一种2^m元域上量子纠错码的构造方法

王 玉*[①] 开晓山[②] 朱士信[②]

[①](合肥学院人工智能与大数据学院 合肥 230601)

[②](合肥工业大学数学学院 合肥 230601)

摘 要：构造具有良好参数的量子码是量子纠错码研究的重要内容。该文利用有限非链环$R=F_{4^m}+vF_{4^m}$上的厄米特对偶包含常循环码来构造2^m元量子码。定义了一种新的Gray 映射ϕ，能够将环R上线性码C的厄米特对偶包含性保持到$\phi(C)$上。研究了环R上常循环码是厄米特对偶包含码的条件。给出了一种构造2^m元量子码的方法，并构造了一些新的4元和8元量子码。

关键词：常循环码；量子码；有限非链环；Gray映射

中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2023)05-1731-06

DOI: 10.11999/JEIT221145

A Construction Method of Quantum Error-correcting Codes over F_{2^m}

WANG Yu[①] KAI Xiaoshan[②] ZHU Shixin[②]

[①](*School of Artificial Intelligence and Big Data*, *Hefei University*, *Hefei* 230601, *China*)

[②](*School of Mathematics*, *Hefei University of Technology*, *Hefei* 230601, *China*)

Abstract: Constructing quantum codes with good parameters is an important part of quantum error-correcting codes research. In this paper, 2^m-ary quantum codes are derived through Hermitian dual-containing constacyclic codes over finite non-chain ring $R=F_{4^m}+vF_{4^m}$. A new Gray map ϕ is defined, which is Hermitian dual-containing preserving from a linear code C over R to $\phi(C)$. The condition for constacyclic codes over R to be Hermitian dual-containing is studied. A method of constructing 2^m-ary quantum codes is presented, and some new 4-ary and 8-ary quantum codes are obtained.

Key words: Constacyclic codes; Quantum codes; Finite non-chain ring; Gray map

1 引言

量子纠错码在量子通信和量子计算领域具有非常重要的应用。因此，构造具有良好参数的量子纠错码成为编码理论领域的一个研究热点。CSS构造[1]和厄米特构造[2]是利用经典纠错码构造量子纠错码的两种常用方法。研究表明，有限域上的循环码及常循环码是构造好量子码的重要来源[3–5]。文献[6]首次通过有限环上的循环码来构造二元量子码，利用的是链环F_2+uF_2。之后，有限非链环上的循环码也被证实可以产生新的量子码，如环F_2+vF_2[7]和F_p+vF_p[8]等。近年来，有限环上的常循环码成为量子码构造的新途径。文献[9]利用CSS构造，通过环F_p+uF_p上的常循环码构建p元量子码。文献[10,11]将这种方法推广到了两类更一般的有限交换非链环上。文献[12]采用厄米特构造，通过环$F_{q^2}+vF_{q^2}$上的常循环码得到了一类q元量子MDS码。文献[13,14]分别利用环$F_{q^2}+uF_{q^2}+\cdots+u^{r-1}F_{q^2}$及$F_{q^2}+u_1F_{q^2}+\cdots+u_rF_{q^2}$上的常循环码获取了新的$q$元量子码。文献[15]利用链环$F_{2^{2m}}+uF_{2^{2m}}$上的厄米特对偶包含常循环码来构建$2^m$元量子码。

截至目前，有限环上常循环码相关文献中构造的量子码主要是二元[6,7]、p元[8–10]和p^m元[11–14](p为奇素数)，构造2^m元量子码的研究还较为少见。本文通过非链环$R=F_{4^m}+vF_{4^m}$上的常循环码来构造2^m元量子码。首先定义了一个从环R到域F_{4^m}上的新Gray映射，然后确定了环R上常循环码为厄米特对偶包含码的条件，最后给出了一种构造2^m元量子码的新方法，并例举了一些新的4元和8元量子码。

收稿日期：2022-09-01；改回日期：2022-11-27；网络出版：2022-12-02

*通信作者： 王玉 wangyu351@hfuu.edu.cn

基金项目：国家自然科学基金(12171134, U21A20428)，安徽省高校优秀青年人才支持计划项目(gxyqZD2021137)

Foundation Items: The National Natural Science Foundation of China (12171134, U21A20428), The Key Project of Support Program for Outstanding Young Talents in University of Anhui Province (gxyqZD2021137)

2 基础知识

记F_{4^m}为4^m元有限域，m为正整数。令$R=F_{4^m}+vF_{4^m}=\{a+vb|a,b\in F_{4^m}\}$，其中$v^2=v$。容易验证，$R$是一个有限非链环，且具有极大理想$\langle 1+v\rangle$和$\langle v\rangle$。$R^n$的$R$-子模$C$称为环$R$上长为$n$的线性码。记

$$\begin{aligned}&C_v=\{\boldsymbol{a}\in F_{4^m}^n|\exists\boldsymbol{b}\in F_{4^m}^n,(1+v)\boldsymbol{a}+v\boldsymbol{b}\in C\},\\&C_{1+v}=\{\boldsymbol{b}\in F_{4^m}^n|\exists\boldsymbol{a}\in F_{4^m}^n,(1+v)\boldsymbol{a}+v\boldsymbol{b}\in C\}\end{aligned}\quad(1)$$

