Algorithmic Approaches to Graph States under the Action of Local Clifford Groups

by

Mohsen Bahramgiri

B. S., Sharif University of Technology, 2000

Submitted to the Department of Mathematics
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2007

Author .....
Department of Mathematics
May 1, 2007

Certified by .....
Peter W. Shor
Morss Professor of Applied Mathematics
Thesis Supervisor

Accepted by .....
Alar Toomre
Chairman, Applied Mathematics Committee

Accepted by .....
Pavel Etingof
Chairman, Department Committee on Graduate Students

Algorithmic Approaches to Graph States under the Action of Local Clifford Groups

by

Mohsen Bahramgiri

Submitted to the Department of Mathematics
on May 1, 2007, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Abstract

Graph states are quantum states (quantum codes) in q^n-dimensional space $(\mathbb{C}^q)^{\otimes n} = \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$ (q being a power of some prime number) which can be described by graphs with edges labeled from the field of order q, $\mathbf{F}_q$. Graph states are determined as a common eigenvector of independent elements of the n-fold Pauli group, on which the local Clifford group has a natural action. This action induces the natural action of the local Clifford group on graph states and hence, its action on graphs. *Locally equivalent* graphs can be described using this action. For q being a prime number, two graphs are locally equivalent when they are located on the same orbit of this action, in other words, when there is an element of the local Clifford group mapping one graph to the other one. When q is some power of a prime number, the definition of this action is the natural generalization of this action in the case where q is prime.

We translate the action of local Clifford groups on graphs to a set of linear and quadratic equations in the field $\mathbf{F}_q$. In the case that q is an odd number, given two arbitrary graphs, we present an efficient algorithm (polynomial in n) to verify whether these graphs are locally equivalent or not.

Moreover, we present a computational method to calculate the number of inequivalent graph states. We give some estimations on the size of the orbits of this action on graphs, and prove that when either q is equal to 2 or is an odd number, the number of inequivalent quantum codes (i.e., the number of classes of equivalency) is equal to $q^{\frac{1}{2}n^2-O(n)}$, which is essentially as large as the total number of graphs.

Thesis Supervisor: Peter W. Shor
Title: Morss Professor of Applied Mathematics

Acknowledgments

I am pleased to thank my advisors, professor Shor and professor Guillemin for their guidance and help throughout this work. My deepest gratitude goes to my wife and parents, and to my family for their continuous and unconditional support. They are my treasures. Thanks to Eaman, Salman, Vahab, MohammadTaghi and Mohsen R. for all discussions and good time we had at MIT and Sharif. I shall also thank my professors at Sharif, prof. Tabesh, prof. Shahshahani, prof. Mahmoudian, prof. Mahdavi-Amiri, prof. Akbari, prof. Daneshgar, prof. Khandani, prof. Hessaraki, prof. Pournaki, and my friends there, Dr. Razvan, Omid, Kasra, Seyyed Reza, Arash, Jafar, Mohsen J., Alireza B. and Morteza. I would like to express my thankfulness to old friends here and back home, Hadi S., Hadi J., Alireza S., Pouria, Mohsen B., Amir, Borgan, Ehsan, Shahriar, Babak, Saeed, Keivan, Afshin, Mehdi, Mostafa and to the Allameh Helli fellows, Mr. Yusefi, Mr. Faripour, and more specially to Yasser, Hossein, Mahdi, Seyyed Mahdi, Mehdi, Farzan, Mr. Misagh, Reza, Hadi and MohammadReza. May Allah bless them all.

Dedicated to my parents, and to my wife.

Contents

List of Tables

Chapter 1

Introduction

Graph states, forming a universal resource for quantum computation based on measurement, have been used in many applications in quantum information theory as well as quantum computation, and have been recently studied extensively. This is due to the fact that these states not only maintain a rich structure, but can be described transparently in different ways.

Graph states have been studied in many aspects in the recent works in quantum computation. In fact, *Bell states*, being just a very simple example of graph states, were used to show that quantum computation and quantum information theory are more powerful rather than the classical analogs. Moreover, the notion of *entanglement*, the significant property of quantum systems compared to the classic ones, has been widely studied for graph states.

