第44卷第3期 中国科学技术大学学报 Vol. 44, No. 3
2014年3月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Mar. 2014

文章编号:0253-2778(2014)03-0207-07

环 $F_2+uF_2+vF_2$ 上的一类重根常循环码

张元婷,朱士信

(合肥工业大学数学学院,安徽合肥 230009)

摘要:主要研究了环 $R=F_2+uF_2+vF_2$ 上长为 2^k 的$(1+u)$循环码,对该常循环码进行了分类,并给出了其计数公式.

关键词:环上码;常循环码;计数公式;重根码

中图分类号:TN911.22 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2014.03.007

AMS Subject Classification (2000): Primary 94B05; Secondary 94B15

引用格式: Zhang Yuanting, Zhu Shixin. A family of repeated-root constacyclic codes over $F_2+uF_2+vF_2$ [J]. Journal of University of Science and Technology of China, 2014,44(3):207-213.
张元婷,朱士信. 环 $F_2+uF_2+vF_2$ 上的一类重根常循环码[J]. 中国科学技术大学学报,2014,44(3):207-213.

A family of repeated-root constacyclic codes over $F_2+uF_2+vF_2$

ZHANG Yuanting, ZHU Shixin

(*School of Mathematics, Hefei University of Technology, Hefei* 230009, *China*)

Abstract: The $(1+u)$-cyclic codes of length 2^k over the ring $R=F_2+uF_2+vF_2$ were studied, and all such codes were classified. A formula for the number of these constacyclic codes was obtained.

Key words: codes over rings; constacyclic codes; mass formula; repeated-root codes

0 引言

1994年,Hammons等证明了某些高效的二元非线性码可以看作 Z_4 线性码在Gray映射下的二元象[1],这使得人们对有限域上的非线性码有了新的认识,同时开辟了有限环上编码理论研究的新领域.各种有限环上的线性码和循环码被人们加以定义和研究[2-5].然而这些文献一般研究的都是有限链环上的编码理论.近年来,Yildiz和Karadeniz研究了环 $F_2+uF_2+vF_2+uvF_2$ 上的线性码和循环码[6-7],并且通过定义各自的Gray映射得到了一些参数较好的二元码.由于 $F_2+uF_2+vF_2+uvF_2$ 不是有限链环,以上文献中研究码的方法在这里就不适用,它似乎更难研究.

1990年,Castagnoli等[8]和Van Lint[9]分别证明了重根循环码有链级构造,虽然它们是渐进坏码,但是在这些码中却存在最优码,这激发研究者对重根循环码进行深入的研究.环 F_2+uF_2 分享了环 Z_4 和域 F_4 很多好的性质,因其特殊的代数结构,其上的循环码和常循环码得到广泛的研究[11-13].本文研究了环 $F_2+uF_2+vF_2$ 上重根长度的$(1+u)$循环码,对该环上长为 $n=2^k$ 的$(1+u)$循环码进行了分

收稿日期:2012-03-28;**修回日期**:2012-07-06

基金项目:国家自然科学基金(61370089)资助.

作者简介:张元婷,女,1987年生,硕士生. 研究方向:代数编码. E-mail: zhang607230@163.com

通讯作者:朱士信,博士/教授. E-mail: zhushixin@hfut.edu.cn

类,并根据这个分类,给出了该长度的$(1+u)$循环码的计数公式.

1 预备知识

环 $R=F_2+uF_2+vF_2$ 满足 $u^2=v^2=0$ 和 $u\cdot v=v\cdot u=0$,显然 R 是一个特征为 2 的含有 8 个元素的可交换的非主理想环,但是它是一个局部环,其唯一的极大理想为

$$I=\{0,u,v,u+v\}.$$

R 上的单位为

$$I_1=\{1,1+u,1+v,1+u+v\},$$

R 上长为 n 的码 C 是 R^n 的一个非空子集. 若 C 是 R^n 的一个 R 子模,则称 C 为 R 上长为 n 的线性码,R^n 上的循环移位 σ 和$(1+u)$循环移位 ν 分别定义为

$$\sigma(x_0,x_1,\cdots,x_{n-1})=(x_{n-1},x_0,\cdots,x_{n-2});$$

$$\nu(x_0,x_1,\cdots,x_{n-1})=((1+u)x_{n-1},x_0,\cdots,x_{n-2}).$$

对一个码 C,若 $\sigma(C)=C$,则称 C 为循环码;若 $\nu(C)=C$,则称 C 为$(1+u)$循环码. 我们把码字

$$c=(c_0,c_1,\cdots,c_{n-1})$$

对应的多项式表示为

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

则 $x\cdot c(x)$为 $c(x)$在环 $R[x]/\langle x^n-(1+u)\rangle$中的一个$(1+u)$循环移位,所以 R 上长为 n 的$(1+u)$循环码是环 $R[x]/\langle x^n-(1+u)\rangle$的一个理想.