则C_v和C_{1+v}都是有限域F_{4^m}上长为n的线性码，且线性码C可以唯一分解表示为$C=(1+v)C_v\oplus vC_{1+v}$。设线性码$C_v$和$C_{1+v}$的生成矩阵分别为$\boldsymbol{G}_1$和$\boldsymbol{G}_2$，则线性码$C$具有生成矩阵$\boldsymbol{G}=\begin{pmatrix}(1+v)\boldsymbol{G}_1\\v\boldsymbol{G}_2\end{pmatrix}$。

设C是环R上长为n的线性码，$\lambda=\alpha+v\beta$是环R的一个单位。若对任意$(c_0,c_1,\cdots,c_{n-1})\in C$，都有$(\lambda c_{n-1},c_0,\cdots,c_{n-2})\in C$，则称$C$为环$R$上的$\lambda$-常循环码。将码字$\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})$等同于其多项式表示$c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$，则环$R$上长为$n$的$\lambda$-常循环码可视为商环$R[x]/\langle x^n-\lambda\rangle$的一个理想。

对$\forall\alpha\in F_{4^m}$，记α的共轭α^{2^m}为$\bar{\alpha}$。环R中元素$\lambda=\alpha+v\beta$的共轭定义为$\bar{\lambda}=\bar{\alpha}+v\bar{\beta}$。任取两个$n$维向量$\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})$和$\boldsymbol{y}=(y_0,y_1,\cdots,y_{n-1})\in R^n$，其厄米特内积定义为

$$\langle\boldsymbol{x},\boldsymbol{y}\rangle_H=x_0\bar{y}_0+x_1\bar{y}_1+\cdots+x_{n-1}\bar{y}_{n-1}\quad(2)$$

设C是环R上长为n的线性码，其厄米特对偶码定义为$C^{\perp_H}=\{\boldsymbol{x}\in R^n|\langle\boldsymbol{x},\boldsymbol{y}\rangle_H=0,\forall\boldsymbol{y}\in C\}$。若$C^{\perp_H}\subseteq C$，则称$C$为厄米特对偶包含码。利用有限域上的厄米特对偶包含码可以构造量子码，其方法如下。

定理1[2](厄米特构造) 设$\mathfrak{C}$是一个有限域F_{q^2}上参数为$[n,k,d]$的厄米特对偶包含码，则存在一个参数为$[[n,2k-n,\ge d]]_q$的量子码。

3 新的Gray映射

下面定义一个从环R到$F_{4^m}^2$的Gray映射ϕ，并证明：如果C是环R上的厄米特对偶包含码，那么$\phi(C)$是有限域F_{4^m}上的厄米特对偶包含码。

定义1 设ω是有限域F_{4^m}的一个本原元，记$\bar{\omega}=\omega^{2^m}$。定义Gray映射

$$\begin{aligned}&\phi:R\to F_{4^m}^2,\\&(1+v)x+vy\mapsto(x+\bar{\omega}y,\omega x+y)\end{aligned}\quad(3)$$

容易验证，当$m>1$时，ϕ是一个双射。可以自然地将它推广到$\phi:R^n\to F_{4^m}^{2n}$，即

$$\begin{aligned}&(c_0,c_1,\cdots,c_{n-1})\mapsto(r_0+\bar{\omega}q_0,r_1+\bar{\omega}q_1,\cdots,r_{n-1}\\&\quad+\bar{\omega}q_{n-1},\omega r_0+q_0,\omega r_1+q_1,\cdots,\omega r_{n-1}+q_{n-1})\end{aligned}\quad(4)$$

其中，$c_i=(1+v)r_i+vq_i,i=0,1,\cdots,n-1$。

对$\forall a\in R$，定义a的Gray重量为$\phi(a)$的汉明重量，即$w_G(a)=w_H(\phi(a))$。向量$\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in R^n$的Gray重量为$w_G(\boldsymbol{x})=w_H(\phi(\boldsymbol{x}))$。$R^n$中向量$\boldsymbol{x}$与$\boldsymbol{y}$的Gray距离定义为$d_G(\boldsymbol{x},\boldsymbol{y})=w_G(\boldsymbol{x}-\boldsymbol{y})$。定义环$R$上线性码$C$的极小Gray距离为$d_G(C)=\min\{d_G(\boldsymbol{c},\boldsymbol{c}')|\boldsymbol{c},\boldsymbol{c}'\in C,\boldsymbol{c}\ne\boldsymbol{c}'\}$。

根据上述定义，可以得到如下结论：

命题1 设C是环R上长为n的线性码，则$\phi(C)$是有限域F_{4^m}上长为$2n$的线性码。映射ϕ是从C(Gray距离)到$\phi(C)$(汉明距离)的保矩映射。

