有限域上两类线性码的构造

李文婷,衡子灵,李晓茹

(长安大学 理学院,西安 710064)

摘 要:利用定义集的方法构造了两类 p 元线性码,研究了它们的参数和重量分布.第一类线性码为三重极小码,可用于构造具有安全高效访问结构上的密钥共享方案.第二类线性码为二重线性码,且当 $p=3$ 时为自正交射影码,可用于构造量子码和强正则图.

关键词:线性码;自正交码;极小码;重量分布

中图分类号:O236.2 **文献标志码**:A **文章编号**:1000-2367(2024)03-0098-08

令 $q=p^m$,其中 p 为素数,m 为正整数,F_q 表示有 q 个元素的有限域.设非空集合 $C\subseteq F_q^n$,若 C 是 F_q^n 的线性子空间,则称 C 是 q 元线性码.如果线性码 C 的码长为 n,维数为 k,最小汉明距离为 d,则记 C 的参数为 $[n,k,d]$,其中 k 表示 C 的信息位数,k/n 称为 C 的传输效率,d 可用于刻画 C 的检错和纠错能力[1].特别地,线性码的最小汉明距离即为其中非零码字汉明重量的最小值.令 A_i 是码长为 n 的线性码 C 中所有汉明重量为 i 的码字个数,则称序列 $(1,A_1,A_2,\cdots,A_n)$ 为 C 的重量分布,称多项式 $A(z)=1+A_1z+A_2z^2+\cdots+A_nz^n$ 为 C 的重量计算器.线性码的重量分布既能用来计算信息在传输过程中发生错误的概率,又能用来衡量码的纠错能力.

对于 F_q 上的 $[n,k]$ 线性码 C,定义码字 $\boldsymbol{c}=(c_1,c_2,\cdots,c_n)\in C$ 的支撑集为 $\mathrm{supp}(\boldsymbol{c})=\{i:c_i\neq 0,1\leq i\leq n\}$.对于 C 中任意与 $\boldsymbol{c}$ 线性无关的码字 $\boldsymbol{c}'$,如果总满足 $\mathrm{supp}(\boldsymbol{c}')\not\subset\mathrm{supp}(\boldsymbol{c})$,则称 $\boldsymbol{c}$ 为极小码字.所有码字都是极小码字的线性码称为极小码.判定线性码为极小码的充分条件如下.

引理 1[2] 设 C 为有限域 F_q 上的线性码,C 中非零码字的最小汉明重量和最大汉明重量分别用 $w_{\min}$ 和 $w_{\max}$ 表示.若 $\dfrac{w_{\min}}{w_{\max}}>\dfrac{q-1}{q}$,则 C 为极小码.

定义线性码 C 的对偶码为 $C^{\perp}=\{\boldsymbol{c}^{\perp}\in F_q^n:\langle\boldsymbol{c}^{\perp},\boldsymbol{c}\rangle=0,\forall\,\boldsymbol{c}\in C\}$,其中 $\langle\boldsymbol{c}^{\perp},\boldsymbol{c}\rangle$ 表示 $\boldsymbol{c}^{\perp}$ 与 $\boldsymbol{c}$ 的标准内积.显然 $C^{\perp}$ 为 F_q 上的 $[n,n-k]$ 线性码.若 $d(C^{\perp})\geq 3$,则称 C 为射影码.若 $C\subset C^{\perp}$,则称 C 为自正交码.当 $p=3$ 时,判定 F_p 上线性码为自正交码的充要条件如下.

引理 2[3] 设 C 为有限域 F_p 上的线性码,$p=3$,则 C 为自正交码当且仅当它的每个码字的重量都能被 3 整除.

线性码具有良好的代数结构以及易于描述和加解密等特性,在计算机系统、通信系统、信息安全、数字签名、多方安全计算以及密钥共享等领域具有广泛的应用.极小码可用于构造具有安全高效访问结构的密钥共

收稿日期:2022-10-24;**修回日期**:2022-11-15.

基金项目:国家自然科学基金(12271059;11901049);陕西省高校科协青年人才托举计划项目(20200505);长安大学中央高校基本科研业务费专项资金(300102122202).

作者简介(通信作者):衡子灵(1990—),男,河南南阳人,长安大学教授,博士,研究方向为编码与密码,E-mail:zilingheng@chd.edu.cn.

引用本文:李文婷,衡子灵,李晓茹.有限域上两类线性码的构造[J].河南师范大学学报(自然科学版),2024,52(3):98-105.(Li Wenting,Heng Ziling,Li Xiaoru.Construction of two families of linear codes over finite fields[J].Journal of Henan Normal University(Natural Science Edition),2024,52(3):98-105.DOI:10.16366/j.cnki.1000-2367.2022.10.24.0001.)

享方案.密钥共享方案是一种设计秘密拆分和恢复方式的方法.2006 年,YUAN 等[4]提出利用极小码构造密钥共享方案的方法.自正交码在量子码的构造中有重要应用.在量子计算和量子通信中,量子码用于检测和纠正量子噪声引起的错误.文献[5－6]分别给出了量子码的 CSS 构造和 Steane 构造方法.利用这两种构造方法,满足一定条件的自正交码可用于构造量子码.射影二重码可用于构造强正则图.文献[7]建立了射影二重码和特定参数强正则图之间的关系.

