Symplectic Graphs over a Finite Local Ring

Monirul Choudhury

Supervisor: Dr. James Cruickshank

Abstract

The symplectic geometry of a vector space over a finite field can be used to generate interesting examples of strongly regular graphs - informally speaking, the regularity structure of these graphs capture the inherent symmetry of the space. These graphs, so-called symplectic graphs, are well-studied in the finite field case. This project provides a survey of the literature in this setting as well as the more general setting over a finite local ring. A finite local ring possesses a natural graded structure that is inherited by a free module defined over it. We aim to capture this graded structure by introducing sequences of generalized symplectic graphs and present some basic results concerning the regularity, automorphism groups and chromatic numbers of these graphs.

Introduction

Strongly regular graphs were introduced in 1963 by Bose as graphs possessing strong structure and symmetry in the field of spectral graph theory [10]. Owing to this rare structure, enumerating interesting examples of these graphs has been a long-standing fascination among graph theorists. In an intersection between finite geometry and algebraic combinatorics, the notion of graphs derived from a symplectic vector space (so-called symplectic graphs) were introduced by Tang and Wan [2]. They showed that these graphs were strongly regular and also determined their automorphism groups and chromatic numbers. In recent years, these results have been generalized to the case of finite local rings [3][4]. In this setting, it was found that the associated symplectic graph inherited much of the structure from the case with finite fields but was generally no longer strongly regular. In Chapter 2, we discuss these results as part of a review of the topic of symplectic graphs. Finally, in Chapter 3, we introduce a generalized symplectic graph defined over a particular class of finite local rings. We refer to these as sequences of symplectic graphs and investigate their chromatic numbers and automorphism groups. The appendix contains some basic results concerning graph and ring theory that are a prerequisite for this project. We also include an implementation of a method to generate symplectic graphs in SageMath.

Chapter 1: Preliminaries

1.1 Graph Theory

Here we present some basic results relating to the topic of strongly regular graphs. See [1] for further reading.

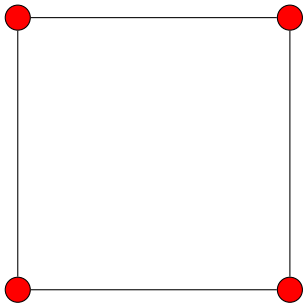
Strongly Regular Graphs

Definition: Suppose G is a graph with n vertices that is not complete nor the union of complete graphs. We say G is a $(n, k, a, c)-$strongly regular graph if:

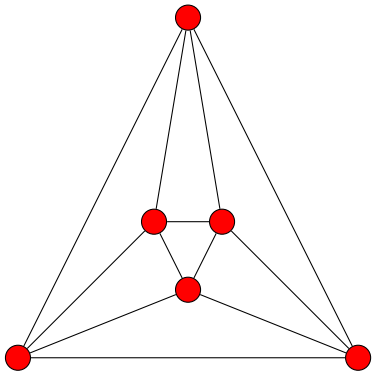
1. G is k-regular
2. any pair of adjacent vertices have a common neighbours
3. any pair of non-adjacent vertices have c common neighbours

Examples

1. The square graph is a (4, 2, 0, 2)-strongly regular graph.
2. The octahedral graph is a (6, 4, 2, 4)-strongly regular graph.



Square Graph



Octahedral Graph

From this restrictive definition, we can also generate the eigenvalues of the adjacency matrix $A(G)$, as well as the multiplicities of these eigenvalues:

Proposition 1.1 (10.2 of [1]) Let G be a (n, k, a, c) strongly regular graph with adjacency matrix A. The eigenvalues of A are given by k, θ, τ with multiplicities $1, m_\theta, m_\tau$ respectively, where:

$$\theta = \frac{(a-c) + \sqrt{(a-c)^2 + 4(k-c)}}{2}, \tau = \frac{(a-c) - \sqrt{(a-c)^2 + 4(k-c)}}{2},$$

$$m_\theta = -\frac{(n-1)\tau + k}{\theta - \tau}, m_\tau = -\frac{(n-1)\theta + k}{\theta - \tau}$$

The numbers (n, k, a, c) are referred to as the parameter set of G. Due to the rigid structure of the strongly regular graphs, there exist feasibility conditions that a parameter set must satisfy in order for a strongly regular graph with that parameter set to be possible. For instance, given possible values (n', k', a', c'), we can compute the multiplicities $m_{\theta'}, m_{\tau'}$ using the equations from above. If these values are not integers, then a strongly regular graph with that parameter set is not possible. We now define a slight generalization of a strongly regular graph.

Defintion: Suppose G is a graph with n vertices that is not complete nor the union of complete graphs. We call G a $(n, k, a, c)-$Deza graph if:

1. G is k-regular
2. any pair of distinct vertices have either a or c common neighbours

1.2 Algebra

Local Rings

The intuitive idea behind a local ring is that they provide an easy way to classify all the units of the ring. Using the axiom of choice, one can show that every non-unit of a ring is contained in a maximal ideal. If a ring R has a unique maximal ideal M, then a unit $r \in R$ can be classified by the property that $r \notin M$.

Definition: Let R be a commutative ring. If R has a unique maximal ideal M, then R is said to be a local ring.

Proposition 1.2 Let R be a local ring with maximal ideal M. If $r \in R$, then either $r \in M$ or r is a unit of R.

Example: Let p be a prime number and n a positive integer. Then $\mathbb{Z}_{p^n}$ is a local ring with maximal ideal (p). The residue field is $\mathbb{Z}_p$.

Let R be a finite local ring with maximal ideal M. R possesses a natural stratification in the following way. For $k \geq 1$ an integer, define M^k to be the ideal generated by k elements in M. Since R is finite, there exists a positive integer n such that $M^n = \{0\}$. Then the stratification on R is given by:

$$R \setminus M \subset M \setminus M^2 \subset ... \subset M^{n-1} \setminus M^n$$

Roughly speaking, this containment determines "how close an element is to be a unit in R". Units are contained in R/M and the further we move to the right,

the further an element is to be a unit. For example, let $R = \mathbb{Z}_{p^n}$ for a prime number p and an integer $n \geq 2$. Note $(p)^k = (p^k)$. The stratification on this ring is given by:

$$\mathbb{Z}_{p^n} \setminus (p) \subset (p) \setminus (p^2) \subset ... \subset (p^{n-1}) \setminus (p^n)$$

If $a \in (p^i)/(p^{i+1})$, then p^i divides a but p^{i+1} does not divide a. The following definition formalizes this concept.

Definition: Let R be a finite local ring with maximal ideal M. Let n be the least positive integer such that $M^n = \{0\}$. For $r \in R$, we define the valuation of r, denoted $v(r)$, in the following way:

$$v(r) = \begin{cases} 0, & \text{if } r \text{ is a unit in } R \\ i, & \text{if } r \in M^i \setminus M^{i+1} \text{ (for } 1 \leq i \leq n-1) \\ n, & \text{if } r = 0 \end{cases}$$

Modules

Much of the theory of vector spaces over a field can be generalized to the concept of a module over a ring. In the present text, we consider only the case where the underlying ring is commutative.

Definition: A non-empty set V is a module over a commutative ring R if V is an abelian group under an operation $+$ that is also equipped with maps $R \times V \to V$, $V \times R \to V$ denoted $r\vec{v}, \vec{v}r$ respectively satisfying:

1. $r(\vec{u} + \vec{v}) = r\vec{u} + r\vec{v}$
2. $r(s\vec{v}) = (rs)\vec{v}$
3. $(r + s)\vec{v} = r\vec{v} + s\vec{v}$
4. $r\vec{v} = \vec{v}r$

for all $\vec{u}, \vec{v} \in V$ and $r, s \in R$.

Definition: Let V, W be R-modules. A map $T : V \to W$ is an $R-$module morphism if for all $\vec{v_1}, \vec{v_2}, \vec{v} \in V$:

- $T(\vec{v_1} + \vec{v_2}) = T(\vec{v_1}) + T(\vec{v_2})$
- $T(r\vec{v}) = rT(\vec{v})$

If T is bijective, then T is an isomorphism between V and W.

In general, modules over a ring may not have a basis. Modules with a basis are called free modules. If every basis of a module V is of the same cardinality n (this is also not guaranteed), then we call V a free module of rank n.

Example:

1. Trivial examples include R as an $R-$module over itself, and $R^n = \{(a_1, a_2, ..., a_n) : a_i \in R\}$ with component-wise addition and scalar multiplication.

