几类指标为2的不可约拟循环码的重量分布

高 健* 张耀宗 孟祥蕊 马芳卉
(山东理工大学数学与统计学院 淄博 255000)

摘 要：少重量线性码在认证码、结合方案以及秘密共享方案的构造中有着重要的应用。如何构造少重量线性码一直是编码理论研究的重要内容。该文通过选取特殊的定义集，构造了有限域上指标为2的不可约拟循环码，利用有限域上的高斯周期确定了几类指标为2的不可约拟循环码的重量分布，并且得到了几类2-重量线性码和3-重量线性码。结果表明，由该文构造的3类2-重量线性码中有两类是极大距离可分(MDS)码，另一类达到了Griesmer界。

关键词：线性码；拟循环码；高斯周期；重量分布
中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2022)12-4312-07
DOI: 10.11999/JEIT211104

Weight Distributions of Some Classes of Irreducible Quasi-cyclic Codes of Index 2

GAO Jian ZHANG Yaozong MENG Xiangrui MA Fanghui
(*School of Mathematics and Statistics*, *Shandong University of Technology*, *Zibo* 255000, *China*)

Abstract: Few-weight linear codes have important applications in constructing authentication codes, association schemes and secret sharing schemes. How to construct few-weight linear codes has always been an important topic of coding theory. In this paper, irreducible quasi-cyclic codes of index 2 over finite fields are constructed by selecting a special defining set. The weight distribution of several classes of irreducible quasi-cyclic codes of index 2 are determined by using Gaussian periods over finite fields. Some classes of 2-weight linear codes and 3-weight linear codes are obtained. The results show that two of the three classes of 2-weight linear codes constructed in this paper are Maximum Distance Separable (MDS) codes and the other class reaches Griesmer bound.

Key words: Linear codes; Quasi-cyclic codes; Gaussian periods; Weight distributions

1 引言

线性码的重量分布是编码理论中的一个重要研究问题。近几年，线性码的重量分布，尤其是循环码的重量分布，被国内外的编码学者广泛关注与研究。Ding等人[1]研究了不可约循环码的重量分布，利用不可约循环码构造了一些参数较好的线性码。基于指数和理论，文献[2,3]在有限域上某些可约循环码的重量分布研究中也取得了很大进展。

少重量线性码，如常重量线性码[4]、2-重量线性码[5]、3-重量线性码[6]以及其他少重量线性码[7,8]等，是重要的线性码类，可用于认证码[9]、结合方案以及秘密共享方案的构造。Ding[10]基于不可约循环码的重量分布构造了几类3-重量线性码。Schmidt等人[11]基于离散傅里叶变换和高斯和理论得到了不可约循环码至多有两个重量的充要条件。Zhou等人[12]构造了7类3-重量循环码并分析了由这些3-重量循环码得到的秘密共享方案的结构。

拟循环码是一类重要的线性码，它与卷积码和低密度校验码密切相关。指标为2的拟循环码也称为分块长度相等的双循环码。Borges等人[13]给出了2元域上双循环码的显式生成元并确定了双循环码及其对偶码生成元之间的关系。Gao等人[14,15]给出了4元双循环码的生成元以及与对偶码生成元之间的关系，并且证明了4元双循环码是渐进优的。Pa-

收稿日期：2021-10-11；改回日期：2022-04-18；网络出版：2022-05-07
*通信作者： 高健 dezhougaojian@163.com
基金项目：国家自然科学基金(12071264, 11701336, 11626144, 11671235)，山东省自然科学基金(ZR2021QA047)，山东省高等学校“青创人才引育计划”
Foundation Items: The National Natural Science Foundation of China (12071264,11701336, 11626144, 11671235), The Natural Science Foundation of Shandong Province (ZR2021QA047), The IC Program of Shandong Institutions of Higher Learning For Youth Innovative Talents

tanker等人[16]利用高斯和确定了几类2元双循环码的重量分布。

本文主要利用有限域上指标为2的不可约拟循环码构造少重量的线性码。首先，基于有限域上的高斯周期，本文给出了几类指标为2的不可约拟循环码的重量分布；其次，基于不可约拟循环码的重量分布，本文构造了几类2-重量线性码和3-重量线性码，其中包括3类最优的2-重量线性码。

2　基本知识

令p是一个素数，$q=p^m$，$r=q^t$，其中m和t是正整数。令F_q表示q元有限域。 ${F_q}^l$的线性子空间称为有限域F_q上码长为l的线性码。A_i表示线性码C中Hamming重量为i的码字个数。 定义码长为l的线性码C的重量分布多项式为$1+A_1x+\cdots+A_lx^l$。

令 $l=m_0+m_1$ 。 如 果C 中 的 任 意 码 字 $c=(c_{1,0},c_{1,1},\cdots,c_{1,m_0-1}|c_{2,0},c_{2,1},\cdots,c_{2,m_1-1})$经循环移位$T$作用后有$T(c)=(c_{1,m_0-1},c_{1,0},\cdots,c_{1,m_0-2}|c_{2,m_1-1},c_{2,0},\cdots,c_{2,m_1-2})\in C$则称线性码$C$是分块长度为$(m_0,m_1)$的双循环码。若$m_0=m_1$，则称线性码$C$是指标为2的拟循环码。

