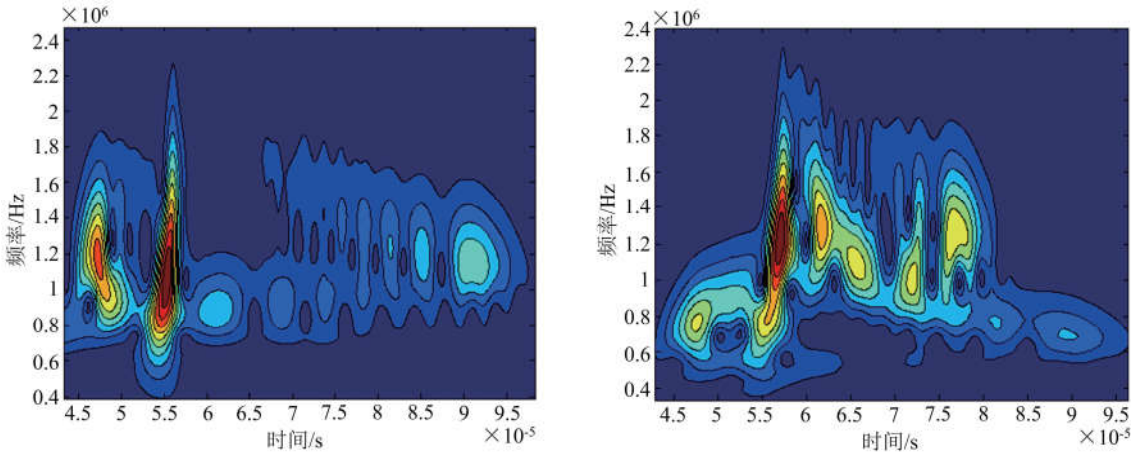

(a)厚度 1.5mm (b) 厚度 2.0mm

图 10 不同厚度下 S 变换时频分布图

Fig.10 Time-frequency distribution of S transform under different thickness

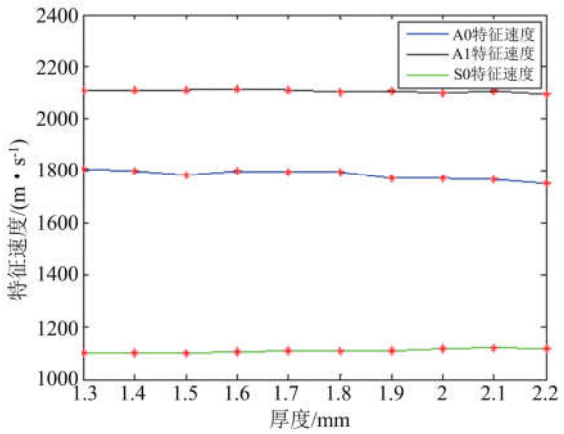

图 11 *A*0、*A*1、*S*0 模式特征速度随厚度变化的曲线

Fig.11 The curve of the feature points velocity in *A*0, *A*1, *S*0 modes changed with different thickness

的;*A*1 模式特征速度局部会有一定波动,整体呈减小趋势,且整体减小幅度只有 20 m/s,相对横、纵波速度对特征速度的影响可以忽略;*A*0 模式特征速度局部波动较大,整体减小 56 m/s,相对横、纵波速度对特征速度的影响略大.这说明本文在 S 变换时频图上选取的特征速度与横、纵波速度、长骨厚度均相关,建议选择 *A*1 和 S0 模式的特征速度作为评价长骨的标准.

4 结论

本文采用 S 变换对仿真的超声导波信号作时频域分析,在时频图上获取 *A*0、*A*1、*S*0 模式的特征速度,再用特征速度评价长骨的泊松比,实现长骨检测.与以往的导波研究相比,该方法不需要进行导波模式分离,既简化了信号处理过程,又避免了模式分离,且无需先验知识.

仿真结果表明,特征速度与长骨导波的横、纵波速度有较高的相关性.长骨的骨密度、弹性模量、泊松比等参数与长骨横波、纵波速度均有直接关系,本文主要研究泊松比与超声导波特征速度之间的关系,发现该特征速度与泊松比具有良好的相关性,并有较高的敏感度.我们同时研究了特征速度与厚度的关系,结果表明,*A*1 和 S0 模式的特征速度对厚度变化不敏感,因此,可以选择 *A*1 和 S0 模式的特征速度对长骨的泊松比参数进行测量.由此可见,特征速度可以作为一种新的评估长骨材料特性的参数,有助于骨质疏松症的诊断和骨折康复状况的监护,具有一定的临床价值.

由于长骨曲面在导波测量中对传感器频率响应及入射角度等有特殊要求,传感器需要定做,因此有关这方面的实验测量结果,我们将在后续工作中进行报道.

参考文献(References)

[1] WEI Y M, PENG H. Study on the transmission system of high frame rate ultrasonic imaging based on the non-diffraction wave[J].Acta Physica Sinica, 2014, 63(19): 198702-198707.

[2] 彭虎,陆建宇,冯焕清,等. Fourier 变换重建超声图像的研究[J]. 中国科学技术大学学报, 2003, 33(5): 619-624.
PENGHu, LU Jianyu, FENG Huanqing, et al. A study on ultrasonic image construction with Fourier transform[J]. Journal of University of Science and Technology of China, 2003, 33(5): 619-624.

[3] NGUYEN K C, LE L H, TRAN T N, et al. Excitation of ultrasonic Lamb waves using a phased array system with two array probes: phantom and in vitro bone studies[J]. Ultrasonics, 2014, 54(5): 1178-1185.

[4] 许凯亮. 超声导波评价长骨状况的研究[D].上海:复旦大学, 2012.

[5] 王东亚,于成龙,彭虎. 基于 FPGA 的合成孔径超声成像波束合成设计[J]. 中国科学技术大学学报,2014, 02:147-152.
WANGDongya, YU Chenglong, PENG Hu. A synthetic aperture beam-former for ultrasound imaging based on FPGA[J]. Journal of University of Science and Technology of China, 2014, 44(2):147-152.

[6] FATERI S, BOULGOURIS N V, WILKINSON A, et al. Frequency-sweep examination for wave mode identification in multimodal ultrasonic guided wave signal[J]. IEEE Transactions on Ultrasonics Ferroelectrics & Frequency Control, 2014, 61(9): 1515-1524.

[7] 罗春苟,他得安,王威琪.基于希尔伯特-黄变换测量超声导波的群速度及材料厚度[J].声学技术,2008, 27(5): 674-679.

[8] TATARINOV A, EGOROV V, SARVAZYAN N, et al. Multi-frequency axial transmission bone ultrasonometer[J]. Ultrasonics, 2014, 54(5): 1162-1169.

[9] KILAPPA V, XU K L, MOILANEN P, et al. Assessment of the fundamental flexural guided wave in cortical bone by an ultrasonic axial-transmission array transducer[J]. Ultrasound in Medicine & Biology, 2013, 39(7): 1223-1232.

[10] MOILANEN P. Ultrasonic guided waves in bone[J]. IEEE Transactions on Ultrasonics Ferroelectrics & Frequency Control, 2008, 55(6):1277-1286.

