环 Z_{2^m} 上一类常循环码的挠码及其应用

朱士信[1,2],孙中华[1],开晓山[1,2]
(1. 合肥工业大学数学学院,安徽合肥 230009;2. 东南大学移动通信国家重点实验室,江苏南京 210096)

摘 要: 该文研究了环 Z_{2^m} 上任意长的 $(1+2\lambda)$-常循环码的挠码及其应用. 首先,给出环 Z_{2^m} 上 $(1+2\lambda)$-常循环码的挠码. 然后,利用挠码得到环 Z_{2^m} 上某些 $(1+2\lambda)$-常循环码的齐次距离分布. 同时,利用挠码证明了环 Z_{2^m} 上 $(2^{m-1}-1)$-常循环自对偶码都是类型 I 码,并利用这类码构造了极优的类型 I 码.

关键词: 常循环码; 挠码; 自对偶码; 距离分布
中图分类号: TN911.22 **文献标识码:** A **文章编号:** 0372-2112 (2016)08-1826-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.08.008

Torsion Codes of a Class of Constacyclic Codes over Z_{2^m} and Their Applications

ZHU Shi-xin[1,2], SUN Zhong-hua[1], KAI Xiao-shan[1,2]
(1. *School of Mathematics, Hefei University of Technology, Hefei, Anhui* 230009, *China*;
2. *National Mobile Communications Research Laboratory, Southeast University, Nanjing, Jiangsu* 210096, *China*)

Abstract: The torsion codes and their applications of $(1+2\lambda)$-constacyclic codes over the ring Z_{2^m} of arbitrary lengths are studied. The torsion codes of $(1+2\lambda)$-constacyclic codes over Z_{2^m} are given firstly. Then by using the torsion codes, the homogeneous distance of some $(1+2\lambda)$-constacyclic codes is obtained and it is proved that all $(2^{m-1}-1)$-constacyclic self-dual codes over Z_{2^m} are Type I. Some extreme Type I codes are constructed from such constacyclic codes.

Key words: constacyclic codes; torsion codes; self-dual codes; distance distribution

1 引言

上世纪九十年代,Hammons 等人在文献[1]中证明了一些高效的二元非线性码 Kerdock 码与 Preparata 码可以看作是 Z_4 - 线性码的二元像,从而使有限环上编码理论获得了突破进展. 自此,许多学者对有限环上的纠错码进行了广泛而深入的研究. 众所周知,码的距离是衡量码的纠错性能的一个重要参数. 文献[2]完全计算了 Z_{2^s} 上长为 2^s 的 λ - 常循环码的 Hamming 距离、齐次距离、Lee 距离和欧几里得距离,其中 λ 为 Z_{2^s} 上形如 $(4k-1)$ 的单位;文献[3]计算了 $GR(2^a,m)$ 上长为 2^s 的负循环码的 Hamming 重量;文献[4]计算了 F_2+uF_2 上长为 2^e 的循环码的各种距离分布. 通常,确定有限环上线性码的各种距离是比较困难的. Norton 与 Sălăgean 在文献[5]中引入了有限链环上的线性码 C 的挠码概念,证明了 C 的 Hamming 距离等于它最高阶挠码的 Hamming 距离. 后来,Doughert 与 Park[6] 将挠码用于研究 Z_{p^m} 上循环码的结构;文献[7]利用挠码给出了环 $F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$ 上任意长 $(1+u)$ - 常循环码的齐次距离分布. 由此可见,挠码在研究有限链环上线性码中起着重要作用. 因此,确定有限链环上线性码的挠码是十分必要的. 本文确立了整数剩余类环 Z_{2^m} 上任意长度的 $(1+2\lambda)$ - 常循环码的挠码,然后将挠码应用于两方面:(1)研究了 Z_{2^m} 上 $(1+2\lambda)$ - 常循环码的 Hamming 距离、齐次距离与欧几里得距离;(2)研究了 Z_{2^m} 上 $(2^{m-1}-1)$ - 常循环自对偶码,证明了这类常循环码是类型 I 码,并且利用这类码构造了极优类型 I 码.

2 预备知识

设 Z_{2^m} 表示整数模 2^m 的剩余类环,对任意 $a\in Z_{2^m}$,

收稿日期:2015-01-08;修回日期:2015-09-07;责任编辑:蓝红杰
基金项目:国家自然科学基金(No. 61370089);安徽省自然科学基金(No. 1508085SQA198, No. 1508085MA13, No. 1408085QF116);2014 年安徽省高校优秀青年支持计划;东南大学移动通信国家重点实验室开放研究基金(No. 2014D04)

