环 Z_4 上自对偶码的构造

袁 健[1,2],朱士信[1,2],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: 利用有限环 Z_4+vZ_4(其中 $v^2=1$)上自对偶码,给出了一种构造 Z_4 上自对偶码的方法. 引入了 $(Z_4+vZ_4)^n$ 到 Z_4^{2n} 的保距 Gray 映射,给出了 Z_4+vZ_4 上自对偶码的性质,证明了 Z_4+vZ_4 上长为 n 的自对偶码的 Gray 像是 Z_4 上长为 $2n$ 的自对偶码,由此构造了 Z_4 上一些极优的类型 I 与类型 Ⅱ 自对偶码.

关键词: Gray 映射; 线性码; 自对偶码
中图分类号: TN991. 22 **文献标识码:** A **文章编号:** 0372-2112 (2016)11-2807-05
电子学报 URL: http://www. ejournal. org. cn **DOI:** 10. 3969/j. issn. 0372-2112. 2016. 11. 034

A Method for Construction Self-dual Codes over Z_4

YUAN Jian[1,2], ZHU Shi-xin[1,2], 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: A Method for Construction self-dual codes over Z_4 is proposed by using self-dual codes over the ring Z_4+vZ_4, where $v^2=1$. A Gray map from $(Z_4+vZ_4)^n$ to Z_4^{2n} is introduced, and some properties about self-dual codes over Z_4+vZ_4 are given. It showns that the Gray image of a self-dual code over Z_4+vZ_4 of length n is a self-dual code over Z_4 of length $2n$. Further, some extremal Type I and Type Ⅱ codes over Z_4 are constructed.

Key words: Gray map; linear codes; self-dual codes

1 引言

上世纪九十年代中期,Hammons 等人[1]的杰出工作使得有限环上的编码理论获得了重大突破. 自此,有限环上纠错码成为了编码理论研究的一个热点[2-4]. 1997 年,Bachoc[5]利用多项式剩余类环 F_q+uF_q 上自对偶码构造了模格,这更激发了学者对有限环上纠错码的研究兴趣. 有限环上自对偶码是一类重要的线性码,它在模格构造与区组设计等方面有着广泛的应用,一直是有限环上纠错码理论研究的重要课题. 文献[6]引入了 Z_4 上类型Ⅱ自对偶码,并且利用 Hensel 提升构造了 Z_4 上类型Ⅱ自对偶码. 文献[7]利用不变理论研究了环 F_2+uF_2 上类型Ⅱ自对偶码. 随着研究的深入,一些有限非链环上的自对偶码也受到了学者的重视. Yildiz 和 Karadeniz 在文献[8]中利用环 $F_2+uF_2+vF_2+uvF_2$ 上自对偶码构造了 F_2+uF_2 上类型Ⅱ码. 随后,他们又在文献[9]中利用有限非链环 Z_4+uZ_4(其中 $u^2=0$)上的线性码构造了 Z_4 上形式自对偶码. 这表明有限非链环上纠错码具有重要的意义和应用前景. 本文利用有限非链环 Z_4+vZ_4(其中 $v^2=1$)上自对偶码构造 Z_4 上自对偶码. 我们引入 $(Z_4+vZ_4)^n$ 到 Z_4^{2n} 的保距映射,给出了 Z_4+vZ_4 上线性码与自对偶码及其 Gray 像的性质,并且 Z_4+vZ_4 上自对偶码构造了一些 Z_4 上自对偶码. 本文借助计算机程序,结合 Z_4+vZ_4 上自对偶码的性质,搜索 Z_4+vZ_4 上类型 I 和类型Ⅱ码,由此得到了 Z_4 上自对偶码. 由于通过计算机搜索 Z_4+vZ_4 上长为 n 的自对偶码的复杂性要比搜索 Z_4 上长为 $2n$ 的自对偶码的复杂性低,从这个意义上,本文改进了 Z_4 上自对偶码的构造方法.

