有限链环上一类常循环码的距离

袁 健 朱士信* 开晓山
(合肥工业大学数学学院 合肥 230009)
(东南大学移动通信国家重点实验室 南京 210096)

摘 要：在编码理论中，线性码的(最小)距离是一个极其重要的参数，它决定了码的纠错能力。设 R 为任一有限交换链环，a 为其最大理想的一个生成元，R^* 为 R 的乘法单位群。对于任意 $w \in R^*$，该文利用 R 上任意长度的 $(1+aw)$-常循环码的生成结构，通过计算这类码的高阶挠码，得到了 R 上任意长度的 $(1+aw)$-常循环码的汉明距离，并研究了这类常循环码的齐次距离。这给编译有限链环上此类常循环码提供了重要的理论依据。

关键词：常循环码；有限链环；汉明距离；齐次距离
中图分类号： TN911.22 **文献标识码**： A **文章编号**：1009-5896(2017)03-0754-04
DOI: 10.11999/JEIT160392

On Distances of Family of Constacyclic Codes over Finite Chain Rings

YUAN Jian ZHU Shixin KAI Xiaoshan
(*School of Mathematics*, *Hefei University of Technology*, *Hefei* 230009, *China*)
(*National Mobile Communications Research Laboratory*, *Southeast University*, *Nanjing* 210096, *China*)

Abstract: In coding theory, the (minimum) distance of a code is a very important invariant, which always determines the error-correcting capability of the code. Let R be an arbitrary commutative finite chain ring, a is a generator of the unique maximal ideal and R^* is the multiplicative group of units of R. In this paper, for any $w \in R^*$, by using the generator polynomials of $(1+aw)$-constacyclic codes of any length over R, higher torsion codes of such codes are calculated. The Hamming distance of all $(1+aw)$-constacyclic codes of any length over R is determined and the exact homogeneous distance of some such codes is obtained. The result provides a theoretical basis for encoding and decoding for such constacyclic codes.

Key words: Constacyclic codes; Finite chain rings; Hamming distance; Homogeneous distance

1 引言

自 20 世纪九十年代中期，Hammons 等人[1]发现一些高效的二元非线性码为 Z_4 上线性码的 Gray 像以来，有限链环上纠错码一直是编码理论研究的热点[2–7]。有限链环上的常循环码是一类非常重要的线性码。有限域或环上码的汉明距离在衡量码的纠错能力起重要作用，Norton 和 Sălăgean[8]利用挠码研究有限链环上线性码的汉明距离。齐次距离在研究有限链环上码中非常重要[6,9]。在本文中，设 R 为任一有限交换链环，a 为其最大理想的一个生成元，R^* 为 R 的乘法单位群。对于任意 $w \in R^*$，我们先引用关于 R 上任意长度的 $(1+aw)$-常循环码结构[10]。利用此生成结构性质，通过计算高阶挠码，结合代数计算程序 MAGAM，得到了 R 上任意长度的所有 $(1+aw)$-常循环码的汉明距离，还研究并得到了这类码齐次距离的一些重要结果。

2 有限链环和常循环码

如果一个有限含幺交换环是局部环并且其最大理想是主理想，那么该环是有限链环。本文中以 R 表示任一有限链环，R^* 表示 R 的乘法单位群。设 a 为 R 的最大理想的一个生成元。于是 a 为一幂零元，本文记 t 为其幂零指数。本文记 R 模其最大理想 $\langle a\rangle$ 的剩余域为 $\overline{R}$，即 $\overline{R}=R/\langle a\rangle=F_{p^r}$，其中 F_{p^r} 为含有 p^r 个元素的有限域，p 为 $\overline{R}$ 的特征。R 的势为 $|R|=|\overline{R}|^t$。R 到 $\overline{R}$ 存在一个自然环满同态映射 $\mu: r$

收稿日期：2016-04-22；改回日期：2016-09-23；网络出版：2016-11-14
*通信作者：朱士信 zhushixin@hfut.edu.cn
基金项目：国家自然科学基金(61370089, 60973125)，东南大学国家移动通信研究实验室开放研究基金(2014D04)，安徽省自然科学基金(1508085SQA198)
Foundation Items: The National Natural Science Foundation of China (61370089, 60973125), The Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (2014D04), The Natural Science Foundation of Anhui Province (1508085SQA198)