我们首先考虑 $S=F_2+uF_2$ 上长为 2^k 的$(1+u)$循环码,注意 S 是一个局部环,其极大理想为$\langle u\rangle$,剩余域为 F_2. 设

$$\mu:S\to F_2,\mu(r)=r(\mathrm{mod}\ u),$$

则 μ 可以自然地拓展为 $S[x]$到 $F_2[x]$中的映射. $\forall r\in S$ 可以唯一地表示为 $r=r_0+r_1u$,其中,$r_0,r_1\in F_2$,则 $\mu(r)=r_0$.

引理 1.1 设

$$a(x)\in S_{2^k}=S[x]/\langle x^{2^k}-(1+u)\rangle,$$

则

① $a(x)$可以唯一地写为

$$a(x)=a_0+a_1(x+1)+a_2(x+1)^2+\cdots+a_{2^k-1}(x+1)^{2^k-1},$$

其中,$a_i\in S,0\leqslant i\leqslant 2^k-1$.

② $a(x)$是 S_{2^k}的一个单位$\Leftrightarrow\mu(a_0)=1$.

证明 ①显然. ②对任意的 $a(x)\in S_{2^k}$,存在 $b\in F_2$,$g(x)\in S_{2^k}$,使得

$$a(x)=\mu(a_0)+ub+(x+1)g(x).$$

令

$$f(x)=ub+(x+1)g(x),$$

则

$$f(x)=a(x)-\mu(a_0).$$

由于 u和 $x+1$ 是 S_{2^k}中的幂零元,因此 $a(x)$是 S_{2^k}中的单位当且仅当 $\mu(a_0)$是一个单位,当且仅当 $\mu(a_0)=1$. □

定理 1.1[10] 环 S_{2^k}是一个有限链环,其极大理想为$\langle x+1\rangle$,剩余域为 F_2,S_{2^k}中不同的理想为$\langle(x+1)^i\rangle$,$0\leqslant i\leqslant 2^{k+1}$.

作同态映射

$$\varphi:R\to S,\varphi(a+ub+vc)=a+ub,$$

映射 φ可以拓展为

$$\varphi:R_{2^k}\to S_{2^k},$$

$$\varphi(c_0+c_1x+\cdots+c_{2^{k-1}}x^{2^{k-1}})=\varphi(c_0)+\varphi(c_1)x+\cdots+\varphi(c_{2^k-1})x^{2^k-1}.$$

引理 1.2 $\forall n\in Z^+,(x+1)^{2^n}=x^{2^n}+1\in R[x]$.

注 下文中的 n均指 2^k.

引理 1.3 设 $a(x)\in R_{2^k}$,则

① $a(x)$可以唯一地写为

$$a(x)=a_0+a_1(x+1)+a_2(x+1)^2+\cdots+a_{2^s-1}(x+1)^{2^s-1},$$

其中,$a_i\in R,0\leqslant i\leqslant 2^s-1$.

② $a(x)$是 R_{2^k}的一个单位当且仅当 $\mu\varphi(a_0)=1$.

证明 ①显然. ②若 $a(x)$是 R_{2^k}的一个单位,则 $\varphi(a(x))$是 S_{2^k}的一个单位,于是由引理 1.1 有 $\mu\varphi(a_0)=1$. 反之假设存在 $a(x)\in R_{2^k}$,使得 $\mu\varphi(a_0)=1$,则 $\varphi(a(x))$是 S_{2^k}中的一个单位,因此存在$b(x)\in R_{2^k}$,使得

$$\varphi(a(x))\varphi(b(x))=1\in S_{2^k},$$

故存在 $h(x)\in R_{2^k}$,使得

$$a(x)b(x)=1+vh(x),$$

则在 R_{2^k}中有$a(x)^2b(x)^2=1$,因此 $a(x)$是 R_{2^k}中的一个单位. □

定理 1.2 环 R_{2^k}是一个局部环,其极大理想为$\langle v,x+1\rangle$,但它不是一个链环.