令$F_r=F_{q^t}$表示q^t元有限域且ζ为其本原元。设$\theta\in {F_r}^*=F_r\backslash\{0\}$，ord $(\theta)=n$，$h(x)$是θ^{-1}在F_q上的极小多项式，$\deg(h(x))=s$，则$F_q[x]/\langle h(x)\rangle=F_{q^s}$是一个$q^s$元有限域且$\theta\in {F_{q^s}}^*=F_{q^s}\backslash\{0\}$。因为$\deg(h(x))=s$，所以$s|t$，$(q^s-1)|(q^t-1)$。令${F_{q^s}}^*=\langle w\rangle$，其中$w=\zeta^{\frac{q^t-1}{q^s-1}}$，则$w$为$F_{q^s}$的本原元。

假设$\theta=w^N$，其中$nN=q^s-1$。定义指标为2的不可约拟循环码为

$$\begin{aligned}C=&\{(\mathrm{Tr}(\alpha\beta_0),\mathrm{Tr}(\alpha\beta_0\theta),\cdots,\mathrm{Tr}(\alpha\beta_0\theta^{n-1})|\\&\mathrm{Tr}(\alpha\beta_1),\mathrm{Tr}(\alpha\beta_1\theta),\cdots,\mathrm{Tr}(\alpha\beta_1\theta^{n-1}))|\alpha\in F_{q^s}\}\end{aligned}\tag{1}$$

其中，$\beta_0,\beta_1\in {F_{q^s}}^*\backslash\langle\theta\rangle$，$\mathrm{Tr}(\cdot)$表示从$F_{q^s}$到$F_q$的迹映射。此外，$C$在$F_q$上的校验多项式为$\theta^{-1}$的极小多项式$h(x)$且维数为$\dim(C)=s$。

设$\mathrm{Tr}_{q/p}$表示从F_q到F_p的迹映射，χ是从F_q到模长为1的复数组成的乘法群的映射，对任意的$x,y\in F_q$有$\chi(x+y)=\chi(x)\chi(y)$。设$b\in F_q$，定义

$$\chi_b(c)=\mathrm{e}^{2\pi\sqrt{-1}\mathrm{Tr}_{q/p}(bc)/p},\forall c\in F_q\tag{2}$$

为F_q上的加法特征。如果$b=0$，则$\chi_0(c)=1$，χ_0称为F_q上的平凡加法特征；如果$b=1$，则χ_1称为F_q上的标准加法特征。

定义${C_i}^{(N,q^s)}=w^i\langle w^N\rangle$，$i=0,1,\cdots,N$，其中$\langle w^N\rangle$表示${F_{q^s}}^*$的一个子群，陪集${C_i}^{(N,q^s)}$称为$F_{q^s}$的阶为$N$的分圆类。根据加法特征和分圆类，定义$F_{q^s}$上的高斯周期为

$${\eta_i}^{(N,q^s)}=\sum_{x\in {C_i}^{(N,q^s)}}\chi(x),\ \ i=0,1,\cdots,N$$

其中，χ是F_{q^s}上的标准加法特征。一般情况下，高斯周期的值很难计算，但是可以通过高斯多项式$\psi_{(N,q^s)}(X)$[17]得到一些特殊的值，其中高斯多项式定义为

$$\psi_{(N,q^s)}(X)=\prod_{i=0}^{N-1}(X-{\eta_i}^{(N,q^s)})$$

引理1[1]　当$N=2$时，高斯周期的值为

$${\eta_0}^{(2,q^s)}=\begin{cases}\dfrac{-1+(-1)^{s\cdot m-1}q^{\frac{s}{2}}}{2}, & p\equiv 1(\mathrm{mod}4)\\ \dfrac{-1+(-1)^{s\cdot m-1}(\sqrt{-1})^{sm}q^{\frac{s}{2}}}{2}, & p\equiv 3(\mathrm{mod}4)\end{cases}$$

和${\eta_1}^{(2,q^s)}=-1-{\eta_0}^{(2,q^s)}$。

引理2[1]　当$N=3$时，高斯多项式$\psi_{(3,q^s)}(X)$的分解如下：

(1)如果$p\equiv 2(\mathrm{mod}3)$，则$s\cdot m$为偶数并且

$$\psi_{(3,q^s)}(X)=\begin{cases}3^{-3}(3X+1+2q^{\frac{s}{2}})(3X+1-q^{\frac{s}{2}})^2,\\ \qquad\dfrac{sm}{2}\text{为偶数}\\ 3^{-3}(3X+1-2q^{\frac{s}{2}})(3X+1+q^{\frac{s}{2}})^2,\\ \qquad\dfrac{sm}{2}\text{为奇数}\end{cases}$$

(2)如果$p\equiv 1(\mathrm{mod}3),s\cdot m\equiv 0(\mathrm{mod}3)$，则

$$\begin{aligned}\psi_{(3,q^s)}(X)=&\frac{1}{27}(3X+1-c_1q^{\frac{s}{3}})\\&\cdot\left(3X+1+\frac{1}{2}(c_1+9d_1)q^{\frac{s}{3}}\right)\\&\cdot\left(3X+1+\frac{1}{2}(c_1-9d_1)q^{\frac{s}{3}}\right)\end{aligned}$$

其中，c_1和d_1满足$4q^{\frac{s}{3}}=c_1^2+27d_1^2,c_1\equiv 1(\mathrm{mod}3)$，$\gcd(c_1,p)=1$。

