กราฟซิมเพล็กติกวางนัยทั่วไปและกราฟเชิงตั้งฉากวางนัยทั่วไปเหนือริงสลับที่จำกัด

นายสิริพงศ์ ศิริสุข

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรดุษฎีบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2561

GENERALIZED SYMPLECTIC GRAPHS AND GENERALIZED ORTHOGONAL GRAPHS OVER FINITE COMMUTATIVE RINGS

Mr. Siripong Sirisuk

A Dissertation Submitted in Partial Fulfillment of the Requirements
for the Degree of Doctoral of Science Program in Mathematics
Department of Mathematics and Computer Science
Faculty of Science
Chulalongkorn University
Academic Year 2018

Thesis Title	GENERALIZED SYMPLECTIC GRAPHS AND GENERALIZED ORTHOGONAL GRAPHS OVER FINITE COMMUTATIVE RINGS
By	Mr. Siripong Sirisuk
Field of Study	Mathematics
Thesis Advisor	Professor Yotsanan Meemark, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Doctoral's Degree

.... Dean of the Faculty of Science

(Professor Polkit Sangvanich, Ph.D.)

THESIS COMMITTEE

.... Chairman

(Professor Patanee Udomkavanich, Ph.D.)

.... Thesis Advisor

(Professor Yotsanan Meemark, Ph.D.)

.... Examiner

(Associate Professor Tuangrat Chaichana, Ph.D.)

.... Examiner

(Assistant Professor Sajee Pianskool, Ph.D.)

.... External Examiner

(Associate Professor Utsanee Leerawat, Ph.D.)

สิริพงศ์ ศิริสุข : กราฟซิมเพล็กติกวางนัยทั่วไปและกราฟเชิงตั้งฉากวางนัยทั่วไปเหนือริงสลับที่จำกัด. (GENERALIZED SYMPLECTIC GRAPHS AND GENERALIZED ORTHOGONAL GRAPHS OVER FINITE COMMUTATIVE RINGS) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ศ.ดร.ยศนันต์ มีมาก, 48 หน้า.

ให้ R เป็นริงสลับที่จำกัดที่มีเอกลักษณ์ n เป็นจำนวนนับ และ β เป็นรูปแบบเชิงเส้นคู่บน R^n ในดุษฎีนิพนธ์ฉบับนี้ เรานับจำนวนมอดูลย่อยเสรีและมอดูลย่อยเสรีไอโซทรอปิกทุกส่วนของ R^n ที่มีแรงก์เป็น s โดยใช้แนวคิดการยกขึ้น เรานิยามกราฟรูปแบบเชิงเส้นคู่วางนัยทั่วไปให้มีเซตของจุดยอดเป็นเซตของมอดูลย่อยเสรีไอโซทรอปิกทุกส่วนของ R^n ที่มีแรงก์เป็น s และการประชิดกันของจุดยอดกำหนดโดยเงื่อนไขบนแรงก์ เราศึกษากราฟนี้เมื่อ (R^n, β) เป็นปริภูมิซิมเพล็กติกและปริภูมิเชิงตั้งฉาก และสามารถระบุดีกรีของแต่ละจุดยอดของกราฟนี้ได้ ถ้า R เป็นริงเฉพาะที่จำกัดเราแสดงได้ว่ากราฟนี้เป็นกราฟถ่ายทอดส่วนโค้งและหากรุปอัตสัณฐานของกราฟได้ด้วย ในท้ายที่สุดเราสามารถแยกกราฟนี้เหนือริงสลับที่จำกัดเป็นผลคูณเทนเซอร์ของกราฟเหนือริงเฉพาะที่จำกัด

ภาควิชา	คณิตศาสตร์และวิทยาการคอมพิวเตอร์	ลายมือชื่อนิสิต	....
สาขาวิชา	คณิตศาสตร์	ลายมือชื่อ อ.ที่ปรึกษาหลัก	....
ปีการศึกษา	2561		

5872830523 : MAJOR MATHEMATICS
KEYWORDS : GENERALIZED BILINEAR FORM GRAPH/ LOCAL RING/ ORTHOGONAL GRAPH/ SYMPLECTIC GRAPH

SIRIPONG SIRISUK : GENERALIZED SYMPLECTIC GRAPHS AND GENERALIZED ORTHOGONAL GRAPHS OVER FINITE COMMUTATIVE RINGS. ADVISOR: PROF. YOTSANAN MEEMARK, Ph.D., 48 pp.

Let R be a finite commutative ring with identity, $n \in \mathbb{N}$ and β a bilinear form on R^n. In this dissertation, we count the numbers of free submodules and totally isotropic free submodules of R^n of rank s by using the lifting idea. We define the *generalized bilinear form graph* whose vertex set is the set of totally isotropic free submodules of R^n of rank s and the adjacency condition is given by some rank conditions. We study this graph when (R^n, β) is a symplectic space and an orthogonal space. We can determine the degree of each vertex of these graphs. If R is a finite local ring, we show that these graphs are arc transitive and obtain their automorphism groups. Finally, we prove that we can decompose the graphs over a finite commutative ring into the tensor products of graphs over finite local rings.

Department:	Mathematics and Computer Science	Student's Signature ....
Field of Study:	Mathematics	Advisor's Signature ....
Academic Year:	2018	

ACKNOWLEDGEMENTS

Firstly, I express my deepest gratitude to my supervisor, Professor Dr. Yotsanan Meemark. His suggestions, advice and guidance are extremely invaluable. He coached me during the creation of this dissertation. Furthermore, he made me more confident in doing research. Next, I am sincerely grateful to Professor Dr. Patanee Udomkavanich, Associate Professor Dr. Tuangrat Chaichana, Assistant Professor Dr. Sajee Pianskool and Associate Professor Dr. Utsanee Leerawat, my thesis committee, for their worthy suggestions and comments.

As well, I am indebted to all of my teachers who have taught me and gave me lessons and skills. Another, I would also like to thank the staff of the Department of Mathematics and Computer Science of Chulalongkorn University for being hospitable. Also, I feel very thankful to all my friends for all the moral support. Moreover, I would like to thank the Science Achievement Scholarship of Thailand (SAST) for financial support during my graduate study.

Last but not least, much appreciation is due to my family-thank you for your love, trust and support.

CONTENTS

	Page
THAI ABSTRACT	iv
ENGLISH ABSTRACT	v
ACKNOWLEDGEMENTS	vi
CONTENTS	vii
CHAPTER I Generalized Bilinear Form Graphs	1
1.1 Finite Commutative Rings	2
1.2 Free Modules	3
1.3 Unimodular Vectors	5
1.4 Rank of Matrices over Commutative Rings	8
1.5 Free Submodules	11
1.6 Bilinear Forms	15
1.7 Graphs	17
1.8 Generalized Bilinear Form Graphs	19
CHAPTER II Generalized Symplectic Graphs	23
2.1 Over Finite Fields	23
2.2 Over Finite Local Rings	26
2.3 Over Finite Commutative Rings	33
CHAPTER III Generalized Orthogonal Graphs	38
3.1 Over Finite Fields	39
3.2 Over Finite Local Rings	40
3.3 Over Finite Commutative Rings	45
REFERENCES	46
VITA	48

CHAPTER I

GENERALIZED BILINEAR FORM GRAPHS

Graphs arising from bilinear forms have been variously studied. The most favorite such graphs are symplectic graphs and orthogonal graphs which have been famously explored in several directions. In this chapter, we present a new class of graphs arising from bilinear forms which will be called *Generalized bilinear form graphs over finite commutative rings*. In order to understand the background of becoming these graphs and their characters deeply, we first introduce all terminologies regarding our graphs. The literature review and the definition of our graphs are presented in the end of this chapter.

As we have known, a graph basically consists of vertices and edges acquired by an adjacency condition. As well, our graphs are studied on free modules over finite commutative rings. The properties of finite commutative rings and free modules are introduced in Sections 1.1 and 1.2, respectively. Next, we exhibit the concept of unimodular vectors in Section 1.3. Indeed, unimodular vectors are concerned in both symplectic graphs and orthogonal graphs. After that, Section 1.4 reveals the notion of rank of matrices over commutative rings which is the key for defining the adjacency condition of our graphs. By design, the vertices of our graphs are made up of certain free submodules. The basic features of free submodules are studied in Section 1.5. Afterwards, Section 1.6 is devoted to bilinear forms which play outstanding roles in our graphs. We introduce the concept of bilinear forms over commutative rings and illustrate some kinds of bilinear forms. Necessarily, Section 1.7 is aimed at writing down the general definitions of graphs. After all things discussed, we give the history of graphs arising from bilinear forms running from the start toward becoming generalized bilinear form graphs in the final section of this chapter.

1.1 Finite Commutative Rings

In this section, we review the information of finite commutative rings. For basic definition, notation and properties, the reader is referred to [1], [8] and [12]. Throughout this dissertation, our rings always contain the identity $1 \neq 0$.

Let R be a ring. An element a in R is a **unit** if there exists an element $b \in R$ such that $ab = 1 = ba$, a is a **zero divisor** if a is non-zero and there exists an element $0 \neq b \in R$ such that $ab = 0 = ba$, and, a is **nilpotent** if there exists a positive integer n such that $a^n = 0$. It is easy to see that the set of units of R form a group under multiplication, called the **group of units** of R and denoted by $R^\times$.

An **ideal** I of a ring R is a nonempty subset of R such that $a - b$, ra and ar are in I for all $a, b \in I$ and $r \in R$. An ideal M of a ring R is **maximal** if $M \neq R$ and for every ideal J of R, if $M \subseteq J \subseteq R$, then $J = M$ or $J = R$. Actually, a ring may own many maximal ideals. However, rings owning a unique maximal ideal are the core of studying finite commutative rings.

A **local ring** R is a commutative ring which has a unique maximal ideal, its unique maximal ideal M is $R \smallsetminus R^\times$, and we call the field R/M the **residue field** of R. This local ring is also equipped with the canonical map $\pi : R \to R/M$ given by $\pi(r) = r + M$ for all $r \in R$.

Example 1.1.1.

1. Every field is a local ring with maximal ideal $\{0\}$.
2. $\mathbb{Z}_{p^t}$ is a local ring with maximal ideal $p\mathbb{Z}_{p^t}$ and residue field $k = \mathbb{Z}_{p^t}/p\mathbb{Z}_{p^t} \cong \mathbb{Z}_p$ for every prime p and $t \in \mathbb{N}$.
3. $\mathbb{Z}$ is not a local ring since it has infinitely many maximal ideals of the form $p\mathbb{Z}$ where p is a prime.

Proposition 1.1.2. [1] *In a finite local ring, every element is either a unit or a nilpotent element.*

This implies that if M is a maximal ideal of a finite local ring R, then $M^t = \{0\}$ for some $t \in \mathbb{N}$.

Next, let R be a finite commutative ring. It is well known that R is isomorphic to a product of finite local rings. More precisely,

$$R \cong R_1 \times R_2 \times \cdots \times R_\ell$$

where $R_1, R_2, \ldots, R_\ell$ are finite local rings with maximal ideals $M_1, M_2, \ldots, M_\ell$, respectively. We also have the projection map $\rho_j : r = (s_1, s_2, \ldots, s_\ell) \mapsto s_j$ for all $j \in \{1, 2, \ldots, \ell\}$.

It follows immediately that

$$R^\times \cong R_1^\times \times R_2^\times \times \cdots \times R_\ell^\times.$$

Moreover, if I is an ideal of R, then $I \cong \rho_1(I) \times \rho_2(I) \times \cdots \times \rho_\ell(I)$ where $\rho_j(I)$ is an associate ideal of R_j for all $j \in \{1, 2, \ldots, \ell\}$.

Proposition 1.1.3. [1] *In a finite commutative ring, every nonzero element is either a unit or a zero divisor.*

Example 1.1.4. Let $n = p_1^{t_1} p_2^{t_2} \ldots p_\ell^{t_\ell}$ where p_j is a prime and $t_j \in \mathbb{N}$ for all $j \in \{1, 2, \ldots, \ell\}$. Then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{t_1}} \times \mathbb{Z}_{p_2^{t_2}} \times \cdots \times \mathbb{Z}_{p_\ell^{t_\ell}},$$

where $\mathbb{Z}_{p_j^{t_j}}$ is a finite local ring with unique maximal ideal $p_j \mathbb{Z}_{p_j^{t_j}}$ and residue field $k_j = \mathbb{Z}_{p_j}$ for all $j \in \{1, 2, \ldots, \ell\}$.

1.2 Free Modules

The concept of modules is known as a generalization of vector spaces. The definition of modules is similar to that of vector spaces. Unlike vector spaces, the scalars of modules are in rings.

Let R be a ring with identity 1_R. An R**-module** or a **module over** R is an abelian group $(V, +)$ with a scalar multiplication $R \times V \to V$, denoted by $r\vec{x}$, the image of $(r, \vec{x})$, which satisfies for all $r, s \in R$ and $\vec{x}, \vec{y} \in V$,

1. $r(\vec{x}+\vec{y}) = r\vec{x} + r\vec{y}$,

2. $(r+s)\vec{x} = r\vec{x} + s\vec{x}$,

3. $r(s\vec{x}) = (rs)\vec{x}$ and

4. $1_R\vec{x} = \vec{x}$.

Example 1.2.1. 1. For a field F, an F-module is just a vector space over F.

2. Every abelian group is a $\mathbb{Z}$-module.

3. Every ring R is a module over itself where the addition and the scalar multiplication are given by ring operations of R.

4. Let R be a ring. Then $V = R^n$, a direct product of n copies of R, is an R-module under pointwise addition and scalar multiplication.

We provide some basic terminologies regarding modules in the following definitions.

Let R be a ring and V an R-module. A subset X of V is called a **submodule** of V if X is an additive subgroup of V and $r\vec{x} \in X$ for any $r \in R$ and $\vec{x} \in X$.

Example 1.2.2. 1. For a field F, all submodules of an F-module which is a vector space over F are the subspaces.

2. Since every abelian group V is a $\mathbb{Z}$-module, all subgroups of V are equivalent to submodules of the $\mathbb{Z}$-module V.

3. For an R-module V, it is easy to see that $R\vec{x}$ is a submodule of V where $\vec{x} \in V$.

Next, let V be an R module. We say V is **generated by** a subset $\{\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_n\}$ if it is the set

$$\{r_1\vec{x}_1 + r_2\vec{x}_2 + \cdots + r_n\vec{x}_n : r_1, r_2, \ldots, r_n \in R\}$$

and we write

$$V = R\vec{x}_1 + R\vec{x}_2 + \cdots + R\vec{x}_n.$$

A set $\{\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_n\}$ is said to be **linearly independent** if it is provided that for any $r_1, r_2, \ldots r_n \in R$, if $r_1\vec{x}_1 + r_2\vec{x}_2 + \cdots + r_n\vec{x}_n = \vec{0}$, then $r_1 = r_2 = \cdots = r_n = 0$. A set that is not linearly independent is said to be **linear dependent**.

If an R-module V is generated by a linearly independent set B, we say that V is a **free R-module** and that B is a **basis** of V.

Let V be a free R-module with basis $\{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$. It is easy to see that $V = R\vec{b}_1 \oplus R\vec{b}_2 \oplus \cdots \oplus R\vec{b}_n$, sometimes written as $V = \bigoplus_{i=1}^{n} R\vec{b}_i$. Besides, every element $\vec{x}$ in V can be written uniquely as a linear combination: $\vec{x} = r_1\vec{b}_1 + r_2\vec{b}_2 + \cdots + r_n\vec{b}_n$ where $r_i \in R$.

In case that R is a commutative ring, every free R-module owns a nice property on its bases.

Lemma 1.2.3. [8] *Let R be a commutative ring. Then every basis of a free R-module has the same cardinality.*

Thus, we call the cardinality of a basis of a free R-module V over a commutative ring R, the **rank** of V.

Example 1.2.4. Let R be a commutative ring. Then $V = R^n$ is a free R-module of rank n with a basis $\{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\}$ where $\vec{e}_i = (0, 0, \ldots, 1, \ldots, 0)$ (the 1 occurs only in the i-coordinate), for all i.

Additionally, Proposition 2.9 of [8] says that any two free R-modules over a commutative ring R with the same rank are isomorphic. Thus, V is a free R-module over a commutative ring R of rank n if and only if $V \cong R^n$. Therefore, we may assume $V = R^n$ for convenience to study free R-modules of rank n.

1.3 Unimodular Vectors

Unimodular vectors are importantly considered in symplectic graphs and orthogonal graphs over finite commutative rings, see [10], [13], [14], [15], and [17]. We show in this section that unimodular vectors over finite commutative rings are exactly linearly independent vectors.

Let R be a commutative ring. Let V be a free R-module of rank n with basis $\{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$. A vector $\vec{x}$ in V is **unimodular** if $\vec{x} = r_1\vec{b}_1 + r_2\vec{b}_2 + \cdots + r_n\vec{b}_n$ and the ideal generated by $r_1, r_2, \ldots, r_n$ is equal to R.

Example 1.3.1. 1. If R is a field, then every nonzero vector in V is unimodular.

2. Let $R = \mathbb{Z}_4$ and $V = \mathbb{Z}_4^4$. Then $(1, 2, 0, 3) \in V$ is unimodular since the ideal $\langle 1, 2, 0, 3\rangle = \mathbb{Z}_4$, but $(2, 0, 2, 0) \in V$ is not unimodular since $\langle 0, 2\rangle \neq \mathbb{Z}_4$.

The unimodularity of a vector is required in the graphs because of a nice relationship between a local ring and its residue field. In fact, for a local ring R with maximal ideal M and the canonical map $\pi : R \to R/M$, if $\vec{x}$ is a unimodular vector in an R-module R^n, then $\pi(x)$ is linearly independent over R/M. We next show that a unimodular vector is itself linearly independent.