用 $\bar{a}$ 表示 a 模 2 约化. 设 $Z_{2^m}[x]$ 表示 Z_{2^m} 上多项式环,对任意 $f(x)\in Z_{2^m}[x]$,用 $\bar{f}(x)$ 表示 $f(x)$ 模 2 约化. 若 $\bar{f}(x)$ 在 $F_2[x]$ 中不可约,则称 $f(x)$ 在 $Z_{2^m}[x]$ 中基本不可约. $Z_{2^m}^N$ 的任意子集 C 叫做 Z_{2^m} 上长为 N 的码. 对任意 $C\subseteq Z_{2^m}^N$,定义 $\bar{C}=\{\bar{\boldsymbol{c}}\,|\,\boldsymbol{c}\in C\}$;对任意 $0\leqslant\gamma\leqslant m-1$,定义码 $(C:2^\gamma)=\{\boldsymbol{c}\in Z_{2^m}^N\,|\,2^\gamma\boldsymbol{c}\in C\}$. 当 C 为 $Z_{2^m}^N$ 的 Z_{2^m} - 子模时,称 C 为 Z_{2^m} 上长为 N 的线性码. 设 C 是 Z_{2^m} 上长为 N 的线性码,对任意 $0\leqslant i\leqslant m-2$,容易验证 $\overline{(C:2^i)}\subseteq(C:2^{i+1})$ 且 $\overline{(C:2^i)}\subseteq\overline{(C:2^{i+1})}$. 二元线性码 $\overline{(C:2^\gamma)}$ 称为 C 的 γ 次挠码,通常 $\bar{C}=\overline{(C:2^0)}$ 称为 C 的剩余码,记为 $\mathrm{Res}(C)$. 对 Z_{2^m} 上长为 N 的线性码,文献[6]证明了 $|C|=\prod_{\gamma=0}^{m-1}|\overline{(C:2^\gamma)}|$.

对 Z_{2^m} 上的单位 η,定义常循环移位 $\tau_\eta(c_0,c_1,\cdots,c_{N-1})=(\eta c_{N-1},c_0,\cdots,c_{N-2})$. 若 Z_{2^m} 上长为 N 的线性码 C 满足 $\tau_\eta(C)=C$,则称 C 为 Z_{2^m} 上长为 N 的 η - 常循环码. 若将 C 中每个码字 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{N-1})$ 看作是多项式 $c(x)=\sum_{i=0}^{N-1}c_ix^i$,则 C 是 Z_{2^m} 上长为 N 的 η - 常循环码当且仅当 C 是商环 $Z_{2^m}[x]/\langle x^N-\eta\rangle$ 的理想. 对任意的 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{N-1})$,$\boldsymbol{d}=(d_0,d_1,\cdots,d_{N-1})\in Z_{2^m}^N$,定义 $\boldsymbol{c}$ 与 $\boldsymbol{d}$ 的欧几里得内积为 $\boldsymbol{c}\cdot\boldsymbol{d}=\sum_{i=0}^{N-1}c_id_i$. Z_{2^m} 上长为 N 的线性码 C 的对偶码定义为 $C^\perp=\{\boldsymbol{c}\in Z_{2^m}^N\,|\,\boldsymbol{c}\cdot\boldsymbol{d}=0,\forall\boldsymbol{d}\in C\}$. 文献[8]证明,若 C 为 Z_{2^m} 上长为 N 的 η - 常循环码,则 $C^\perp$ 为 Z_{2^m} 上长为 N 的 η^{-1} - 常循环码. 若 $C\subseteq C^\perp$,则称 C 为自正交码;若 $C=C^\perp$,则称 C 为自对偶码. 设 C 为 Z_{2^m} 上长为 N 的 η - 常循环码,对 $0\leqslant\gamma\leqslant m-1$,容易证明 $\overline{(C:2^\gamma)}$ 是长为 N 的二元循环码. 本文中,$\eta=1+2\lambda\in Z_{2^m}$,其中 λ 是 Z_{2^m} 中的单位. 对于 Z_{2^m} 上长为 N 的 η - 常循环码,其中 $N=2^sn,s\geqslant 0$,n 是奇数,文献[9]给出了 Z_{2^m} 上长为 N 的 η - 常循环码的结构.

定理 1[9]　设 $x^n-1=\prod_{i=1}^{r}f_i(x)$,其中 $f_i(x)$ 是 x^n-1 在 Z_{2^m} 上的首一基本不可约因子. 若 C 是 Z_{2^m} 上长为 N 的 η - 常循环码,则

$$C=\left\langle\prod_{i=1}^{r}f_i(x)^{k_i}\right\rangle,$$

其中 $0\leqslant k_i\leqslant 2^sm$,且 $|C|=2^{\sum_{i=1}^{r}(2^sm-k_i\deg f_i)}$.

3　环 Z_{2^m} 上 $(1+2\lambda)$ - 常循环码的挠码

为了计算 Z_{2^m} 上 η - 常循环码的挠码,其中 $\eta=1+2\lambda\in Z_{2^m}$,$\lambda$ 是 Z_{2^m} 中的单位. 首先给出几个重要的引理. 记 $R=Z_{2^m}[x]/\langle x^N-\eta\rangle$.

引理 1　在 R 中,$\langle(x^n-1)^{2^r}\rangle=\langle 2\rangle$.

证明　对 l 归纳可证,$(x^n-1)^{2^l}=x^{n2^l}+1-2\alpha_l(x^n)$,其中 $\alpha_l(x^n)$ 为 R 中可逆多项式. 再取 $l=s$ 得,$(x^n-1)^{2^s}=2(1+\lambda-\alpha_s(x^n))$. 因 λ 为 Z_{2^m} 的单位,所以 $1+\lambda-\alpha_s(x^n)$ 为 R 的单位,从而推出 $\langle(x^n-1)^{2^r}\rangle=\langle 2\rangle$.

