Институт за физика

Physica Macedonica **61**, (2012) p. 121-126
ISSN 1409-7168

ENUMERATION OF CODES OVER THE RING $F_q + uF_q$

E. Saltürk[1] and İ. Şiap[2]

[1-2]*Yildiz Technical University, Davutpasa Campus, Mathematics Department, 34210, İstanbul, Turkey*

Abstract. We count the codes over $F_q + uF_q$ by their generator matrices where $u^2 = 0$ and q is a prime power. We prove a theorem that gives a direct formula for counting the distinct (not necessarily inequivalent) linear codes over this ring. As a result of this theorem, we define Generalized Gaussian Numbers and state some of their properties. Finally, we present some number sequences which are new to our best knowledge.

PACS: 02.10.Hh, 02.10.De

1. INTRODUCTION

The number of the subcodes of a linear code is one of the most important problems of the combinatorial coding theory. This problem was completely solved for the codes over finite fields and presented by Gaussian coefficients [8]. Formula which gives the number of subgroups of type μ of a given finite $p-$group of type one were given by Delsarte [3], Djubjuk [4] and Yeh [16] in 1948. Calugareanu [2] found a formula which gives the total number of subgroups of an abelian finite group whose $p-$ranks do not exceed two.

The number of linear quaternary codes has been obtained recently [13]. Further, some interesting number sequences which follow from so called Type I Generalized Gaussian Numbers are also presented [13]. Here, we study the number of linear codes over the ring $F_q + uF_q$ ($u^2 = 0$): This ring has been of great interest to many researchers [1, 7, 10, 11, 15] and also found many applications. Our method for counting the linear codes is based on the construction of the generator matrices of the codes over $F_q + uF_q$. We choose ordered linearly independent elements for the generator matrices. Moreover, we present some new integer sequences which follow as an application of the number of linear codes over $F_q + uF_q$. This family of numbers is called Generalized Gaussian Numbers such as called in [14] due to resemble to the original Gaussian Numbers. Finally, we present some formulas and some new sequences.

Let F_q be a finite field with q elements where q is a prime power. A linear code C of length n over F_q is a subspace of F_q^n.

A linear code over F_q is equivalent to a F_q-code with generator matrix: $(I_k \;\; A)$.

Definition 1. [8] For a positive integer $q \neq 1$ and all nonnegative integers k, the $q-$ary Gaussian coefficient $\left|G_q(n,k)\right|$ $(n \in \mathbb{N})$ are defined by

$$\begin{bmatrix} n \\ 0 \end{bmatrix}_q = 1 \quad \text{and} \quad \begin{bmatrix} n \\ 0 \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\ldots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\ldots(q-1)}, \quad k=1,2,\ldots$$

Theorem 2. [8] The number of distinct (although not necessarily inequivalent) $[n,k]-$ codes over F_q is the $q-$ary Gaussian coefficient $\left|G_q(n,k)\right|$.

For the proof of this theorem and some more details the reader is friendly directed to [8]. Let $R_q = F_q + uF_q$ where q is a prime power and $u^2 = 0$ denote a finite ring of q^2 elements.

Definition 1. An R submodule C of R^n is called an $R-$linear code, the elements of C are called codewords.

Theorem 3. [10] A linear code C over R_q is permutation equivalent to a code with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & A_{11} & A_{12} \\ 0 & uI_{k_2} & uA_{22} \end{pmatrix} \tag{1}$$

where A_{ij}'s denote matrices whose entries are from R_q and I_{k_1}, I_{k_2} are identity matrices of sizes k_1, k_2 respectively. The number of elements of C is equal to $q^{2k_1+k_2}$. A linear code C generated by the matrix (1) is called a $(k_1,k_2)-$type code.

2. CODES OVER $F_q + uF_q$

In this main section, we present a direct formula which gives the number of all distinct codes over R_q which is the main goal of this paper. The ring $F_q + uF_q = F_q[u]/(u^2)$ where $u^2 = 0$ has q^2 elements in total and has both units and non-units. The non-units are multiple of u and units are not. There are $(q-1)q$ units and $q-1$ non-units. If an element of $R_q \setminus \{0\}$ is a unit we say that its order is q^2 (generates the all ring as an ideal) otherwise q.

An element of the ring R_q^n is said to be free if at least one of its entries is a unit otherwise it is called non-free. Hence, free elements of R_q^n are of order q^2 and non-free elements are of order q. Zero vector is of order 1 and it is neither unit nor non-unit.