证明 对$\forall k_1,k_2\in F_{4^m}$及$\boldsymbol{x},\boldsymbol{y}\in R^n$，易证得$\phi(k_1\boldsymbol{x}+k_2\boldsymbol{y})=k_1\phi(\boldsymbol{x})+k_2\phi(\boldsymbol{y})$。因此，$\phi(C)$是有限域$F_{4^m}$上长为$2n$的线性码。任取$\boldsymbol{c},\boldsymbol{c}'\in C$, $d_G(\boldsymbol{c},\boldsymbol{c}')=w_G(\boldsymbol{c}-\boldsymbol{c}')=w_H(\phi(\boldsymbol{c}-\boldsymbol{c}'))=w_H(\phi(\boldsymbol{c})-\phi(\boldsymbol{c}'))=d_H(\phi(\boldsymbol{c}),\phi(\boldsymbol{c}'))$，因此，$\phi$是从$C$(Gray距离)到$\phi(C)$(汉明距离)的保矩映射。 证毕

命题2 设$C=(1+v)C_v\oplus vC_{1+v}$是环$R$上长为$n$的线性码，$d_G$为$C$的极小Gray距离，线性码$C_v,C_{1+v}$的维数分别为$k_1,k_2$，生成矩阵为$\boldsymbol{G}_1,\boldsymbol{G}_2$，则$\phi(C)$具有参数$[2n,k_1+k_2,d_G]_{4^m}$和生成矩阵$\begin{pmatrix}\boldsymbol{G}_1&\omega\boldsymbol{G}_1\\\bar{\omega}\boldsymbol{G}_2&\boldsymbol{G}_2\end{pmatrix}$。

证明 由命题1知，$\phi(C)$具有码长$2n$和极小汉明距离d_G。因为$|\phi(C)|=|C|=|C_v|\cdot|C_{1+v}|=(4^m)^{k_1+k_2}$，所以$\phi(C)$具有维数$k_1+k_2$。又因为$C$具有生成矩阵$\begin{pmatrix}(1+v)\boldsymbol{G}_1\\v\boldsymbol{G}_2\end{pmatrix}$，所以$\phi(C)$具有生成矩阵

$$\begin{pmatrix}\phi((1+v)\boldsymbol{G}_1)\\\phi(v\boldsymbol{G}_2)\end{pmatrix}=\begin{pmatrix}\boldsymbol{G}_1&\omega\boldsymbol{G}_1\\\bar{\omega}\boldsymbol{G}_2&\boldsymbol{G}_2\end{pmatrix}$$ 证毕

注 从生成矩阵可以看出，$\phi(C)$的极小距离$d_G\le\min\{2d_H(C_v),2d_H(C_{1+v})\}$，而在非链环$F_q+vF_q(v^2=v)$上常用Gray映射$\varphi:a+vb\to(a,a+b)$的作用下，$d_H(\varphi(C))=\min\{d_H(C_v),d_H(C_{1+v})\}$。对比发现，本文定义的Gray映射能够提高Gray像的极小距离，这对构造参数好的量子码具有重要的意义。

定理2 设C是环R上长为n的线性码，则$\phi(C^{\perp_H})=\phi(C)^{\perp_H}$。特别地，若$C^{\perp_H}\subseteq C$，则$\phi(C)^{\perp_H}\subseteq\phi(C)$。

证明 任取$\boldsymbol{c}_1=(1+v)\boldsymbol{r}_1+v\boldsymbol{q}_1\in C$，$\boldsymbol{c}_2=(1+v)\boldsymbol{r}_2+v\boldsymbol{q}_2\in C^{\perp_H}$，其中$\boldsymbol{r}_1,\boldsymbol{r}_2,\boldsymbol{q}_1,\boldsymbol{q}_2\in F_{4^m}^n$，则

$$\begin{aligned}\langle\boldsymbol{c}_1,\boldsymbol{c}_2\rangle_H&=((1+v)\boldsymbol{r}_1+v\boldsymbol{q}_1)((1+v)\bar{\boldsymbol{r}}_2+v\bar{\boldsymbol{q}}_2)\\&=(1+v)\boldsymbol{r}_1\bar{\boldsymbol{r}}_2+v\boldsymbol{q}_1\bar{\boldsymbol{q}}_2\end{aligned}\quad(5)$$

因为$\langle\boldsymbol{c}_1,\boldsymbol{c}_2\rangle_H=0$，所以$\boldsymbol{r}_1\bar{\boldsymbol{r}}_2=0$且$\boldsymbol{q}_1\bar{\boldsymbol{q}}_2=0$。因此

$$\begin{aligned}\langle\phi(\boldsymbol{c}_1),\phi(\boldsymbol{c}_2)\rangle_H =&\phi(\boldsymbol{c}_1)\overline{\phi(\boldsymbol{c}_2)}\\ =&(\boldsymbol{r}_1+\bar{\omega}\boldsymbol{q}_1)(\bar{\boldsymbol{r}}_2+\omega\bar{\boldsymbol{q}}_2)\\ &+(\omega\boldsymbol{r}_1+\boldsymbol{q}_1)(\bar{\omega}\bar{\boldsymbol{r}}_2+\bar{\boldsymbol{q}}_2)\\ =&(1+\omega\bar{\omega})\boldsymbol{r}_1\bar{\boldsymbol{r}}_2+(1+\omega\bar{\omega})\boldsymbol{q}_1\bar{\boldsymbol{q}}_2=0\end{aligned} \tag{6}$$