[11] 许凯亮, 谈钊, 他得安, 等. 超声导波的频散补偿与模式分离算法研究[J].声学学报, 2014, 39(1): 99-103.

[12] 郑祥明, 顾向华, 史立丰, 等. 超声兰姆波的时频分析[J].声学学报, 2003, 28(4): 368-374.

[13] ZHANG Z G, XU K L, TA D A, et al. Joint spectrogram segmentation and ridge-extraction method for separating multimodal guided waves in long bones[J].Science China Physics, Mechanics & Astronomy, 2013, 56(7):1317-1323.

[14] STOCKWELL R G, MANSINHA L, LOWE R P. Localization of the complex spectrum: The S transform[J]. IEEE Transactions on Signal Processing, 2002, 44(4): 998-1001.

[15] 孙家驹, 耿介.人的密质骨的力学性能[J].力学进展, 1987, 17(2): 58-73.

[16] 弓健. DXA 技术测量股骨颈骨强度的临床研究[D]. 广州: 暨南大学, 2013.

[17] XU K L, TA D A, WANG W Q. Multiridge-based analysis for separating individual modes from multimodal guided wave signals in long bones[J]. IEEE Transactions on Ultrasonics Ferroelectrics, Freq Control, 2010, 57(11):2480-2490.

第47卷第7期 中国科学技术大学学报 Vol.47,No.7
2017年7月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Jul. 2017

文章编号:0253-2778(2017)7-0315-08

Quadratic residue codes over $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p+v^2\mathbb{F}_p+uv^2\mathbb{F}_p$

QIAN Liqin, SHI Minjia, LIN S O K, PING Jingshui

(*School of Electronics and Information Engineering, Anhui University, Hefei, 230601, China*)

Abstract: Let $R=\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p+v^2\mathbb{F}_p+uv^2\mathbb{F}_p$, where $u^2=1$, $v^3=v$, and p is an odd prime. Quadratic residue codes of prime length $n=q$ over the ring R was investigated, where q ($q\neq p$) is an odd prime such that p is a quadratic residue modulo q. The cyclic codes of length n over R were studied, and then the quadratic residue codes over R in terms of idempotent generators were difined. Moreover, the relation between these codes and their extended codes are discussed. Finally, two specific forms of idempotent generators of quadratic residue codes over $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p+v^2\mathbb{F}_p+uv^2\mathbb{F}_p$ were given to illustrate some results.

Key words: cyclic codes; quadratic residue codes; generating idempotents; dual codes

CLC number: O157.4 **Document code**: A doi:10.3969/j.issn.0253-2778.2017.07.009

2010 Mathematics Subject Classification: Primary 94B15; Secondary 11A15

Citation: QIAN Liqin, SHI Minjia, LIN S O K, et al. Quadratic residue codes over $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p+v^2\mathbb{F}_p+uv^2\mathbb{F}_p$[J]. Journal of University of Science and Technology of China, 2017,47(7):315-322.
钱丽琴,施敏加,LIN S O K,等. 环 $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p+v^2\mathbb{F}_p+uv^2\mathbb{F}_p$ 上的二次剩余码[J]. 中国科学技术大学学报,2017,47(7):315-322.

环 $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p+v^2\mathbb{F}_p+uv^2\mathbb{F}_p$ 上的二次剩余码

钱丽琴[1],施敏加[1,2,3],LIN S O K[1,5],平静水[4]

(1. 安徽大学数学科学学院, 安徽合肥,230601; 2. 东南大学移动通信国家重点实验室,江苏南京,210096;
3. 计算智能与信号处理教育部重点实验室, 安徽合肥, 230039;
4. 淮南师范大学经济系, 安徽淮南, 232038; 5. 金边皇家学院数学系,柬埔寨)

摘要:设 $R=\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p+v^2\mathbb{F}_p+uv^2\mathbb{F}_p$, 其中 $u^2=1$, $v^3=v$, p 是一个奇素数. 本文研究了环 R 上素长度 $n=q$ 的二次剩余码,其中 q ($q\neq p$) 是一个奇素数且 p 是模 q 的二次剩余.我们首先研究了环 R 上长度为 n 的循环码, 根据其幂等生成元定义了环 R 上的二次剩余码,进一步讨论了该环上二次剩余码与其扩展码的关系. 最后,为了验证结果的正确性, 我们给出了 $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p+v^2\mathbb{F}_p+uv^2\mathbb{F}_p$ 上二次剩余码的幂等生成元的两种具体形式.

关键词:循环码; 二次剩余码; 生成幂等元; 对偶码

Received:2016-04-30;**Revised**:2016-12-30

Foundation item:Supported by

Biography:Qian Liqin, female, born in 1991, Master candidate. Research field: Algebraic coding. E-mail: qianliqin_1108@163.com
PING Jingshui, Huainan normal university, School of finance, China. E-mail: kepuduolong@163.com.

Corresponding author:SHI Minjia, PhD/Associate Professor, E-mail: smjwcl.good@163.com

0 Introduction

The class of quadratic residue codes over finite fields plays a significant role in algebraic coding theory. They are cyclic codes of prime length introduced to construct self-dual codes by adding an overall parity-check. They have been studied since the 1960's by Gleason, and in a series of reports by Assmus and Mattson. They are intimately related to Mathieu groups and Witt designs. Their generalizations over rings have been considered[6].

In [1], Bonnecaze A et al. studied quadratic residue codes over $\mathbb{Z}_4$, and their associated unimodular lattices. Gao J et al. researched some results on quadratic residue codes over the ring $\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p+v^3\mathbb{F}_p$ in [3]. Kaya A et al. studied quadratic residue codes over $\mathbb{F}_p+v\mathbb{F}_p$ and their Gray images in [4]. In [5], Liu Y et al. discussed quadratic residue codes over the ring $\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p$. Pless V et al. defined the quadratic residue codes over ring $\mathbb{Z}_4$, and its related properties are discussed in [7]. In [8], Raka M and Kathuria discussed $(1-2u^3)$-constacyclic codes and quadratic residue codes over $\mathbb{F}_p[u]/\langle u^4-u\rangle$. Zhang T et al. studied the quadratic residue codes over $\mathbb{F}_l+v\mathbb{F}_l$ in [11].

Following the above trend, this paper is devoted to studying quadratic residue codes over the ring $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p+v^2\mathbb{F}_p+uv^2\mathbb{F}_p$, where p is an odd prime. This ring is semi-local of order p^6.

1 Preliminary results

Throughout the paper, we let R denote the commutative ring $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p+v^2\mathbb{F}_p+uv^2\mathbb{F}_p$, where $u^2=1$, $v^3=v$, and p is an odd prime. R is a ring of characteristic p and of size p^6[6]. Clearly, $R\cong\mathbb{F}_p[u,v]/\langle u^2-1, v^3-v, uv-vu\rangle$.