Now, we state and prove the main theorem:

Theorem 4. The number of distinct (not necessarily inequivalent) $[n,(k_1,k_2)]-$ codes over R_q is

$$N_{k_1,k_2}^{R_q} = \frac{\prod_{t=1}^{2}\prod_{i=0}^{k_t-1}\left(\left(q^{3-t}\right)^n - \left(q^{2-t}\right)^n q^{\sum_{j=0}^{t-1}k_j q^i}\right)}{\prod_{s=1}^{2}\prod_{r=0}^{k_s-1}\left(\prod_{p=1}^{s}\left(q^{3-s}\right)^{k_p}\prod_{j=s+1}^{2}\left(q^{3-j}\right)^{k_j} - \left(\prod_{p=1}^{s}\left(q^{2-s}\right)^{k_p}\right)\left(q^{1-s}\right)^{k_{s+1}}\prod_{t=s+2}^{2}\left(q^{3-t}\right)^{k_t} q^r\right)} \tag{2}$$

Proof. In order to find linear codes of length n and type (k_1,k_2) over R_q, we construct their generator matrices. First, we choose k_1 linearly independent elements of order q^2 and k_2

linearly independent elements of order q from R_q^n and then we construct a generating set whose elements are linearly independent of type (k_1, k_2).

We choose the first element of order q^2 in $q^{2n} - q^n$ different ways since q^n gives the elements whose order is not q^2. The second element is chosen in $q^{2n} - q^n.q$ different ways. By continuing in the same way, we choose k_1 linearly independent elements of order q^2 in

$$\left(q^{2n} - q^n\right)\left(q^{2n} - q^n.q\right)\ldots\left(q^{2n} - q^n q^{k_1-1}\right) \tag{3}$$

different ways. We first choose k_2 linearly independent elements of order q. We do the first choice in $q^n - q^{k_1}$ different ways since q^{k_1} gives the number of elements whose order is less than q. Continuing in the same way, we obtain k_2 linearly independent elements of order q as

$$\left(q^n - q^{k_1}\right)\left(q^n - q^{k_1+1}\right)\ldots\left(q^n - q^{k_1+k_2-1}\right) \tag{4}$$

By multiplying (3) and (4), the first part of the proof follows:

$$\left(q^{2n} - q^n\right)\left(q^{2n} - q^n.q\right)\ldots\left(q^{2n} - q^n q^{k_1-1}\right)\left(q^n - q^{k_1}\right)\left(q^n - q^{k_1+1}\right)\ldots\left(q^n - q^{k_1+k_2-1}\right) \tag{5}$$

Now, we construct a linearly independent generating set in a similar way we did in the first part of the proof. Here, the number of elements in which we do the choice is $q^{2k_1+k_2}$. Hence, similarly, we write the number of k_1 linearly independent elements of order q^2 and k_2 linearly independent elements of order q as

$$\begin{aligned}&\left(q^{2k_1+k_2} - q^{k_1+k_2}\right)\left(q^{2k_1+k_2} - q^{k_1+k_2+1}\right)\ldots\left(q^{2k_1+k_2} - q^{k_1+k_2+k_1-1}\right)\times\\ &\left(q^{k_1+k_2} - q^{k_1}\right)\left(q^{k_1+k_2} - q^{k_1+1}\right)\ldots\left(q^{k_1+k_2} - q^{k_1+k_2-1}\right).\end{aligned} \tag{6}$$

We take (5) as the numerator and (6) as the denominator, and then the result gives the number.

Corollary 5. The number of distinct (although not necessarily inequivalent) $[n,(k_1,k_2)]-$ codes over $R_2 = F_2 + uF_2$ is

$$N_{k_1,k_2}^{R_2} = \begin{bmatrix} n \\ k_1, k_2 \end{bmatrix} = \frac{\prod_{i=0}^{k_1-1}\left(4^n - 2^{n+i}\right)\prod_{j=0}^{k_2-1}\left(2^n - 2^{k_1+j}\right)}{\prod_{t=0}^{k_1-1}\left(4^{k_1}2^{k_2} - 2^{k_1+k_2+t}\right)\prod_{l=0}^{k_2-1}\left(2^{k_1}2^{k_2} - 2^{k_1+l}\right)}. \tag{7}$$