证明 $\forall a(x)\in R_{2^k}$可以唯一地表示为

$$a(x)=\sum_{i=0}^{2^k-1}a_{0i}(x+1)^i+$$

$$u\sum_{i=0}^{2^k-1}a_{1i}(x+1)^i+v\sum_{i=0}^{2^k-1}a_{2i}(x+1)^i,$$

其中，$a_{0i},a_{1i},a_{2i}\in F_2$，由引理 1.3 知 $a(x)$是零因子当且仅当 $a_{00}=0$. 因此$\langle u,v,x+1\rangle$是 R_{2^k}中的零因子集，由于

$$(x+1)^{2^k}=x^{2^k}+1=u\in R_{2^k}.$$

于是在 R_{2^k}中有

$$\langle u,v,x+1\rangle=\langle v,x+1\rangle,$$

因此 R_{2^k}是一个局部环，其极大理想为$\langle v,x+1\rangle$，假设 $v\in\langle x+1\rangle$，则存在 $f(x),g(x)\in R[x]$使得

$$v=(x+1)f(x)+[x^{2^k}-(1+u)]g(x).$$

令 $x=1$，则 $v=ug(x)$，比较常数项可得到矛盾，因此 $v\notin\langle x+1\rangle$，另一方面，由于 $x+1$ 的幂零指数为 2^{k+1}，而 v 的幂零指数为 2，于是 $x+1\notin\langle v\rangle$，故 R_{2^k}不是一个主理想环，因而不是一个链环. □

2　R_{2^k} 中长为 2^k 的理想的分类

考虑 R_{2^k} 中的任意理想 I，若 $I\in\langle v\rangle$，则 I 中的任一元素必有形式 $v\sum_{i=0}^{2^k-1}b_{1i}(x+1)^i$，其中，$b_{1i}\in F_2$. 设

$$\kappa=\min\{l\mid\forall\, b=(b_{10},b_{11},\cdots,b_{1,n-1})\in I,\ b_{10}=\cdots=b_{1,l-1}=0,b_{1,l}\neq 0\},$$

因此$\forall\, c(x)\in I$，有

$$c(x)=v(x+1)^\kappa\Big(\sum_{i=\kappa}^{2^k-1}c_{1i}(x+1)^{i-\kappa}\Big),$$

即 $I\subseteq\langle v(x+1)^\kappa\rangle$.

另一方面，$\forall\, b(x)\in I$，有

$$b(x)=v(x+1)^\kappa\Big(\sum_{i=\kappa}^{2^k-1}b_{1i}(x+1)^{i-\kappa}\Big)=v(x+1)^\kappa\Big(b_{1\kappa}+\sum_{i=\kappa+1}^{2^k-1}b_{1i}(x+1)^{i-\kappa}\Big).$$

由于 $b_{1\kappa}\neq 0$，故 $b_{1\kappa}+\sum_{i=\kappa+1}^{2^k-1}b_{1i}(x+1)^{i-\kappa}$是 R_{2^k} 的可逆元，所以有

$$v(x+1)^\kappa=b(x)\Big(b_{1\kappa}+\sum_{i=\kappa+1}^{2^k-1}b_{1i}(x+1)^{i-\kappa}\Big)^{-1}\in I,$$

于是有 $I=\langle v(x+1)^\kappa\rangle$. 即在 R_{2^k}中包含在$\langle v\rangle$中的理想为$\langle v(x+1)^\kappa\rangle$，其中，$0\leqslant\kappa\leqslant 2^k$.

下面考虑 $I\not\subset\langle v\rangle$，设 I_v 表示 I 中元素模 v 组成的集合，则 I_v 是 S_{2^k}中的一个非零理想，由定理 1.1 知 S_{2^k}的理想为$\langle(x+1)^i\rangle$，其中，$0\leqslant i\leqslant 2^{k+1}-1$，所以存在 $i\in\{0,1,\cdots,2^{k+1}-1\}$，使得

$$I_v=\langle(x+1)^i\rangle\subseteq S_{2^k},$$

故存在

$$c(x)=\sum_{j=0}^{2^{k+1}-1}c_{0j}(x+1)^j+v\sum_{j=0}^{2^{k+1}-1}c_{1j}(x+1)^j$$

使得$(x+1)^i+vc(x)\in I$，其中，$c_{0j},c_{1j}\in F_2$. 则

$$(x+1)^i+v(x)=(x+1)^i+v\sum_{j=0}^{2^{k+1}-1}c_{0j}(x+1)^j=(x+1)^i+v\sum_{j=0}^{2^k-1}c_{1j}(x+1)^j.$$

下面分两类考虑：

① $0\leqslant i\leqslant 2^k-1$，则当 $0\leqslant i\leqslant l\leqslant 2^k-1$ 时，有

$$v(x+1)^l=v[(x+1)^i+v\sum_{j=0}^{2^k-1}c_{0j}(x+1)^j](x+1)^{l-i}\in I,$$

故

$$(x+1)^i+v\sum_{j=0}^{i-1}c_{0j}(x+1)^j\in I,$$

即要么

$$I=\langle(x+1)^i+v\sum_{j=0}^{i-1}c_{0j}(x+1)^j\rangle,$$

要么$\langle(x+1)^i+v\sum_{j=0}^{i-1}c_{0j}(x+1)^j\rangle$ 是 I 的真子集.

