International Journal of Algebra, Vol. 9, 2015, no. 3, 115 - 121
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ija.2015.529

Quantum Codes over the Ring

$$F_2 + uF_2 + u^2F_2 + ... + u^mF_2$$

Abdullah Dertli

Ondokuz Mayıs University, Faculty of Arts and Sciences
Mathematics Department, Samsun, Turkey

Yasemin Cengellenmis

Trakya University, Faculty of Arts and Sciences
Mathematics Department, Edirne, Turkey

Senol Eren

Ondokuz Mayıs University, Faculty of Arts and Sciences
Mathematics Department, Samsun, Turkey

Abstract

A method to obtain self orthogonal codes over finite field F_2 is given and the parameters of quantum codes which are obtained from cyclic codes over $R = F_2 + uF_2 + u^2F_2 + ... + u^mF_2$ are determined.

Mathematics Subject Classification: 94B05, 94B15

Keywords: Cyclic codes, Quantum codes, Finite rings.

1 Introduction

Quantum error correcting code was discovered by Shor [8]. A first systematic way to construct it from classical linear code was given Calderbank et al [1]. It

has been constructed by using classical cyclic codes over finite field F_q. Later, some people constructed it from linear codes over finite rings.

In [7], a new method to obtain self orthogonal codes over F_2 was given by J.Qian et al. They gave a construction for quantum error correcting codes from cyclic codes over finite ring $F_2 + uF_2$ where $u^2 = 0$. X.Kai, S.Zhu gave construction for quantum codes from cyclic codes over $F_4 + uF_4$ where $u^2 = 0$ in [3]. X.Yin and W.Ma gave existence condition of quantum codes which are derived from cyclic codes over finite ring $F_2 + uF_2 + u^2F_2$ where $u^3 = 0$ in [9]. J.Qian gave a new method constructing quantum error correcting codes from cyclic codes over finite ring $F_2 + vF_2$ where $v^2 = v$ in [5].

This paper is organized as follows. In section 2, we give some knowledges about the finite ring R, the Galois ring $GR(R,t)$ and the codes over finite ring. In section 3, by using Gray map, we show that if C is self orthogonal so is $\psi(C)$. In section 4, a sufficient and necessary condition for cyclic codes over R that contains its dual is given. The parameters of quantum error correcting codes which are obtained from cyclic codes over R are obtained.

2 Preliminaries

Let R be the commutative ring $F_2 + uF_2 + u^2F_2 + ... + u^mF_2 = F_2[u] / \langle u^{m+1} \rangle$ where u is an indeterminate and $u^{m+1} = 0$. The ring is endowed with the obvious addition and multiplication with the property that $u^{m+1} = 0$. R is a finite chain ring with maximal ideal uR and residue field F_2. The ideals are (0), (1), (u),..., (u^m).

A linear code C over R of length n is a R submodule of R^n.An element of C is called a codeword. Let σ be map from R^n to R^n given by $\sigma(r_0, r_1, ..., r_{n-1}) = (r_{n-1}, r_0, ..., r_{n-2})$. Then C is said to be cyclic code if $\sigma(C) = C$. Let the C be a code of length n over R and $P(C)$ be its polynomial representation

$$P(C) = \left\{ \sum_{i=0}^{n-1} r_i x^i \ : (r_0, r_1, ..., r_{n-1}) \in C \right\}$$

A subset C of R^n is a linear cyclic code of length n if and only if its polynomial representation is an ideal of $R[x] / \langle x^n - 1 \rangle$. The homogeneous weight of $r \in R$ is given by

$$w_{\text{hom}}(r) = \begin{cases} 2^{m-1} & \text{if } r \in R \backslash Ru \\ 2^m & \text{if } r \in Ru \backslash \{0\} \\ 0 & \text{otherwise} \end{cases}$$

This extends to a weight function in R^n. For $r = (r_0, r_1, ..., r_{n-1}) \in R^n$ the homogeneous weight of C is defined as

$$w_{\hom}(r) = \sum_{i=0}^{n-1} w_{\hom}(r_i)$$

The minimum homogeneous distance of C is defined as $d_{\hom}(C) = \min\{ d_{\hom}(c, \acute{c})\}$ for any $c,\acute{c} \in C$, $c \neq \acute{c}$ where $d_{\hom}(c, \acute{c})$ is the homogeneous distance two codewords with $d_{\hom}(c, \acute{c}) = w_{\hom}(c - \acute{c})$.

