# 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

施敏加[①②]　杨善林[②]　朱士信[②]
[①](安徽大学数学科学学院　合肥　230039)
[②](合肥工业大学计算机网络系统研究所　合肥　230009)

**摘　要**：研究码字的距离分布是编码理论的一个重要研究方向。该文定义了环 $R=F_2+uF_2+\cdots+u^{k-1}F_2$ 上的 Homogeneous 重量，研究了环 $R$ 上长为 $2^s$ 的 $(1+u)$-常循环码的 Hamming 距离和 Homogeneous 距离。使用了有限环和域的理论，给出了环 $R$ 上长为 $2^s$ 的 $(1+u)$-常循环码和循环自对偶码的结构和码字个数。并利用该常循环码的结构，确定了环 $R$ 上长为 $2^s$ 的 $(1+u)$-常循环码的 Hamming 距离和 Homogeneous 距离分布。

**关键词**：常循环码；Hamming 距离；Homogeneous 距离
**中图分类号**：TN911.22　　**文献标识码**：A　　**文章编号**：1009-5896(2010)01-0112-05
**DOI**: 10.3724/SP.J.1146.2008.01810

# The Distributions of Distances of $(1+u)$-Constacyclic Codes of Length $2^s$ over $F_2+uF_2+\cdots+u^{k-1}F_2$

Shi Min-jia[①②]　Yang Shan-lin[②]　Zhu Shi-xin[②]
[①](*School of Mathematics Sciences of Anhui University*, *Hefei* 230039, *China*)
[②](*Institute of Computer Network System*, *Hefei University of Technology*, Hefei 230009, *China*)

**Abstract**: In coding theory, it is important to study the distance distribution of codewords. The Homogeneous weight over ring $R=F_2+uF_2+\cdots+u^{k-1}F_2$ is defined. Hamming distances and Homogeneous distances of $(1+u)$- constacyclic codes of length $2^s$ over the ring $R$ are studied. By means of the theory of finite rings, the structure of $(1+u)$- constacyclic codes of length $2^s$ over $R$ is also obtained. Especially, the structure and the size of cyclic self-dual codes over the ring are also given. Then, using the structure of such constacyclic codes, the distributions of the Hamming distances and Homogeneous distances of such constacyclic codes are determined.

**Key words**: Constacyclic code; Hamming distance; Homogeneous distance

## 1　引言

最近，多项式剩余类环上的码得到了广泛和充分的研究。从最初文献[1]运用 $F_2+uF_2$ 上的线性码构造格至今，已有大量的文献对此环上的码进行了研究。文献[2]研究了 $F_2+uF_2$ 上的循环码和自对偶码；文献[3]讨论了 $F_2+uF_2$ 上的类型II码；文献[4]给出了 $F_2+uF_2$ 上奇长的 $(1+u)$-常循环码的性质。文献[5]研究了环 $F_2+uF_2+\cdots+u^{k-1}F_2$ 上码长为奇数的循环码；文献[6]中利用环 $F_p+uF_p+\cdots+u^{k-1}F_p$ 来构造最佳跳频序列；文献[7]中研究了 $F_p+uF_p+\cdots+u^{k-1}F_p$ 上单根循环码及自对偶码的结构；文献[8]中证明了环 $F_q[u]/\langle u^s\rangle$ 上所有的单根循环码皆为最大秩距离码；文献[9]中研究了 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上一类重根常循环码。文献[10]中确定了 $GR(2^a,m)$ 上长为 $2^s$ 的负循环码的Hamming距离；文献[11] 确定了 $F_2+uF_2$ 上长为 $2^s$ 的 $(1+u)$-常循环码的距离分布；本文继续研究多项式剩余类环 $R$ 上的长为 $2^s$ 的 $(1+u)$-常循环码的距离分布，首先定义了该环上的Homogeneous重量，该重量是 $F_2+uF_2$ 上Lee重量的一个推广；其次，研究了该环上长为 $2^s$ 的 $(1+u)$-常循环码的Hamming距离和Homogeneous距离，给出了环 $R$ 上长为 $2^s$ 的 $(1+u)$-常循环码和自对偶码的结构和码字个数；最后，利用这个结构，确定了该环上长为 $2^s$ 的 $(1+u)$-常循环码的Hamming距离和Homogeneous距离分布。