近年来,大量文献构造了线性码并研究了它们的重量分布[8－16].DING 等[15]提出利用定义集构造线性码的方法.令 $D=\{d_1,d_2,\cdots,d_n\}\subseteq F_q$,$Tr_{q/p}(x)=x+x^p+x^{p^2}+\cdots+x^{p^{m-1}}$ 表示从 F_q 到 F_p 的迹函数.构造 p 元线性码 $C_D=\{(\mathrm{Tr}_{q/p}(bd_1),\mathrm{Tr}_{q/p}(bd_2),\cdots,\mathrm{Tr}_{q/p}(bd_n)):b\in F_q\}$,其中 D 称为 C_D 的定义集.通过选取合适的定义集 D,可以构造具有良好性能的线性码.YANG 等[16]构造了线性码 $C_D=\{(\mathrm{Tr}_{q/p}(ax^2))_{x\in D}:a\in F_q\}$,其中 $D=\{x\in F_q^*:\mathrm{Tr}_{q/p}(x)\in\langle\alpha^2\rangle\}$,$F_p^*=\langle\alpha\rangle$.文献[17]构造了线性码 $C_D=\{(\mathrm{Tr}_{q/p}(a_1x_1^2+a_2x_2^2+\cdots+a_tx_t^2))_{(x_1,x_2,\cdots,x_t)\in D}:(a_1,a_2,\cdots,a_t)\in F_q^t\}$,其中 $D=\{(x_1,x_2,\cdots,x_t)\in F_q^t\backslash\{(0,0,\cdots,0)\}:\mathrm{Tr}_{q/p}(x_1+x_2+\cdots+x_t)=0\}$.

本文主要构造如下两类 p 元线性码并研究它们的参数及其重量分布.

构造 1　令 $q=p^m$,$S=\{(x_1,x_2)\in F_q^2:\mathrm{Tr}_{q/p}(x_1+x_2)\in\langle\alpha^2\rangle\}$,其中 $m>1$ 为奇数,p 为奇素数且 $F_p^*=\langle\alpha\rangle$.构造线性码 $C_S=\{(\mathrm{Tr}_{q/p}(a_1x_1^2+a_2x_2^2))_{(x_1,x_2)\in S}:(a_1,a_2)\in F_q^2\}$.

构造 2　令 $q=p^m$,其中 p 为奇素数,t 为正整数,$F_p^*=\langle\alpha\rangle$.取定义集

$$D=\{(x_1,x_2,\cdots,x_t)\in F_q^t:\mathrm{Tr}_{q/p}(x_1+x_2+\cdots+x_t)\in\langle\alpha^2\rangle\}.$$

构造 p 元线性码 $C_D=\{(\mathrm{Tr}_{q/p}(a_1x_1+a_2x_2+\cdots+a_tx_t))_{(x_1,x_2,\cdots,x_t)\in D}:(a_1,a_2,\cdots,a_t)\in F_q^t\}$.

结果表明,第一类线性码为三重极小码,可用于构造具有安全高效访问结构上的密钥共享方案.第二类线性码为二重线性码,且当 $p=3$ 时为自正交射影码,可用于构造量子码和强正则图.

1　预备知识

令 $q=p^m$,其中 p 为素数且 m 为正整数,ζ_p 表示 p 次本原复单位根,$F_q^*=\langle\beta\rangle$.

对任意 $a\in F_q$,定义有限域 F_q 的加法特征为函数 $\varphi_a(x)=\zeta_p^{\mathrm{Tr}_{q/p}(ax)}$,$x\in F_q$.特别地,当 $a=0$ 时,称 φ_0 为 F_q 的平凡加法特征;当 $a=1$ 时,称 φ_1 为 F_q 的典范加法特征.显然,对任意 $a\in F_q$,$\varphi_a(x)=\varphi_1(ax)$.加法特征满足如下正交关系[18]:

$$\sum_{x\in F_q}\varphi_1(ax)=\begin{cases}q,\text{若 } a=0,\\0,\text{若 } a\in F_q^*.\end{cases}$$

定义有限域 F_q 的乘法特征为函数 $\psi_j(\beta^k)=\zeta_{q-1}^{jk}$,$k=0,1,\cdots,q-2$,$0\le j\le q-2$.特别地,$\psi_0$ 和 $\eta:=\psi_{(q-1)/2}$ 分别称为平凡乘法特征和二次乘法特征.乘法特征 ψ 的共轭 $\bar{\psi}$ 定义为 $\bar{\psi}(x)=\overline{\psi(x)}$,$x\in F_q^*$.乘法特征满足如下的正交关系[18]:

$$\sum_{x\in F_q^*}\psi_j(x)=\begin{cases}q-1, & \text{若 } j=0,\\0, & \text{若 } j\ne 0.\end{cases}$$

令 φ 为 F_q 的非平凡加法特征,$f\in F_q[x]$ 为正次数多项式.形如 $\sum_{c\in F_q}\varphi(f(c))$ 的特征和称为 Weil 和[18].令 φ 为 F_q 的加法特征,ψ 为 F_q 的乘法特征,定义有限域 F_q 上的高斯和为 $G(\psi,\varphi)=\sum_{x\in F_q^*}\psi(x)\varphi(x)$.

令 η 表示 F_q 的二次乘法特征,η' 表示 F_p 的二次乘法特征.对于任意 $z\in F_p^*$,

$$\eta(z)=\begin{cases}1, & \text{若 } m \text{ 为偶数},\\\eta'(z), & \text{若 } m \text{ 为奇数}.\end{cases}$$

引理 3[18]　令 q 为奇素数 p 的方幂.$f(x)=a_2x^2+a_1x+a_0\in F_q[x]$ 且 $a_2\ne 0$,φ 为 F_q 的非平凡加法特征,则 $\sum_{c\in F_q}\varphi(f(c))=\varphi(a_0-a_1^2(4a_2)^{-1})\eta(a_2)G(\eta,\varphi)$.

