一类 p 元最优线性码和低相关性线性序列的构造

唐永生[1,2],朱士信[1],曹德才[1],Hai Quang Dinh[3]
(1.合肥工业大学数学学院,安徽合肥 230009;2.合肥师范学院数学系,安徽合肥 230601;3.肯特州立大学数学科学系,美国肯特州 OH 44483)

摘 要: 在信息理论中,最优线性码具有很强的纠错能力、低相关性线性序列在密码系统和 CDMA 通信系统中得到了广泛应用. 因此构造最优线性码和构造低相关性线性序列具有重要的研究价值.记 $R = Fp + uFp$,这里的 p 为奇素数.本文首先通过迹映射构造出环 R 上的一类新的线性码,然后将这类新的线性码的删余码通过 Gray 映射得到了域 Fp 上一类最优码.同时,通过迹映射构造出环 R 上的一类线性循环码,将这类线性循环码视为线性周期序列并通过广义 Nechaev-Gray 映射得到了域 Fp 上一类低相关线性周期序列.

关键词: 迹映射; 最优线性码; 低相关性; 线性序列
中图分类号: TN911.22 **文献标识码:** A **文章编号:** 0372-2112 (2014)03-0572-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.03.022

Construction of a Family of p-ary Optimal Linear Codes and Low Correlation Linear Sequences

TANG Yong-sheng[1,2], ZHU Shi-xin[1], CAO De-cai[1], Hai Quang Dinh[3]
(1. *School of Mathematics, Hefei University of Technology, Hefei, Anhui* 230009, *China*; 2. *Department of Mathematics, Hefei Normal University, Hefei, Anhui* 230601, *China*; 3. *Department of Mathematical Sciences, Kent State University, OH*44483, *USA*)

Abstract: In information theory, optimal linear codes have good capability in error-correcting in coding theory and linear sequences with low correlation have been widely used in cryptography and CDMA systems. Therefore, it has great value to study the construction of optimal linear codes and low correlation linear sequences. Let $R = Fp + uFp$, where p is an odd prime. A class of new linear codes over R is constructed by means of the trace map. Then a kind of optimal codes over Fp is obtained via the Gray map from the punctured new linear codes. Furthermore, a class of new linear cyclic codes over R is also constructed by means of the trace map. A kind of low correlation linear sequences over Fp is observed via the generalized Nechaev-Gray map from the class of new linear cyclic codes, which are regarded as a class of linear periodic sequences.

Key words: trace map; optimal linear codes; low correlation; linear sequences

1 引言

20 世纪 90 年代,编码理论的一个突破性进展是 Nechaev[1]发现二元 Kerdock 码可视环 Z_4 上的循环码,这开创了纠错码的一个新的研究方向— 环 Z_4 上的纠错码的理论研究.随后 Hammons 等五人小组[2]在 1994 年证明了一些高效的二元非线性码,如 Preparata 码、Kerdock 码等可视为环 Z_4 上循环码在 Gray 映射下的像. 1997 年,万哲先[3]出版了《Quaternary Codes》.从此以后,人们对环 Z_4 上的纠错码理论进行了深入研究的同时,并开始研究一般的有限环上的纠错码理论.

近年,编码研究者对剩余类多项式环 $F_{p^s}[u]/(u^a) = F_{p^s} + uF_{p^s} + \cdots + u^{a-1}F_{p^s}$ 产生极大的兴趣(p 为素数并且 $u^a = 0$). Bachoc[4]利用了环 $F_p + uF_p$ 上的线性码进行格的构造; Bonnecaze 和 Udaya[5]讨论了环 $F_2 + uF_2$ 上循环自对偶码并利用线性码的 Gray 映射构造了一批二元最优码. Zhu 和 Tang[6]研究了环 $F_2 + uF_2$ 上线性码关于 Lee 重量的一类 MacWilliams 恒等式.施敏加等人[7]研究了环 $F_2 + uF_2$ 上长度为 2^s 的循环码距离. Dinh 和 Nguyen[8]深入研究了环 $F_{2^m} + uF_{2^m} + \cdots + u^{a-1}F_{2^m}$ 上的常循环码. Zhu 和 Wang[9]讨论了环 $F_p + vF_p(v^2 = v)$ 上一类常循环码并利用 Gray 映射获得了域 F_p 上一批最优码. Shi 等人[10]研究了环 $F_p + vF_p(v^2 = 1)$ 上循环码并利用 Gray 映射获得了域 F_p 上一批最优准循环码. Rao 和 Pinnawala[11]利用迹映射构造了环 Z_{p^s} 上一类新的线性码.

