环 $F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$ 上 $(1+u)$-常循环码的齐次距离分布

朱士信　　黄素娟*
(合肥工业大学数学学院　合肥　230009)

摘　要：该文研究了环 $R_k=F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$ 上任意长的 $(1+u)$ -常循环码的齐次距离分布。首先，介绍了环 R_k 上给定长度的 $(1+u)$ -常循环码的挠码。然后利用挠码得到环 R_k 上任意长度的 $(1+u)$ -常循环码的齐次距离的界，并给出了 R_k 上某些 $(1+u)$ -常循环码的齐次距离的准确值。

关键词：常循环码；挠码；齐次距离
中图分类号：TN911.22　　**文献标识码**：A　　**文章编号**：1009-5896(2013)11-2579-05
DOI: 10.3724/SP.J.1146.2013.00274

The Distribution of Homogeneous Distance of $(1+u)$-constacyclic Codes over $F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$

Zhu Shi-xin　　Huang Su-juan
(*School of Mathematics*, *Hefei University of Technology*, *Hefei* 230009, *China*)

Abstract: In this paper, the distribution of homogeneous distance of $(1+u)$ -constacyclic codes over the ring $R_k=F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$ of arbitrary lengths is studied. Firstly, the torsion codes of a $(1+u)$ -constacyclic code over R_k for a given length are introduced. Then, by using the torsion codes, a bound for the homogeneous distance of $(1+u)$ -constacyclic codes over R_k of any length is given. The exact homogeneous distance of some $(1+u)$ -constacyclic codes over R_k is also obtained.

Key words: Constacyclic codes; Torsion codes; Homogeneous distance

1　引言

常循环码具有丰富的代数结构，其性能易于分析；在实践中，常循环码的编译码电路，特别是编码电路也易于实现。因此，无论从理论上还是从实践上常循环码都是一类非常重要的纠错码。码的距离是衡量码好坏的一个重要参数，其与码的纠错能力息息相关，因此研究码的距离分布是非常有意义的。Dinh[1]研究了环 $GR(2^a,m)$ 上长为 2^s 的负循环码的 Hamming 距离，并给出了 Z_{2^a} 上长为 4,8,16 的所有负循环码的 Hamming 距离。随后他在文献[2]中研究了环 Z_{2^a} 上长为 2^s 的负循环码的 Hamming 距离，Lee 距离，Homogeneous 距离及 Euclid 距离分布。文献[3,4]分别研究了环 $GR(2^a,m)$ 上的线性码和负循环码的距离分布。文献[5]研究了环 Z_4 上长度为 2^e 的循环码的 Hamming 距离及 Lee 距离。彭培让等人[6]研究了环 Z_4 上一些长为 2^e 的循环码的 Homogeneous 距离。邓林等人[7]确定了环 F_2+uF_2 上长为 2^s 的 $(1+u)$ -常循环码的 Hamming 距离，Lee 距离及 Euclid 距离分布。施敏加等人[8]将文献[7]的结论推广到环 $F_2+uF_2+\cdots+u^{k-1}F_2$，得到了该环上长度为 2^s 的 $(1+u)$ -常循环码的 Hamming 距离及 Homogeneous 距离分布。随后他们又研究了环 F_2+uF_2 上长度为 2^e 的循环码的 Hamming 距离及 Lee 距离分布[9]。最近，文献[10]给出了环 $GR(2^a,m)$ 上任意长度负循环码的 Homogeneous 距离的一个界。文献[11]中给出了 $F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$ 上长为 p^s 的 $(1+\lambda u)$ 常循环码的 Hamming 距离和 Homogeneous 距离。

本文将文献[8,11]的结论加以推广，研究了环 R_k 上任意长度 $(1+u)$ -常循环码的 Homogeneous 距离分布。我们首先给出了该环上任意长度 $(1+u)$ -常循环码的挠码的定义及结构，然后利用挠码的结构确定了环 R_k 上该常循环码的 Homogeneous 距离分布。

