Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 182–187*

Quadratic residue codes over a non-chain ring extension of $\mathbb{F}_2$

Abidin Kaya akaya@fatih.edu.tr
Department of Mathematics, Fatih University, Istanbul, Turkey
Bahattin Yildiz byildiz@fatih.edu.tr
Department of Mathematics, Fatih University, Istanbul, Turkey
Irfan Siap isiap@yildiz.edu.tr
Department of Mathematics, Yildiz Technical University, Istanbul, Turkey

Abstract. The focus in this work is on quadratic residue codes over the ring $\mathbb{F}_2+v\mathbb{F}_2$. We define these codes in terms of their idempotent generators and show that these codes share the properties analogous to that of quadratic residue codes over finite fields. We study Euclidean and Hermitian self-dual families of codes as extended quadratic residue codes over $\mathbb{F}_2 + v\mathbb{F}_2$. Further, we obtain two optimal self-dual codes from this family.

1 Introduction

Quadratic residue codes fall into the family of BCH codes and have proven to be a promising family of cyclic codes. Pless and Qian studied quaternary quadratic residue codes(over the ring $\mathbb{Z}_4$) and some of their properties in [5]. Recently, Taeri considered quadratic residue codes over the ring $\mathbb{Z}_9$ in [7]. Our aim in this paper is to work on quadratic residue codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2$ which is isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$. Codes over $\mathbb{F}_2 + v\mathbb{F}_2$ were first introduced by Bachoc in [1] together with a new weight. They are shown to be connected to lattices and have since generated interest among coding theorists. For some of the works in the literature about these codes we refer the readers to [1], [2], [3] and [4]. Recently, Zhu et. al. considered the structure of cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$ in [8]. We will first give some preliminaries about the ring $\mathbb{F}_2 + v\mathbb{F}_2$ and codes over $\mathbb{F}_2 + v\mathbb{F}_2$ in section 2. In section 3, quadratic residue codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2$ are defined and it is shown that they share the same general properties with quadratic residue codes over fields. In section 4, we obtain Euclidean self-dual codes for $p = 8r - 1$ and Hermitian self-dual codes for $p = 8r + 1$ as the extended quadratic residue codes over $\mathbb{F}_2 + v\mathbb{F}_2$. The binary images of these codes are also described.

2 Preliminaries

The ring $\mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, 1 + v\}$ is a commutative ring of order 4 and characteristic 2, with the restriction $v^2 = v$. It has two maximal ideals $\{0, v\}$ and

$\{0, 1+v\}$. So, it is not a local ring. A code C of length n over $\mathbb{F}_2 + v\mathbb{F}_2$ is an $(\mathbb{F}_2 + v\mathbb{F}_2)$-submodule of $(\mathbb{F}_2 + v\mathbb{F}_2)^n$. An element of C is called a codeword of C. A generator matrix of C is a matrix whose rows generate C. The Hamming weight of a codeword is the number of non-zero components. The Lee weight is defined as $w_L(0) = 0, w_L(1) = 2, w_L(1+v) = 1 = w_L(v)$ and the following Gray map is a linear isometry;

$$\begin{array}{rcl} \varphi & : & \mathbb{F}_2 + v\mathbb{F}_2 \to \mathbb{F}_2^2 \\ a + bv & \mapsto & (a, a+b)\,. \end{array}$$

It is easily observed that the ring $\mathbb{F}_2 + v\mathbb{F}_2$ is isomorphic to the ring $\mathbb{F}_2 \times \mathbb{F}_2$. In [1], Bachoc defined the following weight on $\mathbb{F}_2 + v\mathbb{F}_2$:

$$w_B(0) = 0, w_B(1) = 1, w_B(1+v) = 2, w_B(v) = 2.$$

The weight of a codeword is the sum of the weights of its components. The minimum Hamming, Lee and Bachoc weights, d_H, d_L and d_B of C are the smallest Hamming, Lee and Bachoc weights among the non-zero codewords of C, respectively. Let $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ be two elements of $(\mathbb{F}_2 + v\mathbb{F}_2)^n$. We consider two inner products, namely, the Euclidean inner product $\langle x, y\rangle_E = \sum x_i y_i$ and the Hermitian inner product $\langle x, y\rangle_H = \sum x_i \overline{y_i}$ where $\overline{0} = 0$, $\overline{1} = 1$, $\overline{v} = 1 + v$ and $\overline{1+v} = v$. The dual code $C^\perp$ of C with respect to the Euclidean inner product is defined as

$$C^\perp = \{x \in (\mathbb{F}_2 + v\mathbb{F}_2)^n \mid \langle x, y\rangle_E = 0 \text{ for all } y \in C\}$$

and the dual code C^* with respect to the Hermitian inner product of C is defined as

$$C^* = \{x \in (\mathbb{F}_2 + v\mathbb{F}_2)^n \mid \langle x, y\rangle_H = 0 \text{ for all } y \in C\}\,.$$