自相关性是衡量序列伪随机性质的一个重要的指标.流密码系统中的密钥流序列或数字签名算法中的伪

收稿日期:2013-04-01;修回日期:2013-06-10;责任编辑:覃怀银
基金项目:安徽省自然科学基金(No.1208085MA14, No.1408085QF116);安徽省高校省级科学研究项目(No.KJ2013B217, No.KJ2013B220, No.KJ2013B221);合肥师范学院一般研究项目(No.2012kj10);国家自然科学基金(No.61370089)

随机数序列应具有低相关特性,这一性质使其能有效地抵抗互相关攻击;另一方面,在 CDMA(Code-Division Multiple-Access)系统中具有低相关性的伪随机序列能够成功地降低来自同一信道中其他使用者的干扰[12]. Ding 等人[13]利用有限域上的循环码构造出一批最优跳频序列. Zhou 等人[14]利用不同的平衡函数构造出一批最优跳频序列. Barg, Ling, Solé 等人发现利用有限环上的线性码可以构造出有限域上的低相关序列. Barg[15]构造出二类二元低相关线性序列. Ling 和 Solé[16]构造出 p 元非线性序列. Lahtonen 等人[17]利用环 Z_8 上 Kerdock 码构造出一类二元非线性低相关序列. 本文利用文献[11]的方法构造了环 F_p+uF_p 上一类新的线性码. 特别地,将这类新的线性码的删余码通过 Gray 映射获得了域 F_p 上一类最优码. 同时,利用文献[15,16]的方法构造出环 F_p+uF_p 上的一类线性循环码,将这类线性循环码视为线性周期序列并通过广义的 Nechaev-Gray 映射得到了域 F_p 上一类低相关线性周期序列.

2　预备知识

设剩余类多项式环 $R=F_p+uF_p$,这里 $u^2=0$,则环 R 是有唯一极大理想(u)的局部环. 环 R 上任意元素 r 都可唯一表示为:$r=r_0+ur_1$,这里 $r_0,r_1\in F_p$;称 $\bar{r}=r_0$ 为 r 的模 u 约化;类似地,称 $\bar{a}(x)=\sum_{i=0}^{k}\bar{a}_ix^i\in F_p[x]$ 为 $a(x)=\sum_{i=0}^{k}a_ix^i\in R[x]$ 的模 u 约化. 若 $\bar{a}(x)$ 为 $F_p[x]$ 中不可约多项式,称多项式 $a(x)$ 为 $R[x]$ 中基本不可约多项式. 设 $h(x)$ 是 $R[x]$ 中 l 次首一基本不可约多项式,称 $\mathrm{GR}(R,l)=R[x]/(h(x))$ 为环 R 的 Galois 环. 取 $\xi=x+(h(x))$,则 ξ 为 $h(x)$ 的一个根,并且 $\mathrm{GR}(R,l)$ 中元素都可唯一表示为:$a_0+a_1\xi+\cdots+a_{l-1}\xi^{l-1}$(其中 $a_i\in R,i=0,1,\cdots,l-1$)的形式,即 $\mathrm{GR}(R,l)=R[\xi]$. 理想(u)是 $R[\xi]$ 的唯一极大理想,它是由 $\mathrm{GR}(R,l)$ 中所有零因子和零元素组成的. 记 $\bar{\xi}=x+(\bar{h}(x))$,那么 $\bar{h}(\xi)=0$ 并且 $F_p[\xi]=F_{p^l}$. 类似于 Galois 域(见文献[12]),可得环 R 的 Galois 扩张 $\mathrm{GR}(R,l)$ 对于给定的 l 是唯一的,并且对于 Galois 扩张 $\mathrm{GR}(R,l)$,有 $\mathrm{GR}(R,l)/(u)\cong F_{p^l}$ 且 $|\mathrm{GR}(R,l)|=p^{2l}$,则对 $\mathrm{GR}(R,l)$ 上任意元素 $c=c_0+uc_1$,其中 $c_0,c_1\in F_{p^l}$. 在 Galois 扩张 $\mathrm{GR}(R,l)$ 中,存在 p^l-1 阶元素 ξ,ξ 为 R 上 l 次基本不可约多项式 $h(x)$ 的根,使得 $\mathrm{GR}(R,l)=R[\xi]$,并且 $h(x)$ 是一个满足 $\deg(h(x))\leqslant l$,且 $h(\xi)=0$ 的唯一的首一多项式. 设 $T=\{0,1,\xi,\cdots,\xi^{p^l-2}\}$,那么对任意 $c\in\mathrm{GR}(R,l)$ 都能被唯一表示为 $c=c_0+uc_1,c_0,c_1\in T$. 设 $c=c_0+uc_1$,$c_0,c_1\in T$,如果 $c_0\neq0$,则称 c 是 $\mathrm{GR}(R,l)$ 中可逆元;否则称 c 是 $\mathrm{GR}(R,l)$ 中不可逆元.

设 R^n 是由 R 上的 n 维向量所组成的集合,即 $R^n=\{(x_0,x_1,\cdots,x_{n-1})\mid x_i\in R,i=0,1,\cdots,n-1\}$. R^n 中任一非空子集 C 称为 R-码,其中 n 称为码的长度. R^n 中 n 维向量称为字,码 C 中的 n 维向量称为码元. R^n 中任一子群称为 R-线性码. 对于任意的 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})$,$\boldsymbol{y}=(y_0,y_1,\cdots,y_{n-1})\in R^n$,定义为:

$$\boldsymbol{x}\cdot\boldsymbol{y}=x_0y_0+x_1y_1+\cdots+x_{n-1}y_{n-1}\tag{1}$$

设 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in R^n$,$\boldsymbol{x}$ 码字的 Hamming 重量可表示为:$W_H(x)=|\{i\mid x_i\neq0\}|$. 对任意的 $\boldsymbol{x},\boldsymbol{y}\in R^n$,$\boldsymbol{x}$ 与 $\boldsymbol{y}$ 之间的 Hamming 距离可表示为:$d_H(\boldsymbol{x},\boldsymbol{y})=W_H(\boldsymbol{x}-\boldsymbol{y})$. 文献[18]已经将 R 内每一个元素的齐次重量定义为:

$$W_{\mathrm{hom}}(r)=\begin{cases}0, & r=0\\ p-1, & r\in R\setminus uR\\ p, & r\in uR\setminus\{0\}\end{cases}\tag{2}$$

任一向量 $\boldsymbol{x}\in R^n$ 的齐次重量定义为每一个分量的齐次重量之和. 对任意的 $\boldsymbol{x},\boldsymbol{y}\in R^n$,$\boldsymbol{x}$ 与 $\boldsymbol{y}$ 之间的齐次距离可表示为:$d_{\mathrm{hom}}(\boldsymbol{x},\boldsymbol{y})=W_{\mathrm{hom}}(\boldsymbol{x}-\boldsymbol{y})$.