Quantum codes, which are of natural importance in *quantum error correcting codes*, contain a significant and well studied subclass, called *stabilizer codes,* and graph states are an special codes in this class which can be described by *graphs.* These states have been studied from this point of view in many aspects, see e.g. [11], [12].

The action of Clifford group on these states can be explained in an appropriate way, in the notion of their stabilizers, see [14]. On the other hand, any stabilizer state is equivalent to a graph state under the local Clifford groups, and one can describe the action of local Clifford groups on graphs by two different types of graph operators.

Also, the local Pauli measurements may be described via some operations on graphs, see [11], [10].

The equivalency of graphs (more precisely, graphs with labeled edges) under the local Clifford groups has been the subject of many works. A recent work of the author of the present thesis leads to presenting a polynomial time algorithm to recognize whether two graph states are equivalent under local Clifford groups or not, see [2] (also see [5], [9] for binary cases).

A *labeled graph* is a graph with labeled edges, where labels are chosen from a (finite) field. This covers the usual (unlabeled) graphs, when one restricts the field to the binary field, $\mathbf{F}_2$. The concept of *local equivalency* in graphs arises naturally not only from many combinatorial concepts, but in studying the relations between different error-correcting codes in *quantum computation.* For simplicity, we discuss the binary case separately to make the notion more clear. In the binary case, i.e., when the field is binary, consider the following operator, called *local complementation.* Choose a vertex, and replace the graph induced by the neighbors of this vertex by its complement. Two graphs are called *locally equivalent* if one can obtain one of them by applying some local operations, as above, to the other one.

In general, when the field is not binary, there are two independent types of operators involved. The first type is just the generalized version of the local complementation operator, and the second one has no correspondence (and is in fact just the trivial operator) in the binary case. Let the graph G be labeled with labels forming a symmetric matrix $G = (g_{ij})$ with zero diagonal over $\mathbf{F}_q$, where q is a power of a prime number, and $\mathbf{F}_q$ is the field with q elements. Let v be a vertex of this graph, and $a \in \mathbf{F}_q$. We define the first type of operators, $*$-operator, as follows. By definition, $G *_a v$ is the graph with labels $G' = (g'_{ij})$ such that $g'_{ij} = g_{ij} + a \cdot g_{vi} g_{vj}$.

The second type of operator, the $\circ$-operator, just multiplies the edges connected to a vertex by a non-zero number $b \in \mathbf{F}_q$. In other words, $G \circ_b v$ is the graph with labels $G'' = (g''_{ij})$, where $g''_{vi} = b g_{vi}$ and $g''_{ij} = g_{ij}$ for i, j unequal to v. Similar to the previous situation, two graphs are called locally equivalent if one can obtain one of them by applying the operators $*$ and $\circ$ to the other one.

Studying and investigating the local equivalency of graphs has become a natural problem in quantum computation, and playing a key role especially in *error-correcting codes*, due to the recent work of [1], [10], [12] and the third chapter of the present thesis. Namely, in the quantum computing setting, some states, called stabilizer states, have a description as the common eigenvector of a subgroup of the *Pauli group*. Using stabilizer states, we may be able to create more preferable quantum codes, due to the property that the resulting codes have relatively shorter descriptions and are more algebraically structured. On the other hand, graph states, an important subset of stabilizer states, are defined based on graphs with labels in a finite field. Combining the theory of error-correcting codes and the tools in generalized graph theory, leads us to describe and investigate the properties of graph states more and more deeply.

Also, we can obtain one of the stabilizer states from another equivalent one by applying the elements of the *local Clifford group* on that state when q is a prime number, and generalize this action in the natural way into the general case. It is already well known that any stabilizer state is equivalent to a graph state under the action of the local Clifford group, and consequently, we may only need to consider graph states for many purposes in studying stabilizer states. On the other hand, some of the graph states are equivalent under the local Clifford group. More precisely, as shown in chapter 2, two graph states are equivalent under the local Clifford group if their associated graphs are locally equivalent by the local operations described earlier. The special case, when $q = 2$, has been studied in the work of *André Bouchet* (see [6], [7]), and a polynomial time algorithm to verify the equivalency of two unlabeled graphs is presented in [5].

