第25卷第4期 数 学 研 究 与 评 论 Vol.25, No.4
2005年11月 JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION Nov., 2005

文章编号: 1000-341X(2005)04-0739-10 **文献标识码**: A

Z_{16} 环上的二次剩余码

谭晓青
(暨南大学数学系, 广东 广州 510632)
(E-mail: txqdoudou@163.com)

摘 要: 本文研究了整数环模 16 剩余类环 Z_{16} 上的二次剩余码, 讨论了它们的幂等生成元及其扩展码的自对偶性等代数性质, 并研究了码长为 7 的 Z_{16} 二次剩余码在两种已有的 Gray 映射下的有趣性质, 尤其是确定了它们的 Lee 重量分布.

关键词: 二次剩余码; 幂等生成元; Gray 映射; Hamming 重量; Lee 重量.
MSC(2000): 94B15
中图分类: O157.4

1 引 言

A.R.Hammons 等人在文 [1] 中研究了 Gray 映射从 Z_4(整数环模 4 的剩余类环) 码获得的非线性二元码, 进而发现许多好的经典非线性码 Kerdock 码、 Preparata 码、 Goethals 码及其相关码均可表示为 Z_4 循环码在 Gray 映射下的像, 从此, 环上码的研究逐渐成为近年来编码领域的热点 [2-6 等]. 二元二次剩余码 (QR 码) 是能被它们的幂等生成元很好定义的循环码, 并且我们知道许多中等大小的 QR 码的最小重量 d, 相对码长 p 而言, d 是相当大的. 因此, 二元 QR 码是一类经典的 "好码". 随着环上码的研究, 一些编码学家也试着探讨环上的 QR 码 [2,6-8]. V.S.Pless 等人在文 [2] 中定义了环 Z_4 上的 QR 码并讨论了其若干性质, 并给出了很有趣的二元码. M.H.Chiu, Stephen Yau 和 Y.Yu 等人则在文 [7] 中定义了 Z_8 上的 QR 码并讨论了其性质, P.Kanwar 的文 [8] 在文 [2] 的基础上试图探讨了一般整数环模 q^m 的剩余类环 Z_{q^m} 下的 QR 码, 但是其所得到的结果主要是理论结果, 应用性不强, 其文也没有给出合适的一般情况下 QR 码的例子. 本文首次定义了环 Z_{16} 上的 QR 码, 并讨论了它们及其扩展码的性质, 文末还给出了码长为 7 的 Z_{16}-QR 码在两种 Gray 映射下的重量分布及其最小重量的一些有趣性质.

2 预备知识

我们先回顾一下环 R 上码的一些定义. 令 $R = Z_{p^m}$, Z_{p^m} 表示整数环模 p^m 的剩余类环. $Z_{p^m}^n$ 表示环 Z_{p^m} 上 n 重向量空间, $Z_{p^m}^n$ 形成一个秩为 n 的自由 Z_{p^m}- 模. $Z_{p^m}^n$ 的任意非空子集称为码长为 n 的 Z_{p^m}- 码. $Z_{p^m}^n$ 的任意 Z_{p^m}- 子模称为码长为 n 的 Z_{p^m}- 线性码. 对于码长为 n 的 Z_{p^m}- 线性码 C, 若有 $(c_0, c_1, c_2, \cdots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, c_1, \cdots, c_{n-2}) \in C$, 则称该线性码是码长为 n 的 Z_{p^m}- 循环码.

定义 2.1 设 p 为一素数, 若 $e(x) \in Z_{p^m}[x]/(x^n-1)$ 满足: $e(x)^2 \equiv e(x) (\mathrm{mod}\quad (x^n-1))$ 则称 $e(x)$ 为 $Z_{p^m}[x]/(x^n-1)$ 的幂等元, 也简称之为 Z_{p^m}- 幂等元.

收稿日期: 2003-05-08

能生成循环码的幂等元 $e(x)$ 称为幂等生成元，文 [7] 已经证明某些 Z_{p^m}- 循环码存在幂等生成元：

引理 2.1 令 C 是码长为 n 的 Z_{p^m}- 循环码，如果 $C=(f)$，若 g 满足 $fg=x^n-1$，且 g 还使得 f 与 g 互素，则 C 在 $Z_{p^m}[x]/(x^n-1)$ 上有一个幂等生成元，且这个幂等生成元生成的循环码是唯一的.

如果已知一个 Z_{p^m}- 循环码的幂等生成元，则由下面的引理能得到其对偶码的幂等生成元 (一个码 C 的对偶码是 $C^{\perp}=\{u\in V\mid u\cdot w=0,$ 对所有的 $w\in C\}$[9], 这里 $V=Z_{p^m}^n$).

引理 2.2 若 Z_{p^m}- 循环码 C 有幂等生成元 $e(x)$, 则其对偶码 $C^{\perp}$ 有幂等生成元 $1-e(x^{-1})$.

若 e_1 和 e_2 是 Z_{16}- 幂等元，容易验证 e_1e_2 和 $e_1+e_2-e_1e_2$ 也是 Z_{16}- 幂等元. 令 $C_1=(e_1)$ 和 $C_2=(e_2)$, 易证 e_1e_2 与 $e_1+e_2-e_1e_2$ 分别是 $C_1\bigcap C_2$ 与 C_1+C_2 的乘法单位元，于是这证明了以下引理

引理 2.3 设 C_1 与 C_2 为 Z_{16}- 循环码，e_1 和 e_2 分别是其 Z_{16}- 幂等生成元，则 $C_1\bigcap C_2$ 有 Z_{16}- 幂等生成元 e_1e_2, C_1+C_2 有 Z_{16}- 幂等生成元 $e_1+e_2-e_1e_2$.