## 2　基本概念和引理

$R$ 是局部环，特征为 2，其唯一的极大理想是 $(u)$，$u$ 的幂零指数为 $k$，即 $u^k=0$。对任意的 $a\in R$，$a$ 可以唯一地表示为 $a=a_0+a_1u+\cdots+a_{k-1}u^{k-1}$，$a_i\in F_2$。$R$ 上长为 $n$ 的线性码是 $R^n$ 的加法子群。如果对 $R$ 的单位 $\lambda$，长为 $n$ 的线性码 $C$ 在自同构 $\sigma_\lambda$：

$$(c_0,c_1,\cdots,c_{n-1})\mapsto(\lambda c_{n-1},c_0,\cdots,c_{n-2})$$

下不变，则称码 $C$ 是 $\lambda$-常循环码。当 $\lambda=1$ 时，称 $C$ 为 $R$ 上的循环码；当 $\lambda=1+u$，称 $C$ 为 $R$ 上的

2008-12-29 收到，2009-06-19 改回
国家自然科学基金(60673074),教育部科学技术研究重点项目(107065)和可信软件测试及可信性评估研究(重大研究计划)基金(90718037)资助课题
通信作者：施敏加　shiminjia_219@tom.com

$(1+u)$- 常循环码。定义由 $R^n$ 到商环 $R[x]/(x^n-\lambda)$ 上的映射 $\rho$：

$$(c_0,c_1,\cdots,c_{n-1})\mapsto c_0+c_1x+\cdots+c_{n-1}x^{n-1}$$

称 $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ 为 $c=(c_0,c_1,\cdots,c_{n-1})$ 的码字多项式。一般地视码字和码字多项式为同一概念。$R$ 上长为 $n$ 的 $\lambda$- 常循环码可以看作是商环 $R[x]/(x^n-\lambda)$ 的理想。

环 $R$ 上的码有两种重量：Hamming 重量和 Homogeneous 重量。分别用 $w_{ha},w_{ho}$ 表示。定义环 $R$ 上的码字的 Hamming 重量为该码字的非零分量的数目。定义环 $R$ 上的 Homogeneous 重量如下。

**定义 1**　环 $R$ 上的 Homogeneous 重量是 $R$ 上的一个重量函数，

$$wt_{ho}:R\to N(\text{自然数}),\ r\mapsto\begin{cases}0, & r=0\\ 2^{k-2}, & r\neq 0,\ r\neq u^{k-1}\\ 2^{k-1}, & r=u^{k-1}\end{cases}$$

$R$ 上长为 $n$ 一个码字 $(c_0,c_1,\cdots,c_{n-1})$ 的 Homogeneous 重量是对应分量的 Homogeneous 重量的和，即 $wt_{ho}(c_0,c_1,\cdots,c_{n-1})=\sum_{i=0}^{n-1}wt_{ho}(c_i)$。

线性码 $C$ 的 Hamming 距离和 Homogeneous 距离分别为码 $C$ 中的非零码字的极小 Hamming 重量和 Homogeneous 重量，分别用 $d_{ha},d_{ho}$ 表示。线性码的这两种距离是它的很重要的参数，在编码及模格的构造中起着很重要的作用。

为了研究环 $R$ 上长为 $2^s(s\geq 1)$ 的 $(1+u)$- 循环码的结构，需要用到下面两个引理。

**引理 1**[12]　设 $R$ 是阶为 $p^\alpha$ 的有限环，$p$ 是素数，则 $R$ 上长为 $n$ 的线性码 $C$ 的码字的数目是 $p^k$，其中 $k$ 是集合 $\{0,1,2,\cdots,\alpha n\}$ 中的某个整数。

**引理 2**[13]　设 $R$ 是有单位元的交换环，$f(x),g(x)\in R[x]$ 均为非零多项式，并且 $g(x)$ 的首项系数是 $R$ 中的单位，则存在唯一确定的多项式 $q(x),r(x)\in R(x)$，使得 $f(x)=q(x)g(x)+r(x)$，且 $\deg r(x)<\deg g(x)$。