When $q \neq 2$, the algebraic structure of the locally equivalent graphs is different, and is more non-linear when compared to the binary case, i.e., when $q = 2$. In chapter 3 we will see that recognizing locally equivalent graphs is equivalent to solving a system of equations, some of which are linear equations while the rest are quadratic. Notice that in the binary field every element satisfies $a^2 = a$, and hence quadratic equations (for instance determinant functions) on the binary field exhibit some linear properties. The algorithm described in [5] takes the advantage of this property of

the binary field. The situation in the non-binary case, where $q \neq 2$, is completely different, and the determinant functions do not exhibit linear properties in general. In chapter 3, we present a method to study this system of equations, and give an algorithm to verify efficiently whether two given graphs are locally equivalent or not.

In chapter 4, we study the system of equations more deeply, and develop some algebraic tools in order to count the number of graphs that are locally equivalent to a fixed one. Giving some estimations on the size of the classes of equivalency, we show that when q is either 2 or an odd number, the number of inequivalent graphs is essentially as large as the total number of graphs.

Chapter 2

Graph States in Binary and Non-Binary Cases

2.1 Preliminaries

We start introducing Pauli groups and graph states with the binary case. Let $\mathcal{G}_n$ be the *Pauli Group* on n qubits, consisting of all $n-$fold tensor products of the form $\alpha v_1 \otimes v_2 \otimes \cdots \otimes v_n$ where $\alpha \in \{\pm 1, \pm i\}$ is an overall phase factor and v_i's are 2×2 matrices which are either the identity σ_0 or one of the Pauli matrices (see [10])

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The *Clifford group* $\mathcal{C}_n$ is the normalizer of $\mathcal{G}_n$ in $U(2^n)$, meaning that it consists of unitary matrices U satisfying $U\mathcal{G}_n U^\dagger = \mathcal{G}_n$. Our main concern will be the *local* Clifford group, $\mathcal{C}_n^l$, which is a subgroup of $\mathcal{C}_n$ consisting of all $n-$fold tensor products of elements in $\mathcal{C}_1$.

An $n-$qubit stabilizer state $|\psi\rangle$ is defined as a simultaneous eigenvector with eigenvalue 1 of n commuting and independent Pauli group elements $M_1, \cdots, M_n$. The state $|\psi\rangle$ is completely determined (up to an overall phase) by the equations

$M_i|\psi\rangle = |\psi\rangle$. The set

$$\mathcal{S} = \{M \in \mathcal{G}_n | \ \ M_i|\psi\rangle = |\psi\rangle\}$$

is called the *stabilizer* of the state $|\psi\rangle$. It is a group of 2^n commuting Pauli operators, all of which have a real overall phase ± 1 and the n operators M_i are called *generators* of $\mathcal{S}$, as each $M \in \mathcal{S}$ can be written as $M = M_1^{x_1} \cdots M_n^{x_n}$, for some $x_i \in \{0, 1\}$.

Graph states, an important subclass of stabilizer states, are defined as follows. Given an $n-$vertex graph with adjacency matrix G, one can define n commuting Pauli operators

$$K_j = \sigma_x^{(j)} \prod_{k=1}^{n} \left(\sigma_z^{(k)}\right)^{g_{kj}},$$

g_{jk} being the entries of the matrix G and $\sigma_x^{(j)}$ being the Pauli operator acting on the j^{th} qubit (and identity elsewhere). The *graph state* $|\psi(G)\rangle$, is the stabilizer state of this set of Pauli matrices, i.e., the state determined by the equation