对于后者，存在

$$f(x)\in I\backslash\langle(x+1)^i+v\sum_{j=0}^{i-1}c_{0j}(x+1)^j\rangle,$$

所以存在 $g(x)\in R_{2^k}$，使得

$$0\neq h(x)=f(x)-g(x)[(x+1)^i+v\sum_{j=0}^{i-1}c_{0j}(x+1)^j]\in I,$$

其中，$h(x)$可以表示为

$$h(x)=\sum_{j=0}^{i-1}h_{0j}(x+1)^j+v\sum_{j=0}^{i-1}h_{1j}(x+1)^j,$$

其中，$h_{0j},h_{1j}\in F_2$，由于 $h(x)\bmod v$在$\langle(x+1)^i\rangle\subseteq S_{2^k}$中，因此 $h_{0j}=0$，$\forall\, 0\leqslant j\leqslant i-1$，即

$$h(x)=v\sum_{j=0}^{i-1}h_{1j}(x+1)^j,$$

由于 $h(x)\neq 0$，故存在最小的整数 k_f，$0\leqslant k_f\leqslant i-1$，使得 $h_{1k_f}\neq 0$，于是

$$h(x)=v\sum_{j=k_f}^{i-1}h_{1j}(x+1)^j=$$

$$v(x+1)^{k_f}(h_{1k_f}+v\sum_{j=k_f+1}^{i-1}h_{1j}(x+1)^{j-k_f}),$$

由于 $h_{1k_f}\neq 0$,则 $h_{1k_f}+v\sum_{j=k_f+1}^{i-1}h_{1j}(x+1)^{j-k_f}$ 是一个可逆元,因此

$$v(x+1)^{k_f}=h(x)(h_{1k_f}+v\sum_{j=k_f+1}^{i-1}h_{1j}(x+1)^{j-k_f})^{-1}\in I.$$

上述表明:对任意的

$$f(x)\in I\backslash\langle(x+1)^i+v\sum_{j=0}^{i-1}c_{0j}(x+1)^j\rangle,$$

存在 $h_{1k_f}\neq 0,0\leqslant k_f\leqslant i-1$,使得 $v(x+1)^{k_f}\in I$. 设

$$\kappa=\min\{k_f\mid f(x)\in I\backslash\langle(x+1)^i+v\sum_{j=0}^{i-1}c_{0j}(x+1)^j\rangle\},$$

明显有

$$\langle(x+1)^i+v\sum_{j=0}^{i-1}c_{0j}(x+1)^j,v(x+1)^\kappa\rangle\subseteq I,$$

而且通过构造知,对 $\forall f(x)\in I,\exists g(x)$,使得

$$f(x)-g(x)[(x+1)^i+v\sum_{j=0}^{i-1}c_{0j}(x+1)^j]\in\langle v(x+1)^\kappa\rangle,$$

所以此时有

$$I=\langle(x+1)^i+v\sum_{j=0}^{i-1}c_{0j}(x+1)^j,v(x+1)^\kappa\rangle=\langle(x+1)^i+v\sum_{j=0}^{\kappa-1}c_{0j}(x+1)^j,v(x+1)^\kappa\rangle.$$

② $2^k\leqslant i\leqslant 2^{k+1}-1$,则

$$(x+1)^i+v\sum_{j=0}^{2^k-1}c_{0j}(x+1)^j\in I,$$

即:要么

$$I=\langle(x+1)^i+v\sum_{j=0}^{2^k-1}c_{0j}(x+1)^j\rangle=\langle u(x+1)^{i-2^k}+v\sum_{j=0}^{2^k-1}c_{0j}(x+1)^j\rangle,$$

要么$\langle(x+1)^i+v\sum_{j=0}^{2^k-1}c_{0j}(x+1)^j\rangle$ 是 I 的真子集.