引理 4[18]　令 $q=p^m$,p 为奇素数且 m 为正整数.令 η,φ_1 分别表示 F_q 的二次乘法特征与典范加法特征,

则 $G(\eta,\varphi_1)=\begin{cases}(-1)^{m-1}\sqrt{q}, & \text{若 } p\equiv 1(\bmod 4),\\ (-1)^{m-1}(\sqrt{-1})^m\sqrt{q}, & \text{若 } p\equiv 3(\bmod 4).\end{cases}$

引理 5[18] 令 φ 是 F_q 的非平凡加法特征,ψ 是 F_q 的 d 阶乘法特征,$d=\gcd(n,q-1)$,则对于任意 a,$b\in F_q$,$a\neq 0$,$\sum\limits_{c\in F_q}\varphi(ac^n+b)=\varphi(b)\sum\limits_{j=1}^{d-1}\bar{\psi}^j(a)G(\psi^j,\varphi)$.

引理 6[18] 令 q 为奇素数 p 的方幂,则 -2 是 F_q 中的平方元当且仅当 $q\equiv 1(\bmod 8)$ 或 $q\equiv 3(\bmod 8)$.

令 $q-1=sN$,其中 s,N 为正整数,且 $s>1$,$N>1$,α 为 F_q 的本原元.定义 F_q 上 N 阶分圆类 $C_i^{(N,q)}=\beta^i\langle\beta^N\rangle$,$i=0,1,\cdots,N-1$,则 $|C_i^{(N,q)}|=\dfrac{q-1}{N}$.$N$ 阶高斯周期定义为 $\eta_i^{(N,q)}=\sum\limits_{x\in C_i^{(N,q)}}\varphi_1(x)$,其中 φ_1 表示 F_q 的典范加法特征.

引理 7[19] 令 $q=p^m$,p 为奇素数且 m 为正整数.则

$$\eta_0^{(2,q)}=\begin{cases}\dfrac{-1+(-1)^{m-1}\sqrt{q}}{2}, & \text{若 } p\equiv 1(\bmod 4),\\ \dfrac{-1+(-1)^{m-1}(\sqrt{-1})^m\sqrt{q}}{2}, & \text{若 } p\equiv 3(\bmod 4).\end{cases}\qquad \eta_1^{(2,q)}=-1-\eta_0^{(2,q)}.$$

令 $q=p^m$,p 为奇素数,m 为正整数,令 χ_1,φ_1 分别表示有限域 F_q 和 F_p 的典范加法特征,ψ 表示 F_q 的乘法特征,η 和 η' 分别表示 F_q 和 F_p 的二次乘法特征.将 $G(\eta,\chi_1)$ 简记为 $G(\eta)$,将 $G(\eta',\varphi_1)$ 简记为 $G(\eta')$,将线性码中码字 $\boldsymbol{c}$ 的汉明重量记为 $wt(\boldsymbol{c})$.设 β 是 F_q 的本原元,则 $\alpha:=\beta^{\frac{q-1}{p-1}}$ 是 F_p 的本原元.

2 三重极小码的构造

令 $S=\{(x_1,x_2)\in F_q^2:\mathrm{Tr}_{q/p}(x_1+x_2)\in\langle\alpha^2\rangle\}$,其中 $m>1$ 为奇数,p 为奇素数且 $F_p^*=\langle\alpha\rangle$.构造 p 元线性码 $C_S=\{(\mathrm{Tr}_{q/p}(a_1x_1^2+a_2x_2^2))_{(x_1,x_2)\in S}:(a_1,a_2)\in F_q^2\}$.显然 C_S 的码长为 $n_S=\dfrac{p-1}{2}p^{2m-1}$.下面研究其重量分布.记

$$N_0=|\{(x_1,x_2)\in F_q^2:\mathrm{Tr}_{q/p}(x_1+x_2)=0,\mathrm{Tr}_{q/p}(a_1x_1^2+a_2x_2^2)=0\}|,$$
$$N=|\{(x_1,x_2)\in F_q^2:\mathrm{Tr}_{q/p}(x_1+x_2)\in\langle\alpha^2\rangle,\mathrm{Tr}_{q/p}(a_1x_1^2+a_2x_2^2)=0\}|,$$
$$N_1=|\{(x_1,x_2)\in F_q^2:\mathrm{Tr}_{q/p}(x_1+x_2)\in\alpha\langle\alpha^2\rangle,\mathrm{Tr}_{q/p}(a_1x_1^2+a_2x_2^2)=0\}|,$$
$$B=|\{(x_1,x_2)\in F_q^2:\mathrm{Tr}_{q/p}(a_1x_1^2+a_2x_2^2)=0\}|.$$

引理 8 令 $q=p^m$,p 为奇素数且 m 为正奇数,则

$$B=\begin{cases}p^{2m}, & \text{若 } a_1=a_2=0,\\ p^{2m-1}, & \text{若 } a_1=0,a_2\neq 0 \text{ 或 } a_1\neq 0,a_2=0,\\ p^{2m-1}+\dfrac{p-1}{p}G(\eta)^2\eta(a_1a_2), & \text{若 } a_1a_2\neq 0.\end{cases}$$

证明 由加法特征和乘法特征的正交关系以及引理 3 可得:

$$B=\sum_{(x_1,x_2)\in F_q^2}\frac{1}{p}\sum_{y\in F_p}\varphi_1(y\,\mathrm{Tr}_{q/p}(a_1x_1^2+a_2x_2^2))=\frac{1}{p}\sum_{(x_1,x_2)\in F_q^2}(1+\sum_{y\in F_p^*}\chi_1(y(a_1x_1^2+a_2x_2^2)))=$$
$$p^{2m-1}+\frac{1}{p}\sum_{y\in F_p^*}\sum_{x_1\in F_q}\chi_1(ya_1x_1^2)\sum_{x_2\in F_q}\chi_1(ya_2x_2^2).$$