3 Z_{16} 环上的二次剩余 (QR) 码

3.1 Z_{16}-QR 码的定义

设 $p\equiv\pm1(\mathrm{mod}\ 8)$ 且 p 为素数 [2], 令 $e_1=\sum_{i\in Q}x^i$, $e_2=\sum_{i\in N}x^i$, 这里 Q 是 p 的二次剩余集，N 是 p 的二次非剩余集. 显然，当 $p\equiv-1(\mathrm{mod}\ 8)$ 时，e_1 和 e_2 即为二元 $[p,(p+1)/2]$QR 码的幂等生成元；当 $p\equiv1(\mathrm{mod}\ 8)$ 时，e_1 和 e_2 即为二元 $[p,(p-1)/2]$QR 码的幂等生成元. 从文 [3] 中，得知 e_1 与 e_2 的二次幂有以下结论：

1. 当 $p\equiv-1(\mathrm{mod}\ 8)$ 即 $p+1=8r$ 时：
(1.1) $e_1^2=2re_1+2re_2-e_1$;
(1.2) $e_2^2=2re_1+2re_2-e_2$.

2. 当 $p\equiv1(\mathrm{mod}\ 8)$ 即 $p-1=8r$ 时：
(2.1) $e_1^2=2re_1+2re_2-e_1+4r$;
(2.1) $e_2^2=2re_1+2re_2-e_2+4r$.

于是，得

1. 当 $p\equiv-1(\mathrm{mod}\ 16)$ 即 $p+1=16r$ 时：
(1.1) $e_1^2=4re_1+4re_2-e_1$;
(1.2) $e_2^2=4re_1+4re_2-e_2$.

2. 当 $p\equiv1(\mathrm{mod}\ 16)$ 即 $p-1=16r$ 时：
(2.1) $e_1^2=4re_1+4re_2-e_1+8r$;
(2.2) $e_2^2=4re_1+4re_2-e_2+8r$.

3. 当 $p\equiv7(\mathrm{mod}\ 16)$ 即 $p-7=16r$ 时：
(3.1) $e_1^2=4re_1+4re_2+2e_2+e_1$;
(3.2) $e_2^2=4re_1+4re_2+2e_1+e_2$.

4. 当 $p\equiv-7(\mathrm{mod}\ 16)$ 即 $p+7=16r$ 时：
(4.1) $e_1^2=4re_1+4re_2-3e_1-2e_2+8r-4$;
(4.2) $e_2^2=4re_1+4re_2-3e_2-2e_1+8r-4$.

Z_{16} 表示整数环模 16 的剩余类环，显然 Z_{16} 有零因子 2,4,8,12. 令 $R_p=Z_{16}[x]/(x^p-1)$. 定义变换 $\mu_a: i\to ai(\mathrm{mod}\ p)(a\in GF(p)$且$a$非零). 若 $f=\sum_{i=0}^{p-1}c_ix^i\in R_p$, 则

$$\mu_a(f)=\sum_{i=0}^{p-1}c_{\mu_a(i)}x^{\mu_a(i)}\quad(\mu_a(i)\equiv ai(\mathrm{mod}\ p)).$$

不难证明 $\mu_a(fg)=\mu_a(f)\mu_a(g)$, f 与 g 为 R_p 上的多项式. 全 1 向量 $1+e_1+e_2$, 记为 h. 我们知道在二元情形下，h 为 $Z_2[x]/(x^p-1)$ 的一个幂等元，而在 R_p 上，$x^p=1\Rightarrow x^{p+t}=x^t\Rightarrow x^ih=h\Rightarrow h^2=(1+e_1+e_2)h=h+\frac{p-1}{2}h+\frac{p-1}{2}h=ph$. 那么，当 $p\equiv-1(\mathrm{mod}\ 8)$ 时：若 $p\equiv-1(\mathrm{mod}\ 16)$, $15h$ 是 R_p 的幂等元，$(15h)^2=15h\Rightarrow 2e_1e_2=14+15e_1^2+15e_2^2+13e_1+13e_2$；若 $p\equiv7(\mathrm{mod}\ 16)$,

[2] 注记： 1. 本文中 p 的假定都满足这一基本性质； 2. -1 为 p 的二次剩余当且仅当 $p\equiv1(\mathrm{mod}\ 4)$; 3. 两个二次剩余的乘积，或两个二次非剩余的乘积都是二次剩余；一个二次剩余和一个二次非剩余的乘积是二次非剩余 [9]

$7h$ 是 R_p 的幂等元， $(7h)^2 = 7h \Rightarrow 2e_1e_2 = 6 + 15e_1^2 + 15e_2^2 + 5e_1 + 5e_2$. 当 $p \equiv 1(\mathrm{mod}\ 8)$ 时：若 $p \equiv 1(\mathrm{mod}\ 16)$, h 是 R_p 的幂等元， $(h)^2 = h \Rightarrow 2e_1e_2 = 15e_1^2 + 15e_2^2 + 15e_1 + 15e_2$ ；若 $p \equiv -7(\mathrm{mod}\ 16)$, $9h$ 是 R_p 的幂等元， $(9h)^2 = 9h \Rightarrow 2e_1e_2 = 8 + 15e_1^2 + 15e_2^2 + 7e_1 + 7e_2$.

有了前面的这些分析，可以得到 R_p 上的幂等元.

定理 3.1.1 设 p 为素数，且 $p \equiv \pm 1(\mathrm{mod}\ 16)$, $R_p = Z_{16}[x]/(x^p - 1)$.

当 $p \equiv -1(\mathrm{mod}\ 16)$ 即 $p + 1 = 16r$ 时：

1. 若 $r = 4k$, $1 + e_i$ 和 $15e_i$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$;
2. 若 $r = 4k + 1$, $8 + 3e_i + 12e_j$ 和 $9 + 4e_i + 13e_j$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$;
3. 若 $r = 4k + 2$,$7e_i + 8e_j$ 和 $1 + 8e_i + 9e_j$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$;
4. 若 $r = 4k + 3$, $8 + 4e_i + 11e_j$ 和 $9 + 5e_i + 12e_j$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$.