如果两个码可以通过置换坐标相互得到,那么称这两个码置换等价. R 上任意一非零的线性码 C 都可置换等价于一个如下形式矩阵

$$\boldsymbol{G}=\begin{pmatrix}\boldsymbol{I}_{r_1} & \boldsymbol{A} & \boldsymbol{D}_1+u\boldsymbol{D}_2\\ \boldsymbol{0} & u\boldsymbol{I}_{r_2} & u\boldsymbol{T}\end{pmatrix}\tag{3}$$

所生成的线性码,其中 $\boldsymbol{A},\boldsymbol{T},\boldsymbol{D}_1,\boldsymbol{D}_2$ 均为域 F_p 上的矩阵,也称矩阵 $\boldsymbol{G}$ 为码 C 的生成矩阵,此时 C 是一个型为 $p^{2r_1}p^{r_2}$ 的 Abelian 群,共包含 $p^{2r_1+r_2}$ 个码字,并且 C 是 R 的一个自由模当且仅当 $r_2=0$. 对环 R 上任一线性码记为 $[n,k_1,d_{\mathrm{hom}},d_H]$,其中 n 表示码长,k_1 表示码的 p 维,d_{hom},d_H 分别表示码的最小齐次距离和最小 Hamming 距离.

3　主要结果

首先,给出环 $\mathrm{GR}(R,l)$ 上的 Frobenius 映射和迹映射的定义并给出迹映射的相关性质,然后利用迹映射及其相关性质构造出环 R 上一类新的线性码并研究该码的删余码的 Gray 象.

定义 1[19]　称映射 $f:\mathrm{GR}(R,l)\to\mathrm{GR}(R,l)$;$c=c_0+uc_1\mapsto c^f=c_0^p+uc_1^p$ 为环 $\mathrm{GR}(R,l)$ 上的 Frobenius 映射.

定义 2[19]　称 $\mathrm{Tr}(c)=c+c^f+\cdots+c^{f^{l-1}}$($\forall c\in\mathrm{GR}(R,l)$)为环 $\mathrm{GR}(R,l)$ 到环 R 的迹映射.

关于迹映射直接验证可得命题 1:

命题 1　(1)$\mathrm{Tr}(c+c')=\mathrm{Tr}(c)+\mathrm{Tr}(c')$,对任意的 $c,c'\in\mathrm{GR}(R,l)$;

(2)$\mathrm{Tr}(\alpha c)=\alpha\mathrm{Tr}(c)$,$\forall c\in\mathrm{GR}(R,l)$,$\forall\alpha\in R$;并

且 Tr 为环 GR(R,l)到环 R 的一个满射.

命题 2 设 Tr 为环 GR(R,l)到环 R 迹映射,υ 是环 GR(R,l)中任一元素.若 υ 取遍环 GR(R,l)中所有元素,那么 Tr($\upsilon\xi^i$),$i=0,1,\cdots,l-1$,取遍 R 内所有元素并且次数相等,为 $p^{2(l-1)}$次;若 υ 取遍环 GR(R,l)中所有的零因子及零元素,那么 Tr($\upsilon\xi^i$),$i=0,1,\cdots,l-1$,取遍 R 内所有零因子和零元素并且次数相等,为 p^{2l-1}次.

证明 对任意的 $\upsilon\in$GR(R,l),考虑环 R 上 l 元组 $V_\upsilon=(\mathrm{Tr}(\upsilon),\mathrm{Tr}(\upsilon\xi),\cdots,\mathrm{Tr}(\upsilon\xi^{l-1}))$.设 $V=\{V_\upsilon\mid\upsilon\in\mathrm{GR}(R,l)\}$且 $\varphi:\mathrm{GR}(R,l)\to V$.因为 GR($R,l$)=$<1,\xi,\xi^2,\cdots,\xi^{l-1}>$是一个 R 模并且 Tr 是一个满射,所以 φ 是一个环 GR(R,l)中的元素与环 R 上 V 中的 l 元组之间的一对一映射.因此,υ 取遍环 GR(R,l)中的所有元素,那么 $V_\upsilon=(\mathrm{Tr}(\upsilon),\mathrm{Tr}(\upsilon\xi),\cdots,\mathrm{Tr}(\upsilon\xi^{l-1}))$中的每一个分量 Tr($\upsilon\xi^i$)取遍 R 内所有元素并且次数相等,为$\frac{p^{2l}}{p^2}=p^{2(l-1)}$次.更进一步,如果 $\upsilon=ua_1\in\mathrm{GR}(R,l)$,$a_1\in T$,即,$\upsilon$ 取遍环 GR(R,l)中的所有的零因子和零元素,那么 $V_\upsilon=(\mathrm{Tr}(\upsilon),\mathrm{Tr}(\upsilon\xi),\cdots,\mathrm{Tr}(\upsilon\xi^{l-1}))$中的每一个分量 Tr($\upsilon\xi^i$)取遍 R 内所有零因子和零元素并且次数相等,为$\frac{p^{2l}}{p}=p^{2l-1}$次.