For any positive integer a, if there is an integer $b(0<b<p)$ such that $ab\equiv1\pmod p$, we write $b=a^{-1}=\frac{1}{a}$. It follows that $v^3-v=v(v+1)(v-1)$. Let $y_1=v$, $y_2=v+1$, $y_3=v-1$ and $\hat{y}_i=\frac{v^3-v}{y_i}$ for $i=1,2,3$. Then there exist $a_i,b_i\in R_1[v]$, such that $a_iy_i+b_i\hat{y}_i=1$, where $R_1=\mathbb{F}_p+u\mathbb{F}_p$. Let $\varepsilon_i=b_i\hat{y}_i$. Then we have $R=\varepsilon_1R\oplus\varepsilon_2R\oplus\varepsilon_3R=\varepsilon_1R_1\oplus\varepsilon_2R_1\oplus\varepsilon_3R_1$. Through a direct calculation, we obtain $R=(1-v^2)R_1\oplus2^{-1}(v^2-v)R_1\oplus2^{-1}(v^2+v)R_1$. Similarly, we have $R_1=2^{-1}(1-u)\mathbb{F}_p\oplus2^{-1}(1+u)\mathbb{F}_p$. Thus we obtain $R=(1-v^2)R_1\oplus2^{-1}(v^2-v)R_1\oplus2^{-1}(v^2+v)R_1=2^{-1}(1-u)(1-v^2)\mathbb{F}_p\oplus2^{-1}(1+u)(1-v^2)\mathbb{F}_p\oplus4^{-1}(1-u)(v^2-v)\mathbb{F}_p\oplus4^{-1}(1+u)(v^2-v)\mathbb{F}_p\oplus4^{-1}(1-u)(v^2+v)\mathbb{F}_p\oplus4^{-1}(1+u)(v^2+v)\mathbb{F}_p$. Denote by $\eta_1,\eta_2,\eta_3,\eta_4,\eta_5,\eta_6$ respectively the following elements of R:

$$\eta_1=2^{-1}(1-u)(1-v^2),$$
$$\eta_2=2^{-1}(1+u)(1-v^2),$$
$$\eta_3=4^{-1}(1-u)(v^2-v),$$
$$\eta_4=4^{-1}(1+u)(v^2-v),$$
$$\eta_5=4^{-1}(1-u)(v^2+v),$$
$$\eta_6=4^{-1}(1+u)(v^2+v).$$

Then we have following direct results from the ring theory.

(i) η_1, η_2, η_3, η_4, η_5, η_6 are non-zero idempotents in R, and $\eta_i\eta_j=0$, if $i\neq j$ for $i,j\in\{1,2,3,4,5,6\}$.

(ii) $\eta_1+\eta_2+\eta_3+\eta_4+\eta_5+\eta_6=1$.

For convenience, we let $R_q=R[x]/\langle x^q-1\rangle$ and $f(x)$ will be abbreviated as f if there is no confusion. If $e\in R_q$ such that $e^2=e$, then e is called an idempotent in R_q.

The following results play a crucial role in studying cyclic codes.

Lemma 2.1 With the notation as above, $\eta_1f_1+\eta_2f_2+\eta_3f_3+\eta_4f_4+\eta_5f_5+\eta_6f_6$ is an idempotent in R_q if and only if f_i are idempotents in $\mathbb{F}_p[x]/\langle x^q-1\rangle$ for $i=1,2,3,4,5,6$.

Proof Let $g=\sum_{i=1}^6\eta_if_i$ be an idempotent in R_q. Then $g=g^2=(\sum_{i=1}^6\eta_if_i)^2=\sum_{i=1}^6\eta_if_i^2=\sum_{i=1}^6\eta_if_i$, which implies $f_i^2=f_i$ for $i=1,2,3,4,5,6$.

Conversely, if f_i are idempotents in $\mathbb{F}_p[x]/$

$\langle x^q-1\rangle$, then $(\sum_{i=1}^{6}\eta_i f_i)^2=\sum_{i=1}^{6}\eta_i^2 f_i^2=\sum_{i=1}^{6}\eta_i f_i$, so $\eta_1 f_1+\eta_2 f_2+\eta_3 f_3+\eta_4 f_4+\eta_5 f_5+\eta_6 f_6$ is an idempotent in R_q.

Let S be a commutative ring with identity. Then we have the following propositions by similar methods in Ref.[5].

Proposition 2.1 Let C be a cyclic code of length n over S generated by the idempotent $\xi(x)$ in $S[x]/\langle x^n-1\rangle$. Then its dual $C^{\perp}$ is generated by the idempotent $1-\xi(x^{-1})$.

Proposition 2.2 Let C and D be cyclic codes of length n over S generated by the idempotents ξ_1,ξ_2 in $S[x]/\langle x^n-1\rangle$. Then $C\bigcap D$ and $C+D$ are generated by the idempotents $\xi_1\xi_2$ and $\xi_1+\xi_2-\xi_1\xi_2$, respectively.

Proposition 2.3 Let M be a 6×6 matrix satisfying $MM^t=\lambda I_6$, where M^t is the transpose matrix of M, I_6 the identity matrix and $\lambda\in\mathbb{F}_p$. The Gray map associated with M from R to $\mathbb{F}_p^6$ is defined as $\Phi_M(a_1+a_2u+a_3v+a_4uv+a_5v^2+a_6uv^2)=(a_1-a_2,a_1+a_2,a_1-a_2-a_3+a_4+a_5-a_6,a_1+a_2-a_3-a_4+a_5+a_6,a_1-a_2+a_3-a_4+a_5-a_6,a_1+a_2+a_3+a_4+a_5+a_6)M$ for any $a_1+a_2u+a_3v+a_4uv+a_5v^2+a_6uv^2\in R$, where a_1, a_2, a_3, a_4, a_5, $a_6\in\mathbb{F}_p$. Then this map is naturally extended to R^n.

3 Cyclic codes over $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p+v^2\mathbb{F}_p+uv^2\mathbb{F}_p$

In order to study the quadratic residue codes over R, we first introduce, in this section, the structure of cyclic code over R.

Let C be a linear code of length n over R. We define

$$C_1=\{x_1\in\mathbb{F}_p^n:\exists\, x_2,x_3,x_4,x_5,x_6\in\mathbb{F}_p^n \text{ such that } \eta_1x_1+\eta_2x_2+\eta_3x_3+\eta_4x_4+\eta_5x_5+\eta_6x_6\in C\};$$

$$C_2=\{x_2\in\mathbb{F}_p^n:\exists\, x_1,x_3,x_4,x_5,x_6\in\mathbb{F}_p^n \text{ such that } \eta_1x_1+\eta_2x_2+\eta_3x_3+\eta_4x_4+\eta_5x_5+\eta_6x_6\in C\};$$

$$C_3=\{x_3\in\mathbb{F}_p^n:\exists\, x_1,x_2,x_4,x_5,x_6\in\mathbb{F}_p^n \text{ such that } \eta_1x_1+\eta_2x_2+\eta_3x_3+\eta_4x_4+\eta_5x_5+\eta_6x_6\in C\};$$

$$C_4=\{x_4\in\mathbb{F}_p^n:\exists\, x_1,x_2,x_3,x_5,x_6\in\mathbb{F}_p^n \text{ such that } \eta_1x_1+\eta_2x_2+\eta_3x_3+\eta_4x_4+\eta_5x_5+\eta_6x_6\in C\};$$

$$C_5=\{x_5\in\mathbb{F}_p^n:\exists\, x_1,x_2,x_3,x_4,x_6\in\mathbb{F}_p^n \text{ such that } \eta_1x_1+\eta_2x_2+\eta_3x_3+\eta_4x_4+\eta_5x_5+\eta_6x_6\in C\};$$

$$C_6=\{x_6\in\mathbb{F}_p^n:\exists\, x_1,x_2,x_3,x_4,x_5\in\mathbb{F}_p^n \text{ such that } \eta_1x_1+\eta_2x_2+\eta_3x_3+\eta_4x_4+\eta_5x_5+\eta_6x_6\in C\}.$$

It is easy to verify that $C_i(i=1,2,3,4,5,6)$ are linear codes of length n over $\mathbb{F}_p$, $C=\eta_1C_1\oplus\eta_2C_2\oplus\eta_3C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6$ and $|C|=|C_1||C_2||C_3||C_4||C_5||C_6|$.

