=(q+1)\cdot q^{n-1-k_b+2}.$$
$$=(q+1)q^{n+1-k_b}\leqslant q^2\cdot q^{n+1-k_b}=q^{n+3-k_b}$$

证毕.

设l是正整数,且满足$\mu_q(n)\leqslant l\leqslant n$. 记

$$\Omega_l=\left\{I\leqslant FG\left|\begin{array}{c}\text{存在子集 }\Theta\subseteq E_0^*,\\ \text{使得 }I=\oplus_{e\in\Theta}FGe,\dim_F I=l\end{array}\right.\right\}\quad(11)$$

设$I\in\Omega_l$,记

$$\bar{I}=FGe_0+I,\ \bar{I}^*=\left\{a\left|a\in\bar{I},I_a=I\right.\right\}\quad(12)$$

注意此时$\dim_F\bar{I}=\dim_F I+1=l+1$,其中$l=k_a,\forall a\in\bar{I}^*$.

引理10　设$D_\lambda^{\leqslant\delta}$如式(6)所示,则

$$D_\lambda^{\leqslant\delta}\subseteq\bigcup_{\mu_q(n)\leqslant l\leqslant n}\bigcup_{I\in\Omega_l}\bigcup_{(b,c)\in(\bar{I}^*\times\bar{I}^*)^{\leqslant\delta}}D_{(b,c)}.$$

证明　任取一个$C_{1,a}\in D_\lambda^{\leqslant\delta}$,则$0<\dfrac{w(C_{1,a})}{2n}\leqslant\delta$. 故存在$(b,c)\in C_{1,a}$使得$0<\dfrac{w(b,c)}{2n}\leqslant\delta$,即$0<w(b,c)\leqslant2n\delta$. 既然$(b,c)\in C_{1,a}$,$D_{(b,c)}\neq\varnothing$. 由引理9(1)知$E_b^*=E_c^*$,从而$E_{0,b}^*=E_{0,c}^*$.

下面我们证明$E_{0,b}^*=E_{0,c}^*\neq\varnothing$. 为此我们利用反证法先证明$bc\neq0$. 因为$w(b,c)>0$,所以$b,c$不能同时为零. 假设$b=0,c\neq0$. 显然$E_b^*=\varnothing$. 故$E_c^*=\varnothing$. 因此对任意的$e\in E^*,ce=0$,从而

$$c=c\cdot1=c\cdot\sum_{e\in E^*}e=\sum_{e\in E^*}ce=0,$$

此与$c\neq0$相矛盾. 假设$b\neq0,c=0$. 利用同样的方法得到$b=0$,此与$b\neq0$相矛盾. 因此得到$bc\neq0$. 假设$E_{0,b}^*=E_{0,c}^*=\varnothing$,即对任意的$e\in E_0^*,be=ce=0$,即得

$$b=b\cdot1=b\cdot\sum_{e\in E^*}e=be_0+\sum_{e\in E_0^*}ce=be_0.$$

同理$c=ce_0$. 这样,$b,c\in FGe_0=Fe_0$. 令$b=\kappa_1e_0,c=\kappa_2e_0$,这里$\kappa_1,\kappa_2\in F^\times$,则

$$w(b,c)=w(\kappa_1e_0,\kappa_2e_0)=w\left(\frac{\kappa_1}{n}\sum_{g\in G}g,\frac{\kappa_2}{n}\sum_{g\in G}g\right)=2n,$$

此与$0<w(b,c)\leqslant2n\delta<2n$相矛盾. 因此$E_{0,b}^*=E_{0,c}^*\neq\varnothing$.