引理 2　设 $C=\left\langle\prod_{i=1}^{r}f_i(x)^{k_i}\right\rangle$ 是 Z_{2^m} 上长为 N 的 η - 常循环码,其中 $f_i(x)$ 是 x^n-1 在 Z_{2^m} 上的首一不可约因子且 $0\leqslant k_i\leqslant 2^sm$,则对任意 $0\leqslant\gamma\leqslant m-1$,$\left\langle\prod_{i=1}^{r}f_i(x)^{\theta_i^{(\gamma)}}\right\rangle\subseteq(C:2^\gamma)$,其中 $\theta_i^{(\gamma)}=k_i-\min\{2^s\gamma,k_i\}$.

证明　对任意 $f(x)\in\left\langle\prod_{i=1}^{r}f_i(x)^{\theta_i^{(\gamma)}}\right\rangle$,存在 $a(x)\in R$ 使得 $f(x)=a(x)\prod_{i=1}^{r}f_i(x)^{\theta_i^{(\gamma)}}$. 由引理 1 知,存在可逆多项式 $b(x)\in R$ 使得 $2=b(x)(x^n-1)^{2^r}$. 所以,

$$\begin{aligned}2^\gamma f(x)&=2^\gamma a(x)\prod_{i=1}^{r}f_i(x)^{\theta_i^{(\gamma)}}\\&=b(x)^\gamma(x^n-1)^{2^r\gamma}a(x)\prod_{i=1}^{r}f_i(x)^{\theta_i^{(\gamma)}}\\&=b(x)^\gamma a(x)\prod_{i=1}^{r}f_i(x)^{2^r\gamma+\theta_i^{(\gamma)}}.\end{aligned}$$

因为 $\theta_i^{(\gamma)}=k_i-\min\{2^s\gamma,k_i\}$,所以 $2^s\gamma+\theta_i^{(\gamma)}\geqslant k_i$,从而 $2^\gamma f(x)\in C$. 由此推出 $f(x)\in(C:2^\gamma)$. 因此,$\left\langle\prod_{i=1}^{r}f_i(x)^{\theta_i^{(\gamma)}}\right\rangle\subseteq(C:2^\gamma)$.

定理 2　设 $C=\left\langle\prod_{i=1}^{r}f_i(x)^{k_i}\right\rangle$ 是 Z_{2^m} 上长为 N 的 η - 常循环码,其中 $f_i(x)$ 是 x^n-1 在 Z_{2^m} 上的首一不可约因子且 $0\leqslant k_i\leqslant 2^sm$,则对任意 $0\leqslant\gamma\leqslant m-1$,$\left\langle\prod_{i=1}^{r}\bar{f}_i(x)^{\tau_i^{(\gamma)}}\right\rangle=\overline{(C:2^\gamma)}$,其中 $\tau_i^{(\gamma)}=\min\{2^s(\gamma+1),k_i\}-\min\{2^s\gamma,k_i\}$.

证明　由引理 2 得,$\left\langle\prod_{i=1}^{r}\bar{f}_i(x)^{\tau_i^{(\gamma)}}\right\rangle\subseteq\overline{(C:2^\gamma)}$. 对每个 $\bar{f}_i(x)$,由于 n 为奇数,则 $\bar{f}_i(x)$ 与 $(x^n-1)/\bar{f}_i(x)=\bar{h}_i(x)$ 在 $F_2[x]$ 中互素. 所以,在 $F_2[x]/\langle x^N-1\rangle$ 中,存在 $a(x),b(x)\in F_2[x]$ 使得 $a(x)\bar{f}_i(x)^l+b(x)\bar{h}_i(x)=1$. 从而

$$a(x)\bar{f}_i(x)^{2^r+l}=\bar{f}_i(x)^{2^r}-b(x)\bar{f}_i(x)^{2^r-1}(x^n-1)$$

即 $a(x)\bar{f}_i(x)^{2^r+l}=\bar{f}_i(x)^{2^r}$. 所以,$\langle\bar{f}_i(x)^{2^r}\rangle=\langle\bar{f}_i(x)^{2^r+l}\rangle$,其中 l 为任意非负整数. 由此推出

$$\left\langle\prod_{i=1}^{r}\bar{f}_i(x)^{\theta_i^{(\gamma)}}\right\rangle=\left\langle\prod_{i=1}^{r}\bar{f}_i(x)^{\tau_i^{(\gamma)}}\right\rangle$$

其中 $\tau_i^{(\gamma)}=\min\{2^s,\theta_i^{(\gamma)}\}=\min\{2^s(\gamma+1),k_i\}-\min\{2^s\gamma,k_i\}$. 从而,

$$|\overline{(C;2^\gamma)}|\geqslant\left|\left\langle\prod_{i=1}^{r}\bar{f}_i(x)^{\tau_i^{(\gamma)}}\right\rangle\right|=2^{2^sn-\sum_{i=1}^{r}\tau_i^{(\gamma)}\deg(f_i)}.$$