Then we have the following theorems and we give the proofs for completeness.

Theorem 3.1 Let $C=\eta_1C_1\oplus\eta_2C_2\oplus\eta_3C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6$ be a cyclic code of length n over R. Then we have

(i) C is cyclic over R if and only if $C_i(i=1,2,3,4,5,6)$ are cyclic over $\mathbb{F}_p$.

(ii) If $C_i=\langle g_i(x)\rangle$, $g_i(x)\in\mathbb{F}_p[x]/\langle x^n-1\rangle$, $g_i(x)|(x^n-1)$, then $C=\langle\eta_1g_1(x),\eta_2g_2(x),\eta_3g_3(x),\eta_4g_4(x),\eta_5g_5(x),\eta_6g_6(x)\rangle$ and $|C|=p^{6n-\sum_{i=1}^{6}\deg(g_i)}$.

Proof (i) Let $s=(s_0,s_1,\cdots,s_{n-1})\in C$ such that $s_i=\eta_1a_i+\eta_2b_i+\eta_3c_i+\eta_4d_i+\eta_5e_i+\eta_6f_i$, where a_i, b_i, c_i, d_i, e_i, $f_i\in\mathbb{F}_p$, $i=0,1,\cdots,n-1$, and $a=(a_0,a_1,\cdots,a_{n-1})$, $b=(b_0,b_1,\cdots,b_{n-1})$, $c=(c_0,c_1,\cdots,c_{n-1})$, $d=(d_0,d_1,\cdots,d_{n-1})$, $e=(e_0,e_1,\cdots,e_{n-1})$, $f=(f_0,f_1,\cdots,f_{n-1})$. Then $a\in C_1$, $b\in C_2$, $c\in C_3$, $d\in C_4$, $e\in C_5$, and $f\in C_6$. Since C is cyclic, $(s_{n-1},s_0,s_1,\cdots,s_{n-2})=(\eta_1a_{n-1}+\eta_2b_{n-1}+\eta_3c_{n-1}+\eta_4d_{n-1}+\eta_5e_{n-1}+\eta_6f_{n-1},\eta_1a_0+\eta_2b_0+\eta_3c_0+\eta_4d_0+\eta_5e_0+\eta_6f_0,\cdots,\eta_1a_{n-2}+\eta_2b_{n-2}+\eta_3c_{n-2}+\eta_4d_{n-2}+\eta_5e_{n-2}+\eta_6f_{n-2})=\eta_1(a_{n-1},a_0,\cdots,a_{n-2})+\eta_2(b_{n-1},b_0,\cdots,b_{n-2})+\eta_3(c_{n-1},c_0,\cdots,c_{n-2})+\eta_4(d_{n-1},d_0,\cdots,d_{n-2})+\eta_5(e_{n-1},e_0,\cdots,e_{n-2})+\eta_6(f_{n-1},f_0,\cdots,f_{n-2})\in C=\eta_1C_1\oplus\eta_2C_2\oplus\eta_3C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6$ if and only if $(a_{n-1},a_0,\cdots,a_{n-2})\in C_1$, $(b_{n-1},b_0,\cdots,b_{n-2})\in C_2$, $(c_{n-1},c_0,\cdots,c_{n-2})\in C_3$, $(d_{n-1},d_0,\cdots,d_{n-2})\in C_4$, $(e_{n-1},e_0,\cdots,e_{n-2})\in C_5$, $(f_{n-1},f_0,\cdots,f_{n-2})\in C_6$, i.e. $C_i(i=1,2,3,$

4,5,6) are cyclic over $\mathbb{F}_p$.

(ii) If $c\in C=\eta_1C_1\oplus\eta_2C_2\oplus\eta_3C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6$, then $c=\sum_{i=1}^{6}\eta_ig_if_i$, $f_i\in\mathbb{F}_p[x]$, $i=1,2,3,4,5,6$, so $C\subseteq\langle\eta_1g_1,\eta_2g_2,\cdots,\eta_6g_6\rangle$. Next, we prove $\langle\eta_1g_1,\eta_2g_2,\cdots,\eta_6g_6\rangle\subseteq C$. Let $f=\sum_{i=1}^{6}\eta_ig_is_i\in\langle\eta_1g_1,\eta_2g_2,\cdots,\eta_6g_6\rangle$, where $s_i\in R[x]$, $i=1,2,3,4,5,6$, then $f=\sum_{i=1}^{6}\eta_ig_i(\eta_1a_i+\eta_2b_i+\eta_3c_i+\eta_4d_i+\eta_5e_i+\eta_6f_i)=\sum_{i=1}^{6}\eta_ig_is_i\in C$, i.e. $\langle\eta_1g_1,\eta_2g_2,\cdots,\eta_6g_6\rangle\subseteq C$. Hence, $C=\langle\eta_1g_1(x),\eta_2g_2(x),\eta_3g_3(x),\eta_4g_4(x),\eta_5g_5(x),\eta_6g_6(x)\rangle$ and $|C|=p^{6n-\sum_{i=1}^{6}\deg(g_i)}$.

Theorem 3.2 Let C be a cyclic code of length n over R. Then the following holds.

(i) There exists a unique polynomial $g(x)\in R[x]$ such that $C=\langle g(x)\rangle$, where $g(x)=\sum_{i=1}^{6}\eta_ig_i(x)$ and $g(x)|x^n-1$.

(ii) If $g_i(x)h_i(x)=x^n-1$ for $i=1,2,3,4,5,6$ and $h(x)=\sum_{i=1}^{6}\eta_ih_i(x)$, then $g(x)h(x)=x^n-1$.

Proof Assume $g=\sum_{i=1}^{6}\eta_ig_i$, then $\langle g\rangle\subseteq C=\langle\eta_1g_1,\eta_2g_2,\eta_3g_3,\eta_4g_4,\eta_5g_5,\eta_6g_6\rangle$. On the other hand, since $\eta_i\eta_j=0(i\neq j)$, we get $\eta_ig_i=\eta_ig$ and thus $C\subseteq\langle g\rangle$. Hence $C=\langle g(x)\rangle$. Let $g_i(x)h_i(x)=x^n-1$, $i=1,2,3,4,5,6$, $h(x)=\sum_{i=1}^{6}\eta_ih_i(x)$. Then $g(x)h(x)=\sum_{i=1}^{6}\eta_i(x^n-1)$, hence $g(x)|x^n-1$. This proof is completed.