对任意向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n),\boldsymbol{y}=(y_1,y_2,\cdots,y_n)\in R^n$，定义 $\boldsymbol{x}$ 与 $\boldsymbol{y}$ 的内积为 $\boldsymbol{x}\cdot\boldsymbol{y}=x_1y_1+\cdots+x_ny_n$。如果有 $\boldsymbol{x}\cdot\boldsymbol{y}=0$，则称 $\boldsymbol{x}$ 与 $\boldsymbol{y}$ 正交。设 $C$ 是环 $R$ 上长 $n$ 为的线性码，令 $C^\perp=\{\boldsymbol{x}\in R^n\mid\boldsymbol{x}\cdot\boldsymbol{y}=0,\forall\boldsymbol{y}\in C\}$，则 $C^\perp$ 也是环 $R$ 上的线性码，称之为 $C$ 的对偶码。

## 3　$R$ 上长为 $2^s$ 的 $(1+u)$- 常循环码的结构

下面讨论环 $R$ 上长为 $2^s(s\geq 1)$ 的 $(1+u)$- 循环码，它恰是环 $R[x]/(x^{2^s}-(1+u))$ 的理想，用 $R(s)$ 表示环 $R[x]/(x^{2^s}-(1+u))$。

**定理 1**　$R$ 上长为 $2^s$ 的 $(1+u)$- 常循环码是 $\langle(x+1)^i\rangle,\ 0\leq i\leq 2^sk$。

**证明**　设 I 是 $R(s)$ 的理想，则 I 的每个元素模 $u$ 形成环 $F_2[x]/(x^{2^s}-1)$ 的理想，而 $F_2[x]/(x^{2^s}-1)$ 的理想是 $\langle(x+1)^j\rangle,0\leq j\leq 2^s$，故 I 的每个元素都可写成：$c(x)(x+1)^j+\sum_{i=1}^{k-1}u^id_i(x)=c(x)(x+1)^j+ud(x)$，$c(x),d_i(x),d(x)\in R(s)$。在 $R(s)$ 中，$u+1=x^{2^s}$，即 $u=(x+1)^{2^s}$，所以 $ud(x)\in\langle(x+1)^{2^s}\rangle$。又在 $R(s)$ 中 $(x+1)^{2^sk}=u^k=0$，所以 $x+1$ 在 $R(s)$ 中的幂零指数是 $2^sk$，故 I 必包含在 $R(s)$ 的某个理想 $\langle(x+1)^j\rangle$ 中，其中 $0\leq j\leq 2^sk$。对 $R(s)$ 中的某个理想 I，令 $\delta$ 是使得 $\mathrm{I}\subseteq\langle(x+1)^j\rangle$ 的最大值 $j$，则存在 $a(x)\in I$ 使得 $a(x)=(x+1)^\delta b(x)$，而 $(x+1,b(x))=1$，其中 $b(x)\in R(s)$。因为 $x+1$ 在 $R(s)$ 中不可逆，所以 $b(x)$ 是 $R(s)$ 中的逆元，因此 $(x+1)^\delta=a(x)[b(x)]^{-1}\in I$，由此得出 $I=\langle(x+1)^\delta\rangle$。因为 $I$ 是 $R(s)$ 的任一理想，所以 $R(s)$ 的理想是 $\langle(x+1)^i\rangle,0\leq i\leq 2^sk$。　　证毕

注意到在 $R(s)$ 中，$(x+1)^{2^s}=u$，因此 $R$ 上长为 $2^s$ 的 $(1+u)$- 常循环码可以记为

$$\begin{aligned}&\langle 1\rangle\supset\langle(x+1)^1\rangle\supset\cdots\supset\langle(x+1)^{2^s}\rangle\\&=\langle u\rangle\supset\langle(x+1)^{2^s+1}\rangle\supset\cdots\supset\langle(x+1)^{2^s\cdot 2}\rangle\\&=\langle u^2\rangle\supset\langle(x+1)^{2^s\cdot 2+1}\rangle\supset\cdots\supset\langle(x+1)^{2^s\cdot 3}\rangle\\&=\langle u^3\rangle\cdots\supset\langle(x+1)^{2^s(k-1)+1}\rangle\supset\cdots\supset\langle(x+1)^{2^s\cdot k}\rangle\\&=\langle 0\rangle\end{aligned}$$