Proposition 1.3.2. *Let R be a finite local ring with maximal ideal M. Let V be a free R-module of rank n with basis $\{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$ and $\vec{x} = r_1\vec{b}_1 + r_2\vec{b}_2 + \cdots + r_n\vec{b}_n$ in V for some $r_1, r_2, \ldots, r_n \in R$. Then the following statements are equivalent.*

(i) $\vec{x}$ is a unimodular vector.

(ii) r_i is a unit for some $i \in \{1, 2, \ldots, n\}$.

(iii) $\{\vec{x}\}$ is a linearly independent set.

Proof. (i) $\Rightarrow$ (ii). Assume that r_i is not a unit for all $i \in \{1, 2, \ldots, n\}$. Since R is a local ring, $r_i \in M$ for all $i \in \{1, 2, \ldots, n\}$. Thus, $(r_1, r_2, \ldots, r_n) \subseteq M$ and so $\vec{x}$ is not a unimodular vector.

(ii) $\Rightarrow$ (iii). Assume that r_i is a unit for some $i \in \{1, 2, \ldots, n\}$. Let $c \in R$ be such that $c\vec{x} = \vec{0}$. Then $cr_i = 0$. Since r_i is a unit, c must be 0 and so $\{\vec{x}\}$ is linearly independent.

(iii) $\Rightarrow$ (i). Assume that $\vec{x}$ is not a unimodular vector. Then the ideal $(r_1, r_2, \ldots, r_n) \neq R$. Since R is local, $(r_1, r_2, \ldots, r_n) \subseteq M$. If $M = \{0\}$, then R is a field and so $\vec{x} = \vec{0}$ and $\{\vec{x}\}$ is linearly dependent. Assume that $M \neq \{0\}$ and let $t \in \mathbb{N}$ be such that $M^t \neq \{0\}$ and $M^{t+1} = \{0\}$. This t exists because every element of a finite local ring is either a unit or a nilpotent element. Choose a nonzero element c in M^t. Then $cr_i \in M^{t+1} = \{0\}$ for all i. Hence, $c\vec{x} = \vec{0}$ and so $\{\vec{x}\}$ is linearly dependent. $\square$

Next, let R be a finite commutative ring decomposed as $R \cong R_1 \times R_2 \times \cdots \times R_\ell$ where R_j is a finite local ring with maximal ideal M_j and residue field $k_j = R_j/M_j$ for all $j \in \{1, 2, \ldots, \ell\}$. Recall the projection map $\rho_j : R \to R_j$ given by $\rho_j : r = (s_1, s_2, \ldots, s_\ell) \mapsto s_j$ for all $j \in \{1, 2, \ldots, \ell\}$.

Let V be a free R-module of rank n. For convenience, we may take $V = R^n$ and for each $\vec{x} = (r_1, r_2, \ldots, r_n)$ in V, we write

$$\rho_j(\vec{x}) = \big(\rho_j(r_1), \rho_j(r_2), \ldots, \rho_j(r_n)\big)$$

for all $j \in \{1, 2, \ldots, \ell\}$.

Observe that for each $j \in \{1, 2, \ldots, \ell\}$,

$$R_1 \times \cdots \times R_{j-1} \times M_j \times R_{j+1} \times \cdots \times R_\ell$$

is a maximal ideal of R and a maximal ideal of R is in this form. If $\vec{x} \in R^n$ and $I(\vec{x})$ is the ideal of R generated by the components of $\vec{x}$, then $I(\vec{x})$ is not equal to R

$\Leftrightarrow$ there is a $j \in \{1, 2 \ldots, \ell\}$ such that

$$I(\vec{x}) \subseteq R_1 \times \cdots \times R_{j-1} \times M_j \times R_{j+1} \times \cdots \times R_\ell$$

$\Leftrightarrow$ there is a $j \in \{1, 2 \ldots, \ell\}$ such that $\rho_j\big(I(\vec{x})\big) \subseteq M_j$.

Therefore, we have shown the next proposition.

Proposition 1.3.3. *For $\vec{x} \in R^n$, we have $\vec{x}$ is unimodular if and only if $\rho_j(\vec{x})$ is unimodular in R_j^n for all $j \in \{1, 2, \ldots, \ell\}$.*

To conclude the desired result on unimodular vectors and linearly independent vectors, we require the following property.

Proposition 1.3.4. *For $\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_s \in R^n$, we have $\{\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_s\}$ is linearly independent over R if and only if $\{\rho_j(\vec{x}_1), \rho_j(\vec{x}_2), \ldots, \rho_j(\vec{x}_s)\}$ is linearly independent over R_j for all $j \in \{1, 2, \ldots, \ell\}$.*

Proof. Assume that $\{\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_s\}$ is linearly independent over R. Let $j \in \{1, 2, \ldots, \ell\}$ and $a_{j1}, a_{j2}, \ldots, a_{js} \in R_j$ be such that $a_{j1}\rho_j(\vec{x}_1) + a_{j2}\rho_j(\vec{x}_2) + \cdots + a_{js}\rho_j(\vec{x}_s) = \vec{0}$. For each $t \in \{1, 2, \ldots, s\}$, we set $a_t = (a_{1t}, \ldots, a_{jt}, \ldots, a_{\ell t})$ where $a_{kt} = 0 \in R_k$ for all $k \in \{1, 2, \ldots, \ell\} \setminus \{j\}$, and so $a_t \in R$. Then $a_1\vec{x}_1 + a_2\vec{x}_2 + \cdots + a_s\vec{x}_s = \vec{0}$. Since $\{\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_s\}$ is linearly independent over R, it follows that $a_1 = a_2 = \cdots = a_s = 0$. Therefore, $a_{j1} = a_{j2} = \cdots = a_{js} = 0$ and so $\{\rho_j(\vec{x}_1), \rho_j(\vec{x}_2), \ldots, \rho_j(\vec{x}_s)\}$ is linearly independent over R_j.

Conversely, assume that $\{\rho_j(\vec{x}_1), \rho_j(\vec{x}_2), \ldots, \rho_j(\vec{x}_s)\}$ is linearly independent over R_j for all $j \in \{1, 2, \ldots, \ell\}$. Let $a_t = (a_{1t}, a_{2t}, \ldots, a_{\ell t}) \in R$ for $t \in \{1, 2, \ldots, s\}$ be such that $a_1\vec{x}_1 + a_2\vec{x}_2 + \cdots + a_s\vec{x}_s = \vec{0}$. Then for each $j \in \{1, 2, \ldots, \ell\}$, we obtain $a_{j1}\rho_j(\vec{x}_1) + a_{j2}\rho_j(\vec{x}_2) + \cdots + a_{js}\rho_j(\vec{x}_s) = \vec{0}$. By the assumption, $a_{j1} = a_{j2} = \cdots = a_{js} = 0$ for all $j \in \{1, 2, \ldots, \ell\}$. Thus, $a_1 = a_2 = \cdots = a_s = 0$, and so $\{\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_s\}$ is linearly independent. $\square$

Combining Propositions 1.3.2–1.3.4 implies that for $\vec{x} \in R^n$, $\vec{x}$ is unimodular if and only if $\{\vec{x}\}$ is linearly independent. We record this important observation in:

Corollary 1.3.5. *Let R be a finite commutative ring and $\vec{x} \in R^n$. Then $\vec{x}$ is unimodular if and only if $\{\vec{x}\}$ is linearly independent.*

1.4 Rank of Matrices over Commutative Rings

McCoy [12] introduced the concept of rank of matrices over commutative rings. It generalizes the usual rank of matrices over fields. This rank is defined by the annihilators of ideals.

For an ideal I of a commutative ring R, the **annihilator** of I is given by

$$\operatorname{Ann}_R I = \{r \in R : ra = 0 \text{ for all } a \in I\}.$$

It is easy to see that $\operatorname{Ann}_R I$ is an ideal of R. Moreover, if I and J are ideals of R such that $I \subseteq J$, then $\operatorname{Ann}_R J \subseteq \operatorname{Ann}_R I$.

Let R be a commutative ring and A an $m \times n$ matrix over R. We define $I_0(A) = R$ and $I_t(A)$ to be the ideal of R generated by the $t \times t$ minors of A for $1 \leq t \leq \min\{m, n\}$. Note that

$$R = I_0(A) \supseteq I_1(A) \supseteq \cdots \supseteq I_{\min\{m,n\}}(A)$$

and so

$$\{0\} = \operatorname{Ann}_R I_0(A) \subseteq \operatorname{Ann}_R I_1(A) \subseteq \cdots \subseteq \operatorname{Ann}_R I_{\min\{m,n\}}(A).$$

The **rank of** A, $\operatorname{rk} A$, is the largest integer r such that $\operatorname{Ann}_R I_r(A) = \{0\}$. If R is a field, it follows that A has t linearly independent columns if and only if there exists a $t \times t$ submatrix B of A such that $\det B \neq 0$, if and only if $I_t(A) = R$, if and only if $\operatorname{Ann}_R I_t(A) = \{0\}$ where $t \leq \min\{m, n\}$. Therefore, $\operatorname{rk} A$ coincides with the maximal number of linearly independent columns of A, so it is the usual rank of A when R is a field.

Example 1.4.1. Let $R = \mathbb{Z}_4$ and $A = \begin{pmatrix} 3 & 2 & 3 & 0 \\ 2 & 1 & 2 & 1 \\ 1 & 2 & 3 & 2 \end{pmatrix}$ be an 3×4 matrix over R. Then $I_0(A) = R, I_1(A) = R, I_2(A) = R$ and $I_3(A) = \langle 2 \rangle$, the ideal generated by 2. It follows that $\operatorname{Ann}_R I_0(A) = \{0\}, \operatorname{Ann}_R I_1(A) = \{0\}, \operatorname{Ann}_R I_2(A) = \{0\}$ and $\operatorname{Ann}_R I_3(A) = \langle 2 \rangle$. Therefore, the rank of A is 2.

Some properties of the rank of matrices are presented as follows.

Proposition 1.4.2. [4] *Let R be a commutative ring and A an $m \times n$ matrix over R. Then*

(1) $0 \leq \operatorname{rk} A \leq \min\{m, n\}$.

(2) $\operatorname{rk} A = \operatorname{rk} A^{\mathrm{T}}$.

(3) $\operatorname{rk} A = \operatorname{rk} PAQ$ *for all* $P \in GL_m(R)$ *and* $Q \in GL_n(R)$.

(4) $\operatorname{rk} A = 0$ *if and only if* $\operatorname{Ann}_R I_1(A) \neq \{0\}$.

(5) If $m = n$, *then* $\operatorname{rk} A < n$ *if and only if* $\det A$ *is the zero or a zero divisor of* R.

(6) The homogeneous system of equations $\vec{x}A = \vec{0}$ *has a non trivial solution if and only if* $\operatorname{rk} A < m$.

(7) If $m \leq n$, *then* A *has rank* m *if and only if the rows of* A *are linearly independent.*

Lemma 1.4.3. [5] *Let* R *be a commutative ring and* A *an* $m \times n$ *matrix over* R *with* $m \leq n$.

(1) If $\vec{b} \in R^n$ *and the system of equations* $\vec{x}A = \vec{b}$ *has a solution, then the solution is unique if and only if* $\operatorname{rk} A = m$.

(2) If R *is finite, then the system of equations* $\vec{x}A = \vec{b}$ *has a solution for every* $\vec{b} \in R^n$ *if and only if* $\operatorname{rk} A = n$.

For matrices over finite local rings, Brawley and Carlitz [3] showed an important relation between the rank of matrices over a finite local ring and that over its residue field.

Lemma 1.4.4. [3] *Let* R *be a finite local ring with unique maximal ideal* M *and the canonical map* $\pi : R \to R/M$. *Then for any matrix* $A = (a_{ij})$ *of* R, *the rank of* A *is* r *if and only if* $\pi(A) = (\pi(a_{ij}))$ *has rank* r *over* $k = R/M$.

Hence, the rank of a matrix over a finite local ring is obtained from computing the rank of its reduction which can be done in an elementary way.

Example 1.4.5. According to a matrix $A = \begin{pmatrix} 3 & 2 & 3 & 0 \\ 2 & 1 & 2 & 1 \\ 1 & 2 & 3 & 2 \end{pmatrix}$ over $\mathbb{Z}_4$ from Example 1.4.1, we can alternatively obtain the rank of matrix A by considering the matrix $\pi(A) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$ over the residue field $\mathbb{Z}_2$. It is obvious that the rank of $\pi(A)$ is 2. By Lemma 1.4.4, the rank of A is 2.

For any finite commutative ring, Bollman and Ramirez [2] showed a nice relationship between the rank of matrices over finite commutative rings and that over finite local rings.

Lemma 1.4.6. [2] *Let R be a finite commutative ring decomposed as $R \cong R_1 \times R_2 \times \cdots \times R_\ell$ where R_j is a finite local ring with the projection map $\rho_j : r = (s_1, s_2, \ldots, s_\ell) \mapsto s_j$ for all $j \in \{1, 2, \ldots, \ell\}$. If $A = (a_{ij})$ is an $m \times n$ matrix over R, then*

$$\operatorname{rk} A = \min_{1 \le j \le \ell} \{\operatorname{rk} \rho_j(A)\},$$

where $\rho_j(A) := \big(\rho_j(a_{ij})\big)$ is a matrix over R_j.

Example 1.4.7. Consider the commutative ring $\mathbb{Z}_{12}$ decomposed as $\mathbb{Z}_4 \times \mathbb{Z}_3$. The isomorphism is given by $\rho : a \mapsto (a + 4\mathbb{Z}, a + 3\mathbb{Z})$ for all $a \in \mathbb{Z}$. Let $A = \begin{pmatrix} 3 & 10 & 7 & 0 \\ 6 & 5 & 2 & 1 \\ 1 & 6 & 11 & 10 \end{pmatrix}$ be a matrix over $\mathbb{Z}_{12}$. Then $\rho_1(A) = \begin{pmatrix} 3 & 2 & 3 & 0 \\ 2 & 1 & 2 & 1 \\ 1 & 2 & 3 & 2 \end{pmatrix}$ is a matrix over $\mathbb{Z}_4$ and $\rho_2(A) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 2 & 2 & 1 \\ 1 & 0 & 2 & 1 \end{pmatrix}$ is a matrix over $\mathbb{Z}_3$. By Example 1.4.1, we obtain that $\operatorname{rk} \rho_1(A) = 2$. As well as, we can see that $\operatorname{rk} \rho_2(A) = 3$. By Lemma 1.4.6, $\operatorname{rk}(A) = \min\{\operatorname{rk} \rho_1(A), \operatorname{rk} \rho_2(A)\} = 2$.

1.5 Free Submodules

For vector spaces over the finite field of order q, there is a well known formula [19] for the number of subspaces of dimension s in a vector space of dimension n given by

$$\begin{bmatrix} n \\ s \end{bmatrix}_q = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{s-1})}{(q^s - 1)(q^s - q) \cdots (q^s - q^{s-1})}.$$

Dougherty and Salturk [6] determined the number of free submodules (they call them "free codes") of R^n of rank s when R is a finite Frobenius commutative ring. They obtained this number by counting the set of s linearly independent vectors.

Let R be a finite commutative ring. Following Meemark and Sriwongsa's lifting idea [17], we can count the number of free submodules of R^n of rank s.

Let X be a free submodule of R^n of rank s with basis $\{\vec{x}_1, \vec{x}_2, \dots, \vec{x}_s\}$. Then we have $X = R\vec{x}_1 \oplus R\vec{x}_2 \oplus \cdots \oplus R\vec{x}_s$ and we use the same letter X to denote an $s \times n$ matrix whose its ith row is $\vec{x}_i$ for all i, that is,

$$X = \begin{pmatrix} \vec{x}_1 \\ \vdots \\ \vec{x}_s \end{pmatrix}.$$

Moreover, if Y is another free submodule of R^n of rank s with basis $\{\vec{y}_1, \vec{y}_2, \dots, \vec{y}_s\}$, we adopt the notation $\begin{pmatrix} X \\ Y \end{pmatrix}$ to denote the augmented $2s \times n$ matrix whose rows are obtained from the matrices X and Y, respectively. Observe that the rank of $\begin{pmatrix} X \\ Y \end{pmatrix}$ does not depend on the choice of bases for X and Y by Proposition 1.4.2 (3). In particular, if X and Y are subspaces over fields, it is clear that $\operatorname{rk}\begin{pmatrix} X \\ Y \end{pmatrix} = \dim(X + Y)$, so $\dim(X \cap Y) = s - t$ if and only if $\operatorname{rk}\begin{pmatrix} X \\ Y \end{pmatrix} = s + t$ where $t \in \{0, 1, \dots, s\}$.

As well, to count the number of free submodules over a finite commutative ring, we first establish properties and the number of free submodules over a finite local ring by lifting them from its residue field.

Theorem 1.5.1. *Let R be a finite local ring with maximal ideal M, residue field $k = R/M$ with q elements and the canonical map $\pi : R \to R/M$.*

(1) If $X = R\vec{x}_1 \oplus R\vec{x}_2 \oplus \cdots \oplus R\vec{x}_s$ is a free submodule of R^n of rank s, then $\pi(X) := k\pi(\vec{x}_1) \oplus k\pi(\vec{x}_2) \oplus \cdots \oplus k\pi(\vec{x}_s)$ is a subspace of k^n over k of dimension s.

(2) Let $\vec{x}_1, \vec{x}_2, \dots, \vec{x}_s \in R^n$. If $k\pi(\vec{x}_1) \oplus k\pi(\vec{x}_2) \oplus \cdots \oplus k\pi(\vec{x}_s)$ is a subspace of k^n over k of dimension s, then

$$R(\vec{x}_1 + \vec{m}_1) \oplus R(\vec{x}_2 + \vec{m}_2) \oplus \cdots \oplus R(\vec{x}_s + \vec{m}_s)$$

is a free submodule of R^n of rank s where $\vec{m}_i \in M^n$ for all $i \in \{1, 2, \ldots, s\}$. Moreover, for $\vec{m}_i, \vec{n}_i \in M^n$ where $i \in \{1, 2, \ldots, s\}$, $R(\vec{x}_1 + \vec{m}_1) \oplus R(\vec{x}_2 + \vec{m}_2) \oplus \cdots \oplus R(\vec{x}_s + \vec{m}_s) = R(\vec{x}_1 + \vec{n}_1) \oplus R(\vec{x}_2 + \vec{n}_2) \oplus \cdots \oplus R(\vec{x}_s + \vec{n}_s)$ if and only if

$$\begin{pmatrix} \vec{x}_1 + \vec{m}_1 \\ \vdots \\ \vec{x}_s + \vec{m}_s \end{pmatrix} = (I_s + N) \begin{pmatrix} \vec{x}_1 + \vec{n}_1 \\ \vdots \\ \vec{x}_s + \vec{n}_s \end{pmatrix}$$

for some $s \times s$ matrix N whose all entries are in M.