In light of Theorems 3.2, we have the following propositions and they can be similarly proved.

Proposition 3.1 Let C be a cyclic code of length n over R with $gcd(n,p)=1$ and $C_i=\langle f_i\rangle$ with f_i ($i=1,2,3,4,5,6$) being idempotents. Then there exits a unique idempotent $e\in C$ with $e=\sum_{i=1}^{6}\eta_if_i$ such that

(i) $C=\langle e\rangle$.

(ii) $C^{\perp}=\langle1-e(x^{-1})\rangle$.

Proposition 3.2 Let C be a cyclic code of length n over R and let $C^{\perp}$ be its dual. Then

(i) $C^{\perp}=\eta_1C_1^{\perp}\oplus\eta_2C_2^{\perp}\oplus\eta_3C_3^{\perp}\oplus\eta_4C_4^{\perp}\oplus\eta_5C_5^{\perp}\oplus\eta_6C_6^{\perp}$.

(ii) $C^{\perp}=\langle\eta_1h_1^{\perp},\eta_2h_2^{\perp},\eta_3h_3^{\perp},\eta_4h_4^{\perp},\eta_5h_5^{\perp},\eta_6h_6^{\perp}\rangle$, where $h_i^{\perp}$ is the reciprocal polynomial of h_i, $i=1,2,3,4,5,6$.

(iii) $|C^{\perp}|=p^{\sum_{i=1}^{6}\deg(g_i)}$.

4 Quadratic residue codes over $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p+v^2\mathbb{F}_p+uv^2\mathbb{F}_p$

In this section, quadratic residue codes over R are defined in terms of their idempotent generators. Let q be an odd prime such that $q\equiv\pm1\pmod 4$. Let Q_q and N_q be the sets of quadratic residues and non-residues modulo q, respectively.

Let $r_1(x)=\prod_{r_1\in Q_q}(x-\alpha^{r_1})$, $r_2(x)=\prod_{r_2\in N_q}(x-\alpha^{r_2})$, where α is a primitive qth root of unity in some extension field of $\mathbb{F}_p$.

We denote $h_1(x)=\sum_{i\in Q_q}x^i$, $h_2(x)=\sum_{i\in N_q}x^i$ and $h(x)=1+h_1(x)+h_2(x)=1+x+x^2+\cdots+x^{q-1}=r_1(x)r_2(x)$. Consider the cyclic codes of length q defined by

$$Q=\langle r_1(x)\rangle,\ N=\langle r_2(x)\rangle,$$
$$\overline{Q}=\langle(x-1)r_1(x)\rangle,$$
$$\overline{N}=\langle(x-1)r_2(x)\rangle.$$

Lemma 4.1[5] If $p>2$ and $q\equiv\pm1\pmod 4$, then idempotent generators of Q, N, $\overline{Q}$, $\overline{N}$ over $\mathbb{F}_p$ are given by

$$E_q(x)=\frac{1}{2}(1+\frac{1}{q})+\frac{1}{2}(\frac{1}{q}-\frac{1}{\theta})h_1+\frac{1}{2}(\frac{1}{q}+\frac{1}{\theta})h_2,$$

$$E_n(x)=\frac{1}{2}(1+\frac{1}{q})+\frac{1}{2}(\frac{1}{q}-\frac{1}{\theta})h_2+\frac{1}{2}(\frac{1}{q}+\frac{1}{\theta})h_1,$$

$$F_q(x)=\frac{1}{2}(1-\frac{1}{q})-\frac{1}{2}(\frac{1}{q}+\frac{1}{\theta})h_1-\frac{1}{2}(\frac{1}{q}-\frac{1}{\theta})h_2,$$

$$F_n(x)=\frac{1}{2}(1-\frac{1}{q})-\frac{1}{2}(\frac{1}{q}+\frac{1}{\theta})h_2-\frac{1}{2}(\frac{1}{q}-\frac{1}{\theta})h_1,$$

respectively, where θ denotes *Gaussian* sum and $\chi(i)$ denotes Legendre symbol, that is

$$\theta=\sum_{i=1}^{q-1}\chi(i)\alpha^i,\chi(i)=\begin{cases}1, & i\in Q_q;\\ -1, & i\in N_q;\\ 0, & p\mid i.\end{cases}$$

For convenience, we let $e_1=E_q(x)$, $e_2=E_n(x)$, $\bar{e}_1=F_q(x)$, $\bar{e}_2=F_n(x)$.

Lemma 4.2 Let p be an odd prime and let η_i ($i=1,2,\cdots,6$) be as in Preliminary results. Then $\eta_1e_i+\eta_2e_j+\eta_3e_k+\eta_4e_l+\eta_5e_m+\eta_6e_n$, $\eta_1\bar{e}_i+\eta_2\bar{e}_j+\eta_3\bar{e}_k+\eta_4\bar{e}_l+\eta_5\bar{e}_m+\eta_6\bar{e}_n$ are idempotents in the ring $R_q=R[x]/\langle x^q-1\rangle$, where e_i, e_j, e_k, e_l, e_m, e_n are not all equal and $\bar{e}_i$, $\bar{e}_j$, $\bar{e}_k$, $\bar{e}_l$, $\bar{e}_m$, $\bar{e}_n$ are not all equal for i, j, k, l, m, $n\in\{1,2\}$.

According to Lemma 4.1, by direct calculation, we get the following lemma.

Lemma 4.3 With the above notation, $e_1+e_2=1+\frac{1}{q}h$, $\bar{e}_1+\bar{e}_2=1-\frac{1}{q}h$, $e_1-\bar{e}_1=\frac{1}{q}h$, $e_2-\bar{e}_2=\frac{1}{q}h$, $e_1e_2=\frac{1}{q}h$ and $\bar{e}_1\bar{e}_2=0$.

We now define quadratic residue codes over R.

Definition 4.1 Let q be an odd prime such that p is a quadratic residue modulo q. The following sixty-two codes are defined as quadratic residue codes over R of length q.