当 $p \equiv 1(\mathrm{mod}\ 16)$ 即 $p - 1 = 16r$ 时有：

1. 若 $r = 4k$, $1 + e_i$ 和 $15e_i$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$;
2. 若 $r = 4k + 1$, $8 + 4e_i + 11e_j$ 和 $9 + 5e_i + 12e_j$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$;
3. 若 $r = 4k + 2$,$7e_i + 8e_j$ 和 $1 + 8e_i + 9e_j$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$;
4. 若 $r = 4k + 3$, $8 + 3e_i + 12e_j$ 和 $9 + 4e_i + 13e_j$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$.

证明 假定 $p + 1 = 16r$, $r = 4k + 1$.

$$
\begin{aligned}
(8 + 3e_1 + 12e_2)^2 &= 9e_1^2 + 8e_1e_2 \\
&= 9e_1^2 + 4(14 + 15e_1^2 + 15e_2^2 + 13e_1 + 13e_2) \\
&= 8 + 4e_1 + 4e_2 + 5e_1^2 + 12e_2^2 \\
&= 8 + 4e_1 + 4e_2 + 5(4re_1 + 4re_2 - e_1) + 12(4re_1 + 4re_2 - e_2) \\
&= 8 + 4re_1 + 4re_2 - e_1 - 8e_2 \qquad (r = 4k + 1) \\
&= 8 + 3e_1 + 12e_2.
\end{aligned}
$$

同样可证 $(8+3e_2+12e_1)^2 = 8+3e_2+12e_1$, $(9+5e_1+12e_2)^2 = 9+5e_1+12e_2$, $(9+5e_2+12e_1)^2 = 9 + 5e_2 + 12e_1$. 其他情形也类似可证. □

定理 3.1.2 设 p 为素数，且 $p \equiv \pm 7(\mathrm{mod}\ 16)$, $R_p = Z_{16}[x]/(x^p - 1)$.

当 $p \equiv 7(\mathrm{mod}\ 16)$ 即 $p - 7 = 16r$ 时有：

1. 若 $r = 4k$, $5 + 3e_i + 6e_j$ 和 $12 + 10e_i + 13e_j$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$;
2. 若 $r = 4k + 1$, $4 + 9e_i + 14e_j$ 和 $13 + 2e_i + 7e_j$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$;
3. 若 $r = 4k + 2$, $5 + 11e_i + 14e_j$ 和 $12 + 2e_i + 5e_j$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$;
4. 若 $r = 4k + 3$, $4 + e_i + 6e_j$ 和 $13 + 10e_i + 15e_j$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$.

当 $p \equiv -7(\mathrm{mod}\ 16)$ 即 $p + 7 = 16r$ 时有：

1. 若 $r = 4k$, $5 + 3e_i + 6e_j$ 和 $12 + 10e_i + 13e_j$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$;
2. 若 $r = 4k + 1$,$4 + e_i + 6e_j$ 和 $13 + 10e_i + 15e_j$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$;
3. 若 $r = 4k + 2$, $5 + 11e_i + 14e_j$ 和 $12 + 2e_i + 5e_j$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$;
4. 若 $r = 4k + 3$, $4 + 9e_i + 14e_j$ 和 $13 + 2e_i + 7e_j$ 是 R_p 的幂等元，其中 $1 \le i \ne j \le 2$.

证明 假定 $p+7=16r$, $r=4k+2$.

$$\begin{aligned}(5+11e_1+14e_2)^2 &= 9+14e_1+9e_1^2+12e_2+4e_1e_2+4e_2^2\\ &= 9+14e_1+12e_2+9e_1^2+4e_2^2+2(8+15e_1^2+15e_2^2+7e_1+7e_2)\\ &= 9+12e_1+10e_2+7e_1^2+2e_2^2\\ &= 9+12e_1+10e_2+7(4re_1+4re_2-3e_1-2e_2+8r-4)\\ &\quad +2(4re_1+4re_2-3e_2-2e_1+8r-4)\\ &= 5+8r+3e_1+6e_2+4re_1+4re_2 \qquad (r=4k+2)\\ &= 5+11e_1+14e_2.\end{aligned}$$

同样可证 $(5+11e_2+14e_1)^2=5+11e_2+14e_1$, $(12+2e_1+5e_2)^2=12+2e_1+5e_2$, $(12+2e_2+5e_1)^2=12+2e_2+5e_1$. 其他情形也类似可证. □

找到这些 R_p 上的幂等元后，就可以定义环 Z_{16} 上的二次剩余码如下.

定义 3.1.1 如果一个 Z_{16}- 循环码由上述两个定理中的某个幂等元生成，则称该 Z_{16}- 循环码为 Z_{16} 二次剩余码，简记为 Z_{16}-QR 码.

3.2 Z_{16}-QR 码的性质

由 R_p 上幂等元的成对出现并根据 Z_{16}-QR 码的定义，得到 $p\equiv -1(\mathrm{mod}\ 16)$ 情形下的 Z_{16}-QR 码有如下性质.