对于后者,存在

$$f(x)\in I\backslash\langle(x+1)^i+v\sum_{j=0}^{2^k-1}c_{0j}(x+1)^j\rangle,$$

所以存在 $g(x)\in R_{2^k}$,使得

$$0\neq h(x)=f(x)-g(x)[(x+1)^i+v\sum_{j=0}^{2^k-1}c_{0j}(x+1)^j]\in I.$$

其中,$h(x)$可以表示为

$$h(x)=\sum_{j=0}^{i-1}h_{0j}(x+1)^j+v\sum_{j=0}^{2^k-1}h_{1j}(x+1)^j,$$

其中,$h_{0j},h_{1j}\in F_2$. 由于

$$h(x)\bmod v\in\langle(x+1)^i\rangle\subseteq S_{2^k},$$

因此 $h_{0j}=0,\forall 0\leqslant j\leqslant i-1$,即

$$h(x)=v\sum_{j=0}^{2^k-1}h_{1j}(x+1)^j=v(x+1)^{k_f}(h_{1k_f}+\sum_{j=k_f+1}^{2^k-1}h_{1j}(x+1)^{j-k_f}),$$

由于 $h_{1k_f}\neq 0$,则 $h_{1k_f}+\sum_{j=k_f+1}^{2^k-1}h_{1j}(x+1)^{j-k_f}$ 是一个可逆元,故

$$v(x+1)^{k_f}=h(x)(h_{1k_f}+\sum_{j=k_f+1}^{2^k-1}h_{1j}(x+1)^{j-k_f})^{-1}\in I.$$

上述表明:

$$\forall f(x)\in I\backslash\langle(x+1)^i+v\sum_{j=0}^{2^k-1}c_{0j}(x+1)^j\rangle,\ \exists h_{1k_f}\neq 0,0\leqslant k_f\leqslant i-1,\ \text{s.t. } v(x+1)^{k_f}\in I.$$

设

$$\kappa=\min\{k_f\mid f(x)\in I\backslash\langle(x+1)^i+v\sum_{j=0}^{2^k-1}c_{0j}(x+1)^j\rangle\},$$

故有

$$\langle(x+1)^i+v\sum_{j=0}^{2^k-1}c_{0j}(x+1)^j,v(x+1)^\kappa\rangle\subseteq I,$$

而且通过构造知,对任意的 $f(x)\in I$,存在 $g(x)$ 使得

$$f(x)-g(x)[(x+1)^i+v\sum_{j=0}^{2^k-1}c_{0j}(x+1)^j]\in\langle v(x+1)^\kappa\rangle,$$

所以此时有

$$I=\langle(x+1)^i+v\sum_{j=0}^{2^k-1}c_{0j}(x+1)^j,v(x+1)^\kappa\rangle=\langle(x+1)^i+v\sum_{j=0}^{\kappa-1}c_{0j}(x+1)^j,v(x+1)^\kappa\rangle=\langle u(x+1)^{i-2^k}+v\sum_{j=0}^{\kappa-1}c_{0j}(x+1)^j,v(x+1)^\kappa\rangle.$$

命题 2.1　R 上长为 n 的理想，有

① $\langle v(x+1)^i\rangle$，其中，$0\leqslant i\leqslant 2^k$.

② $\langle (x+1)^i+v\sum_{j=0}^{i-1}(x+1)^j\rangle$，其中，$0\leqslant i\leqslant 2^k-1$，$c_j\in F_2$.

③ $\langle u(x+1)^{i-2^k}+v\sum_{j=0}^{2^k-1}c_j(x+1)^j\rangle$，其中，$2^k\leqslant i\leqslant 2^{k+1}$，$c_j\in F_2$.

④ $\langle (x+1)^i+v\sum_{j=0}^{\kappa-1}c_j(x+1)^j, v(x+1)^\kappa\rangle$，其中，$0\leqslant i\leqslant 2^k-1$，$c_j\in F_2$，$\kappa<2^k$.

⑤ $\langle u(x+1)^{i-2^k}+v\sum_{j=0}^{\kappa-1}c_j(x+1)^j, v(x+1)^\kappa\rangle$，其中，$2^k\leqslant i\leqslant 2^{k+1}$，$c_j\in F_2$，$\kappa<2^k$.

若理想为这种形式：

$$\langle (x+1)^i+v\sum_{j=0}^{i-1}c_j(x+1)^j\rangle,$$

其中，$0\leqslant i\leqslant 2^k-1$，$c_j\in F_2$，则其也可以表示为 $\langle (x+1)^i+v(x+1)^t h(x)\rangle$，其中，$0\leqslant t<i$，$h(x)$ 要么为 0 要么为单位，$h(x)$ 也可以表示为

$$h(x)=\sum_j h_j(x+1)^j, h_j\in F_2, h_0\neq 0.$$

设 T 是满足

$$v(x+1)^T\in\langle (x+1)^i+v\sum_{j=0}^{i-1}c_j(x+1)^j\rangle$$

的最小非负整数，若 $\kappa\geqslant T$，则

$$\langle (x+1)^i+v\sum_{j=0}^{\kappa-1}c_j(x+1)^j, v(x+1)^\kappa\rangle=\langle (x+1)^i+v\sum_{j=0}^{i-1}c_j(x+1)^j\rangle,$$

所以为了使得到的理想互不相同，我们假设 $\kappa<T$.