引理3[1]　当$N=4$时，高斯多项式$\psi_{(4,q^s)}(X)$的分解如下：

(1)如果$p\equiv 3(\mathrm{mod}4)$，则$s\cdot m$为偶数并且

$$\psi_{(3,q^s)}(X)=\begin{cases}4^{-4}(4X+1+3q^{\frac{s}{2}})(4X+1-q^{\frac{s}{2}})^3,\\ \qquad\dfrac{sm}{2}\text{为偶数}\\ 4^{-4}(4X+1-3q^{\frac{s}{2}})(4X+1+q^{\frac{s}{2}})^3,\\ \qquad\dfrac{sm}{2}\text{为奇数}\end{cases}$$

(2)如果$p\equiv 1(\mathrm{mod}4),s\cdot m\equiv 0(\mathrm{mod}4)$，则

$$\begin{aligned}\psi_{(3,q^s)}(X)=&4^{-4}((4X+1)+q^{\frac{s}{2}}+2u_1q^{\frac{s}{4}})\\&\cdot((4X+1)+q^{\frac{s}{2}}-2u_1q^{\frac{s}{4}})^3\\&\times 4^{-4}((4X+1)-q^{\frac{s}{2}}+4v_1q^{\frac{s}{4}})\\&\cdot((4X+1)-q^{\frac{s}{2}}-4v_1q^{\frac{s}{4}})\end{aligned}$$

其中，u_1,v_1 满足$q^{\frac{s}{2}}=u_1^2+4v_1^2,u_1\equiv 1\,(\mathrm{mod}4)$，$\gcd(u_1,p)=1$。

为了确定指标为2的不可约拟循环码的重量分布，本文还需要以下引理。

引理 4[1] 设e_1是q^s-1的正因数并且$0\le i\le e_1$，则

$$\begin{aligned}&\{xy:y\in F_q{}^*,x\in C_i^{(e_1,q^s)}\}\\&\quad=\tfrac{q-1}{e_1}\ \gcd(\tfrac{q^s-1}{q-1},e_1)\cdot C_i^{(\gcd(\frac{q^s-1}{q-1},e_1),q^s)},\end{aligned}$$

其中 $\dfrac{q-1}{e_1}\gcd\left(\frac{q^s-1}{q-1},e_1\right)\cdot C_i^{(\gcd(\frac{q^s-1}{q-1},e_1),q^s)}$ 表示$C_i^{(\gcd(\frac{q^s-1}{q-1},e_1),q^s)}$中的任意元素在集合$\{xy:y\in F_q^*,x\in C_i^{(e_1,q^s)}\}$中出现的次数均为$\dfrac{q-1}{e_1}\gcd\left(\frac{q^s-1}{q-1},e_1\right)$。

3 几类指标为2的不可约拟循环码的重量分布

设$N>1$是一个正整数且满足$n=\dfrac{q^s-1}{N}$，$N_1=\gcd\left(\dfrac{q^s-1}{q-1},N\right)$。令$\theta=w^N$，其中$w$为$F_{q^s}$的本原元。$Z(q^s,\beta_0)$和$Z(q^s,\beta_1)$分别为使等式$\mathrm{Tr}(\alpha\beta_0\theta^i)=0$和$\mathrm{Tr}(\alpha\beta_1\theta^j)=0$成立的$i,j$的个数。对于$C$中任意的码字$c$，如果$\alpha\ne 0$，则它的Hamming重量为$W_H(c)=2n-Z(q^s,\beta_0)-Z(q^s,\beta_1)$，其中

$$Z(q^s,\beta_0)=\left|\{0\le i\le n-1:\mathrm{Tr}(\alpha\beta_0\theta^i)=0\}\right|,$$

$$Z(q^s,\beta_1)=\left|\{0\le j\le n-1:\mathrm{Tr}(\alpha\beta_1\theta^j)=0\}\right|$$

令χ'为F_q上的加法特征，由引理4有

$$Z(q^s,\beta_0)=\frac{n}{q}+\frac{(q-1)N_1}{Nq}\cdot\eta_k{}^{(N_1,q^s)},$$

$$Z(q^s,\beta_1)=\frac{n}{q}+\frac{(q-1)N_1}{Nq}\cdot\eta_l{}^{(N_1,q^s)}$$

其中，$k,l=0,1,\cdots,N_1-1$。

下面给出当$\beta_0,\beta_1\in F_{q^s}^*\backslash\langle\theta\rangle,N_1=2,3,4$时，式(1)定义的指标为2的不可约拟循环码的重量分布。显然，$C_0{}^{(N_1,q^s)}\backslash C_0{}^{(N,q^s)},C_1{}^{(N_1,q^s)},\cdots,C_{N_1-1}^{(N_1,q^s)}$构成了$F_{q^s}^*\backslash\langle\theta\rangle$的一个划分。定义$S$为$F_{q^s}^*\backslash\langle\theta\rangle$中的一个分圆类。

定理1 设N是q^s-1的正因数且使得$N_1=\gcd\left(\dfrac{q^s-1}{q-1},N\right)=2$，则

情形(1)如果β_0,β_1在相同的分圆类S中，则由式(1)定义的不可约拟循环码的重量分布如表1所示。

情形(2)如果β_0,β_1在不同的分圆类S中，则由式(1)定义的不可约拟循环码的重量分布如表2所示。

证明 对于情形(1)本文只给出当$\beta_0,\beta_1\in C_0^{(2,q^s)}\backslash C_0^{(N,q^s)}$时的证明过程。