Corollary 6. The number of distinct (although not necessarily inequivalent) $[n,(k_1,k_2)]-$ codes over $R_4 = F_4 + uF_4$ is

$$N_{k_1,k_2}^{R_4}(n) = \begin{bmatrix} n \\ k_1, k_2 \end{bmatrix}_{R_4} = \frac{\prod_{i=0}^{k_1-1}\left(16^n - 4^{n+i}\right)\prod_{j=0}^{k_2-1}\left(4^n - 4^{k_1+j}\right)}{\prod_{t=0}^{k_1-1}\left(16^{k_1}4^{k_2} - 4^{k_1+k_2+t}\right)\prod_{l=0}^{k_2-1}\left(4^{k_1}4^{k_2} - 4^{k_1+l}\right)}. \tag{8}$$

Note: If $k_1 = 0$ and q is a prime, then we obtain Gaussian coefficient $\begin{bmatrix} n \\ k_2 \end{bmatrix}_R$.

Example 7. We calculate the number of distinct $\left[2,(1,1)\right]-$codes over $R_4 = F_4 + uF_4$. From (8),

$$N_{1,1}^{R_4}(2) = \frac{\left(16^2 - 4^2\right)\left(4^2 - 4\right)}{\left(16.4 - 4.4\right)\left(4.4 - 4\right)} = 5 \tag{9}$$

distinct $\left[2,(1,1)\right]-$codes over R_4.

Indeed, these codes are given by the following generator matrices:

$$\begin{bmatrix} 1 & 0 \\ 0 & u \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & u \end{bmatrix}, \begin{bmatrix} 1 & w \\ 0 & u \end{bmatrix}, \begin{bmatrix} 1 & \hat{w} \\ 0 & u \end{bmatrix}, \begin{bmatrix} u & 0 \\ 0 & 1 \end{bmatrix}$$

where w and $\hat{w}$ are the elements of R_4.

3. APPLICATIONS

3.1. Properties of $N_{k_1,k_2}^{R_q}$

Similar to Gaussian coefficient, some properties for Generalized Gaussian Numbers (similar results are given for Generalized Gaussian Numbers in Theorem 6 of [14]) are presented in this section where $q = 4$.

Theorem 8. Let n be a positive integer. $R_4 = F_4 + uF_4$, $\left(k, k_1, k_2 \le n\right)$. The numbers $N_{k_1,k_2}^{R_4}(n)$ satisfy the properties given in [14]:

1. $k_1 + k_2 \le n$:

i. $$\begin{bmatrix} n \\ k_1, k_2 \end{bmatrix}_{R_4} = \begin{bmatrix} n \\ n-\left(k_1+k_2\right), k_2 \end{bmatrix}_{R_4},$$

ii. Define $\begin{bmatrix} n \\ 0,0 \end{bmatrix}_{R_4} = 1$ then

$$\begin{bmatrix} n \\ k_1, 0 \end{bmatrix}_{R_4} = \begin{bmatrix} n \\ n-k_1, 0 \end{bmatrix}_{R_4} \quad \begin{bmatrix} n \\ 0, k_2 \end{bmatrix}_{R_4} = \begin{bmatrix} n \\ 0, n-k_2 \end{bmatrix}_{R_4}.$$

2. $k_1 + k_2 = n$, then $\begin{bmatrix} n \\ k_1, k_2 \end{bmatrix}_{R_4} = \begin{bmatrix} n \\ k_2, k_1 \end{bmatrix}_{R_4}$.

3. $\begin{bmatrix} n \\ 0, n \end{bmatrix}_{R_4} = \begin{bmatrix} n \\ n, 0 \end{bmatrix}_{R_4}$.

4. $k \le n$, $k = 1,2,\ldots,n$, then $\begin{bmatrix} n+1 \\ n-(k-1), k \end{bmatrix}_{R_4} = 2^k \begin{bmatrix} n \\ n-k, k \end{bmatrix}_{R_4} + \begin{bmatrix} n \\ n-(k-1), k-1 \end{bmatrix}_{R_4}$.

Proof. The proof follows by applying the definitions.

3.2. Some New and Existing Sequences

Here, we list the number of some linear codes over $R4$ which give us some number sequences. Some of these sequences are new which do not exist in the literature and some of them are existing sequences [12].