既然$E_{0,b}^*=E_{0,c}^*\neq\varnothing$,令

$$I=\oplus_{e\in E_{0,b}^*}FGe=\oplus_{e\in E_{0,c}^*}FGe,l=\dim_F I,$$

则$\mu_q(n)\leqslant l\leqslant n$,且$I\in\Omega_l$,进而

$$\bar{I}=FGe_0+I.$$

下面仅需证明$(b,c)\in(\bar{I}^*\times\bar{I}^*)^{\leqslant\delta}$. 注意

$$b=\sum_{e\in E^*}be=be_0+\sum_{e\in E_0^*}be=be_0+\sum_{e\in E_{0,b}^*}be,$$
$$c=\sum_{e\in E^*}ce=ce_0+\sum_{e\in E_0^*}ce=ce_0+\sum_{e\in E_{0,c}^*}ce,$$

则有$b,c\in FGe_0+I=\bar{I}$. 又易知$I=I_b=I_c$. 故$b,c\in\bar{I}^*$,进而得到$(b,c)\in(\bar{I}^*\times\bar{I}^*)^{\leqslant\delta}$. 证毕.

设$\delta\in[0,1-q^{-2}]$,令q^2元熵函数

$$h_q(\delta)=\delta\log_{q^2}(q^2-1)-\delta\log_{q^2}\delta-(1-\delta)\log_{q^2}(1-\delta),$$

其中,$h_q(0)=0,h_q(1-q^{-2})=1$.

引理11[15]　设$I\leqslant FG$是FG的一个理想,则$I\times I\leqslant(FG)^2$且$\left|(I\times I)^{\leqslant\delta}\right|\leqslant q^{2h_q(\delta)\dim_F(I\times I)}$.

引理12　设$\log_qn\leqslant\mu_q(n)\leqslant l\leqslant n,I\in\Omega_l$,则

$$\left|\bigcup_{(b,c)\in(\bar{I}^*\times\bar{I}^*)^{\leqslant\delta}}D_{(b,c)}\right|\leqslant q^{n+3+4l[h_q(\delta)-\frac{1}{4}]+4h_q(\delta)}.$$

证明　因为$\dim_F\bar{I}=\dim_FI+1=l+1$,所以$\dim_F(\bar{I}\times\bar{I})=2(\dim_FI+1)=2l+2$. 故由引理11知:

$$\left|(I\times I)^{\leqslant\delta}\right|\leqslant q^{2h_q(\delta)(2l+2)}=q^{h_q(\delta)(4l+4)}.$$

再根据引理9(2)得到

$$\begin{aligned}\left|\bigcup_{(b,c)\in(\bar{I}^*\times\bar{I}^*)^{\leqslant\delta}}D_{(b,c)}\right|&\leqslant\sum_{(b,c)\in(\bar{I}^*\times\bar{I}^*)^{\leqslant\delta}}\left|D_{(b,c)}\right|\\&\leqslant\sum_{(b,c)\in(\bar{I}^*\times\bar{I}^*)^{\leqslant\delta}}q^{n+3-k_b}\\&\leqslant\left|(\bar{I}^*\times\bar{I}^*)^{\leqslant\delta}\right|\cdot q^{n+3-l}\\&\leqslant\left|(\bar{I}\times\bar{I})^{\leqslant\delta}\right|\cdot q^{n+3-l}\\&\leqslant q^{h_q(\delta)(4l+4)}\cdot q^{n+3-l}\\&=q^{n+3-l+h_q(\delta)(4l+4)}\\&=q^{n+3+4l[h_q(\delta)-\frac{1}{4}]+4h_q(\delta)}.\end{aligned}$$

证毕.

引理13　符号如上,则$\left|\Omega_l\right|\leqslant n^{\frac{l}{\mu_q(n)}}$.