当$\alpha\in C_0^{(2,q^s)}$时，因为$\beta_0,\beta_1\in C_0^{(2,q^s)}\backslash C_0^{(N,q^s)}$，所以$\alpha\beta_0,\alpha\beta_1\in C_0^{(2,q^s)}$。此时，对于$c\in C$，有$W_H(c)=2n-2\left(\dfrac{n}{q}+\dfrac{2(q-1)}{Nq}\cdot\eta_0^{(2,q^s)}\right)$，出现的频数为$\dfrac{q^s-1}{2}$。同理，当$\alpha\in C_1^{(2,q^s)}$时，对于$c\in C$，有$W_H(c)=2n-2\left(\dfrac{n}{q}+\dfrac{2(q-1)}{Nq}\cdot\eta_1^{(2,q^s)}\right)$，出现的频数为$\dfrac{q^s-1}{2}$。因此，式(1)定义的指标为2的不可约拟循环码的重量分布如表1所示。

对于情形(2)，可采用相同的讨论方法。证毕

推论1 如果β_0,β_1满足定理1中的情形(1)，则式(1)定义的指标为2的不可约拟循环码是一个参数为$\left[\dfrac{2(q^s-1)}{N},s,\dfrac{2(q-1)(q^s-q^{\frac{s}{2}})}{Nq}\right]$的2-重量线性码，其重量分布为$1+\dfrac{q^s-1}{2}x^{\frac{2(q-1)(q^s-q^{\frac{s}{2}})}{Nq}}+\dfrac{q^s-1}{2}x^{\frac{2(q-1)(q^s+q^{\frac{s}{2}})}{Nq}}$。

证明 如果β_0,β_1满足定理1中的情形(1)，则由引理1可知，当$p\equiv 1(\mathrm{mod}4)$时，$\eta_0^{(2,q^s)}=-\dfrac{q^{\frac{s}{2}}+1}{2},\eta_1^{(2,q^s)}=\dfrac{q^{\frac{s}{2}}-1}{2}$；当$p\equiv 3(\mathrm{mod}4)$时，$\eta_0^{(2,q^s)}=\dfrac{q^{\frac{s}{2}}-1}{2},\eta_1^{(2,q^s)}=-\dfrac{q^{\frac{s}{2}}+1}{2}$。将$\eta_0^{(2,q^s)},\eta_1^{(2,q^s)}$的值分别代入表1中，可得到式(1)中定义的指标为2的不可约拟循环码是一个参数为$\left[\dfrac{2(q^s-1)}{N},s,\dfrac{2(q-1)(q^s-q^{\frac{s}{2}})}{Nq}\right]$的2-重量线性码，其重量分布为$1+\dfrac{q^s-1}{2}x^{\frac{2(q-1)(q^s-q^{\frac{s}{2}})}{Nq}}+\dfrac{q^s-1}{2}x^{\frac{2(q-1)(q^s+q^{\frac{s}{2}})}{Nq}}$。证毕

类似于定理1，当$N_1=\gcd\left(\dfrac{q^s-1}{q-1},N\right)=3$时，式(1)定义的指标为2的不可约拟循环码的重量分布由以下定理给出。

表 1 情形(1)：不可约拟循环码的重量分布

重量(i)	频数(A_i)
0	1
$\dfrac{2}{Nq}(q-1)(q^s-1-2\eta_0^{(2,q^s)})$	$\dfrac{q^s-1}{2}$
$\dfrac{2}{Nq}(q-1)(q^s-1-2\eta_1^{(2,q^s)})$	$\dfrac{q^s-1}{2}$

表 2 情形(2)：不可约拟循环码的重量分布

重量(i)	频数(A_i)
0	1
$\dfrac{2}{N}(q-1)q^{s-1}$	q^s-1

定理 2　设 N 是 q^s-1 的正因数且使得 $N_1=\gcd\left(\frac{q^s-1}{q-1},N\right)=3$，则

情形(3) 如果 β_0,β_1 在相同的分圆类 S 中，则式(1)定义的不可约拟循环码的重量分布如表3所示。

情形(4) 如果 β_0,β_1 在不同的分圆类 S 中，则式(1)定义的不可约拟循环码的重量分布如表4所示。

推论 2　设 N 是 q^s-1 的正因子，$N_1=\gcd\left(\frac{q^s-1}{q-1},N\right)=3,p\equiv 2(\mathrm{mod}3)$。若 β_0,β_1 满足定理2中情形(3)且 $s\cdot m\equiv 0(\mathrm{mod}4)$，则式(1)定义的不可约拟循环码是参数为 $\left[\frac{2(q^s-1)}{N},s,\frac{2(q-1)(q^s-q^{\frac{s}{2}})}{Nq}\right]$ 的2-重量线性码，其重量分布为

$$1+\frac{2(q^s-1)}{3}x^{\frac{2(q-1)(q^s-q^{\frac{s}{2}})}{Nq}}+\frac{q^s-1}{3}x^{\frac{2(q-1)(q^s+2q^{\frac{s}{2}})}{Nq}}。$$

若 $s\cdot m\equiv 2(\mathrm{mod}4)$，则式(1)定义的不可约拟循环码是参数为 $\left[\frac{2(q^s-1)}{N},s,\frac{2(q-1)(q^s-2q^{\frac{s}{2}})}{Nq}\right]$ 的2-重量线性码，其重量分布为

$$1+\frac{q^s-1}{3}x^{\frac{2(q-1)(q^s-2q^{\frac{s}{2}})}{Nq}}+\frac{2(q^s-1)}{3}x^{\frac{2(q-1)(q^s+q^{\frac{s}{2}})}{Nq}}。$$