定理 1 设 Tr 为环 GR(R,l)到环 R 的迹映射,那么由矩阵 $\boldsymbol{A}=[\mathrm{Tr}(c_ic_j)]_{\forall c_i,c_j\in\mathrm{GR}(R,l)}$生成的码是环 R 上$[n,k,d_{\mathrm{hom}},d_H]=[p^{2l},l,p^{2l}(p-1),p^{2l-1}(p-1)]$的线性码.

证明 由前面的介绍,设 $h(x)$是 $R[x]$中 l 次首一基本不可约多项式,令 $\xi=x+(h(x))$,则 ξ 为 $h(x)$的一个根,并且 GR(R,l)中任意元素 a 都可唯一表示为:$a=a_0+a_1\xi+\cdots+a_{l-1}\xi^{l-1}$(其中:$a_i\in R$,$i=0,1,\cdots,l-1$)的形式,即 GR($R,l$)=$R[\xi]$.

下面考虑矩阵

$$\boldsymbol{G}=\begin{pmatrix}\mathrm{Tr}(c_1)&\mathrm{Tr}(c_2)&\cdots&\mathrm{Tr}(c_{p^{2l}})\\\mathrm{Tr}(\xi c_1)&\mathrm{Tr}(\xi c_2)&\cdots&\mathrm{Tr}(\xi c_{p^{2l}})\\\vdots&\vdots&\vdots&\vdots\\\mathrm{Tr}(\xi^{l-1}c_1)&\mathrm{Tr}(\xi^{l-1}c_2)&\cdots&\mathrm{Tr}(\xi^{l-1}c_{p^{2l}})\end{pmatrix}\tag{4}$$

其中 $c_i\in$GR(R,l).

由于 $1,\xi,\cdots,\xi^{l-1}$都是 GR(R,l)中可逆元,那么根据命题 2,$\boldsymbol{G}$ 的每一行取 R 内所有元素并且次数相等,为 $p^{2(l-1)}$次;而且 $\boldsymbol{G}$ 的每一行是线性无关的.因此由 $\boldsymbol{G}$ 生成的码是线性的.那么取遍 $\boldsymbol{G}$ 所有行的线性组合即可得到矩阵:

$$\boldsymbol{A}=[\mathrm{Tr}(c_ic_j)]_{\forall c_i,c_j\in\mathrm{GR}(R,l)}\tag{5}$$

因此由矩阵 $\boldsymbol{A}$ 生成的码也是线性的并且由矩阵 $\boldsymbol{A}$ 生成的线性码就是由矩阵 $\boldsymbol{G}$ 生成的.

设 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{p^{2l}-1})$(其中 $x_i\in R$)是由 $\boldsymbol{G}$ 生成的码字.由上面的陈述,x 的分量要么取 R 内所有元素并且次数相等,为 $p^{2(l-1)}$次;要么取 R 内所有零因子和零元素并且次数相等,为 p^{2l-1}次.

因此

$$\begin{aligned}W_{\mathrm{hom}}(\boldsymbol{x})&=p^{2(l-1)}[(p^2-p)(p-1)+(p-1)p]\\&=p^{2l}(p-1)\end{aligned}\tag{6}$$

或者

$$W_{\mathrm{hom}}(\boldsymbol{x})=p^{2l-1}[(p-1)p]=p^{2l}(p-1)\tag{7}$$

那么

$$\min W_{\mathrm{hom}}(\boldsymbol{x})=p^{2l}(p-1)\tag{8}$$

同理

$$W_H(\boldsymbol{x})=p^{2(l-1)}(p^2-1)\tag{9}$$

或者

$$W_H(\boldsymbol{x})=p^{2l-1}(p-1)\tag{10}$$

那么

$$\min W_H(\boldsymbol{x})=p^{2l-1}(p-1)\tag{11}$$

因此由矩阵 $\boldsymbol{A}=[\mathrm{Tr}(c_ic_j)]_{\forall c_i,c_j\in\mathrm{GR}(R,l)}$生成的码是环 R 上线性码$[n,k,d_{\mathrm{hom}},d_H]=[p^{2l},l,p^{2l}(p-1),p^{2l-1}(p-1)]$.

在文献[18]中已经定义了 R 到 F_p^{pn} 的线性 Gray 映射,下面我们引用它的定义.

定义 3[18] 定义 R 到 F_p^p 上的线性 Gray 映射 ϕ 为:

$$\phi:R\to F_p^p\tag{12}$$

$$x+yu\mapsto(y,x\oplus y,\cdots,(p-1)x\oplus y),\tag{13}$$

其中$\oplus$表示 F_p 中的加法.

