Computer Science and Application 计算机科学与应用, 2014, 4, 12-18
http://dx.doi.org/10.12677/csa.2014.41003 Published Online January 2014 (http://www.hanspub.org/journal/csa.html)

A Construction of Cyclic Code from Cyclotomic Sequence of Order Six

Sihao Niu[1*], Guangkui Xu[1,2], Xiwang Cao[1]

[1]Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing
[2]Department of Mathematics and Computational Science, Huainan Normal University, Huainan
Email: *niusihao@126.com, xuguangkuiy@163.com, xwcao@nuaa.edu.cn

Received: Dec. 3rd, 2013; revised: Dec. 28th, 2013; accepted: Jan. 7th, 2014

Abstract: Cyclic code is a subclass of linear codes and has a lot of applications in consumer electronics, data transmission technologies, broadcast systems, and computer applications as it has efficient encoding and decoding algorithms. In this paper, the cyclotomic sequence of order six is employed to construct a class of cyclic codes over $GF(q)$ with prime length, and in addition its linear complexity and minima polynomial are determined. The minimal polynomial is served as the generator polynomial of cyclic code and constructs the cyclic codes over $GF(q)$ with the length of n.

Keywords: Cyclic Codes; Cyclotomic Sequences; Minimal Polynomial; Generator Polynomial

基于六阶分圆序列的循环码的构造

牛思皓[1*]，许广魁[1,2]，曹喜望[1]

[1]南京航空航天大学，理学院数学系，南京
[2]淮南师范学院，数学与计算科学系，淮南
Email: *niusihao@126.com, xuguangkuiy@163.com, xwcao@nuaa.edu.cn

收稿日期：2013 年 12 月 3 日；修回日期：2013 年 12 月 28 日；录用日期：2014 年 1 月 7 日

摘　要：循环码是线性码中的一类，在电子产品、数据传输技术、广播系统有着广泛的应用。由于他们有着高效的编码和解码算法，在计算机中也有着广泛的应用。本文中，首先构造了在 $GF(q)$ 上周期为素数 n 的六阶分圆序列，并且给出了序列的线性复杂度和极小多项式。利用此序列的极小多项式作为循环码的生成多项式，构造了 $GF(q)$ 上长度为 n 的循环码。

关键词：循环码；分圆序列；极小多项式；生成多项式

1. 引言

循环码是线性分组码的一个重要子集，是目前研究的比较成熟的一类线性码。它有许多特殊的代数性质，这些性质有助于按所要求的纠错能力系统的构造这类码。在相同长度和维数下，循环码的汉明重量比其他线性码有更小的下界，具有较强的检错和纠错能

*通讯作者。

力。

循环码也有着良好的编码和解码算法，因此，循环码在有线通讯中有着重要的应用。例如，RS 码广泛应用与数据通信和数据存储系统的差错控制中。RS 码在数字存储设备、数字电视、卫星通信等发挥着重要的作用。文献[1-5]给出了循环码的高效的编码和解码算法。

文献[6-9]给出了循环码的一些构造方法和重要性质。丁存生在文献[6]中用两个素数的 Whiteman 广义分圆序列构造了几类具有良好参数的循环码，并且给出了这些循环码的极小重量的下界。闫统江在文献[7]中利用四阶 Whiteman 广义分圆序列构造了另外几类循环码。在文献[9]中，丁存生利用四阶分圆序列构造了 $GF(q)$ 上长度为奇素数的几类最优的循环码。本文中给出了基于六阶分圆序列的循环码的构造方法。

2. 预备知识

2.1. 周期序列的线性复杂度和极小多项式

设 $\lambda^{\infty}=(\lambda_i)_{i=0}^{\infty}$ 为定义在有限域 $GF(q)$ 上周期为 n 的序列。它的线性复杂度定义为该序列的线性移位寄存器的最短长度，即最小正整数 l 满足

$$-c_0\lambda_i=c_1\lambda_{i-1}+c_2\lambda_{i-2}+\cdots+c_l\lambda_{i-l},$$
$$c_0\neq 0,c_1,\cdots,c_l\in GF(q),$$