2　基本概念

令 $R_k=F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$ (其中 $u^k=0$)，则 R_k 是极大理想为 $\langle u\rangle$ 的局部环，其剩余域为 F_{p^m}。对于 R_k 中任意的元素，都可以唯一地表示成

$$r=r_0+ur_1+u^2r_2+\cdots+u^{k-1}r_{k-1}$$

其中 $r_i\in F_{p^m}$，$0\le i\le k-1$。

定义 $R_k[x]$ 是系数在 R_k 中的多项式环，对于 $R_k[x]$ 中的多项式 $f(x)$，若 $f(x)$ 模 u 约化 $\overline{f}(x)$ 在 $F_{p^m}[x]$ 中不可约，则称 $f(x)$ 是 $R_k[x]$ 中的基本不可约多项式。

2013-03-07 收到，2013-06-13 改回
*通信作者：黄素娟　huangsujuan1019@163.com

对于任意的多项式 $f_1(x),f_2(x)\in R_k[x]$，若存在 $k_1(x),k_2(x)\in R_k[x]$，使得

$$k_1(x)f_1(x)+k_2(x)f_2(x)=1$$

则称 $f_1(x)$ 与 $f_2(x)$ 在 $R_k[x]$ 中互素。

引理 1[12] 设 $f_1(x),f_2(x)\in R_k[x]$，则 $f_1(x)$ 与 $f_2(x)$ 在 $R_k[x]$ 中互素当且仅当 $\overline{f}_1(x)$ 与 $\overline{f}_2(x)$ 在 $F_{p^m}[x]$ 中互素。

环 R_k 上长为 N 的码是 R_k^N 的非空子集，设 C 是环 R_k 上长为 N 的码，若 C 是 R_k^N 的 R_k-子模，则称 C 是环 R_k 上的线性码。

对于环 R_k 上长为 N 的线性码 C，任取 C 中的码字 $c=(c_0,c_1,\cdots,c_{N-1})$，若在置换

$$(c_0,c_1,\cdots,c_{N-1})\to((1+u)c_{N-1},c_0,\cdots,c_{N-2})$$

下得到的码字仍属于 C，则称 C 是环 R_k 上长为 N 的 $(1+u)$-常循环码。

我们将码字 $c=(c_0,c_1,\cdots,c_{N-1})$ 等同于它的多项式表示 $c(x)=c_0+c_1x+\cdots+c_{N-1}x^{N-1}$，则 $xc(x)$ 对应于 $c(x)$ 在环 $R_k[x]/\langle x^N-(1+u)\rangle$ 中的 $(1+u)$-常循环移位。因此，环 R_k 上长为 N 的 $(1+u)$-常循环码等价于环 $R_k[x]/\langle x^N-(1+u)\rangle$ 中的理想。

令 $N=p^sn$，其中 $(n,p)=1$，s 是非负整数。定义：$T_k(s,n,u)=R_k[x]/\langle x^N-(1+u)\rangle$。特别地，当 $k=1$ 时，$T_1(s,n,u)=F_{p^m}[x]/\langle x^N-1\rangle$，即长为 $N=p^sn$ 的循环码是 $T_1(s,n,u)$ 的理想。

设 I 是模 n 的 p^m-分圆陪集的代表元组成的集合。将文献[12]的定理 7.4 作自然推广有如下结论：

定理 1 设 $x^n-1=\prod_{i\in I}f_i(x)$ 是 x^n-1 在 $R_k[x]$ 中的唯一因式分解，其中 $f_i(x)$ 是 $R_k[x]$ 中的首一基本不可约多项式，且两两互素。则环 $T_k(s,n,u)$ 是主理想环，其理想是 $\left\langle\prod_{i\in I}f_i(x)^{s_i}\right\rangle$，$0\le s_i\le p^sk$。等价地，环 R_k 上长为 N 的 $(1+u)$-常循环码为 $C=\left\langle\prod_{i\in I}f_i(x)^{s_i}\right\rangle$，$0\le s_i\le p^sk$，且 $|C|=p^{m\left(kN-\sum_{i\in I}s_i\deg(f_i)\right)}$。

环 R_k 上的齐次重量函数的定义如下：

$$w_{\mathrm{hom}}(r)=\begin{cases}p^{m(k-1)}, & r\in u^{k-1}R_k\backslash\{0\}\\ p^{m(k-2)}(p^m-1), & r\in R_k\backslash u^{k-1}R_k\\ 0, & r=0\end{cases}$$

$c=(c_0,c_1,\cdots,c_{N-1})$ 在环 R_k 上的齐次重量是 c 的分量的齐次重量的有理和。线性码 C 的齐次距离 $d_{\mathrm{hom}}(C)$ 等于 C 的非零码字的最小齐次重量。