若 $a_1=a_2=0$,则 $B=p^{2m-1}+\dfrac{1}{p}(p-1)q^2=p^{2m}$.若 $a_1=0$,$a_2\neq 0$,则

$$B=p^{2m-1}+\frac{q}{p}\sum_{y\in F_p^*}\sum_{x_2\in F_q}\chi_1(ya_2x_2^2)=p^{2m-1}+p^{m-1}G(\eta)\eta(a_2)\sum_{y\in F_p^*}\eta'(y)=p^{2m-1}.$$

同理,若 $a_1\neq 0$,$a_2=0$,则 $B=p^{2m-1}$.若 $a_1a_2\neq 0$,则

$$B=p^{2m-1}+\frac{1}{p}G(\eta)^2\eta(a_1)\eta(a_2)\sum_{y\in F_p^*}\eta(y)^2=p^{2m-1}+\frac{p-1}{p}G(\eta)^2\eta(a_1a_2).$$

引理 9　令 $q=p^m$,p 为奇素数且 m 为正奇数,则

$$N_0=\begin{cases}p^{2m-1}, & \text{若 } a_1=a_2=0,\\ p^{2m-2}, & \text{若 } a_1=0,a_2\neq 0 \text{ 或 } a_1\neq 0,a_2=0,\\ p^{2m-2}+\dfrac{p-1}{p}G(\eta)^2\eta(a_1a_2), & \text{若 } a_1a_2\neq 0 \text{ 且 } \mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})=0,\\ p^{2m-2}, & \text{若 } a_1a_2\neq 0 \text{ 且 } \mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})\neq 0.\end{cases}$$

证明　由加法特征的正交关系以及引理 3 得,

$$N_0=\sum_{(x_1,x_2)\in F_q^2}\Big(\frac{1}{p}\sum_{y\in F_p}\varphi_1(y\mathrm{Tr}_{q/p}(x_1+x_2))\Big)\Big(\frac{1}{p}\sum_{z\in F_p}\varphi_1(z\mathrm{Tr}_{q/p}(a_1x_1^2+a_2x_2^2))\Big)=\frac{1}{p^2}\sum_{(x_1,x_2)\in F_q^2}(1+$$

$$\sum_{y\in F_p^*}\chi_1(y(x_1+x_2)))(1+\sum_{z\in F_p^*}\chi_1(z(a_1x_1^2+a_2x_2^2)))=p^{2m-2}+\frac{1}{p^2}(\Omega_1+\Omega_2+\Omega_3),\tag{1}$$

其中

$$\Omega_1:=\sum_{y\in F_p^*}\sum_{x_1\in F_q}\chi_1(yx_1)\sum_{x_2\in F_q}\chi_1(yx_2)=0,\tag{2}$$

$$\Omega_2:=\sum_{z\in F_p^*}\sum_{x_1\in F_q}\chi_1(za_1x_1^2)\sum_{x_2\in F_q}\chi_1(za_2x_2^2)=\begin{cases}(p-1)p^{2m}, & \text{若 } a_1=a_2=0,\\ 0, & \text{若 } a_1=0,a_2\neq 0 \text{ 或 } a_1\neq 0,a_2=0,\\ (p-1)G(\eta)^2\eta(a_1a_2), & \text{若 } a_1a_2\neq 0,\end{cases}\tag{3}$$

$$\Omega_3:=\sum_{y\in F_p^*}\sum_{z\in F_p^*}\sum_{x_1\in F_q}\chi_1(za_1x_1^2+yx_1)\sum_{x_2\in F_q}\chi_1(za_2x_2^2+yx_2).$$

下面分情况计算 Ω_3.当 $a_1a_2=0$ 时,显然 $\Omega_3=0$.当 $a_1a_2\neq 0$ 时,根据引理 3,

$$\Omega_3=\sum_{y\in F_p^*}\sum_{z\in F_p^*}\chi_1(-\frac{y^2}{4za_1}-\frac{y^2}{4za_2})\eta(za_1)\eta(za_2)G(\eta)^2=$$

$$G(\eta)^2\eta(a_1a_2)\sum_{z\in F_p^*}\Big(\sum_{y\in F_p}\varphi_1(-\frac{y^2}{4z}\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1}))-1\Big),$$

若 $\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})=0$,易知 $\Omega_3=(p-1)^2G(\eta)^2\eta(a_1a_2)$.若 $\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})\neq 0$,根据引理 3 可得

$$\Omega_3=G(\eta)^2\eta(a_1a_2)\Big(\sum_{z\in F_p^*}G(\eta')\eta'(-\frac{\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})}{4z})-(p-1)\Big)=G(\eta)^2\eta(a_1a_2)(G(\eta')\eta'(-\mathrm{Tr}_{q/p}(a_1^{-1}+$$

$$a_2^{-1}))\sum_{z\in F_p^*}\eta'(\frac{1}{4z})-(p-1))=(1-p)G(\eta)^2\eta(a_1a_2),$$

综上所述,

$$\Omega_3:=\begin{cases}(p-1)^2G(\eta)^2\eta(a_1a_2), & \text{若 } \mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})=0,\\ (1-p)G(\eta)^2\eta(a_1a_2), & \text{若 } \mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})\neq 0.\end{cases}\tag{4}$$

由式(1)～(4)可得 N_0 的值.

引理 10　令 $q=p^m$,p 为奇素数且 m 为正奇数,则

$$N+N_1=\begin{cases}(p-1)p^{2m-1}, & \text{若 } a_1=a_2=0,\\ (p-1)p^{2m-2}, & \text{若 } a_1=0,a_2\neq 0 \text{ 或 } a_1\neq 0,a_2=0,\\ (p-1)p^{2m-2}, & \text{若 } a_1a_2\neq 0 \text{ 且 } \mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})=0,\\ (p-1)(p^{2m-2}+\dfrac{1}{p}G(\eta)^2\eta(a_1a_2)), & \text{若 } a_1a_2\neq 0 \text{ 且 } \mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})\neq 0.\end{cases}\tag{5}$$

证明　由 $N_0+N+N_1=B$ 以及引理 8、引理 9 可得 $N+N_1$ 的值.