(i) For $i=1,2,3,4,5,6$,

$$Q_i=\langle(1-\eta_i)e_1+\eta_ie_2\rangle,\ Q_{i+31}=\langle\eta_ie_1+(1-\eta_i)e_2\rangle,$$
$$S_i=\langle(1-\eta_i)\bar{e}_1+\eta_i\bar{e}_2\rangle,$$
$$S_{i+31}=\langle\eta_i\bar{e}_1+(1-\eta_i)\bar{e}_2\rangle.$$

(ii) For $1\leqslant i\leqslant 5$, $i<j\leqslant 6$ and $k=\sum_{t=1}^{i}(6-t)+j$, i.e. $k=7,8,\cdots,21$,

$$Q_k=\langle(\eta_i+\eta_j)e_1+(1-\eta_i-\eta_j)e_2\rangle,$$
$$Q_{k+31}=\langle(1-\eta_i-\eta_j)e_1+(\eta_i+\eta_j)e_2\rangle,$$
$$S_k=\langle(\eta_i+\eta_j)\bar{e}_1+(1-\eta_i-\eta_j)\bar{e}_2\rangle,$$
$$S_{k+31}=\langle(1-\eta_i-\eta_j)\bar{e}_1+(\eta_i+\eta_j)\bar{e}_2\rangle.$$

(iii) For $2\leqslant i\leqslant 5$, $i<j\leqslant 6$ and $l=\sum_{t=1}^{i}(6-t)+j+10$, i.e. $l=22,23,\cdots,31$,

$$Q_l=\langle(\eta_1+\eta_i+\eta_j)e_1+(1-\eta_1-\eta_i-\eta_ie_2)\rangle,$$
$$Q_{l+31}=\langle(1-\eta_1-\eta_i-\eta_j)e_1+(\eta_1+\eta_i+\eta_j)e_2\rangle,$$
$$S_l=\langle(\eta_1+\eta_i+\eta_j)\bar{e}_1+(1-\eta_1-\eta_i-\eta_j)\bar{e}_2\rangle,$$
$$S_{l+31}=\langle(1-\eta_1-\eta_i-\eta_j)\bar{e}_1+(\eta_1+\eta_i+\eta_j)\bar{e}_2\rangle.$$

By Definition 4.1, we can obtain the following theorems.

Theorem 4.1 If $q\equiv\pm 1\pmod 4$, with the notation as in Definition 4.1, then the following assertions hold for the quadratic residue codes over R.

(i) Q_m is equivalent to Q_{m+31} and S_m is equivalent to S_{m+31} for $m=1,2,\cdots,31$.

(ii) $Q_m\cap Q_{m+31}=\langle\frac{1}{q}h\rangle$, $Q_m+Q_{m+31}=R_q$ for $m=1,2,\cdots,31$. Moreover, we have $S_m\cap S_{m+31}=\{0\}$ and $S_m+S_{m+31}=\langle 1-\frac{1}{q}h\rangle$, $m=1,2,\cdots,31$.

(iii) $S_i\cap\langle\frac{1}{q}h\rangle=\{0\}$, $S_i+\langle\frac{1}{q}h\rangle=Q_i$ for $i=1,2,3,4,\cdots,62$.

(iv) $|Q_i|=p^{3(q+1)}$, $|S_i|=p^{3(q-1)}$ for $i=1,2,3,4,\cdots,62$.

Proof (i) For any $a\in\mathbb{F}_p^*$, $n\in\mathbb{N}_q$, let u_n be the multiplier map $u_n:\mathbb{F}_p\to\mathbb{F}_p$ given by $u_n(a)=na\pmod p$ and act on polynomials as $u_n(\sum_i f_ix^i)=\sum_i f_ix^{u_n(i)}$. Then $u_n(h_1)=h_2$ and $u_n(h_2)=h_1$. Therefore $u_n(e_1)=e_2$, $u_n(e_2)=e_1$, $u_n(\bar{e}_1)=\bar{e}_2$, $u_n(\bar{e}_2)=\bar{e}_1$, so $u_n((1-\eta_i)e_1+\eta_ie_2)=(1-\eta_i)e_2+\eta_ie_1$; $u_n((\eta_i+\eta_j)e_1+(1-\eta_i-\eta_j)e_2)=(\eta_i+\eta_j)e_2+(1-\eta_i-\eta_j)e_1$; $u_n((\eta_1+\eta_i+\eta_j)e_1+(1-\eta_1-\eta_i-\eta_j)e_2)=(\eta_1+\eta_i+\eta_j)e_2+(1-\eta_1-\eta_i-\eta_j)e_1$; $u_n((1-\eta_i)\bar{e}_1+\eta_i\bar{e}_2)=(1-\eta_i)\bar{e}_2+\eta_i\bar{e}_1$; $u_n((\eta_i+\eta_j)\bar{e}_1+(1-\eta_i-\eta_j)\bar{e}_2)=(\eta_i+\eta_j)\bar{e}_2+(1-\eta_i-\eta_j)\bar{e}_1$; $u_n((\eta_1+\eta_i+\eta_j)\bar{e}_1+(1-\eta_1-\eta_i-\eta_j)\bar{e}_2)=(\eta_1+\eta_i+\eta_j)\bar{e}_2+(1-\eta_1-\eta_i-\eta_j)\bar{e}_1$.

(ii) When $m=1,2,3,4,5,6$, let $T=(1-\eta_i)e_1+\eta_ie_2$ and $T'=(1-\eta_i)e_2+\eta_ie_1$; $\overline{T}=(1-\eta_i)\bar{e}_1+\eta_i\bar{e}_2$ and $\overline{T}'=(1-\eta_i)\bar{e}_2+\eta_i\bar{e}_1$. We note that $T+T'=e_1+e_2$, $TT'=e_1e_2$, $\overline{T}+\overline{T}'=\bar{e}_1+\bar{e}_2$, $\overline{TT}'=\bar{e}_1\bar{e}_2$. Therefore by Proposition 2.3, $Q_i\cap Q_{i+31}=\langle TT'\rangle=\langle e_1e_2\rangle=\langle\frac{1}{q}h\rangle$, and $Q_i+Q_{i+31}=\langle T+T'-TT'\rangle=\langle e_1+e_2-e_1e_2\rangle=\langle 1\rangle=R_q$; $S_i\cap S_{i+31}=\langle\overline{TT}'\rangle=\langle\bar{e}_1\bar{e}_2\rangle=\{0\}$, and $S_i+S_{i+31}=\langle\overline{T}+\overline{T}'-\overline{TT}'\rangle=\langle\bar{e}_1+\bar{e}_2-\bar{e}_1\bar{e}_2\rangle=\langle 1-\frac{1}{q}h\rangle$.

Similarly, we can prove the result when $m=7,8,\cdots,31$. This proves (ii).

(iii) Using Proposition 2.3, when $i=1,2,3,4,5,6$, we have $\overline{T}(\frac{1}{q}h)=((1-\eta_i)\bar{e}_1+\eta_i\bar{e}_2)(\frac{1}{q}h)$

$=((1-\eta_i)\bar{e}_1+\eta_i\bar{e}_2)(1-\bar{e}_1-\bar{e}_2)=0$. And $\overline{T}+\frac{1}{q}h$ $=(1-\eta_i)\bar{e}_1+\eta_i\bar{e}_2+(1-\eta_i+\eta_i)(\frac{1}{q}h)=(1-\eta_i)$ $(\bar{e}_1+\frac{1}{q}h)+\eta_i(\bar{e}_2+\frac{1}{q}h)=(1-\eta_i)e_1+\eta_i e_2$. Therefore $S_i\bigcap\langle\frac{1}{q}h\rangle=\langle\overline{T}(\frac{1}{q}h)\rangle=\{0\}$, and $S_i+\langle\frac{1}{q}h\rangle=\langle\overline{T}+\frac{1}{q}h-\overline{T}(\frac{1}{q}h)\rangle=\langle(1-\eta_i)e_1+\eta_i e_2\rangle$ $=Q_i$. This proves (iii) for $i=1,2,3,4,5,6$. For $i=7,8,\cdots,62$, the proof follows on the same lines.