2. Let $R = \mathbb{Z}$. If G is an abelian group, then we can turn G into a Z-module by defining for any $n \in \mathbb{Z}, g \in G$:

$$ng = \begin{cases} g + g + ... + g \ (n \text{ times}), & \text{if } n > 0 \\ 0, & \text{if } n = 0 \\ -g - g - ... - g \ (n \text{ times}), & \text{if } n < 0 \end{cases}$$

3. Let $R = \mathbb{Z}_4$ and consider the free module of rank 2, R^2. A basis for this module is $\{(0,1),(1,0)\}$. In the field case, any non-zero vector can be turned into a basis vector. In this more general setting, this is no longer true. For instance, consider $(0,2)$. Let (a_1, a_2) be some other vector and now consider the linear combinations of $\{(0,2),(a_1,a_2)\}$:

$$c_1(0,2) + c_2(a_1,a_2) = (c_2a_1, 2c_1 + c_2a_2)$$

   Note that the vectors (0,1) and (1,0) cannot be simultaneously constructed from this combination and thus (0,2) is never a part of a basis of R^2.

A vector $\vec{v} \in V$ that is part of a basis of V is called a unimodular vector. Unimodular vectors are particularly important when studying the theory of symplectic forms over local rings, so we provide the following characterization for them.

Proposition 1.3: Let V be a free module over a commutative ring R. Let $\{\vec{v_1}, \vec{v_2}, ..., \vec{v_n}\}$ be a basis of V. Let $\vec{v} = x_1\vec{v_1} + x_2\vec{v_2} + ... + x_n\vec{v_n}$. Then the following are equivalent:

1. There exists an $R-$module morphism $T : V \to R$ with $T(\vec{v}) = 1$

2. The ideal $(x_1, x_2, ..., x_n) = R$

3. $\vec{v}$ is unimodular

Proof: $1 \Rightarrow 2$: Suppose the R-modular morphism $T : V \to R$ satisfies $T(\vec{v}) = 1$. Then $T(x_1\vec{v_1} + x_2\vec{v_2} + ... + x_n\vec{v_n}) = x_1T(\vec{v_1}) + x_2T(\vec{v_2}) + ...x_nT(\vec{v_n}) = 1$, where each $T(\vec{v_i}) \in R$ for $i = 1, 2, ..., n$. Thus $(x_1, x_2, ..., x_n) = R$.
$2 \Rightarrow 1$: Suppose $(x_1, x_2, ..., x_n) = R$. Then there exists $y_1, y_2, ..., y_n \in R$ such that $x_1y_1 + x_2y_2 + ... + x_ny_n = 1$. If we let $T : V \to R$ be the R-module morphism such that $T(\vec{v_i}) = y_i$ for $i = 1, 2, ..., n$, then $T(\vec{v}) = 1$.
$2 \Rightarrow 3$: If $(x_1, x_2, ..., x_n) = R$, then $x_i \in R^\times$ for $i = 1, 2, ..., n$. Thus we can write: $\vec{v_i} = x_i^{-1}(\vec{v} - x_1\vec{v_1} - ... - x_{i-1}\vec{v_{i-1}} - x_{i+1}\vec{v_{i+1}} - ... - x_n\vec{v_n})$. Then it can be shown that $\{\vec{v}, \vec{v_1}, ..., \vec{v_{i-1}}, \vec{v_{i+1}}, ..., \vec{v_n}\}$ is a basis of V.

$3 \Rightarrow 1$: Suppose $\{\vec{v}, \vec{w_1}, ..., \vec{w_m}\}$ is a basis of V. Then we can define the R-module morphism $T : V \to R$ by $T(\vec{v}) = 1$ and $T(\vec{w_i}) = 0$ for $i = 1, 2, ..., m$.

Note that if V is a vector space over a field K, then all non-zero vectors are unimodular.

1.3 Symplectic Geometry

The central notion of this topic is that of a symplectic form. We think of this as a bilinear form that satisfies some additional properties. Intuitively, a bilinear form induces a geometry on the space that its defined over, and this is no different for a symplectic form. In the present text, we present only the necessary algebraic details of the form but direct the reader to [9] for further reading on the induced geometry.

Definition: Let R be a commmutative ring and let V be a free $R-$module. A bilinear form on V is a map $\beta : V \times V \to R$ that satisfies:

1. $\beta(\vec{v_1}+\vec{v_2}, \vec{w}) = \beta(\vec{v_1}, \vec{w})+\beta(\vec{v_2}, \vec{w})$ and $\beta(\vec{v}, \vec{w_1}+\vec{w_2}) = \beta(\vec{v}, \vec{w_1})+\beta(\vec{v}, \vec{w_2})$
2. $\beta(\lambda\vec{v}, \vec{w}) = \lambda\beta(\vec{v}, \vec{w})$ and $\beta(\vec{v}, \lambda\vec{w}) = \lambda\beta(\vec{v}, \vec{w})$

for all $\vec{v}, \vec{v_1}, \vec{v_2}, \vec{w}, \vec{w_1}, \vec{w_2} \in V$.

Definition: Let R be a commutative ring and let V be a free R-module of rank $2r$, where $r \geq 1$. A symplectic form on V is a bilinear form β that satisfies:

1. $\beta(\vec{v}, \vec{v}) = 0$ for all $\vec{v} \in V$
2. for fixed $\vec{v} \in V$, $\beta(\vec{v}, \vec{w}) = 0$ for all $\vec{w} \in V$ iff $\vec{v} = 0$

Condition 1 is the main characterization of a symplectic form. When R is a local ring, condition 2 allows us to relate any subspace $W \subset V$ and the orthogonal complement of W, $W^{\perp} = \{\vec{v} \in V : \beta(\vec{v}, \vec{w}) = 0 \text{ for all } \vec{w} \in W\}$:

Theorem 1.4 (Proposition 1.1 of [6]): Let R be a local ring and let V be a free $R-$module of rank $2r$, where $r \geq 1$. Let β be a symplectic form defined on V. If W is a submodule of V, then:

$$\text{rank}(W) + \text{rank}(W^{\perp}) = \text{rank}(V)$$

Let $\vec{v}, \vec{w} \in V$ be unimodular. If $\beta(\vec{v}, \vec{w}) = 1$, then $\{\vec{v}, \vec{w}\}$ is called a hyperbolic pair. The submodule $R\vec{v} \bigoplus R\vec{w} = \{r\vec{v}+s\vec{w} : r, s \in R\}$ of V is called a hyperbolic plane.

Theorem 1.5 (Theorem 1 of [6]): A symplectic space (V, β) over a local ring R is a direct sum of hyperbolic planes.

As a consequence of this theorem, the rank of any symplectic space is even. Furthermore, V possesses a so-called canonical basis consisting of vectors $\{\vec{e_1}, \vec{e_2}, ..., \vec{e_{2r}}\}$, where each $\{\vec{e_{2i-1}}, \vec{e_{2i}}\}$ is a hyperbolic pair for $1 \leq i \leq r$. Let V be as above with two symplectic forms β_1, β_2 with canonical bases $E_1 = \{e_{i1} : 1 \leq i \leq 2r\}, E_2 = \{e_{j2} : 1 \leq j \leq 2r\}$ respectively. Clearly the R-module morphism $\varphi : V \to V$ given by $\varphi(e_{i1}) = e_{i2}$ induces an isomorphism between the symplectic forms, that is, $\beta_2(\vec{v}) = \beta_1(\varphi(\vec{v}))$ for all $\vec{v} \in V$.

Example: Let R be a local ring and let V be a free $R-$module of rank $2r$, where $r \geq 1$. The prototypical example of a symplectic form in this text will be defined using the $2r \times 2r$-matrix N constructed by taking r blocks of the form:

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

For $\vec{v}, \vec{w} \in V$, the symplectic form $\beta : V \times V \to R$ is defined by:

$$\beta(\vec{v}, \vec{w}) = \vec{v}^T N \vec{w}$$

Symplectic Group

Let R be a local ring and let V be free R-module of rank $2r$ (where $r \geq 1$). Let β be a symplectic form defined on R.

Definition: An isometry $\varphi : V \to V$ is an isomorphism such that $\beta(\vec{v}, \vec{w}) = \beta(\varphi(\vec{v}), \varphi(\vec{w}))$ for all $\vec{v}, \vec{w} \in V$. The set of all such isometries forms a group called the symplectic group $Sp(V)$.

When R is a finite local ring, the action of $Sp(V)$ on the unimodular vectors is particularly interesting. In particular, $Sp(V)$ acts transitively on unimodular vectors and hyperbolic pairs:

Lemma 1.6 (Lemma 3.2 of [4]) Let R be a finite local ring and let (V, β) be a symplectic space defined over R. Then the following is true:

1. For $\vec{v}, \vec{w} \in V$ unimodular vectors, there exists an isometry $\varphi \in Sp(V)$ such that $\varphi(\vec{v}) = \vec{w}$.
2. For hyperbolic pairs $\{\vec{v_1}, \vec{v_2}\}$ and $\{\vec{w_1}, \vec{w_2}\}$, there exists an isometry $\varphi \in Sp(V)$ such that $\varphi(\vec{v_1}) = \vec{w_1}$ and $\varphi(\vec{v_2}) = \vec{w_2}$.