Let C be a code over F_2 of length r and let $c = (c_0, c_1, ..., c_{r-1})$ be a codeword of C. The Hamming weight of c is defined as

$$w_H(c) = \sum_{i=0}^{r-1} w_H(c_i)$$

where $w_H(c_i) = 1$ if $c_i = 1$ and $w_H(c_i) = 0$ if $c_i = 0$. The minimum Hamming distance of C is defined as $d_H(C) = \min\{d_H(c, \acute{c})\}$ for any $c,\acute{c} \in C$, $c \neq \acute{c}$ where $d_H(c, \acute{c})$ is the Hamming distance two codewords with $d_H(c, \acute{c}) = w_H(c - \acute{c})$.

For any $x = (x_0, x_1, ..., x_{n-1})$, $y = (y_0, y_1, ..., y_{n-1})$ the inner product is defined as

$$x.y = \sum_{i=0}^{n-1} x_i y_i$$

If $x.y = 0$ then x and y are said to be orthogonal. Let C be linear code of length n over R, the dual code of C,

$$C^{\perp} = \{x : \forall y \in C, x.y = 0\}$$

which is also a linear code over R of length n. A code C is self orthogonal if $C \subseteq C^{\perp}$ and self dual if $C = C^{\perp}$.

Let $R[x]$ be the ring of polynomial over R. By using a natural homomorphic mapping from R to F_2, a polynomial reduction mapping μ is defined as follows

$$\mu : \ R[x] \to F_2[x]$$
$$f(x) = \sum_{i=0}^{q} a_i x^i \longmapsto \sum_{i=0}^{q} \hat{a}_i x^i$$

where $\hat{a}$ denotes the polynomial reduction mod u for any $a \in R$.

A monic polynomial f over $R[x]$ is said to be a basic irreducible polynomial if its projection $\mu(f)$ is irreducible over $F_2[x]$. The Galois ring of R denoted as $GR(R, t)$ is defined as $R[x] / \langle g(x) \rangle$ where $g(x)$ is a monic basic irreducible polynomial in $R[x]$ of degree t. Thus the ring $GR(R, t)$ is a module over R. The basic monic irreducible polynomial of degree t over R can be lifted from a monic irreducible polynomial over F_2. Like Galois fields, $GR(R, t)$ is unique for given t. The group of units of $GR(R, t)$ is given as follows

$$GR(R, t)^* = G_C \times G_A$$

where G_C is cyclic group of order $2^t - 1$, G_A is an Abelian group of order 2^{mt} and $\times$ represents direct product.

The set $\{G_C, 0\}$ is isomorphic to the residue field F_{2^t} and is also a subspace of $GR(R,t)$. Hence the set is a subring over $GR(R,t)$ in [6].

The only ideals of $GR(R,t)$ are (0), (1),..., (u^m). Thus any elements of $GR(R,t)$ can be uniquely represented as $\alpha = \alpha_1 + u\alpha_2 + ... + u^m\alpha_{m+1}$ where $\alpha_i \in F_{2^t}$ and $1 \leq i \leq m+1$ in [6].

3 The Gray Map and Gray Images of Linear Codes Over R

In [2], the Gray map is defined as follows

$$\psi : R^n \to F_2^{2^m n}$$

$$a_0 + ua_1 + ... + u^m a_m \mapsto (a_m, a_m \oplus a_0, a_m \oplus a_1, a_m \oplus a_1 \oplus a_0, a_m \oplus a_2,$$

$$a_m \oplus a_2 \oplus a_0, a_m \oplus a_2 \oplus a_1, a_m \oplus a_2 \oplus a_1 \oplus a_0, a_m \oplus a_3, a_m \oplus a_3 \oplus a_0,$$

$$a_m \oplus a_3 \oplus a_1, a_m \oplus a_3 \oplus a_1 \oplus a_0, a_m \oplus a_3 \oplus a_2, a_m \oplus a_3 \oplus a_2 \oplus a_0, a_m \oplus a_3 \oplus a_2 \oplus a_1,$$

$$a_m \oplus a_3 \oplus a_2 \oplus a_1 \oplus a_0, a_m \oplus a_4, ..., a_m \oplus a_{m-1} \oplus ... \oplus a_4 \oplus a_3 \oplus a_2 \oplus a_1 \oplus a_0)$$

where $\oplus$ is componentwise addition in F_2.

ψ is a weight preserving map from (R^n, Homogeneous weight) to ($F_2^{2^m n}$, Hamming weight) and isometry from (R^n, Homogeneous distance) to ($F_2^{2^m n}$, Hamming distance).

