环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上任意长度的 $(u\lambda-1)$-常循环码

李 平* 朱士信 开晓山
(合肥工业大学数学学院 合肥 230009)

摘 要：该文利用环同态理论，给出了环 $R=F_q+uF_q+\cdots+u^{k-1}F_q$ 上任意长度 N 的所有 $(u\lambda-1)$-常循环码的生成元，λ 是 R 的可逆元。证明了 $R[x]/<x^N+1-u\lambda>$ 是主理想环。给出了环 R 上任意长度 N 的 $(u\lambda-1)$-常循环码的计数。确定了环 R 上任意长度 N 的 $(u\lambda-1)$-常循环码的最高阶挠码的生成多项式，由此给出了环 R 上长度 p^s 的所有 $(u\lambda-1)$-常循环码的汉明距离。

关键词：常循环码；最高阶挠码；负循环码；汉明距离
中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2013)05-1044-05
DOI: 10.3724/SP.J.1146.2012.01257

$(u\lambda-1)$-constacyclic Codes of Arbitrary Lengths over the Ring $F_q+uF_q+\cdots+u^{k-1}F_q$

Li Ping Zhu Shi-xin Kai Xiao-shan
(*School of Mathematics*, *Hefei University of Technology*, *Hefei* 230009, *China*)

Abstract: Let R denote the ring $R=F_q+uF_q+\cdots+u^{k-1}F_q$, and λ be an invertible element of R. By means of the theory of ring homomorphism, the generators of all these $(u\lambda-1)$-constacyclic codes of an arbitrary length N over the ring R are obtained. It is proved that $R[x]/<x^N+1-u\lambda>$ is principal. The number of these $(u\lambda-1)$-constacyclic codes is determined. The generator polynomials of the highest-order torsion codes of all these $(u\lambda-1)$-constacyclic codes are given. As a result, the Hamming distances of all these $(u\lambda-1)$-constacyclic codes are obtained.

Key words: Constacyclic codes; Highest-order Torsion codes; Negacyclic codes; Hamming distances

1 引言

最近，剩余类环 $F_q[u]/<u^k>=F_q+uF_q+\cdots+u^{k-1}F_q$（$q$ 为素数 p 的方幂)(该环简称 R)引起人们极大的兴趣。编码爱好者利用它进行格的构造及最佳跳频序列的构造，还通过它利用线性的Gray映射构造了一批域 F_q 上最优码[1−4]。同时该环上各种常循环码(包括循环码)以及斜(skew)常循环码的结构研究也引起编码爱好者的重视[4−8]。文献[4]获得了环 R 上长为 p^e 的所有的 $(u\lambda-1)$-常循环码的结构及其码字个数，其中 λ 是环 R 的任一可逆元。环 $F_{2^m}+uF_{2^m}$ 上的 $(u\lambda-1)$-常循环码的对偶码仍是 $(u\lambda-1)$-常循环码，因此在该文献中取环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 的 $q=2^m$ 且 $k=2$ 情形，特别研究了环 $F_{2^m}+uF_{2^m}$ 上长为 2^e 的 $(u\lambda-1)$-常循环码的对偶码的结构及其码字个数，并研究了这种常循环的自对偶码。随后，文献[5]给出文献[4]的结果的特殊情形（$k=2$ 且 $p=2$ 的情形，注意 $p=2$ 时 $u\lambda-1=u\lambda+1$)。文献[6]给出了环 $F_2+uF_2+\cdots+u^{k-1}F_2$ 上长为 2^s 的 $(u+1)$-常循环码的汉明距离及齐次距离。文献[7]给出了环 $F_{p^m}+uF_{p^m}$ 上所有的斜常循环码的结构。最近，人们还对环 F_2+uF_2 的扩环 $(F_2+uF_2)[v]/<v^2>$ 即 $F_2+uF_2+vF_2+uvF_2$ 以及 F_2+uF_2 扩环 R_k 上循环码的结构进行研究，并通过Gray 映射获得一批二元最优码[8,9]。本文在文献[4]的基础上研究环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上任意长度的所有 $(u\lambda-1)$-常循环码的结构并给出其最高阶挠码的生成多项式，由此给出了环 R 上长度 p^s 的所有 $(u\lambda-1)$-常循环码的汉明距离。