2 环 Z_4+vZ_4 上的线性码

记 Z_4 表示整数模 4 的剩余类环,它的元素的欧几里得重量 w_E 分别定义为 $w_E(0)=0, w_E(1)=w_E(3)=1, w_E(2)=4$. 对任意的 $x=(x_1,x_2,\cdots,x_n)\in Z_4^n$,定义 x

收稿日期:2015-07-08;修回日期:2016-01-04; 责任编辑:马兰英
基金项目: 国家自然科学基金(No. 61370089);东南大学移动通信国家重点实验室开放研究基金(No. 2014D04);安徽省自然科学基金(No. JZ2015AKZR0021, No. 1508085SQA198)

的欧几里得重量为 $w_E(x)=\sum_{i=1}^{n}w_E(x_i)$. 任取 $x=(x_1,x_2,\cdots,x_n),y=(y_1,y_2,\cdots,y_n)\in Z_4^n$,定义 x 与 y 的欧几里得内积为 $x\cdot y=x_1y_1+x_2y_2+\cdots+x_ny_n$. Z_4 上长为 n 的线性码 C 是 Z_4^n 的一个 Z_4 - 子模,C 中非零码字的欧几里得重量的最小值称为 C 的欧几里得距离,记为 $d_E(C)$. Z_4 上的长为 n 的线性码 C 的对偶码定义为 $C^\perp=\{x\in z_4^n\mid x\cdot c=0,\forall c\in C\}$. 若 $C\subseteq C^\perp$,则称 C 为 Z_4 上自正交码;若 $C=C^\perp$,则称 C 为 Z_4 上自对偶码. 对于 Z_4 上自对偶码 C,若它的每个码字的欧几里得重量都是 8 的倍数,则称码 C 为 Z_4 上类型Ⅱ码. 否则,称码 C 为 Z_4 上类型Ⅰ码. 文献[6]中给出了 Z_4 上类型Ⅰ码与类型Ⅱ码的欧几里得重量的一个上界:

定理 1[6] 若 C 为 Z_4 上长为 n 的类型Ⅱ码,则 $d_E(C)\leqslant 8\lfloor n/24\rfloor+8$;若 C 为 Z_4 上长为 n 的类型Ⅰ码,则当 $n\equiv 23\pmod{24}$ 时,$d_E(C)\leqslant 8\lfloor n/24\rfloor+12$,否则 $d_E(C)\leqslant 8\lfloor n/24\rfloor+8$.

称达到定理 1 中上界的自对偶码为 Z_4 上的极优码. 下面介绍有限环 $Z_4+vZ_4=\{a+bv\mid a,b\in Z_4\}$,其中 $v^2=1$. 为简便起见,用 R 表示环 Z_4+vZ_4. 环 R 是一个特征为 4 的含幺交换环,并且 R 可以看作多项式剩余类环 $Z_4[v]/\langle v^2-1\rangle$. R 的单位元素组成的集合为

$$U=\{1,3,1+2v,3+2v,v,3v,2+v,2+3v\},$$

R 的非单位元素组成的集合为

$$N=\{0,2,2v,2+2v,1+v,3+v,1+3v,3+3v\}.$$

将 R 的非单位分为两个集合:$N_1=\{0,2,2v,2+2v\}$ 和 $N_2=\{1+v,3+v,1+3v,3+3v\}$. 容易验证:

$$\forall r\in R,r^2=\begin{cases}0, & r\in N_1,\\ 2+2v, & r\in N_2,\\ 1, & r\in U.\end{cases}$$

环 R 有 7 个不同的理想,它们分别为:

$\{0\},Z_4+vZ_4,\{0,2+2v\},\langle 2\rangle=\{0,2,2v,2+2v\},\langle 1+v\rangle=\{0,1+v,2+2v,3+3v\},\langle 1+3v\rangle=\{0,1+3v,2+2v,3+v\},\langle 2,1+v\rangle=\{0,2,2v,2+2v,1+v,3+v,1+3v,3+3v\}$.

因此,R 是一个最大理想为 $\langle 2,1+v\rangle$ 的局部环,剩余域为 F_2. 因为 $\langle 2,1+v\rangle$ 在 R 中的零化理想 $Ann(\langle 2,1+v\rangle)=\{0,2+2v\}$ 在 F_2 上的维数为 1,所以 R 是一个局部 Frobenius 环[10,11].