由引理 1 和定理 1 可以得到如下推论 1。

**推论 1**　(1) $R(s)$ 是一个链环，其极大理想为 $\langle x+1\rangle$，$x+1$ 的幂零指数为 $2^sk$，且在 $R(s)$ 中，$\langle(x+1)^{2^s}\rangle=\langle u\rangle$。

(2)设 $C$ 是 $R$ 上长为 $2^s$ 的 $(1+u)$- 常循环码，则 $C=\langle(x+1)^i\rangle,\ 0\leq i\leq 2^sk$，其中 $i$ 是集合 $\{0,1,\cdots,2^sk\}$ 中的某一整数，则 $|C|=2^{2^sk-i}$。

(3)码字 $C$ 的对偶码为 $C^\perp=\langle(x+1)^{2^sk-i}\rangle$，而且 $|C^\perp|=2^i$，当 $2^{s-1}k\leq i\leq 2^sk$ 时，$\langle(x+1)^i\rangle$ 是自正交的，$\langle(x+1)^{2^{s-1}k}\rangle$ 是 $R$ 上长为 $2^s$ 的唯一的自对偶 $(1+u)$- 常循环码。

## 4　$R$ 上长为 $2^s$ 的 $(1+u)$- 常循环码的距离

首先考虑 $R$ 上长为 $2^s$ 的 $(1+u)$- 常循环码的 Hamming 距离。

**引理 3**　设 $C=\langle(x+1)^i\rangle$ 是 $R$ 上长为 $2^s$ 的 $(1+u)$- 常循环码，$i\in\{0,1,\cdots,2^sk\}$，则当 $0\leq i\leq 2^s(k-1)$，$d_{ha}(C)=1$；当 $2^s(k-1)+1\leq i\leq 2^s(k-1)+2^{s-1}$，$d_{ha}(C)=2$。

**证明** 因为 $R(s)$ 的理想形成严格包含升链

$$\begin{aligned}\langle 1\rangle &\supset \left\langle (x+1)^1\right\rangle \supset \cdots \supset \left\langle (x+1)^{2^s}\right\rangle \\ &= \langle u\rangle \supset \left\langle (x+1)^{2^s+1}\right\rangle \supset \cdots \supset \left\langle (x+1)^{2^s\cdot 2}\right\rangle \\ &= \left\langle u^2\right\rangle \supset \cdots \supset \left\langle (x+1)^{2^s\cdot(k-2)+1}\right\rangle \supset \cdots \supset \left\langle (x+1)^{2^s(k-1)}\right\rangle \\ &= \left\langle u^{k-1}\right\rangle \supset \left\langle (x+1)^{2^s(k-1)+1}\right\rangle \supset \cdots \supset \left\langle (x+1)^{2^s\cdot k}\right\rangle = \langle 0\rangle\end{aligned}$$

所以 $d_{ha}\left(\left\langle (x+1)^0\right\rangle\right) \le d_{ha}\left(\left\langle (x+1)^1\right\rangle\right) \le \cdots \le d_{ha}\left(\left\langle (x+1)^{2^s(k-1)}\right\rangle\right)$。又因 $d_{ha}\left(\left\langle (x+1)^0\right\rangle\right) = d_{ha}\left(\left\langle (x+1)^{2^s(k-1)}\right\rangle\right) = 1$，故当 $0 \le i \le 2^s(k-1)$，$d_{ha}(C) = 1$。当 $2^s(k-1)+1 \le i \le 2^s(k-1)+2^{s-1}$，假设 $C$ 中有 Hamming 重量为 1 的码字 $c(x)$，则 $c(x) = x^k, \beta x^k$（$\beta$ 为 $R$ 中的单位），或者 $u^i x^k$，其中 $1 \le i \le k-1$，$0 \le k \le 2^s k-1$。若 $c(x) = x^k$ 或 $\beta x^k$，则由 $c(x)$ 是 $R(s)$ 的逆元可得 $\langle 1\rangle = C$，矛盾；若 $c(x) = u^i x^k$，则由 $x^k$ 是 $R(s)$ 的逆元可得 $\left\langle u^i\right\rangle \subseteq C$，矛盾。因此 $d_{ha}(C) \ge 2$。又 $(x+1)^{2^s(k-1)+1} = u^{k-1}\cdot(x+1) = u^{k-1}x + u^{k-1}$，$(x+1)^{2^s(k-1)+2^{s-1}} = u^{k-1}(x+1)^{2^{s-1}} = u^{k-1}x^{2^{s-1}} + u^{k-1}$，所以 $d_{ha}(C) = 2$。 证毕