引理 11 令 $q=p^m$，p 为奇素数且 m 为正奇数，$S_2=\sum\limits_{y\in F_p^*}\sum\limits_{z\in F_p^*}\sum\limits_{x_1\in F_q}\chi_1(za_1x_1^2+y^2x_1)\sum\limits_{x_2\in F_q}\chi_1(za_2x_2^2+y^2x_2)$，则 $S_2=\begin{cases}0, & \text{若 } a_1a_2=0,\\ (p-1)^2G(\eta)^2\eta(a_1a_2), & \text{若 } a_1a_2\neq 0 \text{ 且 } \mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})=0,\\ -(p-1)G(\eta)^2\eta(a_1a_2), & \text{若 } a_1a_2\neq 0 \text{ 且 } \mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})\neq 0.\end{cases}$

证明 若 $a_1a_2=0$，显然 $S_2=0$. 若 $a_1a_2\neq 0$，则由引理 3 得 $S_2=\sum\limits_{y\in F_p^*}\sum\limits_{z\in F_p^*}\chi_1(-\frac{y^4}{4za_1}-\frac{y^4}{4za_2})\eta(za_1)\eta(za_2)G(\eta)^2=G(\eta)^2\eta(a_1a_2)\sum\limits_{z\in F_p^*}(\sum\limits_{y\in F_p}\varphi_1(-\frac{\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})}{4z}y^4)-1)$.

当 $\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})=0$ 时，$S_2=(p-1)^2G(\eta)^2\eta(a_1a_2)$. 下面设 $\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})\neq 0$. 为了计算 S_2，考虑以下两种情况.

情况 1 令 $p\equiv 3(\mathrm{mod}\ 4)$，则 $\gcd(4,p-1)=2$. 由引理 5 得

$$S_2=G(\eta)^2\eta(a_1a_2)\sum_{z\in F_p^*}\eta'(-\frac{\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})}{4z})G(\eta')-(p-1)G(\eta)^2\eta(a_1a_2)=$$
$$G(\eta)^2\eta(a_1a_2)\sum_{z\in F_p^*}\eta'(-\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1}))\eta'(z)G(\eta')-(p-1)G(\eta)^2\eta(a_1a_2)=$$
$$G(\eta)^2G(\eta')\eta(a_1a_2)\eta'(-\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1}))\sum_{z\in F_p^*}\eta'(z)-(p-1)G(\eta)^2\eta(a_1a_2)=$$
$$-(p-1)G(\eta)^2\eta(a_1a_2).$$

情况 2 令 $p\equiv 1(\mathrm{mod}\ 4)$，则 $\gcd(4,p-1)=4$. 定义高斯周期 $\eta_i^{(4,p)}=\sum\limits_{x\in C_i^{(4,p)}}\varphi_1(x)$，其中 $C_i^{(4,p)}=\alpha^i\langle\alpha^4\rangle$，$i=0,1,2,3$. 方便起见，将 $\eta_i^{(4,p)}$ 记为 η_i，将 $C_i^{(4,p)}$ 记为 C_i. 令 $t_z\equiv\log_\alpha(-\frac{\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})}{4z})(\mathrm{mod}\ 4)$，$t_z\in\{0,1,2,3\}$. 从而

$$S_2=G(\eta)^2\eta(a_1a_2)\sum_{z\in F_p^*}\sum_{y\in F_p^*}\varphi_1(-\frac{\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})}{4z}y^4)=4G(\eta)^2\eta(a_1a_2)\sum_{z\in F_p^*}\eta_{t_z}=$$
$$4G(\eta)^2\eta(a_1a_2)(\sum_{z\in C_0}\eta_{t_z}+\sum_{z\in C_1}\eta_{t_z}+\sum_{z\in C_2}\eta_{t_z}+\sum_{z\in C_3}\eta_{t_z}).$$

①若 $p\equiv 5(\mathrm{mod}\ 8)$，则 $-1\in C_2$. 根据引理 6，$4\in C_2$. 若 $\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})\in C_0$，则

当 $z\in C_0$ 时，$-\frac{\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})}{4z}\in C_0$；当 $z\in C_1$ 时，$-\frac{\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})}{4z}\in C_3$；

当 $z\in C_2$ 时，$-\frac{\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})}{4z}\in C_2$；当 $z\in C_3$ 时，$-\frac{\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})}{4z}\in C_1$.

由 $\eta_0+\eta_1+\eta_2+\eta_3=-1$ 可得，$S_2=4G(\eta)^2\eta(a_1a_2)\frac{p-1}{4}(\eta_0+\eta_3+\eta_2+\eta_1)=-(p-1)G(\eta)^2\eta(a_1a_2)$.

同理，若 $\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})\in C_i(i=1,2,3)$，则 $S_2=-(p-1)G(\eta)^2\eta(a_1a_2)$.

②若 $p\equiv 1(\mathrm{mod}\ 8)$，则 $-1\in C_0$. 由引理 6，$4\in C_0$. 类似①可得，$S_2=-(p-1)G(\eta)^2\eta(a_1a_2)$.

引理 12 令 $q=p^m$，p 为奇素数且 m 为正奇数，则 $N=N_1$.