(3) The number of free submodules of R^n of rank s is

$$|M|^{ns-s^2} \begin{bmatrix} n \\ s \end{bmatrix}_q .$$

Proof. (1) Assume that $X = R\vec{x}_1 \oplus R\vec{x}_2 \oplus \cdots \oplus R\vec{x}_s$ is a free submodule of R^n of rank s. We show that $\{\pi(\vec{x}_1), \pi(\vec{x}_2), \ldots, \pi(\vec{x}_s)\}$ is linearly independent over k. Let $\alpha_1, \alpha_2, \ldots, \alpha_s \in k$ be such that $\alpha_1\pi(\vec{x}_1) + \alpha_2\pi(\vec{x}_2) + \cdots + \alpha_s\pi(\vec{x}_s) = \vec{0}$. Then $\vec{\alpha}\pi(X) = \vec{0}$ where $\vec{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_s)$. Since $\operatorname{rk} X = s$, we have $\operatorname{rk} \pi(X) = s$. Thus, the homogeneous system of equations $\vec{\alpha}\pi(X) = \vec{0}$ has the trivial solution, that is, $\vec{\alpha} = \vec{0}$, and so $\alpha_1 = \alpha_2 = \cdots = \alpha_s = 0$. Hence, $\pi(X) := k\pi(\vec{x}_1) \oplus k\pi(\vec{x}_2) \oplus \cdots \oplus k\pi(\vec{x}_s)$ is a subspace of k^nover k of dimension s.

(2) Assume that $\overline{X} := k\pi(\vec{x}_1) \oplus k\pi(\vec{x}_2) \oplus \cdots \oplus k\pi(\vec{x}_s)$ is a subspace of k^n over k of dimension s. Let $\vec{m}_1, \vec{m}_2, \ldots, \vec{m}_s \in M^n$. We show that $\{\vec{x}_1 + \vec{m}_1, \vec{x}_2 + \vec{m}_2, \ldots, \vec{x}_s + \vec{m}_s\}$ is linearly independent over R. Let $a_1, a_2, \ldots, a_s \in R$ be such that $a_1(\vec{x}_1 + \vec{m}_1) + a_2(\vec{x}_2 + \vec{m}_2) + \cdots + a_s(\vec{x}_s + \vec{m}_s) = \vec{0}$. Then $\vec{a}X' = \vec{0}$ where $\vec{a} = (a_1, a_2, \ldots, a_s)$ and X' is an $s \times n$ matrix whose ith row is $\vec{x}_i + \vec{m}_i$ for all $i \in \{1, 2, \ldots, s\}$. Since $\operatorname{rk} \pi(X') = \operatorname{rk} \overline{X} = s$, it follows that $\operatorname{rk} X' = s$. By Proposition 1.4.2 (6), the homogeneous system of equations $\vec{a}X' = \vec{0}$ has the trivial solution, that is $\vec{a} = \vec{0}$, and so $a_1 = a_2 = \cdots = a_s = 0$. Thus, $R(\vec{x}_1 + \vec{m}_1) \oplus R(\vec{x}_2 + \vec{m}_2) \oplus \cdots \oplus R(\vec{x}_s + \vec{m}_s)$ is a free submodule of R^n of rank s.

Next, let $\vec{m}_i, \vec{n}_i \in M^n$ for all $i \in \{1, 2, \ldots, s\}$, $X_1 = R(\vec{x}_1 + \vec{m}_1) \oplus R(\vec{x}_2 + \vec{m}_2) \oplus \cdots \oplus R(\vec{x}_s + \vec{m}_s)$ and $X_2 = R(\vec{x}_1 + \vec{n}_1) \oplus R(\vec{x}_2 + \vec{n}_2) \oplus \cdots \oplus R(\vec{x}_s + \vec{n}_s)$. Suppose that $X_1 = X_2$. We may assume without loss of generality that $\overline{X} = \begin{pmatrix} I_s & \overline{C} \end{pmatrix}$ where $\overline{C}$ is an $s \times (n-s)$ matrix over k. Then we can write $X_1 = \begin{pmatrix} I_s + N_1 & C_1 \end{pmatrix}$ and $X_2 = \begin{pmatrix} I_s + N_2 & C_2 \end{pmatrix}$ where N_1 and N_2 are $s \times s$ matrices whose all entries are in M and C_1, C_2 are $s \times (n-s)$ matrices over R. Since free submodules X_1 and X_2 are equal, $X_1 = UX_2$ for some $U \in GL_s(R)$. It follows that $I_s + N_1 = U(I_s + N_2)$, and so $U = I_s + (N_1 - UN_2)$.

Conversely, assume that $X_1 = (I_s + N)X_2$ for some $s \times s$ matrix N whose all entries are in M. Since $I_s + N \in GL_s(R)$, we have that X_1 and X_2 generate the same free submodule.

(3) We have seen that a free submodule of R^n of rank s is of the form $R(\vec{x}_1 + \vec{m}_1) \oplus R(\vec{x}_2 + \vec{m}_2) \oplus \cdots \oplus R(\vec{x}_s + \vec{m}_s)$ where $k\pi(\vec{x}_1) \oplus k\pi(\vec{x}_2) \oplus \cdots \oplus k\pi(\vec{x}_s)$ is a subspace of k^n over k of dimension s and $\vec{m}_i \in M^n$. Hence, each subspace of k^n over k of dimension s can be lifted to $|M|^{ns}/|M|^{s^2}$ free submodules of R^n of rank s. Thus, the number of free submodules of R^n of rank s is

$$\frac{|M|^{ns}}{|M|^{s^2}} \begin{bmatrix} n \\ s \end{bmatrix}_q = |M|^{ns-s^2} \begin{bmatrix} n \\ s \end{bmatrix}_q$$

where $\begin{bmatrix} n \\ s \end{bmatrix}_q$ is the number of subspaces of dimension s in a vector space k^n. $\square$

Finally, we let R be a finite commutative ring decomposed as $R_1 \times R_2 \times \cdots \times R_\ell$ where R_j is a finite local ring with maximal ideal M_j and residue field R_j/M_j with q_j elements for all $j \in \{1, 2, \ldots, \ell\}$. The ring R is equipped with the projection map $\rho_j : r = (s_1, s_2, \ldots, s_\ell) \mapsto s_j$ for all $j \in \{1, 2, \ldots, \ell\}$. Observe that for each j and a submodule X of R^n generated by $\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_s$, the submodule $\rho_j(X)$ of R_j^n is generated by $\rho_j(\vec{x}_1), \rho_j(\vec{x}_2), \ldots, \rho_j(\vec{x}_s)$. We also have from Proposition 1.3.4 that $\{\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_s\}$ is linearly independent over R if and only if $\{\rho_j(\vec{x}_1), \rho_j(\vec{x}_2), \ldots, \rho_j(\vec{x}_s)\}$ is linearly independent over R_j for all $j \in \{1, 2, \ldots, \ell\}$. Thus, we have shown:

Lemma 1.5.2. *X is a free submodule of R^n of rank s if and only if $\rho_j(X)$ is a free submodule of R_j^n of rank s for all $j \in \{1, 2, \ldots, \ell\}$.*

Together with the number of free submodules over a finite local ring computed in Theorem 1.5.1, we obtain the next corollary.

Corollary 1.5.3. *The number of free submodules of R^n of rank s is*

$$\prod_{j=1}^{\ell} |M_j|^{ns-s^2} \begin{bmatrix} n \\ s \end{bmatrix}_{q_j}.$$

We end this section with showing examples of free submodules and pointing out that the intersection of two free submodules may not be free.

Example 1.5.4. Let $R = \mathbb{Z}_4$ and $V = R^4$ be a free R-module of rank 4. Let X be the submodule generated by $B_X := \{(1,0,0,0),(0,1,0,0)\}$ and Y the submodule generated by $B_Y := \{(1,0,2,0),(0,0,0,1)\}$. It is easy to see that X and Y are two free submodules of V with bases B_X and B_Y, respectively. Suppose $\vec{x} \in X \cap Y$. Then $x_1(1,0,0,0) + x_2(0,1,0,0) = \vec{x} = y_1(1,0,2,0) + y_2(0,0,0,1)$. So $x_1 = y_1, 2y_1 = 0$ and $x_2 = y_2 = 0$. It follows that $\vec{x}$ is either $(0,0,0,0)$ or $(2,0,0,0)$. Therefore, $X \cap Y = \{(0,0,0,0),(2,0,0,0)\}$ which is not a free submodule over R.

1.6 Bilinear Forms

Let R be a commutative ring. Let V be a free R-module of rank n. A **bilinear form β on** V is a two-variable function $\beta : V \times V \to R$ which is linear in each variable, namely,

$$\beta(\vec{x}+\vec{y},\vec{z}) = \beta(\vec{x},\vec{z}) + \beta(\vec{y},\vec{z}) \text{ and } \beta(r\vec{x},\vec{z}) = r\beta(\vec{x},\vec{z})$$

and

$$\beta(\vec{x},\vec{z}+\vec{w}) = \beta(\vec{x},\vec{z}) + \beta(\vec{x},\vec{w}) \text{ and } \beta(\vec{x},s\vec{z}) = s\beta(\vec{x},\vec{z})$$

for all $\vec{x},\vec{y},\vec{z},\vec{w} \in V$ and $r,s \in R$.

Next, we classify certain bilinear forms. Let β be a bilinear form on V. We say that β is **non-degenerate** if (1) $\vec{x} \in V$ and $\beta(\vec{x},\vec{y}) = 0$ for all $\vec{y} \in V$ implies $\vec{x} = 0$, similarly, if $\vec{y} \in V$ and $\beta(\vec{x},\vec{y}) = 0$ for all $\vec{x} \in V$, then $\vec{y} = 0$, and (2) for any R-linear map $f : V \to R$, there exist $\vec{x}_0, \vec{y}_0 \in V$ such that $f(\vec{x}) = \beta(\vec{x}_0,\vec{x})$

and $f(\vec{x}) = \beta(\vec{x}, \vec{y}_0)$ for all $\vec{x} \in V$, β is **alternating** if $\beta(\vec{x}, \vec{x}) = 0$ for all $\vec{x} \in V$, β is **symmetric** if $\beta(\vec{x}, \vec{y}) = \beta(\vec{y}, \vec{x})$ for all $\vec{x}, \vec{y} \in V$, and β is **skew-symmetric** if $\beta(\vec{x}, \vec{y}) = -\beta(\vec{y}, \vec{x})$ for all $\vec{x}, \vec{y} \in V$.

If β is an alternating bilinear form on V, then

$$0 = \beta(\vec{x} + \vec{y}, \vec{x} + \vec{y}) = \beta(\vec{x}, \vec{x}) + \beta(\vec{x}, \vec{y}) + \beta(\vec{y}, \vec{x}) + \beta(\vec{y}, \vec{y}) = \beta(\vec{x}, \vec{y}) + \beta(\vec{y}, \vec{x})$$

for all $\vec{x}, \vec{y} \in V$. Thus, every alternating bilinear form is skew-symmetric.

Example 1.6.1. 1. Let p be a prime number and let R be the ring of integer modulo p^n, $\mathbb{Z}_{p^n}$, or the field of order p^n, $\mathbb{F}_{p^n}$, where $n \in \mathbb{N}$. For $\nu \geq 1$, let $V = R^{2\nu}$. Define $\beta : V \times V \to R$ by

$$\beta(\vec{x}, \vec{y}) = (x_1, x_2, \dots, x_{2\nu}) \begin{pmatrix} 0 & I_\nu \\ -I_\nu & 0 \end{pmatrix} (y_1, y_2, \dots, y_{2\nu})^{\mathrm{T}}$$

where I_ν is the $\nu \times \nu$ identity matrix, for all $\vec{x} = (x_1, x_2, \dots, x_{2\nu})$ and $\vec{y} = (y_1, y_2, \dots, y_{2\nu})$ in V. Then β is a non-degenerate alternating bilinear form on V.

2. Let p be an odd prime number and let R be the ring of integers modulo p^n, $\mathbb{Z}_{p^n}$, or the field of order p^n, $\mathbb{F}_{p^n}$, where $n \in \mathbb{N}$. For $\nu \geq 1$ and $\delta \in \{0, 1, 2\}$, let $V = R^{2\nu+\delta}$. Define $\beta : V \times V \to R$ by

$$\beta(\vec{x}, \vec{y}) = (x_1, x_2, \dots, x_{2\nu+\delta}) \begin{pmatrix} 0 & I_\nu & \\ I_\nu & 0 & \\ & & \Delta \end{pmatrix} (y_1, y_2, \dots, y_{2\nu+\delta})^{\mathrm{T}}$$

where

$$\Delta = \begin{cases} \varnothing(\text{disappear}) & \text{if } \delta = 0, \\ (1) \text{ or } (z) & \text{if } \delta = 1, \\ \operatorname{diag}(1, -z) & \text{if } \delta = 2, \end{cases}$$

and z is a fixed non-square unit in R, for all $\vec{x} = (x_1, x_2, \dots, x_{2\nu+\delta})$ and $\vec{y} = (y_1, y_2, \dots, y_{2\nu+\delta})$ in V. Then β is a non-degenerate symmetric bilinear form on V.

An R-module automorphism σ on V is an **isometry with respect to** β if $\beta(\sigma(\vec{x}), \sigma(\vec{y})) = \beta(\vec{x}, \vec{y})$ for all $\vec{x}, \vec{y} \in V$. It is clear that the set of isometries on V with respect to β forms a group under composition. It is called the **group of isometries on** (V, β).

If β is non-degenerate and alternating, then we call the pair (V, β) a **symplectic space** and we call its group of isometries a **symplectic group**. If R is of odd characteristic and β is non-degenerate and symmetric, then the pair (V, β) is called an **orthogonal space** and its group of isometries is called an **orthogonal group**.

1.7 Graphs

In this section, we focus on all notions of graphs which will be regarded in this dissertation.

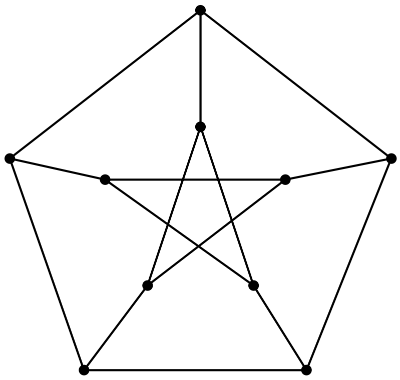
A **graph** $G = (V, E)$ consists of a nonempty set V of vertices and a set E of edges formed by pairs of vertices. A graph is **regular** if each vertex has the same number of neighbors which is called the **degree** of a regular graph. A **complete** graph is a graph in which any two distinct vertices are adjacent. Equivalently, a complete graph with n vertices is a regular graph of degree $n - 1$.

Let G and H be graphs. A function σ from G to H is a **homomorphism** from G to H if g_1 is adjacent to g_2 in G implies $\sigma(g_1)$ is adjacent to $\sigma(g_2)$. A homomorphism from G to H is called an **isomorphism** if it is a bijection and σ^{-1} is a homomorphism from H to G. An isomorphism on G is called an **automorphism**. The set of automorphisms of G is denoted by $\mathrm{Aut}(G)$. It is a group under composition, called the **automorphism group of** G.

A graph G is **vertex transitive** if its automorphism group acts transitively on the vertex set. That is, for any two vertices of G, there is an automorphism carrying one to the other. An **arc** in G is an ordered pair of adjacent vertices and G is **arc transitive** if its automorphism group acts transitively on its arcs. It follows that an arc transitive graph is always vertex transitive and regular.

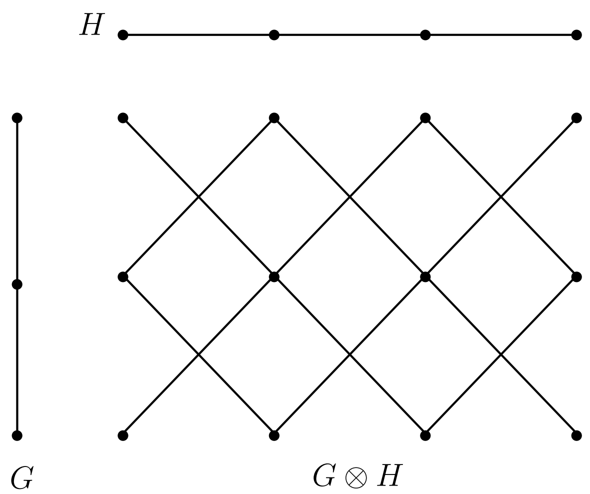
Example 1.7.1. 1. The complete graph is arc transitive.

2. The following Petersen graph is an arc transitive graph.



For two graphs G and H with vertex sets $V(G), V(H)$, respectively, the **tensor product of G and H**, denoted by $G \otimes H$, is the graph whose vertex set is $V(G) \times V(H)$ and (v_1, v_2) is adjacent to (v_1', v_2') if v_1 is adjacent to v_1' in G and v_2 is adjacent to v_2' in H.

Example 1.7.2. The following graph shows the tensor product of the graphs G and H.