**引理 4** 设 $l$ 是整数，且 $1 \le l \le s, c_l = (x+1)^{2^s(k-1)+\sum_{i=1}^{l} 2^{s-i}} \in R(s)$，则 $d_{ha}\left(\left\langle c_l\right\rangle\right) \le 2^l$。

**证明** 在 $R(s)$ 中，$c_l = (x+1)^{2^s(k-1)+\sum_{i=1}^{l} 2^{s-i}} = u^{k-1}\prod_{i=1}^{l}\left(x^{2^{s-i}}+1\right) = u^{k-1}\sum_{i=1}^{2^l} x^{2^s-i\cdot 2^{s-l}}$。因此，对 $1 \le l \le s$，$c_l$ 的 Hamming 重量是 $2^l$，从而 $d_{ha}\left(\left\langle c_l\right\rangle\right) \le 2^l$。 证毕

**引理 5** 设 $C = \left\langle (x+1)^i\right\rangle \subseteq R(s)$ 是 $R$ 上长为 $2^s$ 的 $(1+u)$- 常循环码，其中 $i = 2^s(k-1) + \sum_{j=1}^{l} 2^{s-j} + 1$，$1 \le l \le s-1$，则 $d_{ha}(C) = 2^{l+1}$

**证明** 在 $R(s)$ 中，$(x+1)^i = u^{k-1}(x+1)\cdot\prod_{i=1}^{l}\left(x^{2^{s-i}}+1\right) = u^{k-1}(x+1)\sum_{i=1}^{2^l} x^{2^s-i\cdot 2^{s-l}}$，因此 $(x+1)^i$ 的 Hamming 重量是 $2^{l+1}$，从而 $d_{ha}(C) \le 2^{l+1}$。

设 $f(x) \in C$，则 $f(x) = (x+1)^i g(x)$，其中 $g(x) \in R(s)$。注意到 $(x+1)^{2^{s-l}-1}$ 是次数为 $2^{s-l}-1$ 的首一多项式，由引理 2，存在 $h(x), r(x) \in R(s)$ 使得 $g(x) = (x+1)^{2^{s-l}-1}h(x) + r(x)$，$\deg(r(x)) < 2^{s-l}-1$。则

$$\begin{aligned}f(x) &= (x+1)^i g(x) = (x+1)^{2^s k-2^{s-l}+1}\cdot\left[(x+1)^{2^{s-l}-1}h(x) + r(x)\right] \\ &= (x+1)^{2^s k}h(x) + u^{k-1}\cdot r(x)(x+1)\sum_{i=1}^{2^l} x^{2^s-i\cdot 2^{s-l}} \\ &= u^{k-1}r(x)(x+1)\sum_{i=1}^{2^l} x^{2^s-i\cdot 2^{s-l}}\end{aligned}$$