Theorem 3.1 *If C is an (n, k, d_{hom}) linear codes over R then $\psi(C)$ is a $(2^m n, k, d_H)$ linear codes over F_2 where $d_{\text{hom}} = d_H$.*

Proof It is obvious that $\psi(x+y) = \psi(x) + \psi(y)$ and $\psi(\alpha x) = \alpha\psi(x)$ where $x, y \in R^n$, $\alpha \in F_2$. Thus ψ is linear. As ψ is bijective then $|C| = |\psi(C)|$ so we have $d_{\text{hom}} = d_H$.

Theorem 3.2 *If C is self orthogonal, then $\psi(C)$ is self orthogonal codes.*

Proof Let $c = a_0 + ua_1 + ... + u^m a_m$, $\acute{c} = \acute{a}_0 + u\acute{a}_1 + ... + u^m\acute{a}_m$ where $a_i, \acute{a}_i \in F_2$ for $i = 0, 1, ..., m$. Since C is self orthogonal, so we have $a_0\acute{a}_0 = 0$, $\sum_{i=0}^{m} a_i\acute{a}_{m-i} = 0$ for $1, 2, ..., m$. By using this, we have $\psi(c)\psi(\acute{c}) \equiv 0 \pmod 2$. Therefore, we have $\psi(C)$ is self orthogonal.

We know from [4] that a code C over R of length n is permutation equivalent to a code with generator matrix of the following form

$$G = \begin{bmatrix} I_{k_0} & A_{0,1} & A_{0,2} & \dots & A_{0,m-1} & A_{0,m} \\ 0 & uI_{k_1} & uA_{1,2} & \dots & uA_{1,m-1} & uA_{1,m} \\ 0 & 0 & u^2I_{k_3} & \dots & u^2A_{2,m-1} & u^2A_{2,m} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & u^mI_{k_m} & u^mA_{m,m} \end{bmatrix}$$

For a code C over R the following Torsion codes are defined. For $i = 0, 1, ..., m$

$$Tor_i(C) = \left\{a : \ u^i a \in C\right\}$$

$$Tor_0(C) = \{a \pmod u : \ a \in C\} = \operatorname{Re} s(C)$$

A code with a generator matrix in this form is of type $\{k_0, k_1, ..., k_m\}$ and has $2^{\sum_{i=0}^{m}(m+1-i)k_i}$ vectors.

The code over F_2 with generator matrix

$$G_i = \begin{bmatrix} I_{k_0} & \bar{A}_{0,1} & \bar{A}_{0,2} & \dots & \bar{A}_{0,m-1} & \bar{A}_{0,m} \\ 0 & I_{k_1} & \bar{A}_{1,2} & \dots & \bar{A}_{1,m-1} & \bar{A}_{1,m} \\ 0 & 0 & I_{k_3} & \dots & \bar{A}_{2,m-1} & \bar{A}_{2,m} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & I_{k_i} & \bar{A}_{i,m} \end{bmatrix}$$

where $\bar{A}_{i,j} \equiv A_{i,j} \pmod u$ is the Torsion code and $|Tor_i(C)| = \prod_{j=0}^{i} 2^{k_j}$.

The parameters of C over R are given $\left[n, 2^{\sum_{i=0}^{m}(m+1-i)k_i}, d_{\hom}\right]$ where $d_{\hom}$ is the homogeneous distance of C.

4 Quantum Codes Obtained From Cyclic Codes Over R

In [1], CSS contruction is stated as follows.

Theorem 4.1 *Let C and C_1 be two binary codes with parameters $[n, k, d]$ and $[n, k_1, d_1]$, respectively. If $C^{\perp} \subseteq C_1$ then an $[[n, k + k_1 - n, \min\{d, d_1\}]]$ quantum code can be constructed. Especially, if $C^{\perp} \subseteq C$, then there exist an $[[n, 2k - n, d]]$ code.*

From [9], we have the following theorems.