这个映射很自然地推广 $R^n\to F_p^{pn}$,并且它是一个由(R^n,齐次距离)到(F_p^{pn},Hamming 距离)的保距映射,即 $\forall\boldsymbol{c}_1,\boldsymbol{c}_2\in R^n$,$d_{\mathrm{hom}}(\boldsymbol{c}_1,\boldsymbol{c}_2)=d_H(\phi(\boldsymbol{c}_1),\phi(\boldsymbol{c}_2))$.对 $\boldsymbol{c}=(c^{(p^0)}\mid\cdots\mid c^{(p^{s-1})})\in F_p^{pn}$,一个广义 Nechaev 置换 σ 定义为:

$$\sigma(\boldsymbol{c})=(\sigma(c^{(p^0)}),\cdots,\sigma(c^{(p^{s-1})}))\tag{14}$$

这里 $\sigma(\boldsymbol{a})=(a_{\tau(0)},\cdots,a_{\tau(pn-1)})$并且 $\tau(\gamma n+j)=(\gamma+jn')_pn+j$,$0\leqslant\gamma\leqslant p-1$,$0\leqslant j\leqslant n-1$,$(\gamma+jn')_p$ 表示($\gamma+jn'$)模 p 的最小的剩余类.

码的构造一直是编码研究者研究的热点.一方面,他们希望能够构造出有限域上维数固定,最小距离达到最大的线性码.另一方面,他们希望能够构造出有限域上码长较小,最小距离较大的线性码.从而,构造出的线性码纠错能力较强.设 C 是有限域 F_p 上线性码,如果在有限域 F_p 上具有相同长度,找不到比码 C 的最小距离更大的线性码,那么称线性码 C 为有限域 F_p 上

的最优码.下面我们通过已经构造的环 R 上$[n,k,d_{\hom},d_H]=[p^{2l},l,p^{2l}(p-1),p^{2l-1}(p-1)]$的线性码得到有限域 F_p 上一类最优码.

现将矩阵 $\boldsymbol{A}$ 中全是 0 的列删除,记删除后的矩阵为 $\boldsymbol{A}^*$,那么 $C'=\phi(\boldsymbol{A}^*)$是域 F_p 上线性码且码长为 $p(p^{2l}-1)$,基数为 p^{2l}.因此它是一个$[n,k_2,d_H]=[p(p^{2l}-1),2l,p^{2l}(p-1)]$线性码,这里的 k_2 表示由矩阵 $\boldsymbol{A}^*$ 生成的码在域 F_p 上的维数.通过码表(文献[20])验证,发现 $C'=\phi(\boldsymbol{A}^*)$是域 F_p 上一类最优码.

下面我们给出一个通过构造环 F_3+uF_3 上一类新码得到域 F_3 上一类最优码的例子.

例 1　考虑环 $R=F_3+uF_3$ 上基本不可约多项式 $h(x)=x^2+x+2$,$\mathrm{GR}(R,2)=R[x]/(h(x))$.设 ξ 是 $h(x)$的根,那么 ξ 是 F_3 上的 8 阶本原单位根,$\xi^2=2\xi+1$,此时 $T=\{0,1,\xi,\xi^2,\cdots,\xi^7\}$.由命题 2,$\mathrm{GR}(R,2)=\{c=a+ub\mid a,b\in T\}$.根据定理 1,由矩阵

$$\boldsymbol{G}=\begin{pmatrix}\mathrm{Tr}(c_1) & \mathrm{Tr}(c_2) & \cdots & \mathrm{Tr}(c_{81})\\ \mathrm{Tr}(\xi c_1) & \mathrm{Tr}(\xi c_2) & \cdots & \mathrm{Tr}(\xi c_{81})\end{pmatrix}$$

生成的码是环 R 上线性码$[n,k_1,d_{\hom},d_H]=[3^4,2,3^4\cdot 2,3^3\cdot 2]$.进一步,$\boldsymbol{A}^*$ 线性 Gray 像 $C'=\phi(\boldsymbol{A}^*)$是域 F_3 上线性码$[n,k_2,d_H]=[240,4,162]$.通过码表(文献[20])验证,C'是域 F_3 上的最优码.

下面我们将利用环 R 上一类线性循环码构造出域 F_p 上一类低相关性线性周期序列.文献[18]已经证明了线性码 C 是环 R 上长度为 n 的循环码当且仅当 $\sigma\phi(C)$是域 F_p 上长度为 pn 的线性循环码.首先我们给出一些定义和标记.

设 $a\in F_p$,定义域 F_p 上标准的加法特征为:

$$\chi_1(a)=(\omega_1)^a \tag{15}$$

其中 $\omega_1=\mathrm{e}^{\frac{2\pi i}{p}}$并且 $i^2=-1$.

类似地,设 $b\in R$,定义环 R 上标准的加法特征为:

$$\chi_2(b)=(\omega_2)^b \tag{16}$$

其中 $\omega_2=\mathrm{e}^{\frac{2\pi i}{p^2}}$并且 $i^2=-1$.

定义环 R 上一类循环码组成的集合 $k_{p,l}$和域 F_p 上一类两两互不相同的线性循环序列组成的集合 $S_{p,l}$分别为:

$$k_{p,l}=\{(\mathrm{Tr}(B),\mathrm{Tr}(B\xi),\cdots,\mathrm{Tr}(B\xi^{N-1}))\mid B\in\mathrm{GR}(R,l)\text{并且 }\bar{B}\neq 0\} \tag{17}$$

$$S_{p,l}=\{(\chi_1(x_0),\cdots,\chi_1(x_{pN-1}))\mid(x_0,\cdots,x_{pN-1})\in\sigma\phi(k_{p,l}\setminus uk_{p,l})\}^{\infty} \tag{18}$$

其中 $N=p^l-1$.