证明 令 $A=\sum\limits_{(x_1,x_2)\in F_q^2}\sum\limits_{y\in F_p}\varphi_1(y^2\mathrm{Tr}_{q/p}(x_1+x_2))\sum\limits_{z\in F_p}\varphi_1(z\mathrm{Tr}_{q/p}(a_1x_1^2+a_2x_2^2))$. 一方面，由引理 3 和加法特征的正交关系得：

$$\sum_{y\in F_p}\varphi_1(y^2\mathrm{Tr}_{q/p}(x_1+x_2))=\begin{cases}p, & \text{若 } \mathrm{Tr}_{q/p}(x_1+x_2)=0,\\ G(\eta'), & \text{若 } \mathrm{Tr}_{q/p}(x_1+x_2)\in\langle\alpha^2\rangle,\\ -G(\eta'), & \text{若 } \mathrm{Tr}_{q/p}(x_1+x_2)\in\alpha\langle\alpha^2\rangle,\end{cases}$$

$$\sum_{z\in F_p}\varphi_1(z\mathrm{Tr}_{q/p}(a_1x_1^2+a_2x_2^2))=\begin{cases}p, & 若\ \mathrm{Tr}_{q/p}(a_1x_1^2+a_2x_2^2)=0,\\ 0, & 若\ \mathrm{Tr}_{q/p}(a_1x_1^2+a_2x_2^2)\neq 0.\end{cases}$$

从而

$$A=N_0p^2+(N-N_1)pG(\eta'). \tag{6}$$

另一方面,$A=q^2+\sum_{(x_1,x_2)\in F_q^2}\sum_{y\in F_p^*}\chi_1(y^2(x_1+x_2))+\sum_{(x_1,x_2)\in F_q^2}\sum_{z\in F_p^*}\chi_1(z(a_1x_1^2+a_2x_2^2))+S_2$,其中$S_2=\sum_{(x_1,x_2)\in F_q^2}\sum_{y\in F_p^*}\sum_{z\in F_p^*}\chi_1(y^2(x_1+x_2)+z(a_1x_1^2+a_2x_2^2))$. 由加法特征的正交关系,

$$\sum_{(x_1,x_2)\in F_q^2}\sum_{y\in F_p^*}\chi_1(y^2(x_1+x_2))=\sum_{y\in F_p^*}\sum_{x_1\in F_q}\chi_1(y^2x_1)\sum_{x_2\in F_q}\chi_1(y^2x_2)=0.$$

由引理 3,

$$\sum_{(x_1,x_2)\in F_q^2}\sum_{z\in F_p^*}\chi_1(z(a_1x_1^2+a_2x_2^2))=\begin{cases}(p-1)p^{2m}, & 若\ a_1=a_2=0,\\ 0, & 若\ a_1=0,a_2\neq 0\ 或\ a_1\neq 0,a_2=0,\\ (p-1)G(\eta)^2\eta(a_1a_2), & 若\ a_1a_2\neq 0.\end{cases}$$

再由引理 11 可得:

$$A=\begin{cases}p^{2m+1}, & 若\ a_1=a_2=0,\\ p^{2m}, & 若\ a_1=0,a_2\neq 0\ 或\ a_1\neq 0,a_2=0,\\ p^{2m}+p(p-1)G(\eta)^2\eta(a_1a_2), & 若\ a_1a_2\neq 0\ 且\ \mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})=0,\\ p^{2m}, & 若\ a_1a_2\neq 0\ 且\ \mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})\neq 0.\end{cases} \tag{7}$$

由等式(1)、(6)~(7)可得 $N-N_1$ 的值.

定理 1　令 p 为奇素数,$m>1$ 为奇数. 则线性码 C_S 是参数为$[\frac{p-1}{2}p^{2m-1},m,\frac{(p-1)^2}{2}p^{2m-2}-\frac{p-1}{2}p^{m-1}]$三重极小码,其重量分布如表 1 所示.

表 1　定理 1 中 C_S 的重量分布

Tab. 1　The weight distribution of C_S in theorem 1

重量	0	$\frac{(p-1)^2}{2}p^{2m-2}-\frac{p-1}{2}p^{m-1}$	$\frac{(p-1)^2}{2}p^{2m-2}$	$\frac{(p-1)^2}{2}p^{2m-2}+\frac{p-1}{2}p^{m-1}$
频次	1	$\frac{p-1}{2}p^{m-1}(p^m-3)$	$2(p^m-1)+\frac{(p^m-1)^2+(p-1)}{p}$	$\frac{p-1}{2}p^{m-1}(p^m-1)$

证明　记码字 $\boldsymbol{c}=(\mathrm{Tr}_{q/p}(a_1x_1^2+a_2x_2^2))_{(x_1,x_2)\in S}\in C_S$ 的汉明重量为$wt(\boldsymbol{c})$. 则 $wt(\boldsymbol{c})=n_S-N$. 由引理 4、引理 10 以及引理 12 可得 N 的值. 当 $p\equiv 1(\mathrm{mod}\ 4)$ 时,

$$wt(\boldsymbol{c})=\begin{cases}0, & 若\ a_1=a_2=0,\\ \frac{(p-1)^2}{2}p^{2m-2}, & 若\ a_1=0,a_2\neq 0\ 或\ a_1\neq 0,a_2=0\ 或\ a_1a_2\neq 0,\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})=0,\\ \frac{(p-1)^2}{2}p^{2m-2}+\frac{p-1}{2}p^{m-1}, & 若\ a_1a_2\neq 0,\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})\neq 0\ 且\ \eta(a_1a_2)=-1,\\ \frac{(p-1)^2}{2}p^{2m-2}-\frac{p-1}{2}p^{m-1}, & 若\ a_1a_2\neq 0\ 且\ \mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})\neq 0\ 且\ \eta(a_1a_2)=1.\end{cases}$$

由于 $A_0=1$,从而 C_S 的维数为 m. 下面计算每个非零重量的频次,设 $C_i^{(2,q)}=\beta^i\langle\beta^2\rangle,i=0,1,\eta_i^{(2,q)}=\sum_{x\in C_i^{(2,q)}}\chi_1(x)$. 当 $a_1=0,a_2\neq 0$ 或 $a_1\neq 0,a_2=0$ 或 $a_1a_2\neq 0,\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})=0$ 时,对应重量记为 w_1. 根据迹函数的性质可得 $A_{w_1}=2(p^m-1)+\frac{(p^m-1)^2+(p-1)}{p}$.