3 挠码

设 C 是环 $R_k=F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$ 上长为 $N=p^sn$ 的码，其中 $(n,p)=1$，定义 $\overline{C}=\{\overline{c}|c\in C\}$。对任意的 η，$0\le\eta\le k-1$，我们定义码：

$$(C:u^\eta)=\{c\in R_k^N\mid u^\eta c\in C\}$$

对于环 R_k 上长为 N 的线性码 C，易证 $(C:u^i)\subseteq(C:u^{i+1})$ 且 $\overline{(C:u^i)}\subseteq\overline{(C:u^{i+1})}$，对 $0\le i\le k-2$ 成立。通常称 $\overline{C}=\overline{(C:u^0)}$ 为剩余码，记为 $\mathrm{Res}(C)$。若 C 是环 R_k 上的 $(1+u)$-常循环码，则容易验证 $(C:u^\eta)$ 是环 R_k 上的 $(1+u)$-常循环码，$\overline{(C:u^\eta)}$ 是 F_{p^m} 上的循环码。码 $(C:u^\eta)$ 称为 C 的 η 次挠码。

下面的定理类似于文献[13]中的定理 1：

定理 2 设 C 是环 R_k 上的线性码，则有 $|C|=\prod_{\eta=0}^{k-1}|\overline{(C:u^\eta)}|$。

引理 2 在 $T_k(s,n,u)$ 中，有 $\langle(x^n-1)^{p^s}\rangle=\langle u\rangle$。

证明 $(x^n-1)^{p^s}=x^{n\cdot p^s}-1=(1+u)-1=u$，故 $\langle(x^n-1)^{p^s}\rangle=\langle u\rangle$。 证毕

引理 3 设 $f(x)$ 是 x^n-1 在 $F_{p^m}[x]$ 中的因式，则在 $T_1(s,n,u)$ 中，$\langle f(x)^{p^s+l}\rangle=\langle f(x)^{p^s}\rangle$，$l$ 是任意的正整数。

证明 令 $g(x)=(x^n-1)/f(x)$，由于 $f(x)$ 与 $g(x)$ 在 $F_{p^m}[x]$ 中互素，则 $f(x)^l$ 与 $g(x)^{p^s}$ 在 $F_{p^m}[x]$ 中互素，l 为任意的正整数。因此，存在 $\varphi(x),\psi(x)\in F_{p^m}[x]$，使得

$$\varphi(x)f(x)^l+\psi(x)g(x)^{p^s}=1$$

则在 $T_1(s,n,u)$ 中，有

$$\begin{aligned}\varphi(x)f(x)^{p^s+l}&=[1-\psi(x)g(x)^{p^s}]\cdot f(x)^{p^s}\\&=f(x)^{p^s}-\psi(x)(x^n-1)^{p^s}\\&=f(x)^{p^s}\end{aligned}$$

所以，$\langle f(x)^{p^s+l}\rangle=\langle f(x)^{p^s}\rangle$，$l$ 为任意的正整数。 证毕

引理 4 设 C 是环 R_k 上长为 $N=p^sn$ 的 $(1+u)$-常循环码，其生成多项式是 $\prod_{i\in I}f_i(x)^{s_i}$，其中 $f_i(x)$ $(i\in I)$ 是 x^n-1 在 $R_k[x]$ 中的首一基本不可约多项式，$0\le s_i\le p^sk$。设 η 是满足 $0\le\eta\le k-1$ 的整数，则 $(C:u^\eta)$ 包含环 R_k 上长为 $N=p^sn$ 的 $(1+u)$-常循环码 $\left\langle\prod_{i\in I}f_i(x)^{\theta_i^{(\eta)}}\right\rangle$，其中 $\theta_i^{(\eta)}=s_i-\min\{p^s\eta,s_i\}$。

证明 设 $D=\left\langle\prod_{i\in I}f_i(x)^{\theta_i^{(\eta)}}\right\rangle\subseteq T_k(s,n,u)$，其中 $\theta_i^{(\eta)}=s_i-\min\{p^s\eta,s_i\}$。对于任意的 $f(x)\in D$，有