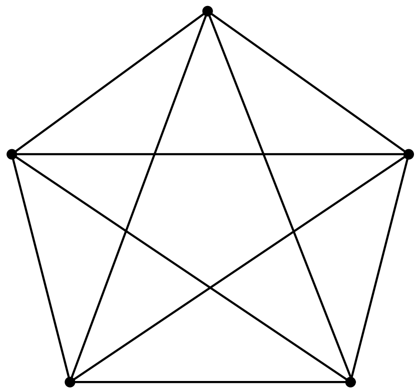
A useful property of an automorphism of tensor product of graphs is proved in Theorem 2.11 of [17]. We record it in the following lemma.

Lemma 1.7.3. *Let G and H be graphs. Then* $\mathrm{Aut}(G) \times \mathrm{Aut}(H) \subseteq \mathrm{Aut}(G \otimes H)$.

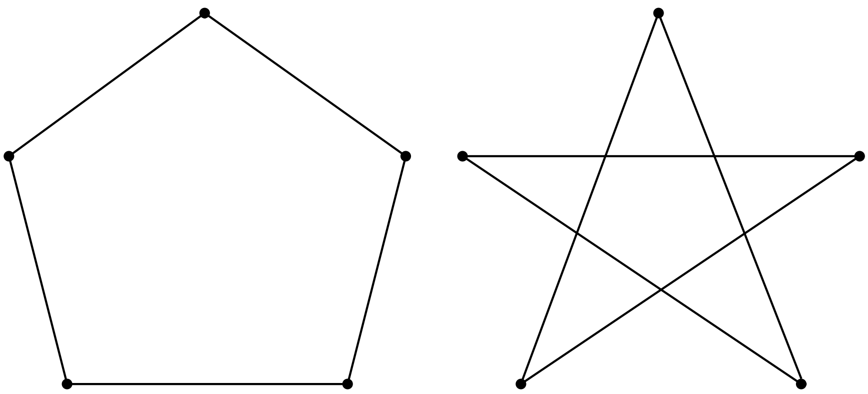
For the end of this section, we introduce a decomposition of a graph which will play an important role in our graphs over finite commutative rings.

A **decomposition** of a graph G is a family of edge-disjoint subgraphs of G such that any edge of G belongs to exactly one subgraph.

Example 1.7.4. Consider the following complete graph with five vertices.



It can be decomposed into a family of two following graphs.



1.8 Generalized Bilinear Form Graphs

Let R be a finite commutative ring, V a free R-module of rank n and β a bilinear form on V.

For any two free submodules X and Y of V of rank s with bases $\{\vec{x}_1, \ldots, \vec{x}_s\}$ and $\{\vec{y}_1, \ldots, \vec{y}_s\}$, we have the associate $s \times s$ matrix for β given by

$$\Big(\beta(\vec{x}_i, \vec{y}_j)\Big) \text{ where } i, j \in \{1, \ldots, s\}.$$

By Proposition 1.4.2 (3), the rank of this matrix is independent of choices of bases for X and Y. Thus, we may denote this rank by $\operatorname{rk} \beta(X, Y)$.

We finally introduce the last terminology before revealing the definition of generalized bilinear form graphs, namely the notion of totally isotropic submodules. A submodule X of V is **totally isotropic** if $\beta(\vec{x},\vec{y}) = 0$ for all $\vec{x},\vec{y} \in X$. If X is a free submodule of V with basis $\{\vec{x}_1,\ldots,\vec{x}_s\}$, then X is totally isotropic if and only if $\beta(\vec{x}_i,\vec{x}_j) = 0$ for all $i,j \in \{1,\ldots,s\}$.

Example 1.8.1. Let R be a finite local ring. For $\nu \geq 1$, let $V = R^{2\nu}$ be a free R-module with a bilinear form $\beta : V \times V \to R$ by

$$\beta(\vec{x},\vec{y}) = (x_1,x_2,\ldots,x_{2\nu}) \begin{pmatrix} 0 & I_\nu \\ -I_\nu & 0 \end{pmatrix} (y_1,y_2,\ldots,y_{2\nu})^{\mathrm{T}}.$$

for all $\vec{x} = (x_1,x_2,\ldots,x_{2\nu})$ and $\vec{y} = (y_1,y_2,\ldots,y_{2\nu})$ in V. If $s \leq \nu$, then a free submodule generated by $\{\vec{e}_1,\vec{e}_1,\ldots,\vec{e}_s\}$ is totally isotropic. More generally, if $i_1,i_2,\ldots,i_s$ are s indices such that $1 \leq i_1 < i_2 < \cdots < i_s \leq \nu$, then a free submodule generated by $\{e_{i_1},e_{i_2},\ldots,e_{i_s}\}$ is a totally isotropic submodule.

There are many graphs defined on totally isotropic free submodules. In 2006, Tang and Wan [18] defined graphs over symplectic spaces over finite fields. The vertex of this symplectic graph is the set of subspaces of dimension one and its adjacency condition is given by for two subspaces with bases $\{\vec{x}\}$ and $\{\vec{y}\}$, respectively, they are adjacent if $\beta(\vec{x},\vec{y}) \neq 0$. Note that any subspace of dimension one of a symplectic space is clearly totally isotropic. Two years later, Gu and Wan [7] introduced graphs over orthogonal spaces over finite fields of odd characteristic. These orthogonal graphs are defined analogously to symplectic graphs but the vertex set is not the set of subspaces of dimension one. The vertex set is the set of totally isotropic subspaces of dimension one. Note that the totally isotropic condition is required to avoid loops in our graphs.

Meemark and Prinyasart [13] generalized the concept of symplectic graphs over finite fields to symplectic graphs over finite commutative rings. They introduced symplectic graphs over $\mathbb{Z}_{p^n}$ the ring of integers modulo p^n where p is prime and $n \geq 1$. After that, symplectic graphs and orthogonal graphs over other finite commutative rings have been explored such as symplectic graphs modulo pq

where p and q are primes [11] and over finite local rings [14], and orthogonal graphs over Galois rings of odd characteristic [10]. Meemark and Puirod [15] completely studied symplectic graphs over finite commutative rings. Recently, Meemark and Sriwongsa [17] worked on orthogonal graphs over finite commutative rings of odd characteristic. They used the lifting theorem which lifts results over a finite local ring from the ones over its residue field. This approach is clean and is more effective in determining the number of common neighbors of adjacent and non-adjacent vertices.

The vertex set of their graphs over finite commutative rings is the set of totally isotropic submodules generated by a unimodular vector. However, we have shown in Corollary 1.3.5 that unimodular vectors coincide with linearly independent vectors in finite commutative rings. Thus, the vertex set of a symplectic graph or an orthogonal graph is the set of totally isotropic free submodules of rank one. Two submodules with bases $\{\vec{x}\}$ and $\{\vec{y}\}$, respectively, are adjacent if $\beta(\vec{x}, \vec{y})$ is in $R^\times$.

Zeng et al. [21] gave another generalization of symplectic graphs over finite fields called **the generalized symplectic graphs**. Its vertex set is the set of totally isotropic s-dimensional subspaces of a symplectic space, where $s \geq 1$, and two vertices X and Y are adjacent if $\operatorname{rk} \beta(X, Y) = 1$ and $\dim(X \cap Y) = s - 1$. When $s = 1$, a generalized symplectic graph is a symplectic graph. Later, Huo and Zhang [9] worked on an **orthogonal graph of type** $(s, s-1, 0)$ over a finite field. It is a graph whose vertex set is the set of totally isotropic subspaces of dimension $s \geq 1$ and two vertices X and Y are adjacent if and only if $\operatorname{rk} \beta(X, Y) = 0$ and $\dim(X \cap Y) = s - 1$. Observe that $\dim(X \cap Y) = s - 1$ is equivalent to $\operatorname{rk} \begin{pmatrix} X \\ Y \end{pmatrix} = s + 1$. This rank can be used in our generalization of the graphs because, over a commutative ring, the intersection of two free submodules X and Y may not be free but we can always compute the rank of $\begin{pmatrix} X \\ Y \end{pmatrix}$.

Let R be a finite commutative ring, V a free R-module of rank n and β a bilinear form on V. A **generalized bilinear form graph of V of type** (s, r, t) is the graph whose vertex set is the set of totally isotropic free submodules of V of rank s and two vertices X and Y are adjacent if $\operatorname{rk}\beta(X,Y)=r$ and $\operatorname{rk}\begin{pmatrix}X\\Y\end{pmatrix}=s+t$. If (V,β) is a symplectic space, the graph is called a **generalized symplectic graph of V of type** (s,r,t) and denoted by $\mathscr{S}_R(n,s,r,t)$ and if (V,β) is an orthogonal space, the graph is called a **generalized orthogonal graph of V of type** (s,r,t) and denoted by $\mathscr{O}_R(n,s,r,t)$.

Let $\{\vec{x}\}$ and $\{\vec{y}\}$ be two linearly independent sets over R. Clearly, $\beta(\vec{x},\vec{y})\in R^\times$ if and only if $\operatorname{rk}\Big(\beta(\vec{x},\vec{y})\Big)=1$. Moreover, if $\beta(\vec{x},\vec{y})\in R^\times$, then $\{\vec{x},\vec{y}\}$ is linearly independent, and so the rank of $\begin{pmatrix}\vec{x}\\\vec{y}\end{pmatrix}$ is two by Proposition 1.4.2 (7). This implies that the graph $\mathscr{S}_R(n,1,1,1)$ is a symplectic graph over R and the graph $\mathscr{O}_R(n,1,1,1)$ is an orthogonal graph over R. The symplectic and orthogonal graphs over finite commutative rings are completely studied in [15] and [17], respectively.

In what follows, we obtain results on generalized symplectic graphs and generalized orthogonal graphs over a finite commutative ring in Chapters 2 and 3, respectively. The combinatorial approach is the lifting theorem similar to [17]. As usual, we divide the study into three cases: over finite fields, over finite local rings and over finite commutative rings. We can determine the degree of each vertex of these graphs. If R is a finite local ring, we show that these graphs are arc transitive and obtain their automorphism groups. Finally, we can decompose the graphs over a finite commutative ring into the tensor products of graphs over finite local rings.

CHAPTER II

GENERALIZED SYMPLECTIC GRAPHS

This chapter is devoted to study generalized symplectic graphs over finite commutative rings. We begin with the results of general symplectic graphs over finite fields. After that, we carry on those results to the generalized symplectic graphs over finite local rings by the lifting idea. Finally, the generalized symplectic graphs over finite commutative rings are presented.

First of all, we discuss a nice result of symplectic spaces over finite local rings which is convenient to study our graphs.

Let R be a finite local ring and (V, β) be a symplectic space over R of rank 2ν where $\nu \geq 1$. Then (V, β) possesses a basis $\mathcal{B} = \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_{2\nu}\}$ such that

$$\left(\beta\right)_{\mathcal{B}} = \begin{pmatrix} 0 & I^{\nu} \\ -I^{\nu} & 0 \end{pmatrix}.$$

We denote this matrix by K. Therefore, if $\vec{x} = x_1\vec{b}_1 + x_2\vec{b}_2 + \cdots + x_{2\nu}\vec{b}_{2\nu}$ and $\vec{y} = y_1\vec{b}_1 + y_2\vec{b}_2 + \cdots + y_{2\nu}\vec{b}_{2\nu}$ in V, then

$$\begin{aligned} \beta(\vec{x}, \vec{y}) &= (x_1, x_2, \ldots, x_{2\nu})K(y_1, y_2, \ldots, y_{2\nu})^{\mathrm{T}} \\ &= (x_1y_{\nu+1} + x_2y_{\nu+2} + \cdots + x_\nu y_{2\nu}) - (x_{\nu+1}y_1 + x_{\nu+2}y_2 + \cdots + x_{2\nu}y_\nu). \end{aligned}$$

This basis is useful in studying symplectic spaces over finite local rings, especially, over finite fields.

2.1 Over Finite Fields

For generalized symplectic graphs over finite fields, the number of vertices is given in [19]. We apply results in [20] to prove that the graph is arc transitive and determine the degree of the graph in the end of this section.

Let $\mathbb{F}_q$ be the finite field of order q and (V, β) be a symplectic space over $\mathbb{F}_q$ of dimension 2ν where $\nu \geq 1$. The generalized symplectic graph of V of type (s, r, t) has the set of totally isotropic subspaces of dimension s where $1 \leq s \leq \nu$ as the vertex set. Wan determined the number of totally isotropic subspaces of V of dimension s in Corollary 3.19 of [19]. It equals to

$$n_{S_{\mathbb{F}_q}}(2\nu, s) = \frac{\prod_{i=\nu-s+1}^{\nu}(q^{2i}-1)}{\prod_{i=1}^{s}(q^i-1)}.$$

For two vertices X and Y of $\mathscr{S}_{\mathbb{F}_q}(2\nu, s, r, t)$,

$$X \text{ is adjacent to } Y \Leftrightarrow \operatorname{rk}\beta(X,Y) = r \text{ and } \operatorname{rk}\begin{pmatrix} X \\ Y \end{pmatrix} = s+t.$$

To compute the degree of our graphs, we first show that the generalized symplectic graphs are arc transitive by applying the following lemma.

Lemma 2.1.1. [20] *Let $\mathbb{F}_q$ be the finite field of order q, (V, β) a symplectic space over $\mathbb{F}_q$ of dimension 2ν where $\nu \geq 1$ and X, X', Y, Y' totally isotropic subspaces of dimension s.*

(1) If $X \neq Y$ with $\operatorname{rk}(XKY^{\mathrm{T}}) = r$ and $\dim(X \cap Y) = s-t$, then $\max\{0, s+t-\nu\} \leq r \leq t$ and $1 \leq t \leq s$.

(2) $\operatorname{rk}(XKY^{\mathrm{T}}) = \operatorname{rk}(X'KY'^{\mathrm{T}})$ and $\dim(X \cap Y) = \dim(X' \cap Y')$ if and only if there exists a $2\nu \times 2\nu$ matrix U with $UKU^{\mathrm{T}} = K$ such that $X' = XU$ and $Y' = YU$.

Remark 2.1.2. Let R be a finite local ring. Let X and Y be two free submodules of V of rank s and $1 \leq t$. Suppose $\operatorname{rk}(XKY^{\mathrm{T}}) = r$ and $\operatorname{rk}\begin{pmatrix} X \\ Y \end{pmatrix} = s+t$. Since $\begin{pmatrix} X \\ Y \end{pmatrix}$ is an $2s \times 2\nu$ matrix, we have $t \leq s$. Then $\operatorname{rk}(\pi(X)K\pi(Y)^{\mathrm{T}}) = r$ and $\operatorname{rk}\begin{pmatrix} \pi(X) \\ \pi(Y) \end{pmatrix} = s+t$, so $\dim\big(\pi(X) \cap \pi(Y)\big) = s-t$. Since $t \neq 0$, we have $\pi(X) \neq \pi(Y)$, so $X \neq Y$. By Lemma 2.1.1 (1), $\max\{0, s+t-\nu\} \leq r \leq t$. Thus, we may study generalized symplectic graphs of type (s,r,t) over finite local rings only when $1 \le s \le \nu$ and r,t satisfy $\max\{0, s+t-\nu\} \le r \le t$ and $1 \le t \le s$.

Next, we let R be a a finite commutative ring decomposed as $R_1 \times R_2 \times \cdots \times R_\ell$ where R_j is a finite local ring. Let $X = \big(\rho_1(X), \rho_2(X), \dots, \rho_\ell(X)\big)$ and $Y = \big(\rho_1(Y), \rho_2(Y), \dots, \rho_\ell(Y)\big)$ be two free submodules of V of rank s and $1 \le t$. Suppose that $\operatorname{rk}\beta(X,Y) = r$ and $\operatorname{rk}\begin{pmatrix} X \\ Y \end{pmatrix} = s+t$. By Lemma 1.4.6, we obtain $\min_{1\le j\le \ell} \operatorname{rk}(\rho_j(X)K\rho_j(Y)^{\mathrm{T}}) = r$ and $\min_{1\le j\le\ell} \operatorname{rk}\begin{pmatrix} \rho_j(X) \\ \rho_j(Y) \end{pmatrix} = s+t$. It follows that there are $r_1, r_2, \dots, r_\ell$ and $t_1, t_2, \dots, t_\ell$ with $r = \min\{r_1, r_2, \dots, r_\ell\}$ and $t = \min\{t_1, t_2, \dots, t_\ell\}$ such that $\operatorname{rk}(\rho_j(X)K\rho_j(Y)^{\mathrm{T}}) = r_j$ and $\operatorname{rk}\begin{pmatrix} \rho_j(X) \\ \rho_j(Y) \end{pmatrix} = s + t_j$ for all $j \in \{1,2,\dots,\ell\}$. Since $1 \le t \le t_j$, we have $1 \le t_j \le s$ and $\max\{0, s+t_j-\nu\} \le r_j \le t_j$ for all $j \in \{1,2,\dots,\ell\}$. Assume that $r = r_{j_1}$ and $t = t_{j_2}$ for some $j_1, j_2 \in \{1,2,\dots,\ell\}$. The minimality of r and of t implies that $\max\{0, s+t-\nu\} \le \max\{0, s+t_{j_1}-\nu\} \le r_{j_1} = r$ and $r \le r_{j_2} \le t_{j_2} = t$. Thus, $\max\{0, s+t-\nu\} \le r \le t$. Therefore, we may study generalized symplectic graphs of type (s,r,t) over finite commutative rings only when $1 \le s \le \nu$ and r,t satisfy $\max\{0, s+t-\nu\} \le r \le t$ and $1 \le t \le s$. This concludes the remark.

Let $1 \le s \le \nu$. All generalized symplectic graphs of V of type (s,r,t) have the same vertex set. Theorem 2.1 of [20] implies that

$$\Big\{ \Big\{ (X,Y) : \operatorname{rk}(XKY^{\mathrm{T}}) = r \text{ and } \dim(X \cap Y) = s-t \Big\} : \\ \max\{0, s+t-\nu\} \le r \le t \text{ and } 1 \le t \le s \Big\}$$

is a partition of the set of order pairs of distinct totally isotropic subspaces of V of dimension s. Therefore, the complete graph of $n_{S_{\mathbb{F}_q}}(2\nu, s)$ vertices is decomposed into generalized symplectic graphs of V of type (s,r,t) where $1 \le t \le s$ and $\max\{0, s+t-\nu\} \le r \le t$.

