Proceedings of the International MultiConference of Engineers and Computer Scientists 2014 Vol II,
IMECS 2014, March 12 - 14, 2014, Hong Kong

$\mathbb{Z}_2(\mathbb{Z}_2+u\mathbb{Z}_2)-$Linear Cyclic Codes

Taher Abualrub, Irfan Siap, and Ismail Aydogdu

***Abstract*—Let $n=\alpha+2\beta$. In this paper, we introduce a new type of linear and cyclic codes defined over the ring $\mathbb{Z}_2R$ where $\mathbb{Z}_2=\{0,1\}$ is the binary finite field and the ring $R=\{0,1,u,u+1\}$ where $u^2=0$. We give the definition of these codes as subsets of the ring $\mathbb{Z}_2^\alpha\times R^\beta$. We give a one-to-one correspondence between elements in $\mathbb{Z}_2^\alpha\times R^\beta$ and elements in the ring $R_{\alpha,\beta}=\mathbb{Z}_2[x]/(x^\alpha-1)\times R[x]/\left(x^\beta-1\right)$, and hence relate these codes to subsets of the ring $R_{\alpha,\beta}$. We prove that C is a $\mathbb{Z}_2R$-cyclic code if and only if C is an $R[x]$-submodule of $R_{\alpha,\beta}$. We provide some examples of $\mathbb{Z}_2R-$linear cyclic codes that produce optimal binary linear codes.**

***Index Terms*—Linear codes, $\mathbb{Z}_2R$-linear codes, submodules.**

I. Introduction

Let $n=\alpha+2\beta$ where $\alpha,\ \beta$ are positive integers. Consider the finite field $\mathbb{Z}_2=\{0,1\}$ and the finite ring $\mathbb{Z}_2+u\mathbb{Z}_2=R=\{0,1,u,u+1\}$ where $u^2=0$. It is known that the ring $\mathbb{Z}_2$ is a subring of the ring R. We construct the ring

$$\mathbb{Z}_2R=\{(e_1,e_2)\mid e_1\in\mathbb{Z}_2 \text{ and } e_2\in R\}.$$

The ring $\mathbb{Z}_2R$ is not closed under standard multiplication $(\bmod 2)$ by the element u in the ring R. This implies that the ring is NOT an $R-$module under the operation of standard multiplication. To make the ring $\mathbb{Z}_2R$ an $R-$module we need to introduce the following method of multiplications: Define the mapping

$$\begin{aligned}\eta &: R\to\mathbb{Z}_2 \text{ by}\\ \eta(r+uq) &= r.\end{aligned}$$

So, $\eta(0)=0,\ \eta(1)=1,\ \eta(u)=0$ and $\eta(u+1)=1$. It is clear that the mapping η is a ring homomorphism. Now for any element $d\in R$, define the following multiplication

$$d*(e_1,e_2)=(\eta(d)e_1,de_2).$$

This a well-defined multiplication. In fact this multiplication can be generalized over the ring $\mathbb{Z}_2^\alpha\times R^\beta$ in the following way: for any $d\in R$ and $v=(a_0,a_1,...,a_{\alpha-1},b_0,b_1,...,b_{\beta-1})\in\mathbb{Z}_2^\alpha\times R^\beta$ define

$$dv=(\eta(d)a_0,\eta(d)a_1,...,\eta(d)a_{\alpha-1},db_0,db_1,...,db_{\beta-1}).$$

This definition gives us the following result:

Lemma 1: The ring $\mathbb{Z}_2^\alpha\times R^\beta$ is an $R-$module under the above definition.

Definition 2: A non-empty subset C of $\mathbb{Z}_2^\alpha\times R^\beta$ is called a $\mathbb{Z}_2R$-linear code if C is an R-submodule of $\mathbb{Z}_2^\alpha\times R^\beta$.

T. Abualrub is with the Department of Mathematics and Statistics at the American University of Sharjah, Sharjah, UAE, e-mail: abualrub@aus.edu.

I. Siap and I. Aydogdu are with Department of Mathematics at Yildiz Technical University, Istanbul, Turkey. e-mail: isiap (iaydogdu) @yildiz.edu.tr.