$$K_j|\psi(G)\rangle = |\psi(G)\rangle, j = 1, \cdots, n.$$

We can now define the action of the local Clifford group on the stabilizer states. Assume that the stabilizer state $|\psi\rangle$ has the stabilizer generators $M_1, \cdots, M_n$. An element of the local Clifford group, U, has the following action on the stabilizer generators:

$$UM_iU^\dagger = N_i \in \mathcal{G}_n,$$

and once again, the Pauli operators N_i's are independent and hence determine a stabilizer state, which is $U|\psi\rangle$ (see [10]). Note that this action does not necessarily map a graph state into a graph state in general, but, there *are* in fact some local Clifford operators which maps a graph state into another graph state. We call two graphs G and H *locally equivalent* when there is a local Clifford operator U such that

$$U|\psi(G)\rangle = |\psi(H)\rangle.$$

The properties of this relationship on graphs has been studies well in details in other

sections of this chapter, as well as in the next chapters.

This concept was already observed from some combinatorial points of view and has been studied in the binary cases (see [5], [6] and [7]). In general, when the field is not binary, this concept has arisen recently in the field of quantum error correcting codes. In the rest of this chapter, and also in the following chapters, we study the properties of locally equivalent graphs deeply and attack and solve a couple of major problems in this area, for instance, verifying efficiently locally equivalent labeled graphs, and counting the number of classes of local equivalency.

2.2 Non-equivalent graph states

Let us again focus on the binary case, where the field is just the field of order 2. In this case, the graphs are just the ordinary graphs. It is known that two graph states are equivalent under local Clifford group if and only if their associated graphs are equivalent under *local complementation* operators (see for instance [10]), by which we mean the following operator. Suppose that v is a vertex of a graph G. To *locally complement* G at v, consider all neighborhoods of v in G and complement the subgraph of G induced by these vertices to obtain a new graph, denoted by $G * v$. Two graphs are called *locally equivalent* if one of them is obtained from the other one by a series of local complementation operators. This concept (in the binary case) has been extensively studied in graph theory, also there is a polynomial time algorithm to recognize whether two unlabeled graphs are locally equivalent or not (see [5], [7]).

A *tree* is a connected graph which contains no cycles. The following theorem is an interesting result on locally equivalent graphs (see [6]).

Theorem 1. *Any two locally equivalent trees are isomorphic.*

Notice that there are graphs which are not locally equivalent to a tree, and [6] presents a polynomial time algorithm to recognize whether a given graph is locally equivalent to a tree or not. This theorem tells us that if two trees are not isomorphic then they are not locally equivalent, so that the number of non-isomorphic trees on

n vertices is a lower bound on the number of graphs which are not mutually locally equivalent.

The following theorem gives us an approximated number of non-isomorphic graphs. One can find a proof for this fact in [15].

Theorem 2. *Let T_n be the number of non-isomorphic trees on n vertices, then*

$$T_n = \frac{\beta^3 \alpha^{9/2}}{4\sqrt{\pi}} \cdot \frac{\alpha^{-n}}{n^{5/2}} + O(\frac{\alpha^{-n}}{n^{7/2}}),$$

where $\alpha \approx 0.3383219$ and $\beta \approx 7.924780$.

We thus obtain the following result, presenting a lower bound for the number of non-equivalent graph states under the action of the local Clifford group, whose graphs are connected and mutually non-isomorphic.

Remark. *Let A_n be the number of graph states whose associated graphs are mutually non-isomorphic trees. Then for large enough values of n,*

$$A_n \approx \frac{\beta^3 \alpha^{9/2}}{4\sqrt{\pi}} \cdot \frac{\alpha^{-n}}{n^{5/2}} \approx 0.5349485 \frac{\alpha^{-n}}{n^{5/2}},$$

where $\alpha \approx 0.3383219$.

Let χ_n be the number of graph states which are not equivalent under the local Clifford group and their associated graphs are connected and mutually non-isomorphic.

Theorem 3. *$A_n \approx 0.5349485 \frac{\alpha^{-n}}{n^{5/2}}$ is a lower bound for χ_n*

We will computationally solve the problem of counting the number of classes of equivalency in chapter 4.