Now, we show that our graphs are arc transitive.

Theorem 2.1.3. *A generalized symplectic graph over a finite field is arc transitive.*

Proof. Let X_1, X_2, Y_1, Y_2 be four vertices in a generalized symplectic graph such that X_1 is adjacent to Y_1 and X_2 is adjacent to Y_2. Then $\dim(X_1 \cap Y_1) = \dim(X_2 \cap Y_2)$ and $\mathrm{rk}(X_1 K Y_1^{\mathrm{T}}) = \mathrm{rk}(X_2 K Y_2^{\mathrm{T}})$. By Lemma 2.1.1 (2), there exists an $2\nu \times 2\nu$ matrix U with $UKU^{\mathrm{T}} = K$ such that $X_2 = X_1 U$ and $Y_2 = Y_1 U$. Hence, the map $Z \mapsto ZU$ for all vertices Z in $\mathscr{S}_{\mathbb{F}_q}(2\nu, s, r, t)$ is a graph automorphism mapping X_1 to X_2 and Y_1 to Y_2. $\square$

Since our graph is arc transitive, it is regular. Then, we let P be a fixed vertex in $\mathscr{S}_{\mathbb{F}_q}(2\nu, s, r, t)$ and count the degree of P. A vertex X adjacent to P is a totally isotropic subspace of V of dimension s satisfying $\mathrm{rk}(PKX^{\mathrm{T}}) = r$ and $\dim(P \cap X) = s - t$. Wei and Wang gave the number of these subspaces in Theorem 2.7 of [20]. We denote this number by $d_{S_{\mathbb{F}_q}}(r, t)$. We record the above discussion in the next theorem.

Theorem 2.1.4. *Let $\mathbb{F}_q$ be the finite field of order q, (V, β) a symplectic space over $\mathbb{F}_q$ of dimension 2ν where $\nu \geq 1$, $1 \leq s \leq \nu$ and r, t satisfy $\max\{0, s+t-\nu\} \leq r \leq t$ and $1 \leq t \leq s$. Then the generalized symplectic graph of V of type (s, r, t) has*

$$n_{S_{\mathbb{F}_q}}(2\nu, s) = \frac{\prod_{i=\nu-s+1}^{\nu}(q^{2i}-1)}{\prod_{i=1}^{s}(q^i-1)}$$

vertices and it is regular of degree

$$d_{S_{\mathbb{F}_q}}(r, t) = q^{2r(\nu-s)+(t-r)^2+\frac{r(r+1)}{2}} \begin{bmatrix} s \\ s-t \end{bmatrix}_q \begin{bmatrix} t \\ r \end{bmatrix}_q n_{S_{\mathbb{F}_q}}(2(\nu-s), t-r).$$

2.2 Over Finite Local Rings

In this section, we give the generalized symplectic graphs over local rings by applying the results over finite fields and using the lifting idea. Relationships between symplectic spaces over finite local rings and symplectic spaces over finite fields are firstly studied. Next, we determine the number of vertices which is the number of totally isotropic free submodules. After that, we present the lifting theorem of our graphs which is effective in showing that the graphs are regular, computing their degrees and presenting that they are arc transitive.

Let R be a finite local ring with maximal ideal M and residue field $k = R/M$, and let (V, β) be a symplectic space over R of rank 2ν where $\nu \geq 1$. A symplectic space (V, β) over R induces the symplectic space (V', β') over k of dimension 2ν where β' is given via the canonical map $\pi : R \to k$ by

$$\beta'(\pi(\vec{x}), \pi(\vec{y})) = \pi(\beta(\vec{x}, \vec{y}))$$

for all $\vec{x}, \vec{y} \in V$. Hence, if X is a totally isotropic submodule of (V, β), then $\pi(X)$ is a totally isotropic subspace of (V', β'). Moreover, if X is a totally isotropic free submodule of (V, β) of rank s, then $\pi(X)$ is a totally isotropic subspace of (V', β') of dimension s by Theorem 1.5.1 (1). We first count the number of totally isotropic free submodules of V.

Theorem 2.2.1. *Let R be a finite local ring with maximal ideal M and residue field $k = R/M$, (V, β) a symplectic space over R of rank 2ν where $\nu \geq 1$ and $\overline{X}$ a totally isotropic subspace of the induced symplectic space (V', β') of dimension s. Then the number of totally isotropic free submodules of V of rank s whose reduction is $\overline{X}$ is $|M|^{2\nu s - \binom{s}{2} - s^2}$. Hence, the number of totally isotropic free submodules of V of rank s equals*

$$|M|^{2\nu s - \binom{s}{2} - s^2} n_{S_k}(2\nu, s).$$

Proof. By elementary row operations and permuting the coordinates of $\overline{X}$, we may write $\overline{X} = \begin{pmatrix} \overline{I}_s & \overline{A} \end{pmatrix}$ where $\overline{A}$ is an $s \times (2\nu - s)$ matrix over k. Then we assume that $\vec{x}_1, \vec{x}_2, \dots, \vec{x}_s \in V$ are such that $\overline{X} = k\pi(\vec{x}_1) \oplus k\pi(\vec{x}_2) \oplus \cdots \oplus k\pi(\vec{x}_s)$, where for each $a \in \{1, 2, \dots, s\}$,

$$\vec{x}_a = (x_{a1}, \dots, x_{a\nu}, x_{a(\nu+1)}, \dots, x_{a(2\nu)}) \text{ with } x_{aa} = 1$$
$$\text{and } x_{ab} = 0 \text{ for all } b \in \{1, \dots, s\} \smallsetminus \{a\}.$$

Thus, $R(\vec{x}_1 + \vec{m}_1) \oplus R(\vec{x}_2 + \vec{m}_2) \oplus \cdots \oplus R(\vec{x}_s + \vec{m}_s)$ where $\vec{m}_a \in M^{2\nu}$ for all $a \in \{1, 2 \dots, s\}$ is a free submodule of V of rank s whose reduction is $\overline{X}$. Among these free submodules, we determine the number of totally isotropic free submodules by counting the choices of $\vec{m}_a \in M^{2\nu}$ for all $a \in \{1,2,\ldots,s\}$ such that $\beta(\vec{x}_i+\vec{m}_i,\vec{x}_j+\vec{m}_j)=0$ for all $i,j \in \{1,2,\ldots,s\}$. Since (V,β) is symplectic, $\beta(\vec{x}_i+\vec{m}_i,\vec{x}_i+\vec{m}_i)=0$ and if $\beta(\vec{x}_i+\vec{m}_i,\vec{x}_j+\vec{m}_j)=0$, then $\beta(\vec{x}_j+\vec{m}_j,\vec{x}_i+\vec{m}_i)=0$ for all $i,j \in \{1,2,\ldots,s\}$. Hence, we choose $\vec{m}_a \in M^{2\nu}$ for all $a \in \{1,2,\ldots,s\}$ satisfying the system of $\binom{s}{2}$ equations

$$\beta(\vec{x}_i+\vec{m}_i,\vec{x}_j+\vec{m}_j)=0 \ \text{ for all } i,j \in \{1,2,\ldots,s\} \text{ with } i<j.$$

We rearrange the equations by running the (i,j) as

$$(1,2),(1,3),\ldots,(1,s),(2,3),(2,4),\ldots,(2,s),(3,4),(3,5),\ldots,(3,s),\ldots,(s-1,s).$$

For each $a \in \{1,2,\ldots,s\}$, let

$$\vec{m}_a = (m_{a1},m_{a2},\ldots,m_{a\nu},m_{a(\nu+1)},m_{a(\nu+2)},\ldots,m_{a(2\nu)}),$$

where $m_{ab} \in M$ for all $b \in \{1,2,\ldots,2\nu\}$. We first arbitrarily choose $m_{ab} \in M$ for $a \in \{1,2,\ldots,s\}$, $b \in \{1,2,\ldots,\nu\}$ and $m_{a(\nu+b)}$ for $a \in \{1,2,\ldots,s\}$, $b \in \{1,2,\ldots,\nu\}$ with $a \le b$. Then we show that there are unique $m_{a(v+b)}$ for all $a \in \{1,2,\ldots,s\}$, $b \in \{1,2,\ldots,\nu\}$ and $a>b$ satisfying the above $\binom{s}{2}$ equations. Now, we have the system of $\binom{s}{2}$ linear equations $\vec{m}C=\vec{y}$ where

$$\vec{m} = (m_{2(\nu+1)},m_{3(\nu+1)},\ldots,m_{s(\nu+1)},m_{3(\nu+2)},m_{4(\nu+2)},\ldots,m_{s(\nu+2)},\ldots,m_{s(\nu+s-1)})$$

is an $\binom{s}{2}$-variable vector, $\vec{y} \in R^{\binom{s}{2}}$ and C is an $\binom{s}{2} \times \binom{s}{2}$ matrix over R. Consider the equation $\beta(\vec{x}_i+\vec{m}_i,\vec{x}_j+\vec{m}_j)=0$ where $i<j$. Note that

$$\begin{aligned}&\vec{x}_i+\vec{m}_i\\=&(m_{i1},\ldots,m_{i(i-1)},1+m_{ii},m_{i(i+1)},\ldots,m_{is},x_{i(s+1)}+m_{i(s+1)},\ldots,x_{i(2\nu)}+m_{i(2\nu)})\end{aligned}$$

and

$$\begin{aligned}&\vec{x}_j+\vec{m}_j\\=&(m_{j1},\ldots,m_{j(j-1)},1+m_{jj},m_{j(j+1)},\ldots,m_{js},x_{j(s+1)}+m_{j(s+1)},\ldots,x_{j(2\nu)}+m_{j(2\nu)}).\end{aligned}$$

Then

$$\begin{aligned}
&\beta(\vec{x}_i+\vec{m}_i,\vec{x}_j+\vec{m}_j)\\
=&\Big(m_{i1}(x_{j(\nu+1)}+m_{j(\nu+1)})+\cdots+m_{i(i-1)}(x_{j(\nu+i-1)}+m_{j(\nu+i-1)})\\
&+(1+m_{ii})(x_{j(\nu+i)}+m_{j(\nu+i)})+m_{i(i+1)}(x_{j(\nu+i+1)}+m_{j(\nu+i+1)})\\
&+\cdots+(x_{i\nu}+m_{i\nu})(x_{j(2\nu)}+m_{j(2\nu)})\Big)\\
-&\Big(m_{j1}(x_{i(\nu+1)}+m_{i(\nu+1)})+\cdots+m_{j(j-1)}(x_{i(\nu+j-1)}+m_{i(\nu+j-1)})\\
&+(1+m_{jj})(x_{i(\nu+j)}+m_{i(\nu+j)})+m_{j(j+1)}(x_{i(\nu+j+1)}+m_{i(\nu+j+1)})\\
&+\cdots+(x_{j\nu}+m_{j\nu})(x_{i(2\nu)}+m_{i(2\nu)})\Big).
\end{aligned}$$

Thus, the coefficient of $m_{a(\nu+b)}$ for $a\in\{1,2,\ldots,s\}$, $b\in\{1,2,\ldots,\nu\}$ with $a>b$ is $1+m_{ii}\in R^\times$ if $a=j$ and $b=i$, and is in M otherwise. Hence, $C=(c_{ij})$ where $c_{ij}\in R^\times$ if $i=j$ and $c_{ij}\in M$, otherwise. Clearly, $\pi(C)=I_{\binom{s}{2}}$. So $\operatorname{rk} C=\operatorname{rk}\pi(C)=\binom{s}{2}$. By Lemma 1.4.3, the system of $\binom{s}{2}$ equations has a unique solution. Thus, there are unique $m_{a(v+b)}$ for all $a\in\{1,2,\ldots,s\}$, $b\in\{1,2,\ldots,\nu\}$ and $a>b$ such that the $\binom{s}{2}$ equations hold. It follows that there are $|M|^{2\nu s-\binom{s}{2}}$ choices for $\vec{m}_a\in M^{2\nu}$ for all $a\in\{1,2,\ldots,s\}$ such that $\beta(\vec{x}_i+\vec{m}_i,\vec{x}_j+\vec{m}_j)=0$ for all $i,j\in\{1,2,\ldots,s\}$. By Theorem 1.5.1 (2), the number of free totally isotropic submodules of V of rank s whose reduction is $\overline{X}$ is

$$\frac{|M|^{2\nu s-\binom{s}{2}}}{|M|^{s^2}}=|M|^{2\nu s-\binom{s}{2}-s^2}.$$

This shows that each totally isotropic subspace of V' of dimension s can be lifted to $|M|^{2\nu s-\binom{s}{2}-s^2}$ totally isotropic free submodules of V of rank s. Therefore, the number of totally isotropic free submodules of V of rank s is $|M|^{2\nu s-\binom{s}{2}-s^2}n_{S_k}(2\nu,s)$ as desired. □

We have seen that the vertices of a generalized symplectic graph over a finite local ring relate to the vertices of the graph over its residue field. The following theorem gives the relation of the adjacency conditions of those two generalized symplectic graphs.

Theorem 2.2.2 (Lifting Theorem)**.** *Let R be a finite local ring with maximal ideal M and residue field $k = R/M$, (V, β) a symplectic space over R of rank 2ν where $\nu \geq 1$, $1 \leq s \leq \nu$ and r, t satisfy* $\max\{0, s+t-\nu\} \leq r \leq t$ *and* $1 \leq t \leq s$. *Let $\kappa = n_{S_k}(2\nu, s)$ and $\{\vec{x}_i^{(1)}\}_{i=1}^s, \{\vec{x}_i^{(2)}\}_{i=1}^s, \ldots, \{\vec{x}_i^{(\kappa)}\}_{i=1}^s$ be sets of vectors in V such that $\{\bigoplus_{i=1}^s k\pi(\vec{x}_i^{(1)}), \bigoplus_{i=1}^s k\pi(\vec{x}_i^{(2)}), \ldots, \bigoplus_{i=1}^s k\pi(\vec{x}_i^{(\kappa)})\}$ is the vertex set of $\mathscr{S}_k(2\nu, s, r, t)$. For each $j \in \{1, 2, \ldots, \kappa\}$, we write $\bigoplus_{i=1}^s R(\vec{x}_i^{(j)} + M^{2\nu})$ for the set*

$$\left\{ \bigoplus_{i=1}^{s} R(\vec{x}_i^{(j)} + \vec{m}_i^{(j)}) : \vec{m}_i^{(j)} \in M^{2\nu} \text{ and } \beta(\vec{x}_l^{(j)} + \vec{m}_l^{(j)}, \vec{x}_{l'}^{(j)} + \vec{m}_{l'}^{(j)}) = 0 \right.$$
$$\left. \text{for all } i, l, l' \in \{1, 2, \ldots, s\} \right\}.$$

Then the following statements hold.

(1) The set $\left\{\bigoplus_{i=1}^s R(\vec{x}_i^{(1)} + M^{2\nu}), \bigoplus_{i=1}^s R(\vec{x}_i^{(2)} + M^{2\nu}), \ldots, \bigoplus_{i=1}^s R(\vec{x}_i^{(\kappa)} + M^{2\nu})\right\}$ is a partition of the vertex set of $\mathscr{S}_R(2\nu, s, r, t)$. Moreover, any two distinct vertices in $\bigoplus_{i=1}^s R(\vec{x}_i^{(j)} + M^{2\nu})$ are non-adjacent vertices for all $j \in \{1, 2, \ldots, \kappa\}$.

(2) The cardinality of $\bigoplus_{i=1}^s R(\vec{x}_i^{(j)} + M^{2\nu})$ is $|M|^{2\nu s - \binom{s}{2} - s^2}$ for all $j \in \{1, 2, \ldots, \kappa\}$.

(3) For two vertices X and Y of $\mathscr{S}_R(2\nu, s, r, t)$, X is adjacent to Y if and only if $\pi(X)$ is adjacent to $\pi(Y)$ in $\mathscr{S}_k(2\nu, s, r, t)$.

(4) For $j, j' \in \{1, 2, \ldots, \kappa\}$, if $\bigoplus_{i=1}^s k\pi(\vec{x}_i^{(j)})$ is adjacent to $\bigoplus_{i=1}^s k\pi(\vec{x}_i^{(j')})$ in $\mathscr{S}_k(2\nu, s, r, t)$, then X is adjacent to X' for all $X \in \bigoplus_{i=1}^s R(\vec{x}_i^{(j)} + M^{2\nu})$ and $X' \in \bigoplus_{i=1}^s R(\vec{x}_i^{(j')} + M^{2\nu})$.

Proof. The first part of (1) follows from Theorem 1.5.1 (2) and the fact that if X is a totally isotropic free submodule of V of rank s, then $\pi(X)$ is a totally isotropic subspace of V' of dimension s. Next, let $X = \bigoplus_{i=1}^s R(\vec{x}_i^{(j)} + \vec{m}_i^{(j)})$ and $X' = \bigoplus_{i=1}^s R(\vec{x}_i^{(j)} + \vec{n}_i^{(j)})$ be two vertices in a partite set $\bigoplus_{i=1}^s R(\vec{x}_i^{(j)} + M^{2\nu})$ for some $j \in \{1, 2, \ldots, \kappa\}$. Then $\pi(X) = \bigoplus_{i=1}^s k\pi(\vec{x}_i^{(j)}) = \pi(X')$. By Lemma 1.4.4, we obtain $\operatorname{rk} \beta(X, X') = \operatorname{rk} \pi(\beta(X, X')) = \operatorname{rk} \beta'(\pi(X), \pi(X')) = 0$ and $\operatorname{rk} \begin{pmatrix} X \\ X' \end{pmatrix} =$

$\operatorname{rk}\begin{pmatrix}\pi(X)\\ \pi(X')\end{pmatrix} = \operatorname{rk}\pi(X) = s$, so X is not adjacent to X'. This proves (1). For (3), we note that X is adjacent to Y if and only if $\operatorname{rk}\beta(X,Y) = r$ and $\operatorname{rk}\begin{pmatrix}X\\ Y\end{pmatrix} = s+t$ if and only if $\operatorname{rk}\pi(\beta(X,Y)) = \operatorname{rk}\beta'(\pi(X),\pi(Y)) = r$ and $\operatorname{rk}\pi\begin{pmatrix}X\\ Y\end{pmatrix} = \operatorname{rk}\begin{pmatrix}\pi(X)\\ \pi(Y)\end{pmatrix} = s+t$ if and only if $\pi(X)$ is adjacent to $\pi(Y)$ in $\mathscr{S}_k(2\nu,s,r,t)$. Finally, (2) follows from Theorem 2.2.1 and (4) follows from (3). $\square$

The lifting theorem can be used to determine the degree of a vertex of our graphs.