2 主要结果

环 R 是有限链环，关于环 R 的结构，文献[10−13]中均有介绍。环 R 上码长为 n 的线性码是指 R^n 的 R-子模。设 ϖ 为环 R 的可逆元。环 R 上码长为 n 线性码 C 叫做 ϖ-常循环码，若 $\forall(x_0,x_1,\cdots,x_{n-1})\in C$，均有 $(\varpi x_{n-1},x_0,x_1,\cdots,x_{n-2})\in C$。将码字与它的多项

2012-09-28 收到，2012-12-28 改回
国家自然科学基金(60973125)，安徽省自然科学基金(1208085MA14)，中央高校基本科研业务费专项基金(2012HGXJ0040)，合肥工业大学博士专项基金(2010HGBZ0550)和合肥工业大学青年教师创新基金(2011HGQC1023)资助课题
*通信作者：李平 lpmath@126.com

式表示等同，则环 R 上码长为 n 的 ϖ - 常循环码亦即商环 $R[x]/\langle x^n-\varpi\rangle$ 的理想。不引起混淆时，多项式 $f(x)$ 可简记为 f，$f(x)+\langle x^n-\gamma\rangle$ 可简记为 $f(x)$ 或 f。

我们首先定义映射 ϕ 如下：

$$\phi: R\to F_q, r_0+r_1u+\cdots+r_{k-1}u^k\to r_0,\quad r_i\in F_q,\ 0\le i\le k-1 \tag{1}$$

则 ϕ 是环 R 到 F_q 的环满同态，通常称作模 u 约化，自然地 ϕ 可扩展成 $R[x]$ 到 $F_q[x]$ 的环满同态。

命题1　映射 ϕ 可扩展成 $R[x]/<x^N+1-u\lambda>$ 到 $F_q[x]/<x^N+1>$ 的环满同态(仍记成 ϕ)，N 是任意正整数。

证明　注意到 $R[x]$ 中多项式均可写成 $g_0(x)+ug_1(x)+\cdots+u^{k-1}g_{k-1}(x)$ 的形式，其中 $g_i(x)\in F_q[x]$, $0\le i\le k-1$。设 ϕ 为：$\phi: R[x]/<x^N+1-u\lambda>\to F_q[x]/<x^N+1>$, $g_0(x)+ug_1(x)+\cdots+u^{k-1}g_{k-1}(x)+<x^N+1-u\lambda>\to g_0(x)+<x^N+1>$。

如果

$$\begin{aligned}&g_0(x)+ug_1(x)+\cdots+u^{k-1}g_{k-1}(x)+<x^N+1-u\lambda>\\&\quad=h_0(x)+uh_1(x)+\cdots+u^{k-1}h_{k-1}(x)\\&\qquad+<x^N+1-u\lambda>\end{aligned} \tag{2}$$

则在 $R[x]$ 中 $x^N+1-u\lambda$ 整除 $(h_0-g_0)+u(h_1-g_1)+\cdots+u^{k-1}(h_{k-1}-g_{k-1})$，从而在 $F_q[x]$ 中 x^N+1 整除 h_0-g_0，从而在 $F_q[x]/<x^N+1>$ 中 $g_0(x)+<x^N+1>=h_0(x)+<x^N+1>$，这就证明了 $\phi: R[x]/<x^N+1-u\lambda>\to F_q[x]/<x^N+1>$ 确实是一个映射，则 ϕ 显然是满射。又很容易验证 ϕ 关于加法和乘法保持运算，故 ϕ 是环满同态。　证毕