证明　设$I\in\Omega_l$,则存在$\Theta\subseteq E_0^*$使得$I=\oplus_{e\in\Theta}FGe$. 故$l=\dim_FI=\sum\limits_{e\in\Theta}\dim_FFGe\geqslant\sum\limits_{e\in\Theta}\mu_q(n)=\left|\Theta\right|\mu_q(n)$,即得$\left|\Theta\right|\leqslant\dfrac{l}{\mu_q(n)}$. 因此$\Theta$在$E_0^*$中的选取个数$\left|E_0^*\right|^{|\Theta|}\leqslant\left|E_0^*\right|^{\frac{l}{\mu_q(n)}}$,即得$\left|\Omega_l\right|\leqslant\left|E_0^*\right|^{\frac{l}{\mu_q(n)}}$. 再注意到

$$\left|E_0^*\right|=r+s\leqslant n-1<n.\text{ 故}\left|\Omega_l\right|\leqslant n^{\frac{l}{\mu_q(n)}}.$$

证毕.

定理5　设$\dfrac{1}{4}-h_q(\delta)-\dfrac{\log_qn}{2\mu_q(n)}>0$,则

$$\left|D_\lambda^{\leqslant\delta}\right|\leqslant q^{n+4-4\mu_q(n)[\frac{1}{4}-h_q(\delta)-\frac{\log_qn}{2\mu_q(n)}]}.$$

证明 根据引理10,引理12和引理13可得

$$\begin{aligned}\left|D_{\lambda}^{\leqslant\delta}\right| &\leqslant \sum_{\mu_q(n)\leqslant l\leqslant n}\sum_{l\in\Omega_l} q^{n+3+4l[h_q(\delta)-\frac{1}{4}]+4h_q(\delta)}\\ &\leqslant \sum_{\mu_q(n)\leqslant l\leqslant n} n^{\frac{l}{\mu_q(n)}}\cdot q^{n+3+4l[h_q(\delta)-\frac{1}{4}]+4h_q(\delta)}\\ &= \sum_{\mu_q(n)\leqslant l\leqslant n} q^{\frac{l\log_q n}{\mu_q(n)}}\cdot q^{n+3+4l[h_q(\delta)-\frac{1}{4}]+4h_q(\delta)}\\ &\leqslant \sum_{\mu_q(n)\leqslant l\leqslant n} q^{n+4-4l[\frac{1}{4}-h_q(\delta)-\frac{\log_q n}{4\mu_q(n)}]}\\ &\leqslant \sum_{\mu_q(n)\leqslant l\leqslant n} q^{n+4-4\mu_q(n)[\frac{1}{4}-h_q(\delta)-\frac{\log_q n}{4\mu_q(n)}]}\\ &\leqslant n\cdot q^{n+4-4\mu_q(n)[\frac{1}{4}-h_q(\delta)-\frac{\log_q n}{4\mu_q(n)}]}\\ &= q^{n+4-4\mu_q(n)[\frac{1}{4}-h_q(\delta)-\frac{\log_q n}{2\mu_q(n)}]}.\end{aligned}$$

证毕.

4.3 渐近好的指数为2的Hermitian LCD拟交换群码

首先我们需要确保满足定理4和定理5的前提条件的一系列正整数是存在的. 因此下面的引理是必要的.

引理14[26] 设$\mu_q(n_i)$如式(1)所示,则一定存在无穷多个正整数$n_1,n_2,\cdots$满足下列条件:(1)$n_1,n_2,\cdots$都是奇数;(2)$n_1,n_2,\cdots$都与q互素;(3)$\lim\limits_{i\to\infty}\dfrac{\log_q n_i}{\mu_q(n_i)}=0$.

根据引理14,我们也可以得到$\mu_q(n_i)$有如下的变化趋势:

$$\begin{aligned}\lim_{i\to\infty}\frac{1}{\mu_q(n_i)} &= \lim_{i\to\infty}\frac{1}{\log_q n_i}\cdot\frac{\log_q n_i}{\mu_q(n_i)}\\ &= \lim_{i\to\infty}\frac{1}{\log_q n_i}\cdot\lim_{i\to\infty}\frac{\log_q n_i}{\mu_q(n_i)}=0\cdot 0=0,\end{aligned}$$

即得$\lim\limits_{i\to\infty}\mu_q(n_i)=\infty$.