Theorem 2.2.3. *Let R be a finite local ring with unique maximal ideal M and residue field $k = R/M$, (V,β) a symplectic space of rank 2ν where $\nu \geq 1$, $1 \leq s \leq \nu$ and r,t satisfy $\max\{0, s+t-\nu\} \leq r \leq t$ and $1 \leq t \leq s$. Then the generalized symplectic graph of V of type (s,r,t) has $|M|^{2\nu s-\binom{s}{2}-s^2} n_{S_k}(2\nu,s)$ vertices and it is regular of degree $|M|^{2\nu s-\binom{s}{2}-s^2} d_{S_k}(r,t)$.*

Proof. Let X be any vertex in $\mathscr{S}_R(2\nu,s,r,t)$. Then $\pi(X)$ is a vertex in $\mathscr{S}_k(2\nu,s,r,t)$ of degree $d_{S_k}(r,t)$. By the lifting theorem, X has degree $|M|^{2\nu s-\binom{s}{2}-s^2} d_{S_k}(r,t)$. Thus, $\mathscr{S}_R(2\nu,s,r,t)$ is regular of degree $|M|^{2\nu s-\binom{s}{2}-s^2} d_{S_k}(r,t)$. $\square$

Next, we find the automorphism group of our generalized symplectic graph over a finite local ring. It can be described by the automorphism group of the generalized symplectic graph over its residue field based on the idea of Theorem 4.2 of [15].

Theorem 2.2.4. *Let R be a finite local ring with unique maximal ideal M and residue field $k = R/M$, (V,β) a symplectic space of rank 2ν, $\nu \geq 1$, $1 \leq s \leq \nu$ and r,t satisfy $\max\{0, s+t-\nu\} \leq r \leq t$ and $1 \leq t \leq s$. Then*

$$\operatorname{Aut}\big(\mathscr{S}_R(2\nu,s,r,t)\big) \cong \operatorname{Aut}\big(\mathscr{S}_k(2\nu,s,r,t)\big) \times \big(\operatorname{Sym}(|M|^{2\nu s-\binom{s}{2}-s^2})\big)^{n_{S_k}(2\nu,s)}.$$

Proof. Let $\bigoplus_{i=1}^{s} R\vec{x}_i^{(1)}, \bigoplus_{i=1}^{s} R\vec{x}_i^{(2)}, \ldots, \bigoplus_{i=1}^{s} R\vec{x}_i^{(\kappa)}$ be vertices in $\mathscr{S}_R(2\nu, s, r, t)$ such that the vertex set of $\mathscr{S}_k(2\nu, s, r, t)$ is

$$\left\{ \bigoplus_{i=1}^{s} k\pi(\vec{x}_i^{(j)}) : j \in \{1, 2, \ldots, \kappa\} \right\},$$

where $\kappa = n_{S_k}(2\nu, s)$. The lifting theorem shows that the subgraph of $\mathscr{S}_R(2\nu, s, r, t)$ induced from the vertex set $\big\{ \bigoplus_{i=1}^{s} R\vec{x}_i^{(j)} : j \in \{1, 2, \ldots, \kappa\} \big\}$ is isomorphic to the graph $\mathscr{S}_k(2\nu, s, r, t)$. Moreover, each automorphism of $\mathscr{S}_R(2\nu, s, r, t)$ corresponds with an automorphism of the graph $\mathscr{S}_k(2\nu, s, r, t)$ and a permutation of vertices in the set $\bigoplus_{i=1}^{s} R(\vec{x}_i^{(j)} + M^{2\nu})$ for all $j \in \{1, 2 \ldots, \kappa\}$. Hence,

$$\begin{aligned} \mathrm{Aut}\big(\mathscr{S}_R(2\nu, s, r, t)\big) &\cong \mathrm{Aut}\big(\mathscr{S}_k(2\nu, s, r, t)\big) \times \prod_{j=1}^{\kappa} \mathrm{Sym}\big(\big| \bigoplus_{i=1}^{s} R(\vec{x}_i^{(j)} + M^{2\nu}) \big|\big) \\ &= \mathrm{Aut}\big(\mathscr{S}_k(2\nu, s, r, t)\big) \times \big(\mathrm{Sym}(|M|^{2\nu s - \binom{s}{2} - s^2})\big)^{\kappa} \end{aligned}$$

because $|\bigoplus_{i=1}^{s} R(\vec{x}_i^{(j)} + M^{2\nu})| = |M|^{2\nu s - \binom{s}{2} - s^2}$ for all $j \in \{1, 2 \ldots, \kappa\}$. $\square$

Finally, we prove that our graph is arc transitive.

Theorem 2.2.5. *A generalized symplectic graph over a finite local ring R is arc transitive.*

Proof. Let $\bigoplus_{i=1}^{s} R\vec{x}_i^{(1)}, \bigoplus_{i=1}^{s} R\vec{x}_i^{(2)}, \ldots, \bigoplus_{i=1}^{s} R\vec{x}_i^{(\kappa)}$ be vertices in a generalized symplectic graph $\mathscr{S}_R(2\nu, s, r, t)$ over R such that the vertex set of the generalized symplectic graph $\mathscr{S}_k(2\nu, s, r, t)$ over the residue field k of R is

$$\left\{ \bigoplus_{i=1}^{s} k\pi(\vec{x}_i^{(j)}) : j \in \{1, 2, \ldots, \kappa\} \right\},$$

where $\kappa = n_{S_k}(2\nu, s)$. The lifting theorem shows that the subgraph H of the graph $\mathscr{S}_R(2\nu, s, r, t)$ induced from the vertex set $\big\{ \bigoplus_{i=1}^{s} R\vec{x}_i^{(j)} : j \in \{1, 2, \ldots, \kappa\} \big\}$ is isomorphic to the generalized symplectic graph $\mathscr{S}_k(2\nu, s, r, t)$. To prove that $\mathscr{S}_R(2\nu, s, r, t)$ is arc transitive, let A, B, C, D be vertices in $\mathscr{S}_R(2\nu, s, r, t)$ such that A is adjacent to B and C is adjacent to D. Then $A \in \bigoplus_{i=1}^{s} R(\vec{x}_i^{(a)} + M^{2\nu})$, $B \in \bigoplus_{i=1}^{s} R(\vec{x}_i^{(b)} + M^{2\nu})$, $C \in \bigoplus_{i=1}^{s} R(\vec{x}_i^{(c)} + M^{2\nu})$ and $D \in \bigoplus_{i=1}^{s} R(\vec{x}_i^{(d)} + M^{2\nu})$ for some $a, b, c, d \in \{1, \ldots, \kappa\}$ with $a \neq b$ and $c \neq d$. Hence, $\pi(A) = \bigoplus_{i=1}^{s} k\pi(\vec{x}_i^{(a)})$ is adjacent to $\pi(B) = \bigoplus_{i=1}^{s} k\pi(\vec{x}_i^{(b)})$ and $\pi(C) = \bigoplus_{i=1}^{s} k\pi(\vec{x}_i^{(c)})$ is adjacent to $\pi(D) = \bigoplus_{i=1}^{s} k\pi(\vec{x}_i^{(d)})$. Since $\mathscr{S}_k(2\nu, s, r, t)$ is arc transitive, there exists an automorphism $T \in \mathrm{Aut}(\mathscr{S}_k(2\nu, s, r, t))$ such that $T(\pi(A)) = \pi(C)$ and $T(\pi(B)) = \pi(D)$. Thus, T is also an automorphism on the subgraph H which maps $\bigoplus_{i=1}^{s} R\vec{x}_i^{(a)}$ to $\bigoplus_{i=1}^{s} R\vec{x}_i^{(c)}$ and $\bigoplus_{i=1}^{s} R\vec{x}_i^{(b)}$ to $\bigoplus_{i=1}^{s} R\vec{x}_i^{(d)}$.

Finally, for $\alpha \in \{a, b, c, d\}$, we let σ_α be a permutation on $\bigoplus_{i=1}^{s} R(\vec{x}_i^{(\alpha)} + M^{2\nu})$ such that $\sigma_a(A) = \bigoplus_{i=1}^{s} R\vec{x}_i^{(a)}$, $\sigma_b(B) = \bigoplus_{i=1}^{s} R\vec{x}_i^{(b)}$, $\sigma_c(C) = \bigoplus_{i=1}^{s} R\vec{x}_i^{(c)}$ and $\sigma_d(D) = \bigoplus_{i=1}^{s} R\vec{x}_i^{(d)}$. For $\alpha \in \{1, \ldots, \kappa\} \smallsetminus \{a, b, c, d\}$, let σ_α be the identity permutation on $\bigoplus_{i=1}^{s} R(\vec{x}_i^{(\alpha)} + M^{2\nu})$. By Theorem 2.2.4, the map $T \times \prod_{i=1}^{\kappa} \sigma_i$ is an automorphism on $\mathscr{S}_R(2\nu, s, r, t)$ and it carries A to C and B to D as desired. $\square$

2.3 Over Finite Commutative Rings

In this section, we finally present the results of generalized symplectic graphs over finite commutative rings. We shall see shortly that the root of the graphs over finite commutative rings consists of the graphs over finite local rings. Certainly, the number of vertices is discussed. The decomposition of the graph over a finite commutative ring is exposed at last.

Let R be a finite commutative ring decomposed as $R \overset{\varphi}{\cong} R_1 \times R_2 \times \cdots \times R_\ell$ where R_j is a finite local ring with maximal ideal M_j and residue field $k_j = R_j/M_j$ for all $j \in \{1, 2, \ldots, \ell\}$ and (V, β) a symplectic space of rank 2ν where $\nu \geq 1$. For convenience, we take $V = R^{2\nu}$. Then for $\vec{x} = (x_1, x_2, \ldots, x_{2\nu})$ and $\vec{y} = (y_1, y_2, \ldots, y_{2\nu})$ in V,

$$\begin{aligned} \beta(\vec{x}, \vec{y}) &= \beta\big((x_1, x_2, \ldots, x_{2\nu}), (y_1, y_2, \ldots, y_{2\nu})\big) \\ &= \Big(\beta_1\big(\rho_1(\vec{x}), \rho_1(\vec{y})\big), \beta_2\big(\rho_2(\vec{x}), \rho_2(\vec{y})\big), \ldots, \beta_\ell\big(\rho_\ell(\vec{x}), \rho_\ell(\vec{y})\big)\Big), \end{aligned}$$

where β_j is an associate bilinear form on $V_j := R_j^{2\nu}$ for all $j \in \{1, 2, \ldots, \ell\}$. So $\beta(\vec{x}, \vec{y}) = 0 \in R$ if and only if $\beta_j\big(\rho_j(\vec{x}), \rho_j(\vec{y})\big) = 0 \in R_j$ for all $j \in \{1, 2, \ldots, \ell\}$. Together with Lemma 1.5.2, we have a free submodule X of V is a totally isotropic free submodule of rank s if and only if $\rho_j(X)$ is a totally isotropic free submodule of V_j of rank s for all $j \in \{1, 2, \dots, \ell\}$. Thus, by Theorem 2.2.1, we can conclude that the number of totally isotropic free submodules of V of rank s is

$$\prod_{j=1}^{\ell} |M_j|^{2\nu s - \binom{s}{2} - s^2} n_{S_{k_j}}(2\nu, s).$$

Now, we assume that $1 \leq s \leq \nu$ and let r, t satisfy $\max\{0, s+t-\nu\} \leq r \leq t$ and $1 \leq t \leq s$. The above number is the number of vertices of the graph $\mathscr{S}_R(2\nu, s, r, t)$. Note that, under the isomorphism φ, we can view each vertex X of the graph $\mathscr{S}_R(2\nu, s, r, t)$ as $\big(\rho_1(X), \rho_2(X), \dots, \rho_\ell(X)\big)$ where $\rho_j(X)$ is a totally isotropic free submodule of V_j of rank s for all $j \in \{1, 2, \dots, \ell\}$. In other words, we have

$$\Big\{\big(\rho_1(Z), \rho_2(Z), \dots, \rho_\ell(Z)\big) : Z \text{ is a totally isotropic free submodule of } V \text{ of rank } s\Big\}$$

is the vertex set of $\mathscr{S}_R(2\nu, s, r, t)$.

Suppose that $X = \big(\rho_1(X), \rho_2(X), \dots, \rho_\ell(X)\big)$ and $Y = \big(\rho_1(Y), \rho_2(Y), \dots, \rho_\ell(Y)\big)$ be two vertices in $\mathscr{S}_R(2\nu, s, r, t)$. By Lemma 1.4.6, it implies that

$$\begin{aligned}
&X \text{ is adjacent to } Y \\
&\qquad \Leftrightarrow \operatorname{rk} \beta(X, Y) = r \text{ and } \operatorname{rk} \begin{pmatrix} X \\ Y \end{pmatrix} = s + t, \\
&\qquad \Leftrightarrow \min_{1 \leq j \leq \ell} \operatorname{rk} \beta_j\big(\rho_j(X), \rho_j(Y)\big) = r \text{ and } \min_{1 \leq j \leq \ell} \operatorname{rk} \begin{pmatrix} \rho_j(X) \\ \rho_j(Y) \end{pmatrix} = s + t. \qquad (2.1)
\end{aligned}$$

Under this set-up, we proceed to prove the following decomposition theorem.

Theorem 2.3.1. *Let R be a finite commutative ring decomposed as $R \cong R_1 \times R_2 \times \cdots \times R_\ell$ where R_j is a finite local ring, (V, β) a symplectic space of rank 2ν, $\nu \geq 1$, $1 \leq s \leq \nu$. Then the generalized symplectic graph $\mathscr{S}_R(2\nu, s, r, t)$ can be decomposed into a family of subgraphs*

$$\mathscr{S}_{R_1}(2\nu, s, r_1, t_1) \otimes \mathscr{S}_{R_2}(2\nu, s, r_2, t_2) \otimes \cdots \otimes \mathscr{S}_{R_\ell}(2\nu, s, r_\ell, t_\ell)$$

where $1 \leq t_j \leq s$ and $\max\{0, s + t_j - \nu\} \leq r_j \leq t_j$ for all $j \in \{1, 2, \dots, \ell\}$ and $r = \min\{r_1, r_2, \dots, r_\ell\}$ and $t = \min\{t_1, t_2, \dots, t_\ell\}$. Every subgraph in this family is *arc transitive and has the same vertex set as the graph* $\mathscr{S}_R(2\nu, s, r, t)$. *In addition, the number of subgraphs in this family is*

$$(e_{0,0})^\ell - (e_{0,1})^\ell - (e_{1,0})^\ell + (e_{1,1})^\ell$$

where

$$\begin{aligned} e_{a,b} = & \frac{\big(r - s - t + \nu + 1 - (a-b)\big)\big(t - r - s + \nu + 2 + (a-b)\big)}{2} \\ & + (v - s + 1)(2s - r - \nu - b) \end{aligned}$$

for any a, b *in* $\{0, 1\}$.

Proof. Clearly, the vertex sets of $\mathscr{S}_R(2\nu, s, r, t)$ and each tensor product graph in the family are the same. We first show that the tensor product graph

$$\mathscr{G} = \mathscr{S}_{R_1}(2\nu, s, r_1, t_1) \otimes \mathscr{S}_{R_2}(2\nu, s, r_2, t_2) \otimes \cdots \otimes \mathscr{S}_{R_\ell}(2\nu, s, r_\ell, t_\ell)$$

is an arc transitive subgraph of $\mathscr{S}_R(2\nu, s, r, t)$. Let $X = \big(\rho_1(X), \rho_2(X), \ldots, \rho_\ell(X)\big)$ and $Y = \big(\rho_1(Y), \rho_2(Y), \ldots, \rho_\ell(Y)\big)$ be two vertices in $\mathscr{G}$. Assume that X is adjacent to Y. Then $\rho_j(X)$ is adjacent to $\rho_j(Y)$ in $\mathscr{S}_{R_j}(2\nu, s, r_j, t_j)$ for all $j \in \{1, 2, \ldots, \ell\}$. In other words, $\operatorname{rk} \beta_j\big(\rho_j(X), \rho_j(Y)\big) = r_j$ and $\operatorname{rk} \begin{pmatrix} \rho_j(X) \\ \rho_j(Y) \end{pmatrix} = s + t_j$ for all $j \in \{1, 2, \ldots, \ell\}$. Since $r = \min\{r_1, r_2, \ldots, r_\ell\}$ and $t = \min\{t_1, t_2, \ldots, t_\ell\}$, we obtain that X is adjacent to Y in $\mathscr{S}_R(2\nu, s, r, t)$ by (2.1). This implies that $\mathscr{G}$ is a subgraph of $\mathscr{S}_R(2\nu, s, r, t)$. From Lemma 1.7.3, we obtain

$$\operatorname{Aut}\big(\mathscr{S}_{R_1}(2\nu, s, r_1, t_1)\big) \times \operatorname{Aut}\big(\mathscr{S}_{R_2}(2\nu, s, r_2, t_2)\big) \times \cdots \times \operatorname{Aut}\big(\mathscr{S}_{R_\ell}(2\nu, s, r_\ell, t_\ell)\big) \subseteq \operatorname{Aut}(\mathscr{G}).$$

Since the graph $\mathscr{S}_{R_j}(2\nu, s, r_j, t_j)$ is arc transitive for all $j \in \{1, 2, \ldots, \ell\}$, it follows that $\mathscr{G}$ is arc transitive as desired.