Note that this definition was introduced in [4], and it is a little bit different than the definition of $\mathbb{Z}_2\mathbb{Z}_4-$additive codes that appears in [1-3]. In the case of $\mathbb{Z}_2\mathbb{Z}_4-$additive codes, subgroups of $\mathbb{Z}_2^\alpha\times\mathbb{Z}_4^\beta$ are the same as $\mathbb{Z}_4$-submodules of $\mathbb{Z}_2^\alpha\times\mathbb{Z}_4^\beta$ and hence a non-empty subset C of $\mathbb{Z}_2^\alpha\times Z_4^\beta$ is called a $\mathbb{Z}_2Z_4$-additive code if C is a subgroup (or $\mathbb{Z}_4-$submodule) of $\mathbb{Z}_2^\alpha\times\mathbb{Z}_4^\beta$. On the other hand subgroups of $\mathbb{Z}_2^\alpha\times R^\beta$ are different than $R-$submodules of $\mathbb{Z}_2^\alpha\times R^\beta$. The subgroups of $\mathbb{Z}_2^\alpha\times R^\beta$ are closed only under binary operation while submodules are subgroups of $\mathbb{Z}_2^\alpha\times R^\beta$ that are also closed under multiplications by elements in the ring R. This is the reason for referring to them as $\mathbb{Z}_2R$-linear codes and not additive codes as the case of $\mathbb{Z}_2\mathbb{Z}_4$. It is worth mentioning that if $\beta=0$, then theses codes are binary linear codes and if $\alpha=0$, then they are the linear codes over the ring R.

If C is a $\mathbb{Z}_2R$-additive code then as a group it is isomorphic to $\mathbb{Z}_2^{k_0}\times\mathbb{Z}_2^{2k_1}\times\mathbb{Z}_2^{k_2}$.

Definition 3: If $C\subseteq\mathbb{Z}_2^\alpha\times R^\beta$ is a $\mathbb{Z}_2R$-linear code, group isomorphic to $\mathbb{Z}_2^{k_0}\times\mathbb{Z}_2^{2k_1}\times\mathbb{Z}_2^{k_2}$, then C is called a $\mathbb{Z}_2R$-additive code of type $(\alpha,\beta,k_0,k_1,k_2)$ where $k_0,\ k_1$, and k_2 are defined above.

Next, we introduce the definition of a cyclic linear code which is a natural extension of the classical definition of a cyclic code.

II. $\mathbb{Z}_2R-$linear cyclic codes.

Definition 4: A subset C of $\mathbb{Z}_2^\alpha\times R^\beta$ is called a $\mathbb{Z}_2R$-linear cyclic code if

1) C is a linear code, and
2) For any codeword $u=(a_0a_1\ldots a_{\alpha-1},b_0b_1\ldots b_{\beta-1})\in C$, its cyclic shift

$$T(u)=(a_{\alpha-1}a_0\ldots a_{\alpha-2},b_{\beta-1}b_0\ldots b_{\beta-2})$$

is also in C.

An element $c=(a_0a_1\ldots a_{\alpha-1},b_0b_1\ldots b_{\beta-1})\in\mathbb{Z}_2^\alpha\times R^\beta$ can be identified with a module element consisting of two polynomials

$$\begin{aligned}c(x) &= \begin{pmatrix} a_0+a_1x+\ldots+a_{\alpha-1}x^{\alpha-1},\\ b_0+b_1x+\ldots+b_{\beta-1}x^{\beta-1}\end{pmatrix}\\ &= (a(x),b(x))\end{aligned}$$

in $R_{\alpha,\beta}=\mathbb{Z}_2[x]/(x^\alpha-1)\times R[x]/\left(x^\beta-1\right)$. This identification gives a one-to-one correspondence between elements in $\mathbb{Z}_2^\alpha\times R^\beta$ and elements in $R_{\alpha,\beta}$

Let $f(x)=f_0+f_1x+\ldots+f_tx^t\in R[x]$, $(g(x),h(x))\in R_{\alpha,\beta}$ and consider the following multiplication

$$f(x)*(g(x),h(x))=(\eta(f(x))g(x),f(x)h(x)).$$

ISBN: 978-988-19253-3-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

where

$$\eta\left(f(x)\right)=\eta\left(f_0\right)+\eta\left(f_1\right)x+\ldots+\eta\left(f_t\right)x^t$$

This multiplication operation on $R_{\alpha,\beta}$ leads to the following easily proven theorem.

Theorem 5: The multiplication above is well-defined. Moreover, $R_{\alpha,\beta}$ is an $R[x]$-module with respect to this multiplication.

As is common in the discussion of cyclic codes, we can regard codewords of a cyclic code C as vectors or as polynomials interchangeably. In either case, we use the same notation C to denote the set of all codewords. We follow this convention in the definition below and in the rest of the paper.