$\mapsto r+\langle a\rangle$。此映射可以自然开拓为 $R[x]$ 到 $\overline{R}[x]$ 的一个环同态，我们仍将它记作 μ。对于任意 $f(x)\in R[x]$，我们记其在 μ 下的像为 $\mu(f(x))=\overline{f}(x)$。根据文献[11]，对于 R 中任一非零元 α，存在唯一的 $i\in\{0,1,\cdots,t\}$ 和唯一的单位 $v\in R$，使得 $\alpha=va^i$，其中 v 在模 a^{t-i} 下唯一。对于 $f_1(x),f_2(x)\in R[x]$，若有 $\lambda_1(x),\lambda_2(x)\in R[x]$ 使得 $\lambda_1(x)f_1(x)+\lambda_2(x)f_2(x)=1$，则称 $f_1(x),f_2(x)$ 在 $R[x]$ 上互素。$f_1(x),f_2(x)$ 在 $R[x]$ 上互素当且仅当 $\overline{f}_1(x),\overline{f}_2(x)$ 在 $\overline{R}[x]$ 上互素[11]。

设 N 为任一正整数。R 上长度为 N 的线性码是 R^N 的一个 R-子模。对于某一固定的单位 $\lambda\in R$ 和 R 上长度为 N 的线性码 C，若对于任意码字 $(c_0,c_1,\cdots,c_{N-1})\in C$ 都有 $(\lambda c_{N-1},c_0,\cdots,c_{N-2})\in C$，则称 C 为 R 上长度为 N 的 λ-常循环码。特别的，当 $\lambda=1$ (或 -1)时，λ-常循环码为循环码(或负循环码)。通常地，将码字 $c=(c_0,c_1,\cdots,c_{N-1})$ 等同于其多项式表示 $c(x)=c_0+c_1x+\cdots+c_{N-1}x^{N-1}$，则 R 上任一长度为 N 的 λ-常循环码都恰为 $R[x]\Big/\left\langle x^N-\lambda\right\rangle$ 的一个理想。本文设 $N=p^sn$，其中 $\gcd(p,n)=1$，s 为非负整数；记 $\lambda=1+aw$，其中 $w\in R^*$；设 $x^n-1=\prod_{i=1}^{m}f_i(x)$，其中 $f_i(x)$ ($0\le i\le t-1$)为 x^n-1 在 $R[x]$ 上的首一不可约因式。

定理 1[10]　每一个互不相同的 R 上长度为 N 的 λ-常循环码可唯一表示成 $C=\left\langle\prod_{i=1}^{m}f_i(x)^{k_i}\right\rangle$，其中 $0\le k_i\le p^st$，$i=1,2,\cdots,m$。R 上长度为 N 的 λ-常循环码的数目为 $\left(p^st+1\right)^m$。上述码 C 中码字数目为 $|C|=\left|\overline{R}\right|^{\sum_{i=1}^{m}\left(p^st-k_i\right)\deg\left(f_i(x)\right)}$。

3　汉明距离和齐次距离

一些高效的二元非线性码可以看作是 Z_4 上线性码在一个 Z_4^n (n 为该线性码的长度)关于李距离到 Z_2^{2n} 关于汉明距离的保距 Gray 映射下的像。文献[9]把 Z_4 上的这个 Gray 映射的概念推广到有限链环上。R 中元素的齐次重量[9]的定义：

$$w_{\hom}(\alpha):R\to N,$$

$$\alpha\mapsto\begin{cases}\left(p^r-1\right)p^{r(t-2)}, & \alpha\in R\setminus\left\langle a^{t-1}\right\rangle\\ p^{r(t-1)}, & \alpha\in\left\langle a^{t-1}\right\rangle\setminus\{0\}\\ 0, & \alpha=0\end{cases}$$

码中任一码字的齐次重量为它的所有分量的齐次重量的和。线性码 C 的齐次距离 $d_{\hom}(C)$ 为码 C 所有非零码字的齐次重量中的最小值。汉明重量和汉明距离按照通常的定义。下面来研究 R 上长度为 N 的 λ-常循环码的汉明距离和齐次距离。