证明：　当 β_0,β_1 满足定理2中情形(3)时，如果 $s\cdot m\equiv 0(\mathrm{mod}4)$，此时 $\frac{s\cdot m}{2}$ 为偶数，由引理2可得 $\eta_0^{(3,q^s)}=-\frac{1+2q^{\frac{s}{2}}}{3},\eta_1^{(3,q^s)}=\eta_1^{(3,q^s)}=-\frac{1-2q^{\frac{s}{2}}}{3}$，将其代入表3，可得到推论2中的第1种结果；如果 $s\cdot m\equiv 2(\mathrm{mod}4)$，此时 $\frac{s\cdot m}{2}$ 为奇数，则由引理2可得 $\eta_0^{(3,q^s)}=-\frac{1-2q^{\frac{s}{2}}}{3},\eta_1^{(3,q^s)}=\eta_1^{(3,q^s)}=-\frac{1+2q^{\frac{s}{2}}}{3}$，将其代入表3，可得到推论2中的另一种结果。证毕

表 3　情形(3)：不可约拟循环码的重量分布

重量(i)	频数(A_i)
0	1
$\frac{2}{Nq}(q-1)(q^s-1-3\eta_0^{(3,q^s)})$	$\frac{q^s-1}{3}$
$\frac{2}{Nq}(q-1)(q^s-1-3\eta_1^{(3,q^s)})$	$\frac{q^s-1}{3}$
$\frac{2}{Nq}(q-1)(q^s-1-3\eta_2^{(3,q^s)})$	$\frac{q^s-1}{3}$

表 4　情形(4)：不可约拟循环码的重量分布

重量(i)	频数(A_i)
0	1
$\frac{1}{Nq}(q-1)[2(q^s-1)-3(\eta_0^{(3,q^s)}+\eta_1^{(3,q^s)})]$	$\frac{q^s-1}{3}$
$\frac{1}{Nq}(q-1)[2(q^s-1)-3(\eta_1^{(3,q^s)}+\eta_2^{(3,q^s)})]$	$\frac{q^s-1}{3}$
$\frac{1}{Nq}(q-1)[2(q^s-1)-3(\eta_2^{(3,q^s)}+\eta_0^{(3,q^s)})]$	$\frac{q^s-1}{3}$

类似于推论2的证明方法，可得到以下3个结论。

推论 3　设 N 是 q^s-1 的正因子，$N_1=\gcd\left(\frac{q^s-1}{q-1},N\right)=3,p\equiv 2(\mathrm{mod}3)$。若 β_0,β_1 满足定理2中的情形(4)且 $s\cdot m\equiv 0(\mathrm{mod}4)$，则式(1)定义的不可约拟循环码是参数为 $\left[\frac{2(q^s-1)}{N},s,\frac{2(q-1)(q^s-q^{\frac{s}{2}})}{Nq}\right]$ 的2-重量线性码，其重量分布为

$$1+\frac{2(q^s-1)}{3}x^{\frac{(q-1)(2q^s+q^{\frac{s}{2}})}{Nq}}+\frac{q^s-1}{3}x^{\frac{2(q-1)(q^s-q^{\frac{s}{2}})}{Nq}}。$$

若 $s\cdot m\equiv 2(\mathrm{mod}4)$，则式(1)定义的不可约拟循环码是参数为 $\left[\frac{2(q^s-1)}{N},s,\frac{(q-1)(2q^s-q^{\frac{s}{2}})}{Nq}\right]$ 的2-重量线性码，其重量分布为

$$1+\frac{2(q^s-1)}{3}x^{\frac{(q-1)(2q^s-q^{\frac{s}{2}})}{Nq}}+\frac{2(q^s-1)}{3}x^{\frac{2(q-1)(q^s+q^{\frac{s}{2}})}{Nq}}。$$

推论 4　设 N 是 q^s-1 的正因子，$N_1=\gcd\left(\frac{q^s-1}{q-1},N\right)=3,p\equiv 1(\mathrm{mod}3)$。若 β_0,β_1 满足定理2中的情形(3)且 $s\cdot m\equiv 0(\mathrm{mod}3)$，则式(1)定义的不可约拟循环码是一个参数为 $\left[\frac{2(q^s-1)}{N},s\right]$ 的3-重量线性码，其重量分布为

$$1+\frac{q^s-1}{3}x^{\frac{2(q-1)(q^s-c_1q^{\frac{s}{3}})}{Nq}}+\frac{q^s-1}{3}x^{\frac{2(q-1)(q^s+\frac{1}{2}(c_1+9d_1)q^{\frac{s}{3}})}{Nq}}+\frac{q^s-1}{3}x^{\frac{2(q-1)(q^s+\frac{1}{2}(c_1-9d_1)q^{\frac{s}{3}})}{Nq}}。$$