Definition 6: A subset $C\subseteq R_{\alpha,\beta}$ is called a $\mathbb{Z}_2R$-cyclic code if

1) C is a subgroup of $R_{\alpha,\beta}$, and
2) If

$$c(x)=\left(\begin{array}{c} a_0+a_1x+\ldots+a_{\alpha-1}x^{\alpha-1}, \\ b_0+b_1x+\ldots+b_{\beta-1}x^{\beta-1}\end{array}\right)\in C,$$

then for any $a\in R$, we have

$$ax{*}c(x)=\left(\begin{array}{c}\eta\left(a\right)\left(a_{\alpha-1}{+}a_0x+\ldots+a_{\alpha-2}x^{\alpha-1}\right), \\ a\left(b_{\beta-1}{+}b_0x+\ldots+b_{\beta-2}x^{\beta-1}\right)\end{array}\right)$$

is also in C.

Theorem 7: A code C is a $\mathbb{Z}_2R$-cyclic code if and only if C is an $R[x]$-submodule of $R_{\alpha,\beta}$.

III. Examples

In this section we introduce some examples within this family of codes which have good parameters.

Example 8: Let $R_{2,3}=\mathbb{Z}_2[x]/(x^2-1)\times R[x]/(x^3-1)$ and consider a $\mathbb{Z}_2R-$linear cyclic code of the form $\mathcal{C}=\left((x-1),(x^2+x+1)+u\right)$. The code $\mathcal{C}$ has $2^22^2=16$ codewords.

$$C=\left\{\begin{array}{c}(0,0,0,0,0),(1,1,1+u,1,1),(1,1,1+u,1+u,1),\\ (1,1,1,1+u,1),(1,1,1+u,1+u,1+u),\\ (1,1,1,1,1+u),(1,1,1+u,1,1+u),(1,1,1,1+u,1+u),\\ (1,1,1,1,1),(0,0,u,u,u),(0,0,u,u,0),\ (0,0,0,u,u),\\ (0,0,u,0,u),(0,0,0,0,u),(0,0,u,0,0),(0,0,0,u,0)\end{array}\right\}$$

Example 9: Let $\mathcal{C}$ be a $\mathbb{Z}_2R-$linear cyclic code of type $(7,7;3,0,3)$ in the form of $\mathcal{C}=\left(1+x+x^2+x^4,u(1+x)\right)$. Therefore C has the generator matrix,

$$\begin{bmatrix}1&1&1&0&1&0&0&u&u&0&0&0&0&0\\0&1&1&1&0&1&0&0&u&u&0&0&0&0\\0&0&1&1&1&0&1&0&0&u&u&0&0&0\\1&0&0&1&1&1&0&0&0&0&u&u&0&0\\0&1&0&0&1&1&1&0&0&0&0&u&u&0\\1&0&1&0&0&1&1&0&0&0&0&0&u&u\end{bmatrix}.$$

The Gray image gives the optimal binary linear code with parameters $[21,6,8]$.

Example 10: Let $\mathcal{C}$ be a $\mathbb{Z}_2R-$linear cyclic code of type $(15,15;4,1,0)$ in the form of

$$\mathcal{C}=\left(\begin{array}{c}1+x+x^2+x^4+x^5+x^8+x^{10},1+x+x^2+\ldots\\ +x^{14}+u(1+x+x^2+x^4+x^5+x^8+x^{10})\end{array}\right).$$

The Gray image gives the binary linear code which has good parameters $[45,6,22]$.

IV. Conclusion

In this work, linear and cyclic codes are introduced over the ring $\mathbb{Z}_2R$ where $\mathbb{Z}_2=\{0,1\}$ is the binary finite field and the ring $R=\{0,1,u,u+1\}$ where $u^2=0$. Their algebraic structure is studied. It is shown that code C is a $\mathbb{Z}_2R$-cyclic code if and only if C is an $R[x]$-submodule of $R_{\alpha,\beta}$. Our examples show that these codes can be used to construct optimal binary linear codes.

References

[1] T. Abualrub, I. Siap, and N. Aydin, "Z2Z4-additive Cyclic Codes," IEEE transaction on Information Theory, accepted (October 2013).

[2] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva, $\mathbb{Z}_2Z_4$-linear codes: generator matrices and duality, Design, Codes, and Cryptography, volume 54, number 2, pp. 167-179, August 2009.

[3] H. Rifà-Pous, J. Rifà, L. Ronquillo, $\mathbb{Z}_2Z_4$-additive perfect codes in Steganography, Advances in Mathematics of Communications vol. 5, issue 3, pp. 425-433, 2011.

[4] I. Aydogdu, T. Abualrub, I. Siap, " On $\mathbb{Z}_2\mathbb{Z}_2[u]-$additive Codes", International Journal of Computer Mathematics, accepted (November 2013).

ISBN: 978-988-19253-3-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)