$f(x)=g(x)\cdot\prod_{i\in I}f_i(x)^{\theta_i^{(\eta)}}$，$g(x)\in T_k(s,n,u)$。由引理 2 知，存在可逆元 $\beta(x)\in T_k(s,n,u)$，使得 $\beta(x)\cdot(x^n-1)^{p^s}=u$。因此，

$$\begin{aligned}u^\eta f(x)&=u^\eta g(x)\prod_{i\in I}f_i(x)^{\theta_i^{(\eta)}}\\&=\beta(x)^\eta(x^n-1)^{p^s\eta}g(x)\prod_{i\in I}f_i(x)^{\theta_i^{(\eta)}}\\&=g(x)\beta(x)^\eta\prod_{i\in I}f_i(x)^{\tau_i^{(\eta)}}\end{aligned}$$

其中 $\tau_i^{(\eta)}=p^s\eta+s_i-\min\{p^s\eta,s_i\}$。则 $u^\eta f(x)\in C$，所以 $f(x)\in(C:u^\eta)$，从而 $D\subseteq(C:u^\eta)$。　　证毕

定理 3　设 C 是环 R_k 上长为 $N=p^sn$ 的 $(1+u)$-常循环码，其生成多项式是 $\prod_{i\in I}f_i(x)^{s_i}$，其中 $f_i(x)(i\in I)$ 是 x^n-1 在 $R_k[x]$ 中的首一基本不可约多项式，$0\le s_i\le p^sk$。设 η 是满足 $0\le\eta\le k-1$ 的整数，则 $\overline{(C:u^\eta)}$ 是 F_{p^m} 上长为 $N=p^sn$ 的循环码，其生成多项式为 $\prod_{i\in I}\bar{f}_i(x)^{\tau_i^{(\eta)}}$，其中 $\tau_i^{(\eta)}=\min\{p^s(\eta+1),s_i\}-\min\{p^s\eta,s_i\}$。

证明　根据引理 4，对于任意的 η，$0\le\eta\le k-1$，有 $\overline{(C:u^\eta)}\supseteq\left\langle\prod_{i\in I}\bar{f}_i(x)^{\theta_i^{(\eta)}}\right\rangle$，其中 $\theta_i^{(\eta)}=s_i-\min\{p^s\eta,s_i\}$。设 $\bar{D}=\left\langle\prod_{i\in I}\bar{f}_i(x)^{\theta_i^{(\eta)}}\right\rangle\subseteq T_1(s,n,u)$，根据引理 3，我们得到

$$\bar{D}=\left\langle\prod_{i\in I}\bar{f}_i(x)^{\theta_i^{(\eta)}}\right\rangle=\left\langle\prod_{i\in I}\bar{f}_i(x)^{\tau_i^{(\eta)}}\right\rangle$$

其中

$$\begin{aligned}\tau_i^{(\eta)}&=\min\{p^s,s_i-\min\{p^s\eta,s_i\}\}\\&=\min\{p^s(\eta+1),s_i\}-\min\{p^s\eta,s_i\}\end{aligned}$$

从而得到 $|\overline{(C:u^\eta)}|\ge p^{t_\eta}$，其中

$$t_\eta=m\left(N-\sum_{i\in I}\tau_i^{(\eta)}\cdot\deg(f_i)\right)$$

所以

$$\begin{aligned}\prod_{\eta=0}^{k-1}|\overline{(C:u^\eta)}|&\ge p^{t_0+t_1+\cdots+t_{k-1}}\\&=p^{m\left(kN-\sum_{i\in I}\sum_{\eta=0}^{k-1}\tau_i^{(\eta)}\deg(f_i)\right)}\\&=p^{m\left(kN-\sum_{i\in I}s_i\deg(f_i)\right)}\end{aligned}$$

由定理 2，我们得到

$$|C|=\prod_{\eta=0}^{k-1}|\overline{(C:u^\eta)}|=p^{m\left(kN-\sum_{i\in I}s_i\deg(f_i)\right)}$$

因此，对任意的 η，$0\le\eta\le k-1$，必有 $|\overline{(C:u^\eta)}|=|\bar{D}|$，从而 $\overline{(C:u^\eta)}=\bar{D}$，即结论成立。　　证毕

根据定理 3，我们有 $\mathrm{Res}(C)=\left\langle\prod_{i\in I}\bar{f}_i(x)^{\tau_i^{(0)}}\right\rangle$，其中 $\tau_i^{(0)}=\min\{p^s,s_i\}$，$\overline{(C:u^{k-1})}=\left\langle\prod_{i\in I}\bar{f}_i(x)^{\tau_i^{(k-1)}}\right\rangle$，$\tau_i^{(k-1)}=s_i-\min\{p^s(k-1),s_i\}$。