C is Euclidean self-dual if $C = C^\perp$ and Hermitian self-dual if $C = C^*$. The following theorems, taken from [8] characterize the structure of cyclic codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2$:

Theorem 1. *[8] For any cyclic code C of length n over $\mathbb{F}_2 + v\mathbb{F}_2$, there is a unique polynomial $g(x)$ such that $C = (g(x))$, and $g(x) \mid x^n - 1$, where $g(x) = g_1(x) + v(g_1(x) + g_2(x))$.*

Theorem 2. *[8] Every ideal of $R_n = (\mathbb{F}_2 + v\mathbb{F}_2)[x]/(x^n - 1)$ is principal.*

Theorem 3. *[8] If n is odd then every cyclic code over $\mathbb{F}_2 + v\mathbb{F}_2$ has a unique idempotent generator, i.e., it has a generator $a(x) \in R_n$ such that $a(x)^2 = a(x)$.*

In the sequel we let $p \equiv \pm 1 \pmod 8$ and $R_p := (\mathbb{F}_2 + v\mathbb{F}_2)[x](x^p - 1)$.

Lemma 1. *$\{(1+v)f + vh \mid f$ and h are idempotents in $\mathbb{F}_2[x]/(x^p - 1)\}$ is the set of all idempotents in R_p .*

Theorem 4. *Any cylic code C of length p over $\mathbb{F}_2 + v\mathbb{F}_2$ has a unique idempotent generator of the form $(1+v)f + vh$ where p is an odd prime and f and h are idempotents in $\mathbb{F}_2[x]/(x^p - 1)$.*

3 Quadratic residue codes over $\mathbb{F}_2 + v\mathbb{F}_2$

We will use idempotents to describe quadratic residue codes over $\mathbb{F}_2 + v\mathbb{F}_2$. For the rest of this work $e_1(x) = \sum_{i \in Q_p} x^i$ and $e_2(x) = \sum_{i \in N_p} x^i$, where Q_p denotes the set of quadratic residues modulo p and N_p denotes the set of quadratic non-residues modulo p and $h = 1 + e_1 + e_2$ is the polynomial that corresponds to the all 1-vector of length p. Let a be a non-zero element of $\mathbb{F}_p$, the map $\mu_a : \mathbb{F}_p \to \mathbb{F}_p$ is defined as $\mu_a(i) = ai \pmod p$. It is easy to see that $\mu_a(fg) = \mu_a(f)\,\mu_a(g)$ for polynomials f and g in R_p.

3.1 Case I

If $p = 8r - 1$ then e_1 and e_2 are generating idempotents of $\left[p, \frac{p+1}{2}\right]$ binary quadratic residue codes so $e_1 e_2 = h$. In the following, we define $(\mathbb{F}_2 + v\mathbb{F}_2)$-QR codes and investigate their properties.

Definition 1. *If $p = 8r-1$ let $Q_1 = ((1+v)\,e_1 + ve_2)$, $Q_2 = ((1+v)\,e_2 + ve_1)$ and $Q_1' = ((1+v)\,(1+e_2) + v\,(1+e_1))$, $Q_2' = ((1+v)\,(1+e_1) + v\,(1+e_2))$. These four codes are called quadratic residue codes over $\mathbb{F}_2 + v\mathbb{F}_2$ of length p.*

Theorem 5. *With the notation as in the above definition, the following hold for $(\mathbb{F}_2 + v\mathbb{F}_2)$-QR codes:*

a) Q_1 and Q_2 are equivalent and Q_1' and Q_2' are equivalent;

b) $Q_1 \cap Q_2 = (h)$ and $Q_1 + Q_2 = (\mathbb{F}_2 + v\mathbb{F}_2)\,[x] \,/\, (x^p - 1)$ where $h = 1 + e_1 + e_2$ the all one vector;

c) $|Q_1| = 4^{(p+1)/2} = |Q_2|$;

d) $Q_1 = Q_1' + \langle h \rangle$, $Q_2 = Q_2' + \langle h \rangle$;

e) $|Q_1'| = 4^{(p-1)/2} = |Q_2'|$;

f) Q_1' and Q_2' are self-orthogonal and $Q_1^{\perp} = Q_1'$ and $Q_2^{\perp} = Q_2'$;

g) $Q_1' \cap Q_2' = \{0\}$ and $Q_1' + Q_2' = \langle 1 + h \rangle$

3.2 Case II

If $p = 8r + 1$ then e_1 and e_2 are generating idempotents of $\left[p, \frac{p-1}{2}\right]$ binary quadratic residue codes so $e_1 e_2 = 0$.