Chapter 2: Symplectic Graphs

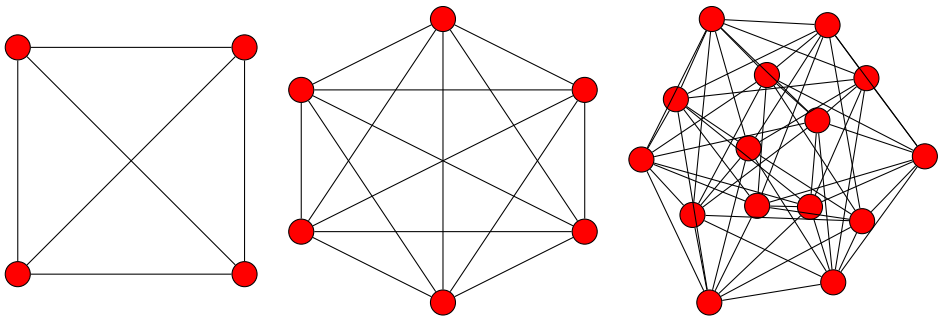
In this section, we discuss the theory of symplectic graphs as presented in the literature. We present some basic results when R is a finite field [2] and then extend this theory to when R is a finite local ring [3][4].

2.1 Over a Finite Field

Let $\mathbb{F}_q$ be a finite field of order q. Let V be a vector space of dimension $2r$ ($r \geq 1$) over $\mathbb{F}_q$. Let β be a symplectic form defined on V. Let $\sim$ be the equivalence relation defined on $V \setminus \{0\}$ by $\vec{v} \sim \vec{w}$ iff $\vec{v} = \lambda\vec{w}$ for $\lambda \in \mathbb{F}_q$. The symplectic graph over $\mathbb{F}_q$, $\mathcal{G}_{Sp(\mathbb{F}_q^{2r})}$, is then constructed as follows. The vertex set is the set of all equivalence classes $(V \setminus \{0\})/\sim$. Adjacency is defined between $[\vec{v}]$ and $[\vec{w}]$ iff $\beta(\vec{v}, \vec{w}) \neq 0$.

Note that V and $\mathbb{F}_q^{2r}$ are isomorphic and thus the symplectic graphs defined over V and $\mathbb{F}_q^{2r}$ are themselves isomorphic. What this means is that, for all intents and purposes, we can take $V = \mathbb{F}_q^{2r}$. Similarly, since all symplectic forms over a vector space are isomorphic, for computational purposes we consider only a symplectic form. In this project we take the symplectic form defined using the matrix N constructed in the previous section.

Examples: The following displays $\mathcal{G}_{Sp(\mathbb{F}_3^2)}$, $\mathcal{G}_{Sp(\mathbb{F}_5^2)}$, $\mathcal{G}_{Sp(\mathbb{F}_2^4)}$.



$\mathcal{G}_{Sp(\mathbb{F}_3^2)}$ $\mathcal{G}_{Sp(\mathbb{F}_5^2)}$ $\mathcal{G}_{Sp(\mathbb{F}_2^4)}$

Note that $\mathcal{G}_{Sp(\mathbb{F}_3^2)}$ is a complete graph on 4 vertices and $\mathcal{G}_{Sp(\mathbb{F}_5^2)}$ is a complete graph on 6 vertices. Also note that $\mathcal{G}_{Sp(\mathbb{F}_2^4)}$ is a $(15, 8, 4, 4)-$strongly regular graph.

Strong Regularity and Chromatic Number

Theorem 2.1 (Theorem 2.1 of [2]):

1. If $r = 1$, $\mathcal{G}_{Sp(\mathbb{F}_q^2)}$ is a complete graph on $q + 1$ vertices.

2. For $r > 1$, $\mathcal{G}_{Sp(\mathbb{F}_q^{2r})}$ is a strongly regular graph with parameters

$$\left(\tfrac{q^{2r}-1}{q-1}, q^{2r-1}, q^{2r-2}(q-1), q^{2r-2}(q-1)\right)$$

Proof: Suppose $r \geq 1$. Note that $\mathbb{F}_q^{2r}\backslash\{0\} = q^{2r}-1$ and so $(\mathbb{F}_q^{2r}\backslash\{0\})/\sim = \frac{q^{2r}-1}{q-1}$. Let $[\vec{v}] \in V(\mathcal{G}_{Sp(\mathbb{F}_q^{2r})})$. The degree of $[\vec{v}]$ is equal to the number of $[\vec{w}] \notin [\vec{v}]^{\perp}$. By Theorem 1.4, $\dim([\vec{v}]) + \dim([\vec{v}]^{\perp}) = 2r \Rightarrow \dim([\vec{v}]^{\perp}) = 2r-1$. Thus $\deg([\vec{v}]) = \frac{q^{2r}-q^{2r-1}}{q-1} = q^{2r-1}$.
Let $[\vec{v}], [\vec{w}] \in V(\mathcal{G}_{Sp(\mathbb{F}_q^{2r})})$. $[\vec{u}] \in V(\mathcal{G}_{Sp(\mathbb{F}_q^{2r})})$ is adjacent to both $[\vec{v}], [\vec{w}]$ iff $[\vec{u}] \notin [\vec{v}]^{\perp} \cup [\vec{w}]^{\perp}$. We have

$$|[\vec{v}]^{\perp} \cup [\vec{w}]^{\perp}| = |[\vec{v}]^{\perp}| + |[\vec{w}]^{\perp}| - |([\vec{v}]^{\perp} \cap [\vec{w}]^{\perp})|$$

where $([\vec{v}]^{\perp} \cap [\vec{w}]^{\perp}) = [\vec{v}, \vec{w}]^{\perp}$. Once again by Theorem 1.5, $\dim([\vec{v}, \vec{w}]^{\perp}) = 2r-2$ and so the number of $[\vec{u}] \notin [\vec{v}]^{\perp} \cup [\vec{w}]^{\perp}$ is equal to $\frac{q^{2r}-1-(q^{2r-1})-(q^{2r-1})+q^{2r-2}}{q-1} = q^{2r-2}(q-1)$.

It can be shown that $\mathcal{G}_{Sp(\mathbb{F}_q^{2r})})$ is $(q^r+1)-$partite. As a consequence, the following holds regarding the chromatic number:

Theorem 2.2 (Theorem 2.4 of [2]): $\chi(\mathcal{G}_{Sp(\mathbb{F}_q^{2r})}) = q^r + 1$.

Automorphism Groups

Earlier we made the point that almost all graphs have trivial automorphism groups. The remarkable fact is that the symplectic graphs have strong regularity structures and also have non-trivial automorphism groups, where the symplectic group $Sp(\mathbb{F}_q^{2r})$ induces automorphisms on $Sp^{2r}(\mathbb{F}_q)$.

Theorem 2.3: Let $T \in Sp(\mathbb{F}_q^{2r})$. Define by:

$$\varphi_T : V(\mathcal{G}_{Sp(\mathbb{F}_q^{2r})}) \to V(\mathcal{G}_{Sp(\mathbb{F}_q^{2r})})$$
$$\varphi_T([\vec{v}]) = [T\vec{v}]$$

Then $\varphi_T \in Aut(\mathcal{G}_{Sp(\mathbb{F}_q^{2r})})$.

Furthermore, due to Lemma 1.6, elements of $Sp(\mathbb{F}_q^{2r})$ induce vertex-transitive and edge-transitive automorphisms on $\mathcal{G}_{Sp(\mathbb{F}_q^{2r})}$.

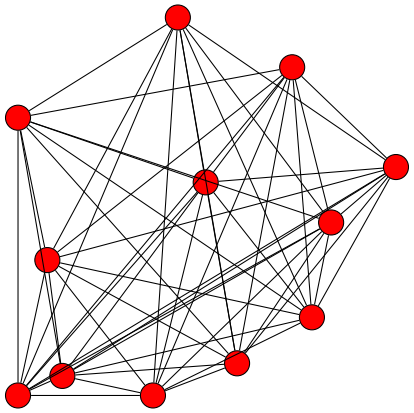
2.2 Over a Finite Local Ring

We now discuss the main case where R is a finite local ring. The main citations for this section are [4] [5]. The results regarding this case involve combinatorial arguments in the literature. The presentation of this section will differ in that the theory will be extracted from the finite field case by considering the canonical

map into the residue field. The main tool for this method will be Lemma 2.5, which we prove in its entirety. First we outline the set-up.