To show that this family is a decomposition of our generalized symplectic graph, we let

$$\mathscr{G} = \mathscr{S}_{R_1}(2\nu, s, r_1, t_1) \otimes \mathscr{S}_{R_2}(2\nu, s, r_2, t_2) \otimes \cdots \otimes \mathscr{S}_{R_\ell}(2\nu, s, r_\ell, t_\ell)$$

and

$$\mathscr{G}' = \mathscr{S}_{R_1}(2\nu, s, r_1', t_1') \otimes \mathscr{S}_{R_2}(2\nu, s, r_2', t_2') \otimes \cdots \otimes \mathscr{S}_{R_\ell}(2\nu, s, r_\ell', t_\ell')$$

be two tensor product graphs in the family and suppose that two vertices $X = \big(\rho_1(X), \rho_2(X), \ldots, \rho_\ell(X)\big)$ and $Y = \big(\rho_1(Y), \rho_2(Y), \ldots, \rho_\ell(Y)\big)$ are adjacent in both graphs $\mathscr{G}$ and $\mathscr{G}'$. Then for each $j \in \{1, 2, \ldots, \ell\}$, $\rho_j(X)$ is adjacent to $\rho_j(Y)$ in both $\mathscr{S}_{R_j}(2\nu, s, r_j, t_j)$ and $\mathscr{S}_{R_j}(2\nu, s, r_j', t_j')$. Then $r_j = \operatorname{rk} \beta_j\big(\rho_j(X), \rho_j(Y)\big) = r_j'$ and $s + t_j = \operatorname{rk} \begin{pmatrix} \rho_j(X) \\ \rho_j(Y) \end{pmatrix} = s + t_j'$ for all $j \in \{1, 2, \ldots, \ell\}$. This forces that $\mathscr{G} = \mathscr{G}'$. Therefore, the edge sets of these tensor product graphs are disjoint.

Next, we let $X = \big(\rho_1(X), \rho_2(X), \ldots, \rho_\ell(X)\big)$ and $Y = \big(\rho_1(Y), \rho_2(Y), \ldots, \rho_\ell(Y)\big)$ be any two adjacent vertices in $\mathscr{S}_R(2\nu, s, r, t)$. By (2.1), we have

$$\min_{1 \le j \le \ell} \operatorname{rk} \beta_j\big(\rho_j(X), \rho_j(Y)\big) = r \text{ and } \min_{1 \le j \le \ell} \operatorname{rk} \begin{pmatrix} \rho_j(X) \\ \rho_j(Y) \end{pmatrix} = s + t.$$

Hence, X and Y are adjacent in the tensor product graph

$$\mathscr{S}_{R_1}(2\nu, s, r_1, t_1) \otimes \mathscr{S}_{R_2}(2\nu, s, r_2, t_2) \otimes \cdots \otimes \mathscr{S}_{R_\ell}(2\nu, s, r_\ell, t_\ell)$$

where $\operatorname{rk} \beta_j\big(\rho_j(X), \rho_j(Y)\big) = r_j$ and $\operatorname{rk} \begin{pmatrix} \rho_j(X) \\ \rho_j(Y) \end{pmatrix} = s + t_j$ for all $j \in \{1, 2, \ldots, \ell\}$.

Finally, we determine the number of subgraphs in the family by counting the ℓ-tuples of ordered pairs $\big((t_1, r_1), (t_2, r_2), \ldots, (t_\ell, r_\ell)\big)$ satisfying $1 \le t_j \le s$ and $\max\{0, s + t_j - \nu\} \le r_j \le t_j$ for all $j \in \{1, 2, \ldots, \ell\}$ and $t = \min\{t_1, t_2, \ldots, t_\ell\}$ and $r = \min\{r_1, r_2, \ldots, r_\ell\}$. Let the set U consist of ℓ-tuples of ordered pairs $\big((t_1, r_1), (t_2, r_2), \ldots, (t_\ell, r_\ell)\big)$ satisfying $1 \le t_j \le s$ and $\max\{0, s + t_j - \nu\} \le r_j \le t_j$ for all $j \in \{1, 2, \ldots, \ell\}$. For $a, b \in \{0, 1\}$, we let $E_{a,b}$ be the set of ℓ-tuples of ordered pairs $\big((t_1, r_1), (t_2, r_2), \ldots, (t_\ell, r_\ell)\big)$ in U such that $t + a \le \min\{t_1, t_2, \ldots, t_\ell\}$ and $r + b \le \min\{r_1, r_2, \ldots, r_\ell\}$. Therefore, the desired cardinality is equal to $|E_{0,0} \smallsetminus (E_{0,1} \cup E_{1,0})|$.

Now, we count the members of $E_{a,b}$. We first determine the number of (t_1, r_1) satisfying $1 \le t_1 \le s$, $\max\{0, s + t_1 - \nu\} \le r_1 \le t_1$ and $t + a \le t_1$ and $r + b \le r_1$.

Note that we have $1 \leq t \leq t+a \leq t_1$ and $0 \leq r \leq r+b \leq r_1$. Thus, (t_1, r_1) must satisfy $t+a \leq t_1 \leq s$ and $\max\{s+t_1-\nu, r+b\} \leq r_1 \leq t_1$. Since $t+a \leq t_1 \leq s$, we may write $t_1 = (t+a)+i$ for some $i \in \{0, 1, \ldots, s-(t+a)\}$ so that for each $i \in \{0, 1, \ldots, s-(t+a)\}$, we can count the choices of r_1 satisfying $\max\{s+t_1-\nu, r+b\} \leq r_1 \leq t_1$.

Case 1. $0 \leq i \leq (r+b)-s-(t+a)+\nu$. It follows that $s+t_1-\nu = s+(t+a)+i-\nu \leq s+(t+a)+(r+b)-s-(t+a)+\nu-\nu = r+b$. Then $\max\{s+t_1-\nu, r+b\} = r+b$. Thus, we choose r_1 such that $r+b \leq r_1 \leq (t+a)+i$ and so there are $(t+a)+i-(r+b)+1 = t-r+1+(a-b)+i$ choices of r_1.

Case 2. $s-(t+a) \geq i \geq (r+b)-s-(t+a)+\nu+1$. Then $s+t_1-\nu = s+(t+a)+i-\nu \geq s+(t+a)+(r+b)-s-(t+a)+\nu+1-\nu = (r+b)+1 \geq r+b$. This forces that $\max\{s+t_1-\nu, r+b\} = s+t_1-\nu$. Thus, we choose r_1 such that $s+t_1-\nu \leq r_1 \leq t_1$ and so there are $\nu-s+1$ choices for r_1.

From both cases, we have the number of (t_1, r_1) is

$$\begin{aligned} e_{a,b} := & \sum_{i=0}^{r-s-t+\nu-(a-b)} \big(t-r+1+(a-b)+i\big) + \sum_{i=r-s-t+\nu+1-(a-b)}^{s-t-a} (\nu-s+1) \\ = & \frac{\big(r-s-t+\nu+1-(a-b)\big)\big(t-r-s+\nu+2+(a-b)\big)}{2} \\ & + (v-s+1)\big(2s-r-\nu-b\big). \end{aligned}$$

For other $j \in \{2, 3, \ldots, \ell\}$, the number of (t_j, r_j) can be obtained in the same way and they also equal $e_{a,b}$. Hence, $|E_{a,b}| = (e_{a,b})^{\ell}$. Therefore,

$$\begin{aligned} |E| &= |E_{0,0} \smallsetminus (E_{0,1} \cup E_{1,0})| \\ &= |E_{0,0}| - |E_{0,1}| - |E_{1,0}| + |E_{1,1}| \\ &= (e_{0,0})^{\ell} - (e_{0,1})^{\ell} - (e_{1,0})^{\ell} + (e_{1,1})^{\ell}. \end{aligned}$$

This completes the proof of the theorem. $\square$

CHAPTER III

GENERALIZED ORTHOGONAL GRAPHS

In this chapter, we present nice analogous results of the graphs in the orthogonal case. Generalized orthogonal graphs over finite commutative rings of odd characteristic behave in the same way as generalized symplectic graphs. Again, we classify the study into three cases: over finite fields, over finite local rings and over finite commutative rings of odd characteristic. Most results and their proofs are analogous to the symplectic case. In what are different, the number of vertices and the degrees of the graphs are showed. In fact, the key for the outcomes is Theorem 3.2.2 which will be proved in detail. Many results follow afterward.

We have seen that studying graphs on symplectic space is more convenient since this space has a nice basis as discussed in the previous chapter. Similarly, it was showed in [16] that an orthogonal space over a finite local ring of odd characteristic also has an effective basis.

Let R be a finite local ring of odd characteristic with unique maximal ideal M and let (V_δ, β) be an orthogonal space of rank $2\nu+\delta$, where $\nu \geq 1$ and $\delta \in \{0,1,2\}$. Then (V_δ, β) possesses a basis $\mathcal{B} = \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_{2\nu+\delta}\}$ such that

$$\Big(\beta\Big)_{\mathcal{B}} = \begin{pmatrix} 0 & I_\nu & \\ I_\nu & 0 & \\ & & \Delta \end{pmatrix},$$

where

$$\Delta = \begin{cases} \varnothing \text{ (disappear)} & \text{if } \delta = 0, \\ (1) \text{ or } (z) & \text{if } \delta = 1, \\ \operatorname{diag}(1, -z) & \text{if } \delta = 2, \end{cases}$$

and z is a fixed non-square unit in R. We denote this matrix by L. Thus, if $\vec{x} = x_1\vec{b}_1 + x_2\vec{b}_2 + \cdots + x_{2\nu+\delta}\vec{b}_{2\nu+\delta}$ and $\vec{y} = y_1\vec{b}_1 + y_2\vec{b}_2 + \cdots + y_{2\nu+\delta}\vec{b}_{2\nu+\delta}$ in V_δ, then

$$\begin{aligned}\beta(\vec{x},\vec{y}) &= (x_1, x_2, \ldots, x_{2\nu+\delta})L(y_1, y_2, \ldots, y_{2\nu+\delta})^{\mathrm{T}} \\ &= \begin{cases} \sum_{i=1}^{\nu}(x_i y_{\nu+i} + x_{\nu+i}y_i), & \text{if } \delta = 0, \\ \sum_{i=1}^{\nu}(x_i y_{\nu+i} + x_{\nu+i}y_i) + x_{2\nu+1}y_{2\nu+1}\Delta, & \text{if } \delta = 1, \\ \sum_{i=1}^{\nu}(x_i y_{\nu+i} + x_{\nu+i}y_i) + x_{2\nu+1}y_{2\nu+1} - zx_{2\nu+2}y_{2\nu+2}, & \text{if } \delta = 2. \end{cases}\end{aligned}$$

We apply this basis to study generalized orthogonal graphs over finite local rings, particularly, finite fields of odd characteristic.

3.1 Over Finite Fields

For generalized orthogonal graphs over $\mathbb{F}_q$ of odd characteristic, the number of vertices which is the number of totally isotropic subspaces of an orthogonal space over $\mathbb{F}_q$ is given in Corollary 6.23 in [19]. It equals to

$$n_{O_{\mathbb{F}_q}}(2\nu+\delta, s) = \frac{\prod_{i=\nu-s+1}^{\nu}(q^i - 1)(q^{i+\delta-1} + 1)}{\prod_{i=1}^{s}(q^i - 1)}$$

For two vertices X and Y of $\mathscr{O}_{\mathbb{F}_q}(2\nu+\delta, s, r, t)$,

$$X \text{ is adjacent to } Y \Leftrightarrow \operatorname{rk}\beta(X,Y) = r \text{ and } \operatorname{rk}\begin{pmatrix} X \\ Y \end{pmatrix} = s + t.$$

In order to determine the degree of our graphs, we require the following lemma.

Lemma 3.1.1. [20] *Let $\mathbb{F}_q$ be a finite field of odd characteristic, (V_δ, β) be an orthogonal space of dimension $2\nu+\delta$ where $\nu \geq 1$ with $\delta \in \{0,1,2\}$ and X, X', Y, Y' totally isotropic subspaces of dimension s.*

(1) If $X \neq Y$ with $\operatorname{rk}(XLY^{\mathrm{T}}) = r$ and $\dim(X \cap Y) = s - t$, then $\max\{0, s+t-\nu\} \leq r \leq t$ and $1 \leq t \leq s$.

(2) $\operatorname{rk}(XLY^{\mathrm{T}}) = \operatorname{rk}(X'LY'^{\mathrm{T}})$ and $\dim(X \cap Y) = \dim(X' \cap Y')$ if and only if there exists a $2\nu \times 2\nu$ matrix U with $ULU^{\mathrm{T}} = L$ such that $X' = XU$ and $Y' = YU$.

As the discussion in Remark 2.1.2, we may study generalized orthogonal graphs of type (s, r, t) over finite commutative rings of odd characteristic only when $1 \leq s \leq \nu$ and r, t satisfy $\max\{0, s+t-\nu\} \leq r \leq t$ and $1 \leq t \leq s$.

Next, we can apply the previous lemma to show that our graphs are arc transitive. The proof is similar to the symplectic case (Theorem 2.1.3).

Theorem 3.1.2. *A generalized orthogonal graph over a finite field of odd characteristic is arc transitive.*

Since our graph is arc transitive, it is regular. Then, we let P be a fixed vertex in $\mathscr{O}_{\mathbb{F}_q}(2\nu+\delta, s, r, t)$. A vertex X adjacent to P is a totally isotropic subspace of V_δ of dimension s satisfying $\mathrm{rk}(PLX^{\mathrm{T}}) = r$ and $\dim(P \cap X) = s - t$. Again, Wei and Wang determined the number of these subspaces in Theorem 4.5 of [20]. We denote this number by $d_{O_{\mathbb{F}_q}}(r, t)$. We record the above discussion in the next theorem.

Theorem 3.1.3. *Let $\mathbb{F}_q$ be a finite field of odd characteristic, (V_δ, β) be an orthogonal space of dimension $2\nu+\delta$ where $\nu \geq 1$ and $\delta \in \{0,1,2\}$, $1 \leq s \leq \nu$ and r, t satisfy $\max\{0, s+t-\nu\} \leq r \leq t$ and $1 \leq t \leq s$. Then the generalized orthogonal graph of V of type (s, r, t) has*

$$n_{O_{\mathbb{F}_q}}(2\nu+\delta, s) = \frac{\prod_{i=\nu-s+1}^{\nu}(q^i-1)(q^{i+\delta-1}+1)}{\prod_{i=1}^{s}(q^i-1)}$$

vertices and it is regular of degree

$$d_{O_{\mathbb{F}_q}}(r, t) = q^{r(2(\nu-s)+\delta)+(t-r)^2+\frac{r(r+1)}{2}} \begin{bmatrix} s \\ s-t \end{bmatrix}_q \begin{bmatrix} t \\ r \end{bmatrix}_q n_{O_{\mathbb{F}_q}}(2(\nu-s)+\delta, t-r).$$

3.2 Over Finite Local Rings

In this section, we study generalized orthogonal graphs over finite local rings of odd characteristic. We start with discussing a relationship between an orthogonal space over a finite local ring and over its residue field. We use this relationship to determine the number of totally isotropic free submodules of an orthogonal space. Next, we expose the lifting theorem of generalized orthogonal graphs. Finally, we show their properties: regularities, degrees, automorphism groups and transitivities.

Let R be a finite local ring of odd characteristic with unique maximal ideal M and let (V_δ, β) be an orthogonal space of rank $2\nu+\delta$, where $\nu \geq 1$ and $\delta \in \{0,1,2\}$. An orthogonal space (V_δ, β) over R induces the orthogonal space (V'_δ, β') over k of dimension $2\nu+\delta$ where β' is given via the canonical map $\pi : R \to k$ by

$$\beta'(\pi(\vec{x}), \pi(\vec{y})) = \pi(\beta(\vec{x}, \vec{y}))$$

for all $\vec{x}, \vec{y} \in V_\delta$. As well, if X is a totally isotropic free submodule of (V_δ, β) of rank s, then $\pi(X)$ is a totally isotropic subspace of (V'_δ, β') of dimension s.

An orthogonal space (V_δ, β) with the basis presented in the first part of this chapter and the induced orthogonal space (V'_δ, β') are useful in studying our graphs, especially, the number of vertices in our graphs. To count the number of vertices in our graphs which is the number of totally isotropic free submodules of V_δ, we require the following lemma.

Lemma 3.2.1. [17] *Let R be a finite local ring of odd characteristic. Let (V_δ, β) be an orthogonal space of rank $2\nu+\delta$ with basis $\{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_{2\nu+\delta}\}$ where $\nu \geq 1$ and $\delta \in \{0,1,2\}$ and $\vec{x} = r_1\vec{b}_1 + r_2\vec{b}_2 + \cdots + r_{2\nu+\delta}\vec{b}_{2\nu+\delta} \in V_\delta$ for some $r_1, r_2, \ldots, r_{2\nu+\delta} \in R$. Then $\vec{x}$ is unimodular if and only if r_i is a unit for some $i \in \{1, 2, \ldots, 2\nu\}$.*

Now, we are ready to determine the number of totally isotropic free submodules of V_δ.