4　齐次距离

设 $C=\left\langle\prod_{i\in I}f_i(x)^{s_i}\right\rangle$ 是环 R_k 上长为 $N=p^sn$ 的 $(1+u)$-常循环码，其中 $(n,p)=1$，$f_i(x)(i\in I)$ 是 x^n-1 在 $R_k[x]$ 中的首一基本不可约多项式，$0\le s_i\le p^sk$。对于任意的 η，$0\le\eta\le k-1$，设 d_η 为循环码 $\overline{(C:u^\eta)}=\left\langle\prod_{i\in I}\bar{f}_i(x)^{\tau_i^{(\eta)}}\right\rangle$ 的 Hamming 距离，其中 $\tau_i^{(\eta)}=\min\{p^s(\eta+1),s_i\}-\min\{p^s\eta,s_i\}$，显然，$d_0\ge d_1\ge\cdots\ge d_{k-1}$。

我们首先考虑环 R_k 上长为 $N=p^sn$ 的 $(1+u)$-常循环码的 Hamming 距离，且该距离完全由循环码 $\overline{(C:u^{k-1})}$ 确定。

定理 4　设 C 是环 R_k 上长为 $N=p^sn$ 的 $(1+u)$-常循环码，其生成多项式是 $\prod_{i\in I}f_i(x)^{s_i}$，其中 $f_i(x)(i\in I)$ 是 x^n-1 在 $R_k[x]$ 中的首一基本不可约多项式，$0\le s_i\le p^sk$，则 $d_H(C)=d_{k-1}$。

证明　由文献[14]的定理 4.2 和定理 3 即可得。

定理 5　设 C 是环 R_k 上长为 $N=p^sn$ 的 $(1+u)$-常循环码，其生成多项式是 $\prod_{i\in I}f_i(x)^{s_i}$，其中 $f_i(x)(i\in I)$ 是 x^n-1 在 $R_k[x]$ 中的首一基本不可约多项式，$0\le s_i\le p^sk$。则

$$\begin{aligned}&p^{m(k-2)}\min\{(p^m-1)d_{k-2},\,p^md_{k-1}\}\\&\le d_{\mathrm{hom}}(C)\le p^{m(k-1)}d_{k-1}\end{aligned}$$

证明　设 c 是 C 中的任意非零码字，则存在 r，$0\le r\le k-1$，使得 c 可以表示成如下形式：$c=u^rv$，其中 $v\in R_k^N$ 不能被 u 整除。则有 $0\ne\bar{v}\in\overline{(C:u^r)}$，从而 $w_H(\bar{v})\ge d_r$。

若 $0\le r\le k-2$，则 $w_{\mathrm{hom}}(c)\ge p^{m(k-2)}(p^m-1)d_r$，因为 $d_0\ge d_1\ge\cdots\ge d_{k-2}$，所以有 $w_{\mathrm{hom}}(c)\ge p^{m(k-2)}\cdot(p^m-1)d_{k-2}$，则 $d_{\mathrm{hom}}(C)\ge p^{m(k-2)}(p^m-1)d_{k-2}$。

若 $r=k-1$，则 $d_{\hom}(C)\geq p^{m(k-1)}d_{k-1}$。因此

$$d_{\hom}(C)\geq \min\{p^{m(k-2)}(p^m-1)d_{k-2},p^{m(k-1)}d_{k-1}\}$$
$$=p^{m(k-2)}\min\{(p^m-1)d_{k-2},p^m d_{k-1}\}$$

另一方面，注意到 $u^{k-1}\overline{v}=u^{k-1}v\in C$，则 $d_{\hom}(C)\leq p^{m(k-1)}d_{k-1}$。

综上可得，

$$p^{m(k-2)}\min\{(p^m-1)d_{k-2},\ p^m d_{k-1}\}\leq d_{\hom}(C)\leq p^{m(k-1)}d_{k-1}$$

证毕

推论 1 设 C 是环 R_k 上长为 $N=p^s n$ 的 $(1+u)$-常循环码，其生成多项式是 $\prod_{i\in I}f_i(x)^{s_i}$，其中 $f_i(x)$ $(i\in I)$ 是 x^n-1 在 $R_k[x]$ 中的首一基本不可约多项式，$0\leq s_i\leq p^s k$。若 $(p^m-1)d_{k-2}\geq p^m d_{k-1}$，则 $d_{\hom}(C)=p^{m(k-1)}d_{k-1}$。