这表明$\phi(C^{\perp_H})\subseteq\phi(C)^{\perp_H}$。另外，

$$|\phi(C^{\perp_H})|=|C^{\perp_H}|=\frac{|R|^n}{|C|}=\frac{(4^m)^{2n}}{|\phi(C)|}=|\phi(C)^{\perp_H}| \tag{7}$$

因此，$\phi(C^{\perp_H})=\phi(C)^{\perp_H}$。特别地，若$C^{\perp_H}\subseteq C$，则$\phi(C)^{\perp_H}=\phi(C^{\perp_H})\subseteq\phi(C)$。　证毕

4　环R上的厄米特对偶包含常循环码

设$C=(1+v)C_v\oplus vC_{1+v}$是环$R$上长为$n$的线性码，$\lambda=\alpha+v\beta=(1+v)\alpha+v(\alpha+\beta)$是环$R$的一个单位，其中$\alpha,\beta\in F_{4^m}$。文献[16]给出了环$F_{q^2}+vF_{q^2}$上常循环码的一些基本性质，$q$为素数方幂。令其中$q=2^m$，可以直接得到下面两个结论。

命题3　C是环R上的λ-常循环码当且仅当C_v是域F_{4^m}上的α-常循环码，C_{1+v}是域F_{4^m}上的$(\alpha+\beta)$-常循环码。

命题4　设C是环R上的λ-常循环码，则$C^{\perp_H}=(1+v)C_v^{\perp_H}\oplus vC_{1+v}^{\perp_H}$，其中$C_v^{\perp_H}$，$C_{1+v}^{\perp_H}$分别是域$F_{4^m}$上的$\alpha^{-2^m}$-常循环码和$(\alpha+\beta)^{-2^m}$-常循环码。

从命题4容易得出：

引理1　设C是环R上的λ-常循环码，则$C^{\perp_H}\subseteq C$的充分必要条件是$C_v^{\perp_H}\subseteq C_v$且$C_{1+v}^{\perp_H}\subseteq C_{1+v}$。

由命题3、命题4及引理1易知，满足$C^{\perp_H}\subseteq C$的必要条件是$\alpha^{-2^m}=\alpha$且$(\alpha+\beta)^{-2^m}=\alpha+\beta$，即$C^{\perp_H}$也是环$R$上的$\lambda$-常循环码。

引理2　设C是环R上的λ-常循环码，ω是有限域F_{4^m}的一个本原元。令$\alpha=\omega^{\mu_1(2^m-1)},\alpha+\beta=\omega^{\mu_2(2^m-1)}$，其中$\mu_1,\mu_2\in\{0,1,\cdots,2^m\}$，则$C^{\perp_H}$也是环$R$上的$\lambda$-常循环码。

证明　因为$\omega^{4^m}=\omega$，所以$\alpha^{-2^m}=\omega^{\mu_1(-4^m+2^m)}=\omega^{\mu_1(2^m-1)}=\alpha$。类似地，可以证明$(\alpha+\beta)^{-2^m}=\alpha+\beta$。由命题4和命题3知，$C^{\perp_H}$也是环$R$上的$\lambda$-常循环码。　证毕

接下来补充一个有限域F_{q^2}(q为素数方幂)上厄米特对偶包含常循环码的结论。设$\mathfrak{C}=\langle g(x)\rangle$是有限域$F_{q^2}$上长为$n$的$\eta$-常循环码，$\mathrm{ord}_{q^2}(\eta)=r$且$\gcd(q,n)=1$，则存在一个$rn$次本原单位根$\delta$使得$\delta^n=\eta$，即$x^n-\eta=\prod_{i=0}^{n-1}(x-\delta^{1+ir})$。令$\Omega=\{1+ir|0\le i\le n-1\}n-1\}$，对每个$j\in\Omega$，记$C_j^{rn}$为包含$j$的$q^2$-模$rn$的分圆陪集。称集合$Z=\{j\in\Omega|g(\delta^j)=0\}$为常循环码$\mathfrak{C}$的定义集，它是一些分圆陪集$C_j^{rn}$的并集。

引理3[3]　设$\mathfrak{C}$是有限域F_{q^2}上长为n的η-常循环码，其定义集为Z。若$\mathfrak{C}^{\perp_H}$也是一个η-常循环码，则$\mathfrak{C}^{\perp_H}\subseteq\mathfrak{C}$当且仅当$Z\cap Z^{-q}=\varnothing$，其中$Z^{-q}=\{-qj \mod rn|j\in Z\}$。