对于任意的 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{N-1})\in R^N$,特征和定义为

$$\lambda_2(\boldsymbol{x})=\sum_{j=0}^{N-1}\chi_2(x_j) \tag{19}$$

如果记 $N_j(x)$为 $j\in R$ 在 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{N-1})$中出现的次数,那么等式(19)等价于

$$\lambda_2(\boldsymbol{x})=\sum_{j=0}^{p^2-1}N(x_j)\chi_2(j) \tag{20}$$

类似地,对于任意的 $\boldsymbol{y}=(y_0,y_1,\cdots,y_{pN-1})\in F_p^{pN}$,特征和定义为

$$\lambda_1(\boldsymbol{y})=\sum_{j=0}^{pN-1}\chi_1(y_j) \tag{21}$$

如果记 $N_j(y)$为 $j\in F_p$ 在 $y=(y_0,y_1,\cdots,y_{pN-1})$中出现的次数,那么等式(21)等价于

$$\lambda_1(\boldsymbol{y})=\sum_{j=0}^{p-1}N(y_j)\chi_1(j) \tag{22}$$

集合 $S_{p,l}$里的线性循环序列的最大非平凡相关性参数定义为:$\lambda_{\max}=\max\{|\lambda_1(y)|:y=\sigma\phi(x),x\in k_{p,l}\setminus uk_{p,l}\}$.记集合 $S_{p,l}$里的线性循环序列为$[pN,M,\lambda_{\max}\leqslant\lambda]$,这里 pN 表示线性循环序列的周期,M 表示集合 $S_{p,l}$的容量,λ 表示 $\lambda_{\max}$的上界.下面我们将分别计算出集合 $S_{p,l}$的容量和 λ.

定理 2　集合 $S_{p,l}$的容量为

$$|S_{p,l}|=p^{l-1} \tag{23}$$

证明　如果视集合 $\sigma\phi(uk_{p,l})$里的元素为线性周期序列,则该序列是由 p 重周期为 p^l-1 的 p 元 m 序列构成.另一方面,文献[18]已经证明了线性码 C 是环 R 上长度为 N 的循环码当且仅当 $\sigma\phi(C)$是域 F_p 上长度为 pN 的线性循环码.因此视集合 $\sigma\phi(k_{p,l}\setminus uk_{p,l})$里的元素为线性周期序列,则该序列的周期是 $p(p^l-1)$.因此 $\sigma\varphi(k_{p,l}\setminus uk_{p,l})$里含有不同的循环序列的容量是 $\dfrac{p^{2l}-p^l}{p(p^l-1)}=p^{l-1}$.

引理 1　对任意的 $x\in R$,只有下列三种情形发生:

(1)如果 $x=0$,那么 $N_j(\sigma\phi(x))=\delta_{j,0}p$,

(2)如果 $x\in(u)\setminus\{0\}$,那么 $N_j(\sigma\phi(x))=\delta_{j,x_1}p$,

(3)如果 $x\in R\setminus(u)$,那么对任意的 $j\in F_p$ 有 $N_j(\sigma\cdot\phi(x))=1$.

证明　设 $x\in R$,则 $x=x_0+ux_1$,这里 $x_0,x_1\in F_p$.因此

当 $x=0$ 时,$\sigma\phi(x)=\sigma\phi(x_0+ux_1)=0$.

当 $x\in(u)\setminus\{0\}$时,则 $x_0=0,x_1\neq 0$.

当 $x\in R\setminus(u)$时,则 $x_0\neq 0$.设 $y=\sigma\phi(x)\in F_p$,根据有限域上的线性性质,y 可以取到 F_p 中所有元素并且次数相等.

命题 3　对任意 $\boldsymbol{x}\in R^n$,有

$$\mathrm{Tr}(\lambda_2(x))=\lambda_1(\sigma\phi(\boldsymbol{x})) \tag{24}$$

证明　为了方便,我们只证 $n=1$,对于 n 为其他正

整数可以自然推广.设 $x\in R$,则 $x=x_0+ux_1$,这里 x_0,$x_1\in F_p$.下面根据引理 1 的三种情况分别讨论:

(1)如果 $x=0$,那么 $\lambda_2(x)=N_0(x)=1$.因此 $\mathrm{Tr}(\lambda_2(x))=p=\lambda_1(\sigma\phi(x))$.

(2)如果 $x\in(u)\setminus\{0\}$,则 $x_0=0$,$x_1\neq 0$.记 $x=pj(1\leqslant j\leqslant p-1)$,因为 $\omega_2^p=\omega_1$,所以 $\lambda_2(x)=\omega_2^{pj}=\omega_1^j$.从而 $\mathrm{Tr}(\lambda_2(x))=\lambda_1(\sigma\phi(x))$.

(3)如果 $x\in R\setminus(u)$,那么 $0\leqslant j\leqslant p-1$,$N_{pj}(x)=0$.因此 $\mathrm{Tr}(\lambda_2(x))=0$.由于所有的 $N_i(\sigma\phi(x))$都是相同的.因此 $\lambda_1(\sigma\phi(x))=0$.