Definition 2. *If $p = 8r + 1$ let $Q_1 = ((1+v)\,(1+e_1) + v\,(1+e_2))$, $Q_2 = ((1+v)\,(1+e_2) + v\,(1+e_1))$, $Q_1' = ((1+v)\,e_2 + ve_1)$, $Q_2' = ((1+v)\,e_1 + ve_2)$. These four codes are called quadratic residue codes over $\mathbb{F}_2 + v\mathbb{F}_2$ of length p.*

Theorem 6. *With the notation as in the above definition, the following hold for $(\mathbb{F}_2 + v\mathbb{F}_2)$-QR codes:*

a) Q_1 *and* Q_2 *are equivalent and* Q_1' *and* Q_2' *are equivalent;*

b) $Q_1 \cap Q_2 = (h)$ *and* $Q_1 + Q_2 = (\mathbb{F}_2 + v\mathbb{F}_2)[x]/(x^p - 1)$ *where* $h = 1 + e_1 + e_2$ *the all one vector;*

c) $|Q_1| = 4^{(p+1)/2} = |Q_2|$;

d) $Q_1 = Q_1' + \langle h \rangle$, $Q_2 = Q_2' + \langle h \rangle$;

e) $|Q_1'| = 4^{(p-1)/2} = |Q_2'|$;

f) $Q_1^{\perp} = Q_2'$ *and* $Q_2^{\perp} = Q_1'$;

g) $Q_1' \cap Q_2' = \{0\}$ *and* $Q_1' + Q_2' = \langle 1 + h \rangle$

4 Extended quadratic residue codes and binary images

In this section, we define extended quadratic residue codes over $\mathbb{F}_2 + v\mathbb{F}_2$. Further, we provide two optimal self-dual codes as applications to the main theorems. The extended code of a code C over $\mathbb{F}_2 + v\mathbb{F}_2$ will be denoted by $\overline{C}$, which is the code obtained by adding an overall parity check with respect to the Euclidean product to each codeword of C.

Theorem 7. *Suppose* $p = 8r - 1$ *and* Q_1, Q_2 *are* $\mathbb{F}_2 + v\mathbb{F}_2$*-QR codes in Theorem 5. Then* $\overline{Q_1}$ *and* $\overline{Q_2}$ *are self-dual.*

Example 1. *For* $p = 7$ *we get the Euclidean self-dual code* $\overline{Q_1}$ *with* $d_L\left(\overline{Q_1}\right) = 4 = d_H\left(\overline{Q_1}\right)$ *so it corresponds to* $[16, 8, 4]$ *optimal self-dual binary code and* $d_B\left(\overline{Q_1}\right) = 7$. Q_1 *which is generated by the idempotent* $e = (1 + v)\left(x + x^2 + x^4\right) + v\left(x^3 + x^5 + x^6\right)$ *in* R_7.

A self-dual code is called Type IV if all the Hamming weights are even, a binary code is called even if all the weights are even.

Proposition 1. *[1] [3] If* $C = (1 + v)C_1 \oplus vC_2$ *then* C *is a Euclidean self-dual if and only if* C_1 *and* C_2 *are binary self-dual codes.* $C = (1 + v)C_1 \oplus vC_2$ *is Euclidean Type IV self-dual if and only if* $C_1 = C_2$.

Proposition 2. *[1] [3] If* $C = (1 + v)C_1 \oplus vC_2$ *then* C *is a Hermitian self-dual if and only if* $C_1 = C_2^{\perp}$. $C = (1 + v)C_1 \oplus vC_1^{\perp}$ *is Hermitian Type IV self-dual if and only if* C_1 *and* $C_1^{\perp}$ *are even codes.*

The following gives an upper bound on the distances of Hermitian self-dual codes.

Theorem 8. *[1] Let* C *be a Hermitian self-dual code of length* n *over* $\mathbb{F}_2 \times \mathbb{F}_2$ *then* $w_B(C) \leq 2([n/3] + 1)$.

Codes that meet this bound are called extremal codes and Bachoc has shown that they correspond to extremal modular lattices. In the next theorem we would like to introduce another family of Hermitian self-dual codes by using quadratic residue codes:

Theorem 9. *Suppose $p = 8r+1$ and Q'_1, Q'_2 are $\mathbb{F}_2+v\mathbb{F}_2$-QR codes in Theorem 3.2. Then $Q'_1 + \langle \boldsymbol{v} \rangle$, $Q'_2 + \langle \boldsymbol{v} \rangle$, $Q'_1 + \langle \mathbf{1} + \boldsymbol{v} \rangle$ and $Q'_2 + \langle \mathbf{1} + \boldsymbol{v} \rangle$ are Hermitian self-dual codes of length p where $\boldsymbol{v}$ denotes the polynomial vh which corresponds to all-v vector and $\mathbf{1} + \boldsymbol{v}$ denotes the polynomial $(1 + v)\, h$ which corresponds to all-$(1 + v)$ vector.*