推论 2 设 C 是环 R_k 上长为 $N=p^s n$ 的 $(1+u)$-常循环码，其生成多项式是 $\prod_{i\in I}f_i(x)^{s_i}$，其中 $f_i(x)(i\in I)$ 是 x^n-1 在 $R_k[x]$ 中的首一基本不可约多项式，$0\leq s_i\leq p^s k$。令 $\sigma=\max_{i\in I}\{s_i\}$，则

(1) 若 $1\leq\sigma\leq p^s(k-2)$，则 $d_{\hom}(C)=p^{m(k-2)}\cdot(p^m-1)$。

(2) 若 $p^s(k-2)+1\leq\sigma\leq p^s(k-1)$，则 $d_{\hom}(C)=p^{m(k-1)}$。

证明 (1)若 $1\leq\sigma\leq p^s(k-2)$，则 $\overline{(C:u^{k-2})}=\overline{(C:u^{k-1})}=\langle 1\rangle$。于是由定理 5 可得

$$p^{m(k-2)}(p^m-1)\leq d_{\hom}(C)\leq p^{m(k-1)}$$

又 $\prod_{i\in I}f_i(x)^{p^s(k-2)}=(x^n-1)^{p^s(k-2)}=u^{k-2}\in C$，则

$$d_{\hom}(C)\leq p^{m(k-2)}(p^m-1)$$

从而

$$d_{\hom}(C)=p^{m(k-2)}(p^m-1)$$

(2)若 $p^s(k-2)+1\leq\sigma\leq p^s(k-1)$，则 $\overline{(C:u^{k-2})}\neq\langle 0\rangle$ 或 $\langle 1\rangle$，$\overline{(C:u^{k-1})}=\langle 1\rangle$，于是，$(p^m-1)d_{k-2}\geq p^m d_{k-1}$。因此，$d_{\hom}(C)=p^{m(k-1)}$。 证毕

利用挠码，我们可以得到环 R_k 上长为 $N=p^s n$ 的某些 $(1+u)$-常循环码齐次距离。然而，当 $\sigma=\max_{i\in I}\{s_i\}>p^s(k-1)$ 时，很难准确地确定环 R_k 上长为 $N=p^s n$ 的 $(1+u)$-常循环码的齐次距离。所以，环 R_k 上很多长为 $N=p^s n$ 的 $(1+u)$-常循环码的齐次距离的准确值无法确定。

设 $C_0=\langle\overline{f}(x)\rangle$ 是长为 n 的单根循环码，我们现在利用 C_0 来给出一个上界。

设 C 是环 R_k 上长为 $N=p^s n$ 的 $(1+u)$-常循环码，其生成多项式是 $g(x)=\prod_{i\in I}f_i(x)^{s_i}$，其中 $f_i(x)(i\in I)$ 是 x^n-1 在 $R_k[x]$ 中的首一基本不可约多项式，$0\leq s_i\leq p^s k$。定义 $f(x)$ 是 $g(x)$ 中重数 $s_i>p^s(k-1)$ 的那些基本不可约因式 $f_i(x)$ 的乘积。

引理 5 设 $C_1=\langle\overline{f}(x)^{p^s}\rangle$ 是长为 $N=p^s n$ 的循环码，$C_2=\langle\overline{f}(x)\rangle$ 是长为 n 的循环码，则 $d_H(C_1)=d_H(C_2)$。

证明 根据文献[15]中的定理 1 可得。

推论 3 设 C 是环 R_k 上长为 $N=p^s n$ 的 $(1+u)$-常循环码，其生成多项式是 $g(x)=\prod_{i\in I}f_i(x)^{s_i}$，令 $C_0=\langle\overline{f}(x)\rangle$，$d$ 是 C_0 的 Hamming 距离。$\sigma=\max_{i\in I}\{s_i\}>p^s(k-1)$，$me$ 是 $\sigma-p^s(k-1)$ 的 p-adic 展开的非零系数的个数，则