环 R 中的每个元素可唯一的表示为 $a+bv$,其中 $a,b\in Z_4$. 我们定义 R 中元素 $a+bv$ 的欧几里得重量 w_E 为 $w_E(a+bv)=w_E(b)+w_E(a+2b)$. 对于任意向量 $x=(x_1,x_2,\cdots,x_n)\in R^n$,定义 x 的欧几里得重量为 $w_E(x)=\sum_{i=1}^{n}w_E(x_i)$. 定义任意两个向量 $x,y\in R^n$ 的欧几里得距离为 $d_E(x,y)=d_E(x-y)$. 环 R 上长为 n 的码 C 是 R^n 的一个非空子集,码 C 的欧几里得距离 $d_E(C)$ 定义为 C 中两个不同码字之间的欧几里得距离的最小值. 环 R 上长为 n 的线性码 C 是 R^n 的一个 R - 子模,C 的欧几里得重量 $w_E(C)$ 定义为所有码字欧几里得重量的最小值. 显然,若 C 是 R 上的线性码,则 $d_E(C)=w_E(C)$. 我们用 (n,M,d_E) 表示长为 n,码字数目为 M,欧几里得距离为 d_E 的环 R 或 Z_4 上的码.

下面我们引入一个 R^n 到 Z_4^{2n} 上的 Gray 映射

$$\phi:R^n\to Z_4^{2n}$$

$$(c_0,c_1,\cdots,c_{n-1})\mapsto(b_0,b_1,\cdots,b_{n-1},a_0+2b_0,a_1+2b_1,\cdots,a_{n-1}+2b_{n-1})$$

其中 $c_i=a_i+b_iv,i=0,1,\cdots,n-1$. 显然,$\phi$ 是一个双射. 根据欧几里得重量定义,容易得到下面结论:

定理 2 映射 ϕ 诱导出(欧几里得距离)到(欧几里得距离)的 Z_4 - 线性保距映射. 因此,若 C 为 R 上参数为 (n,M,d_E) 的线性码,则 $\phi(C)$ 是 Z_4 上参数为 $(2n,M,d_E)$ 的线性码.

在 R^n 上引入内积. 对于任意 $x=(x_1,x_2,\cdots,x_n),y=(y_1,y_2,\cdots,y_n)\in R^n$,定义 $x\cdot y=x_1y_1+x_2y_2+\cdots+x_ny_n$. R 上的长为 n 的线性码 C 的对偶码定义为 $C^\perp=\{x\in R^n\mid x\cdot c=0,\forall c\in C\}$. 易证 $C^\perp$ 也是 R 上的长为 n 的线性码. 因为 R 是一个 Frobenius 环,所以有 $|C||C^\perp|=16^n$(参见[10]).

3 R 上自对偶码及其 Gray 像

设 C 是 R 上的线性码,若 $C\subseteq C^\perp$,则称 C 为 R 上自正交码;若 $C=C^\perp$,则称 C 为 R 上自对偶码. R 中由元素 2 生成的理想 $\langle 2\rangle$ 可以看作 R 上长为 1 的自对偶码,利用直积的方法[11],容易看到环 R 上存在任意长度的自对偶码. 任取 $c=(c_1,c_2,\cdots,c_{n-1})\in C$,用 $n_U(c)$ 表示 c 的属于 U 的分量数目,$n_{N_2}(c)$ 表示 c 的属于 N_2 的分量数目. 为了构造 Z_4 上自对偶码,首先给出 R 上自对偶码的性质.

定理 3 设 C 为 R 上长为 n 的线性码,则下面结论成立:

(1) 若 C 是自正交码,则对于任一码字 $c\in C$,$n_{N_2}(c)\equiv 0\pmod 2$ 且 $n_U(c)\equiv 0\pmod 4$. 因此,R 上自正交码的每个码字的欧几里得重量都是 4 的倍数.

(2)若 C 是自对偶码,则 C 包含全 2 向量和全 $(2+2v)$ 向量.