推论 5　设 N 是 q^s-1 的正因子，$N_1=\gcd\left(\frac{q^s-1}{q-1},N\right)=3,p\equiv 1(\mathrm{mod}3)$。若 β_0,β_1 满足定理2中的情形(4)且 $s\cdot m\equiv 0(\mathrm{mod}3)$，则式(1)定义的不可约拟循环码是参数为 $\left[\frac{2(q^s-1)}{N},s\right]$ 的3-重量线性码，其重量分布为

$$1+\frac{q^s-1}{3}x^{\frac{(q-1)(2q^s+\frac{1}{2}(9d_1-c_1)q^{\frac{s}{3}})}{Nq}}+\frac{q^s-1}{3}x^{\frac{(q-1)(2q^s-\frac{1}{2}(c_1+9d_1)q^{\frac{s}{3}})}{Nq}}+\frac{q^s-1}{3}x^{\frac{(q-1)(2q^s+c_1q^{\frac{s}{3}})}{Nq}}。$$

类似定理1，当 $N_1=\gcd\left(\frac{q^s-1}{q-1},N\right)=4$ 时，式(1)定义的不可约拟循环码的重量分布由以下定理给出。

定理 3　设 N 是 q^s-1 的正因数使得 $N_1=\gcd\left(\frac{q^s-1}{q-1},N\right)=4$，则

情形(5)如果 β_0,β_1 在相同的分圆类 S 中，则式(1)定义的不可约拟循环码的重量分布如表5所示。

表 5 情形(5)：不可约拟循环码的重量分布

重量(i)	频数(A_i)
0	1
$\frac{2}{Nq}(q-1)(q^s-1-4\eta_0^{(4,q^s)})$	$\frac{q^s-1}{4}$
$\frac{2}{Nq}(q-1)(q^s-1-4\eta_1^{(4,q^s)})$	$\frac{q^s-1}{4}$
$\frac{2}{Nq}(q-1)(q^s-1-4\eta_2^{(4,q^s)})$	$\frac{q^s-1}{4}$
$\frac{2}{Nq}(q-1)(q^s-1-4\eta_3^{(4,q^s)})$	$\frac{q^s-1}{4}$

表 6 情形(6)：不可约拟循环码的重量分布

重量(i)	频数(A_i)
0	1
$\frac{2}{Nq}(q-1)[(q^s-1)-2(\eta_0^{(4,q^s)}+\eta_1^{(4,q^s)})]$	$\frac{q^s-1}{4}$
$\frac{2}{Nq}(q-1)[(q^s-1)-2(\eta_1^{(4,q^s)}+\eta_2^{(4,q^s)})]$	$\frac{q^s-1}{4}$
$\frac{2}{Nq}(q-1)[(q^s-1)-2(\eta_2^{(4,q^s)}+\eta_3^{(4,q^s)})]$	$\frac{q^s-1}{4}$
$\frac{2}{Nq}(q-1)[(q^s-1)-2(\eta_3^{(4,q^s)}+\eta_0^{(4,q^s)})]$	$\frac{q^s-1}{4}$

表 7 情形(7)：不可约拟循环码的重量分布

重量(i)	频数(A_i)
0	1
$\frac{2}{Nq}(q-1)[(q^s-1)-2(\eta_0^{(4,q^s)}+\eta_2^{(4,q^s)})]$	$\frac{q^s-1}{2}$
$\frac{2}{Nq}(q-1)[(q^s-1)-2(\eta_1^{(4,q^s)}+\eta_3^{(4,q^s)})]$	$\frac{q^s-1}{2}$

情形(6)如果下列条件之一成立，则式(1)定义的不可约拟循环码的重量分布如表6所示。

(a) $\beta_0,\beta_1\in\{C_0^{(4,q^s)}\backslash C_0^{(N,q^s)},C_1^{(4,q^s)}\}$；

(b) $\beta_0,\beta_1\in\{C_0^{(4,q^s)}\backslash C_0^{(N,q^s)},C_3^{(4,q^s)}\}$；

(c) $\beta_0,\beta_1\in\{C_1^{(4,q^s)},C_2^{(4,q^s)}\}$；

(d) $\beta_0,\beta_1\in\{C_2^{(4,q^s)},C_3^{(4,q^s)}$。

情形(7) 如果下列条件之一成立，则式(1)定义的不可约拟循环码的重量分布如表7所示。

(e) $\beta_0,\beta_1\in\{C_0^{(4,q^s)}\backslash C_0^{(N,q^s)},C_2^{(4,q^s)}\}$；

(f) $\beta_0,\beta_1\in\{C_1^{(4,q^s)},C_3^{(4,q^s)}\}$。

由引理3、推论2和定理3，可得到以下推论。

推论 6 设 N 是q^s-1 的正因子，$N_1=\gcd\left(\frac{q^s-1}{q-1},N\right)=4,p\equiv3(\mathrm{mod}4)$。若$\beta_0,\beta_1$满足定理3中的情形(5)且$s\cdot m\equiv0(\mathrm{mod}4)$，则式(1)定义的不可约拟循环码是参数为$\left[\frac{2(q^s-1)}{N},s,\frac{2(q-1)(q^s-q^{\frac{s}{2}})}{Nq}\right]$的2-重量线性码，其重量分布为

$$1+\frac{3(q^s-1)}{4}x^{\frac{2(q-1)(q^s-q^{\frac{s}{2}})}{Nq}}+\frac{q^s-1}{4}x^{\frac{2(q-1)(q^s+3q^{\frac{s}{2}})}{Nq}}。$$