Let R be a finite local ring with maximal ideal M and residue field k. Let V be a free R-module of rank $2r$ (for $r \geq 1$) equipped with a symplectic form $\beta : V \times V \to R$. The vertex set of the symplectic graph $\mathcal{G}_{Sp(V)}$ is the set of lines $R\vec{v} = \{r\vec{v} : r \in R \text{ and } \vec{v} \text{ a unimodular vector}\}$. Vertices $R\vec{v}$ and $R\vec{w}$ are adjacent to each other iff $\beta(\vec{v}, \vec{w}) \in R^{\times}$.

Example: $\mathcal{G}_{Sp(\mathbb{Z}_9^2)}$ is a $(12, 9, 6, 9)-$strongly regular graph.



Let $\pi : R \to k$ be the canonical map defined by $\pi(r) = r + M$ for $r \in R$ and let $E = \{\vec{e_1}, \vec{e_2}, ..., \vec{e_{2r}}\}$ be the canonical basis of V. The map π induces a map from V onto the vector space k^{2r}, which is given by:

$$\pi(x_1\vec{e_1} + x_2\vec{e_2} + ... + x_{2r}\vec{e_{2r}}) = (\pi(x_1), \pi(x_2), ..., \pi(x_{2r}))$$

In this way, every element of k^{2r} can be written as $\pi(\vec{v})$ for some $\vec{v} \in V$. The requirement for using unimodular vectors in the construction of symplectic graphs over local rings lies in the fact that $\pi(\vec{v}) \neq 0$ iff $\vec{v} \in V$ is unimodular. This can be seen in the following classification of unimodular vectors.

Theorem 2.4 (Theorem 2.2 of [4]) A vector $\vec{v} = x_1\vec{e_1} + x_2\vec{e_2} + ... + x_{2r}\vec{e_{2r}}$ in V is unimodular iff $x_i \in R^{\times}$ for some $i = 1, 2, ..., 2r$.

We can also define a symplectic form on k^{2r} β' derived from β as follows:

$$\beta'(\pi(\vec{v}), \pi(\vec{w})) = \pi(\beta(\vec{v}, \vec{w}))$$

The important thing to note is that $\beta'(\pi(\vec{v}), \pi(\vec{w})) \neq 0$ iff $\beta(\vec{v}, \vec{w}) \in R^{\times}$, from which the following lemma holds.

Lemma 2.5 (Lemma 3.1 of [5]): Let R be a finite local ring with maximal ideal M and residue field k. Let (V, β) be a symplectic space defined over R. Let $\kappa = |V(\mathcal{G}_{Sp(k^{2r})})| = \frac{|k|^{2r}-1}{|k|-1}$. Let $\vec{x_1}, \vec{x_2}, ..., \vec{x_{2r}}$ be unimodular vectors in V such that:

$$V(\mathcal{G}_{Sp(k^{2r})}) = \{\pi(\vec{x_i}) : i = 1, 2, ..., \kappa\}$$

Let $R(\vec{x_i} + M^{2r}) = \{R(\vec{x_i} + \vec{m}) : \vec{m} \in M^{2r}\}$. Then the following holds:

1. $|R(\vec{x_i} + M^{2r})| = |M|^{2r-1}$ for all $i = 1, 2, ..., \kappa$.
2. The set $\Pi : \{R(\vec{x_1} + M^{2r}), R(\vec{x_2} + M^{2r}), ..., R(\vec{x_\kappa} + M^{2r})\}$ is a graph partition of $V(\mathcal{G}_{Sp(V)})$.
3. For unimodular vectors $\vec{v}, \vec{w}$, $R\vec{v}$ and $R\vec{w}$ are adjacent vertices in $\mathcal{G}_{Sp(V)}$ iff $\pi(\vec{v})$ and $\pi(\vec{w})$ are adjacent vertices in $\mathcal{G}_{Sp(k^{2r})}$.
4. For distinct $i, j = 1, 2, ..., \kappa$, if $\pi(x_i)$ and $\pi(x_j)$ are adjacent vertices, then $R(\vec{x_i} + \vec{m_1})$ and $R(\vec{x_j} + \vec{m_2})$ are adjacent for all $\vec{m_1}, \vec{m_2} \in M^{2r}$.

Proof:

1. To count $|R(\vec{x_i} + M^{2r})|$, first note that there are $|M|^{2r}$ vectors of the form $\vec{x_i} + \vec{m}$. The lines $R(\vec{x_i} + \vec{m})$ however are not all unique. Suppose $R(\vec{x_i} + \vec{m_1}) = R(\vec{x_i} + \vec{m_2})$. Then $\vec{x_i} + \vec{m_1} = \alpha(\vec{x_i} + \vec{m_2})$ and $\vec{x_i} + \vec{m_2} = \beta(\vec{x_i} + \vec{m_1})$. From this we see that $\alpha\beta = 1$ and that $1 - \alpha \in M$ or $\alpha = 1 + \mu, \mu \in M$. Thus $\vec{x_i} + \vec{m_1} = (1 + \mu)(\vec{x_i} + \vec{m_2})$. On the other hand, if $\vec{x_i} + \vec{m_1} = (1 + \mu)(\vec{x_i} + \vec{m_2})$ for $\mu \in M$, then $R(\vec{x_i} + \vec{m_1}) = R(\vec{x_i} + \vec{m_2})$ as $(1 + \mu) \in R^\times$ (R is a local ring). Thus $|R(\vec{x_i} + M^{2r})| = \frac{|M|^{2r}}{|M|}$ as each $\vec{x_i} + \vec{m}$ contributes $|M|$ times to the count of $|R(\vec{x_i} + M^{2r})|$, one for each such $\mu \in M$.
2. Let $\sim$ be the equivalence relation on the vertex set $V(\mathcal{G}_{Sp(V)})$ given by $R\vec{v} \sim R\vec{w}$ iff $\pi(\vec{v}) = \pi(\vec{w})$. The resulting set partition of $V(\mathcal{G}_{Sp(V)})$ is the set Π. Let $\vec{v}, \vec{w} \in R(\vec{x_i} + M^{2r})$ for some $i = 1, 2, ..., \kappa$. Then $\beta'(\pi(\vec{v}), \pi(\vec{w})) = \beta'(\pi(\vec{x_i}), \pi(\vec{x_i})) = 0$ and thus $\beta(\vec{v}, \vec{w}) \notin R^\times$ and hence $R\vec{v}$ and $R\vec{w}$ are not adjacent vertices in $\mathcal{G}_{Sp(V)}$.
3. This follows from the fact $\beta'(\pi(\vec{v}), \pi(\vec{w})) \neq 0$ iff $\beta(\vec{v}, \vec{w}) \in R^\times$.
4. This follows from 3.

Theorem 2.6: Let R be a finite local ring with unique maximal ideal M. Let (V, β) be a symplectic space over R of dimension $2r$. Then:

1. If $r = 1$, then $\mathcal{G}_{Sp(V)}$ is a strongly regular graph with parameters

$$(|R| + |M|, |R|, |R^\times|, |R|)$$

2. If $r \geq 2$, then $\mathcal{G}_{Sp(V)}$ is a strictly Deza graph with parameters

$$\left(\tfrac{|R|^{2r}-|M|^{2r}}{|R^\times|}, |R|^{2r-1}, |R|^{2r-2}|R^\times|, |R|^{2r-1}\right)$$

Proof: The main idea is to use Theorem 2.1 in conjunction with Lemma 2.5.

1. If $r = 1$, then the graph $\mathcal{G}_{Sp(k^2)}$ is a complete graph on $|k| + 1$ vertices. There are $|k|+1$ sets in the partition of $V(\mathcal{G}_{Sp(V)})$ each with $|M|$ vertices. The number of vertices in $\mathcal{G}_{Sp(V)}$ is then given by $(|k|+1)(|M|) = |R|+|M|$. From (4) of Lemma 2.5, each vertex $R\vec{v}$ is adjacent to $|k||M| = |R|$ vertices as $\mathcal{G}_{Sp(k^2)}$ is complete.

   Suppose $R\vec{v}, R\vec{w}$ are adjacent vertices. Then $R\vec{v}, R\vec{w}$ are in distinct sets in the partition. The vertices adjacent to both are then the $|k|-1$ sets in the partition in which they do not belong. This gives $(|k| - 1)(|M|) = |R^\times|$ such vertices.

   Suppose $R\vec{v}, R\vec{w}$ are non-adjacent vertices. Then they belong to the same set in the partition. Thus every vertex which either are adjacent to is a vertex that both are adjacent to.

2. If $r \geq 2$, the graph $\mathcal{G}_{Sp(k^{2r})}$ is a strongly regular graph with parameters $(\frac{|k|^{2r}-1}{|k|-1}, |k|^{2r-1}, |k|^{2r-2}(|k| - 1), |k|^{2r-2}(|k| - 1))$. The proof is similar to above to show that $\mathcal{G}_{Sp(V)}$ satisfies the first two parameters.