证明 (1) 设 C 是 R 上的自正交码,则对任一 $c\in C,c\cdot c=0$. 但在 R 中,

$$\begin{aligned}c\cdot c&=n_{N_2}(c)(2+2v)+n_U(c)\\&=2n_{N_2}(c)+n_U(c)+(2n_{N_2}(c))v.\end{aligned}$$

因此,

$$n_{N_2}(c)\equiv 0(\mathrm{mod}2)\text{且}\ n_U(c)\equiv 0(\mathrm{mod}4).$$

注意到 N_2 中的元素的欧几里得重量都是 2,N_1 中的元素的欧几里得重量为 0 或 4 或 8,即是 4 的倍数,而 U 中元素的欧几里得重量模 4 余 1. 由此可得,R 上自正交码的每个码字的欧几里得重量都是 4 的倍数.

(2) 在环 R 中,容易验证:当 $r\in U$ 时,$r\cdot(2+2v)=2+2v$;当 $r\in N$ 时,$r\cdot(2+2v)=0$.

设 C 是 R 上的自对偶码,对任一 $c\in C$,$(2+2v,2+2v,\cdots,2+2v)\cdot c=n_U(c)(2+2v)$. 由(1)知,$n_U(c)$ 是 4 的倍数,从而 $(2+2v,2+2v,\cdots,2+2v)\in C^{\perp}=C$,即 C 中包含全 $2+2v$ 向量. 同理,C 也包含全 2 向量.

由定理 3(1),R 上自对偶码的每个码字的欧几里得重量都是 4 的倍数. 同时,由于 R 中 $2+2v$ 的欧几里得重量为 8,根据定理 3(2),R 上自对偶码中一定存在欧几里得重量是 8 的倍数的码字. 由此,我们引入下面定义:

定义 1　设 C 是 R 上的自对偶码,若它的每个码字的欧几里得重量都是 8 的倍数,则称 C 为类型Ⅱ码,否则称 C 为类型Ⅰ码.

为了构造 Z_4 上自对偶码,下面考虑 R 上自对偶码的 Gray 像.

定理 4　设 C 为 R 上长为 n 的线性码,则 $\phi(C^{\perp})=\phi(C)^{\perp}$. 而且,若 C 是 R 上长为 n 自对偶码,则 $\phi(C)$ 为 Z_4 上长为 $2n$ 的自对偶码. 若 C 是 R 上长为 n 的类型Ⅱ码,则 $\phi(C)$ 为 Z_4 上长为 $2n$ 的类型Ⅱ码.

证明　因为 ϕ 是一个双射保距映射,并且

$$|\phi(C^{\perp})|=|C^{\perp}|=16^n/|C|=4^{2n}/|\phi(C)|=|\phi(C)^{\perp}|,$$

所以只需证明 $\phi(C^{\perp})\subseteq\phi(C)^{\perp}$. 设 $c=(a_0+b_0v,a_1+b_1v,\cdots,a_{n-1}+b_{n-1}v)$,$c'=(a'_0+b'_0v,a'_1+b'_1v,\cdots,a'_{n-1}+b'_{n-1}v)\in R^n$,且满足 $c\cdot c'=0$,下面证明 $\phi(c)\cdot\phi(c')=0$. 由于

$$c\cdot c'=\sum_{i=0}^{n-1}(a_ia'_i+b_ib'_i)+v\sum_{i=0}^{n-1}(a_ib'_i+a'_ib_i)=0,$$

所以

$$\sum_{i=0}^{n-1}(a_ia'_i+b_ib'_i)=\sum_{i=0}^{n-1}(a_ib'_i+a'_ib_i)=0.$$

于是

$$\phi(c)\cdot\phi(c')=\sum_{i=0}^{n-1}(a_ia'_i+b_ib'_i)+2\sum_{i=0}^{n-1}(a_ib'_i+a'_ib_i)=0,$$

从而 $\phi(C^{\perp})=\phi(C)^{\perp}$.

由定理 4 可以看出映射 ϕ 保持正交性,即 R^n 上正交的两个向量,通过映射 ϕ 得到它们的 Gray 像在 Z_4^{2n} 上也正交. 但是,反之不成立. 例如,向量(1,2),(2,1)$\in Z_4^2$ 正交,但是它们在 ϕ 下的原象,即 $\phi^{-1}((1,2))=v$,$\phi^{-1}((2,1))=1+2v$ 并不正交.