For a fixed graph G, there is an algorithm to count the number of graphs locally equivalent to G (see [7]). This number, of course varies from one graph to another. For instance, the number of graphs locally equivalent to the complete graph over n vertices is $n+1$, but this number for a path of length n is $O((1+\sqrt{3})^n)$. The lower bound presented in the theorem can be compared to the real values of χ_n for small values of n in Table 2.1 (values of χ_n are taken from [12]).

n	$\frac{\log \chi_n}{n}$	$\frac{\log A_n}{n}$
5	0.2772	0.2197
6	0.3996	0.2310
7	0.4654	0.3138
8	0.5768	0.3612
9	0.6763	0.4012
10	0.8049	0.4465
11	0.9643	0.4821
12	1.1714	0.5137

Table 2.1: Values of χ_n

2.3 Non-binary stabilizer codes

The theory of non-binary stabilizer codes and non-binary stabilizer states have been studied widely, see [1], [13]. In this theory the notion of stabilizer codes as well as graph states are defined based on Pauli and Clifford groups. In this section, we establish a description of the action of local Clifford groups on graph states by operations on their graphs.

Through this section, let p be an odd prime number, $\omega = e^{2\pi i/p}$ and $\mathbf{F}_p$ be the finite field of p elements. Also suppose that $\mathbb{C}^p$ is the state space of every particle in the quantum system, and $\{|x\rangle; x \in \mathbf{F}_p\}$ is an orthonormal basis for this space.

Definition. For $a, b \in \mathbf{F}_p$, define unitary operators $X(a)$ and $Z(b)$ on $\mathbb{C}^p$ as follows;

$$X(a)|x\rangle = |x + a\rangle,$$

$$Z(b)|x\rangle = \omega^{bx}|x\rangle.$$

The following properties are proved in [13].

Lemma 1.

(i) $X(a)X(a') = X(a + a'), Z(b)Z(b') = Z(b + b')$ *and* $X(a)^\dagger = X(-a), Z(b)^\dagger = Z(-b)$.

(ii) $\{X(a)Z(b); a, b \in \mathbf{F}_p\}$ *is a basis for the space of operators over* $\mathbb{C}^p$.

(iii) $Z(b)X(a) = \omega^{ab}X(a)Z(b)$.

(iv) *$X(a)Z(b)$ and $X(a')Z(b')$ commute if and only if $ab' - ba' = 0$.*

Using these properties, we can now define the *generalized Pauli group*, generated by these operators, as seen below;

$$\mathcal{G} = \{\omega^c X(a)Z(b); a, b, c \in \mathbf{F}_p\}.$$

Also, the *Pauli group over n particles* is the $n-$fold tensor product of $\mathcal{G}$

$$\mathcal{G}_n = \{\omega^c X(\mathbf{a})Z(\mathbf{b}); \mathbf{a}, \mathbf{b} \in \mathbf{F}_p^n, c \in \mathbf{F}_p\},$$

where $X(\mathbf{a}) = X(\mathbf{a}_1) \otimes X(\mathbf{a}_2) \otimes \cdots \otimes X(\mathbf{a}_n)$ and $Z(\mathbf{b}) = Z(\mathbf{b}_1) \otimes Z(\mathbf{b}_2) \otimes \cdots \otimes Z(\mathbf{b}_n)$. One can easily check that two elements $\omega^c X(\mathbf{a})Z(\mathbf{b})$ and $\omega^{c'} X(\mathbf{a}')Z(\mathbf{b}')$ commute if and only if $\mathbf{a} \cdot \mathbf{b}' - \mathbf{b} \cdot \mathbf{a}' = 0$ (dot product is the ordinary inner product on $\mathbf{F}_p^n$, i.e., $\sum_{i=1}^{n} \mathbf{a}_i \mathbf{b}'_i - \mathbf{a}'_i \mathbf{b}_i = 0$). We are now able to define Clifford groups.