   Suppose $R\vec{v}, R\vec{w}$ are adjacent vertices. Note then that $\pi(\vec{v}), \pi(\vec{w})$ are adjacent vertices with $|k|^{2r-2}(|k|-1)$ vertices of common adjacency. Thus the vertices adjacent to both $R\vec{v}, R\vec{w}$ is given by $(|M|^{2r-1})(|k|^{2r-2})(|k| - 1)) = |R|^{2r-2}|R^\times|$.

   If $R\vec{v}, R\vec{w}$ are non-adjacent vertices then there are now two possibilities as $\mathcal{G}_{Sp(k^{2r})}$ is no longer complete. Suppose $R\vec{v}, R\vec{w}$ are in the same set in the partition of the vertex set. Once again the number of common adjacent vertices is simply the degree of each vertex which is $|R|^{2r-1}$.

   If $R\vec{v}, R\vec{w}$ are non-adjacent vertices such that $\pi(\vec{v}) \neq \pi(\vec{w})$, then $\pi(\vec{v}), \pi(\vec{w})$ have $|k|^{2r-2})(|k| - 1)$ vertices of common adjacency. This translates to $|R|^{2r-2}|R^\times|$ vertices of common adjacency for $R\vec{v}, R\vec{w}$.

Theorem 2.7 (Theorem 3.2 of [5]): The chromatic number of $\mathcal{G}_{Sp(V)}$ is $|k|^r + 1$.

Proof: Recall that $\chi(\mathcal{G}_{Sp(k^{2r})} = |k|^r + 1$ from Theorem 2.2. Let $\vec{x_1}, \vec{x_2}, ..., \vec{x_{2r}}$ be unimodular vectors in V such that $\mathcal{V}(\mathcal{G}(k^{2r})) = \{\pi(\vec{x_i}) : i = 1, 2, ..., \kappa\}$, where $\kappa = |V(\mathcal{G}_{Sp(k^{2r})})|$. Consider the subgraph induced by these vertices. Since this graph is isomorphic to $\mathcal{G}_{Sp(k^{2r})}$, the chromatic number of this induced subgraph is $|k|^r + 1$. Thus $\chi(\mathcal{G}_{Sp(V)}) \geq |k|^r + 1$. Finally note that $\chi(\mathcal{G}_{Sp(V)}) \leq |k|^r + 1$ as $\mathcal{G}_{Sp(V)}$ is $|k|^r + 1$-partite.

The discussion of automorphism groups remains the same as in the finite field case: elements of $Sp_R(V)$ induce graph automorphisms on $\mathcal{G}_{Sp(V)}$. Due to Lemma 1.6, certain induced automorphisms are vertex-transitive and edge-transitive.

Chapter 3: Sequences of Symplectic Graphs

Here $R = \mathbb{Z}_{p^n}$ for $n \geq 2$. Recall that R is a local ring which possesses a natural stratification given by the valuation of the ring. In this context, the valuation takes on a very particular form.

Definition: Let $R = \mathbb{Z}_{p^n}$ for $n \geq 2$. For $r \in R$, the valuation of R is defined by $v(r) = i$ if p^i divides r but p^{i+1} does not divide r. Then $r = \lambda p^i$ for $\lambda \in R^\times$.

Where (V, β) was a symplectic space over R of dimension $2r$, where $r \geq 1$, the vertex set of the symplectic graph $\mathcal{G}_{Sp(V)}$ consisted of lines of unimodular vectors. The aim of this section is to introduce a "sequence of generalized symplectic graphs" over $R = \mathbb{Z}_{p^n}$ where the vertex set of each symplectic graph is more general. The main tool for this construction is the fact that the valuation of the ring provides a natural stratification on V. First we outline the set-up.

Here $V = R^{2r}$ for $r \geq 1$. Define an equivalence relation $\sim$ on $V \setminus 0$ by $[a] \sim [b]$ if and only if $a = \lambda b$ for a $\lambda \in R^\times$. Denote by $(V \setminus \{0\})/\sim$ the set of all equivalence classes of this relation. The stratification on V is given by:

Definition: We say $(a_1, a_2, ..., a_{2r}) \in V$ is of type i if $\min\{v(a_j) : 1 \geq j \geq 2r\} = i$. For $i = 0, 1, ..., n-1$, let T_i denote the set of all vectors in $(V \setminus \{0\})/\sim$ that are of type i.

Note that the vectors of type 0 are simply the unimodular vectors. Further note that $T_0, T_1, ..., T_{n-i}$ provides a partition of $(V \setminus \{0\})/\sim$.

Proposition 3.1: $|T_i| = \frac{(p^{n-i})^{2v} - (p^{n-i-1})^{2v}}{p^{n-i} - p^{n-i-1}}$

Proof: Note that

(number of elements in R^{2r} of type i) = (number of elements in R^{2r} of type $\geq i$) - (number of elements in R^{2r} of type $> i$)

This is $(p^{n-i})^{2v} - (p^{n-i-1})^{2v}$. In each equivalence class there are $p^{n-i} - p^{n-i-1}$ such elements, corresponding to the number of units that change an element of order i. Thus the formula holds.

Let N be the $2r \times 2r$ block diagonal matrix in $Mat(R)$ with r blocks of the form

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

For simplicity, the symplectic form β is defined on V by $\beta(a, b) = a^T N b$ for $a, b \in V$.

Proposition 3.2 Let $a_1, a_2 \in \mathbb{Z}_{p^n}$ with $v(a_1) = i, v(a_2) = j$, where $j > i$. Then:

1. $v(a_1 + a_2) = i$
2. $v(a_1 a_2) = i + j$ if $i + j \leq n$ and n if $i + j > n$

Proof: For (1), we have $a_1 = \lambda p^i, a_2 = \lambda p^j$ and so $a_1 + a_2 = p^i(\lambda + \mu p^{j-i})$. By property of local rings, $\lambda + \mu p^{j-i} \in R^\times$. The proof of (2) is similar.

Proposition 3.3 Let $[a] \in T_i, [b] \in T_j$. Then $c(\beta([a], [b])) \geq i + j$.

Proof: Note $(\beta([a], [b])) = [a]^T N[b] = a_1 b_2 - a_2 b_1 + ... + a_{2r-1} b_{2r} - a_{2r} b_{2r-1}$. The order of each $a_k \geq i$, and the order of each $b_l \geq j$ and so the order of $a_k b_l \geq i + j$. Thus by the previous proposition, the order of the sum is greater than or equal to $i + j$.

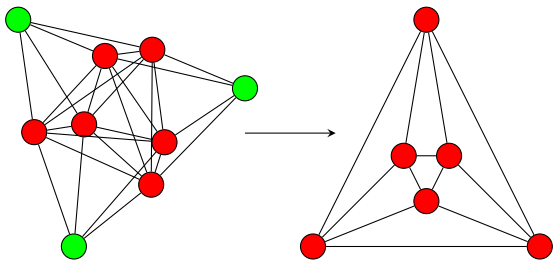
3.1 General Construction

Define a sequence of graphs $\mathcal{G}_0, \mathcal{G}_1, ..., \mathcal{G}_{n-1}$ derived from the symplectic form β on V as follows. In each $\mathcal{G}_i$, the vertex set is the union $V(\mathcal{G}_i) = T_0 \cup T_1 \cup ... \cup T_{n-i-1}$ and where two vertices $[a]$ and $[b]$ are adjacent if and only if:

$$v(\beta([a], [b])) < n - i$$

Note that $\mathcal{G}_{n-1}$ is simply the symplectic graph $\mathcal{G}_{Sp(\mathbb{Z}_{p^n}^{2r})}$.

Example: Let $R = \mathbb{Z}_4$, $V = \mathbb{Z}_4^2$. The sequence is outlined below in this case.



$\mathcal{G}_0$ $\mathcal{G}_1$

T_0 vectors are denoted as red vertices, T_1 are denoted as green vertices. Note that the degree of each vector in T_0 is 7 and the degree of each vector in T_1 is 4 in $\mathcal{G}_0$. Also the degree of each vector in T_0 is 4 in $\mathcal{G}_1$.

Example Let $R = \mathbb{Z}_8$, $V = \mathbb{Z}_8^2$. We outline the degree sequence of each graph.

$\mathcal{G}_0 = [18, 14, 8, 18, 18, 18, 18, 18, 8, 18, 18, 14, 18, 14, 18, 14, 14, 8, 18, 14, 8]$

$\mathcal{G}_1 = [14, 8, 14, 14, 14, 14, 14, 14, 14, 14, 8, 14, 8, 14, 8, 8, 14, 8]$

$$\mathcal{G}_2 = [8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8]$$

In $\mathcal{G}_0$, T_0 vectors are of degree 18, T_1 vectors are of degree 14, T_2 vectors are of degree 8. In $\mathcal{G}_1$, T_0 vectors are of degree 14, T_1 vectors are of degree 8. Finally $\mathcal{G}_\in$, T_0 vectors are of degree 8. This idea generalizes in the following theorem.