(iv) According to (ii), we have $|Q_i\bigcap Q_{i+31}|$ $=|\langle\frac{1}{q}h\rangle|=p^6$, and since $p^{6q}=|R_q|=|Q_i+Q_{i+31}|=\frac{|Q_i||Q_{i+31}|}{|Q_i\bigcap Q_{i+31}|}=\frac{|Q_i|^2}{p^6}$, $|Q_i|^2=p^{6(q+1)}$, so $|Q_i|=p^{3(q+1)}$. Similar argument gives $|Q_i|=p^{3(q+1)}$ for $i=7,8,\cdots,31$. Now for $i=1,2,\cdots,62$, we have $p^{3(q+1)}=|Q_i|=|S_i+\langle\frac{1}{q}h\rangle|=|S_i||\langle\frac{1}{q}h\rangle|=|S_i|p^6$, since $|S_i\bigcap\langle\frac{1}{q}h\rangle|=|\langle 0\rangle|=1$. This gives $|S_i|=p^{3(q-1)}$.

Theorem 4.2　If $q\equiv 3\pmod 4$ and p is a quadratic residue modulo q, then the following assertions hold for the quadratic residue codes over R:

(i) $Q_i^{\perp}=S_i$, $i=1,2,\cdots,62$,

(ii) S_i is self-orthogonal, $i=1,2,\cdots,62$.

Proof　As $-1\in N_q$, according to Proposition 2.2, since $C_1=\langle e_1\rangle$, we have $C_1^{\perp}=\langle 1-e_1(x^{-1})\rangle$ with $1-e_1(x^{-1})=1-\frac{1}{2}(1+\frac{1}{q})-\frac{1}{2}(\frac{1}{q}-\frac{1}{\theta})h_2-\frac{1}{2}(\frac{1}{q}-\frac{1}{\theta})h_1=\bar{e}_1$, so $C_1^{\perp}=\langle\bar{e}_1\rangle$. Similarly, $C_2^{\perp}=\langle\bar{e}_2\rangle$. For $i=1,2,3,4,5,6$, we have $Q_i^{\perp}=\langle 1-((1-\eta_i)e_1+\eta_i e_2)(x^{-1})\rangle=\langle(1-\eta_i)\bar{e}_1+\eta_i\bar{e}_2\rangle$, which implies $Q_i^{\perp}=S_i$. Using (iii) of Theorem 4.5, we have $S_i\subseteq Q_i=S_i^{\perp}$. Hence, S_i is self-orthogonal. Similarly, we also have $Q_i=S_i^{\perp}$ and S_i is self-orthogonal for $i=7,8,\cdots,62$. This proves the results.

We get the following proposition, whose proof is easy and thus omitted.

Proposition 4.1　If $q\equiv 1\pmod 4$ and p is a quadratic residue modulo q, then the following assertions hold for the quadratic residues codes over R:

(i) $Q_i^{\perp}=S_{i+31}$, $i=1,2,\cdots,31$.

(ii) $Q_{i+31}^{\perp}=S_i$, $i=1,2,\cdots,31$.

5　Extended quadratic residue codes over $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p+v^2\mathbb{F}_p+uv^2\mathbb{F}_p$

In this section, we discuss the properties of extended quadratic residue codes over R.

Definition 5.1　The extended code of a code C over R will be denoted by C, which is the code obtained by adding a specific column to the generator matrix of C. In addition, define the generator matrix of $\hat{Q}_i$ as

$$\begin{array}{c} \infty \quad 0 \quad 1 \quad 2 \quad \cdots \quad q-1 \\ \begin{pmatrix} 0 & & & & & \\ 0 & & & G'_i & & \\ \vdots & & & & & \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix} \end{array}$$

where G'_i generates S_i $(i=1,2,\cdots,62)$, and the row above the horizontal bar shows the column labelling by $\mathbb{F}_q\cup\infty$.

Theorem 5.1　If $q\equiv 3\pmod 4$, with the notation Q_i $(i=1,2,\cdots,62)$ as in Definition 4.1, then $\overline{Q}_i^{\perp}=\hat{Q}_i$. In particular, if $q\equiv -1\pmod p$, then $\hat{Q}_i$ are self-dual.

Proof　Theorem 4.1 tells us that $Q_i=S_i+\langle\frac{1}{q}h\rangle$ $(i=1,2,\cdots,62)$ and then the generator matrix of $\hat{Q}_i$ is

$$\begin{array}{c} \infty \quad 0 \quad 1 \quad 2 \quad \cdots \quad q-1 \\ \begin{pmatrix} 0 & & & & & \\ 0 & & & G'_i & & \\ \vdots & & & & & \\ -1 & \frac{1}{q} & \frac{1}{q} & \frac{1}{q} & \cdots & \frac{1}{q} \end{pmatrix} \end{array}$$

where G'_i is a generator matrix of S_i. Since S_i are self-orthogonal, any two rows of G'_i are

orthogonal. According to the proof of (iii) in Theorem 4.5, we know that each row of G'_i are orthogonal together with the vector $(\frac{1}{q}h)$. Since $(1,h)\cdot(-1,\frac{1}{q}h)=0$, then $|\overline{Q}_i^{\perp}|=|\hat{Q}_i|=p^{3(q+1)}$. That is, $\overline{Q}_i^{\perp}=\hat{Q}_i$. In particular, if $q\equiv -1 \pmod p$, $\overline{Q}_i$ are linear codes generated by the matrix

$$\overline{G}_i=\begin{array}{c} \begin{matrix} \infty & 0 & 1 & 2 & \cdots & q-1 \end{matrix} \\ \begin{pmatrix} 0 & & & & & \\ 0 & & & G'_i & & \\ \vdots & & & & & \\ -1 & -1 & -1 & -1 & \cdots & -1 \end{pmatrix} \end{array}$$

Obviously, $(1,h)\in\overline{G}_i$. Hence, $\overline{Q}_i^{\perp}=\overline{Q}_i$. That is, $\overline{Q}_i$ are self-dual.

Similar to the proof of Theorem 5.1, we have the following theorem.

Theorem 5.2 If $q\equiv 1 \pmod 4$, with the notation $Q_i(i=1,2,\cdots,62)$ as in Definition 4.1, then $\overline{Q}_i^{\perp}=\hat{Q}_{i+31}$, $\overline{Q}_{i+31}^{\perp}=\hat{Q}_i(i=1,2,\cdots,31)$. In particular, if $q\equiv -1 \pmod p$, then $\overline{Q}_i^{\perp}=\overline{Q}_{i+31}$, $\overline{Q}_{i+31}^{\perp}=\overline{Q}_i(i=1,2,\cdots,31)$.