设 C 为 R 上长度为 N 的线性码。对于 $0\le i\le t-1$，定义 C 的第 i 阶挠码[7]为 $\mathrm{Tor}_i(C)=\{\overline{c}\,|\,a^ic\in C\}$。显然 $\mathrm{Tor}_i(C)$ ($0\le i\le t-1$)为 $\overline{R}$ 上长度为 N 的线性码，并且 $\mathrm{Tor}_0(C)\subseteq\mathrm{Tor}_1(C)\subseteq\cdots\subseteq\mathrm{Tor}_{t-1}(C)$。通常称 $\mathrm{Tor}_0(C)=\overline{C}$ 为剩余码，有时记 $\mathrm{Re}\,s(C)$。设 C 为 R 上长度为 N 的线性码，其标准形式的生成矩阵为

$$\begin{pmatrix}I_{k_0} & A_{01} & A_{02} & \cdots & A_{0,t-1} & A_{0,t}\\ 0 & aI_{k_1} & aA_{12} & \cdots & aA_{1,t-1} & aA_{1,t}\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & a^{t-1}I_{k_{t-1}} & a^{t-1}A_{t-1,t}\end{pmatrix}$$

其中该分块矩阵的分块的列的长度分别为 $k_0,k_1,\cdots,k_{t-1}$，$N-\sum_{i=0}^{t-1}k_i$，$k_i\ge0$。由文献[7]，有 $|C|=\left|\overline{R}\right|^{\sum_{j=0}^{t-1}(t-j)k_j}$。对每一 $0\le i\le t-1$，$\mathrm{Tor}_i(C)$ 的生成矩阵为

$$\begin{pmatrix}I_{k_0} & \overline{A}_{01} & \overline{A}_0 & \cdots & \overline{A}_{0,i} & \cdots & \overline{A}_{0t}\\ 0 & I_{k_1} & \overline{A}_{12} & \cdots & \overline{A}_{1,i} & \cdots & \overline{A}_{1,t}\\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & I_{k_i} & \cdots & \overline{A}_{it}\end{pmatrix}$$

于是 $\left|\mathrm{Tor}_i(C)\right|=\prod_{j=0}^{i}\left|\overline{R}\right|^{k_j}$。所以，$\prod_{i=0}^{t-1}\left|\mathrm{Tor}_i(C)\right|=\prod_{i=0}^{t-1}\prod_{j=0}^{i}\left|\overline{R}\right|^{k_j}=\left|\overline{R}\right|^{\sum_{j=0}^{t-1}(t-j)k_j}=|C|$。

定理 2　设 C 为 R 上长度为 N 的线性码。则 $|C|=\prod_{i=0}^{t-1}\left|\mathrm{Tor}_i(C)\right|$。

设 $C=\left\langle\prod_{i=1}^{m}f_i(x)^{k_i}\right\rangle$ 为 R 上长度为 N 的 λ-常循环码，$0\le k_i\le p^st$。对于每一 $0\le j\le t-1$，$\mathrm{Tor}_j(C)$ 显然为 $\overline{R}$ 长度为 N 的循环码。记 $R_N=R[x]\Big/\left\langle x^n-\lambda\right\rangle$ 和 $\overline{R}_N=\overline{R}[x]\Big/\left\langle x^n-1\right\rangle$。则有 $\mathrm{Tor}_j(C)$ 为 $\overline{R}_N$ 的理想。为确定 $\mathrm{Tor}_j(C)$ ($0\le j\le t-1$)，我们先给出两个引理。

引理 1　设 $g(x)$ 为 x^n-1 在 $\overline{R}[x]$ 中的首一因式。则对于任意正整数 l，在 $\overline{R}_N$ 上有 $\left\langle g(x)^{l+p^s}\right\rangle=\left\langle g(x)^{p^s}\right\rangle$。

证明　设 $h(x)=(x^n-1)/g(x)$。因为 $g(x)$，$h(x)$ 在 $\overline{R}[x]$ 上互素，所以 $g(x)^l$ 与 $h(x)^{p^s}$ 在 $\overline{R}[x]$ 上互素。于是，存在 $\beta(x),\theta(x)\in\overline{R}[x]$，使得在 $\overline{R}[x]$ 上，$\beta(x)g(x)^l+\theta(x)h(x)^{p^s}=1$。所以在 $\overline{R}_N$ 上，有 $\beta(x)\cdot g(x)^{l+p^s}=\left[1-\theta(x)h(x)^{p^s}\right]g(x)^{p^s}=g(x)^{p^s}$。　证毕