定理 3.2.1 设 p 为素数，且 $p\equiv -1(\mathrm{mod}\ 16)$ 即 $p+1=16r$ 时，若 $r=4k$，令 $Q_1=(15e_1)$, $Q_2=(15e_2)$, $Q_1'=(1+e_2)$, $Q_2'=(1+e_1)$; 若 $r=4k+1$，令 $Q_1=(8+3e_1+12e_2)$, $Q_2=(8+3e_2+12e_1)$, $Q_1'=(9+4e_1+13e_2)$, $Q_2'=(9+4e_2+13e_1)$; 若 $r=4k+2$，令 $Q_1=(7e_1+8e_2)$, $Q_2=(7e_2+8e_1)$, $Q_1'=(1+8e_1+9e_2)$, $Q_2'=(1+8e_2+9e_1)$; 若 $r=4k+3$，令 $Q_1=(8+4e_1+11e_2)$, $Q_2=(8+4e_2+11e_1)$, $Q_1'=(9+5e_1+12e_2)$, $Q_2'=(9+5e_2+12e_1)$, 则对 Z_{16}-QR 码 Q_1,Q_2,Q_1',Q_2' 有以下结论成立：

(a) Q_1 与 Q_2 等价， Q_1' 与 Q_2' 等价;

(b) $Q_1\cap Q_2=\tilde{h}$, 且 $Q_1+Q_2=R_p$, $\tilde{h}=15h=15(1+e_1+e_2)$;

(c) $|\,Q_1\,|=16^{(p+1)/2}=|\,Q_2\,|$;

(d) $Q_1=Q_1'+(\tilde{h})$, $Q_2=Q_2'+(\tilde{h})$;

(e) $|\,Q_1'\,|=16^{(p-1)/2}=|\,Q_2'\,|$.

证明 我们只证明 $r=4k+1$ 的情形，其他 r 情形类似可证.

(a) 令 x 为 N 中的一个元素 (N 是 p 的二次非剩余集), 于是映射 μ_x 交换 e_1 与 e_2, 即 $\mu_x(e_1)=e_2$, $\mu_x(e_2)=e_1$, 所以 $\mu_x(8+3e_1+12e_2)=8+3e_2+12e_1$ 且 $\mu_x(9+4e_1+13e_2)=9+4e_2+13e_1$, 这样 (a) 得证.

(b) $\tilde{h}=15h=15+15e_1+15e_2=15+(8+3e_1+12e_2)+(8+3e_2+12e_1)$

$$\begin{aligned}&\Rightarrow (8+3e_1+12e_2)\tilde{h}=(8+3e_1+12e_2)[15+(8+3e_1+12e_2)+(8+3e_2+12e_1)]\\ &=15(8+3e_1+12e_2)+(8+3e_1+12e_2)^2+(8+3e_1+12e_2)(8+3e_2+12e_1)\\ &=(8+3e_1+12e_2)(8+3e_2+12e_1).\end{aligned}$$

另一方面： (因为 $8+15(p-1)/2=8+15(16r-1-1)/2=8r-7=32k+1\equiv 1(\mathrm{mod}\ 16)$)

$$(8+3e_1+12e_2)\tilde{h}=8\tilde{h}+3\frac{p-1}{2}\tilde{h}+12\frac{p-1}{2}\tilde{h}=(8+15\frac{p-1}{2})\tilde{h}=\tilde{h},$$

所以 $(8+3e_1+12e_2)(8+3e_2+12e_1)=\tilde{h}$, 由引理 2.3, $Q_1\bigcap Q_2$ 有幂等生成元 $\tilde{h}$, 因此 $|Q_1\bigcap Q_2|=|(\tilde{h})|=16$. 又由引理 2.3, Q_1+Q_2 有幂等生成元： $(8+3e_1+12e_2)+(8+3e_2+12e_1)-(8+3e_1+12e_2)(8+3e_2+12e_1)=15e_1+15e_2-(15+15e_1+15e_2)=1$. 所以 $Q_1+Q_2=R_p$ 且 $|Q_1+Q_2|=16^p$.

(c) 因为 $|Q_1+Q_2|=|Q_1|\cdot|Q_2|/|Q_1\bigcap Q_2|\Rightarrow|Q_1|=|Q_2|=16^{\frac{p+1}{2}}$.

(d) (因为 $7+15\cdot\frac{p-1}{2}=7+15\cdot\frac{(16r-1-1)}{2}=7+15(8r-1)=8r-8=32k\equiv 0(\mathrm{mod}\ 16)$)

$$\begin{aligned}(9+4e_1+13e_2)\tilde{h}&=7h+12e_1h+3e_2h\\&=7h+12\cdot\frac{p-1}{2}\cdot h+3\cdot\frac{p-1}{2}\cdot h\\&=(7+15\cdot\frac{p-1}{2})h=0.\end{aligned}$$

这意味着 $Q_1'\bigcap(\tilde{h})=0$, 由引理 2.3, $Q_1'+(\tilde{h})$ 有幂等生成元 $(9+4e_1+13e_2)+\tilde{h}-(9+4e_1+13e_2)\tilde{h}=9+4e_1+13e_2+15+15e_1+15e_2=8+3e_1+12e_2$, 所以 $Q_1'+(\tilde{h})=(8+3e_1+12e_2)=Q_1$. 同理可证： $Q_2'+(\tilde{h})=Q_2$.

(e) 因为 $16^{\frac{p+1}{2}}=|Q_1|=|Q_1'+(\tilde{h})|=|Q_1'|\cdot|(\tilde{h})|=16\cdot|Q_1'|\Rightarrow|Q_1'|=16^{\frac{p-1}{2}}$. 同理可证： $|Q_2'|=16^{\frac{p-1}{2}}$. □

类似地, 对于 $p\equiv 1(\mathrm{mod}\ 16)$ 情形下的 Z_{16}-QR 码有如下性质.

定理 3.2.2 设 p 为素数, 且 $p\equiv 1(\mathrm{mod}\ 16)$ 即 $p-1=16r$ 时, 若 $r=4k$, 令 $Q_1=(1+e_1)$, $Q_2=(1+e_2)$, $Q_1'=(15e_2)$, $Q_2'=(15e_1)$; 若 $r=4k+1$, 令 $Q_1=(9+5e_1+12e_2)$, $Q_2=(9+5e_2+12e_1)$, $Q_1'=(8+4e_1+11e_2)$, $Q_2'=(8+4e_2+11e_1)$; 若 $r=4k+2$, 令 $Q_1=(1+8e_1+9e_2)$, $Q_2=(1+8e_2+9e_1)$, $Q_1'=(7e_1+8e_2)$, $Q_2'=(7e_2+8e_1)$; 若 $r=4k+3$, 令 $Q_1=(9+4e_1+13e_2)$, $Q_2=(9+4e_2+13e_1)$, $Q_1'=(8+3e_1+12e_2)$, $Q_2'=(8+3e_2+12e_1)$, 则对 Z_{16}-QR 码 Q_1,Q_2,Q_1',Q_2' 有以下结论成立：

(a) Q_1 与 Q_2 等价， Q_1' 与 Q_2' 等价;

(b) $Q_1\cap Q_2=h$ 且 $Q_1+Q_2=R_p$;

(c) $|Q_1|=16^{(p+1)/2}=|Q_2|$;

(d) $Q_1=Q_1'+(h)$, $Q_2=Q_2'+(h)$;

(e) $|Q_1'|=16^{(p-1)/2}=|Q_2'|$;

下面这个定理说明了定义的 Z_{16}-QR 码具有极好的对偶性.