若$s\cdot m\equiv2(\mathrm{mod}4)$，则式(1)定义的不可约拟循环码是参数为$\left[\frac{2(q^s-1)}{N},s,\frac{2(q-1)(q^s-3q^{\frac{s}{2}})}{Nq}\right]$的2-重量线性码，其重量分布为

$$1+\frac{3(q^s-1)}{4}x^{\frac{2(q-1)(q^s+q^{\frac{s}{2}})}{Nq}}+\frac{q^s-1}{4}x^{\frac{2(q-1)(q^s-3q^{\frac{s}{2}})}{Nq}}。$$

推论 7 设 N 是q^s-1 的正因子，$N_1=\gcd\left(\frac{q^s-1}{q-1},N\right)=4$，$p\equiv3(\mathrm{mod}4)$。如果$\beta_0,\beta_1$满足定理3中的情形(6)或情形(7)，则式(1)定义的指标为2的不可约拟循环码是参数为$\left[\frac{2(q^s-1)}{N},s,\frac{2(q-1)(q^s-q^{\frac{s}{2}})}{Nq}\right]$的2-重量线性码，其重量分布为$1+\frac{q^s-1}{2}x^{\frac{2(q-1)(q^s-q^{\frac{s}{2}})}{Nq}}+\frac{q^s-1}{2}x^{\frac{2(q-1)(q^s+q^{\frac{s}{2}})}{Nq}}$。

推论 8 设 N 是q^s-1 的正因子，$N_1=\gcd\left(\frac{q^s-1}{q-1},N\right)=4,p\equiv1(\mathrm{mod}4)$。若$\beta_0,\beta_1$满足定理3中的情形(7)且$s\cdot m\equiv0(\mathrm{mod}4)$，则式(1)定义的指标为2的不可约拟循环码是参数为$\left[\frac{2(q^s-1)}{N},s\right]$的2-重量线性码，其重量分布为

$$1+\frac{q^s-1}{2}x^{\frac{2(q-1)(q^s+(u_1+2v_1)q^{\frac{s}{4}})}{Nq}}+\frac{q^s-1}{2}x^{\frac{2(q-1)(q^s-(u_1+2v_1)q^{\frac{s}{4}})}{Nq}}。$$

4 最优码的构造

定 理 4 设 N 是q^s-1 的正因子，$N_1=3,p\equiv2(\mathrm{mod}3),s\cdot m\equiv2(\mathrm{mod}4)$。若$\beta_0,\beta_1$满足定理2中的情形(4)，则有

(1)如果$p=2,s=2,N=3(2^m-1)$，则式(1)定义的指标为2的不可约拟循环码是一类2-重量MDS码，其参数为$\left[\frac{2}{3}(2^m+1),2,\frac{1}{3}(2^{m+1}-1)\right]$。

(2)如果$s=2,2N=3(p^m-1)$，则式(1)定义的指标为2的不可约拟循环码是一类达到Griesmer界的最优码，其参数为$\left[\frac{4}{3}(p^m+1),2,\frac{2}{3}(2p^m-1)\right]$。

证明 将情形(1)中所给的条件代入推论4，可得式(1)定义的指标为2的不可约拟循环码是一类2-重量线性码且其参数满足$n=k+d-1$。由引理5可得到一类2-重MDS码，其参数为$\left[\frac{2}{3}(2^m+1),2,\frac{1}{3}(2^{m+1}-1)\right]$。

将情形(2)中所给的条件代入推论4，可得到式(1)定义的指标为2的不可约拟循环码是一类2-重量线性码且参数满足$n=\sum_{i=0}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil$。由引理6可

得到一类达到Griesmer界的最优码，其参数为$\left[\frac{4}{3}(p^m+1), 2, \frac{2}{3}(2p^m-1)\right]$。　　证毕

例1　令$(N_1, p, m, s, N)=(3,2,3,2,21)$。由定理4，式(1)定义的指标为2的不可约拟循环码是F_8上参数为[6,2,5]的2-重量MDS码，其重量分布为$1+42x^5+21x^6$。

例2　令$(N_1, p, m, s, N)=(3,11,1,2,15)$。由定理4，式(1)定义的指标为2的不可约拟循环码是F_{11}上参数为[16,2,14]的达到Griesmer界的2-重量最优码，其重量分布为$1+80x^{14}+40x^{16}$。

类似于定理4，可由以下定理得到另一类2-重量MDS码。

定理5　设N是q^s-1的正因子，$N_1=4$，$p\equiv 3(\mathrm{mod}4)$。若β_0, β_1满足定理3中的情形(6)或情形(7)，$s=2, N=4(p^m-1)$，则式(1)定义的指标为2的不可约拟循环码是一类2-重量MDS码，其参数为$\left[\frac{1}{2}(p^m+1), 2, \frac{1}{2}(p^m-1)\right]$。

例3　令$(N_1, p, m, s, N)=(4,3,3,2,104)$。由定理5，式(1)定义的指标为2的不可约拟循环码是F_{27}上参数为[14,2,13]的2-重量MDS码，其重量分布为$1+364x^{13}+364x^{14}$。

5　结论

本文研究了有限域上指标为2的不可约拟循环码的重量分布，构造了几类2-重量线性码和3-重量线性码。特别地，本文得到了3类最优的2-重量线性码。如何利用$Z_pZ_p[v]$-加性码[18,19]的重量分布构造有限域上的最优码是一个有意义的研究问题。

参 考 文 献

[1] DING Cunsheng and YANG Jing. Hamming weights in irreducible cyclic codes[J]. *Discrete Mathematics*, 2013, 313(4): 434–446. doi: 10.1016/j.disc.2012.11.009.