对于任一 $0\le j\le t-1$，定义 $\left(C:a^j\right)=\left\{c\in R^N\left|a^jc\in C\right.\right\}$[9]。显然 $\mathrm{Tor}_j(C)=\overline{\left(C:a^j\right)}$。容易验证，$\left(C:a^j\right)$ 也是 R 上长度为 N 的 λ-常循环码。

引理 2 设 $C=\left\langle\prod_{i=1}^m f_i(x)^{k_i}\right\rangle$ 为 R 上长度为 N 的 λ-常循环码，$0\le k_i\le p^st$。设 j 为一整数且 $0\le j\le t-1$。则 $\left(C:a^j\right)$ 包含生成多项式为 $\prod_{i=1}^m f_i(x)^{l_i^{(j)}}$ 的 R 上长度为 N 的 λ-常循环码，其中 $l_i^{(j)}=k_i-\min\left\{p^sj,k_i\right\}$，$i=1,2,\cdots,m$。

证明 设 $D=\left\langle\prod_{i=1}^m f_i(x)^{l_i^{(j)}}\right\rangle$，其中 $l_i^{(j)}=k_i-\min\left\{p^sj,k_i\right\}$。对于任意 $f(x)\in D$，我们有存在某一 $g(x)\in R_N$ 使得 $f(x)=g(x)\prod_{i=1}^m f_i(x)^{l_i^{(j)}}$。根据文献[9]，有 $\left\langle\left(x^n-1\right)^{p^s}\right\rangle=\langle a\rangle\subseteq R_N$。所以存在可逆元 $\beta(x)\in R_N$ 使得 $\beta(x)\left(x^n-1\right)^{p^s}=a$。于是 $a^jf(x)=\beta(x)^j\cdot\left(x^n-1\right)^{p^sj}g(x)\prod_{i=1}^m f_i(x)^{l_i^{(j)}}=g(x)\beta(x)^j\prod_{i=1}^m f_i(x)^{\tau_i^{(j)}}$，其中 $\tau_i^{(j)}=p^sj+k_i-\min\left\{p^sj,k_i\right\}$。显然 $a^jf(x)\in C$，即 $f(x)\in\left(C:a^j\right)$。所以 $C\supseteq D$。

结合上面两个引理和定理 2，可以确定出 R 上长度为 N 的 λ-常循环码的挠码的结构。

定理 3 设 $C=\left\langle\prod_{i=1}^m f_i(x)^{k_i}\right\rangle$ 为 R 上长度为 N 的 λ-常循环码，$0\le k_i\le p^st$。设 j 为一整数且 $0\le j\le t-1$。则 $\mathrm{Tor}_j(C)$ 为 $\overline{R}$ 长度为 N 的生成多项式为 $\prod_{i=1}^m\overline{f}_i(x)^{\tau_i^{(j)}}$ 的循环码，其中 $\tau_i^{(j)}=\min\left\{p^s(j+1),k_i\right\}-\min\left\{p^sj,k_i\right\}$，$i=1,2,\cdots,m$。

证明 由引理 2，对于每一 $0\le j\le t-1$，有 $\mathrm{Tor}_j(C)\supseteq\left\langle\prod_{i=1}^m\overline{f}_i(x)^{l_i^{(j)}}\right\rangle$，其中 $l_i^{(j)}=k_i-\min\left\{p^sj,k_i\right\}$。设 $\overline{D}=\left\langle\prod_{i=1}^m\overline{f}_i(x)^{l_i^{(j)}}\right\rangle\subseteq\overline{R}_N$。根据引理 1，可得 $\overline{D}=\left\langle\prod_{i=1}^m\overline{f}_i(x)^{l_i^{(j)}}\right\rangle=\left\langle\prod_{i=1}^m\overline{f}_i(x)^{\tau_i^{(j)}}\right\rangle$，其中

$$\begin{aligned}\tau_i^{(j)}&=\min\left\{p^s,k_i-\min\left\{p^sj,k_i\right\}\right\}\\&=\min\left\{p^s(j+1),k_i\right\}-\min\left\{p^sj,k_i\right\}\end{aligned}$$