定理 2.1　R 上长为 n 的理想可以划分为以下几类：

（Ⅰ）平凡的理想：$\langle 0\rangle$，$\langle 1\rangle$.

（Ⅱ）主理想且生成元不首一：

① $\langle v(x+1)^i\rangle$，其中，$0\leqslant i\leqslant 2^k-1$.

② $\langle u(x+1)^{i-2^k}+v(x+1)^t h(x)\rangle$，其中，$2^k\leqslant i\leqslant 2^{k+1}-1$，$0\leqslant t<2^k$，$h(x)$ 为 0 或单位，$h(x)$ 可以表示为

$$h(x)=\sum_j h_j(x+1)^j, h_j\in F_2, h_0\neq 0.$$

（Ⅲ）主理想且生成元首一：

$$\langle (x+1)^i+v(x+1)^t h(x)\rangle,$$

其中，$1\leqslant i\leqslant 2^k-1$，$0\leqslant t<i$，$h(x)$ 为 0 或单位，$h(x)$ 可以表示为

$$h(x)=\sum_j h_j(x+1)^j, h_j\in F_2, h_0\neq 0.$$

（Ⅳ）非主理想且有一个生成元首一：

$$\langle (x+1)^i+v(x+1)^t h(x), v(x+1)^\kappa\rangle,$$

其中，$1\leqslant i\leqslant 2^k-1$，$T$ 是满足

$$v(x+1)^T\in[(x+1)^i+v(x+1)^t h(x)]$$

的最小非负整数，$\kappa<T$，$\deg h(x)\leqslant\kappa-t-1$.

（Ⅴ）非主理想且两个生成元均不首一：

$$\langle u(x+1)^{i-2^k}+v(x+1)^t h(x), v(x+1)^\kappa\rangle,$$

其中，$2^k\leqslant i\leqslant 2^{k+1}-1$，$\kappa<T$，$\deg h(x)\leqslant\kappa-t-1$.

3　R_{2^k} 中长为 2^k 的理想的个数的计数公式

引理 3.1　设 T 是满足

$$v(x+1)^T\in\langle (x+1)^i+v(x+1)^t h(x)\rangle$$

的最小非负整数，则当 $1\leqslant i\leqslant 2^k-1$ 时，$T=i$. 当 $2^k\leqslant i\leqslant 2^{k+1}-1$ 时，

$$T=\begin{cases}2^k, & \text{若 } h(x)=0;\\ \min\{2^k, 2^{k+1}-i+t\}, & \text{若 } h(x)\neq 0.\end{cases}$$

证明　当 $1\leqslant i\leqslant 2^k-1$ 时由于

$$v(x+1)^i=v[(x+1)^i+v(x+1)^t h(x)]\in C,$$

故 $T\leqslant i$. 若 $h(x)=0$，则 $T=i$. 若 $h(x)\neq 0$，则 $h(x)$ 是 R_{2^k} 的一个单位，因为

$$v(x+1)^T\in\langle (x+1)^i+v(x+1)^t h(x)\rangle,$$

则存在 $f(x)\in R_{2^k}$，使得

$$v(x+1)^T=f(x)[(x+1)^i+v(x+1)^t h(x)].$$

其中，$f(x)$ 可以表示为

$$f(x)=\sum_{j=0}^{2^{k+1}-1}b_{0j}(x+1)^j+v\sum_{j=0}^{2^k-1}b_{1j}(x+1)^j,$$

其中，$b_{0j}, b_{1j}\in F_2$. 则

$$v(x+1)^T=\Big[\sum_{j=0}^{2^{k+1}-1}b_{0j}(x+1)^j+v\sum_{j=0}^{2^k-1}b_{1j}(x+1)^j\Big]\cdot[(x+1)^i+v(x+1)^t h(x)]=$$

$$(x+1)^i\sum_{j=0}^{2^{k+1}-1}b_{0j}(x+1)^j+$$

$$v(x+1)^i\sum_{j=0}^{2^k-1}b_{1j}(x+1)^j+$$

$$v(x+1)^t h(x)\sum_{j=0}^{2^k-1} b_{0j}(x+1)^j =$$
$$(x+1)^i \sum_{j=0}^{2^{k+1}-i-1} b_{0j}(x+1)^j +$$
$$(x+1)^{2^{k+1}} \sum_{j=2^{k+1}-i}^{2^{k+1}} b_{0j}(x+1)^{i+j-2^{k+1}} +$$
$$v(x+1)^i \sum_{j=0}^{2^k-1} b_{1j}(x+1)^j +$$
$$v(x+1)^t h(x)\sum_{j=0}^{2^k-1} b_{0j}(x+1)^j =$$
$$v(x+1)^i \sum_{j=0}^{2^k-1} b_{1j}(x+1)^j.$$

于是 $T\geqslant i$, 故 $T=i$. 对于 $2^k\leqslant i\leqslant 2^{k+1}-1$ 可类似地讨论. □

定理 3.1 R 上长为 2^k 的$(1+u)$循环码共有 $2^{2^k+3}-3\cdot 2^k-7$ 个.