对所有的 $i\geq l$ 都成立。

多项式 $c(x)=c_0+c_1x+\cdots+c_lx^l$ 称为序列 λ^{∞} 的特征多项式。因为序列 λ^{∞} 的周期为 n，不妨设 $\{\lambda_0,\lambda_1,\cdots,\lambda_{n-1}\}$ 是序列 λ^{∞} 的第一个周期，则其生成多项式定义为 $\Lambda^n(x)=\lambda_0+\lambda_1x+\cdots+\lambda_{n-1}x^{n-1}$。因此该序列的极小多项式定义为

$$m_{\lambda}(x)=\frac{x^n-1}{\gcd\left(x^n-1,\Lambda^n(x)\right)},\tag{1}$$

序列 λ^{∞} 的线性复杂度定义为

$$L=n-\deg\left(\gcd\left(x^n-1,\Lambda^n(x)\right)\right).\tag{2}$$

2.2. q 元循环码定义及其构造方法

设 q 是一个素数的方幂。若 $GF(q)^n$ 为 $GF(q)$ 上的 n 维线性空间，则称 $GF(q)$ 上的参数为 $[n,k,d]$ 的线性码是 $GF(q)^n$ 的一个 k 维子空间。

q 元线性码 C 叫做循环码，是指 $(c_0,c_1,\cdots,c_{n-1})\in C$，则循环移位得到 $(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C$。对于任意的 $(c_0,c_1,\cdots,c_{n-1})\in GF(q)^n$ 满足

$$c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}\in GF(q)[x]\Big/\left(x^n-1\right),$$

这时 $GF(q)$ 上长度为 n 的线性码对应于 $GF(q)[x]\Big/\left(x^n-1\right)$ 的一个子集。$GF(q)[x]\Big/\left(x^n-1\right)$ 是主理想环当且仅当环 $GF(q)[x]\Big/\left(x^n-1\right)$ 的理想都是主理想。

设 $C=\langle g(x)\rangle$ 是循环码且 $h(x)=\left(x^n-1\right)\Big/g(x)$，则称 $g(x)$ 是循环码的生成多项式，$h(x)$ 是循环码的校验多项式。文献[9]给出了几类基于四阶分圆序列的循环码的构造方法，本文中将利用多项式(1)作为循环码的生成多项式给出一类基于六阶分圆序列的循环码的构造方法。由多项式(1)作为生成多项式的循环码 C_{λ}，称为是由序列 λ^{∞} 定义的参数为 (n,k) 的循环码。

2.3. 分圆理论

设 r 是奇素数，则 $GF(r)^*$ 是循环群，令其生成元为 α 且 $d=ord_r(\alpha)$ 表示 α 模 r 的阶。则 $d=ord_r(\alpha)=r-1$。对于正整数 $n>1,e>1$，令其满足 $r-1=ef$。e 阶分圆类有如下定义：

$$C_i^{(e,r)}=\alpha^i\left\langle\alpha^e\right\rangle,i=0,1,\cdots,e-1.$$

则

$$GF(r)^*=C_0^{(e,r)}\cup C_1^{(e,r)}\cup\cdots\cup C_{e-1}^{(e,r)},$$
$$GF(r)=GF(r)^*\cup\{0\}.$$

e 阶分圆数定义为 $(i,j)_e=\left|\left(C_i^{(e,r)}+1\right)\cap C_j^{(e,r)}\right|$，对所有的 $0\leq i\leq e-1,0\leq j\leq e-1$。根据 $C_i^{(e,r)}$ 的定义，由文献[7]可得到下面的结论。

引理 2.1.

1) 对每个 $a\in C_i^{(e,r)}$，则有 $aC_j^{(e,r)}=C_{(i+j)\bmod e}^{(e,r)}$；

2) 若 f 为偶数，则 $-1\in C_0^{(6,r)}$。

2.4. 高斯周期

高斯周期定义为

$$\eta_i^{(e,r)}=\sum_{\chi\in C_i^{(e,r)}}\chi(x),i=0,1,\cdots,e-1,$$

其中 χ 称为有限域 $GF(r)$ 上的典范加法特征。

根据引理 2.1，可以给出高斯周期的一些性质。

引理 2.2.[10] 设 r 是奇素数，则 $GF(r)^*$ 是循环群，$C_i^{(e,r)}$ 是同上所定义的 $GF(r)^*$ 上的 N 阶分圆类，则高斯周期有以下性质：

1) $\sum_{i=0}^{e-1}\eta_i^{(e,r)}=-1$；

2) $\sum_{i=0}^{e-1}\eta_i^{(e,r)}\eta_{i+k}^{(e,r)}=r\theta_k-f$，$k\in\{0,1,\cdots,e-1\}$，其中，

$$\theta_k=\begin{cases}1, & \text{当}f\text{是偶数，}k=0\text{时}\\ 1, & \text{当}f\text{是奇数，}k=\dfrac{e}{2}\text{时}\\ 0, & \text{其它}\end{cases}$$