根据引理1—引理3，可以得到环R上常循环码是厄米特对偶包含码的一个判定条件。

定理3　设C是环R上长为n的λ-常循环码，$\alpha=\omega^{\mu_1(2^m-1)},\alpha+\beta=\omega^{\mu_2(2^m-1)}$，$\mu_1,\mu_2\in\{0,1,\cdots,2^m\}$。设$Z_1$和$Z_2$分别是域$F_{4^m}$上常循环码$C_v$和$C_{1+v}$的定义集，则$C^{\perp_H}\subseteq C$当且仅当$Z_i\cap {Z_i}^{-2^m}=\varnothing$, $i=1,2$, 其中${Z_i}^{-2^m}=\{-2^mj \mod r_in|j\in Z_i\}$, $r_1=\mathrm{ord}_{4^m}(\alpha)$, $r_2=\mathrm{ord}_{4^m}(\alpha+\beta)$。

证明　由引理2知，当$\alpha=\omega^{\mu_1(2^m-1)}$，$\alpha+\beta=\omega^{\mu_2(2^m-1)}$时，$C_v^{\perp_H}$是域$F_{4^m}$上的$\alpha$-常循环码，$C_{1+v}^{\perp_H}$是域$F_{4^m}$上的$(\alpha+\beta)$-常循环码。根据引理3，此时$C_v^{\perp_H}\subseteq C_v$及$C_{1+v}^{\perp_H}\subseteq C_{1+v}$当且仅当$Z_i\cap {Z_i}^{-2^m}=\varnothing$。再由引理1及等价的传递性可知，$C^{\perp_H}\subseteq C$当且仅当$Z_i\cap {Z_i}^{-2^m}=\varnothing$。　证毕

5　2^m元域上量子码的构造

设$\lambda=(1+v)\alpha+v(\alpha+\beta)$，且$\alpha=\omega^{\mu_1(2^m-1)}$，$\alpha+\beta=\omega^{\mu_2(2^m-1)}$，$\mu_1,\mu_2\in\{0,1,\cdots,2^m\}$。根据定理1—定理3，本节给出一种利用环$R$上$\lambda$-常循环码来构造$2^m$元量子码的方法，具体如下：

定理4　设$C=(1+v)C_v\oplus vC_{1+v}$是环$R$上长为$n$的$\lambda$-常循环码，$Z_1$和$Z_2$分别是码$C_v$和$C_{1+v}$的定义集，若对$i=1,2$都有$Z_i\cap {Z_i}^{-2^m}=\varnothing$成立，则存在一个参数为$[[2n,2k-2n,\ge d]]_{2^m}$的量子码，其中$k$和$d$分别为线性码$\phi(C)$的维数和极小汉明距离。

证明　根据定理3，若对$i=1,2$都有$Z_i\cap {Z_i}^{-2^m}=\varnothing$成立，则$C^{\perp_H}\subseteq C$。再由定理2可得$\phi(C)^{\perp_H}\subseteq\phi(C)$，即$\phi(C)$是有限域$F_{4^m}$上的厄米特对偶包含码。又因为$\phi(C)$具有参数$[2n,k,d]_{4^m}$，由定理1知，存在一个参数为$[[2n,2k-2n,\ge d]]_{2^m}$的量子码。　证毕

下面通过两个具体的例子来解释定理4中的构造方法。

例1　设$m=2$, $n=17$, $\mu_1=0$, $\mu_2=1$，则$\alpha=\omega^0=1$, $\alpha+\beta=\omega^3$，即C是环$R=F_{4^2}+vF_{4^2}$上长为17的$(1+v+v\omega^3)$-常循环码。易知$\mathrm{ord}_{4^2}(\alpha)=1$, $\mathrm{ord}_{4^2}(\alpha+\beta)=5$。设$Z_1=C_1^{17}=\{1,16\}$, $Z_2=C_1^{85}\cup C_6^{85}=\{1,16,6,11\}$，则$C_v=\langle g_1(x)\rangle=\langle x^2+\omega^3x+1\rangle$，$C_{1+v}=\langle g_2(x)\rangle=\langle(x^2+\omega^2x+\omega^3)(x^2+\omega^3x+\omega^3)\rangle$。此外，$Z_1^{-4}=\{13,4\}$，$Z_2^{-4}=\{81,21,61,41\}$。因此对$i=1,2$有$Z_i\cap {Z_i}^{-4}=\varnothing$。由

命题2知，$\phi(C)$具有码长34和维数28。借助MAGMA软件，通过命题2中生成矩阵可以计算出$\phi(C)$的极小汉明距离为5。因此，$\phi(C)$具有参数$[34,28,5]_{4^2}$。根据定理4，可以构造出一个参数为$[[34,22,\geq 5]]_4$的新量子码。类似地，利用环$R=F_{4^2}+vF_{4^2}$上长为17的$(1+v+v\omega^3)$-常循环码，通过选择不同的定义集，可以得到多个码长为34的4元新量子码，如表1所示，其中生成多项式$x^k+a_1x^{k-1}+\cdots+a_{k-1}x+a_k$被简记为$1a_1\cdots a_k$。

注 从极小距离d和码率$\dfrac{k}{n}$两个方面，将表1中量子码与通用量子码表文献[17]中相近长度的最优量子码参数进行比较，可以发现：$[[34,22,\geq 5]]_4$比文献[17]中的$[[33,21,4]]_4$及$[[36,22,4]]_4$具有更好的参数；$[[34,18,\geq 6]]_4$比文献[17]中的$[[33,13,5]]_4$及$[[32,15,6]]_4$参数更好；$[[34,14,\geq 7]]_4$和$[[34,10,\geq 8]]_4$分别比文献[17]中的$[[32,10,7]]_4$和$[[33,6,8]]_4$的码率更大；$[[34,6,\geq 9]]_4$比文献[17]中的$[[40,2,8]]_4$具有更好的参数。