注意到 R 上由 2 生成的长为 1 的自对偶码是类型Ⅰ码,利用直积方法[11]可知,R 上任意长的类型Ⅰ码都存在,而对于 R 上类型Ⅱ码有下面的结果:

定理 5　环 R 上长为 n 的类型Ⅱ码存在当且仅当 n 是 4 的倍数.

证明　由文献[6]可知,对于 Z_4 上长为 N 的自对偶码,仅当 N 是 8 的倍数时,存在 Z_4 上长为 N 的类型Ⅱ码. 因为 ϕ 是保距映射,所以若 R 上长为 n 的类型Ⅱ码存在,则 n 是 4 的倍数. 反过来,设 n 是 4 的倍数,令 $C=\langle(v,1,1,1),(3,v,1,3),(3,3,v,1),(3,1,3,v)\rangle$,则 C 是 R 上长为 4 的类型Ⅱ码. C 的欧几里得重量计数器为 $W_C(z)=1+128z^8+126z^{16}+z^{32}$. 因此,$C$ 是一个参数为 $(4,4^4,8)$ 的类型Ⅱ码. 根据文献[11,Lemma 3.2],$C\times C$,$C\times C\times C$,$C\times C\times C\times C$,……分别为 R 上长为 8,12,16,……的类型Ⅱ码. 所以,当 n 是 4 的倍数时,R 上长为 n 的类型Ⅱ码存在.

下面给出类型Ⅰ码和类型Ⅱ码的欧几里得重量的上界.

定理 6　设 d_E 是 R 上长为 n 的类型Ⅰ码或类型Ⅱ码的欧几里得重量,则 $d_E\leqslant 8\lfloor n/12\rfloor+8$.

证明　由定理 4,如果 C 是 R 上长为 n 的类型Ⅱ码或类型Ⅰ码,那么 $\phi(C)$ 为 Z_4 上长为 $2n$ 的类型Ⅱ码或类型Ⅰ码. 因为 ϕ 是保距映射,根据定理 1 立即可以得到结论. 因为 $2n\neq 23(\mathrm{mod}24)$,所以 d_E 的上界不变.

若 R 上自对偶码满足定理 6 中的上界 $d_E=8\lfloor n/12\rfloor+8$,则称 C 为环 R 上的极优码.

4　Z_4 上自对偶码

本节,利用前面的结论,再结合计算机程序搜索 R 上类型Ⅰ码和类型Ⅱ码,由此构造 Z_4 上的自对偶码.

例 1　考虑 R 上长为 1 的自对偶码. 取 $C_1=\langle 2\rangle$,则 C_1 是 R 上的参数为(1,4,4)的类型Ⅰ最优码,其欧几里得重量计数器为 $W_{C_1}(z)=1+2z^4+z^8$. 因此,$\phi(C_1)$ 是 Z_4 上参数为 $(2,4^0 2^2,4)$ 的类型Ⅰ码.

例 2　考虑 R 上长为 2 的自对偶码. 取 $C_2=\langle(1+v,1-v),(2,2)\rangle$,则 C_2 是 R 上参数为(2,16,4)的类型Ⅰ最优码,其欧几里得重量计数器为 $W_{C_2}(z)=1+8z^4+6z^8+z^{16}$. 因此,$\phi(C_2)$ 是 Z_4 上参数为 $(4,4^1 2^2,4)$ 类型Ⅰ码.

例 3　考虑 R 上长为 3 的自对偶码. 取 $C_3=\langle(0,1+v,1-v),(1+v,0,1-v),(2,2,2)\rangle$,则 C_3 是 R 上参数为(3,64,4)的极优类型Ⅰ码,其欧几里得重量计数器为 $W_{C_3}(z)=1+12z^4+27z^8+20z^{12}+3z^{16}+z^{24}$. 因此,$\phi(C_3)$ 是 Z_4 上参数为 $(6,4^2 2^2,4)$ 的类型Ⅰ码.