故 $|C|=\prod_{\gamma=0}^{m-1}|\overline{(C;2^\gamma)}|\geqslant\prod_{\gamma=0}^{m-1}2^{2^sn-\sum_{i=1}^{r}\tau_i^{(\gamma)}\deg(f_i)}$ 且

$$\prod_{\gamma=0}^{m-1}2^{2^sn-\sum_{i=1}^{r}\tau_i^{(\gamma)}\deg(f_i)}=2^{2^snm-\sum_{\gamma=0}^{m-1}\sum_{i=1}^{r}\tau_i^{(\gamma)}\deg(f_i)}=2^{2^snm-\sum_{i=1}^{r}k_i\deg(f_i)}.$$

而由定理 1 知, $|C|=2^{2^snm-\sum_{i=1}^{r}k_i\deg(f_i)}$. 因此,对任意 $0\leqslant\gamma\leqslant m-1$, $\overline{(C;2^\gamma)}=\left\langle\prod_{i=1}^{r}\bar{f}_i(x)^{\tau_i^{(\gamma)}}\right\rangle$.

从定理 2 可得,当 $\gamma=0$ 时, $\mathrm{Res}(C)=\left\langle\prod_{i=1}^{r}\bar{f}_i(x)^{\tau_i^{(0)}}\right\rangle$,其中 $\tau_i^{(0)}=\min\{2^s,k_i\}$;当 $\gamma=m-1$ 时, $\overline{(C;2^{m-1})}=\left\langle\prod_{i=1}^{r}\bar{f}_i(x)^{\tau_i^{(m-1)}}\right\rangle$,其中 $\tau_i^{(m-1)}=k_i-\min\{2^s(m-1),k_i\}$. 特别地,当 $0\leqslant\max_{1\leqslant i\leqslant r}\{k_i\}\leqslant2^s(m-1)$ 时, $\overline{(C;2^{m-1})}=\langle1\rangle$. 记 $\delta=\min_{1\leqslant i\leqslant r}\{k_i\}$,若 $C\neq\{\mathbf{0}\}$,即 $0\leqslant\delta<2^sm$,则存在 $0\leqslant\gamma_0\leqslant m-1$ 使得, $2^s\gamma_0\leqslant\delta<2^s(\gamma_0+1)$.

推论 1 设 $C=\left\langle\prod_{i=1}^{r}f_i(x)^{k_i}\right\rangle$ 是 Z_{2^n} 上长为 N 的 η -常循环码且整数 γ_0 满足 $2^s\gamma_0\leqslant\min_i\{k_i\}<2^s(\gamma_0+1)$,则 γ_0 是使得 $\overline{(C;2^\gamma)}\neq\{\mathbf{0}\}$ 最小的非负整数.

4 挠码的应用

4.1 环 Z_{2^m} 上 $(1+2\lambda)$ -常循环码的齐次距离

由于齐次距离在有限链环上有许多重要的应用,从而引起研究者们的关注. 下面利用挠码确定某些 Z_{2^n} 上 η -常循环码的确切的齐次距离,对一般 Z_{2^n} 上的 η -常循环码,给出齐次距离的一个界.

定义 1[2] 环 Z_{2^n} 上的齐次重量定义为 Z_{2^n} 上的重量函数

$$Wt_{Hom}:Z_{2^n}\to N,r\mapsto\begin{cases}0,\text{若 } r=0\\2^{m-2},\text{若 } r\neq0,r\neq2^{m-1}\\2^{m-1},\text{若 } r=2^{m-1}\end{cases}.$$

环 Z_{2^n} 上码字的齐次重量定义为它各分量齐次重量的和. 对任意 $0\leqslant\gamma\leqslant m-1$,用 d_γ 表示 $\overline{(C;2^\gamma)}$ 的最小汉明距离. 对任意的非零码 C,设 γ_0 是使得 $\overline{(C;2^\gamma)}\neq\{\mathbf{0}\}$ 的最小值,显然, $d_{\gamma_0}\geqslant d_{\gamma_0+1}\geqslant\cdots\geqslant d_{m-1}$. 由文献[5]可知 $d_H(C)=d_{m-1}$. 记 $d_{Hom}(C)$ 表示 C 的最小齐次距离. 下面利用汉明距离,给出齐次距离的一个界.

定理 3 设 $C=\left\langle\prod_{i=1}^{r}f_i(x)^{k_i}\right\rangle$ 是 Z_{2^n} 上长为 N 的 η -常循环码,其中 $f_i(x)$ 是 x^n-1 在 Z_{2^n} 上的首一不可约因子且 $0\leqslant k_i\leqslant2^sm$. 令 γ_0 满足 $2^s\gamma_0\leqslant\min_{1\leqslant i\leqslant r}\{k_i\}<2^s(\gamma_0+1)$,则

(1) 当 $\gamma_0\leqslant m-2$ 时, $2^{m-2}d_{\gamma_0}\leqslant d_{\mathrm{Hom}}(C)\leqslant2^{m-1}d_{m-1}$.

(2) 当 $\gamma_0=m-1$ 时, $d_{\mathrm{Hom}}(C)=2^{m-1}d_{m-1}$.