定理6 设正整数序列$n_1,n_2,\cdots$满足引理14中的三个条件,G_i是n_i阶有限交换群,$i=1,2,\cdots$,则存在Hermitian LCD 2-拟交换群码$C_i\leqslant(FG)^2$, $i=1,2,\cdots$使得码序列$C_1,C_2,\cdots$是渐近好的.

证明 设$\delta\in[0,1-q^{-2}]$,$\lambda\in(FG_i)^{\times}$,定义

$$D_{i,\lambda}=\left\{C_{1,a}\middle|\, a\overline{a}=\lambda-1,\ a\in FG_i\right\};$$

$$D_{i,\lambda}^{\leqslant\delta}=\left\{C_{1,a}\middle|\, C_{1,a}\in D_{i,\lambda},\Delta(C_{1,a})\leqslant\delta\right\}.$$

因为$\lim\limits_{i\to\infty}\dfrac{\log_q n_i}{\mu_q(n_i)}=0$,所以

$$\frac{1}{4}-h_q(\delta)-\frac{\log_q n_i}{2\mu_q(n_i)}>0 \text{ 和 } \frac{\log_q n_i}{\mu_q(n_i)}\leqslant 1.$$

又由于$\lim\limits_{i\to\infty}\mu_q(n_i)=\infty$,因此根据定理4和定理5,有

$$\begin{aligned}\frac{\left|D_{i,\lambda}^{\leqslant\delta}\right|}{\left|D_{i,\lambda}\right|} &\leqslant \frac{q^{n_i+4-4\mu_q(n_i)[\frac{1}{4}-h_q(\delta)-\frac{\log_q n_i}{2\mu_q(n_i)}]}}{q^{n_i-2}}\\ &= q^{-4\mu_q(n_i)[\frac{1}{4}-h_q(\delta)-\frac{\log_q n_i}{2\mu_q(n_i)}]+6}\to 0\ (i\to\infty).\end{aligned}$$

取$C_i\in D_{i,\lambda}-D_{i,\lambda}^{\leqslant\delta}$, $i=1,2,\cdots$,则存在长为n_i的Hermitian LCD 2-拟交换群码序列$C_1,C_2,\cdots$使得$n_i\to\infty(i\to\infty)$且满足

(1)码长$2n_i\to\infty(i\to\infty)$;

(2)C_i的码率$R(C_i)\geqslant\dfrac{1}{2}$, $i=1,2,\cdots$;

(3)C_i的相对最小距离$\Delta(C_i)\geqslant\delta(i=1,2,\cdots)$.

即存在Hermitian LCD 2-拟交换群码$C_i\leqslant(FG)^2$, $i=1,2,\cdots$使得码序列$C_1,C_2,\cdots$是渐近好的.

证毕.

5 结论

本文在拟交换群码上引入Hermitian内积,基于群表示论和概率论方法构造了一类Hermitian LCD拟交换群码,并证明了在任意有限域上都存在渐近好的Hermitian LCD拟交换群码. 这一点与自对偶拟交换群码的存在性条件(需要-1是有限域F中的平方元)不同. 我们将来的研究兴趣拟聚焦于非交换群码的渐近性的研究,将它们的渐近性与自对偶性, LCD性相结合进行研究.

参考文献

[1] 冯克勤, 刘凤梅. 代数与通信[M]. 北京: 高等教育出版社, 2005.
FENG K Q, LIU F M. Algebra and Communication[M]. Beijing: Higher Education Press, 2005. (in Chinese)

[2] 冯贵良, 吴新文. 代数几何码[M]. 北京: 科学出版社, 1998.
FENG G L, WU X W. Algebraic Geometric Code[M]. Beijing: Science Press, 1998. (in Chinese)

[3] SHANNON C E. A mathematical theory of communication[J]. The Bell System Technical Journal, 1948, 27(3): 379-423.

[4] PIERCE J. Limit distribution of the minimum distance of random linear codes[J]. IEEE Transactions on Information Theory, 1967, 13(4): 595-599.