多项式 $f(x)$ 的模 u 约化通常记成 $\overline{f}(x)$。如果 $\overline{f}(x)$ 是 $F_q[x]$ 中不可约多项式，则称 $f(x)$ 是 $R[x]$ 中基本不可约多项式。$R[x]$ 中两个多项式 f_1, f_2 叫做互素的，如果存在 $R[x]$ 中两个多项式 g_1, g_2 使得 $f_1g_1+f_2g_2=1$，此时可记 $\gcd(f_1,f_2)=1$。注意到 R 是有限链环，据文献[12]有下面的引理 1。

引理 1　$R[x]$ 中两个多项式 $f_1(x)$与$f_2(x)$ 互素当且仅当在 $F_q[x]$ 中 $\overline{f}_1(x)$ 与 $\overline{f}_2(x)$ 互素。

注意到 F_q 是环 R 的子环，故 $F_q[x]$ 中多项式皆可视为 $R[x]$ 中多项式。从而 $F_q[x]$ 到 $R[x]$ 的 Hensel 提升是平凡的。

本文只考虑 q 是奇素数 p 的任意正整数方幂的情形。假设 q 与 n 互素。易知 q 与 $2n$ 也互素。由于总有 $x^{2n}-1=(x^n-1)(x^n+1)$，用 I 表示模 $2n$ 的 q - 分圆陪集的最小完全代表团，用 I_1 表示模 n 的 q - 分圆陪集的最小完全代表团。由于奇数 q 与 $2n$ 互素，故存在最小正整数 r 使得 $q^r\equiv 1\bmod(2n)$，即 q 模 $2n$ 的乘法阶为 r，则域 F_{q^r} 中存在乘法阶为 $2n$ 的元素 ξ。对每一个 $i\in I$, ξ^i 在 F_q 上的最小多项式记为 $f_i(x)$，则

$$\begin{aligned}x^{2n}-1&=(x^n-1)(x^n+1)=\prod_{i\in I}f_i(x)\\&=\prod_{2i\in I}f_{2i}(x)\cdot(x^n+1)=\prod_{i\in I_1}f_{2i}(x)\cdot(x^n+1)\end{aligned} \tag{3}$$

从而 $x^n+1=\prod_{i\in I}f_i(x)/\prod_{i\in I_1}f_{2i}(x)=\prod_{i\in I,i\text{是奇数}}f_i(x)$。根据 Hensel 引理，$x^n+1$ 在 $R[x]$ 中可唯一地分解为首一基本不可约多项式的乘积，而 F_q 是环 R 的子环，故有下面的引理。

引理 2　假设 q 是奇素数 p 的任意正整数方幂且 q 与 n 互素。若 $x^n+1=\prod_{i\in I}f_i(x)\Big/\prod_{i\in I_1}f_{2i}(x)=\prod_{i\in I,i\text{是奇数}}f_i(x)$ 是 x^n+1 在 $F_q[x]$ 中分解为首一不可约多项式的乘积的表达式，则其也是 x^n+1 在 $R[x]$ 中分解为首一基本不可约多项式的乘积的唯一的表达式。