例 2 设 $m=3,n=35,\mu_1=0,\mu_2=3$，则$\alpha=\omega^0=1$，$\alpha+\beta=\omega^{21}$，即C是环$R=F_{4^3}+vF_{4^3}$上长为35的$(1+v+v\omega^{21})$-常循环码。易知$\mathrm{ord}_{4^3}(\alpha)=1$，$\mathrm{ord}_{4^3}(\alpha+\beta)=3$。设$Z_1=C_5^{35}\cup C_6^{35}=\{5,6,34\}$，$Z_2=C_{10}^{105}=\{10\}$，则$C_v=\langle g_1(x)\rangle=\langle(x+\omega^9)(x^2+\omega^{57}x+\omega^9)\rangle$，$C_{1+v}=\langle g_2(x)\rangle=\langle x+\omega^6\rangle$。此外，$Z_1^{-8}=\{30,22,8\}$，$Z_2^{-8}=\{25\}$。因此对$i=1,2$有$Z_i\cap Z_i^{-8}=\varnothing$。由命题2知，$\phi(C)$具有码长70和维数66。借助MAGMA 软件，通过命题2中生成矩阵可以计算出$\phi(C)$的极小汉明距离为4。因此，$\phi(C)$具有参数$[70,66,4]_{8^2}$。根据定理4，可以构造出一个参数为$[[70,62,\geq 4]]_8$的新量子码，它比量子码表文献[17]中的$[[70,46,3]]_8$具有更大的极小距离和维数。

表2和表3分别利用环$F_{4^2}+vF_{4^2}$及$F_{4^3}+vF_{4^3}$上长为n的常循环码构造出一些不同长度的4元和8元新量子码。与量子码表文献[17]及文献[15]中的量子码相比，它们具有更大的码率或者极小距离，即参数更优。特别地，表中量子码$[[6,2,3]]_4$, $[[10,2,5]]_8$, $[[14,10,3]]_8$, $[[14,8,4]]_8$, $[[42,38,3]]_8$为量子MDS码(量子码参数$[[n,k,d]]_q$必须满足$2d\leq n-k+2$，使等式成立的量子码称为量子MDS码)。此外，量子码$[[30,24,\geq 3]]_4$，$[[34,26,\geq 4]]_4$，$[[70,62,\geq 4]]_8$，$[[98,92,\geq 3]]_8$，$[[126,118,\geq 4]]_8$的参数满足$2d\geq n-k$。考虑到当$n>q^2+2$时，量子MDS码不存在，因此这些码的参数也是最优的。

6 结束语

本文定义了一个从有限环$R=F_{4^m}+vF_{4^m}$到有限域F_{4^m}上的Gray映射，研究了环R上厄米特对偶包含常循环码的条件，在此基础上提出了一种构造

表 1 码长为34的新的4元量子码

$g_1(x)$	$g_2(x)$	$\phi(C)$	$[[n,k,d]]_4$
$1\omega^3 1$	$(1\omega^2\omega^3)(1\omega^3\omega^3)$	$[34,28,5]_{16}$	$[[34,22,\geq 5]]_4$
$(1\omega^3 1)(1\omega^6 1)$	$(1\omega^2\omega^3)(1\omega^3\omega^3)$	$[34,26,6]_{16}$	$[[34,18,\geq 6]]_4$
$(1\omega^3 1)(1\omega^6 1)$	$(1\omega^3\omega^3)(1\omega^{11}\omega^3)(1\omega^{13}\omega^3)$	$[34,24,7]_{16}$	$[[34,14,\geq 7]]_4$
$(1\omega^3 1)(1\omega^6 1)(1\omega 1)$	$(1\omega^3\omega^3)(1\omega^{11}\omega^3)(1\omega^{13}\omega^3)$	$[34,22,8]_{16}$	$[[34,10,\geq 8]]_4$
$(1\omega^3 1)(1\omega^6 1)(1\omega 1)$	$(1\omega^3\omega^3)(1\omega^{11}\omega^3)(1\omega^{13}\omega^3)(1\omega^6\omega^3)$	$[34,20,9]_{16}$	$[[34,6,\geq 9]]_4$