Table 1: The number of codes of given type and length

(k_1,k_2)	**n**	**Number**	(k_1,k_2)	**n**	**Number**	(k_1,k_2)	**n**	**Number**
(0,1)	1	1	(1,0)	1	1	(2,1)	3	21
	2	5		2	20		4	28560
	3	21		3	336		5	31164672
	4	85		4	5440		6	32411258880
	5	341		5	87296		7	
	6	1365		6	1397760		8	
	7	5461		7	22368256			
	8	21845		8	358158480			
(k_1,k_2)	**n**	**Number**	(k_1,k_2)	**n**	**Number**	(k_1,k_2)	**n**	**Number**
(1,1)	2	5	(1,2)	3	21	(2,2)	4	357
	3	420		4	7140		5	973896
	4	28560		5	1947792		6	8507955456
	5	1855040		6	59579520		7	
	6	119159040						

Table 2: Some new and existing sequences

$a_n^{0,1}$	Existing sequence (A002450)	$a_n^{1,2}$	New sequence
$a_n^{0,2}$	Existing sequence (A006105)	$a_n^{1,3}$	New sequence
$a_n^{0,3}$	Existing sequence (A006106)	$a_n^{2,0}$	New sequence
$a_n^{1,0}$	Existing sequence (A166984)	$a_n^{2,1}$	New sequence
$a_n^{1,1}$	New sequence	$a_n^{2,2}$	New sequence

These sequences are compared to Sloane's list [12]. Some of them exist and some are new. The sequences $\mathbf{a_n^{0,2}}$ (A006105) and $\mathbf{a_n^{0,3}}$ (A006106) given in Table 2 give the Gaussian coefficient $\left|G_{R_4}(n,2)\right|$ and $\left|G_{R_4}(n,3)\right|$, respectively.

4. CONCLUSION

In this paper, we have developed and proved a direct formula for the number of linear codes over the ring $F_q + uF_q$. We also obtained some new interesting number sequences. Further research on this topic would be studying the number of linear codes over different finite rings. Also, studying the properties of generalized Gaussian numbers is an interesting topic to be explored further.

REFERENCES

[1] T. Abualrub and I. Siap, pp. 520-529, Constacyclic codes over F2+uF2, Journal of The Franklin Institute, **346**, (2009)

[2] G. Calugareanu, pp. 157-167, The total number of subgroups of a finite Abelian group, Scientiae Mathematicae Japonicae **60**, No.1 (2004)

[3] S. Delsarte, pp. 600-609, Fonctions de Möbius sur les groupes abeliens finis, Annals of Math. **49**, (1948)

[4] P.E. Djubjuk, pp. 351-378, On the number of subgroups of a finite abelian group, Izv. Akad. Nauk SSSR Ser. Mat. **12**, (1948)

[5] T. Honold and I. Landjev, Linear codes over finite chain rings, The Electronic Journal of Combinatorics **7**, (2000)

[6] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Sole, The ℤ4-Linearity of Kerdock, Preparata, Goethals, and Related Codes, IEEE Transactions on Information Theory, **40**, (1994).

[7] S. Ling, P. Sole, pp. 983-997, Type II Codes Over F4 +uF4, European Journal of Combinatorics, 22, (2001)

[8] F.J. MacWilliams, N.J.A Sloane, The Theory Of Error Correcting Codes, North-Holland Pub. Co., (1977)

[9] B.R. McDonald, Finite Rings with Identity, Pure and Applied Mathematics, Marcel Dekker, (1974).

[10] M. Ozen and I. Siap, pp. 17-29, Linear codes over Fq[u]=(us) with respect to the Rosenbloom-Tsfasman metric, Designs Codes and Cryptography, 38, (2006)

[11] J.F. Qian, L.N. Zhang, S.X. Zhu, pp. 820-823, (1+u)-Constacyclic and cyclic codes over F2+uF2, Applied Mathematics Letters, 19, (2006)

[12] N. J. Sloane A, On-Line Encyclopaedia of Integer Sequences, Published electronically at http://www.research.att.com/njas/sequences.

[13] E. Salturk, I. Siap, pp. 250-259, Generalized Gaussian Numbers Related to Linear Codes over Galois Rings, European Journal of Pure and Applied Mathematics, 5, (2012)

[14] I. Siap, Linear Codes over F2+uF2 and Their Complete Weight Enumerators, OSU Dijen Conference, Codes and Designs, Ohio State Unv. Math. Res. Inst. Publ. 10, Walter de Gruyter, (2002)

[15] Y. Yeh, pp. 323 – 327, On prime power abelian groups. Bull. AMS, 54, (1948)