假设 $N=p^sn$, s 为非负整数且 p 与 n 互素。记 $\Re=R[X]/<x^N+1-u\lambda>$。

引理 3　x^n+1 是 $\Re$ 的幂零元，且幂零指数为 p^sk。

证明　首先在 $\Re$ 中 $(x^n+1)^{p^sk}=(x^N+1)^k=(u\lambda)^k=0$。其次证明在 $\Re$ 中 $(x^n+1)^{p^sk-1}\ne 0$：若在 $\Re$ 中 $(x^n+1)^{p^sk-1}=0$，由于在 $\Re$ 中 $(x^n+1)^{p^s(k-1)}=(x^N+1)^{k-1}=(u\lambda)^{k-1}\ne 0$, $(x^n+1)^{p^sk-1}=(x^n+1)^{p^sk-p^s}(x^n+1)^{p^s-1}=(u\lambda)^{k-1}(x^n+1)^{p^s-1}=0$，从而在 $R[x]$ 中 $x^N+1-u\lambda$ 整除非零多项式 $(u\lambda)^{k-1}(x^n+1)^{p^s-1}$，但 $x^N+1-u\lambda$ 是首一多项式，且其次数 N 大于 $(p^s-1)n$，矛盾。故在 $R[x]$ 中 $x^N+1-u\lambda$ 不可能整除非零多项式 $(u\lambda)^{k-1}(x^n+1)^{p^s-1}$，从而在 $\Re$ 中 $(x^n+1)^{p^sk-1}\ne 0$。故 x^n+1 是 $\Re$ 的幂零元，且幂零指数为 p^sk。　证毕

引理 4　若 $f(x)$ 和 x^n+1 在 $R[x]$ 中互素，则 $f(x)$ 是 $\Re$ 的可逆元。

证明　若 $f(x)$ 和 x^n+1 在 $R[x]$ 中互素，则在 $R[x]$ 中存在多项式 $\alpha(x),\beta(x)$ 使得 $f(x)\alpha(x)+(x^n+1)\beta(x)=1$，从而 $f(x)\alpha(x)=1-(x^n+1)\beta(x)$，记 $\theta(x)=(x^n+1)\beta(x)$，则在 $\Re$ 中，$1=1-\theta^{p^sk}=(1-\theta)(1+\theta+\cdots+\theta^{p^sk-1})$，从而 $1-\theta$ 是 $\Re$ 的可逆元，故 $f(x)$ 也是 $\Re$ 的可逆元。　证毕

引理 5　假设 q 是奇素数 p 的任意正整数方幂且 q 与 n 互素。若 $f(x)$ 是 x^n+1 在 $F_q[x]$ 中的一个首一因子，v 是任一正整数，则在 $\Re$ 中总有 $<f^{p^sk}(x)>=<f^{p^sk+v}(x)>$。

证明 记 $f\hat{f}=x^n-1$，由题设 $f(x)$ 和 $\hat{f}(x)$ 在 $F_q[x]$ 中互素，从而对任一正整数 v，$f^v(x)$ 和 $\hat{f}^{p^sk}(x)$ 在 $F_q[x]$ 中互素，由引理 1 知：$f^v(x)$ 和 $\hat{f}^{p^sk}(x)$ 在 $R[x]$ 中也互素。因此，存在 $\omega_v(x),\pi_v(x)\in R[x]$，使得在 $R[x]$ 中 $\omega_v(x)f^v(x)+\pi_v(x)\hat{f}^{p^sk}(x)=1$。从而在 $\Re$ 中，$\omega_v(x)\ f^{p^sk+v}(x)=[1-\pi_v(x)\ \hat{f}^{p^sk}(x)]\ f^{p^sk}(x)=f^{p^sk}(x)-\pi_v(x)(x^n+1)^{p^sk}=f^{p^sk}(x)$。

因此对任一正整数 v，在 $\Re$ 中总有 $<f^{p^sk}(x)>=<f^{p^sk+v}(x)>$。 证毕

定理 1 假设 q 是奇素数 p 的任意正整数方幂且 q 与 n 互素。设 $x^n+1=\prod_{i\in I}f_i(x)\Big/\prod_{i\in I_1}f_{2i}(x)=\prod_{i\in I,i是奇数}f_i(x)$ 是 x^n+1 在 $F_q[x]$ 中分解为首一不可约多项式的乘积的表达式。如果 C 是环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上长度为 $N=p^sn$ 的 $(u\lambda-1)$-常循环码，则 C 可表成 $C=<\prod_{i\in I,i是奇数}f_i^{s_i}(x)>$，这里 $0\le s_i\le p^sk$。