即 $\theta_k=1$ 当且仅当 $-1\in C_k^{(e,r)}$。

2.5. 循环码的极小距离

高斯周期与高斯和有着紧密的联系。通过离散傅立叶变换，可以得到

$$\eta_i^{(N,r)}=\frac{1}{N}\sum_{j=0}^{N-1}\zeta_N^{-ij}G\left(\psi^j\right)=\frac{1}{N}\left[-1+\sum_{j=0}^{N-1}\zeta_N^{-ij}G\left(\psi^j\right)\right],\quad(3)$$

其中 $\zeta_N=\mathrm{e}^{2\pi\sqrt{-1}/N}$，$\psi$ 是 $GF(r)^*$ 上阶数为 N 的乘法特征。一般情况下，高斯周期的值很难通过计算得到。为了计算循环码的汉明重量的下界，首先给出下面的引理。

引理 2.3. 对于任意的整数 i，满足 $0\le i\le N-1$，可以得到

$$\left|\eta_i^{(N,r)}+\frac{1}{N}\right|\le\left\lfloor\frac{(N-1)\sqrt{r}}{N}\right\rfloor\quad(4)$$

证明：当 $j=0$ 时，$G(\psi_0)=\sum_{x\in F_r^*}\chi(x)=-1$。

所以，

$$\begin{aligned}\left|\eta_i^{(N,r)}+\frac{1}{N}\right|&=\left|\frac{1}{N}\sum_{j=0}^{N-11}\zeta_N^{-ij}G\left(\psi^j\right)+\frac{1}{N}\right|\\&=\left|\frac{1}{N}G(\psi_0)+\frac{1}{N}\sum_{j=1}^{N-11}\zeta_N^{-ij}G\left(\psi^j\right)+\frac{1}{N}\right|\\&=\left|\frac{1}{N}\sum_{j=1}^{N-11}\zeta_N^{-ij}G\left(\psi^j\right)\right|\\&\le\frac{1}{N}\sum_{j=1}^{N-1}\left|G\left(\psi^j\right)\right|\le\left\lfloor\frac{(N-1)\sqrt{r}}{N}\right\rfloor\end{aligned}$$

。

令 $\gcd(n,q)=1$，且 $k=ord_n(q)$ 是 q 模 n 的阶数。设 $r=q^k$，N 是整除 $r-1$ 的正整数，n 是满足 $n=(r-1)/N$ 的正整数。设 α 是 $GF(r)^*$ 上的本原元，$\theta=\alpha^N$。则集合

$$\begin{aligned}\overline{C}(r,N)=\Big\{&\left(\mathrm{Tr}_{r/q}(a+b),\mathrm{Tr}_{r/q}(a\theta+b),\cdots,\right.\\&\left.\mathrm{Tr}_{r/q}\left(a\theta^{n-1}+b\right)\right)\Big|a,b\in GF(r)\Big\}\end{aligned}\quad(5)$$

是 $GF(q)$ 上参数为 $[n,k+1]$ 的循环码，$\mathrm{Tr}_{r/q}$ 是 $GF(r)$ 到 $GF(q)$ 上的迹函数。

由文献[11]的定理可以得到，$\overline{C}(r,N)$ 是 $GF(q)$ 上以 $(x-1)m_{\theta^{-1}}(x)$ 为校验多项式的循环码，其中 $m_{\theta^{-1}}(x)$ 是 $GF(q)$ 上以 θ^{-1} 为极小多项式的不可约多项式。

引理 2.4.[9] N 是整除 $r-1$ 的正整数，$k=ord_n(q)$ 是 q 模 n 的阶数。设 $N_1=\gcd((r-1)/(q-1),N)$，则(3)中 $\overline{C}(r,N)$ 是 $GF(q)$ 上参数为 $[n,k+1,d]$ 的循环码，循环码的极小距离 d 满足

$$d\ge\min\left((q-1)\left\lfloor\frac{r-\lfloor(r-1)\sqrt{r}\rfloor}{qN}\right\rfloor,\ \frac{(q-1)(r-1)-1}{qN}-\frac{q-1}{q}\left\lfloor\frac{(N-1)\sqrt{r}}{N}\right\rfloor\right)$$

定理 2.5. 令 $k=\dfrac{n-1}{3}$ 且 $q-1<n$，$q\in C_0^{(6,n)}$，则 $GF(q)$ 上以 $(x-1)m_{\theta^{-1}}(x)$ 为校验多项式的循环码的参数为 $[n,(n+2)/3,d]$，

$$d\ge\frac{(q-1)(r-1)-1}{qN}-\frac{q-1}{q}\left\lfloor\frac{(N-1)\sqrt{r}}{N}\right\rfloor$$

其中 $N=\left(q^{(n-1)/3}-1\right)/3$。

证明：因为 $k=ord_n(q)=(n-1)/3$ 且 $q-1<n$，所以多项式 $\Omega_1^{(6,n)}(x)$ 是 $GF(q)$ 上的不可约多项式。因为(3)中循环码的校验多项式为 $(x-1)m_{\theta^{-1}}(x)$，所以循环码的维数等于 $(n+2)/3$。