于是，$\left|\mathrm{Tor}_j(C)\right|\ge\left|\overline{R}\right|^{T_j}$，其中 $T_j=N-\sum_{i=1}^m\tau_i^{(j)}\deg\left(f_i(x)\right)$。所以

$$\begin{aligned}\prod_{j=0}^{t-1}\left|\mathrm{Tor}_j(C)\right|&\ge\left|\overline{R}\right|^{T_0+T_1+\cdots+T_{t-1}}\\&=\left|\overline{R}\right|^{tN-\sum_{i=1}^m\sum_{j=0}^{t-1}\tau_i^{(j)}\deg(f_i(x))}=\left|\overline{R}\right|^{tN-\sum_{i=1}^m k_i\deg(f_i(x))}\end{aligned}$$

根据定理 1 和定理 2，我们有 $|C|=\prod_{j=0}^{t-1}\left|\mathrm{Tor}_j(C)\right|=\left|\overline{R}\right|^{tN-\sum_{i=1}^m k_i\deg(f_i(x))}$。所以，对任一 $0\le j\le t-1$，$\left|\mathrm{Tor}_j(C)\right|=\left|\overline{D}\right|$。因此，$\mathrm{Tor}_j(C)=\overline{D}$。证毕

根据定理 3，有 $\mathrm{Tor}_{t-1}(C)=\left\langle\prod_{i=1}^m\overline{f}_i(x)^{\tau_i^{(t-1)}}\right\rangle$，其中 $\tau_i^{(t-1)}=k_i-\min\left\{p^s(t-1),k_i\right\}$。设 $C=\left\langle\prod_{i=1}^m f_i(x)^{k_i}\right\rangle$ 为 R 上长度为 N 的 λ-常循环码，$0\le k_i\le p^st$。对于每一 $0\le j\le t-1$，用 d_j 表示 $\mathrm{Tor}_j(C)$ 的汉明距离。显然，$d_0\ge d_1\ge\cdots\ge d_{t-1}$。根据文献[8]，$R$ 上长度为 N 的 λ-常循环码 C 的汉明距离为 $d_H(C)=d_{t-1}$。

例 1 在 $Z_{81}[x]$ 上，$x^{11}-1=f_1(x)f_2(x)f_3(x)$，其中 $f_1(x)=x-1$，$f_2(x)=x^5+66x^4-x^3+x^2+65x-1$，$f_3(x)=x^5+16x^4-x^3+x^2+15x-1$。一共有 $37^3=50653$ 个不同的 Z_{81} 上长度为 99 的 13-常循环码。每一常循环码具有的形式：$C=\langle f_1^{k_1}f_2^{k_2}f_3^{k_3}\rangle$，其中 $0\le k_1,k_2,k_3\le 36$。这样的常循环码比相同长度的 F_{81} 上的循环码在数目上多很多。然而每一这样的常循环码的汉明距离都是可计算的。取 $C_1=\left\langle f_1^{28}f_2^{36}f_3^{35}\right\rangle$，$C_2=\left\langle f_1^{31}f_2^3f_3^{30}\right\rangle$，则 $\mathrm{Tor}_3(C_1)=\langle\overline{f}_1\overline{f}_2^9\overline{f}_3^8\rangle$，$\mathrm{Tor}_3(C_2)=\langle\overline{f}_1^4\overline{f}_3^3\rangle$。利用 MAGMA，我们有 $d_H(C_1)=22$，$d_H(C_2)=3$。

下面我们研究 R 上长度为 N 的 λ-常循环码的齐次距离。我们先给出齐次距离一个界。

定理 4 设 $C=\left\langle\prod_{i=1}^m f_i(x)^{k_i}\right\rangle$ 为 R 上长度为 N 的 λ-常循环码，$0\le k_i\le p^st$。则

$$\begin{aligned}&p^{r(t-2)}\min\left\{\left(p^r-1\right)d_{t-2},p^rd_{t-1}\right\}\\&\le d_{\mathrm{hom}}(C)\le p^{r(t-1)}d_{t-1}\end{aligned}$$