当 $a_1a_2\neq 0,\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})\neq 0$ 且 $\eta(a_1a_2)=-1$ 时,对应重量记为 w_2,下面计算 A_{w_2}. 显然 $|\{a_1\in F_q^*,$

$a_2 \in F_q^*:\eta(a_1a_2)=-1\}|=\dfrac{(q-1)^2}{2}$.记 $T_{-1}=|\{a_1\in F_q^*,a_2\in F_q^*:\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})=0,\eta(a_1a_2)=-1\}|$.从而

$$T_{-1}=\frac{1}{p}\Big(\sum_{a_1\in C_0^{(2,q)}}\sum_{a_2\in C_1^{(2,q)}}\Big(1+\sum_{y\in F_p^*}\chi_1(y(a_1+a_2))\Big)+\sum_{a_1\in C_1^{(2,q)}}\sum_{a_2\in C_0^{(2,q)}}\Big(1+\sum_{y\in F_p^*}\chi_1(y(a_1+a_2))\Big)\Big)=$$

$$\frac{(q-1)^2}{2p}+\frac{1}{p}\sum_{y\in F_p^*}\sum_{a_1\in C_0^{(2,q)}}\chi_1(ya_1)\sum_{a_2\in C_1^{(2,q)}}\chi_1(ya_2)+\frac{1}{p}\sum_{y\in F_p^*}\sum_{a_1\in C_1^{(2,q)}}\chi_1(ya_1)\sum_{a_2\in C_0^{(2,q)}}\chi_1(ya_2)=$$

$$\frac{(q-1)^2}{2p}+\frac{1}{p}\Big(\sum_{y\in C_0^{(2,q)}}\sum_{a_1\in C_0^{(2,q)}}\chi_1(ya_1)\sum_{a_2\in C_1^{(2,q)}}\chi_1(ya_2)+\sum_{y\in C_0^{(2,q)}}\sum_{a_1\in C_1^{(2,q)}}\chi_1(ya_1)\sum_{a_2\in C_0^{(2,q)}}\chi_1(ya_2)+$$

$$\sum_{y\in C_1^{(2,q)}}\sum_{a_1\in C_0^{(2,q)}}\chi_1(ya_1)\sum_{a_2\in C_1^{(2,q)}}\chi_1(ya_2)+\sum_{y\in C_1^{(2,q)}}\sum_{a_1\in C_1^{(2,q)}}\chi_1(ya_1)\sum_{a_2\in C_0^{(2,q)}}\chi_1(ya_2)\Big)=\frac{(q-1)^2}{2p}+$$

$$\frac{p-1}{2p}(\eta_0^{(2,q)},\eta_1^{(2,q)}+\eta_1^{(2,q)}\eta_0^{(2,q)}+\eta_1^{(2,q)}\eta_0^{(2,q)}+\eta_0^{(2,q)}\eta_1^{(2,q)})=\frac{(q-1)^2}{2p}+\frac{2(p-1)}{p}\eta_0^{(2,q)}\eta_1^{(2,q)}.$$

由引理 7 得 $A_{w_2}=\dfrac{(q-1)^2}{2}-T_{-1}=\dfrac{p-1}{2}p^{m-1}(p^m-1)$.当 $a_1a_2\neq 0,\mathrm{Tr}_{q/p}(a_1^{-1}+a_2^{-1})\neq 0$ 且 $\eta(a_1a_2)=1$ 时,同理可得 $A_{w_3}=\dfrac{p-1}{2}p^{m-1}(p^m-3)$.

当 $p\equiv 3(\mathrm{mod}\ 4)$ 时,同理可得 C_S 的重量分布.这两种情形下重量分布相同.此外,由引理 1 容易验证 C_S 是一个极小码.

3 二重线性码的构造

令 $q=p^m$,t 为正整数,$F_p^*=\langle\alpha\rangle$.取定义集 $D=\{(x_1,x_2,\cdots,x_t)\in F_q^t:\mathrm{Tr}_{q/p}(x_1+x_2+\cdots+x_t)\in\langle\alpha^2\rangle\}$.构造 p 元线性码 $C_D=\{(\mathrm{Tr}_{q/p}(a_1x_1+a_2x_2+\cdots+a_tx_t))_{(x_1,x_2,\cdots,x_t)\in D}:(a_1,a_2,\cdots,a_t)\in F_q^t\}$.

定理 2 令 p 为奇素数,t 为正整数.则 C_D 是一个二重线性码,参数为$[\dfrac{p-1}{2}p^{tm-1},m,\dfrac{(p-1)^2p^{tm-2}}{2}]$,其重量分布如表 2 所示.特别地,当 $p=3$ 时,C_D 既是一个自正交码,又是一个射影码.

表 2 定理 2 中的 C_D 重量分布

Tab. 2 The weight distribution of C_D in theorem 2

重量	0	$\dfrac{(p-1)^2p^{tm-2}}{2}$	$\dfrac{(p-1)p^{tm-1}}{2}$
频次	1	$p^{tm}-p$	$p-1$

证明 利用与定理 1 类似证明方法,易证 C_D 重量分布如表 2 所示.特别地,当 $p=3$ 时,C_D 的重量可以被 3 整除.由引理 2 得,C_D 是一个三元自正交码.由 Pless 幂等式易知 C_D 是一个三元射影码.