例 4 考虑 R 上长为 4 的自对偶码. 在定理 6 的证明中,已经给出一个 R 上的长为 4 的 $(4,4^4,8)$ 的极优类型Ⅱ码. 该码的 Gray 象是四元 OCTA 码[1]. 若 C_4 是 R 上的长为 4,且由下面 5 个向量生成的线性码:$(1,3,1,1+2v)$,$(0,2+2v,0,2+2v)$,$(2+v,2+v,1,3+2v)$,$(0,2,3+v,1+v)$ 和 $(0,0,2,2)$,则 C_4 是 R 上参数为 $(4,256,8)$ 的极优类型Ⅱ码,其欧几里得重量计数器为 $W_{C_4}(z)=1+132z^8+118z^{16}+4z^{24}+z^{32}$. 因此,$\phi(C_4)$ 是 Z_4 上参数为 $(8,4^32^2,8)$ 的极优类型Ⅱ码.

例 5 考虑 R 上长为 6 的自对偶码. 设 C_6 是 R 上的长为 6,且由下列向量生成线性码:$(1-v,1-v,1-v,1-v,1-v,1-v)$,$(0,2v,0,0,0,2)$,$(0,0,2v,0,0,2)$,$(0,0,0,2v,0,2)$,$(0,0,0,0,2v,2)$,$(0,0,0,0,0,2+2v)$,$(2,0,0,0,0,2)$,$(0,2,0,0,0,2)$,$(0,0,2,0,0,2)$,$(0,0,0,2,0,2)$,$(0,0,0,0,2,2)$,则 C_6 是 R 上参数为 $(6,4^6,8)$ 的极优类型Ⅰ码,其欧几里得重量计数器为

$$W_{C_6}(z)=1+66z^8+2048z^{12}+495z^{16}+924z^{24}+495z^{32}+66z^{40}+z^{48}.$$

因此,$\phi(C_6)$ 是 Z_4 上参数为 $(12,4^12^{10},8)$ 的极优类型Ⅰ码.

例 6 考虑 R 上长为 8 的自对偶码.

(1) 设 $C_8^{(1)}$ 是 R 上的长为 8,且由下列向量生成的线性码:$(1,3,1,1+2v,0,0,0,0)$,$(2+v,2+v,1,3+2v,0,0,0,0)$,$(0,2+2v,0,2+2v,0,0,0,0)$,$(0,2,3+v,1+v,0,0,0,0)$,$(0,0,2,2,0,0,0,0)$,$(0,0,0,0,v,1,1,1)$,$(0,0,0,0,3,v,1,3)$,$(0,0,0,0,3,3,v,1)$,$(0,0,0,0,3,1,3,v)$,则 $C_8^{(1)}$ 是 R 上参数为 $(8,4^8,8)$ 的极优类型Ⅱ码,其欧几里得重量计数器为

$$W_{C_8^{(1)}}(z)=1+260z^8+17140z^{16}+31740z^{24}+15382z^{32}+764z^{40}+244z^{48}+4z^{56}+z^{64}.$$

因此,$\phi(C_8^{(1)})$ 是 Z_4 上参数为 $(16,4^72^2,8)$ 的极优类型Ⅱ码.

(2) 设 $C_8^{(2)}$ 是 R 上的长为 8,且由下列向量生成的线性码:$(1,0,0,0,2v,3v,3v,3v)$,$(0,1,0,0,3v,2v,3v,3v)$,$(0,0,1,0,3v,3v,2v,3v)$,$(0,0,0,1,3v,3v,3v,2v)$,则 $C_8^{(2)}$ 是 R 上参数为 $(8,4^8,8)$ 的极优类型Ⅰ码,其欧几里得重量计数器为

$$W_{C_8^{(2)}}(z)=1+224z^8+2176z^{12}+7836z^{16}+14848z^{20}+17088z^{24}+13056z^{28}+6932z^{32}+2560z^{36}+608z^{40}+128z^{44}+28z^{48}+z^{64}.$$

因此,$\phi(C_8^{(2)})$ 是 Z_4 上参数为 $(16,4^82^0,8)$ 的极优类型Ⅰ码.

(3) 设 $C_8^{(3)}$ 是 R 上的长为 8,且由下列向量生成的线性码:

$(1,0,0,0,2+2v,3v,3v,3v)$,
$(0,1,0,0,3v,2+2v,2+3v,2+v)$,
$(0,0,1,0,3v,2+v,2+2v,2+3v)$,
$(0,0,0,1,3v,2+3v,2+v,2+2v)$.