注意到 $u^{k-1}r(x)(x+1) \in \left\langle (x+1)^{2^s+1}\right\rangle$。由引理 3 可知，$u^{k-1}r(x)(x+1)$ 的 Hamming 重量至少是 2，于是 $u^{k-1}r(x)(x+1)$ 总可写成 $u^{k-1}r(x)(x+1) = u^{k-1}\cdot(x^{i_1} + x^{i_2} + \cdots + x^{i_n})$，其中 $0 \le i_1 < i_2 < \cdots < i_n \le 2^{s-l}-1$，$n$ 是 $\ge 2$ 的整数。所以

$$\begin{aligned}&u^{k-1}r(x)(x+1)\sum_{i=1}^{2^l} x^{2^s-i\cdot 2^{s-l}} \\ &\quad = u^{k-1}\left(x^{i_1} + x^{i_2} + \cdots + x^{i_n}\right)\sum_{i=1}^{2^l} x^{2^s-i\cdot 2^{s-l}}\end{aligned}$$

注意到 $\sum_{i=1}^{2^l} x^{2^s-i\cdot 2^{s-l}}$ 任意相邻两项次数相差 $2^{s-l}$。另一方面，对任意 $e, f \in \{1,2,\cdots,n\}$ 都有 $0 < i_e - i_f \le 2^{s-l}-1$，则 $u^{k-1}r(x)(x+1)\sum_{j=1}^{2^k} x^{2^s-j\cdot 2^{s-k}}$ 的 Hamming 重量为 $2^l n$，$n$ 是 $2 \le n \le 2^{s-l}$ 的某个整数，则 $f(x)$ 的 Hamming 重量为 0 或 $\ge 2^{l+1}$，由此可以推出 $d_{ha}(C) = 2^{l+1}$。 证毕

**定理 2** 设 $C = \left\langle (x+1)^i\right\rangle \subseteq R(s)$ 是 $R$ 上长为 $2^s$ 的 $(1+u)$- 常循环码，$i \in \{0,1,2,\cdots,2^s k\}$，则

$$d_{ha}(C) = \begin{cases}0, & i = 2^s k \\ 1, & 0 \le i \le 2^s(k-1) \\ 2, & 2^s(k-1)+1 \le i \le 2^s(k-1)+2^{s-1} \\ 2^{l+1}, & 2^s(k-1) + \sum_{j=1}^{l} 2^{s-j} + 1 \le i \le 2^s \cdot(k-1) + \sum_{j=1}^{l+1} 2^{s-j}, \ 1 \le l \le s-2 \\ 2^s, & i = 2^s k - 1\end{cases}$$

**证明** 引理 3 已经证明了当 $0 \le i \le 2^s(k-1)$ 和 $2^s(k-1)+1 \le i \le 2^s(k-1)+2^{s-1}$ 时的情形。对于 $i = 2^s k-1$，因为 $(x+1)^{2^s k-1} = (x+1)^{2^s(k-1)+2^s-1} = u^{k-1}(1+x+\cdots+x^{2^s-1})$，所以 $d_{ha} = 2^s$。故只需证明对任意 $1 \le l \le s-2$，$2^s(k-1) + \sum_{j=1}^{l} 2^{s-j} + 1 \le i \le 2^s\cdot(k-1) + \sum_{j=1}^{l+1} 2^{s-j}$ 时，有 $d_{ha}(C) = 2^{l+1}$ 成立即可。因为

$\left\langle (x+1)^{2^s(k-1)+\sum_{j=1}^{l}2^{s-j}+1}\right\rangle \supset \cdots \supset \left\langle (x+1)^{2^s(k-1)+\sum_{j=1}^{l+1}2^{s-j}}\right\rangle$，根据引理 4，若 $2^s(k-1)+\sum_{j=1}^{l}2^{s-j}+1 \le i \le 2^s(k-1)+\sum_{j=1}^{l+1}2^{s-j}$，则 $d_{ha}(C) \le 2^{l+1}$。另一方面，根据引理 5，$d_{ha}\left(\left\langle (x+1)^{2^s(k-1)+\sum_{j=1}^{l}2^{s-j}+1}\right\rangle\right)=2^{l+1}$。　　证毕

注记：$k \ge 2$ 时，则 $2^{s-1}k \le 2^s(k-1)$，因此 $R$ 上长为 $2^s$ 的唯一的自对偶 $(1+u)$- 常循环码 $\left\langle (x+1)^{2^{s-1}k}\right\rangle \subseteq R(s)$ 的 Hamming 重量为 1。