下面给出一些由 Magma 生成的例子,由 http://www.codetables.de/中的 Code Table 可以验证其为最优码.

例 1 令 $t=2,m=2,p=3$,则 C_D 为$[27,4,18]$最优码,$C_D^{\perp}$ 为$[27,23,3]$最优码.

例 2 令 $t=2,m=3,p=3$ 或 $t=3,m=2,p=3$,则 C_D 为$[243,6,162]$最优码,$C_D^{\perp}$ 为$[243,237,3]$最优码.

例 3 令 $t=3,m=1,p=3$,则 C_D 为$[9,6,3]$最优码,$C_D^{\perp}$ 为$[9,3,6]$最优码.由参数易知 C_D 为 NMDS 码.

4 总 结

本文通过选取定义集的方法构造了两类具有良好性质的 p 元线性码,确定了其参数和重量分布.主要结果及其应用如下:1)定理 1 中构造的线性码 C_S 为三重线性码,且为极小码.2)定理 2 中构造的线性码 C_D 为

二重线性码.当 $p=3$ 时，C_D 是一个自正交码，且为射影码.特别地，C_D 在一些情形下是最优码.3)本文得到的极小码可用于构造具有安全、高效访问结构上的密钥共享方案.三元自正交码可用于构造量子码.二重射影码可用于构造强正则图.

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.

[2] ASHIKHMIN A，BARG A.Minimal vectors in linear codes[J].IEEE Transactions on Information Theory，1998，44(5)：2010-2017.

[3] HUFFMAN W C，PLESS V.Fundamentals of Error-Correcting Codes[M].Cambridge：Cambridge University Press，2003.

[4] YUAN J，DING C S.Secret sharing schemes from three classes of linear codes[J].IEEE Transactions on Information Theory，2006，52(1)：206-212.

[5] STEANE A M.Simple quantum error-correcting codes[J].Physical Review A，1996，54(6)：4741.

[6] STEANE A M.Enlargement of Calderbank-Shor-Steane quantum codes[J].IEEE Transactions on Information Theory，1999，45(7)：2492-2495.

[7] CALDERBANK R，KANTOR W M.The geometry of two-weight codes[J].Bulletin of the London Mathematical Society，1986，18(2)：97-122.

[8] 杨淑娣，岳勤.一类线性码的完全重量分布[J].计算机工程与科学，2019，41(2)：281-285.
YANG S D，YUE Q.Complete weight enumerators of a class of linear codes[J].Computer Engineering & Science，2019，41(2)：281-285.

[9] 屈龙江，海昕，李超.纠错编码中的代数理论与方法[J].大学数学，2015，31(1)：7-13.
QU L J，HAI X，LI C.Algebraic theory and methods of error-correcting code[J].College Mathematics，2015，31(1)：7-13.

[10] 耿普，李超.有限域上线性码的深度分布与周期分布[J].应用科学学报，2007，25(3)：263-265.
GENG P，LI C.Depth distribution and period distribution of linear codes on finite field[J].Journal of Applied Sciences，2007，25(3)：263-265.

[11] 李超，冯克勤，胡卫群.一类性能好的线性码的构造[J].电子学报，2003，31(1)：51-53.
LI C，FENG K Q，HU W Q.Construction of A class of linear codes with good parameters[J].Acta Electronica Sinica，2003，31(1)：51-53.

[12] 胡丽琴，岳勤，朱小萌.具有两个非零点循环码的权重分布[J].中国科学：数学，2014，44(9)：1021-1034.
HU L Q，YUE Q，ZHU X M.Weight distributions of a class of cyclic codes with two nonzeros[J].Scientia Sinica(Mathematica)，2014，44(9)：1021-1034.

[13] 卢虹，杨淑娣，张同慧.基于 Weil 和的一类线性码的研究[J].河北大学学报(自然科学版)，2022，42(4)：350-357.
LU H，YANG S D，ZHANG T H.A class of linear codes from Weil sums[J].Journal of Hebei University(Natural Science Edition)，2022，42(4)：350-357.

[14] LI C J，YUE Q，FU F W.A construction of several classes of two-weight and three-weight linear codes[J].Applicable Algebra in Engineering，Communication and Computing，2017，28(1)：11-30.

[15] DING K L，DING C S.A class of two-weight and three-weight codes and their applications in secret sharing[J].IEEE Transactions on Information Theory，2015，61(11)：5835-5842.

[16] YANG S D，YAO Z G，ZHAO C G.A class of three-weight linear codes and their complete weight enumerators[J].Cryptography and Communications，2017，9(1)：133-149.

[17] AHN J，KA D，LI C J.Complete weight enumerators of a class of linear codes[J].Designs，Codes and Cryptography，2017，83(1)：83-99.

[18] LIDL R，NIEDERREITER H.Finite fields[M].2nd ed.Cambridge：Cambridge University Press，1997.

[19] MYERSON G.Period polynomials and Gauss sums for finite fields[J].Acta Arithmetica，1981，39(3)：251-264.

Constructions of two families of linear codes over finite fields

Li Wenting，Heng Ziling，Li Xiaoru

(School of Science，Chang'an University，Xi'an 710064，China)

Abstract：Two families of linear codes are constructed based on the defining-set method. The parameters and weight distributions of the codes are studied. The first family of linear codes have three weights and are minimal. They can be used to construct secret sharing schemes with interesting access structures. The second family of linear codes have two weights. If $p=3$，they are projective and self-orthogonal codes which can be used to construct strongly regular graphs and quantum codes.

Keywords：linear code；self-orthogonal code；minimal code；weight distribution

[责任编校　陈留院　赵晓华]