$C_8^{(3)}$ 是 R 上参数为 $(8,4^8,8)$ 的极优类型Ⅱ码,其欧几里得重量计数器为

$$W_{C_8^{(3)}}(z)=1+480z^8+15516z^{16}+34496z^{24}+13638z^{32}+1376z^{40}+28z^{48}+z^{64}.$$

因此,$\phi(C_8^{(3)})$ 是 Z_4 上参数为 $(16,4^82^0,8)$ 的极优类型Ⅱ码.

5 总结

本文通过引入 Z_4+vZ_4 到 Z_4^2 的 Gray 映射,利用有限环 Z_4+vZ_4 上自对偶码构造了 Z_4 上自对偶码,由此给出了一种构造 Z_4 上自对偶码的方法. 利用这种方法,再借助计算机编程搜索,得到了 Z_4 上一些极优的类型Ⅰ与类型Ⅱ自对偶码. 与利用计算机直接搜索 Z_4 上自对偶码相比较,本文所给的方法降低了搜索的复杂性. 进一步的工作是探索利用本文的方法将 Z_4 上自对偶码在一定的长度内进行完全分类.

参考文献

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

[2] 吴波, 朱士信, 李平. 环 F_p+uF_p 上的 Kerdock 码与 Preparata 码[J]. 电子学报, 2008, 36(7): 1364-1367.
Wo Bo, Zhu Shi-xin, Li Ping. Kerdock codes and Preparata codes over rings F_p+uF_p[J]. Acta Electronica Sinica, 2008, 36(7): 1364-1367. (in Chinese)

[3] 朱士信, 许和乾, 施敏加. 环 Z_4 上线性码关于 RT 距离 MacWalliams 恒等式[J]. 电子学报, 2009, 37(5): 1115-1118.
Zhu Shi-xin, Xu He-qian, Shi Min-jia. MacWalliams identities of linear codes over ring Z_4 with respect to the RT metric [J]. Acta Electronica Sinica, 2009, 37(5): 1115-1118. (in Chinese)

[4] 施敏加, 杨善林. 非主理想环 F_p+vF_p 上线性码的 MacWalliams 恒等式[J]. 电子学报, 2011, 39(10): 2449-2453.
Shi Min-jia, Yang Shan-lin. MacWilliams identities of linear codes over non-principal ideal ring F_p+vF_p[J]. Acta Electronica Sinica, 2011, 39(10): 2449-2453. (in Chinese)

[5] Bachoc C. Applications of coding theory to the construction of modular lattices [J]. Journal of Combinatorial The-

ory Series A,1997,78(1): 92 – 119.

[6] Bonnecaze A, Solé P, Bachoc C, Mourrain B. Type Ⅱ codes over Z_4[J]. IEEE Transactions on Information Theory,1997,43(3): 969 – 976.

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

[8] Yildiz B, Karadeniz S. Self-dual codes over $F_2 + uF_2 + vF_2 + uvF_2$[J]. Journal of the Franklin Institute, 2010, 347(10):1888 – 1894.

[9] Yildiz B, Karadeniz S. Linear codes over $Z_4 + uZ_4$: MacWilliams identities, projections, and formally self-dual codes[J]. Finite Fields and Their Applications, 2014, 27: 24 – 40.

[10] Wood J. Duality for modules over finite rings and applications to coding theory[J]. The American Journal of Mathematics, 1999, 121(3): 555 – 575.

[11] Doughterty S T, Kim J L, Kulosman H, Liu H W. Self-dual codes over commutative Frobenius rings[J]. Finite Fields and Their Applications, 2010, 16(1): 14 – 26.

作者简介

袁　健　男,1988 年生,合肥工业大学博士生,研究方向为代数编码.
E-mail: yuanjian@mail.hfut.edu.cn

朱士信(通信作者)　男,1962 年生,合肥工业大学教授,博士生导师,国家级教学名师,国家"万人计划"第一批教学名师. 长期从事编码理论、序列密码与信息安全等研究.
E-mail: zhushixin@hfut.edu.cn

开晓山　男,1975 年生,合肥工业大学副教授,硕士生导师,主要从事编码理论与信息安全研究.
E-mail: kxs6@sina.com