(1)若 $\sigma=p^s k$，则 $d_{\hom}(C)\leq p^{m(k-1)}d$。

(2)若 $p^s(k-1)<\sigma<p^s k$，则

$$d_{\hom}(C)\leq\min\{p^{m(k+e-1)},\ p^{m(k-1)}d\}$$

证明 (1)由于 $f(x)$ 是 $g(x)$ 中重数 $s_i>p^s(k-1)$ 的那些基本不可约因式 $f_i(x)$ 的乘积，所以 $\overline{(C:u^{k-1})}\supseteq\langle\overline{f}(x)^{p^s}\rangle$，从而 $d_{k-1}\leq d_H(\langle\overline{f}(x)^{p^s}\rangle)$。根据引理 5 有

$$d_H(\langle\overline{f}(x)^{p^s}\rangle)=d_H(\langle\overline{f}(x)\rangle)=d_H(C_0)=d$$

所以，$d_{\hom}(C)\leq p^{m(k-1)}d_{k-1}\leq p^{m(k-1)}d$。

(2)若 $p^s(k-1)<\sigma<p^s k$，则

$$\prod_{i\in I}f_i(x)^{\sigma}=(x^n-1)^{\sigma}=(x^n-1)^{p^s(k-1)}\cdot(x^n-1)^{\sigma-p^s(k-1)}=u^{k-1}\cdot(x^n-1)^{\sigma-p^s(k-1)}\in C$$

所以，$(x^n-1)^{\sigma-p^s(k-1)}\in(C:u^{k-1})$，从而 $d_{\hom}(C)\leq p^{m(k-1)}d_{k-1}\leq p^{m(k+e-1)}$。再由 (1) 知 $d_{\hom}(C)\leq p^{m(k-1)}d$，所以 $d_{\hom}(C)\leq\min\{p^{m(k+e-1)},\ p^{m(k-1)}d\}$。

证毕

例 1 当 $p=2$ 时，设 $C_i=\langle(x+1)^i\rangle$ 是 R_k 上长为 2^s 的 $(1+u)$-常循环码，其中 $i\in\{0,1,\cdots,2^s k\}$。则根据推论 2，我们可以得到：

(1) 若 $0\leq i\leq 2^s(k-2)$，则 $d_{\hom}(C_i)=2^{m(k-2)}\cdot(2^m-1)$；

(2) 若 $2^s(k-2)+1\leq i\leq 2^s(k-1)$，则 $d_{\hom}(C_i)=2^{m(k-1)}$；

(3) 若 $2^s k-2^{s-t}+1\leq i\leq 2^s k-2^{s-t-1}$，$0\leq t\leq s-1$，则 $\overline{(C:u^{k-1})}=\langle(x+1)^j\rangle$，其中 $2^s-2^{s-t}+1\leq j\leq 2^s-2^{s-t-1}$，且 $\overline{(C:u^{k-2})}=\langle 0\rangle$。于是根据推论 1，有 $d_{\hom}(C_i)=2^{m(k-1)}d_{k-1}=2^{m(k-1)+t+1}$。

(4)若 $i=2^s k$，则 $d_{\hom}(C_i)=0$。特别地，当 $m=1$ 时与文献[8]定理 3 的结论相符合。

例 2　设 $C_i=\langle (x-1)^i\rangle$ 是 R_k 上长为 p^s 的 $(1+u)$-常循环码，其中 $i\in\{0,1,\cdots,p^s k\}$。则根据推论 2，我们可以得到：

(1) 若 $0\le i\le p^s(k-2)$，则 $d_{\hom}(C_i)=p^{m(k-2)}\cdot(p^m-1)$；

(2)若 $p^s(k-2)+1\le i\le p^s(k-1)$，则 $d_{\hom}(C_i)=p^{m(k-1)}$；

(3)若 $p^s k-p^{s-t}+1\le i\le p^s k-p^{s-t-1}$，$0\le t\le s-1$，则 $\overline{(C{:}u^{k-1})}=\langle (x-1)^j\rangle$，其中 $p^s-p^{s-t}+1\le j\le p^s-p^{s-t-1}$，且 $\overline{(C{:}u^{k-2})}=\langle 0\rangle$。于是根据推论 1，有

$$d_{\hom}(C_i)=p^{m(k-1)}d_{k-1}=\begin{cases}(\alpha+2)p^{m(k-1)}, & p^s(k-1)+\alpha p^{s-1}+1\le i\le p^s(k-1)+(\alpha+1)p^{s-1},\ 0\le\alpha\le p-2\\ (\beta+1)p^{l+m(k-1)}, & p^s k-p^{s-l}+(\beta-1)p^{s-l-1}+1\le i\le p^s k-p^{s-l}+\beta p^{s-l-1},\ 1\le\beta\le p-1,\ 1\le l\le s-1\end{cases}$$