[2] BAE S, LI Chengju, and YUE Qin. On the complete weight enumerators of some reducible cyclic codes[J]. *Discrete Mathematics*, 2015, 338(12): 2275–2287. doi: 10.1016/j.disc.2015.05.016.

[3] 管玥, 施敏加, 张欣, 等. 有限域上两类新的2-重量码的构造[J]. 电子学报, 2019, 47(3): 714–718. doi: 10.3969/j.issn.0372-2112.2019.03.028.

GUAN Yue, SHI Minjia, ZHANG Xin, *et al*. The construction of two new series of two-weight codes over finite fields[J]. *Acta Electronica Sinica*, 2019, 47(3): 714–718. doi: 10.3969/j.issn.0372-2112.2019.03.028.

[4] SHI Minjia, ZHU Shixin, and YANG Shanlin. A class of optimal p-ary codes from one-weight codes over $F_p[u]/\langle u^m\rangle$[J]. *Journal of The Franklin Institute*, 2013, 350(5): 929–937. doi: 10.1016/j.jfranklin.2012.05.014.

[5] SHI Minjia, GUAN Yue, and SLOÉ P. Two new families of two-weight codes[J]. *IEEE Transaction on Information Theory*, 2017, 63(10): 6240–6246. doi: 10.1109/TIT.2017.2742499.

[6] SHI Minjia, WU Rongsheng, LIU Yan, *et al*. Two and three weight codes over F_p+uF_p[J]. *Cryptography and Communications*, 2017, 9(5): 637–646. doi: 10.1007/s12095-016-0206-5.

[7] SHI Minjia and ZHANG Yiping. Quasi-twisted codes with constacyclic constituent codes[J]. *Finite Fields and Their Applications*, 2016, 39: 159–178. doi: 10.1016/j.ffa.2016.01.010.

[8] SHI Minjia, QIAN Liqin, and SLOÉ P. On self-dual negacirculant codes of index two and four[J]. *Designs, Codes and Cryptography*, 2018, 86(11): 2485–2494. doi: 10.1007/s10623-017-0455-0.

[9] 杜小妮, 吕红霞, 王蓉. 一类四重和六重线性码的构造[J]. 电子与信息学报, 2019, 41(12): 2995–2999. doi: 10.11999/JEIT180939.

DU Xiaoni, LÜ Hongxia, and WANG Rong. Construction of a class of linear codes with four-weight and six-weight[J]. *Journal of Electronics & Information Technology*, 2019, 41(12): 2995–2999. doi: 10.11999/JEIT180939.

[10] DING Cunsheng. A class of three-weight and four-weight codes[M]. CHEE Y M, LI Chao, LING San, *et al*. Coding and Cryptology. IWCC 2009. Lecture Notes in Computer Science. Berlin: Springer, 2009: 34–42. doi: 10.1007/978-3-642-01877-0_4.

[11] SCHMIDT B and WHITE C. All two-weight irreducible cyclic codes?[J]. *Finite Fields and Their Applications*, 2002, 8(1): 1–17. doi: 10.1006/ffta.2000.0293.

[12] ZHOU Zhengchun and DING Cunsheng. Seven classes of three-weight cyclic codes[J]. *IEEE Transactions on Communications*, 2013, 61(10): 4120–4126. doi: 10.1109/TCOMM.2013.072213.130107.

[13] BORGES J, FERNÁNDEZ-CÓRDOBA C, and TENVALLS R. Z_2-double cyclic codes[J]. *Designs, Codes and Cryptography*, 2018, 86(3): 463–479. doi: 10.1007/s10623-017-0334-8.

[14] GAO Jian, SHI Minjia, WU Tingting, *et al*. On double cyclic codes over Z_4[J]. *Finite Fields and Their Applications*, 2016, 39: 233–250. doi: 10.1016/j.ffa.2016.02.003.

[15] GAO Jian and HOU Xiaotong. Z_4-Double cyclic codes are asymptotically good[J]. *IEEE Communications Letters*, 2020, 24(8): 1593–1597. doi: 10.1109/LCOMM.2020.2992501.

[16] PATANKER N and SINGH S K. Weight distribution of a subclass of Z_2-double cyclic codes[J]. *Finite Fields and Their Applications*, 2019, 57: 287–308. doi: 10.1016/j.ffa.2019.03.003.

[17] MYERSON G. Period polynomials and Gauss sums for finite fields[J]. *Acta Arithmetica*, 1981, 39(3): 251–264. doi: 10.4064/aa-39-3-251-264.

[18] DIAO Lingyu, GAO Jian, and LU Jiyong. Some results on $Z_pZ_p[v]$-additive cyclic codes[J]. *Advances in Mathematics of Communications*, 2020, 14(4): 557–572. doi: 10.3934/amc.2020029.

[19] HOU Xiaotong and GAO Jian. $Z_pZ_p[v]$-additive cyclic codes are asymptotically good[J]. *Journal of Applied Mathematics and Computing*, 2021, 66(1/2): 871–884. doi: 10.1007/s12190-020-01466-w.

高 健：男，副教授，博士，研究方向为编码理论及其应用.
张耀宗：男，硕士生，研究方向为编码理论及其应用.
孟祥蕊：女，硕士生，研究方向为编码理论及其应用.
马芳卉：女，讲师，博士，研究方向为编码理论及其应用.

责任编辑：马秀强