证明 (Ⅰ) 平凡理想有:$\langle 0\rangle$,$\langle 1\rangle$共 2 个且互不相同.

(Ⅱ) 主理想且生成元不首一:

(ⅰ) $\langle v(x+1)^i\rangle$,其中,$0\leqslant i\leqslant 2^k-1$. 所以不同的码个数为 2^k.

(ⅱ) $\langle u(x+1)^{i-n}+v(x+1)^t h(x)\rangle$,其中,$2^k\leqslant i\leqslant 2^{k+1}-1$,$0\leqslant t<2^k$,$h(x)$为 0 或单位.

① 若 $h(x)=0$,则$(1+u)$循环码的形式为 $\langle u(x+1)^{i-n}\rangle$,其中,$2^k\leqslant i\leqslant 2^{k+1}-1$,所以不同的码个数为 2^k.

② 若 $h(x)\neq 0$,则 $h(x)$为单位,可以表示为

$$h(x)=\sum_j h_j(x+1)^j,$$

其中,$h_j\in F_2$,$h_0\neq 0$,$T=\min\{2^k,2^{k+1}+t-i\}$,为了得到不同的理想,我们假设 $t+j<T$,即 $0\leqslant j\leqslant T-t-1$,所以不同的码个数为

$$\sum_{i=2^k+1}^{2^{k+1}-1}\sum_{t=0}^{i-2^k-1} 2^{2^{k+1}-i-1}+\sum_{i=2^k}^{2^{k+1}-1}\sum_{t=i-2^k}^{2^k-1} 2^{2^k-t-1}=$$
$$3\cdot 2^{2^k}-2^{k+1}-3.$$

(Ⅲ) 主理想且生成元首一:

$$\langle (x+1)^i+v(x+1)^t h(x)\rangle,$$

其中,$1\leqslant i\leqslant 2^k-1$,$0\leqslant t<i$,$h(x)$为 0 或单位.

① 若 $h(x)=0$,则$(1+u)$循环码的形式为 $\langle (x+1)^i\rangle$,其中,$1\leqslant i\leqslant 2^k-1$,所以不同的码个数为 2^k-1.

② 若 $h(x)\neq 0$,则 $h(x)$为单位,可以表示为

$$h(x)=\sum_j h_j(x+1)^j,$$

其中,$h_j\in F_2$,$h_0\neq 0$,$T=i$,为了得到不同的理想,我们假设 $t+j<T$,即 $0\leqslant j\leqslant i-t-1$,所以不同的码个数为

$$\sum_{i=1}^{2^k-1}\sum_{t=0}^{i-1} 2^{i-t-1}=2^{2^k}-2^k-1.$$

(Ⅳ) 非主理想且有一个生成元首一:

$$\langle (x+1)^i+v(x+1)^t h(x),v(x+1)^\kappa\rangle,$$

其中,$1\leqslant i\leqslant 2^k-1$. T 是满足

$$v(x+1)^T\in[(x+1)^i+v(x+1)^t h(x)]$$

的最小非负整数,$\kappa<T$,$\deg h(x)\leqslant\kappa-t-1$.

① 若 $h(x)=0$,则这种形式的$(1+u)$循环码为 $\langle (x+1)^i,v(x+1)^\kappa\rangle$,其中,$1\leqslant i\leqslant 2^k-1$,$\kappa<i$,所以不同的码个数为

$$\sum_{i=1}^{2^k-1} i=2^{2k-1}-2^{k-1}.$$

② 若 $h(x)\neq 0$,则 $h(x)$为单位,可以表示为

$$h(x)=\sum_j h_j(x+1)^j,$$

其中,$h_j\in F_2$,$h_0\neq 0$,$T=i$,为了得到不同的理想,我们假设 $t+j<\kappa$,即 $0\leqslant j\leqslant\kappa-t-1$,所以不同的理想个数为

$$\sum_{i=2}^{2^k-1}\sum_{t=0}^{i-2}\sum_{\kappa=t+1}^{i-1} 2^{\kappa-t-1}=2^{2^k}-2^{2k-1}-2^{k-1}-1.$$

(Ⅴ) 非主理想且两个生成元均不首一:

$$\langle u(x+1)^{i-2^k}+v(x+1)^t h(x),v(x+1)^\kappa\rangle,$$

其中,$2^k\leqslant i\leqslant 2^{k+1}-1$,$\kappa<T$,$\deg h(x)\leqslant\kappa-t-1$.