证明 设 C 是 $\Re=R[X]/<x^N+1-u\lambda>$ 的任一理想，由命题 1 知 ϕ 是 $R[x]/<x^N+1-u\lambda>$ 到 $F_q[x]/<x^N+1>$ 的环满同态，从而 $\phi(C)$ 是 $F_q[x]/<x^N+1>$ 的理想(即 F_q 上长为 N 的负循环码)，由域上负循环码的理论，它的生成多项式整除 x^N+1，而 $x^N+1=(x^n+1)^{p^s}=\prod_{i\in I,i是奇数}f_i^{p^s}$，故 $\phi(C)$ 可表成 $<\prod_{i\in I,i是奇数}f_i^{k_i}(x)>$ 的形式，这里 $0\le k_i\le p^s$，$f_i(x)$ 皆为 x^N+1 在 $F_q[x]$ 中的首一不可约因子。从而 $\forall c(x)\in C$，存在 $g(x),h(x)\in\Re$，使得 $c(x)=g(x)\cdot\prod_{i\in I,i是奇数}f_i^{k_i}(x)+uh(x)$，由于在 $\Re$ 中 $(x^n+1)^{p^s}=x^N+1=u\lambda$，而 λ 是可逆元，故 $u\in<(x^n+1)^{p^s}>=<\prod_{i\in I,i是奇数}f_i^{p^s}>$。因此，$C$ 包含在 $\Re$ 的某个理想 $<\prod_{i\in I,i是奇数}f_i^{\tau_i}>$ 中，这里 τ_i 皆为整数且 $0\le\tau_i\le p^sk$。对每一个奇数 $i\in I$，选择最大的 τ_i 使得 $C\subseteq<\prod_{i\in I,i是奇数}f_i^{\tau_i}>$。对每一个奇数 $i\in I$，每一个最大的 τ_i 记为 s_i，则 $0\le s_i\le p^sk$，且 $C\subseteq<\prod_{i\in I,i是奇数}f_i^{s_i}>$。由 s_i 的最大性，存在 $a(x)\in C$，使得 $a(x)=\rho(x)\prod_{i\in I,i是奇数}f_i^{s_i}$，这里 $\rho(x)$ 与 $f_i(x)$ ($\forall i\in I$ 且 i 是奇数)皆互素。由此 $\rho(x)$ 与 x^n+1 互素。由引理 4，$\rho(x)$ 是 $\Re$ 的可逆元，从而 $\prod_{i\in I,i是奇数}f_i^{s_i}\in C$，$<\prod_{i\in I,i是奇数}f_i^{s_i}>\subseteq C$。综上可得 $C=<\prod_{i\in I,i是奇数}f_i^{s_i}>$。如前所述，对每一个奇数 $i\in I$，$0\le s_i\le p^sk$。如果对某个奇数 $m\in I$，$s_m>p^sk$，记 $s_m=p^sk+v$，由引理 5 及这些 $f_i(x)$ 的两两互素性，$C=<\prod_{i\in I,i是奇数}f_i^{s_i}>=<f_m^{p^sk+v}\cdot\prod_{i\in I,i\ne m,i是奇数}f_i^{s_i}>=<f_m^{p^sk}\cdot\prod_{i\in I,i\ne m,i是奇数}f_i^{s_i}>$。 证毕

根据上述定理中 $f_i(x)$ 的两两互素性知 $<\prod_{i\in I,i是奇数}f_i^{s_i}>$，$0\le s_i\le p^sk$，是两两不同的，因此有下面的结论。

推论 1 环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上长度为 $N=p^sn$ 的 $(u\lambda-1)$-常循环码共有 $(p^sk+1)^\chi$ 个，这里 χ 即模 $2n$ 的 q-分圆陪集的个数减去模 n 的 q-分圆陪集的个数，亦即 x^n+1 在 $F_q[x]$ 中的首一不可约因子的数目。

下面给出环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上 $(u\lambda-1)$-常循环码与域 F_q 上相同码长的负循环码的汉明距离之间的联系，并给出文献[4]中环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上所有码长为 p^s 的 $(u\lambda-1)$-常循环码的汉明距离。