Theorem 3.4: Consider the symplectic graph sequence with the set-up as above. Let $0 \leq j \leq n-1$ and $0 \leq i \leq n-j-1$. Then the following holds:

1. The degree of every element of T_i in the graph $\mathcal{G}_j$ is the same. Thus we use the term "the degree of T_i in $\mathcal{G}_j$", denoted $\deg(T_i)^j$.
2. In $\mathcal{G}_j$, we have:
$$\deg(T_0)^j > \deg(T_1)^j > ... > \deg(T_{n-j-1})^j$$
3. $\deg(T_i)^j = \deg(T_{i+1})^{j-1}$

Proof:

1. Let $[a], [b] \in T_i$. Then we can write $[a] = p^i[a'], [b] = p^i[b']$, where $[a'], [b']$ are unimodular vectors. Recall from Lemma 1.6 there exists an isometry $T \in Sp_R(V)$ such that $T(a') = b'$. Define by:
$$\varphi_T : V(\mathcal{G}_j) \to V(\mathcal{G}_j)$$
$$\varphi_T([v]) = [Tv]$$
Note that $\varphi_T([a]) = [b]$. For a vertex $[c]$, $v(\beta([a],[c])) < n-j$ iff $v(\beta(\varphi_T([a]), \varphi_T([c]))) = v(\beta([b], \varphi_T([c]))) < n-j$ as T is an isometry. Thus $\deg([a]) = \deg([b])$.
2. For $0 \leq i \leq n-j-2$, we show $\deg(T_i)^j > \deg(T_{i+1})^j$. Consider $p^{i+1}[a] \in T_{i+1}$, where $[a]$ is a unimodular vector. Proposition 3.3 implies that if $p^{i+1}[a]$ is adjacent to a vertex $[c]$, then $p^i[a]$ is adjacent to $[c]$. Thus $\deg(T_i)^j \geq \deg(T_{i+1})^j$.
To show this inequality is strict, note that there exists a unimodular vector $[b]$ such that $\beta([a],[b]) \in R^\times$ or that $v(\beta([a],[b]) \in R^\times) = 0$ (to see that this is true, consider the symplectic graph over a finite local ring constructed in the previous section and note that each vertex has non-zero degree). Now $p^i[a]$ is adjacent to $p^{n-j-i-1}[a]$ but $p^{i+1}[a]$ is not adjacent to $p^{n-j-i-1}[a]$ by Proposition 3.3.
3. Let $[a]$ be a unimodular vector. Let $[c] \in V(\mathcal{G}_j)$ such that $v(p^i[a],[c]) < n-j$. Then $v(p^{i+1}[a],[c]) = v(p^i[a],[c]) + 1 < n-j+1$. Thus if $[c]$ is adjacent to $p^i[a]$ in $\mathcal{G}_j$, then $[c]$ is adjacent to $p^{i+1}[a]$ in $\mathcal{G}_{j-1}$. Thus $\deg(T_i)^j \leq \deg(T_{i+1})^{j-1}$. We can show the reverse inequality is also true very similarly.

3.2 The Case Where r = 1

The above theorem highlights some basic regularity structure when $r \geq 1$. In this section, we discuss the case where $r = 1$ more extensively.

Lemma 3.5: For all $[a] \in T_i$ in $\mathcal{G}_0$:

$$\begin{aligned}\deg([a]) &= |V(\mathcal{G}_0)| - (|T_{n-1}| + ... + ...|T_{n-i}| + p^i(n-i)) \\ &= |T_{n-i+1}| + ... + |T_0| - p^i(n-i)\end{aligned}$$

Proof: Let $\overline{\mathcal{G}_0}$ denote the complement graph of $\mathcal{G}_0$. Here adjacency is defined between vertices $[a]$ and $[b]$ if and only $[a]N[b] = 0 \mod p^n$. Without loss of generality, let $[a_1, a_2] = [\lambda p^i, \mu p^k] \in T_i$ where $\lambda, \mu \in R^\times$ and $k \geq i$. Then

$$[\lambda p^i, \mu p^k]N[b_1, b_2] = p^i(\lambda b_2 - \mu p^{k-i} b_1)$$

This is equivalent to solving $b_2 = \lambda^{-1}\mu p^{k-1} b_1 \mod p^{n-i}$. We have p^{n-i} options for b_1 corresponding to the set of integers modulo p^{n-i}, each giving a solution for b_2, denoted α_m for $m = 0, 1, ..., p^{n-i} - 1$. We can thus write the solution set as follows:

$$\begin{aligned}\{(0 + p^{n-i}k_0, \alpha_0 + p^{n-i}l_0), (1 + p^{n-i}k_1, \alpha_1 + p^{n-i}l_1), ..., (p^{n-i} - 1 + \\ p^{n-i}k_{p^{n-i}-1}, \alpha_{p^{n-i}-1} + p^{n-i}l_{p^{n-i}-1})\}\end{aligned}$$

Here $k_m, l_m = 0, 1, ..., p^i$. Note that the vectors $(0 + p^{n-i}k_0, \alpha_0 + p^{n-i}l_0)$ in $V \setminus 0/\sim$ correspond precisely to the vectors in $T_{n-1}, ..., T_{n-i}$. If $v(m) = 0, 1, ..., n - i + 1$, then $(m, \alpha_m + p^{n-i}l_m)$ gives all vectors of type m that solve this equation, of which there are p^i. Thus the degree of $[a] \in T_i$ in $\mathcal{G}_0$ is equal to:

$$|T_{n-1}| + ... + ...|T_{n-i}| + p^i(n-i)$$

The result follows.

Theorem 3.6: Let $0 \leq j \leq n-1$ and $0 \leq i \leq n-j-1$. If $[a] \in T_i$, then:

$$\deg[a] = |T_{n-i-j+1}| + ... + |T_0| - p^{i+j}(n-i-j)$$

Proof: By Theorem 3.4, $\deg(T_i)^j = \deg(T_{i+1})^{j-1} = ... = \deg(T_{i+j})^0$. The result follows from Lemma 3.5.

When $r = 1$, the graph sequence has an interesting combinatorial construction using partitions. This construction can also be used to calculate the chromatic number of each $\mathcal{G}_i$.

Lemma 3.7: For $k \in \mathbb{Z}_p$, let $A_k^i = \{p^i[1, pj + k], j \in \mathbb{Z}_{p^{n-i-1}}\}$ and $A_p^i = \{p^i[j, 1], 0 \leq j < p^{n-i}$ and p divides $j\}$. Then the sets $A_0^i, A_1^i, ..., A_p^i$ form a partition of T_i.

Proof: First we show that $\bigcup_{k=0}^{p} A_k^i = T_i$. Clearly $\bigcup_{k=0}^{p} A_k^i \subset T_i$ so we show the converse. Let $[a,b] \in T_i$. Consider two cases.
Case 1: $[a,b] = [p^i, \lambda p^l]$ where $\lambda \in R^\times$ satifying $0 < \lambda < p^{n-l}$ and $n \geq l \geq i$. If $l = i$, then the result follows so suppose otherwise. Then write:

$$p^i[1, \lambda p^{l-i}] = p^i[1, p(\lambda p^{l-i-1})]$$

Finally note that $0 \leq \lambda p^{l-i-1} \leq p^{n-i-1}$. Thus $[a,b] \in A_0^i$.
Case 2: $[a,b] = [\lambda p^l, p^i]$ where $\lambda \in R^\times$ satifying $0 < \lambda < p^{n-l}$ and $n \geq l \geq i$. If $l = i$, then $[\lambda p^i, p^i] = [p^i, \lambda^{-1} p^i]$ and we return to the first case. If $l > i$, then $p^i[\lambda p^{l-i}, 1] \in A_p^i$.
Now suppose for $0 \leq k \leq l \leq p$, $A_k^i \cap A_l^i \neq \varnothing$. If $l = p$, k must also be equal to p. If $l \neq p$, this means that there exists j_1, j_2 such that:

$$p^i[1, pj_1 + k] = p^i[1, pj_2 + l] \Rightarrow p(j_1 - j_2) = l - k \Rightarrow p | l - k \Rightarrow l = k$$

as both $l, k \in \mathbb{Z}_p$.

Corollary to Lemma 3.7: For $k = 0, 1, ..., p$, $|A_k^i| = p^{n-i-1}$.

Proof: Counting argument using above.