定理 3.2.3 设 p 为素数,

(1) 若 $p\equiv -1(\mathrm{mod}\ 16)$ 即 $p+1=16r$ 时， Q_1,Q_2,Q_1',Q_2' 如定理 3.2.1 定义, 则 Q_1' 与 Q_2' 是自正交码, 且 $Q_1^{\perp}=Q_1'$, $Q_2^{\perp}=Q_2'$;

(2) 若 $p\equiv 1(\mathrm{mod}\ 16)$ 即 $p-1=16r$ 时， Q_1,Q_2,Q_1',Q_2' 如定理 3.2.2 定义, 则 $Q_1^{\perp}=Q_2'$, $Q_2^{\perp}=Q_1'$.

证明 只证明 $r=4k+1$ 的情形, 其他 r 情形类似可证.

(1) 若 $p+1=16r$, 由引理 2.2, $Q_1^{\perp}$ 有幂等生成元： $1-[8+3e_1(x^{-1})+12e_2(x^{-1})]=9+13e_1(x^{-1})+4e_2(x^{-1})=9+13e_2+4e_1$, (因为 $p\equiv -1(\mathrm{mod}\ 16)$, 所以 -1 是 p 的二次非剩余,

$\Rightarrow e_1(x^{-1})=e_2(x), e_2(x^{-1})=e_1(x)$). 因此 $Q_1^{\perp}=Q_1'$, 且 $Q_1'\subseteq Q_1=Q_1'^{\perp}$, 所以 Q_1' 是自正交码. 同理可证 $Q_2^{\perp}=Q_2'$, 且 Q_2' 是自正交码.

(2) 若 $p-1=16r$, 由引理 2.2, $Q_1^{\perp}$ 有幂等生成元: $1-[9+5e_1(x^{-1})+12e_2(x^{-1})]=8+11e_1(x^{-1})+4e_2(x^{-1})=8+11e_1+4e_2$, (因为 $p\equiv 1(\mathrm{mod}\ 16)$, 所以 -1 是 p 的二次剩余, $\Rightarrow e_1(x^{-1})=e_1(x), e_2(x^{-1})=e_2(x)$). 因此 $Q_1^{\perp}=Q_2'$, 同理可证 $Q_2^{\perp}=Q_1'$. □

对于 $p\equiv\pm 7(\mathrm{mod}\ 16)$ 情形下的 Z_{16}-QR 码类似的有如下性质 (包括其对偶性质).

定理 3.2.4 设 p 为素数, 且 $p\equiv 7(\mathrm{mod}\ 16)$ 即 $p-7=16r$ 时, 若 $r=4k$, 令 $Q_1=(12+10e_1+13e_2)$, $Q_2=(12+10e_2+13e_1)$, $Q_1'=(5+3e_1+6e_2)$, $Q_2'=(5+3e_2+6e_1)$; 若 $r=4k+1$, 令 $Q_1=(4+e_1+6e_2)$, $Q_2=(4+e_2+6e_1)$, $Q_1'=(13+10e_1+15e_2)$, $Q_2'=(13+10e_2+15e_1)$; 若 $r=4k+2$, 令 $Q_1=(12+2e_1+5e_2)$, $Q_2=(12+2e_2+5e_1)$, $Q_1'=(5+11e_1+14e_2)$, $Q_2'=(5+11e_2+14e_1)$; 若 $r=4k+3$, 令 $Q_1=(4+9e_1+4e_2)$, $Q_2=(4+9e_2+4e_1)$, $Q_1'=(13+2e_1+7e_2)$, $Q_2'=(13+2e_2+7e_1)$, 则对 Z_{16}-QR 码 Q_1, Q_2, Q_1', Q_2' 有以下结论成立:

(a) Q_1 与 Q_2 等价, Q_1' 与 Q_2' 等价;

(b) $Q_1\cap Q_2=\tilde{h}$ 且 $Q_1+Q_2=R_p$, $\tilde{h}=7h=7(1+e_1+e_2)$;

(c) $|Q_1|=16^{(p+1)/2}=|Q_2|$;

(d) $Q_1=Q_1'+(\tilde{h})$, $Q_2=Q_2'+(\tilde{h})$;

(e) $|Q_1'|=16^{(p-1)/2}=|Q_2'|$;

(f) Q_1' 与 Q_2' 是自正交码且 $Q_1'^{\perp}=Q_1'$, $Q_2'^{\perp}=Q_2'$.