Definition. *Generalized Clifford group $\mathcal{C}_n$ is the normalizer of $\mathcal{G}_n$. Also generalized local Clifford group is the $n-$fold tensor product of Clifford group of order one, i.e., $\mathcal{C}_1 = \mathcal{C}$.*

Suppose that $h \in \mathcal{C}$ and therefore, $hX(1)h^\dagger$ and $hZ(1)h^\dagger$ are elements in $\mathcal{G}$. Set $hX(1)h^\dagger = \omega^c X(a)Z(b)$ and $hZ(1)h^\dagger = \omega^{c'} X(a')Z(b')$. Since $Z(1)X(1) = \omega X(1)Z(1)$, we have $ab' - ba' = 1$. Theorem 4 states that this is the only condition on h necessary to make it in some sense an element of C, see [8].

Theorem 4. *For any a, b, c, a', b' and c' in $\mathbf{F}_p$, such that $ab' - ba' = 1$, there exists $h \in C$ such that $hX(1)h^\dagger = \omega^c X(a)Z(b)$ and $hZ(1)h^\dagger = \omega^{c'} X(a')Z(b')$.*

In order to introduce the notion of stabilizer codes, we should first study some properties of eigenvalues and eigenspaces of elements in $\mathcal{G}_n$.

Lemma 2. *Let $g = \omega^c X(\mathbf{a})Z(\mathbf{b}) \in \mathcal{G}_n$. Then for every positive integer k,*

$$g^k = \omega^{(kc+\binom{k}{2}\mathbf{a}\cdot\mathbf{b})} X(k\mathbf{a})Z(k\mathbf{b}),$$

where $\binom{k}{2}$ is the binomial coefficient.

Proof. We give a proof for this lemma using an induction on k. There is nothing to prove for $k = 1$. Provided the result for k, we have

$$g^{k+1} = \big(\omega^c X(\mathbf{a})Z(\mathbf{b})\big)\big(\omega^{(kc+\binom{k}{2}\mathbf{a}\cdot\mathbf{b})} X(k\mathbf{a})Z(k\mathbf{b})\big)$$

$$= \omega^{((k+1)c+\binom{k}{2}\mathbf{a}\cdot\mathbf{b})} X(\mathbf{a})\big(Z(\mathbf{b})X(k\mathbf{a})\big)Z(k\mathbf{b})$$

$$= \omega^{((k+1)c+\binom{k}{2}\mathbf{a}\cdot\mathbf{b})} X(\mathbf{a})\big(\omega^{k\mathbf{a}\cdot\mathbf{b}} X(k\mathbf{a})Z(\mathbf{b})\big)Z(k\mathbf{b})$$

$$= \omega^{((k+1)c+\binom{k+1}{2}\mathbf{a}\cdot\mathbf{b})} X((k+1)\mathbf{a})Z((k+1)\mathbf{b}).$$

□

Since by definition, $X(p\mathbf{a}) = Id$, $Z(p\mathbf{b}) = Id$ and $\omega^p = 1$, one concludes that $g^p = Id$ for any $g \in \mathcal{G}_n$ (notice that we are now using the fact that p is odd). This statement shows that eigenvalues of the elements of $\mathcal{G}_n$ are the $p-$th roots of the unity, with varying multiplicities.

Lemma 3. *Suppose that $g = \omega^c X(\mathbf{a})Z(\mathbf{b}) \in \mathcal{G}_n$ is not a scalar multiple of the identity. Let*

$$P_j = \frac{1}{p}(Id + \omega^{-j}g + \omega^{-2j}g + \cdots + \omega^{-(p-1)j}g)$$

for $j = 0, 1, \cdots, (p-1)$, then P_j is the projection on ω^j- eigenspace of g. Also all P_j's have the same rank.