定理 2 设 C 是环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上长度为 $N=p^sn$ 的 $(u\lambda-1)$-常循环码，正如定理 1 所述，C 可表成 $C=<\prod_{i\in I,i是奇数}f_i^{s_i}(x)>$，这里 $0\le s_i\le p^sk$。$x^n+1=\prod_{i\in I,i是奇数}f_i(x)$ 是 x^n+1 在 $F_q[x]$ 中分解为首一不可约多项式的乘积的表达式。则

$$C\cap<u^{k-1}>=<u^{k-1}\cdot\prod_{i\in I,i是奇数}f_i^{s_i-\min\{s_i,p^s(k-1)\}}> \quad (4)$$

且记 $\overline{C}=<\prod_{i\in I,i是奇数}\overline{f}_i^{\,s_i-\min\{s_i,p^s(k-1)\}}(x)>\subseteq F_q[x]/<x^N+1>$ 时，则 C 的汉明距离 $d_H(C)$ 等于 $\overline{C}$ 的汉明距离 $d_H(\overline{C})$。

证明 在 $R[X]/<x^N+1-u\lambda>$ 中 $(x^n+1)^{p^s}=x^N+1=u\lambda$，从而 $u^{k-1}\lambda^{k-1}=\prod_{i\in I,i是奇数}f_i^{p^s(k-1)}$。注意到 λ 为可逆元，$C\cap<u^{k-1}>=<\prod_{i\in I,i是奇数}f_i^{s_i}>\cap<\prod_{i\in I,i是奇数}f_i^{p^s(k-1)}>=<\prod_{i\in I,i是奇数}f_i^{\max\{s_i,p^s(k-1)\}}>=<\prod_{i\in I,i是奇数}f_i^{p^s(k-1)}\cdot\prod_{i\in I,i是奇数}f_i^{s_i-\min\{s_i,p^s(k-1)\}}>=<u^{k-1}\cdot\prod_{i\in I,i是奇数}f_i^{s_i-\min\{s_i,p^s(k-1)\}}>$。

记 $T_{k-1}(C)=\{\overline{f(x)}\mid u^{k-1}f(x)\in C\}$。$\forall\alpha(x)\in\overline{C}$，存在 $\beta(x)\in F_q[x]$，使得

$$\alpha(x)=\beta(x)\prod_{i\in I,i\text{是奇数}}\overline{f}_i^{\,s_i-\min\{s_i,p^s(k-1)\}}$$

为简洁起见，下面记 $\tau_i=\min\{s_i,p^s(k-1)\}$。取 $\gamma(x)\in R[x]$，使得 $\overline{\gamma}(x)=\beta(x)$ (注意到 F_q 是 R 子环，取 $\gamma(x)=\beta(x)$ 亦可)，则

$$u^{k-1}\gamma(x)\prod_{i\in I,i\text{是奇数}}f_i^{\tau_i}\in<u^{k-1}\prod_{i\in I,i\text{是奇数}}f_i^{\tau_i}> \tag{5}$$

又已证明

$$<u^{k-1}\prod_{i\in I,i\text{是奇数}}f_i^{\tau_i}>=C\cap<u^{k-1}> \tag{6}$$

故 $u^{k-1}\gamma(x)\prod_{i\in I,i\text{是奇数}}f_i^{\tau_i}\in C$，从而 $\alpha(x)\in T_{k-1}(C)$。故 $\overline{C}\subseteq T_{k-1}(C)$。