In [2] it is proven that there are no extremal codes for the lengths greater than 10, a self-dual code is called optimal if it has the best possible distance. Betsumiya et. al. obtained unique optimal self-dual codes for lengths 17 and 18 which are obtained by quadratic residue codes in a different way in the next examples:

Example 2. *For $p = 17$, the code $Q'_1+\langle \boldsymbol{v} \rangle$ is the unique optimal Hermitian self-dual code of length 17 with $d_B\left(Q'_1 + \langle v \rangle\right) = 10$ and Bachoc weight enumerator*

$$1 + 187z^{10} + 1156z^{12} + 2924z^{14} + 10030z^{16} + 18513z^{18} + 27744z^{20} \\ +29954z^{22} + 23188z^{24} + 12019z^{26} + 850z^{30} + 85z^{32} + z^{34}.$$

Example 3. *For $p = 17$, the extended quadratic residue code $\overline{Q_1}$ is the unique optimal Hermitian self-dual code of length 18 with $d_B\left(\overline{Q_1}\right) = 12$ and Bachoc weight enumerator*

$$1 + 1734z^{12} + 1836z^{14} + 13158z^{16} + 23869z^{18} + 46818z^{20} + 55080z^{22} \\ +57324z^{24} + 37026z^{26} + 18054z^{28} + 6324z^{30} + 756z^{32} + 153z^{34} + 2z^{36}$$

$d_H\left(\overline{Q_1}\right) = 6 = d_L\left(\overline{Q_1}\right)$ and $\overline{Q_1}$ is an optimal Hermitian Type IV self-dual code of length 18 as given in [4].

Example 4. *For $p = 23$, the extended quadratic residue code $\overline{Q_1}$ is Euclidean self-dual code with $d_B\left(\overline{Q_1}\right) = 14$, $d_H\left(\overline{Q_1}\right) = 8 = d_L\left(\overline{Q_1}\right)$ and Lee weight enumerator*

$$1 + 1518z^{8} + 5152z^{12} + 577599z^{16} + 3910368z^{20} + 7787940z^{24} \\ +3910368z^{28} + 577599z^{32} + 5152z^{36} + 1518z^{40} + z^{48}.$$

Theorem 10. *Suppose $p = 8r+1$ and Q_1, Q_2 are $\mathbb{F}_2+v\mathbb{F}_2$-QR codes in Theorem 6. Then $\overline{Q_1}$ and $\overline{Q_2}$ are Hermitian self-dual codes.*

We finish this section with the following theorem describing the duality relation between the extended quadratic residue codes:

Theorem 11. *Suppose $p = 8r+1$ and Q_1, Q_2 are $\mathbb{F}_2+v\mathbb{F}_2$-QR codes in Theorem 6. Then the Euclidean dual of $\overline{Q_1}$ is $\overline{Q_2}$ and the Euclidean dual of $\overline{Q_2}$ is $\overline{Q_1}$.*

Theorem 12. *The Gray images of the extended quadratic residue codes over $\mathbb{F}_2 + v\mathbb{F}_2$ are self-dual binary codes if $p = 8r - 1$ and formally self-dual binary codes if $p = 8r + 1$.*

References

[1] C. Bachoc, "Application of coding theory to the construction of modular lattices", *J. Combin. Theory Ser. A*, vol.78, pp. 92–119, 1997.

[2] K. Betsumiya, T.A. Gulliver, M. Harada, "Extremal Self-Dual Codes over $\mathbb{F}_2 \times \mathbb{F}_2$", *Design code cryptogr.*, vol.28, no.2, pp. 171–186, 2003.

[3] S.T. Dougherty, P. Gaborit, M. Harada, A. Munemasa, P. Sole, "Type IV Self Dual codes over Rings", *IEEE Trans. Inform. Theory*, vol.45, no.7, pp. 2345–2360, 1999.

[4] K. Betsumiya and M. Harada, "Optimal self-dual codes over $\mathbb{F}_2 \times \mathbb{F}_2$ with respect to the Hamming weight", *IEEE Trans. Inf. Theory*, vol.50, no.2, pp. 356–358, 2004.

[5] V. Pless, Z. Qian, "Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$", *IEEE Trans. Inform. Theory*, vol.42, no.5, pp. 1594–1600, 1996.

[6] S. Roman, *Coding and Information Theory,* Springer Graduate Texts in Mathematics, 1992.

[7] B.Taeri, "Quadratic Residue Codes over $\mathbb{Z}_9$", *J. Korean Math. Soc.*, vol.46, no.1, pp. 13–30, 2009.

[8] S.X. Zhu, Y. Wang, M.J. Shi, "Some Results on Cyclic Codes over $\mathbb{F}_2+v\mathbb{F}_2$", *IEEE Trans. Inf. Theory*, vol.56, no.4, pp. 1680–1684, 2010.