证明 对 C 中的任意非零码字 $\boldsymbol{c}$,由推论 1 知, $\boldsymbol{c}$ 可以表示为 $\boldsymbol{c}=2^{\gamma_0}(c_0,c_1,\cdots,c_{N-1})$,其中 $(c_0,c_1,\cdots,c_{N-1})\in Z_{2^n}^N$. 显然 $d_H(\boldsymbol{c})\geqslant d_{\gamma_0}$. 所以,当 $\gamma_0\leqslant m-2$ 时, $d_{\mathrm{Hom}}(\boldsymbol{c})\geqslant2^{m-2}d_{\gamma_0}$,由此推出 $d_{\mathrm{Hom}}(C)\geqslant2^{m-2}d_{\gamma_0}$. 当 $\gamma_0=m-1$, $d_{\mathrm{Hom}}(\boldsymbol{c})\geqslant2^{m-1}d_{m-1}$,由此推出 $d_{\mathrm{Hom}}(C)\geqslant2^{m-1}d_{m-1}$.

另一方面,存在 $(c_0,c_1,\cdots,c_{N-1})\in Z_{2^n}^N$,使得 $\boldsymbol{c}'=2^{m-1}(c_0,c_1,\cdots,c_{N-1})\in C$,且 $d_H(\boldsymbol{c}')=d_{m-1}$,注意到 $d_{\mathrm{Hom}}(\boldsymbol{c}')=2^{m-1}d_H(\boldsymbol{c}')$,所以 $d_{\mathrm{Hom}}(C)\leqslant2^{m-1}d_{m-1}$. 所以,当 $\gamma_0\leqslant m-2$ 时, $2^{m-2}d_{\gamma_0}\leqslant d_{\mathrm{Hom}}(C)\leqslant2^{m-1}d_{m-1}$;当 $\gamma_0=m-1$ 时, $d_{\mathrm{Hom}}(C)=d_{\mathrm{Hom}}(C)=2^{m-1}d_{m-1}$.

推论 2 设 $C=\left\langle\prod_{i=1}^{r}f_i(x)^{k_i}\right\rangle$ 是 Z_{2^n} 上长为 N 的 η -常循环码,其中 $f_i(x)$ 是 x^n-1 在 Z_{2^n} 上的首一不可约因子且 $0\leqslant k_i\leqslant2^sm$. 令 $\sigma=\max_{1\leqslant i\leqslant r}\{k_i\}$,则

(1) 当 $0\leqslant\sigma\leqslant2^s(m-2)$ 时, $d_{\mathrm{Hom}}(C)=2^{m-2}$.

(2) 当 $2^s(m-2)+1\leqslant\sigma\leqslant2^s(m-1)$ 时, $d_{\mathrm{Hom}}(C)=2^{m-1}$.

证明 当 $0\leqslant\sigma\leqslant2^s(m-2)$ 时,由定理 2 得 $\overline{(C;2^{m-2})}=\langle1\rangle$,所以 $d_{\gamma_0}\geqslant d_{m-2}=1$. 由定理 3 得 $2^{m-2}\leqslant d_{\mathrm{Hom}}(C)$. 注意到 $\prod_{i=1}^{r}f_i(x)^{2^s(m-2)}=(x^n-1)^{2^s(m-2)}\in C$,根据引理 1 得 $2^{m-2}\in C$. 所以, $d_{\mathrm{Hom}}(C)\leqslant2^{m-2}$. 由此推出 $d_{\mathrm{Hom}}(C)=2^m$.

当 $2^s(m-2)+1\leqslant\sigma\leqslant2^s(m-1)$ 时,由定理 2 得 $\overline{(C;2^{m-1})}=\langle1\rangle$,即 $d_{m-1}(C)=1$. 且 $\overline{(C;2^{m-2})}=\left\langle\prod_{i\in S}\bar{f}_i(x)^{k_i-2^s(m-2)}\right\rangle$,其中 $S=\{1\leqslant i\leqslant r\mid2^s(m-2)+1\leqslant k_i\leqslant2^s(m-1)\}$. 由条件得, $S\neq\phi$ 且 $S\neq\{1,\cdots,r\}$. 若 $\overline{(C;2^{m-2})}$ 中有重量为 1 的码字,设该码字为 x^j,而 $(x^j,\bar{f}_i(x)^{2^s})=1$,由 $x^j\in\overline{(C;2^{m-2})}$ 推出 $1\in\overline{(C;2^{m-2})}$. 此时 $\overline{(C;2^{m-2})}=\langle1\rangle$,矛盾,故 $d_{k-2}\geqslant2$. 由定理 3 得 $2^{m-2}\cdot2\leqslant2^{m-2}d_{\gamma_0}\leqslant d_{\mathrm{Hom}}(C)\leqslant2^{m-1}$,由此得到 $d_{\mathrm{Hom}}(C)=2^{m-1}$.

例 1 环 Z_4 上长为 6 的负循环码的共 25 个,在 $Z_4[x]$ 中, $x^3-1=f_0(x)f_1(x)$,其中 $f_0(x)=x-1$, $f_1(x)=x^2+x+1$. 设 $\langle f_0(x)f_1(x)^4\rangle$,由定理 2 得, $\bar{C}=\langle\bar{f}_0(x)\bar{f}_1(x)^2\rangle$, $\overline{(2:C)}=\langle\bar{f}_1(x)^2\rangle$. 所以, $d_0=6$, $d_1=3$. 由定理 3 (1)得, $d_0\leqslant d_{\mathrm{Hom}}(C)\leqslant2d_1$. 即 $d_{\mathrm{Hom}}(C)=6$. 从而 C 是 Z_4 上 $(6,2^3,6)$ -线性码.