(4)若 $i=p^s k$，则 $d_{\hom}(C_i)=0$。与文献[11]定理 4.1 的结论相符合。

5　结束语

本文研究了环 R_k 上任意长度 $(1+u)$-常循环码的齐次距离分布，为更好了解该常循环码提供了理论根据。环 R_k 上其它类型常循环码的各种距离分布是一个值得进一步研究的问题。

参 考 文 献

[1] Dinh H Q. Negacyclic codes of length 2^s over Galois rings[J]. *IEEE Transactions on Information Theory*, 2005, 51(4): 4252–4262.

[2] Dinh H Q. Complete distance of all negacyclic codes of length 2^s over Z_{2^a} [J]. *IEEE Transactions on Information Theory*, 2007, 53(1): 147–161.

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

[4] Zhu S X and Kai X S. The Hamming distances of negacyclic codes of length 2^s over $\mathrm{GR}(2^a,m)$ [J]. *Journal of System Science and Complexity*, 2008, 21(1): 60–66.

[5] Kai X S and Zhu S X. On the distances of cyclic codes of length 2^s over Z_4 [J]. *Discrete Mathematics*, 2010, 310(1): 12–20.

[6] 彭培让, 郑喜英, 孔波. 环 Z_4 上长为 2^s 的循环码的齐次距离[J]. 河南大学学报(自然科学版), 2012, 42(2): 121–124.
Peng P R, Zheng X Y, and Kong B. Homogeneous distance of cyclic codes of length 2^s on ring Z_4 [J]. *Journal of Henan University (Natural Science)*, 2012, 42(2): 121–124.

[7] 邓林, 朱士信, 韩江洪. 环 F_2+uF_2 上长为 2^s 的 $(1+u)$-常循环码的距离分布[J]. 中国科技大学学报, 2008, 38(10): 1810–1814.
Deng L, Zhu S X, and Han J H. The distribution of distances of $(1+u)$-constacyclic codes of length 2^s over F_2+uF_2 [J]. *Journal of University of Science and Technology of China*, 2008, 38(10): 1810–1814.

[8] 施敏加, 杨善林, 朱士信. 环 $F_2+uF_2+\cdots+u^{k-1}F_2$ 上长为 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.
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.

[9] 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 M J, Yang S L, and Zhu S X. On minimum distances of cyclic codes of length 2^s over F_2+uF_2 [J]. *Acta Electronic Sinica*, 2011, 39(1): 29–34.

[10] Zhu S X and Kai X S. Negacyclic codes over Galois rings of characteristic 2^a [J]. *Science China Mathematics*, 2012, 55(4): 869–879.

[11] 刘晓娟, 朱士信. 环 $F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$ 上的长为 p^s 的 $(1+\lambda u)$ 常循环码的距离分布[J]. 中国科学技术大学学报, 2012, 42(11): 931–935.
Liu X J and Zhu S X. The distributions of distances of $(1+\lambda u)$-constacyclic codes of length p^s over $F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$ [J]. *Journal of University of Science and Technology of China*, 2012, 42(11): 931–935.

[12] Dinh H Q and Nguyen H D. On some classes of constacyclic codes over polynomial residue rings[J]. *Mathematics of Communications*, 2012, 6(2): 175–191.

[13] Han M, Ye Y P, Zhu S X, *et al*.. Cyclic codes over $R=F_p+uF_p+\cdots+u^{k-1}F_p$ with length $p^s n$ [J]. *Information Science*, 2011, 181(4): 926–934.

[14] Sălăgean A. Repeated-root cyclic and negacyclic codes over a finite chain ring[J]. *Discrete Applied Mathematics*, 2005, 154(2): 413–419.

[15] Castagnoli G, Massey J L, Schoeller P A, *et al*.. On repeated-root cyclic codes[J]. *IEEE Transactions on Information Theory*, 1991, 37(2): 337–342.

朱士信：　男，1962 年生，教授，博士生导师，研究方向为代数编码、信息安全、非线性移位寄存器序列.

黄素娟：　女，1989 年生，硕士生，研究方向为代数编码与密码.