再证 $T_{k-1}(C)\subseteq\overline{C}$：$\forall g(x)\in T_{k-1}(C)$，存在 $h(x)\in R[x]$，使得 $\overline{h}(x)=g(x)$ 且 $u^{k-1}h(x)\in C$，又 $u^{k-1}h(x)\in<u^{k-1}>$，从而 $u^{k-1}h(x)\in C\cap<u^{k-1}>=<u^{k-1}\prod_{i\in I,i\text{是奇数}}f_i^{\tau_i}>$，又由于 $R[x]$ 中每个多项式 $a(x)$ 可表成 $a_0(x)+ua_1(x)+\cdots+u^{k-1}a_{k-1}(x)$ 形式，其中 $a_i(x)\in F_q[x],0\le i\le k-1$，$0\le i\le k-1$，故存在 $\xi(x)\in R[x]$，使得 $g(x)=\overline{h}(x)=\overline{\xi}(x)\prod_{i\in I,i\text{是奇数}}\overline{f}_i^{\tau_i}$，从而 $g(x)\in<\prod_{i\in I,i\text{是奇数}}\overline{f}_i^{\tau_i}>=\overline{C}$。这就证明了 $\overline{C}=T_{k-1}(C)$。在文献[13]中把 $T_{k-1}(C)$ 叫做码 C 的 $k-1$ 阶挠码(即码 C 的最高阶挠码)，文献[13]深入讨论了有限链环上线性码的各阶挠码的联系及性质，已知有限链环上线性码的汉明距离等于它的最高阶挠码(它是有限链环的剩余域上的码)的汉明距离，故 C 的汉明距离 $d_H(C)$ 等于 $\overline{C}$ 的汉明距离 $d_H(\overline{C})$。证毕

关于 $n=1$ 的情形，$x+1$ 本身就是 $R[x]$ 中基本不可约多项式，即 $x+1$ 是 $F_q[x]$ 中不可约多项式。由本文的定理 1 可推出文献[4]的定理 3，即：$R[X]/<x^{p^e}+1-u\lambda>$ 是个有限链环，其所有的理想(即 R 上长为 p^e 的 $(u\lambda-1)$-常循环码)是 $<(x+1)^i>$，$i=0,1,2,\cdots,p^e\cdot k$。

关于 $C=<(x+1)^i>\subseteq R[X]/<x^{p^e}+1-u\lambda>$，$i=0,1,2,\cdots,p^e\cdot k$，由定理 2，$\overline{C}=<(x+1)^{i-\min\{i,p^e(k-1)\}}>\subseteq F_q[x]/<x^{p^e}+1>$，而在文献[14]中(见文献[14]的定理 4.11)已经完全决定了域 F_q 上码长为 p^e 的所有的负循环码的汉明距离，亦即下面的引理 6。

引理 6　设 q 是奇素数 p 的方幂，D 是域 F_q 上码长为 p^e 的非零负循环码，$\exists j:0\le j<p^e$，使得 $D=<(x+1)^j>\subseteq F_q[x]/<x^{p^e}+1>$。

$$d_H(D)=\begin{cases}1, & j=0\\ 2, & 1\le j\le p^{e-1}\\ \beta+2, & \beta p^{e-1}+1\le j\le(\beta+1)p^{e-1},\\ & 1\le\beta\le p-2\\ (\tau+1)p^k, & p^e-p^{e-\upsilon}+(\tau-1)p^{e-\upsilon-1}\\ & +1\le j\le p^e-p^{e-\upsilon}+\tau p^{e-\upsilon-1},\\ & 1\le\tau\le p-1,\ 1\le\upsilon\le e-1\end{cases} \tag{7}$$

$j=p^e$ 所对应的仅有一个码字(即零码字)的负循环码 D 的汉明距离规定为 0。

由定理 2 和引理 6，可得下面的定理 3。

定理 3　关于 $C=<(x+1)^i>\subseteq R[X]/<x^{p^e}+1-u\lambda>$，$i=0,1,2,\cdots,p^e\cdot k$，$\overline{C}=<(x+1)^{i-\min\{i,p^e(k-1)\}}>\subseteq F_q[x]/<x^{p^e}+1>$，从而

$$d_H(C)=d_H(\overline{C})=\begin{cases}1, & i\le p^e(k-1)\\ d_H(<(x+1)^{i-p^e(k-1)}>), & i>p^e(k-1)\end{cases} \tag{8}$$

