International Journal of Mathematics and
Computer Science, **19**(2024), no. 4, 1111–1115

Counting Free Linear Codes with a Given Number of Standard Basis Vectors over Finite Commutative Rings

Patipat Chumket[1], **Siripong Sirisuk**[2]

[1]Department of Mathematics
Faculty of Science Technology and Agriculture
Yala Rajabhat University
Yala 95000, Thailand

[2]Department of Mathematics and Statistics
Faculty of Science and Technology
Thammasat University
Pathum Thani 12120, Thailand

email: patipat.c@yru.ac.th, siripong.srs@gmail.com

(Received March 2, 2024, Accepted April 13, 2024,
Published June 1, 2024)

Abstract

In this article, we present the number of free linear codes over any finite commutative ring which have a given rank and a given number of standard basis vectors.

1 Introduction

Enumeration problems concerning linear codes over finite fields have been extensively studied. A classic formula for the number of r-dimensional linear codes of length n over $\mathbb{F}_q$ is given by $\left[\begin{smallmatrix} n \\ r \end{smallmatrix}\right]_q = \prod_{i=0}^{r-1} \frac{q^n-q^i}{q^r-q^i}$, known as the Gaussian coefficient (see [9] for the proof). The code alphabets are usually elements in fields; however, in many important situations, the alphabets are elements in commutative rings where the properties of commutative rings

Key words and phrases: Free linear code, standard basis vector, local ring.
The corresponding author is Siripong Sirisuk.
AMS (MOS) Subject Classifications: 15A03, 94B05, 13A05.
ISSN 1814-0432, 2024, http://ijmcs.future-in-tech.net

can affect the structure of the codes. Therefore, codes over commutative rings have been continuously explored [2, 3, 8].

Abdel-Ghaffar [1] presented the number of linear codes with a specified number of standard basis vectors over finite fields. Certainly, standard basis vectors are often used to define the code's structure and properties. This result over finite fields was later generalized to the number of free linear codes over some finite commutative rings, specifically commutative local rings [7]. In this paper, we complete the study of free linear codes with prescribed standard basis vectors over arbitrary finite commutative ring.

This paper is organized as follows: Section 2 is devoted to some definitions and properties of finite commutative rings and linear codes over finite commutative rings. In Section 3, we analyze the number of free linear codes with a given number of standard basis vectors over a finite commutative ring.

2 Preliminaries

Let R be a finite commutative ring. The set of units in R is denoted by $R^\times$. If R is a field, then $R^\times = R \setminus \{0\}$. A *local ring* is a ring with a unique maximal ideal. A field is a commutative local ring with a unique maximal ideal $\{0\}$. If R is a commutative local ring with maximal ideal M, then the *quotient ring* R/M is a field called the *residue field*; moreover, $R^\times = R \setminus M$. It is well known that a finite commutative ring R can be decomposed as $R = R_1 \times R_2 \times \cdots \times R_h$, where R_α is a finite local ring for all α. The ring R is always equipped with a class of projections $\rho_\alpha \colon R \to R_\alpha$ for each $\alpha \in \{1, 2, \ldots, h\}$ such that $x = (\rho_1(x), \rho_2(x), \ldots, \rho_h(x))$ for $x \in R$. Furthermore, $R^\times = R_1^\times \times R_2^\times \times \cdots \times R_h^\times$. For more information on commutative rings, see [5].

A *free linear code* of R^n over R is a free submodule of the R module R^n; i.e., a submodule with a basis. The number of vectors on a basis of a free linear code X is called the *rank of* X. If R is a field, then free linear codes coincide with subspaces and the rank of a free linear codes is its dimension. Note that the R module R^n possesses a basis $\{\vec{e_1}, \vec{e_2}, \ldots, \vec{e_n}\}$, where $\vec{e_i} = (e_{i1}, e_{i2}, \ldots, e_{in}) \in R^n$, where $e_{ii} = 1$ and $e_{ij} = 0$ for all $i \neq j$. We therefore call $\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n$ the *standard basis vectors*. The number of r-dimensional linear codes of $\mathbb{F}_q^n$ of is given by $\left[{n \atop r} \right]_q = \prod_{i=0}^{r-1} \frac{q^n - q^i}{q^r - q^i}$. We call $\left[{n \atop r} \right]_q$ the *Gaussian coefficient*. Moreover, we can prove that $\left[{n \atop r} \right]_q = \left[{n \atop n-r} \right]_q$. This number of linear cods of $\mathbb{F}_q^n$ is generalized to the case over finite commutative rings as follows:

Lemma 2.1. *[6] Let R be a finite commutative ring decomposed as $R =$*

$R_1 \times R_2 \times \cdots \times R_h$, where R_α is a finite local ring with maximal ideal M_α and residue field of order q_α for all α.