[5] VARSHAMOV R R. Estimate of the number of signals in error correcting codes(in Russian) [J]. Doklady Akademii Nauk SSSR, 1957,117(5): 739-741.

[6] MACWILLIAMS F J, SLOANE N J A. The Theory of Error-Correcting Codes[M]. New York: Elsevier/North Holland, 1977.

[7] LIN S, WELDON E J. Long BCH codes are bad[J]. Information and Control, 1967, 11(4): 445-451.

[8] CASTAGNOLI G, MASSEY J L, SCHOELLER P A, et al. On repeated-root cyclic codes[J]. IEEE Transactions on Information Theory, 1991, 37(2): 337-342.
[9] MARTINEZ-PEREZ C, WILLEMS W. Is the class of cyclic codes asymptotically good?[J]. IEEE Transactions on Information Theory, 2006, 52(2): 696-700.
[10] CHEN C L, PETERSON W W, WELDON E J. Some results on quasi-cyclic codes[J]. Information and Control, 1969, 15(5): 407-423.
[11] CHEPYZHOV V V. New lower bounds for the minimal distance of linear quasi-cyclic and almost linear cyclic codes[J]. Problemy Peredachi Inf, 1992, 28(1): 39-51.
[12] KASAMI T. A Gilbert-Varshamov bound for quasi-cycle codes of rate 1/2[J]. IEEE Transactions on Information Theory, 1974, 20(5): 679.
[13] FAN Y, LIU H. Quasi-cyclic codes of index[J]. IEEE Transactions on Information Theory, 2016, 62(11): 6342-6347.
[14] MI J F, CAO X W. Asymptotically good quasi-cyclic codes of fractional index[J]. Discrete Mathematics, 2018, 341(2): 308-314.
[15] FAN Y, LIU H L. Thresholds of random quasi-abelian codes[J]. IEEE Transactions on Information Theory, 2015, 61(1): 82-90.
[16] LIN L R, FAN Y. Self-dual 2-quasi abelian codes[J]. IEEE Transactions on Information Theory, 2022, 68(10): 6417-6425.
[17] LING S, SOLE P. Good self-dual quasi-cyclic codes exist[J]. IEEE Transactions on Information Theory, 2003, 49(4): 1052-1053.
[18] MARTINEZ-PEREZ C, WILLEMS W. Self-dual doubly even 2-quasi-cyclic transitive codes are asymptotically good[J]. IEEE Transactions on Information Theory, 2007, 53(11): 4302-4308.
[19] CARLET C, GUILLEY S. Complementary Dual Codes for Counter-Measures to Side-Channel Attacks[M]//Coding Theory and Applications. Cham: Springer International Publishing, 2015: 97-105.
[20] MASSEY J L. Linear codes with complementary duals[J]. Discrete Mathematics, 1992, 106: 337-342.
[21] SENDRIER N. Linear codes with complementary duals meet the Gilbert-Varshamov bound[J]. Discrete Mathematics, 2004, 285(1): 345-347.
[22] ALPERIN J L, BELL B. Group Representations[M]. Switzerland: Springer-Verlag, 1995.
[23] 邱维声. 有限群与紧群的表示论[M]. 北京: 北京大学出版社, 1997.
[24] WAN Z X. Lectures on Finite Fields and Galois Rings[M]. Singapore: World Scientific, 2003.
[25] ZHANG G H, LIN L R, QIN C Y, et al. Hermitian self-dual 2-quasi-abelian codes[J]. Finite Fields and Their Applications, 2024, 94: 102357.
[26] FAN Y, LIN L R. Dihedral group codes over finite fields[J]. IEEE Transactions on Information Theory, 2021, 67(8): 5016-5025.

作者简介

张光辉　男，1973 年 4 月出生于河南省叶县. 现为宿迁学院数理学院教授. 主要研究方向为代数编码与密码.

E-mail: zghui@squ.edu.cn