当 $i>p^e(k-1)$ 时，记 $j=i-p^e(k-1)$，则

$$d_H(C)=d_H(<(x+1)^j>)=\begin{cases}2, & 1\le j\le p^{e-1}\\ \beta+2, & \beta p^{e-1}+1\le j\le(\beta+1)p^{e-1},\\ & 1\le\beta\le p-2\\ (\tau+1)p^k, & p^e-p^{e-\upsilon}+(\tau-1)p^{e-\upsilon-1}+1\\ & \le j\le p^e-p^{e-\upsilon}+\tau p^{e-\upsilon-1},\\ & 1\le\tau\le p-1,\ 1\le\upsilon\le e-1\end{cases} \tag{9}$$

3　结束语

本文给出了环 R 上任意长度 N 的所有的 $(u\lambda-1)$-常循环码的生成元，给出了环 R 上任意长度 N 的 $(u\lambda-1)$-常循环码的计数。确定了环 R 上任意长度 N 的 $(u\lambda-1)$-常循环码的的最高阶挠码的生成多项式，由此给出了环 R 上长度 p^s 的所有 $(u\lambda-1)$ -常循环码的汉明距离。一个值得探讨的问题是研究该环上其它特定长度(比如长度为 $2p^s$)的 $(u\lambda-1)$-常循环码的汉明距离和该环上各种长度的 $(u\lambda-1)$-常循环码的齐次距离。还可继续探讨环 R 上各种长度的其它常循环码的结构及其各种距离和各种重量的分布。

参 考 文 献

[1] 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.

[2] Kai Xiao-shan, Zhu Shi-xin, and Li Ping. $(1+u\lambda)$-constacyclic codes over $F_p[u]/<u^m>$ [J]. *Journal of the Franklin Institute*, 2010, 347(3): 751–762.

[3] Han Mu, Ye You-pei, Zhu Shi-xin, *et al*.. Cyclic codes over $F_p+uF_p+\cdots+u^{k-1}F_p$ with length p^sn [J]. *Information Sciences*, 2011, 181(4): 926–934.

[4] 朱士信, 李平, 吴波. 环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上一类重根常循环码[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.

[5] Dinh H Q. Constacyclic codes of length 2^s over Galois extension rings of F_2+uF_2 [J]. *IEEE Transactions on Information Theory*, 2009, 55(4): 1730–1740.

[6] 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 Min-jia, Yang Shan-lin, and Zhu Shi-xin. 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.

[7] Jitman S. Skew constacyclic codes over finite chain rings [J]. *Advances in Mathematics of Communications*, 2012, 6(1): 39–63.

[8] Dougherty S T, Karadeniz S, and Yildiz B. Cyclic codes over R_k [J]. *Designs, Codes and Crypytography*, 2012, 63(1): 113–126.

[9] Yildiz B and Karadeniz S. Cyclic codes over $F_2+uF_2+vF_2+uvF_2$ [J]. *Designs, Codes and Crypytography*, 2011, 58(3): 221–234.

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

[11] Kai Xiao-shan and Zhu Shi-xin. Negacyclic self-dual codes over finite chain rings[J]. *Designs, Codes and Crypytography*, 2012, 62(2): 161–174.

[12] Norton G H and Sălăgean A. On the structure of linear and cyclic codes over a finite chain ring[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2000, 10(2): 489–506.

[13] Dougherty S T, Kim Jon-lark, and Liu Hong-wei. Constructions of self-dual codes over finite commutative chain rings[J]. *International Journal of Information and Coding Theory*, 2010, 1(2): 171–190.

[14] Dinh H Q. On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions[J]. *Finite Fields and Their Applications*, 2008, 14(1): 22–40.

李 平： 男，1971 年生，副教授，硕士生导师，主要从事编码理论研究.

朱士信： 男，1962 年生，教授，博士生导师，主要从事编码理论及序列密码研究.

开晓山： 男，1975 年生，博士，硕士生导师，主要从事编码理论研究.