证明 设 c 为 C 中的任意一个非零码字。存在 δ，$0\le\delta\le t-1$，使得 c 可表示为 $a^\delta b$，其中 $b\in R^N$ 的分量中至少有一个是单位。于是 $0\ne\overline{b}\in\mathrm{Tor}_\delta(C)$，$w_H(\overline{b})\ge d_\delta$。如果 $0\le\delta\le t-2$，那么 $w_{\mathrm{hom}}(c)\ge(p^r-1)p^{r(t-2)}d_\delta$。所以，$w_{\mathrm{hom}}(c)\ge(p^r-1)p^{r(t-2)}d_{t-2}$，从而 $d_{\mathrm{hom}}(C)\ge(p^r-1)p^{r(t-2)}d_{t-2}$。如果 $\delta=t-1$，那么我们有 $d_{\mathrm{hom}}(C)\ge p^{r(t-1)}d_{t-1}$。因此，$d_{\mathrm{hom}}(C)\ge p^{r(t-2)}\min\left\{\left(p^r-1\right)d_{t-2},p^rd_{t-1}\right\}$。另外，$d_{\mathrm{hom}}\left(a^{t-1}\mathrm{Tor}_{t-1}(C)\right)=p^{r(t-1)}d_{t-1}$ 且 $a^{t-1}\mathrm{Tor}_{t-1}(C)$ 是 C 的一个子码。所以，$d_{\mathrm{hom}}(C)\le p^{r(t-1)}d_{t-1}$。证毕

从定理 4 的证明中可知，定理的结论对于 R 上任意的线性码都是成立的。当 $d_{t-1}\le\left\lfloor\left(1-\frac{1}{p^r}\right)d_{t-2}\right\rfloor$

时，我们得到精确的齐次距离 $d_{\hom}(C)=p^{r(t-1)}d_{t-1}$。由定理 4 易得：

推论 1　设 $C=\left\langle\prod_{i=1}^{m}f_i(x)^{k_i}\right\rangle$ 为 R 上长度为 N 的 λ-常循环码，$0\le k_i\le p^st$。设 $\lambda=\max\limits_{1\le i\le m}\{k_i\}$。则下列结论成立：

(1) 如果 $1\le\lambda\le p^s(t-2)$，那么 $d_{\hom}(C)=(p^r-1)p^{r(t-2)}$。

(2) 如果 $p^s(t-2)+1\le\lambda\le p^s(t-1)$，那么 $d_{\hom}(C)=p^{r(t-1)}$。

对于 $\lambda=\max\limits_{1\le i\le m}\{k_i\}>p^s(t-1)$ 的情况，确定其精确的齐次距离是困难的。但是对于长度 $N=p^s$，利用挠码可以计算出所有的 R 上长度为 N 的 λ-常循环码的齐次距离。下面给出这个计算过程作为一个例子。文献[2]为下面例 2 的一个特殊情况。

例 2　设 $C_i=\left\langle(x-1)^i\right\rangle$ 为 R 上长度为 p^s 的 λ-常循环码，其中 $0\le i\le p^st$。我们有

(1)如果 $0\le i\le p^s(t-2)$，那么根据推论 1，$d_{\hom}(C_i)=(p^r-1)p^{r(t-2)}$。

(2)如果 $p^s(t-2)+1\le i\le p^s(t-1)$，那么根据推论 1，$d_{\hom}(C_i)=p^{r(t-1)}$。

(3) 如果 $p^s(t-1)+\beta p^{s-1}+1\le i\le p^s(t-1)+(\beta+1)p^{s-1}$，其中 $0\le\beta\le p-2$，那么根据定理 3，我们有 $\mathrm{Tor}_{t-1}(C_i)=\langle(x-1)^l\rangle$，其中 $\beta p^{s-1}+1\le l\le(\beta+1)p^{s-1}$，$0\le\beta\le p-2$；$\mathrm{Tor}_{t-2}(C_i)=\langle(x-1)^{p^s}\rangle=\langle 0\rangle$。由定理 4，$d_{\hom}(C_i)=p^{r(t-1)}d_{t-1}$。根据文献[12]，有 $d_{t-1}=\beta+2$。所以 $d_{\hom}(C_i)=(\beta+2)\cdot p^{r(t-1)}$。