1. *X is a free linear code of R^n of rank r if and only if $\rho_\alpha(X)$ is a free linear code of R_α^n of rank r for all $\alpha \in \{1, 2, \ldots, h\}$.*
2. *The number of free linear codes of R^n of rank r is $\prod_{\alpha=1}^{h} |M_\alpha|^{nr-r^2} \left[{n \atop r} \right]_{q_\alpha}$.*

3 Main results

In this section, we present the number of free linear codes of R^n with a given number of standard basis vectors when R is an arbitrary finite commutative ring. We need some lemmas.

Lemma 3.1. *[7] Let R be a finite commutative local ring with maximal ideal M, residue field of order q, and natural map $\pi \colon R \to R/M$ given by $r \mapsto r + M$. Suppose that $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$ is a set of indices of size k.*

1. *If X is a free linear code of R^n of rank r containing standard basis vectors $\vec{e}_{i_1}, \vec{e}_{i_2}, \ldots, \vec{e}_{i_k}$, then $\pi(X)$ is a linear code of $(R/M)^n$ of dimension r containing standard basis vectors $\vec{e}_{i_1}, \vec{e}_{i_2}, \ldots, \vec{e}_{i_k}$.*
2. *Any linear code of $(R/M)^n$ of dimension r containing standard basis vectors $\vec{e}_{i_1}, \vec{e}_{i_2}, \ldots, \vec{e}_{i_k}$ can be lifted to $|M|^{(n-r)(r-k)}$ free linear codes of R^n of rank r containing standard basis vectors $\vec{e}_{i_1}, \vec{e}_{i_2}, \ldots, \vec{e}_{i_k}$.*
3. *The number of free linear codes of R^n of rank r containing standard basis vectors $\vec{e}_{i_1}, \vec{e}_{i_2}, \ldots, \vec{e}_{i_k}$ is given by $|M|^{(n-r)(r-k)} \left[{n-k \atop n-r} \right]_q$.*

Lemma 3.2. *Let R be a finite commutative ring decomposed as $R = R_1 \times R_2 \times \cdots \times R_h$, where R_α is a finite local ring with maximal ideal M_α and residue field of order q_α. Suppose that $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$ is a set of indices of size k.*

1. *A free linear code X of R^n of rank r contains standard basis vectors $\vec{e}_{i_1}, \vec{e}_{i_2}, \ldots, \vec{e}_{i_k}$ if and only if a free linear code $\rho_\alpha(X)$ of R_α^n of rank r contains $\vec{e}_{i_1}, \vec{e}_{i_2}, \ldots, \vec{e}_{i_k}$ for all $\alpha \in \{1, 2 \ldots, h\}$.*
2. *The number of free linear codes of R^n of rank r containing standard basis vectors $\vec{e}_{i_1}, \vec{e}_{i_2}, \ldots, \vec{e}_{i_k}$ is given by*

$$\prod_{\alpha=1}^{h} |M_\alpha|^{(n-r)(r-k)} \begin{bmatrix} n-k \\ n-r \end{bmatrix}_{q_\alpha}.$$

Proof. (1) Lemma 2.1 implies that X is a free linear code of R^n of rank r if and only if $\rho_\alpha(X)$ is a free linear code of R_α^n of rank r for all $\alpha \in \{1, 2, \ldots, h\}$. For a standard basis vector $\vec{e}_i \in R^n$, we have $\vec{e}_i = (\rho_1(\vec{e}_i), \rho_2(\vec{e}_2), \ldots, \rho_h(\vec{e}_i))$. Thus, a free linear code X contains standard basis vectors $\vec{e}_{i_1}, \vec{e}_{i_2}, \ldots, \vec{e}_{i_k}$ in R^n if and only if a free linear code $\rho_\alpha(X)$ of R_α^n contains $\vec{e}_{i_1}, \vec{e}_{i_2}, \ldots, \vec{e}_{i_k}$ in R_α^n for all $\alpha \in \{1, 2 \ldots, h\}$.