Let $\varphi : (R^2 \setminus \{0\})/\sim \to (R^2 \setminus \{0\})/\sim$ be defined by $\varphi([a,b]) = p[a,b]$. Then $\varphi(A_k^i) = A_k^{i+1}$. In particular, let $j \in \mathbb{Z}_{p^{n-i-2}}$ and let $k \in \mathbb{Z}_p$. Let $j_l = j + lp^{n-i-2}$, where $l \in \mathbb{Z}_p$. Note that $j_l \in \mathbb{Z}_{p^{n-i-1}}$ and also that

$$\varphi(p^i[1, pj_l + k]) = p^{i+1}[1, pj_l + k] = p^{i+1}[1, pj + k] \in A_k^{i+1}$$

Similarly if we let $j \in \mathbb{Z}_{p^{n-i-1}}$ with $p | j$, we can consider $j_l \in \mathbb{Z}_{p^{n-i}}$ defined by $j_l = j + lp^{n-i-1}$. It also follows that:

$$\phi(p^i[j_l, 1]) = p^{i+1}[j, 1] \in A_p^{i+1}$$

We can conduct a similar analysis in the other direction with the conclusion being that for $k = 0, 1, ..., p$, A_k^i is partitioned into p^{n-i-2} classes where each class consists of p elements corresponding to the inverse image of some element in A_k^{i+1} under φ.

Proposition 3.8 Let $[a,b] \in A_k^i$, $[c,d] \in A_l^j$ with $j > i$. If $\phi^{j-i}([a,b]) = [c,d]$, then $\beta([a,b],[c,d]) = 0$. Otherwise:

$$v(\beta([a,b],[c,d])) = \begin{cases} i + j + 1, & \text{if } k = l \\ i + j, & \text{otherwise} \end{cases}$$

The above theory allows us to construct the graph $\mathcal{G}_i$ in a more combinatorial way. First write the vertex set $V(\mathcal{G}_i) = T_0 \cup T_1 \cup ... \cup Tn - i - 1$ as follows:

$$\begin{array}{cccc} A_0^0 & A_0^1 & \dots & A_0^{n-i-1} \\ A_1^0 & A_1^1 & \dots & A_1^{n-i-1} \\ \vdots & \vdots & \ddots & \vdots \\ A_p^0 & A_p^1 & \dots & A_p^{n-i-1} \end{array}$$

Recall that in this setting adjacency is defined between $[a], [b] \in V(\mathcal{G}_i)$ iff $v(\beta([a],[b])) < n-i$. Assume that all vertices are connected and remove edges as follows.

Let $k = 0, 1, ..., p$ and let $[a_{j,k}, b_{j,k}] \in A_k^j$. There are three types of edges that we need to remove.

1. For $l = 1, 2, ..., n-i-1-j$, remove edges between $[a_{j,k}, b_{j,k}]$ and $\phi^l([a_{j,k}, b_{j,k}])$.
2. If $l + j \geq n - i$, then remove all edges between $[a_{j,k}, b_{j,k}]$ and A_m^l for $m = 0, 1, ..., p$ but $m \neq k$.
3. If $l + j + 1 \geq n - i$, then remove all edges between $[a_{j,k}, b_{j,k}]$ and A_k^l.

Corollary: The chromatic number of $\mathcal{G}_i$ is $p+1$ if $i = n-1$ and $(p+1)p^{n-1}$ otherwise.

Proof: If $i = n-1$, this is the case covered by Theorem 2.7. Suppose $i < n-1$. For $0 \leq k \leq p$, note that the graph consisting of the vertices in A_k^0 is complete. Thus assign to each vertex in A_k^0 a unique colour. Then since each $A_k^j = \phi^j(A_k^0)$ for $j = 1, 2, ..., n-i-1$, these colours are sufficient for the sequence $A_k^0, A_k^1, ..., A_k^{n-i-1}$. Each sequence $A_k^0, A_k^1, ..., A_k^{n-i-1}$ is then coloured by p^{n-1} colours, with there being $p+1$ such sequences.

References

[1] C.Godsil, G.Royle, *Algebraic Graph Theory*, Springer, 2001

[2] Z.Tang, Z.Wan, *Symplectic Graphs and their Automorphisms*, European Journal of Combinatorics Volume 27, Issue 1, January 2006, Pages 38-50

[3] Y.Meemark, T.Prinyasart, *On Symplectic Graphs Modulo p^n*, Discrete Mathematics Volume 311, Issue 17, 6 September 2011, Pages 1874-1878

[4] Y.Meemark, T.Puirod, *Symplectic Graphs over Finite Local Rings*, European Journal of Combinatorics Volume 34, Issue 7, October 2013, Pages 1114-1124

[5] Y. Meemark, T. Puirod, *Symplectic Graphs over Finite Commutative Rings*, European Journal of Combinatorics Volume 41, October 2014, Pages 298-307

[6] W.Klingenberg, *Symplectic Groups over Local Rings*, American Journal of Mathematics Volume 85, No. 2 (Apr 1963), Pages 232-240

[7] I.Herstein, *Topics in Algebra*

[8] D.Dummit, R.Foote, *Abstract Algebra*

[9] E.Artin, *Geometric Algebra*

[10] R.C.Bose, *Strongly Regular Graphs, Partial Geometries and Partially Balanced Designs*, Pacific J. Math 13 (1963) 389–419. (p. 122)

Appendix

(A) Basic Concepts in Graph Theory

Let G be a graph. We denote the vertices of G by $V(G)$ and the edges by $E(G)$. For vertices u, v, by $u \sim v$ we will mean that u and v are adjacent. The complement of a graph G, denoted $\overline{G}$, is constructed by taking the vertex set of G and defining adjacency between vertices u and v if and only if u and v are not adjacent in G.

A graph G is k-regular if every vertex in G has k neighbours. Let G be a graph with n vertices. If every pair of distinct vertices are adjacent, then G is referred to as the complete graph on n vertices, denoted K_n.

A graph G is k-partite if the vertex set $V(G)$ can be partitioned into k disjoint sets such that if two vertices are in the same set, then they are non-adjacent.

Suppose G is a graph with n vertices. The adjacency matrix $A(G)$ is the $n \times n$ matrix where the rows and columns correspond to the vertices of G and where:

$$A(G)_{u,v} = \begin{cases} 1, & \text{if } u \sim v \\ 0, & \text{otherwise} \end{cases}$$

Graph Automorphisms

Let G, H be graphs. A mapping $\varphi : V(G) \to V(H)$ is a graph homomorphism if $u \sim v$ implies $\varphi(u) \sim \varphi(v)$. If φ is a bijection and φ^{-1} is also a homomorphism, then φ is a graph isomorphism. An isomorphism $\varphi : V(G) \to V(G)$ is called an automorphism, and the set of all automorphisms form a group called the automorphism group $Aut(G)$, where the group operation is given by the composition of maps.

Example: $Aut(K_n) = S_n$, the symmetric group of order n.

A well-known fact in graph theory is that almost all graphs are asymmetric, or their automorphism consists only of the identity map. Graphs with non-trivial automorphism groups are thus quite special and rare.

A graph G is said to be vertex-transitive if for all distinct $u, v \in V(G)$, there exists $\varphi \in Aut(G)$ such that $\varphi(u) = v$. If for any distinct edges $(u_1, v_1), (u_2, v_2) \in E(G)$, there exists $\varphi \in Aut(G)$ such that $\varphi(u_1) = u_2$ and $\varphi(v_1) = v_2$, then G is said to be edge-transitive.

(B) Basic Concepts in Ring Theory

Here we discuss the ideas of rings, ring homomorphisms, ideals, quotient rings and also define a local ring. The discussion of these ring-theoretic concepts will mirror the ideas of group homomorphisms, normal subgroups and quotient rings. See [7] [8] for more details.

Basic Concepts in Ring Theory

We consider a ring as a generalization of a field - we remove the requirement that multiplication is necessarily commutative and that multiplicative inverses exist for all non-zero elements. In a ring, invertible elements are called units. We will adopt the convention that the unit element 1 is in the ring, although certain texts remove this property also. Explicitly, the definition reads:

Definition: A ring R is a non-empty set with two operations, $+$ and $\cdot$, such that:

- R is an abelian group under $+$ with identity element 0
- $a \cdot b \in R$ (closure)
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associative law)
- $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ (distributive laws)
- $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$

Remark: From here on out, we will omit using $\cdot$ and so ab will be understood to mean $a \cdot b$.

Examples:

1. The ring of integers $\mathbb{Z}$ under the usual operations of addition and multiplication. The units of $\mathbb{Z}$ are 1 and -1.
2. For positive integer n, the ring of integers modulo n, $\mathbb{Z}_n$. $\mathbb{Z}_n$ is a field if and only if n is prime.
3. Let R be a ring. The set of all $n \times n$ matrices with entries in R, $M_n(R)$ is a ring where multiplication is given by ordinary matrix multiplication. Note that multiplication is not necessarily commutative in this example. If R is a field, then the units of $M_n(R)$ are the matrices with non-zero determinant.