6 Examples

In this section, we give some examples to illustrate the main results obtained in this paper. Using Magma [2], we search, among all the 62 inequivalent codes, the codes having highest minimum distance of different lengths over different fields. In the following examples, we take $M_0=I_6$, the identity matrix,

$$M_1=\begin{pmatrix} 0 & 1 & 2 & 2 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 2 & 2 & 2 & 0 & 2 & 0 \\ 1 & 2 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 2 & 2 & 1 \\ 1 & 0 & 1 & 2 & 1 & 0 \end{pmatrix},$$

$$M_2=\begin{pmatrix} 2 & 3 & 3 & 2 & 3 & 3 \\ 3 & 2 & 3 & 3 & 2 & 3 \\ 3 & 3 & 2 & 3 & 3 & 2 \\ 2 & 3 & 3 & 5 & 4 & 4 \\ 3 & 2 & 3 & 4 & 5 & 4 \\ 3 & 3 & 2 & 4 & 4 & 5 \end{pmatrix}$$

satisfying $M_1M_1^t=I_6$ over $\mathbb{F}_3$ and $M_1M_1^t=2I_6$ over $\mathbb{F}_7$.

Example 1 Let $p=3$ and $q=11$. The sets of quadratic residues and non-residues modulo q are $Q_q=\{1,3,4,5,9\}$, and $N_q=\{2,6,7,8,10\}$, respectively. Then $h_1(x)=\sum_{i\in Q_q}x^i=x^9+x^5+x^4+x^3+x$, $h_2(x)=\sum_{i\in N_q}x^i=x^{10}+x^8+x^7+x^6+x^2$, $\overline{e}_1=x^{10}+x^8+x^7+x^6+x^2+1$, $\overline{e}_2=x^9+x^5+x^4+x^3+x+1$. $e_1=2x^9+2x^5+2x^4+2x^3+2x$, $e_2=2x^{10}+2x^8+2x^7+2x^6+2x^2$. So $S_1=\langle(1-2^{-1}(1-u)(1-v^2))\overline{e}_1+2^{-1}(1-u)(1-v^2)\overline{e}_2\rangle$, $S_7=\langle(2^{-1}(1-u)(1-v^2)+2^{-1}(1+u)(1-v^2))\overline{e}_1+(1-2^{-1}(1-u)(1-v^2)-2^{-1}(1+u)(1-v^2))\overline{e}_2\rangle$.

The codes over $\mathbb{F}_3$ obtained from the extended quadratic residue codes over R are as follows:

- $\Phi_{M_0}(\overline{Q}_1)$ is a $[72,36,6]$ self-dual code.
- $\Phi_{M_1}(\overline{Q}_7)$ is a $[72,36,12]$ self-dual code.

Example 2 Let $p=7$ and $q=3$. Then $h_1(x)=x$, $h_2(x)=x^2$, $\overline{e}_1=3x^2+6x+5$, $\overline{e}_2=6x^2+3x+5$. $e_1=x^2+4x+3$, $e_2=4x^2+x+3$. So $S_1=\langle(1-2^{-1}(1-u)(1-v^2))\overline{e}_1+2^{-1}(1-u)(1-v^2)\overline{e}_2\rangle$, $S_{13}=\langle(2^{-1}(1+u)(1-v^2)+4^{-1}(1+u)(v^2-v))\overline{e}_1+(1-2^{-1}(1+u)(1-v^2)-4^{-1}(1+u)(v^2-v))\overline{e}_2$.

$\%_0\rangle$, $S_{31}\}=\langle\%(2^{-1}(1-u)(1-v^2)+4^{-1}(1-u)(v^2+v)+4^{-1}(1+u)(v^2+v))\overline{e}_1+(1-2^{-1}(1-u)(1-v^2)-4^{-1}(1-u)(v^2+v)-4^{-1}(1+u)(v^2+v))\overline{e}_2\%\rangle$.

The codes over $\mathbb{F}_7$ obtained from the extended quadratic and quadratic residue codes over R are as follows:

- $\Phi_{M_0}(\overline{Q}_1)$ is a $[24,12,3]$ self-dual code.
- $\Phi_{M_2}(\overline{Q}_{13})$ is a $[24,12,4]$ self-dual code.
- $\Phi_{M_0}(S_1)$ is a $[18,6,3]$ self-orthogonal

code.

• $\Phi_{M_2}(S_{13})$ is a [18, 6, 9] self-orthogonal code.

7 Conclusion

In this paper, we studied some properties of quadratic residue codes over the ring $R=\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p+v^2\mathbb{F}_p+uv^2\mathbb{F}_p$, where $u^2=1$, $v^3=v$, and p is an odd prime. The research results in this article can enrich the theory of error correcting codes over finite rings. Many codes are derived from the quadratic residue codes over R.

Acknowledgement The authors are grateful to Solé for careful reading and helpful comments. This research is supported by National Natural Science Foundation of China (61202068), the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (2015D11), Technology Foundation for Selected Overseas Chinese Scholar, Ministry of Personnel of China (05015133) and Key projects of support program for outstanding young talents in Colleges and Universities (gxyqZD2016008).

References

[1] BONNECAZE A, SOLÉ P, CALDERBANK A R. Quaternary quadratic residue codes and unimodular lattices [J]. IEEE Transactions on Information Theory, 1995, 41(2): 366-377.

[2] BOSMA W, CANNON J. Handbook of Magma Functions [Z]. Sydney, 1995.

[3] GAO J, MA F H. Some results on quadratic residue codes over the ring $F_p+vF_p+v^2F_p+v^3F_p$ [J]. Discrete Mathematics Algorithms & Applications, 2017, 9(3): 1750035(1-9).

[4] KAYA A, YILDIZ B, SIAP I. New extremal binary self-dual codes of length 68 from quadratic residue codes over $F_2+uF_2+u^2F_2$[J]. Finte Fields and Their Applications, 2014, 29(1): 160-177.

[5] LIU Y, SHI M J, SOLÉ P. Quadratic residue codes over $F_p+vF_p+v^2F_p$[J]. Lecture Notes in Computer Science, 2015, 9061: 204-211.

[6] MACWILLIAMS J, SLOANE N J A. The theory of Error Correcting Codes [M]// North- Holland Publishing, 1977, 68(1):185-186.

[7] PLESS V S, QIAN Z Q. Cyclic codes and quadratic residue codes over Z_4 [J]. IEEE Transactions on Information Theory, 1996, 42(5): 1594-1600.

[8] RAKA M, KATHURIA L, GOYAL M. $(1-2u^3)$-constacyclic codes and quadratic residue codes over $F_p[u]/\langle u^4-u\rangle$[J]. Cryptography and Communications, 2017, 9(4): 459-473.

[9] SHI M J, SOLÉ P, WU B. Cyclic codes and the weight enumerator of linear codes over $F_2+uF_2+u^2F_2$[J]. Applied Computational Mathematics, 2013, 12(2): 247-255.

[10] ZHU S X, WANG Y, SHI M J. Some results on cyclic codes over F_2+vF_2 [J]. IEEE Transactions on Information Theory, 2010, 56(4): 1680-1684.

[11] 张涛，朱士信. 环 F_l+vF_l 上的二次剩余码[J]. 中国科学技术大学学报,2012, 42(3): 207-213.
ZHANG T, ZHU S X. Quadratic residue codes over F_l+vF_l [J]. Journal of University of Science and Technology of China, 2012, 42(3): 207-213.