引理 2[21] 设 $B\in\mathrm{GR}(R,l)$并且 $\bar{B}\neq 0$,那么

$$\left|\sum_{a\in R\setminus\{0\}}\sum_{x\in T}\mathrm{e}^{2\pi i\frac{\mathrm{Tr}(aBx)}{p^2}}\right|\leqslant p^{\lceil l/p\rceil}\left\lfloor\frac{p^{\lfloor l/p\rfloor}\dfrac{p^2-p}{2}(p-1)\lfloor 2p^{(l/2)-\lfloor l/p\rfloor}\rfloor}{p^{\lceil l/p\rceil}}\right\rfloor \tag{25}$$

其中$\lceil a\rceil$和$\lfloor b\rfloor$分别表示不小于 a 的最小的整数和不大于 b 的最大整数.

定理 3

$$\lambda_{\max}\leqslant\frac{1}{p-1}p^{\lceil l/p\rceil}\left\lfloor\frac{p^{\lfloor l/p\rfloor}\dfrac{p^2-p}{2}(p-1)\lfloor 2p^{(l/2)-\lfloor l/p\rfloor}\rfloor}{p^{\lceil l/p\rceil}}\right\rfloor+p \tag{26}$$

证明 设 $\boldsymbol{x}\in S_{p,l}\setminus uS_{p,l}$,$\boldsymbol{y}=\sigma\phi(\boldsymbol{x})$.

根据命题 3,可得

$$\lambda_1(\boldsymbol{y})=\sum_{c_1=0}^{p-1}\sum_{x\in T\setminus\{0\}}\mathrm{e}^{2\pi i\frac{\mathrm{Tr}((1+c_1u)Bx)}{p^2}} \tag{27}$$

对 $0\leqslant k\leqslant p-1$,设

$$\phi_k(B)=\sum_{c_1=0}^{p-1}\sum_{x\in T}\mathrm{e}^{2\pi i\frac{\mathrm{Tr}((k+c_1u)Bx)}{p^2}} \tag{28}$$

结合等式(27)和等式(28),有

$$\lambda_1(y)=\phi_1(B)-p \tag{29}$$

根据命题 3,可得

$$\sum_{a\in R}\sum_{x\in T}\mathrm{e}^{2\pi i\frac{\mathrm{Tr}(aBx)}{p^2}}=\sum_{k=1}^{p-1}\phi_k(B)=p^l+(p-1)\phi_1(B).$$

另一方面

$$\sum_{a\in R}\sum_{x\in T}\mathrm{e}^{2\pi i\frac{\mathrm{Tr}(aBx)}{p^2}}=p^l+\sum_{a\in R\setminus\{0\}}\sum_{x\in T}\mathrm{e}^{2\pi i\frac{\mathrm{Tr}(aBx)}{p^2}} \tag{30}$$

因此

$$(p-1)\phi_1(B)=\sum_{a\in R\setminus\{0\}}\sum_{x\in T}\mathrm{e}^{2\pi i\frac{\mathrm{Tr}(aBx)}{p^2}} \tag{31}$$

根据引理 2,可得

$$(p-1)|\phi_1(B)|\leqslant p^{\lceil l/p\rceil}\left\lfloor\frac{p^{\lfloor l/p\rfloor}\dfrac{p^2-p}{2}(p-1)\lfloor 2p^{(l/2)-\lfloor l/p\rfloor}\rfloor}{p^{\lceil l/p\rceil}}\right\rfloor \tag{32}$$

因此

$$\lambda_{\max}\leqslant\frac{1}{p-1}p^{\lfloor l/p\rfloor}\left\lfloor\frac{p^{\lfloor l/p\rfloor}\dfrac{p^2-p}{2}(p-1)\lfloor 2p^{(l/2)-\lfloor l/p\rfloor}\rfloor}{p^{\lceil l/p\rceil}}\right\rfloor+p.$$

表 1 周期为 $p(p^l-1)$,容量为 p^{l-1}的线性循环序列的最大非平凡相关性参数比较(p 为素数)

序列	p	T	M	$\lambda_{\max}$
Barg[15]	2	$2(2^l-1)$	2^{l-1}	$2(2^{l/2-1}+1)$
Ling,Solé[16]	奇素数	$p(p^l-1)$	p^{l-1}	$(p-1)p^{l/2+1}$
本序列	奇素数	$p(p^l-1)$	p^{l-1}	$\frac{1}{p-1}p^{\lceil l/p\rceil}\left\lfloor\frac{p^{\lfloor l/p\rfloor}\frac{p^2-p}{2}(p-1)\lfloor 2p^{(l/2)-\lfloor l/p\rfloor}\rfloor}{p^{\lceil l/p\rceil}}\right\rfloor+p$

4 总结

在信息理论中,找到一种能够构造最优线性码的方法和找到一种能够构造低相关性的线性序列的方法都是具有重要的价值.记 $R=F_p+uF_p$,这里 p 为奇素数.本文首先通过迹映射构造出环 R 上的一类新的线性码,然后将这类新的线性码的删余码通过 Gray 映射得到了域 F_p 上一类最优码.同时,通过迹映射构造出环 R 上的一类线性循环码,将这类线性循环码视为线性周期序列并通过广义 Nechaev-Gray 映射得到了域 F_p 上一类低相关线性周期序列.

参考文献

[1] Nechaev A. Kerdock code in a cyclic form[J]. Discrete Mathematics Applications, 1991, 1(4): 365 – 384.