定理 3.2.5 设 p 为素数, 且 $p\equiv -7(\mathrm{mod}\ 16)$ 即 $p+7=16r$ 时, 若 $r=4k$, 令 $Q_1=(5+3e_1+6e_2)$, $Q_2=(5+3e_2+6e_1)$, $Q_1'=(12+10e_1+13e_2)$, $Q_2'=(12+10e_2+13e_1)$; 若 $r=4k+1$, 令 $Q_1=(13+2e_1+7e_2)$, $Q_2=(13+2e_2+7e_1)$, $Q_1'=(4+9e_1+4e_2)$, $Q_2'=(4+9e_2+4e_1)$; 若 $r=4k+2$, 令 $Q_1=(5+11e_1+14e_2)$, $Q_2=(5+11e_2+14e_1)$, $Q_1'=(12+2e_1+5e_2)$, $Q_2'=(12+2e_2+5e_1)$; 若 $r=4k+3$, 令 $Q_1=(13+10e_1+15e_2)$, $Q_2=(13+10e_2+15e_1)$, $Q_1'=(4+e_1+6e_2)$, $Q_2'=(4+e_2+6e_1)$, 则对 Z_{16}-QR 码 Q_1,Q_2,Q_1',Q_2' 有以下结论成立:

(a) Q_1 与 Q_2 等价, Q_1' 与 Q_2' 等价;

(b) $Q_1\cap Q_2=\tilde{h}$ 且 $Q_1+Q_2=R_p$, $\tilde{h}=9h=9(1+e_1+e_2)$;

(c) $|Q_1|=16^{(p+1)/2}=|Q_2|$;

(d) $Q_1=Q_1'+(\tilde{h})$, $Q_2=Q_2'+(\tilde{h})$;

(e) $|Q_1'|=16^{(p-1)/2}=|Q_2'|$;

(f) $Q_1^{\perp}=Q_2'$, $Q_2^{\perp}=Q_1'$.

3.3 Z_{16}-QR 码的扩展码

扩展的 QR 码是二元自对偶码理论的最基本的例子, 所以类似地我们讨论 Z_{16}-QR 码的扩展码, 进而发现它们与扩展二元 QR 码有着相似的性质.

定义 3.3.1 Z_{16}- 码 C 的每一个码字增加一个全一致校验位所得到的码称为 C 的扩展码, 记为 $\bar{C}$.

用通常的增加 "全一致校验位" 的方法扩展 Z_{16}-QR 码的 Q_1 和 Q_2, 对于某些 Z_{16}-QR 码 Q_1 和 Q_2 的扩展码有以下一些性质.

定理 3.3.1 p 为素数，若 $p+1=16r$, Q_1, Q_2 为定理 3.2.1 中所定义的，令 $\bar{Q}_1$ 和 $\bar{Q}_2$ 表示它们的扩展码，则有 $\bar{Q}_1$ 和 $\bar{Q}_2$ 都是自对偶码.

证明 只证明 $r=4k+1$ 的情形，其他 r 情形的证明类似.

因为 $Q_1=Q_1'+(\tilde{h})$, $\tilde{h}=15h$, 则 $\bar{Q}_1$ 有 $(p+1)/2\cdot(p+1)$ 生成矩阵：

$$\begin{pmatrix} 0 & & & & & \\ 0 & & & G_1' & & \\ \vdots & & & & & \\ 15 & 15 & 15 & 15 & \cdots & 15 \end{pmatrix}$$

G_1' 的每一行是 $9+4e_1+13e_2$ 的循环移位，G_1' 即是 Q_1' 的生成矩阵. 因为 Q_1' 是自正交的，所以 G_1' 中的任意两行正交，任意行与自身正交而且也跟 $\tilde{h}=15h$ 正交. 又因为向量 $(15,\tilde{h})$ 与自身正交而且 $|\bar{Q}_1|=|Q_1|=16^{(p+1)/2}$, 比较 $\bar{Q}_1$ 与 $\bar{Q}_1^{\perp}$ 的阶，它们相等，所以 $\bar{Q}_1$ 是自对偶码，同理可证 $\bar{Q}_2$ 也是自对偶码. □

当 $p=1+16r$ 时，定义 $\tilde{Q}_1$ 为以下生成矩阵所生成的 Z_{16}- 码：

$$\begin{pmatrix} 0 & & & & & \\ 0 & & & G' & & \\ \vdots & & & & & \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix}$$

这里 G' 为定理 3.2.2 中所定义的 Q_1' 或 Q_2' 的生成矩阵. 这个矩阵不是 Q_1 或者 Q_2 的扩展码，因为全 1 向量的所有分量和不一定是 $0(\mathrm{mod}\ 16)$ 的.

定理 3.3.2 p 为素数，若 $p-1=16r$, Q_1, Q_2 为定理 3.2.2 中所定义的，令 $\bar{Q}_1$ 和 $\bar{Q}_2$ 表示它们的扩展码，则有 $\bar{Q}_1$ 的对偶是 $\bar{Q}_2$, $\bar{Q}_2$ 的对偶是 $\tilde{Q}_1$.

证明 只证明 $r=4k+1$ 的情形，其他 r 情形的证明类似.

在这种情形下 $\bar{Q}_1$ 有 $(p+1)/2\cdot(p+1)$ 生成矩阵：

$$\begin{pmatrix} 0 & & & & & \\ 0 & & & G_1' & & \\ \vdots & & & & & \\ 15 & 1 & 1 & 1 & \cdots & 1 \end{pmatrix}$$

G_1' 的每一行是 $8+4e_1+11e_2$ 的循环移位. 因为 G_1' 生成 Q_1'，而且由定理 3.2.2, $Q_2^{\perp}=Q_1'$，所以 $\bar{Q}_1$ 生成矩阵的每一行与前面定义的 $\bar{Q}_2$ 的每一行正交. 比较 $\bar{Q}_1$ 的对偶码与 $\bar{Q}_2$ 的阶，两者相等，所以 $\bar{Q}_1$ 的对偶是 $\bar{Q}_2$. 同理可证 $\bar{Q}_2$ 的对偶是 $\tilde{Q}_1$. □

4 码长 7 的 Z_{16}-QR 码在两种 Gray 映射下的像及 Lee 重量分布

向量的 Hamming 重量是编码理论中的一个重要概念，它与码的纠错能力、译码算法都有着紧密的联系. 其定义为：设 $\vec{x}\in V_n$, 称向量 $\vec{x}=(x_1,x_2,\cdots,x_n)$ 坐标不为零的个数为该向量的 Hamming 重量，记为 $wt(\vec{x})$. 我们沿用这一定义来定义 Z_{16}-QR 码的 Hamming 重量. 对 Z_{16}，我们可以按 M.H.Chiu, Stephen Yau 和 Y.Yu 的文章 [7] 及 C. Carlet[10] 与 San Ling 文章 [11] 两种方式定义其到 Z_2^8 的 Gray 映射并有两种相应的 Lee 重量. 在这里，我们完全的计算了码长 7 的 Z_{16}-QR 码的 Lee 重量分布以及 Hamming 重量分布，并比较了这两种 Gray 映射.