由 $q-1<n$，n 是素数可以得到

$$N_1=\gcd\left(\frac{q^{(n-1)/3}-1}{q-1},N\right)=N/(q-1).$$

则极小距离 d 由引理 2.4 可以得到。

3. 基于六阶分圆序列的循环码的构造

设 n 是一个素数，$n\equiv1(\mathrm{mod}3)$，则 n 可以表示成 $n=u^2+3v^2$，$u\equiv1(\mathrm{mod}3)$，v 的符号是不确定的。对

于素数 q，令 $q=3$，且 $\gcd(n,3)=1$。设 η 是 $GF(3)$ 扩域上的 n 阶本原单位根，$ord_n(q)$ 是 q 模 n 的乘法阶。

定义 $\Omega_i^{(6,n)}(x)=\prod_{i\in C_i^{(6,n)}}\left(x-\eta^i\right)$，$C_i^{(6,n)}$ 称为 $GF(n)$ 上的 6 阶分圆类，则 $x^n-1=(x-1)\prod_{i=0}^{5}\Omega_i^{(6,n)}(x)$，显然 $\Omega_i^{(6,n)}(x)\in GF(3)[x]$。

下面我们将给出基于六阶分圆序列的循环码的构造，为此先给出 $GF(3)$ 上的序列 λ^∞。定义

$$\lambda_i=\begin{cases}1, & i \bmod n\in C_0^{(6,n)}\cup C_3^{(6,n)}\\ -1, & i \bmod n\in C_1^{(6,n)}\cup C_4^{(6,n)}\\ 0, & \text{其它}\end{cases},\ i\ge 0.$$

此序列即是 $GF(3)$ 上的序列。

为了计算序列的极小多项式和线性复杂度，我们需要计算 $\gcd\left(x^n-1,\Lambda(x)\right)$，并且需要给出下面的多项式

$$\Lambda(x)=\sum_{i\in C_0^{(6,n)}\cup C_3^{(6,n)}}x^i-\sum_{i\in C_1^{(6,n)}\cup C_4^{(6,n)}}x^i \tag{5}$$

$$\Gamma(x)=\sum_{i\in C_1^{(6,n)}\cup C_4^{(6,n)}}x^i-\sum_{i\in C_2^{(6,n)}\cup C_5^{(6,n)}}x^i \tag{6}$$

由引理 2.2 可得到

$$\sum_{i\in C_0^{(6,n)}}\eta^i+\sum_{i\in C_1^{(6,n)}}\eta^i+\sum_{i\in C_2^{(6,n)}}\eta^i+\sum_{i\in C_3^{(6,n)}}\eta^i+\sum_{i\in C_4^{(6,n)}}\eta^i+\sum_{i\in C_5^{(6,n)}}\eta^i=-1$$

由(5)式和(6)式，以及引理 2.1 可得到下面的引理。

引理 3.1

$$\Lambda(\eta^a)=\begin{cases}\Lambda(\eta), & a\in C_0^{(6,n)}\\ \Gamma(\eta), & a\in C_1^{(6,n)}\\ -(\Lambda(\eta)+\Gamma(\eta)), & a\in C_2^{(6,n)}\\ \Lambda(\eta), & a\in C_3^{(6,n)}\\ \Gamma(\eta), & a\in C_4^{(6,n)}\\ -(\Lambda(\eta)+\Gamma(\eta)), & a\in C_5^{(6,n)}\end{cases},$$

并且 $\Lambda(\eta^0)=\Lambda(1)=0$。

证明： 由引理 2.1 知，如果 $a\in C_i^{(6,n)}$，则有 $aC_j^{(6,n)}=C_{(i+j)\bmod 6}^{(6,n)}$。

当 $a\in C_0^{(6,n)}$ 时，则 $aC_i^{(6,n)}=C_i^{(6,n)}$，所以

$$\Lambda(\eta^a)=\sum_{i\in C_0^{(6,n)}\cup C_3^{(6,n)}}\eta^{ai}-\sum_{i\in C_1^{(6,n)}\cup C_4^{(6,n)}}\eta^{ai}=\sum_{i\in C_0^{(6,n)}\cup C_3^{(6,n)}}x^i-\sum_{i\in C_1^{(6,n)}\cup C_4^{(6,n)}}x^i=\Lambda(\eta).$$