Theorem 4.2 *Suppose C is a cyclic code of odd length n over R, then there are unique monic polynomials F_i for $i = 0, 1, ..., m+1$ such that $C =< \widehat{F}_1, u\widehat{F}_2, ..., u^m\widehat{F}_{m+1} >$ where $F_0F_1...F_{m+1} = x^n - 1$ and $\widehat{F}_i$ denotes the product of all F_j except F_i. Moreover $|C| = 2^s$ where $s = \sum_{i=0}^{m} (m+1-i) \deg F_{i+1}$.*

Theorem 4.3 *Let C be a cyclic code of odd length n over R and $C =< \widehat{F}_1, u\widehat{F}_2, ..., u^m\widehat{F}_{m+1} >$ where $F_0F_1...F_{m+1} = x^n - 1$, then $C^\perp =< \widehat{F}_0^*, u\widehat{F}_{m+1}^*, u^2\widehat{F}_m^* ..., u^m\widehat{F}_2^* >$ where $\widehat{F}_i^*$ are reciprocal polynomial of $\widehat{F}_i$ and $\left|C^\perp\right| = 2^t$ where $t = \sum_{i=1}^{m+1} i. \deg F_{i+1}$.*

Lemma 4.4 *A binary linear cyclic code C with generator polynomial $g(x)$ contains its dual code if and only if*

$$x^n - 1 \equiv 0 \pmod{gg^*}$$

where $g^*(x) = x^{n-k} g\left(\frac{1}{x}\right)$.

We have a sufficient and necessary condition for cyclic codes over R that contains its dual.

Theorem 4.5 *Suppose C is a cyclic code of odd length n over R, then $C^\perp \subseteq C$ iff*

$$x^n - 1 \equiv 0 \left(\mathrm{mod} \left(u^i \widehat{F}_{i+1}\right) \left(u^j \widehat{F}_{m+1-j}^*\right)\right)$$

where $0 \leq i, j \leq m$.

So, we have the parameters of quantum codes as follows.

Theorem 4.6 *Let C be a cyclic code of odd length n over R with 2^s elements where $s = \sum_{i=0}^{m} (m+1-i) \deg F_{i+1}$, $x^n - 1 = \prod_{i=0}^{m+1} F_i$. If $C^\perp \subseteq C$, then there exist a quantum error correcting code with parameters $[[2^m n, 2s - 2^m n, d_{\mathrm{hom}}]]$ where d_{hom} is the minimum homogeneous distance of C.*

5 Conclusion

In [7] and [9] they obtained quantum error-correcting codes from cyclic codes over finite rings F_2+uF_2 and $F_2+uF_2+u^2F_2$, respectively. We have generalized it to finite ring $R = F_2 + uF_2 + u^2F_2 + ... + u^mF_2$ and we have the parameters of quantum codes which are obtained from cyclic codes over R.

References

[1] A. R. Calderbank, E. M. Rains, P. M. Shor, N. J. A. Sloane, Quantum error correction via codes over $GF(4)$, *IEEE Trans. Inf. Theory,* **44** (1998), 1369 - 1387. http://dx.doi.org/10.1109/18.681315

[2] Y.Cengellenmis, On $(1-u^m)$ −Cyclic Codes Over $F_2 + uF_2 + u^2F_2 + ... + u^mF_2$, *Int. J. Contemp. Math. Sciences,* **4** (2009), 987 - 992.

[3] X. Kai, S. Zhu, Quaternary construction of quantum codes from cyclic codes over $F_4 + uF_4$, *Int. J. Quantum Inform.,* **9** (2011), 689 - 700. http://dx.doi.org/10.1142/s0219749911007757

[4] M. Mehrdad, Torsion Codes Over a Finite Chain Rings, *Second Workshop on Algebra and its Applications,* (2012).

[5] J. Qian, Quantum codes from cyclic codes over $F_2 + vF_2$, *Journal of Inform.& computational Science,* **6** (2013), 1715 - 1722. http://dx.doi.org/10.12733/jics20101705

[6] J. Qian, L. Zhang, S. Zhu, Cyclic Codes Over $F_p + uF_p + ... + u^{k-1}F_p$, *IEICE Trans. Fundamentals,* **3** (2005). http://dx.doi.org/10.1093/ietfec/e88-a.3.795

[7] J. Qian, W. Ma, W. Gou, Quantum codes from cyclic codes over finite ring , *Int. J. Quantum Inform.,* **7** (2009), 1277 - 1283. http://dx.doi.org/10.1142/s0219749909005560

[8] P. W. Shor, Scheme for reducing decoherence in quantum computer memory, *Phys. Rev. A,* **52** (1995), 2493- 2496. http://dx.doi.org/10.1103/physreva.52.r2493

[9] X. Yin, W. Ma, Gray Map And Quantum Codes Over The Ring $F_2+uF_2+u^2F_2$, *International Joint Conferences of IEEE TrustCom-11,* (2011).

Received: March 8, 2015; Published: March 22, 2015