4.2 环 Z_{2^m} 上 $2^{m-1}-1$ -常循环自对偶码

当 $m\geqslant3$ 时,取 $\lambda=2^{m-2}-1\in Z_{2^n}$,则 $\eta=2^{m-1}-1$.

此时,$\eta^2 \equiv 1 (\mathrm{mod} 2^m)$,故在 Z_{2^m} 中 $\eta = \eta^{-1}$. 本节中 $m \geqslant 3$,令 $\rho = 2^m - 1$,则 Z_{2^m} 上长为 N 的 ρ - 常循环码的对偶码仍是 ρ - 常循环码. 下面,利用高阶挠码研究 Z_{2^m} 上长为 N 的 ρ - 常循环自对偶码的欧几里得距离性质. 首先,给出欧几里得重量与距离等相关概念. 对 $\forall x \in Z_{2^m}$,x 的欧几里得重量定义为 $\min\{x^2, (2^m - x)^2\}$. 对 $\forall \boldsymbol{c} \in Z_{2^m}^N$,定义 $\boldsymbol{c}$ 的欧几里得重量 $w_E(\boldsymbol{c})$ 为各分量的欧几里得重量的和. 定义 $\boldsymbol{c}_1, \boldsymbol{c}_2 \in Z_{2^m}^N$ 的欧几里得距离为 $w_E(\boldsymbol{c}_1 - \boldsymbol{c}_2)$. Z_{2^m} 上线性码 C 的最小欧几里得距离 $d_E(C)$ 定义为 C 中非零码字的欧几里得重量的最小值. Z_{2^m} 上的自对偶码称为类型Ⅱ码,如果它的每个码字的欧几里得重量都为 2^{m+1} 的倍数. 否则,称为类型Ⅰ码. Z_{2^m} 上自对偶码在区组设计与模格构造等方面起到重要作用[10,11].

对任意的整数 i,存在最小正整数 k 使得 $i2^k \equiv i (\mathrm{mod} n)$,称集合 $C_i = \{i, 2i, \cdots, 2^{k-1}i\}$ 是包含 i 的 2 模 n 的分圆陪集. 若 $-i \in C_i$,则称 C_i 是对称的. 否则,称为非对称的. 易知,非对称分圆陪集 C_i 与 C_{-i} 成对出现. 设 S_1, S_2 分别是 2 模 n 的对称分圆陪集代表元和非对称陪集代表元组成的集合. 设 ξ 是 Z_2 扩域中的一个 n 次本原单位根,则 Z_2 上 ξ^i 的极小多项式 $\bar{f}_i = \prod_{j \in C_i} (x - \xi^j)$,根据 Hensel 引理,$x^n - 1$ 在 Z_{2^m} 上可以唯一分解为 $x^n - 1 = \prod_{i \in S_1} f_i(x) \prod_{i \in S_2} f_i(x) f_{-i}(x)$,其中 $f_i(x)$ 是 $x^n - 1$ 在 Z_{2^m} 上的首一不可约因子. 文献[8]给出了 Z_{2^m} 上长为 N 的 ρ - 常循环自偶码的生成多项式如下:

$$\prod_{i \in S_1} f_i(x)^{2^{s-1}m} \prod_{i \in S_2} f_i(x)^{s} f_{-i}(x)^{2^s m - s_i}, \quad (*)$$

其中 $0 \leqslant s_i \leqslant 2^s m$.

定理 4　环 Z_{2^m} 上长为 N 的 ρ - 常循环自对偶码都是类型Ⅰ码.

证明　设 C 是 Z_{2^m} 上长为 N 的 ρ - 常循环自对偶码,其生成多项式形如(*)式,注意到 s_i 和 $2^s m - s_i$ 必有一个不超过 $2^{s-1}m$,不妨设 $s_i \leqslant 2^{s-1}m$,则 $(x^{n2^{s-1}} - 1)\bar{g}_1(x)(x^{n2^{s-1}} - 1)\bar{g}_1(x) f(x) = \prod_{i \in S_1} f_i(x)^{2^{s-1}m} \prod_{i \in S_2} f_i(x)^{2^{s-1}m} f_{-i}(x)^{2^s m} \in C$.

记 $D = \langle f(x) \rangle \subseteq R$. 当 m 为偶数时,由定理 3.3 得,$\overline{(D:2^{\frac{m}{2}})} = \left\langle \prod_{i \in S_2} \bar{f}_{-i}(x)^{2^s} \right\rangle$. 令 $\bar{h}(x) = \prod_{i \in S_2} \bar{f}_{-i}(x)$,因为 $\bar{f}_{-i}(x)$ 是非对称的,所以 $\bar{h}(x)$ 的非零项数为奇数,否则,$x+1$ 整除 $\bar{h}(x)$,矛盾. 因此,$\bar{h}(x)$ 的汉明重量为奇数. 所以,存在 $h_1(x) \in R, 2^{\frac{m}{2}} h(x) = 2^{\frac{m}{2}} (\bar{h}(x) + 2h_1(x)) \in D \subseteq C$,而 $w_E(2^{\frac{m}{2}} h(x)) = (1 + 2a)2^m$,其中 a 是某整数. 因此,C 是类型Ⅰ码.