(4) 如果 $p^st-p^{s-k}+(j-1)p^{s-k-1}+1\le i\le p^st-p^{s-k}+jp^{s-k-1}$，其中 $1\le j\le p-1$，$1\le k\le s-1$，那么，与上面(3)相似的讨论，我们有 $d_{\hom}(C_i)=(j+1)p^{r(t-1)+k}$。

(5)如果 $i=p^st$，那么有 $C_i=\{0\}$。

4　结束语

本文研究了有限链环上的一类常循环码的距离。根据这类常循环码的已知结构，通过计算其高阶挠码，对任一给定的这类常循环码，其汉明距离都可以利用本文方法计算。本文还探究了这类常循环码的齐次距离，得到了关于这类码的齐次距离的一个界，并得到了在某些特殊情况下这类码的精确的齐次距离。这给编译有限链环上此类常循环码提供了重要的理论依据。完全确定该类码在任意情况下的精确齐次距离是一个待研究的问题。

参 考 文 献

[1] HAMMONS A R Jr., KUMAR 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. doi: 10.1109/18.312154.

[2] 施敏加, 杨善林, 朱士信. 环 $F_2+uF_2+\cdots+u^{k-1}F_2$ 上长度为 2^s 的 $(1+u)$-常循环码的距离分布[J]. 电子与信息学报, 2010, 32(1): 112–116. doi: 10.3724/SP.J.1146.2008.01810.
SHI M J, YANG S L, and ZHU S X. The distributions of distances of $(1+u)$-constacyclic codes of length 2^s over $F_2+uF_2+\cdots+u^{k-1}F_2$ [J]. *Journal of Electronics & Information Technology*, 2010, 32(1): 112–116. doi: 10.3724/SP.J.1146.2008.01810.

[3] KONG B, ZHENG X Y, and MA H J. The depth spectrums of constacyclic codes over finite chain rings[J]. *Discrete Mathematics*, 2015, 338(2): 256–261. doi: 10.1016/j.disc.2014.09.013.

[4] QIAN K Y, ZHU S X, and KAI X S. On cyclic self-orthogonal codes over Z_{2^m} [J]. *Finite Fields and Their Applications*, 2015, 33: 53–65. doi: 10.1016/j.ffa.2014.11.005.

[5] DINH H Q, DHOMPONGSA S, and SRIBOONCHITTA S. Repeated-root constacyclic codes of prime power length over $F_{p^m}[u]\big/\langle u^a\rangle$ and their duals[J]. *Discrete Mathematics*, 2016, 339(6): 1706–1715. doi: 10.1016/j.disc.2016.01.020.

[6] WOLFMANN J. Negacyclic and cyclic codes over Z_4 [J]. *IEEE Transactions on Information Theory*, 1999, 45(7): 2527–2532. doi: 10.1109/18.796397.

[7] NORTON G H and SĂLĂGAN A. On the structure of linear and cyclic codes over a finite chain ring[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2000, 10(6): 489–506. doi: 10.1007/PL00012382.

[8] NORTON G H and SĂLĂGAN A. On the Hamming distance of linear codes over a finite chain ring[J]. *IEEE Transactions on Information Theory*, 2000, 46(3): 1060–1067. doi: 10.1109/18.841186.

[9] GREFERATH M and SCHMIDT S E. Gray isometries for finite chain rings and a nonlinear ternary $(36,3^{12},15)$ code[J]. *IEEE Transactions on Information Theory*, 1999, 45(7): 2522–2524. doi: 10.1109/18.796395.

[10] CAO Y L. On constacyclic codes over finite chain rings[J]. *Finite Fields and Their Applications*, 2013, 24: 124–135. doi: 10.1016/j.ffa.2013.07.001.

[11] MCDONALD B R. Finite Rings with Identity[M]. New York, Marcel Dekker Press, 1974: 56–97.

[12] DINH H Q. Constacyclic codes of length p^s over $F_{p^m}+uF_{p^m}$ [J]. *Journal of Algebra*, 2010, 324(5): 940–950. doi: 10.1016/j.jalgebra.2010.05.027.

袁　健：　男，1988 年生，博士生，研究方向为代数编码.

朱士信：　男，1962 年生，教授，博士生导师，研究方向为代数编码理论、信息安全与序列密码等.

开晓山：　男，1975 年生，副教授，研究方向为编码理论与信息安全等.