当 $a\in C_1^{(6,n)}$ 时，则 $aC_i^{(6,n)}=C_{(i+1)\bmod 6}^{(6,n)}$，所以

$$\Lambda(\eta^a)=\sum_{i\in C_0^{(6,n)}\cup C_3^{(6,n)}}\eta^{ai}-\sum_{i\in C_1^{(6,n)}\cup C_4^{(6,n)}}\eta^{ai}=\sum_{i\in C_1^{(6,n)}\cup C_4^{(6,n)}}x^i-\sum_{i\in C_2^{(6,n)}\cup C_5^{(6,n)}}x^i=\Gamma(x).$$

当 $a\in C_2^{(6,n)}$ 时，则 $aC_i^{(6,n)}=C_{(i+2)\bmod 6}^{(6,n)}$，所以

$$\Lambda(\eta^a)=\sum_{i\in C_0^{(6,n)}\cup C_3^{(6,n)}}\eta^{ai}-\sum_{i\in C_1^{(6,n)}\cup C_4^{(6,n)}}\eta^{ai}=-(\Lambda(\eta)+\Gamma(\eta)).$$

同理，当 $a\in C_3^{(6,n)}$ 时，$a\in C_{(i+3)\bmod 6}^{(6,n)}$，所以

$$\Lambda(\eta^a)=\sum_{i\in C_0^{(6,n)}\cup C_3^{(6,n)}}\eta^{ai}-\sum_{i\in C_1^{(6,n)}\cup C_4^{(6,n)}}\eta^{ai}=\sum_{i\in C_0^{(6,n)}\cup C_3^{(6,n)}}x^i-\sum_{i\in C_1^{(6,n)}\cup C_4^{(6,n)}}x^i=\Lambda(\eta).$$

当 $a\in C_4^{(6,n)}$ 时，则 $aC_i^{(6,n)}=C_{(i+4)\bmod 6}^{(6,n)}$，所以

$$\Lambda(\eta^a)=\sum_{i\in C_0^{(6,n)}\cup C_3^{(6,n)}}\eta^{ai}-\sum_{i\in C_1^{(6,n)}\cup C_4^{(6,n)}}\eta^{ai}=\sum_{i\in C_1^{(6,n)}\cup C_4^{(6,n)}}x^i-\sum_{i\in C_2^{(6,n)}\cup C_5^{(6,n)}}x^i=\Gamma(x).$$

当 $a\in C_5^{(6,n)}$ 时，则 $a\in C_{(i+5)\bmod 6}^{(6,n)}$，所以

$$\Lambda(\eta^a)=\sum_{i\in C_0^{(6,n)}\cup C_3^{(6,n)}}\eta^{ai}-\sum_{i\in C_1^{(6,n)}\cup C_4^{(6,n)}}\eta^{ai}=-(\Lambda(\eta)+\Gamma(\eta)).$$

引理 3.2.[10] 如果 $-1\in C_0^{(6,n)}$，$3\in C_0^{(6,n)}$，则

1)

$$\eta_l^2=\left(\sum_{i\in C_l^{(6,n)}}\eta^i\right)^2$$
$$=(l,l)\eta_0+(l-1,l-1)\eta_1+(l-2,l-2)\eta_2+(l-3,l-3)\eta_3+(l-4,l-4)\eta_4+(l-5,l-5)\eta_5+\frac{n-1}{6}$$

2)

$$\eta_l\eta_{l+3}=\sum_{i\in C_l^{(6,n)}}\sum_{j\in C_{l+3}^{(6,n)}}\eta^{i-j}$$
$$=(l+3,l)\eta_0+(l+2,l-1)\eta_1+(l+1,l-2)\eta_2+(l,l-3)\eta_3+(l-1,l-4)\eta_4+(l-2,l-5)\eta_5$$

引理 3.3.[12] 假设 $n=6f+1$ 为奇素数，并且 $4n=L^2+27M^2$，其中 $L\equiv 1(\bmod 3)$，$3\mid M$　f 为偶数

时，则 $-1\in C_0, 3\in C_0$， $\eta_i\left(i=0,1,2,3,4,5\right)$ 的值在[12]的表 3 中已给出。如下：