Similar to group homomorphisms, we can consider ring homomorphisms.

Definition Let R, R' be rings. A map $\varphi : R \to R'$ is a ring homomorphism if for all $a, b \in R$:

- $\varphi(a + b) = \varphi(a) + \varphi(b)$
- $\varphi(ab) = \varphi(a)\varphi(b)$

The set $\{r \in R : \varphi(r) = 0\}$ is referred to as the kernel of φ, $Ker(\varphi)$. If φ is a bijection, then we call it an isomorphism and the rings R, R' are isomorphic. Alternatively, φ is an isomorphism if and only if $Ker(\varphi) = \{0\}$.

Ideals, Maximal Ideals and Quotient Rings

The theory of group homomorphisms imply the notions of normal subgroups and quotient groups, and analogues to these ideas exist in ring theory as well in ideals and quotient rings. The topic of quotient rings is very briefly discussed so the reader is encouraged to see [topics in algebra] for a more in-depth treatment.

Definition: A non-empty subset U of R is an ideal if:

- U is a subgroup of R under addition
- For every $u \in U, r \in R$, $ur, ru \in R$.

Examples:

1. Trivial examples include the ring R itself and $\{0\}$. These are the only ideals of a commutative ring R if and only if R is a field.
2. Let R be a ring and let $A = \{a_1, a_2, ..., a_k\} \subset R$. The ideal generated by A, denoted $(a_1, a_2, ..., a_k)$, is the set $\{a_1r_1+a_2r_2+...+a_kr_k : r_1, r_2, ..., r_k \in R\}$.
3. If $R = \mathbb{Z}$, every ideal U is the ideal generated by some $n \in \mathbb{Z}$. Note that if p is a prime number dividing n, then $(n) \subset (p)$. Also if U is an ideal such that $(p) \subset U$, then either $U = (p)$ or $U = \mathbb{Z}$. In this sense the ideals (p) are "larger" than all other ideals (n). This idea motivates our definition of a maximal ideal.

Definition: A maximal ideal $M \neq R$ of a ring R is an ideal such that if U is an ideal of R satisfying $M \subset U \subset R$, then either $U = M$ or $U = R$.

In example 2. above, the maximal ideals are precisely the ideals (p) generated by prime numbers p. We now construct the quotient ring R/U from an ideal U in a ring R.

Define the equivalence relation $\sim$ on R by $r \sim s$ if $r - s \in U$. For $r \in R$, if $r \sim s$, then $s = r + u$ for $u \in U$. If we let $r + U = \{r + u : u \in U\}$, then the equivalence classes can be denoted by $r + U$. Let $R/U = \{r + U : r \in R\}$. We will turn this set into a ring by defining addition and multiplication by:

$$(a+U)+(b+U)=(a+b)+U$$
$$(a+U)(b+U)=ab+U$$

Addition and multiplication can be shown to be well-defined operations and R/U can be shown to be a ring with these operations. The additive and multiplicative identity are given by U and $1+U$ respectively. The rings $R, R/U$ are related by the homomorphism $\varphi : R \to R/U$ given by $\varphi(r) = [r+U]$. Note that $Ker(\varphi) = U$. The following theorem provides a necessary and sufficient condition for R/U to be a field.

Theorem: Let R be a commutative ring with ideal M. Then R/M is a field if and only if M is a maximal ideal. If R/M is a field, we refer to it as a residue field.

Example: In $\mathbb{Z}$, $\mathbb{Z}/(n) = \mathbb{Z}_n$. This is a field if and only if n is prime.

(C) Code and Computations

In this section, we outline the code used to generate examples of symplectic graphs in this project. Sagemath was used for these implementation. Let N be the $2r \times 2r$ block diagonal matrix in with r blocks of the form

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

For all computations in this project, the symplectic form β was defined using the matrix N.

Symplectic Graphs over a Finite Field

Let $\mathbb{F}_q$ be a finite field of order q. The following code generates the symplectic graph $\mathcal{G}_{Sp(\mathbb{F}_q^{2r})}$, where $r \geq 1$.

```
#the function constructs the symplectic graph over F_q^2r for given
     values of q and r.

def symplectic_graph_finite_field(q,r):

    #contruct dictionary where the keys of the dictionary are
    indices and the values are the elements of
    #the projective space
    proj_space = {}
    j = 0
    for i in ProjectiveSpace(2*r - 1, GF(q)):
        proj_space[j] = vector(i)
        j = j + 1

    #construct symplectic matrix
    v = [i for i in range(2*r) if i % 2 == 0]
    N = matrix(GF(q),2*r, 2*r)
```

```
16
17      for i in v:
18          N[i, i+1] = 1
19          N[i+1, i] = -1
20
21      #construct adjacency matrix, A is initialized as the zero
        matrix and the (i,j) entry is changed to 1 iff
22      #the corresponding elements in the projective space are
        adjacent.
23      A = matrix(j, j)
24
25      for i in proj_space:
26          for j in proj_space:
27              if i != j:
28                  if (proj_space[i] * N * proj_space[j]) != 0:
29                      A[i,j] = 1
30
31      return Graph(A)
```

Symplectic Graphs over a Finite Local Ring

Let $R = \mathbb{Z}_{p^n}$, where p is a prime number and $n \geq 1$. The code below generates the symplectic graph $\mathcal{G}_{Sp(R^{2r})}$, where $r \geq 1$..

```
1  #given n, generates the inverses in the ring Z mod n
2
3  def Inverses(n):
4      inverses = []
5      for i in Integers(n):
6          for j in Integers(n):
7              if mod(i*j,n) == 1:
8                  inverses.append(i)
9      return inverses
```

```
1  #given (n, v), generates the vertex set of the symplectic graph
       defined over the ring Z mod n
2
3  def vertex_set(n, v):
4      import numpy
5      inverses = Inverses(n)
6      tuples = [vector(t) for t in Tuples(Integers(n), 2*v)]
7      unimodular_vector = []
8
9      #remove all non-unimodular vector
10     for i in range(len(tuples)):
11         if any(j in inverses for j in tuples[i]):
12             unimodular_vector.append(tuples[i])
13
14     #remove multiples
15     for i in range(len(unimodular_vector)):
16         for j in range(len(unimodular_vector)):
17             if i != j:
18                 for k in inverses:
19                     if numpy.array_equal(unimodular_vector[j],
       numpy.multiply(unimodular_vector[i],k)):
20                         unimodular_vector[j] = zero_vector(2*v)
```

```
21
22      new_tuples = [t for t in unimodular_vector if t != zero_vector
        (2*v)]
23
24      return new_tuples
```

```
1  #given n and v, generates the symplectic graph over the module (Z_n
       )^2v
2  def graph(n,v):
3      inverses = Inverses(n)
4      V = vertex_set(n,v)
5
6      j = 0
7      vertices = {}
8      for i in V:
9          vertices[j] = vector(i)
10         j = j+1
11
12     #construct symplectic matrix
13     r = [i for i in range(2*v) if i % 2 == 0]
14     N = matrix(Integers(n),2*v, 2*v)
15
16     for i in r:
17         N[i, i+1] = 1
18         N[i+1, i] = -1
19
20     A = matrix(j,j)
21
22     for i in vertices:
23         for j in vertices:
24             if i!=j:
25                 a = vertices[i] * N * vertices[j]
26                 if (a in inverses):
27                     A[i,j] = 1
28
29     return Graph(A)
```

Sequences of Symplectic Graphs

The above code can be customized to generate the sequence of symplectic graphs discussed in Chapter 3. For instance, to generate a more general vertex set we use:

```
1  #given (n, v), generates the vertex set of the graph G_0, i.e. the
       non-zero vectors under the relation identifying multiples by
       units
2
3  def vertex_set(n, v):
4      import numpy
5      inverses = Inverses(n)
6      tuples = [vector(t) for t in Tuples(Integers(n), 2*v)]
7
8      for i in range(len(tuples)):
```

```
        for j in range(len(tuples)):
            if i != j:
                for k in inverses:
                    if numpy.array_equal(tuples[j], numpy.multiply(
    tuples[i],k)):
                        tuples[j] = zero_vector(2*v)

    new_tuples = [t for t in tuples if t != zero_vector(2*v)]

    return new_tuples
```

The function `graph` is adjusted by varying the adjacency condition in the final block. As example, the following block was used to generate $\mathcal{G}_1$ over $\mathbb{Z}_8^2$:

```
    for i in vertices:
        for j in vertices:
            if i!=j:
                a = vertices[i] * N * vertices[j]
                if ((a != mod(0,n)) and (a != mod(4,n))):
                    A[i,j] = 1
```

A cleaner, more general implementation is clearly possible using these ideas as a basis but was not covered in this project.