根据定理 2，可得 $R$ 上所有长为 $2^s$ 的 $(1+u)$- 常循环码的 Homogeneous 距离分布。

**定理 3**　设 $C=\left\langle (x+1)^i\right\rangle \subseteq R(s)$，$i \in \{0,1,\cdots,2^s k\}$ 是 $R$ 上长为 $2^s$ 的 $(1+u)$- 常循环码，则

$$d_{ho}(C)=\begin{cases}0, & i=2^s k\\ 2^{k-2}, & 0\le i\le 2^s(k-2)\\ 2^{k-1}, & 2^s(k-2)+1\le i\le 2^s(k-1)\\ 2^k, & 2^s(k-1)+1\le i\le 2^s(k-1)+2^{s-1}\\ 2^{k+l}, & 2^s(k-1)+\sum_{j=1}^{l}2^{s-j}+1\le i\le 2^s\cdot(k-1)+\sum_{j=1}^{l+1}2^{s-j},\\ & 1\le l\le s-1\end{cases}$$

**证明**　如果 $0 \le i \le 2^s(k-2)$，则 $\langle 1\rangle \supseteq C \supseteq \left\langle u^{k-2}\right\rangle$，因为 $d_{ho}(\langle 1\rangle)=d_{ho}\left(\left\langle u^{k-2}\right\rangle\right)=2^{k-2}$，所以 $d_{ho}(C)=2^{k-2}$。如果 $2^s(k-2)+1 \le i \le 2^s(k-1)$，则 $\left\langle u^{k-2}(x+1)\right\rangle \supseteq C \supseteq \left\langle u^{k-1}\right\rangle$，因为 $d_{ho}\left\langle u^{k-2}(x+1)\right\rangle = d_{ho}\left\langle u^{k-1}\right\rangle = 2^{k-1}$，所以 $d_{ho}(C)=2^{k-1}$。如果 $2^s(k-1)+1 \le i \le 2^s\cdot(k-1)+2^{s-1}$，则 $\left\langle u^{k-1}(x+1)\right\rangle \supseteq C \supseteq \left\langle u^{k-1}(x+1)^{2^{s-1}}\right\rangle$，由定理 2 可知，$\left\langle u^{k-1}(x+1)\right\rangle$ 和 $\left\langle u^{k-1}(x+1)^{2^{s-1}}\right\rangle$ 的 Hamming 重量都是 2，则 $d_{ho}\left\langle u^{k-1}(x+1)\right\rangle = d_{ho}\left\langle u^{k-1}(x+1)^{2^{s-1}}\right\rangle = 2^k$，则 $d_{ho}(C)=2^k$。若对 $1 \le l \le s-1$，如果 $2^s(k-1)+\sum_{j=1}^{l}2^{s-j}+1 \le i \le 2^s(k-1)+\sum_{j=1}^{l+1}2^{s-j}$，则 $\left\langle u^{k-1}(x+1)^{1+\sum_{j=1}^{l}2^{s-j}}\right\rangle \supseteq C \supseteq \left\langle u^{k-1}(x+1)^{\sum_{j=1}^{l+1}2^{s-j}}\right\rangle$，根据定理 2，$d_{ho}\left\langle u^{k-1}(x+1)^{1+\sum_{j=1}^{l}2^{s-j}}\right\rangle = d_{ho}\cdot\left\langle u^{k-1}(x+1)^{\sum_{j=1}^{l+1}2^{s-j}}\right\rangle = 2^{l+1}\cdot 2^{k-1}=2^{k+l}$，因此 $d_{ho}(C)=2^{k+l}$。　　证毕

注意到在环 $F_2+uF_2$ 上（$k=2$ 时的情形），Homogeneous 重量就是 Lee 重量，因此作为定理 2 的一种特殊情况，可以得到 $F_2+uF_2$ 上长为 $2^s$ 的所有 $(1+u)$- 常循环码的 Lee 距离分布。