Theorem 3.2.2. *Let R be a finite local ring of odd characteristic with maximal ideal M and residue field $k = R/M$, (V_δ, β) an orthogonal space over R of rank $2\nu+\delta$, where $\nu \geq 1$ and $\delta \in \{0,1,2\}$ and $\overline{X}$ a totally isotropic subspace of the induced orthogonal space (V'_δ, β') of dimension s. Then the number of totally isotropic free submodules of V_δ of rank s whose reduction is $\overline{X}$ is $|M|^{(2\nu+\delta)s-\binom{s+1}{2}-s^2}$. Hence, the number of totally isotropic free submodules of V_δ of rank s equals*

$$|M|^{(2\nu+\delta)s-\binom{s+1}{2}-s^2} n_{O_k}(2\nu+\delta, s).$$

Proof. Lemma 3.2.1 implies that any linearly independent vector in V_δ has a unit in some coordinate in $\{1, 2, \ldots, 2\nu\}$. By elementary row operation and permuting the coordinates in $\{1, 2, \ldots, 2\nu\}$, we write $\overline{X} = \begin{pmatrix} \overline{I}_s & \overline{A} & \overline{B} \end{pmatrix}$ where $\overline{A}$ is an $s \times (2\nu - s)$ matrix and $\overline{B}$ is an $s \times \delta$ matrix over k. Then we assume that $\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_s \in V_\delta$ are such that $\overline{X} = k\pi(\vec{x}_1) \oplus k\pi(\vec{x}_2) \oplus \cdots \oplus k\pi(\vec{x}_s)$, where for each $a \in \{1, 2, \ldots, s\}$, $\vec{x}_a = (x_{a1}, \ldots, x_{a\nu}, x_{a(\nu+1)}, \ldots, x_{a(2\nu)}, x_{a(2\nu+1)}, \ldots, x_{a(2\nu+\delta)})$ with $x_{aa} = 1$ and $x_{ab} = 0$ for all $b \in \{1, \ldots, s\} \smallsetminus \{a\}$. Thus, $R(\vec{x}_1 + \vec{m}_1) \oplus R(\vec{x}_2 + \vec{m}_2) \oplus \cdots \oplus R(\vec{x}_s + \vec{m}_s)$ where $\vec{m}_a \in M^{2\nu+\delta}$ for all $a \in \{1, 2 \ldots, s\}$ is a free submodule of V_δ of rank s whose reduction is $\overline{X}$. Among these free submodules, we determine the number totally isotropic free submodules by counting the choices of $\vec{m}_a \in M^{2\nu+\delta}$ for all $a \in \{1, 2, \ldots, s\}$ such that $\beta(\vec{x}_i + \vec{m}_i, \vec{x}_j + \vec{m}_j) = 0$ for all $i, j \in \{1, 2, \ldots, s\}$. Since (V_δ, β) is orthogonal, if $\beta(\vec{x}_i + \vec{m}_i, \vec{x}_j + \vec{m}_j) = 0$, then $\beta(\vec{x}_j + \vec{m}_j, \vec{x}_i + \vec{m}_i) = 0$ for all $i, j \in \{1, 2, \ldots, s\}$. Hence, we choose $\vec{m}_a \in M^{2\nu+\delta}$ for all $a \in \{1, 2, \ldots, s\}$ satisfying the system of $\binom{s+1}{2}$ equations

$$\beta(\vec{x}_i + \vec{m}_i, \vec{x}_j + \vec{m}_j) = 0 \quad \text{for all } i, j \in \{1, 2, \ldots, s\} \text{ with } i \leq j.$$

For each $a \in \{1, 2, \ldots, s\}$, let

$$\vec{m}_a = (m_{a1}, m_{a2}, \ldots, m_{a\nu}, m_{a(\nu+1)}, m_{a(\nu+2)}, \ldots, m_{a(2\nu)}, m_{a(2\nu+1)}, \ldots, m_{a(2\nu+\delta)}),$$

where $m_{ab} \in M$ for all $b \in \{1, 2, \ldots, 2\nu + \delta\}$. We first arbitrarily choose $m_{ab} \in M$ for $a \in \{1, 2, \ldots, s\}$, $b \in \{1, 2, \ldots, \nu\}$, $m_{a(\nu+b)}$ for $a \in \{1, 2, \ldots, s\}$, $b \in \{1, 2, \ldots, \nu\}$ with $a < b$, and $m_{a(2\nu+1)}, \ldots, m_{a(2\nu+\delta)}$. Then we show that there are unique $m_{a(v+b)}$ for all $a \in \{1, 2, \ldots, s\}$, $b \in \{1, 2, \ldots, \nu\}$ and $a \geq b$ satisfying the above $\binom{s+1}{2}$ equations. Let

$$\vec{m} = (m_{1(\nu+1)}, m_{2(\nu+1)}, \ldots, m_{s(\nu+1)}, m_{2(\nu+2)}, m_{3(\nu+2)}, \ldots, m_{s(\nu+2)}, \ldots, m_{s(\nu+s)}).$$

Then we write those $\binom{s+1}{2}$ equations in an linear system $\vec{m}C = \vec{y}$ where $\vec{m}$ is an $\binom{s+1}{2}$ variable vector, C is the $\binom{s+1}{2} \times \binom{s+1}{2}$ coefficient matrix over R and $\vec{y} \in R^{\binom{s+1}{2}}$. It is similar to the proof of Theorem 2.2.1 in showing that the coefficient matrix C is of rank $\binom{s+1}{2}$. Thus, there are unique $m_{a(v+b)}$ for all $a \in \{1, 2, \ldots, s\}$, $b \in \{1, 2, \ldots, \nu\}$ and $a \geq b$ such that the $\binom{s+1}{2}$ equations hold.

Hence, there are $|M|^{(2\nu+\delta)s-\binom{s+1}{2}}$ choices for $\vec{m}_a \in M^{2\nu+\delta}$ for all $a \in \{1,2,\ldots,s\}$ such that $\beta(\vec{x}_i+\vec{m}_i, \vec{x}_j+\vec{m}_j) = 0$ for all $i,j \in \{1,2,\ldots,s\}$. By Theorem 1.5.1 (2), the number of totally isotropic free submodules of V_δ of rank s whose reduction is $\overline{X}$ is

$$\frac{|M|^{(2\nu+\delta)s-\binom{s+1}{2}}}{|M|^{s^2}} = |M|^{(2\nu+\delta)s-\binom{s+1}{2}-s^2}.$$

Therefore, the number of totally isotropic free submodules of V_δ of rank s equals

$$|M|^{(2\nu+\delta)s-\binom{s+1}{2}-s^2} n_{O_k}(2\nu+\delta, s).$$

This completes the proof. $\square$

We also have the lifting theorem for generalized orthogonal graphs over finite local rings. Its proof is analogous to the symplectic case (Theorem 2.2.2).

Theorem 3.2.3 (Lifting Theorem)**.** *Let R be a finite local ring of odd characteristic with maximal ideal M and residue field $k = R/M$, (V_δ, β) an orthogonal space over R of rank $2\nu+\delta$ where $\nu \geq 1$ and $\delta \in \{0,1,2\}$, $1 \leq s \leq \nu$ and r,t satisfy* $\max\{0, s+t-\nu\} \leq r \leq t$ *and* $1 \leq t \leq s$. *Let $\kappa = n_{O_k}(2\nu+\delta, s)$ and $\{\vec{x}_i^{(1)}\}_{i=1}^s, \{\vec{x}_i^{(2)}\}_{i=1}^s, \ldots, \{\vec{x}_i^{(\kappa)}\}_{i=1}^s$ be sets of vectors in V_δ such that the set $\{\bigoplus_{i=1}^s k\pi(\vec{x}_i^{(1)}), \bigoplus_{i=1}^s k\pi(\vec{x}_i^{(2)}), \ldots, \bigoplus_{i=1}^s k\pi(\vec{x}_i^{(\kappa)})\}$ is the vertex set of the graph $\mathscr{O}_k(2\nu+\delta, s, r, t)$. For each $j \in \{1,2,\ldots,\kappa\}$, we write $\bigoplus_{i=1}^s R(\vec{x}_i^{(j)} + M^{2\nu+\delta})$ for the set*

$$\left\{ \bigoplus_{i=1}^{s} R(\vec{x}_i^{(j)} + \vec{m}_i^{(j)}) : \vec{m}_i^{(j)} \in M^{2\nu+\delta} \textit{ and } \beta(\vec{x}_l^{(j)} + \vec{m}_l^{(j)}, \vec{x}_{l'}^{(j)} + \vec{m}_{l'}^{(j)}) = 0 \right.$$
$$\left. \textit{for all } i,l,l' \in \{1,2,\ldots,s\} \right\}.$$

Then the following statements hold.

(1) The set $\left\{\bigoplus_{i=1}^s R(\vec{x}_i^{(1)}+M^{2\nu+\delta}), \bigoplus_{i=1}^s R(\vec{x}_i^{(2)}+M^{2\nu+\delta}), \ldots, \bigoplus_{i=1}^s R(\vec{x}_i^{(\kappa)}+M^{2\nu+\delta})\right\}$ is a partition of the vertex set of $\mathscr{O}_R(2\nu+\delta, s, r, t)$. Moreover, any two distinct vertices in $\bigoplus_{i=1}^s R(\vec{x}_i^{(j)} + M^{2\nu+\delta})$ are non-adjacent vertices for all $j \in \{1,2,\ldots,\kappa\}$.

(2) The cardinality of $\bigoplus_{i=1}^{s} R(\vec{x}_i^{(j)} + M^{2\nu+\delta})$ *is* $|M|^{(2\nu+\delta)s-\binom{s+1}{2}-s^2}$ *for all* $j \in \{1, 2, \ldots, \kappa\}$.

(3) For two vertices X *and* Y *of* $\mathscr{O}_R(2\nu+\delta, s, r, t)$, X *is adjacent to* Y *if and only if* $\pi(X)$ *is adjacent to* $\pi(Y)$ *in* $\mathscr{O}_k(2\nu+\delta, s, r, t)$.

(4) For $j, j' \in \{1, 2, \ldots, \kappa\}$, *if* $\bigoplus_{i=1}^{s} k\pi(\vec{x}_i^{(j)})$ *is adjacent to* $\bigoplus_{i=1}^{s} k\pi(\vec{x}_i^{(j')})$ *in* $\mathscr{O}_k(2\nu+\delta, s, r, t)$, *then* X *is adjacent to* X' *for all* $X \in \bigoplus_{i=1}^{s} R(\vec{x}_i^{(j)} + M^{2\nu+\delta})$ *and* $X' \in \bigoplus_{i=1}^{s} R(\vec{x}_i^{(j')} + M^{2\nu+\delta})$.

The lifting theorem implies results for generalized orthogonal graphs over finite local rings similar to the symplectic case (Theorems 2.7–2.9) as follows.

Theorem 3.2.4. *Let* R *be a finite local ring of odd characteristic with unique maximal ideal* M *and residue field* $k = R/M$, (V_δ, β) *an orthogonal space over* R *of rank* $2\nu + \delta$, *where* $\nu \geq 1$ *and* $\delta \in \{0, 1, 2\}$, $1 \leq s \leq \nu$ *and* r, t *satisfy* $\max\{0, s + t - \nu\} \leq r \leq t$ *and* $1 \leq t \leq s$. *Then*

(1) The generalized orthogonal graph of V *of type* (s, r, t) *has*

$$|M|^{(2\nu+\delta)s-\binom{s+1}{2}-s^2} n_{O_k}(2\nu+\delta, s)$$

vertices and it is regular of degree

$$|M|^{(2\nu+\delta)s-\binom{s+1}{2}-s^2} d_{O_k}(r, t).$$

(2) The automorphism group of $\mathscr{O}_R(2\nu+\delta, s, r, t)$ *is*

$$\begin{aligned}\mathrm{Aut}(\mathscr{O}_R(2\nu+\delta, s, r, t)) \cong &\mathrm{Aut}(\mathscr{O}_k(2\nu+\delta, s, r, t)) \\ &\times (\mathrm{Sym}(|M|^{(2\nu+\delta)s-\binom{s+1}{2}-s^2}))^{n_{O_k}(2\nu+\delta,s)}.\end{aligned}$$

(3) The generalized orthogonal graph over R *is arc transitive.*

3.3 Over Finite Commutative Rings

Finally, we present results for generalized orthogonal graphs over finite commutative rings of odd characteristic. Again, the proof is analogous to the ones discussed in Section 2.3. We note that the number $e_{a,b}$ equals to the one in Theorem 2.3.1 since the conditions on s, r, t of Lemma 3.1.1 are the same.

Theorem 3.3.1. *Let R be a finite commutative ring of odd characteristic decomposed as $R \cong R_1 \times R_2 \times \cdots \times R_\ell$ where R_j is a finite local ring of odd characteristic with maximal ideal M_j and residue field $k_j = R_j/M_j$ for all $j \in \{1, 2, \ldots, \ell\}$, (V_δ, β) an orthogonal space over R of rank $2\nu + \delta$, where $\nu \geq 1$ and $\delta \in \{0, 1, 2\}$, $1 \leq s \leq \nu$ and r, t satisfy $\max\{0, s+t-\nu\} \leq r \leq t$ and $1 \leq t \leq s$. The generalized orthogonal graph $\mathscr{O}_R(2\nu + \delta, s, r, t)$ has*

$$\prod_{j=1}^{\ell} |M_j|^{(2\nu+\delta)s - \binom{s+1}{2} - s^2} n_{O_{k_j}}(2\nu + \delta, s)$$

vertices. It can be decomposed into a family of subgraphs

$$\mathscr{O}_{R_1}(2\nu + \delta, s, r_1, t_1) \otimes \mathscr{O}_{R_2}(2\nu + \delta, s, r_2, t_2) \otimes \cdots \otimes \mathscr{O}_{R_\ell}(2\nu + \delta, s, r_\ell, t_\ell)$$

where $1 \leq t_j \leq s$ and $\max\{0, s + t_j - \nu\} \leq r_j \leq t_j$ for all $j \in \{1, 2, \ldots, \ell\}$ and $r = \min\{r_1, r_2, \ldots, r_\ell\}$ and $t = \min\{t_1, t_2, \ldots, t_\ell\}$. Every subgraph in this family is arc transitive and has the same vertex set as the graph $\mathscr{O}_R(2\nu + \delta, s, r, t)$. In addition, the number of subgraphs in this family is

$$(e_{0,0})^\ell - (e_{0,1})^\ell - (e_{1,0})^\ell + (e_{1,1})^\ell$$

where

$$e_{a,b} = \frac{\big(r - s - t + \nu + 1 - (a - b)\big)\big(t - r - s + \nu + 2 + (a - b)\big)}{2} + (v - s + 1)(2s - r - \nu - b)$$

for any a, b in $\{0, 1\}$.

REFERENCES

[1] Bini, G., Flamini, F.: *Finite Commutative Rings and Their Applications*, Spring Science & Business Media, New York, 2012.

[2] Bollman, D., Ramirez H.: On the enumeration of matrices over finite commutative rings, *Amer. Math. Monthly* **76**, 1019–1023 (1969).

[3] Brawley, J.V., Carlitz, L.: Enumeration of matrices with prescribed row and column sums, *Linear Algebra Appl.* **6**, 165–174 (1973).

[4] Brown, W.C.: *Matrices over Commutative Rings*, Marcel Dekker, Inc., New York, 1993.

[5] Ching, W.S.: Linear equations over commutative rings, *Linear Algebra Appl.* **18**, 257–266 (1977).

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

[7] Gu, Z., Wan, Z.: Orthogonal graphs of odd characteristic and their automorphisms, *Finite Fileds Appl.* **14**, 291–313 (2008).

[8] Hungerford, T.W.: *Algebra*, Springer, New York, 1974.

[9] Huo, L., Zhang, G.: Subconstituents of the orthogonal graph of type $(m, m-1, 0)$ of odd characteristic, *Linear Algebra Appl.* **524**, 1–21 (2017).

[10] Li, F., Guo, J., Wang, K.: Orthogonal graphs over Galois rings of odd characteristic, *European J. Combin.* **39**, 113–121 (2014).

[11] Li, F., Wang, K., Guo, J.: Symplectic graphs modulo pq, *Discrete Math.* **313**, 650–655 (2013).

[12] McCoy, N.H.: *Rings and Ideals*, Carus Math. Monogr. No. 8, Math. Assoc. of Am., 1948.

[13] Meemark, Y., Prinyasart, T.: On symplectic graphs modulo p^n, *Discrete Math.* **311**, 1874–1878 (2011).

[14] Meemark, Y., Puirod, T.: Symplectic graphs over finite local rings, *European J. Combin.* **34**, 1114–1124 (2013).

[15] Meemark, Y., Puirod, T.: Symplectic graphs over finite commutative rings, *European J. Combin.* **41**, 298–307 (2014).

[16] Meemark, Y., Sriwongsa, S.: Cogredient standard forms of orthogonal matrices over finite local rings of odd characteristic, *arXiv:1506.06710 [math.NT]* (2015).

[17] Meemark, Y., Sriwongsa, S.: Orthogonal graphs over finite commutative rings of odd characteristic, *Finite Fields Appl.* **40**, 26–45 (2016).

[18] Tang, Z., Wan, Z.: Symplectic graphs and their automorphisms, *European J. Combin.* **27**, 38–50 (2006).

[19] Wan, Z.: *Geometry of Classical Groups over Finite Fields*, 2nd edition, Science Press, Beijing, New York, 2002.

[20] Wei, H., Wang, Y.: Suborbits of the transitive set of subspaces of type $(m, 0)$ under finite classical groups, *Algebra Colloq.* **3**, 73–84 (1996).

[21] Zeng, L., Chai, Z., Feng, R., et al.: Full automorphism group of the generalized symplectic graph, *Sci. China Math.* **56**, 1509–1520 (2013).

VITA

Name	Mr. Siripong Sirisuk
Date of Birth	23 March 1991
Place of Birth	Nakhon Si Thammarat, Thailand
Education	M.Sc. (Mathematics), Chulalongkorn University, 2015
	B.Sc. (Mathematics) (Second Class Honours), Chulalongkorn University, 2013
Scholarship	The Science Achievement Scholarship of Thailand (SAST)
Conference	Oral presentation: *Generalized bilinear form graphs over finite commutative rings*, The 7$^{\text{th}}$ International Conference on Matrix Analysis and Applications (ICMAA 2018), 22–25 June 2018, Shinshu University (Nagano Campus), Japan