表 2 新的4元量子码

n	λ	$g_1(x)$	$g_2(x)$	$\phi(C)$	$[[n,k,d]]_4$	$[[n',k',d']]_4$
3	$1+v+v\omega^3$	$1\omega^5$	1ω	$[6,4,3]_{16}$	$[[6,2,3]]_4$	MDS
7	$1+v+v\omega^3$	1011	$1\omega^9 0\omega^{12}$	$[14,8,6]_{16}$	$[[14,2,\geq 6]]_4$	$[[14,0,4]]_4$[15]
11	$1+v+v\omega^3$	$1\omega^5 11\omega^{10} 1$	$1\omega^8\omega^6\omega^9\omega^7 1$	$[22,12,7]_{16}$	$[[22,2,\geq 7]]_4$	$[[24,0,6]]_4$[17]
15	1	$(1\omega)(1\omega^2)$	$1\omega^4$	$[30,27,3]_{16}$	$[[30,24,\geq 3]]_4$	$[[31,21,3]]_4$[17]
17	1	$1\omega^3 1$	$1\omega^6 1$	$[34,30,4]_{16}$	$[[34,26,\geq 4]]_4$	$[[34,24,4]]_4$[15]
19	$1+v+v\omega^3$	$1\omega^{10}0\omega^{10}\omega^{10}\omega^5\omega^5\omega^5 1$	$1\omega^7 0\omega\omega^{13}\omega^5\omega^2\omega^{11}\omega^8$	$[38,20,11]_{16}$	$[[38,2,\geq 11]]_4$	$[[40,2,8]]_4$[17]
45	1	$(1\omega)(100\omega^4)$	$(1\omega^2)(100\omega^5)$	$[90,82,4]_{16}$	$[[90,74,\geq 4]]_4$	$[[90,66,4]]_4$[17]
63	$1+v+v\omega^3$	$111\omega^5$	1ω	$[126,122,3]_{16}$	$[[126,118,\geq 3]]_4$	$[[127,113,3]]_4$[17]
77	1	$1\omega^5 11\omega^{10} 1$	1011	$[154,146,4]_{16}$	$[[154,138,\geq 4]]_4$	$[[154,128,4]]_4$[17]
85	1	$(1\omega^2\omega^3)(1\omega^4\omega^6)$	$(1\omega^9\omega^9)(1\omega^8\omega^{12})$	$[170,162,4]_{16}$	$[[170,154,\geq 4]]_4$	$[[171,151,4]]_4$[17]
91	$1+v+v\omega^3$	$1\omega^4\omega^{13} 1$	$(1\omega^3\omega^8\omega^9)(1\omega^7\omega^4\omega^9)$	$[182,173,5]_{16}$	$[[182,164,\geq 5]]_4$	$[[185,149,5]]_4$[17]

表 3　新的8元量子码

n	λ	$g_1(x)$	$g_2(x)$	$\phi(C)$	$[[n,k,d]]_8$	$[[n',k',d']]_8$
5	$1+v+v\omega^7$	$1\omega^{42}1$	$1\omega^{56}\omega^{28}$	$[10,6,5]_{64}$	$[[10,2,5]]_8$	MDS
7	$1+v+v\omega^{21}$	$1\omega^9$	$1\omega^3$	$[14,12,3]_{64}$	$[[14,10,3]]_8$	MDS
7	$1+v+v\omega^{21}$	$1\omega^9$	$(1\omega^3)(1\omega^{12})$	$[14,11,4]_{64}$	$[[14,8,4]]_8$	MDS
21	$1+v+v\omega^{21}$	$1\omega^3$	1ω	$[42,40,3]_{64}$	$[[42,38,3]]_8$	MDS
35	$1+v+v\omega^{21}$	$(1\omega^9)(1\omega^{57}\omega^9)$	$1\omega^6$	$[70,66,4]_{64}$	$[[70,62,\geq 4]]_8$	$[[70,46,3]]_8$[17]
39	$1+v+v\omega^{21}$	$(1\omega^{47}\omega^{42})(1\omega^{31}\omega^{21})$	$(1\omega^{27}\omega^{35})(1\omega^{45}\omega^{14})$	$[78,70,5]_{64}$	$[[78,62,\geq 5]]_8$	$[[78,46,5]]_8$[17]
49	$1+v+v\omega^7$	$1\omega^9$	$(1\omega^{22})(1\omega^{31})$	$[98,95,3]_{64}$	$[[98,92,\geq 3]]_8$	$[[99,89,3]]_8$[17]
63	1	$(1\omega)(1\omega^2)$	$(1\omega^3)(1\omega^4)$	$[126,122,4]_{64}$	$[[126,118,\geq 4]]_8$	$[[127,113,3]]_8$[17]
65	$1+v+v\omega^{21}$	$(1\omega^4 1)(1\omega^8 1)$	$(1\omega^{52}\omega^{21})(1\omega^{19}\omega^{21})$	$[130,122,5]_{64}$	$[[130,114,\geq 5]]_8$	$[[133,113,5]]_8$[17]
73	$1+v+v\omega^7$	$1\omega^{36}01$	$10\omega^{50}\omega^{21}$	$[146,140,4]_{64}$	$[[146,134,\geq 4]]_8$	$[[147,122,4]]_8$[17]
91	$1+v+v\omega^7$	$(1\omega^9)(1\omega^{31}\omega^{36})$	$(1\omega^{52})(1\omega^{44}\omega^{50})(1\omega^{61})$	$[182,175,5]_{64}$	$[[182,168,\geq 5]]_8$	$[[183,143,4]]_8$[17]

2^m元量子码的新方法，并据此构造了有限域F_4和F_8上的一些新量子码。通过不同有限环上的常循环码构造更多2^m元新量子码是一个值得继续探索的问题。

参 考 文 献

[1] CALDERBANK A R, RAINS E M, SHOR P M, *et al.* Quantum error correction via codes over GF(4)[J]. *IEEE Transactions on Information Theory*, 1998, 44(4): 1369–1387. doi: 10.1109/18.681315.