[2] Hammons A R, Kumar Jr P V, Calderbank A R, et al. The Z_4-linearity of Kerdock, Preparata, Goethals and related codes[J]. IEEE Transactions on Information Theory, 1994, 40(2): 301 –

319.
[3] Wan Z X. Quaternary Codes [M]. Singapore: World Scientific, 1997.93 – 112.
[4] Bachoc C. Application of coding theory to the construction of modular lattices [J]. Journal of Combinational Theory, Series A, 1997, 78(1): 92 – 119.
[5] Bonnecaze A, Udaya P. Cyclic codes and self-dual codes over $F_2 + uF_2$ [J]. IEEE Transactions on Information Theory, 1999, 45(4): 1250 – 1255.
[6] Zhu S X, Tang Y S. A MacWilliams type identity on Lee weight for linear codes over $F_2 + uF_2$ [J]. Journal of Systems Science and Complexity, 2012, 25(1): 186 – 194.
[7] 施敏加,杨善林,朱士信.环 $F_2 + uF_2$ 上长度为 2^s 的循环码的距离[J].电子学报,2011,39(1):29 – 34.
Shi Min-jia, Yang Shan-lin, Zhu Shi-xin. On minimum distances of cyclic codes of length 2^s over $F_2 + uF_2$ [J]. Acta Electronica Sinica, 2011, 39(1): 29 – 34. (in Chinese)
[8] Dinh H Q, Nguyen H D T. On some classes of constacyclic codes over polynomial residue rings [J]. Advances in Mathematics of Communications, 2012, 6(2): 175 – 191.
[9] Zhu S X, Wang L Q. A class of constacyclic codes over $F_p + vF_p$ and its Gray image [J]. Discrete Mathematics, 2011, 311(23-24): 2677 – 2682.
[10] Shi M J, Yang S L, Zhu S X. Good p-ary quasic-cyclic codes from cyclic codes over $F_p + vF_p$ [J]. Journal of Systems Science and Complexity, 2012, 25: 375 – 384.
[11] Rao A, Pinnawala N. New linear codes over Z_p^s via the trace map [A]. Rao A, Pinnawala N. 2005 Preceedings of the IEEE International Symposium on Information Theory [C]. Adelaide, Australia: IEEE, 2005. 124 – 126.
[12] Golomb S W, Gong G. Signal Design for Good Correlation-For Wireless Communication, Cryptography, and Radar [M]. Cambridge, UK: Cambridge University Press, 2005. 419 – 421.
[13] Ding C S, Yang Y, Tang X H. Optimal sets of frequency hopping sequences from linear cyclic codes [J]. IEEE Transactions on Information Theory, 2010, 56(7): 3605 – 3612.
[14] Zhou Z C, Tang X H, Peng D Y, et al. New constructions for optimal sets of frequency-hopping sequences [J]. IEEE Transactions on Information Theory, 2011, 57(6): 3831 – 3840.
[15] Barg A. Two families of low-correlated binary sequences [J]. Applicable Algebra in Engineering, Communication and Computing, 1996, 7(6): 433 – 437.
[16] Ling S and Solé P. Nonlinear p-ary sequences [J]. Applicable Algebra in Engineering, Communication and Computing, 2003, 14(2): 117 – 125.
[17] Lahtonen J, Ling S, Solé P and Zinovievd D. Z_8-Kerdock codes and pseudorandom binary sequences [J]. Journal of Complexity, 2004, 20(2-3): 318 – 330.
[18] Amarra M C V, Nemenzo F R. On $(1 - u)$-cyclic codes over $F_p^k + uF_p^k$ [J]. Applied Mathematics Letters, 2008, 21(11): 1129 – 1133.
[19] 吴波,朱士信,李平.环 $F_p + uF_p$ 上 Kerdock 码和 Preparata 码[J].电子学报,2008,36(7):1364 – 1367.
Wu Bo, Zhu Shi-xin, Li Ping. Kerdock code and Preparata code over ring $F_p + uF_p$ [J]. Acta Electronica Sinica, 2008, 36(7): 1364 – 1367. (in Chinese)
[20] Code Tables: Bounds on the Parameters of Varous Types of Codes [EB/OL]. http://www.codetables.de/, 2009-09-07.
[21] Ling S and Ozbudak F. An Improvement on the bounds of Weil exponential sums over Galois rings with some application [J]. IEEE Transactions on Information Theory, 2004, 50(10): 2529 – 2539.

作者简介

唐永生(通信作者)　男,1981 年 9 月出生于安徽庐江县,现为合肥师范学院讲师,合肥工业大学计算机与信息学院博士研究生,主要从事代数编码及线性和非线性移位寄存器序列的研究.
E-mail: ysh_tang@163.com

朱士信　男,1962 年 7 月出生于安徽枞阳县,现为合肥工业大学数学学院院长、教授、博士生导师.获国家级教学名师荣誉称号.在国内外发表学术论文 100 余篇.主要从事代数编码及线性和非线性移位寄存器序列的研究.
E-mail: zhushixin@hfut.edu.cn

曹德才　男,1989 年 10 月出生于安徽六安市,硕士研究生,主要从事代数编码的研究.
E-mail: caodecai89@163.com

Hai Quang Dinh　男,1976 年出生于越南,现为肯特州立大学数学科学系副教授,博士生导师.美国环论及其应用中心会员,主要从事代数编码理论、环与模理论的研究.