Proof. Since $g^p = Id$, clearly $P_j^2 = P_j$ and $gP_j = \omega^j P_j$. Therefore, it is sufficient to prove that P_j's have the same rank. Since g is not a scaler multiple of the identity, at least one of $\mathbf{a}_i$'s or $\mathbf{b}_i$'s is non-zero. For instance, suppose that $\mathbf{a}_i \neq 0$ (the other

case is similar). One can simply verify that

$$Z_i(k)P_jZ_i(-k) = P_{j-k\mathbf{a}_i}$$

holds for every k. Finally, since $\mathbf{a}_i$ is non-zero, all P_j's are conjugates to each other and thus have the same rank. □

We can now define a stabilizer code as a common eigenspace for eigenvalue one, of a subgroup of $\mathcal{G}_n$. It is easy to check that for a subgroup S, similar to the binary case, this common eigenspace is non-trivial provided that S is abelian and does not contain any scalar multiple of identity, except Id itself (see [13]). We call such a subgroup a *valid* one.

In order to define graph states, we should investigate the properties of stabilizer codes more precisely. Consider a valid subgroup S of $\mathcal{G}_n$. Let $S = \langle g_1, \cdots, g_k \rangle$ be a minimal set of generators for S, so that no subset of $\{g_1, \cdots, g_k\}$ generates S. Suppose that $g_i = \omega^{c_i} X(\mathbf{a^i})Z(\mathbf{b^i})$. Since the only scalar multiple of the identity in S is itself, for any $\mathbf{a}, \mathbf{b} \in \mathbf{F}^n$, there exists at most one element of the form $\omega^c X(\mathbf{a})Z(\mathbf{b})$ in S. Therefore, without any kind of ambiguity, in order to represent the elements of S, we can drop the scaler coefficient ω^c from its representation. In this case, for any $\omega^c X(\mathbf{a})Z(\mathbf{b}), \omega^{c'} X(\mathbf{a}')Z(\mathbf{b}') \in S$, we can write

$$(X(\mathbf{a})Z(\mathbf{b}))(X(\mathbf{a}')Z(\mathbf{b}')) \equiv X(\mathbf{a}+\mathbf{a}')Z(\mathbf{b}+\mathbf{b}'),$$

as an equality in S. Therefore, using this notation, the group S is the set of elements $X(\mathbf{a})Z(\mathbf{b})$, such that $(\mathbf{a}, \mathbf{b})$ is in the vector subspace of dimension $2n$, $\mathbf{F}^{2n}$, generated by $(\mathbf{a^i}, \mathbf{b^i})$'s. Therefore, we can define the matrix

$$A = \left(\begin{array}{c|c} \mathbf{a^1} & \mathbf{b^1} \\ \mathbf{a^2} & \mathbf{b^2} \\ \vdots & \vdots \\ \mathbf{a^k} & \mathbf{a^k} \end{array} \right)$$

as a *generating matrix* for S.

The proof of the following properties are straight forward.

Lemma 4. *Using the above notation,*

(i) $S = \{xA; x \in \mathbf{F}^k\}$.

(ii) $rank(A) = k$.

(iii) *Rows of A are orthogonal with respect to the inner product defined as*

$$\langle (\mathbf{a}, \mathbf{b}), (\mathbf{a}', \mathbf{b}') \rangle = \mathbf{a} \cdot \mathbf{b}' - \mathbf{b} \cdot \mathbf{a}'.$$

(iv) *The matrix UA is also a generating matrix for S, for any invertible $k \times k$ matrix U.*

Lemma 5. *Suppose that P_{ij} is the projection over the eigenspace of g_i with respect to the eigenvalue ω^j. Then $P_{10}P_{20}\cdots P_{k0}$ is the projection over the code space. Also, all $P_{1j_1}P_{2j_2}\cdots P_{kj_k}$'s have the same rank.*