**推论 2**　设 $C=\left\langle (x+1)^i\right\rangle$ 是 $F_2+uF_2$ 上长为 $2^s$ 的 $(1+u)-$ 常循环码，$i \in \{0,1,2,\cdots,2^{s+1}\}$，则

$$d_{ho}(C)=\begin{cases}0, & i=2^{s+1}\\ 1, & i=0\\ 2, & 1\le i\le 2^s\\ 4, & 2^s+1\le i\le 2^s+2^{s-1}\\ 2^{2+l}, & 2^s+\sum_{j=1}^{l}2^{s-j}+1\le i\le 2^s+\sum_{j=1}^{l+1}2^{s-j},\\ & 1\le l\le s-1\end{cases}$$

## 5　结束语

本文讨论了环 $R$ 上长为 $2^s$ 的 $(1+u)$- 常循环码的结构，由此确定了环 $R$ 上长为 $2^s$ 的 $(1+u)$- 常循环码的 Hamming 距离和 Homogeneous 距离。环 $R$ 上的其它偶长的 $(1+u)$- 常循环码以及该环上长为 $2^s$ 的循环码的各种距离分布也是一个值得研究的问题。

## 参 考 文 献


[1] Bachoc C. Applications of coding theory to the construction of modular Lattices[J]. *Combinatorial Theory, Series A*, 1997, 78(1): 92–119.

[2] Bonnecaze A and Udaya P. Cyclic codes and self-dual codes over $F_2+uF_2$ [J]. *IEEE Transactions on Information Theory*, 1999, 45(4): 1250–1255.

[3] Dougherty S T, Gaborit P, Harada M, and Solé.P. Type Ⅱ codes over $F_2+uF_2$ [J]. *IEEE Transactions on Information Theory*, 1999, 45(1): 32–45.

[4] Qian Jian-fa, Zhang Li-na, and Zhu Shi-xin. $(1+u)$-constacyclic and cyclic codes over $F_2+uF_2$ [J]. *Applied Mathematics Letters*, 2006, 19(8): 820–823.

[5] 钱建发，朱士信．$F_2+uF_2+\cdots+u^kF_2$ 环上的循环码[J]. 通信学报, 2006, 27(9): 86–88.
Qian Jian-fa and Zhu Shi-xin. Cyclic codes over ring $F_2+uF_2+\cdots+u^kF_2$ [J]. *Journal on Communications*, 2006, 27(9): 86–88.

[6] Udaya P and Siddiqi M U. Optimal large linear complexity frequency hopping patterns derived from polynomial residue rings [J]. *IEEE Transactions on Information Theory*, 1998,

44(4): 1492–1503.

[7] Qian J F and Zhu S X. Cyclic codes over $F_p + uF_p + \cdots + u^{k-1}F_p$ [J]. *IEICE Transactions on Fundamentals*, 2005, E88-A(3): 795–797.

[8] Ozen M and Siap I. Linear codes over $F_q[u]/\langle u^s \rangle$ with respect to the Rosenbloom-tasfasm an metric[J]. *Designs, Codes and Cryptology*, 2006, 38(1): 17–29.

[9] 朱士信, 李平, 吴波. 环 $F_q + uF_q + \cdots + u^{k-1}F_q$ 上一类重根循环码[J]. 电子与信息学报, 2008, 30(6): 1394–1396.
Zhu Shi-xin, Li Ping, and Wu Bo. A class of repeated-root constacyclic codes over the ring $F_q + uF_q + \cdots + u^{k-1}F_q$ [J]. *Journal of Electronics & Information Technology*, 2008, 30(6): 1394–1396.

[10] Zhu Shi-xin and Kai Xiao-shan. The Hamming distances of negacyclic codes of length $2^s$ over $GR(2^a, m)$ [J]. *Journal of System Science and Complexity*, 2008, 21(1): 60–66.

[11] 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 Lin, Zhu Shi-xin, and Han Jiang-hong. 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.

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

[13] McDonald B R. Finite Rings with Identity[M]. New York: Marcel Dekker, 1974, Chapter II.

施敏加： 男，1980年生，博士，研究方向为代数编码与密码.

杨善林： 男，1948年生，教授，博士生导师，研究方向为信息和网络安全.

朱士信： 男，1962年生，教授，博士生导师，研究方向为代数编码与密码.