4.1 推广文 [7] 的 Gray 映射

我们将文 [7] 中所定义的 $Z_8 \to Z_2^4$ 的 Gray 映射推广到 $Z_{16} \to Z_2^8$. 首先定义从 $Z_{16} \to Z_2^8$ 的映射 α 与 $\beta_i (i = 1, 2, \cdots, 8)$ 为下页表一.

因此，可以定义 Gray 映射 $\varphi : Z_{16}^N \to Z_2^{8N}$ 为 $\varphi(c) = (\beta_1(c), \beta_2(c), \cdots, \beta_8(c))$. 显然，对所有的 $c \in Z_{16}^N$, 有 $\alpha(c) + \beta_1(c) + \beta_2(c) + \cdots + \beta_8(c) = 0$. 根据这种 Gray 映射的特点，定义 4.1.1 定义了 Z_{16} 上的一种 Lee 重量，为区别后面的另一种 Lee 重量定义，我们把这种 Lee 重量记为 Lee^1 重量.

定义 4.1.1 对于 Z_{16} 上的元素 $c \in Z_{16}$, 定义其 Lee^1 重量为:

c	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$wt_{L^1}(c)$	0	1	2	3	4	5	6	7	8	7	6	5	4	3	2	1

那么 Z_{16} 上一个向量的 Lee^1 重量即为它分量 Lee^1 重量之和.

由定理 3.2.4, 知道当 p=7 时，所定义的 Z_{16}-QR 码为 $Q_1 = (12 + 10e_1 + 13e_2), Q_2 = (12 + 10e_2 + 13e_1), Q_1' = (5 + 3e_1 + 6e_2), Q_2' = (5 + 3e_2 + 6e_1)$, 因为 $Q_1 = Q_2, Q_1' \subseteq Q_1$, 所以要确定 $p = 7$ 的 Z_{16}-QR 码的最小重量，只需考察码 Q_1 的码字空间就可以了.

c	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\alpha(c)$	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$\beta_1(c)$	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
$\beta_2(c)$	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0
$\beta_3(c)$	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0
$\beta_4(c)$	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0
$\beta_5(c)$	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0
$\beta_6(c)$	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0
$\beta_7(c)$	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0
$\beta_8(c)$	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0

(表一)

知道 Q_1 的生成矩阵 G_1 为 7×7 的矩阵 (每一行为 $12 + 10e_1 + 13e_2$ 的循环移位):

$$\begin{pmatrix} 12 & 10 & 10 & 13 & 10 & 13 & 13 \\ 13 & 12 & 10 & 10 & 13 & 10 & 13 \\ 13 & 13 & 12 & 10 & 10 & 13 & 10 \\ 10 & 13 & 13 & 12 & 10 & 10 & 13 \\ 13 & 10 & 13 & 13 & 12 & 10 & 10 \\ 10 & 13 & 10 & 13 & 13 & 12 & 10 \\ 10 & 10 & 13 & 10 & 13 & 13 & 12 \end{pmatrix}_{7\times 7}$$

事实上， G_1 可以最后化简为 4×7 的矩阵:

$$\begin{pmatrix} 1 & 2 & 0 & 13 & 3 & 13 & 0 \\ 0 & 1 & 2 & 0 & 13 & 3 & 13 \\ 0 & 0 & 1 & 11 & 3 & 8 & 11 \\ 0 & 0 & 0 & 1 & 6 & 5 & 15 \end{pmatrix}_{4\times 7}$$

通过计算机计算得知， $p = 7$ 的 Z_{16}-QR 码的 Hamming 重量及 Lee^1 重量有以下性质:

定理 4.1.1 $p = 7$ 的 Z_{16}-QR 码的最小 Hamming 重量为 3, 最小 Lee^1 重量为 7. 其 Hamming 重量分布为 (表二), Lee^1 重量分布为 (表三)(其中 $A_0(Lee^1) = A_{56}(Lee^1) = 1$).

i	0	1	2	3	4	5	6	7
A_i(Hamming)	1	0	0	7	497	3822	19502	41707

(表二)

i	7,49	8,48	9,47	10,46	11,45	12,44	13,43	14,42	15,41	16,40	17,39
$A_i(\text{Lee}^1)$	2	14	70	42	28	182	224	296	518	700	882
i	18,38	19,37	20,36	21,35	22,34	23,33	24,32	25,31	26,30	27,29	28
$A_i(\text{Lee}^1)$	1162	1582	1876	2270	2814	3052	3269	3556	3878	4200	4300

(表三)

从 Gray 映射的定义，我们就可以看出，φ 是从 Z_{16}^N(Lee^1 距离) 到 Z_2^{8N}(Hamming 距离) 下的一个保距映射. 而且通过计算，我们还得知 Z_{16}-QR 码在这种 Gray 映射定义下像的 Hamming 重量分布与 (表三) 完全相同，于是，这也验证了这种 Gray 映射的保距性.