1) 当 $ind_\eta 2\equiv 0\left(\mathrm{mod}\,3\right)$ 时，

当 $n\equiv 1\left(\mathrm{mod}\,36\right)$ 时，

$$\eta_0=\eta_1=\eta_2=\eta_3=\eta_4=0,\eta_5=-1;$$

当 $n\equiv 13\left(\mathrm{mod}\,36\right)$ 时，

$$\eta_1=\eta_2=\eta_3=\eta_4=\eta_5=1,\eta_0=0;$$

当 $n\equiv 25\left(\mathrm{mod}\,36\right)$ 时，

$$\eta_1=\eta_2=\eta_3=\eta_4=\eta_5=-1,\eta_0=1.$$

2) 当 $ind_\eta 2\equiv 1\left(\mathrm{mod}\,3\right)$ 时

当 $n\equiv 1\left(\mathrm{mod}\,36\right)$ 时，

$$\eta_1=\eta_4=0,\eta_0=\eta_2=\eta_5=1,\eta_3=-1;$$

当 $n\equiv 13\left(\mathrm{mod}\,36\right)$ 时，

$$\eta_0=\eta_3=\eta_4=-1,\eta_2=\eta_5=1,\eta_1=0;$$

当 $n\equiv 25\left(\mathrm{mod}\,36\right)$ 时，

$$\eta_0=\eta_1=\eta_3=0,\eta_2=\eta_5=-1,\eta_4=1;$$

3) 当 $ind_\eta 2\equiv 2\left(\mathrm{mod}\,3\right)$ 时

当 $n\equiv 1\left(\mathrm{mod}\,36\right)$ 时，

$$\eta_0=\eta_3=0,\eta_1=\eta_2=\eta_5=1,\eta_4=-1;$$

当 $n\equiv 13\left(\mathrm{mod}\,36\right)$ 时，

$$\eta_0=\eta_3=\eta_5=-1,\eta_1=\eta_4=1,\eta_2=0;$$

当 $n\equiv 25\left(\mathrm{mod}\,36\right)$ 时，

$$\eta_0=\eta_2=\eta_3=0,\eta_1=\eta_4=-1,\eta_5=1.$$

下面我们将给出序列 λ^∞ 的极小多项式和线性复杂度，即给出循环码的生成多项式结果如下面的定理所示：

定理 3.4. 设 n 是一个素数，且 $n\equiv 1\left(\mathrm{mod}\,3\right)$，$n=u^2+3v^2$，$u\equiv 1\left(\mathrm{mod}\,3\right)$，$v$ 的符号是不确定的。λ^∞ 是定义在 $GF\left(q\right)$ 上的序列。由序列 λ^∞ 定义的 $GF\left(q\right)$ 上的循环码 C_λ 的参数为 $\left[n,k,d\right]$，并且循环码 C_λ 的生成多项式即为序列 λ^∞ 的极小多项式，维数 $k=n-\deg\left(m_\lambda\left(x\right)\right)$，则循环码 C_λ 的生成多项式为：

1) 当 $ind_\eta 2\equiv 0\left(\mathrm{mod}\,3\right)$ 时，极小多项式，即循环码 C_λ 生成多项式为

$$g\left(x\right)=m_\lambda\left(x\right)=\begin{cases}\dfrac{x^n-1}{\left(x-1\right)\Omega_0^{(6,n)}\left(x\right)\Omega_3^{(6,n)}\left(x\right)}, & n\equiv 1\left(\mathrm{mod}\,36\right)\\ \dfrac{x^n-1}{\left(x-1\right)\Omega_1^{(6,n)}\left(x\right)\Omega_4^{(6,n)}\left(x\right)}, & n\equiv 13\left(\mathrm{mod}\,36\right)\\ \dfrac{x^n-1}{\left(x-1\right)\Omega_1^{(6,n)}\left(x\right)\Omega_4^{(6,n)}\left(x\right)}, & n\equiv 25\left(\mathrm{mod}\,36\right).\end{cases}$$

线性复杂度为

$$L=n-\deg\left(\gcd\left(x^n-1,\Lambda^n\left(x\right)\right)\right)=n-\frac{n+2}{3}=\frac{2n-2}{3}。$$

即由序列 λ^∞ 定义循环码 C_λ 的生成多项式为 $m_\lambda\left(x\right)$，它的参数为 $\left[n,\left(n+2\right)/3,d\right]$。循环码的极小距离 d 满足定理 2.5 所给定的下界。

2) 当 $ind_\eta 2\equiv 1\left(\mathrm{mod}\,3\right)$ 时，极小多项式，即循环码 C_λ 生成多项式为

$$g\left(x\right)=m_\lambda\left(x\right)=\begin{cases}\dfrac{x^n-1}{\left(x-1\right)\Omega_0^{(6,n)}\left(x\right)\Omega_3^{(6,n)}\left(x\right)}, & n\equiv 1\left(\mathrm{mod}\,36\right)\\ \dfrac{x^n-1}{\left(x-1\right)\Omega_1^{(6,n)}\left(x\right)\Omega_4^{(6,n)}\left(x\right)}, & n\equiv 13\left(\mathrm{mod}\,36\right)\\ \dfrac{x^n-1}{\left(x-1\right)\Omega_1^{(6,n)}\left(x\right)\Omega_4^{(6,n)}\left(x\right)}, & n\equiv 25\left(\mathrm{mod}\,36\right)\end{cases}$$