(2) For $R = R_1 \times R_2 \times \cdots \times R_h$ where R_α is a finite local ring, Lemma 3.1 implies that the number of free linear codes of R_α^n containing $\vec{e}_{i_1}, \vec{e}_{i_2}, \ldots, \vec{e}_{i_k}$ is given by $|M_\alpha|^{(n-r)(r-k)} \left[{n-k \atop n-r} \right]_{q_\alpha}$ for any $\alpha \in \{1, 2, \ldots, h\}$. By (1), the number of free linear codes of R^n of rank r containing standard basis vectors $\vec{e}_{i_1}, \vec{e}_{i_2}, \ldots, \vec{e}_{i_k}$ is given by $\prod_{\alpha=1}^h |M_\alpha|^{(n-r)(r-k)} \left[{n-k \atop n-r} \right]_{q_\alpha}$. □

The previous lemma provides the number of free linear codes of R^n containing the given k standard basis vectors. These codes may contain additional standard basis vectors. To obtain the number of free linear codes of R^n of rank r containing exactly k arbitrary standard basis vectors, we finally apply the Inclusion-Exclusion principle [4] and obtain the desired number in the following main theorem.

Theorem 3.3. *Let R be a finite commutative ring decomposed as $R = R_1 \times R_2 \times \cdots \times R_h$, where R_α is a finite local ring with maximal ideal M_α and residue field of order q_α. Then the number of free linear codes of R^n of rank r containing exactly k standard basis vectors is equal to*

$$\sum_{i=k}^{r} \left((-1)^{i-k} \binom{i}{k} \binom{n}{i} \left(\prod_{\alpha=1}^{h} |M_\alpha|^{(n-r)(r-i)} \begin{bmatrix} n-i \\ n-r \end{bmatrix}_{q_\alpha} \right) \right).$$

Proof. For any set $\mathcal{I} \subseteq \{1, 2, \ldots, n\}$ of indices, we let $D_{\mathcal{I}}$ be the number of free linear codes of R^n of rank r containing the standard basis vectors $\vec{e}_i$ for all $i \in \mathcal{I}$. By the Inclusion-Exclusion principle [4], the number of free linear codes of R^n of rank r containing exactly k standard basis vectors is described by

$$\sum_{i=k}^{m} \left((-1)^{i-k} \binom{i}{k} \sum_{\mathcal{I} \subseteq \{1,2,\ldots,n\}, |\mathcal{I}|=i} D_{\mathcal{I}} \right).$$

Note that we have $\binom{n}{i}$ such sets $\mathcal{I}$ of size i. Lemma 3.2 shows that if $\mathcal{I}$ is of size i, then

$$D_{\mathcal{I}} = \left(\prod_{\alpha=1}^{h} |M_\alpha|^{(n-r)(r-i)} \begin{bmatrix} n-i \\ n-r \end{bmatrix}_{q_\alpha} \right).$$

The number of free linear codes of R^n of rank r containing exactly k standard basis vectors is therefore given by

$$\sum_{i=k}^{r}\left((-1)^{i-k}\binom{i}{k}\binom{n}{i}\left(\prod_{\alpha=1}^{h}|M_\alpha|^{(n-r)(r-i)}\begin{bmatrix}n-i\\ n-r\end{bmatrix}_{q_\alpha}\right)\right),$$

as desired. □

Acknowledgment. This study was supported by Thammasat University Research Fund, Contract No. TUFT 27/2565.

References

[1] K. Abdel-Ghaffar, Counting matrices over finite fields having a given number of rows of unit weight, Linear Algebra Appl., **436**, (2012), 2665–2669.

[2] S.T. Dougherty, Algebraic Coding Theory Over Finite Commutative Rings, SpringerBriefs in Mathematics, Springer, 2017.

[3] S.T. Dougherty, E. Saltürk, Counting codes over rings, Des. Codes Cryptogr., **73**, (2014), 151–165.

[4] M. Hall Jr., Combinatorial Theory, Second Edition, Wiley, NY, 1986.

[5] N.H. McCoy, Rings and ideals, Carus Math. Monogr. No. 8, Mathematical Association of America, 1948.

[6] S. Sirisuk, Y. Meemark, Generalized symplectic graphs and generalized orthogonal graphs over finite commutative rings, Linear Multilinear Algebra, **67,** (2019), 2427–2450.

[7] S. Sirisuk, Enumeration of some matrices and free linear codes over commutative finite local rings, Special Matrices, **10**, (2022), 109–116.

[8] P. Solé, Codes over Rings, Series on Coding Theory and Cryptology: Vol. 6, World Scientific Publishing Co., Singapore, 2009.

[9] Z. Wan, Geometry of classical groups over finite fields, Second Edition, Science Press, New York/Beijing, 2002.