4.2 另一种 Z_{16} 上的 Gray 映射

C.Carlet 在文 [10] 中将原始 (Z_4 上的)Gray 映射推广到了 Z_{2^k} 上，而 San Ling 在文 [11] 中则将 Gray 映射推广到了更一般的 $Z_{p^{k+1}}$ 上，而且也证明了在 $p=2$ 时与 Carlet 定义的 Gray 映射推广形式也置换等价. 参考文 [11] 所定义的 Gray 映射，得到 Z_{16} 上元素的 Gray 映射表 (表四).

c	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\beta_1(c)$	0	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0
$\beta_2(c)$	0	1	1	0	0	1	1	0	1	0	0	1	1	0	0	1
$\beta_3(c)$	0	1	0	1	1	0	1	0	1	0	1	0	0	1	0	1
$\beta_4(c)$	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0
$\beta_5(c)$	0	0	1	1	1	1	0	0	1	1	0	0	0	0	1	1
$\beta_6(c)$	0	0	1	1	0	0	1	1	1	1	0	0	1	1	0	0
$\beta_7(c)$	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0
$\beta_8(c)$	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

(表四)

由 (表四), 即得 Z_{16} 上 Gray 映射为 $\varphi: Z_{16}^n \to Z_2^{8n}$, $\varphi(c)=(\beta_1(c),\beta_2(c),\cdots,\beta_8(c))$, $c\in Z_{16}^n$. 从 Gray 映射表 (表四) 可以看到，除了 8 的 Gray 映射象的 Hamming 重量为 8 以及 0 的 Gray 映射象的 Hamming 重量为 0 外，其他元素的 Gray 映射象的 Hamming 重量都为 4, 这个特点指引我们定义 Z_{16} 上元素的 Lee 重量，记之为 Lee^2 重量.

定义 4.2.1 对于 Z_{16} 上的元素 $c\in Z_{16}$, 其 Lee^2 重量如下定义：

c	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$wt_{L^2}(c)$	0	4	4	4	4	4	4	4	8	4	4	4	4	4	4	4

那么 Z_{16} 上一个向量的 Lee^2 重量即为它分量 Lee^2 重量之和.

由 Z_{16} 上向量 Lee^2 重量的定义, 我们知道 Z_{16} 上向量的此种 Gray 映射也是一个从 Z_{16}^n(Lee^2 距离) 到 Z_2^{8n}(Hamming 距离) 下的保距映射. 通过计算，我们得到码长 7 的 Z_{16}-QR 码 Lee^2 重量分布：

定理 4.2.1 $p=7$ 的 Z_{16}-QR 码的最小 Lee^2 重量为 16. 其 Lee^2 重量分布为：

i	0,56	16,40	20,36	24,32	28
$A_i(\mathrm{Lee}^2)$	1	434	2576	14413	30688

通过计算可知 Z_{16}-QR 码在 Gray 映射定义下像的 Hamming 重量分布与其 Lee^2 重量分布也相同，这说明该 Gray 映射 φ 也是从 $Z_{16}^n(\mathrm{Lee}^2$ 距离) 到 Z_2^{8n}(Hamming 距离) 下的保距映射.

4.3 两种 Gray 映射的比较

从前面的分析，我们已经清楚的知道，这两种定义方式下的 Gray 映射都是从 Z_{16}^n(Lee 距离) 到 Z_2^{8n}(Hamming 距离) 下的保距映射. 对于这两种 Gray 映射，从我们所举例 $p=7$ 的 Z_{16}-QR 码的重量计算，就可以看出，以第二种方式定义的 Gray 映射，其相应的 Lee 重量定义使得重量基数更小，这使计算更为简便，而且所得的重量分布也更清晰并有着更大的最小 Lee 重量，所以第二种方式定义的 Gray 映射更好.

致谢 作者感谢陈豪教授的指导，并感谢他引领作者进入编码这一有趣的研究领域.

参考文献:

[1] HAMMONS A R Jr, 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] PLESS V S, QIAN Zhong-qiang. *Cyclic codes and quadratic residue codes over Z_4* [J]. IEEE Trans. Inform. Theory, 1996, **42**(5): 1594–1600.
[3] WOLFMANN J. *Negacyclic and cyclic codes over Z_4* [J]. IEEE Trans. Inform. Theory, 1999, **45**(5): 2527–2532.
[4] WOLFMANN J. *Binary images of cyclic codes over Z_4* [J]. IEEE Trans.Inform. Theory, 2001, **47**(5): 1773–1779.
[5] PLESS V, SOLÉ P, QIAN Zhong-qiang. *Cyclic self dual codes* [J]. Finite Fields Appl., 1997, **3**(1): 48–69.
[6] BONNECAZE A, SOLÉP, CALDERBANK A R. *Quaternary quadratic residue codes and unimodular lattices* [J]. IEEE Trans. Inform. Theory, 1995, **41**(2): 366–377.
[7] CHIU M H, YAU S S T, YU Y. *Z_8-cyclic codes and quadratic residue codes* [J]. Adv. in Appl. Math., 2000, **25**(1): 12–33.
[8] PRAMOD K. *Quadratic residue codes over the integers modulo q^m* [J]. Contemp. Math. 2000, **259**: 299–312.
[9] PLESS V S. *Introduction to the Theory of Error-Correcting Codes* [M]. 2nd ed. New York: Wiley-Interscience, 1989.
[10] CARLET C. *Z_{2^k}-linear codes* [J]. IEEE Trans. Inform. Theory, 1998, **44**(4): 1543–1547.
[11] LING S, BLACKFORD J T. *$Z_{p^{k+1}}$-linear codes* [J]. IEEE Trans.Inform.Theory, 2002, **48**(9): 2592–2605.

Quadratic Residue Code over Z_{16}

TAN Xiao-qing
(Dept. of Math., Jinan University, Guangzhou 510630, China)

Abstract: In this paper, we study quadratic residue (QR) codes over integral ring mod 16 residue class ring Z_{16}, and discuss their algebra properties, including their generator and the self-duality of their extended codes, etc. We also investigate some interesting properties of Z_{16}-QR codes of length 7 under two kinds of Gray maps, and especially study their Lee weight distribution.

Key words: quadratic residue code; idempotent generator; Gray map; Hamming weight; Lee weight.