线性复杂度为

$$L=n-\deg\left(\gcd\left(x^n-1,\Lambda^n\left(x\right)\right)\right)=n-\frac{n+2}{3}=\frac{2n-2}{3}。$$

即由序列 λ^∞ 定义循环码 C_λ 的生成多项式为 $m_\lambda\left(x\right)$，它的参数为 $\left[n,\left(n+2\right)/3,d\right]$。循环码的极小距离 d 满足定理 2.5 所给定的下界。

3) 当 $ind_\eta 2\equiv 2\left(\mathrm{mod}\,3\right)$ 时，极小多项式，即循环码 C_λ 生成多项式为

$$g\left(x\right)=m_\lambda\left(x\right)=\begin{cases}\dfrac{x^n-1}{\left(x-1\right)\Omega_0^{(6,n)}\left(x\right)\Omega_3^{(6,n)}\left(x\right)}, & n\equiv 1\left(\mathrm{mod}\,36\right)\\ \dfrac{x^n-1}{\left(x-1\right)\Omega_1^{(6,n)}\left(x\right)\Omega_4^{(6,n)}\left(x\right)}, & n\equiv 13\left(\mathrm{mod}\,36\right)\\ \dfrac{x^n-1}{\left(x-1\right)\Omega_1^{(6,n)}\left(x\right)\Omega_4^{(6,n)}\left(x\right)}, & n\equiv 25\left(\mathrm{mod}\,36\right)\end{cases}$$

线性复杂度为

$$L=n-\deg\left(\gcd\left(x^n-1,\Lambda^n\left(x\right)\right)\right)=n-\frac{n+2}{3}=\frac{2n-2}{3}.$$

即由序列 λ^∞ 定义循环码 C_λ 的生成多项式为 $m_\lambda\left(x\right)$，它的参数为 $\left[n,\left(n+2\right)/3,d\right]$。循环码的极小距离 d 满足定理 2.5 所给定的下界。

证明： 1. 1) 当 $n\equiv 1\left(\mathrm{mod}\,36\right)$ 时，

$$\eta_0=\eta_1=\eta_2=\eta_3=\eta_4=0,\eta_5=-1.$$

当 $a\in C_0^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=\Lambda\left(\eta\right)=0$；

当 $a\in C_1^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=\Gamma\left(\eta\right)=1\neq 0$；

当 $a\in C_2^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=-\left(\Lambda\left(\eta\right)+\Gamma\left(\eta\right)\right)=-1\neq 0$；

当 $a\in C_3^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=\Lambda\left(\eta\right)=0$；

当 $a\in C_4^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=\Gamma\left(\eta\right)=1\neq 0$；

当 $a\in C_5^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=-\left(\Lambda\left(\eta\right)+\Gamma\left(\eta\right)\right)=-1\neq 0$；

所以，它的极小多项式，即生成多项式为

$$g\left(x\right)=m_\lambda\left(x\right)=\frac{x^n-1}{\gcd\left(x^n-1,\Lambda^n\left(x\right)\right)}=\frac{x^n-1}{\left(x-1\right)\Omega_0^{(6,n)}\left(x\right)\Omega_3^{(6,n)}\left(x\right)},$$

线性复杂度

$$L=n-\deg\left(\gcd\left(x^n-1,\Lambda^n\left(x\right)\right)\right)=n-\frac{n-1}{3}=\frac{2n+1}{3}.$$

2) 当 $n\equiv 13\left(\mathrm{mod}\,36\right)$ 时，

$$\eta_1=\eta_2=\eta_3=\eta_4=\eta_5=1,\eta_0=0.$$

当 $a\in C_0^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=\Lambda\left(\eta\right)=-1\neq 0$；

当 $a\in C_1^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=\Gamma\left(\eta\right)=0$；

当 $a\in C_2^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=-\left(\Lambda\left(\eta\right)+\Gamma\left(\eta\right)\right)=1\neq 0$；

当 $a\in C_3^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=\Lambda\left(\eta\right)=-1\neq 0$；

当 $a\in C_4^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=\Gamma\left(\eta\right)=0$；

当 $a\in C_5^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=-\left(\Lambda\left(\eta\right)+\Gamma\left(\eta\right)\right)=1\neq 0$；

所以，它的极小多项式，即生成多项式为

$$g\left(x\right)=m_\lambda\left(x\right)=\frac{x^n-1}{\left(x-1\right)\Omega_1^{(6,n)}\left(x\right)\Omega_4^{(6,n)}\left(x\right)},$$