[2] ASHIKHMIN A and KNILL E. Nonbinary quantum stabilizer codes[J]. *IEEE Transactions on Information Theory*, 2001, 47(7): 3065–3072. doi: 10.1109/18.959288.

[3] KAI Xiaoshan, ZHU Shixin, and LI Ping. Constacyclic codes and some new quantum MDS codes[J]. *IEEE Transactions on Information Theory*, 2014, 60(4): 2080–2086. doi: 10.1109/TIT.2014.2308180.

[4] CHEN Bocong, LING San, and ZHANG Guanghui. Application of constacyclic codes to quantum MDS codes[J]. *IEEE Transactions on Information Theory*, 2015, 61(3): 1474–1484. doi: 10.1109/TIT.2015.2388576.

[5] 朱士信, 黄山, 李锦. 有限域上常循环厄密特对偶包含码及其应用[J]. 电子与信息学报, 2018, 40(5): 1072–1078. doi: 10.11999/JEIT170735.

ZHU Shixin, HUANG Shan, and LI Jin. Constacyclic Hermitian dual-containing codes over finite fields and their application[J]. *Journal of Electronics & Information Technology*, 2018, 40(5): 1072–1078. doi: 10.11999/JEIT170735.

[6] QIAN Jianfa, MA Wenping, and GUO Wangmei. Quantum codes from cyclic codes over finite ring[J]. *International Journal of Quantum Information*, 2009, 7(6): 1277–1283. doi: 10.1142/S0219749909005560.

[7] QIAN Jianfa. Quantum codes from cyclic codes over F_2+vF_2[J]. *Journal of Information and Computational Science*, 2013, 10(6): 1715–1722. doi: 10.12733/jics20101705.

[8] ASHRAF M and MOHAMMAD G. Construction of quantum codes from cyclic codes over F_p+vF_p[J]. *International Journal of Information and Coding Theory*, 2015, 3(2): 137–144. doi: 10.1504/IJICOT.2015.072627.

[9] GAO Jian and WANG Yongkang. u-Constacyclic codes over F_P+uF_p and their applications of constructing new non-binary quantum codes[J]. *Quantum Information Processing*, 2018, 17(1): 4. doi: 10.1007/s11128-017-1775-8.

[10] ALAHMADI A, ISLAM H, PRAKASH O, *et al.* New quantum codes from constacyclic codes over a non-chain ring[J]. *Quantum Information Processing*, 2021, 20(2): 60. doi: 10.1007/s11128-020-02977-y.

[11] ISLAM H, PRAKASH O, and VERMA R K. New quantum codes from constacyclic codes over the ring $R_{k,m}$[J]. *Advances in Mathematics of Communications*, 2022, 16(1): 17–35. doi: 10.3934/amc.2020097.

[12] WANG Yu, KAI Xiaoshan, SUN Zhonghua, *et al.* Quantum codes from Hermitian dual-containing constacyclic codes over $\mathbb{F}_{q^2}+v\mathbb{F}_{q^2}$[J]. *Quantum Information Processing*, 2021, 20(3): 122. doi: 10.1007/s11128-021-03052-w.

[13] SHI Xiaoping, HUANG Xinmei, and YUE Qin. Construction of new quantum codes derived from constacyclic codes over $F_{q^2}+uF_{q^2}+\cdots+u^{r-1}F_{q^2}$[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2021, 32(5): 603–620. doi: 10.1007/s00200-020-00415-1.

[14] ISLAM H, PATEL S, PRAKASH O, *et al.* A family of

constacyclic codes over a class of non-chain rings $A_{q,r}$ and new quantum codes[J]. *Journal of Applied Mathematics and Computing*, 2022, 68(4): 2493–2514. doi: 10.1007/s12190-021-01623-9.

[15] TANG Yongsheng, YAO Ting, SUN Zhonghua, *et al*. Nonbinary quantum codes from constacyclic codes over polynomial residue rings[J]. *Quantum Information Processing*, 2020, 19(3): 84. doi: 10.1007/s11128-020-2584-z.

[16] LIU Yan, SHI Minjia, SEPASDAR Z, *et al*. Construction of Hermitian self-dual constacyclic codes over $F_{q^2}+vF_{q^2}$[J]. *Applied and Computational Mathematics*, 2016, 15(3): 359–369.

[17] EDEL Y. Some good quantum twisted codes[EB/OL]. https://www.mathi.uni-heidelberg.de/~yves/Matritzen/QTBCH/QTBCHIndex.html, 2022.

王　玉：男，副教授，博士，研究方向为代数编码.

开晓山：男，教授，博士生导师，研究方向为代数编码.

朱士信：男，教授，博士生导师，研究方向为代数编码理论、信息安全与序列密码等.

责任编辑：马秀强