当 m 为奇数,由定理 2 得,$\overline{(D:2^{\frac{m-1}{2}})} = \left\langle (x^n - 1)^{2^{s-1}} \prod_{i \in S_2} \bar{f}_{-i}(x)^{2^{s-1}} \right\rangle$. 令 $\bar{g}(x) = (x^{n2^{s-1}} - 1)\bar{g}_1(x)$,其中 $\bar{g}_1(x) = \prod_{i \in S_2} \bar{f}_{-i}(x)^{2^{s-1}}$,类似地可证 $\bar{g}_1(x)$ 的汉明重量为奇数,所以 $w_H(\bar{g}) = 2l$,l 为某奇数. 于是,存在 $g_2(x) \in R$ 使得 $2^{\frac{m-1}{2}} g(x) = 2^{\frac{m-1}{2}} (\bar{g}(x) + 2g_2(x)) \in D \subseteq C$,从而 $w_E(2^{\frac{m-1}{2}} g(x)) = 2^{m-1} 2b = 2^m b$,$b$ 为某奇数. 因此,C 是类型Ⅰ码.

定理 5　设 C 是 Z_{2^m} 上以(*)为生成多项式的 ρ - 常循环自对偶码,d_E 是 C 的欧几里得距离. 若 γ_0 满足:$2^s \gamma_0 \leqslant \min_i \{2^{s-1} m, s_i, 2^s m - s_i\} < 2^s(\gamma_0 + 1)$,则 $d_E \geqslant \min_{\gamma_0 \leqslant i \leqslant m-1} \{2^{2i} d_i\}$.

证明　易证 γ_0 是使得 $\overline{(C:2^\gamma)} \neq \{\boldsymbol{0}\}$ 的最小值,所以任意非零码字 $\boldsymbol{c} \in C$,存在 $i (\gamma_0 \leqslant i \leqslant m-1)$ 使得:$\boldsymbol{c} = 2^i \boldsymbol{b}$,其中 $\boldsymbol{b} \in Z_{2^m}^N$ 且 $\bar{\boldsymbol{b}} \neq 0$. 显然 $d_E(\boldsymbol{c}) \geqslant 2^{2i} d_H(\bar{\boldsymbol{b}})$,注意到 $\boldsymbol{c} \in (C:2^i)$,所以 $d_H(\bar{\boldsymbol{b}}) \geqslant d_i$,从而推出 $d_E(\boldsymbol{c}) \geqslant 2^{2i} d_i$. 所以 $d_E \geqslant \min_{\gamma_0 \leqslant i \leqslant m-1} \{2^{2i} d_i\}$.

定理 4 指出环 Z_{2^m} 上的 ρ - 常循环自对偶码总是类型Ⅰ码. 文献[11]给出了 Z_{2^m} 上长为 N 的类型Ⅰ码的欧几里得距离界:

若 $2\lfloor N/24 \rfloor \leqslant 2^m - 3$,则

$$d_E \leqslant \begin{cases} 2^{m+1}(\lfloor \frac{N}{24} \rfloor + 1), \text{若 } N \neq 23 \\ 3 \cdot 2^m, \text{若 } N = 23 \end{cases} \quad (**)$$

当 $2\lfloor N/24 \rfloor \leqslant 2^m - 3$ 时,称 Z_{2^m} 上满足(**)界的类型Ⅰ码为极优码. 下面利用挠码构建 Z_{2^m} 上极优类型Ⅰ码.

例 2　在 $Z_8[x]$ 中,$x^7 - 1 = f_0(x) f_1(x) f_3(x)$,其中 $f_0(x) = x - 1$,$f_1(x) = x^3 + 6x^2 + 5x - 1$,$f_3(x) = x^3 + 3x^2 + 2x - 1$. 设 C 是 Z_8 上长为 14 的 3 - 常循环自对偶码,其生成多项式为 $g(x) = f_0(x)^3 f_1(x)^2 f_3(x)^4$. 在 $\frac{Z_8[x]}{(x^{14} - 3)}$ 中,$g(x) = 6 + 4x + 2x^4 + 4x^5 + 4x^6 + 6x^7 + 6x^8 + 4x^9 - 2x^{11} + 2x^{12} + 6x^{13}$.

由定理 2 得:$\mathrm{Res}(C) = \{0\}$,$\overline{(C:2)} = \langle \bar{f}_0(x) \bar{f}_3(x)^2 \rangle$,$\overline{(C:2^2)} = \langle 1 \rangle$,所以 $d_1 = 4$,$d_2 = 1$. 再由定理 5 得,$d_E \geqslant 16$,所以 C 是极优的类型Ⅰ码. 同理,$\langle f_0(x)^3 f_1(x)^4 f_3(x)^2 \rangle$ 也是极优的类Ⅰ型码.