① 若 $h(x)=0$,则这种形式的$(1+u)$循环码为 $\langle u(x+1)^{i-2^k},v(x+1)^\kappa\rangle$,其中,$2^k\leqslant i\leqslant 2^{k+1}-1$,$T=2^k$,所以不同的码个数为

$$\sum_{i=2^k}^{2^{k+1}-1} 2^k=2^{2k}.$$

② 若 $h(x)\neq 0$,则 $h(x)$为单位,可以表示为

$$h(x)=\sum_j h_j(x+1)^j,$$

其中,$h_j\in F_2$,$h_0\neq 0$,$T=\min\{2^k,2^{k+1}-i+t\}$,为了得到不同的理想,我们假设 $t+j<\kappa$,即 $0\leqslant j\leqslant\kappa-t-1$,所以不同的理想个数为

$$\sum_{i=2^k+1}^{2^{k+2}-2}\sum_{t=0}^{i-2^k-1}\sum_{\kappa=t+1}^{2^{k+1}+t-i-1} 2^{\kappa-t-1}+\sum_{i=2^k}^{2^{k+1}-2}\sum_{t=i-2^k}^{2^k-2}\sum_{\kappa=t+1}^{2^k-1} 2^{\kappa-t-1}=$$
$$3\cdot 2^{2^k}-2^{k+1}-2^{2k}-3.$$

综上所述，R 长为 2^k 的$(1+u)$循环码共有 $2^{2^k+3}-3\cdot 2^k-7$ 个.

4 结论

我们对 $R=F_2+uF_2+vF_2$ 上长为 2^k 的$(1+u)$循环码进行了分类，并给出了 R 上长为 2^k 的循环码个数的计数公式. 该环及其扩环上的其他的常循环码的分类和计数有待进一步研究，还可以考虑其他的性质.

参考文献(References)

[1] Hammons A R, Kumar P V, Calderbank A R, et al. The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes[J]. IEEE Trans Inform Theory, 1994, 40(2): 301-319.

[2] Calderbank A R, Sloane N J A. Modular and p-adic cyclic codes[J]. Des Codes Crypotogr, 1995, 6(1): 21-35.

[3] Kanwar P, López-Permouth S R. Cyclic codes over the integer modulo p^m[J]. Finite Fields Appl, 1997, 3(4): 334-352.

[4] Norton G H, Sălăgean A. On the structure of linear and cyclic codes over finite chain ring[J]. Applicable Algebra in Engineering, Communication and Computing, 2000, 10(6): 489-506.

[5] Dinh H Q, López-Permouth S R. Cyclic and negacyclic codes over finite chain rings[J]. IEEE Trans Inform Theory, 2004, 50(8): 1 728-1 744.

[6] Yildiz B, Karadenniz S. Linear codes over $F_2+uF_2+vF_2+uvF_2$[J]. Des Codes Crypotogr, 2010, 54(1): 61-81.

[7] Yildiz B, Karadenniz S. Cyclic codes over $F_2+uF_2+vF_2+uvF_2$[J]. Des Codes Crypotogr, 2011, 58(3): 221-234.

[8] Castagnoli G, Massey J L, Schoeller P A, et al. On repeated-root cyclic codes[J]. IEEE Trans Inform Theory, 1991, 37(2): 337-342.

[9] Van Lint J H. Repeated-root cyclic codes[J]. IEEE Trans Inform Theory, 1991, 37(2): 343-345.

[10] Abualrub T, Siap I. Constacyclic codes over F_2+uF_2[J]. J Frank Inst, 2009, 346:520-529.

[11] Abualrub T, Siap I. Cyclic codes over the rings Z_2+uZ_2 and $Z_2+uZ_2+u^2Z_2$[J]. Des Codes Crypt, 2007, 42(3): 273-287.

[12] Bonnecaze A, Udaya P. Cyclic codes and self-dual codes over F_2+uF_2[J]. IEEE Trans Inform Theory, 1999, 45(4):1 250-1 255.

[13] Li Ping, Zhu Shixin. Cyclic codes of length 2^e over F_2+uF_2[J]. Journal of Electronics & Information Technology, 2007, 29(5): 1 124-1 126.
李平，朱士信. 环 F_2+uF_2 上长为 2^e 的循环码[J]. 电子与信息学报, 2007, 29(5): 1 124-1 126.