线性复杂度

$$L=n-\deg\left(\gcd\left(x^n-1,\Lambda^n\left(x\right)\right)\right)=n-\frac{n-1}{3}=\frac{2n+1}{3}.$$

3) 当 $n\equiv 25\left(\mathrm{mod}\,36\right)$ 时，

$$\eta_1=\eta_2=\eta_3=\eta_4=\eta_5=-1,\eta_0=1。$$

当 $a\in C_0^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=\Lambda\left(\eta\right)=2\neq 0$；

当 $a\in C_1^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=\Gamma\left(\eta\right)=0$；

当 $a\in C_2^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=-\left(\Lambda\left(\eta\right)+\Gamma\left(\eta\right)\right)=1\neq 0$；

当 $a\in C_3^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=\Lambda\left(\eta\right)=2\neq 0$；

当 $a\in C_4^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=\Gamma\left(\eta\right)=0$；

当 $a\in C_5^{(6,n)}$ 时，$\Lambda\left(\eta^a\right)=-\left(\Lambda\left(\eta\right)+\Gamma\left(\eta\right)\right)=1\neq 0$；

所以，它的极小多项式，即生成多项式为

$$g\left(x\right)=m_\lambda\left(x\right)=\frac{x^n-1}{\left(x-1\right)\Omega_1^{(6,n)}\left(x\right)\Omega_4^{(6,n)}\left(x\right)},$$

线性复杂度

$$L=n-\deg\left(\gcd\left(x^n-1,\Lambda^n\left(x\right)\right)\right)=n-\frac{n+2}{3}=\frac{2n-2}{3}.$$

同理，当 $ind_\eta 2\equiv 1\left(\mathrm{mod}\,3\right)$ 和 $ind_\eta 2\equiv 2\left(\mathrm{mod}\,3\right)$ 时，序列 λ^∞ 的极小多项式 $m_\lambda\left(x\right)$，即循环码的生成多项式和维数可由引理 3 得到。

例 取 $q=3$，$n=61$，则 C_λ 是 $GF\left(3\right)$ 上参数为 $\left[61,21,41\right]$ 的循环码。

取 $q=3$，$n=127$，则 C_λ 是 $GF\left(3\right)$ 上参数为 $\left[127,43,85\right]$ 的循环码。

4. 结论

本篇文章，我们给出了基于六阶分圆序列构造了循环码的构造方法。计算了在 $GF\left(q\right)$ 上周期为素数 n 的序列的极小多项式和线性复杂度。利用极小多项式 $m_\lambda\left(x\right)$ 作为循环码 C_λ 的生成多项式 $g\left(x\right)$，构造并计算了在 $GF\left(q\right)$ 上参数为 $\left[n,k,d\right]$ 的循环码 C_λ。

基金项目

安徽省淮南师范学院自然科学研究项目(No. 2013XJ67)。

参考文献 (References)

[1] Cheng, Q. and Wan, D. (2007) On the list and bounded distance decodability of Reed-Solomon codes. *SIAM Journal on Computing*, **37**, 195-209.

[2] Cheng, Q. and Wan, D. (2010) Complexity of decoding positive rate Reed-Solomon codes. *IEEE Transactions on Information*

Theory, **56**, 5217-5222.

[3] Chien, R.T. (1964) Cyclic decoding procedure for the Bose-Chaudhuri-Hocquenghem codes. *IEEE Transactions on Information Theory*, **10**, 357-363.

[4] Forney, G.D. (1965) On decoding BCH codes. *IEEE Transactions on Information Theory*, **11**, 549-557.

[5] Prange, E. (1958) Some cyclic error-correcting codes with simple decoding algorithms. Air Force Cambridge Research Center-TN-58-156, Cambridge.

[6] Ding, C. (2012) Cyclic codes from the two-prime sequences. *IEEE Transactions on Information Theory*, **58**, 3881-3891.

[7] Sun, Y., Yan, T. and Li, H. (2013) Cyclic codes from the two-prime Whiteman's generalized cyclotomic sequences with order 4. http://arxiv.org/abs/1303.6378

[8] Ding, C. (2013) A q-polynomial approach to cyclic codes. *Finite Fields and Their Applications*, **20**, 1-14.

[9] Ding, C. (2013) Cyclic codes from cyclotomic sequences of order four. *Finite Fields and Their Applications*, **23**, 8-34.

[10] Storer, T. (1967) Cyclotomy and difference sets. Markham, Chicago.

[11] Delsarte, P. (1975) On subfield subcodes of modified Reed-SoloMon codes. *IEEE Transactions on Information Theory*, **21**, 575-576.

[12] Yin, Y. and Cao, X. (2012) The autorrelation values and linear complexity of a class of generalized ternary sequence. *Computer Science and Application*, **2**, 165-171.