例 3　在 $Z_{16}[x]$ 中,$x^7 - 1 = f_0(x) f_1(x) f_3(x)$,其中 $f_0(x) = x - 1$,$f_1(x) = x^3 + 6x^2 + 5x - 1$,$f_3(x) = x^3 + 11x^2 + 10x - 1$. 设 C 是 Z_{16} 上长为 14 的 7 - 常循环自对偶码,其生成多项式为 $g(x) = f_0(x)^4 f_1(x)^5 f_3(x)^3$. 在

$Z_8[x]/(x^{14}-7)$ 中，$g(x)=2x^{13}+12x^{12}+8x^{11}+2x^{10}+6x^9+2x^8+2x^6+12x^5+8x^4+2x^3+6x^2+2x+4$.

由定理 2 得：$\mathrm{Res}(C)=\{\mathbf{0}\}$，$\overline{(C:2)}=\langle \bar{f}_0(x)^2\bar{f}_1(x)^2\bar{f}_3(x)\rangle$，$\overline{(C:2^2)}=\langle \bar{f}_1(x)\rangle$，$\overline{(C:2^3)}=\langle 1\rangle$，所以 $d_1=8$，$d_2=2$，$d_3=1$. 再由定理 5 得，$d_E\geqslant 32$，所以 C 是极优的类型 I 码. 同理，$\langle f_0(x)^4f_1(x)^3f_3(x)^5\rangle$ 也是极优的类 I 型码.

5 总结

本文给出了环 Z_{2^n} 上任意长的 $(1+2\lambda)$ - 常循环码的挠码，利用挠码讨论了 Z_{2^n} 上 $(1+2\lambda)$ - 常循环码的齐次距离分布，并证明了 $(2^{m-1}-1)$ - 常循环自对偶码为类型 I 码. 最后，利用常循自对偶码，构造了 Z_8 与 Z_{16} 上极优的类型 I 码. 一个值得考虑的问题是利用挠码研究 Z_{2^n} 上任意长度的循环码.

参考文献

[1] A R Hammons, P V Kumar, A R Calderbank, N JA Sloane, P Solé. The Z_4 - linearity of Kerdock, Preparata, Goethals, and related codes[J]. IEEE Transactions on Information Theory, 1994, 40(2): 301 - 319.

[2] H Q Dinh. 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.

[3] S Zhu, X Kai. The hamming distances of negacyclic codes of length 2^s over GR(2^a, m) [J]. Journal of Systems Science and Complexity, 2008, 21(1): 60 - 66.

[4] 施敏加，杨善林，朱士信. 环 F_2+uF_2 上长为 2^e 的循环码的距离[J]. 电子学报，2011，39(1)：29 - 34.
Shi Min-jia, Yang Shan-lin, Zhu Shi-xin. On minimum distance of cyclic codes of length 2^e over F_2+uF_2[J]. Acta Electronica Sinica, 2011, 39(1): 29 - 34. (in Chinese)

[5] G H Norton, A Salagean. On the hamming distance of linear and cyclic codes over a finite chain ring[J]. IEEE Transactions on Information Theory, 2000, 46(3): 1060 - 1067.

[6] S T Dougherty, Y H Park. On modular cyclic codes[J]. Finite Fields and Their Application, 2007, 13(1): 31 - 57.

[7] 朱士信，黄素娟. 环 $F_{pm}+uF_{pm}+\cdots+u^{k-1}F_{pm}$ 上 $(1+u)$ - 常循环码的齐次距离分布[J]. 电子与信息学报，2013，35(11)：2580 - 2583.
Zhu Shi-xin, Huang Su-juan. The distribution of homogeneous distance of $(1+u)$-constacyc-lic codes over $F_{pm}+uF_{pm}+\cdots+u^{k-1}F_{pm}$[J]. Journal of Electronics and Information Technology, 2013, 35(11): 2580 - 2583. (in Chinese)

[8] X Kai, S Zhu, Y Tang. Some constacyclic self-dual codes over the integers modulo 2^m[J]. Finite Fields and Their Applications, 2012, 18(2): 258 - 270.

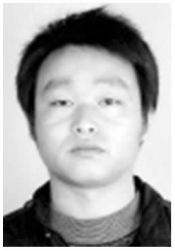
[9] S Zhu, X Kai. A class of constacyclic codes over z_{pm}[J]. Finite Fields and Their Applications, 2010, 16(4): 243 - 254.

[10] S T Dougherty, T A Gulliver, M Harada. Type Ⅱ self-dual codes over finite rings and even unimodular lattices[J]. Journal of Algebraic Combinatorics, 1997, 9(3): 233 - 250.

[11] E Bannai, S T Dougherty, M Harada, M Oura. Type Ⅱ codes, even unimodular lattices, and invariant rings[J]. IEEE Transactions on Information Theory, 1999, 45(4): 1194 - 1205.

作者简介

朱士信 男，1962 年生，教授，博士生导师，获国家级教学名师、国家“万人计划”教学名师荣誉称号. 主要从事编码理论、序列密码与信息安全研究.
E-mail：zhushixin@hfut.edu.cn



孙中华（通信作者） 男，1989 年生，硕士研究生，研究方向为代数编码.
E-mail：sunzhonghuas@163.com