Proof. All g_i's commute, and therefore by lemma 3, all P_{ij}'s commute as well and the first argument follows immediately. Since $(\mathbf{a^i}, \mathbf{b^i})$'s are independent, we can find $(\mathbf{e^i}, \mathbf{f^i})$'s, such that $h_i = X(\mathbf{e^i})Z(\mathbf{f^i})$ commutes with each g_l, where $l \neq i$, and also, $h_i g_i h_i^\dagger = \omega^{r_i} g_i$ for arbitrary r_i. In other words, $(\mathbf{e^i}, \mathbf{f^i})$ is orthogonal to all $(\mathbf{a^l}, \mathbf{b^l})$'s but $(\mathbf{a^i}, \mathbf{b^i})$. Now let $h = h_1 h_2 \cdots h_k$, we have $hP_{1j_1}P_{2j_2}\cdots P_{kj_k}h^\dagger = P_{1(j_1 - r_1)}P_{2(j_2 - r_2)}\cdots P_{k(j_k - r_k)}$. Since r_i's are arbitrary, all $P_{1j_1}P_{2j_2}\cdots P_{kj_k}$'s are conjugates to each other, and therefore have the same rank. □

Using this lemma, we conclude that $rank(P_{10}P_{20}\cdots P_{k0}) = p^{n-k}$. Therefore, if we have n independent generators, we get a one dimensional code space, i.e., a *stabilizer state.*

Next, we consider the action of the local Clifford group on stabilizer spaces. If $h = h_1 h_2 \cdots h_n \in \mathcal{C}^{\otimes n}$ is an element of the local Clifford group, then $hSh^\dagger$ is also an abelian subgroup of $\mathcal{G}_n$, and the only scalar multiple of the identity in $hSh^\dagger$ is again

Id itself. If S is the stabilizer group of the state $|\phi\rangle$, then $hSh^\dagger$ is the stabilizer group of some state which is denoted by $h|\phi\rangle$.

Suppose that

$$h_i X(1) h_i{}^\dagger = \omega^{d_i} X(e_i) Z(f_i),$$

$$h_i Z(1) h_i^\dagger = \omega^{d_i'} X(e_i') Z(f_i').$$

We have $e_i f_i' - f_i e_i' = 1$. By a simple calculation, one can check that the generating matrix of $hSh^\dagger$ is the matrix AY, where

$$Y = \begin{pmatrix} E & F \\ E' & F' \end{pmatrix},$$

and

$$E = diag(e_1, \cdots, e_n), F = diag(f_1, \cdots, f_n),$$

$$E' = diag(e_1', \cdots, e_n'), F' = diag(f_1', \cdots, f_n').$$

Lemma 6. *Two stabilizer states with generating matrices A, B are equivalent under the action of the local Clifford group, if and only if there exist invertible matrices U, Y, such that*

$$Y = \begin{pmatrix} E & F \\ E' & F' \end{pmatrix},$$

where

$$E = diag(e_1, \cdots, e_n), F = diag(f_1, \cdots, f_n),$$

$$E' = diag(e_1', \cdots, e_n'), F' = diag(f_1', \cdots, f_n'),$$

and $e_i f_i' - f_i e_i' = 1$, for any i, and $B = UAY$ holds as well.

Proof. The proof follows from the above discussion together with lemma 4. □

This lemma can be restated in the following way

Lemma 6′. *Two stabilizer states with generating matrices A, B are equivalent under the action of the local Clifford group, if and only if there exists an invertible*

matrix Y, such that

$$Y = \begin{pmatrix} E & F \\ E' & F' \end{pmatrix},$$

where

$$E = diag(e_1, \cdots, e_n), F = diag(f_1, \cdots, f_n),$$

$$E' = diag(e'_1, \cdots, e'_n), F' = diag(f'_1, \cdots, f'_n),$$

and $e_i f'_i - f_i e'_i = 1$, for any i, and also, rows of B are orthogonal to rows of AY.

Proof. By lemma 4, rows of B are orthogonal to each other, and $rank(B) = n$. Therefore, rows of B span a vector subspace of dimension n, in the space of dimension $2n$. On the other hand, this subspace is orthogonal to itself, so that any vector orthogonal to rows of B is in this subspace. Now suppose that rows of AY are orthogonal to rows of B. Hence, rows of AY are in the subspace generated by B, and since $rank(AY) = n$, there exists an invertible matrix U such that $B = UAY$.

The other direction follows from lemma 6.

□

We can now define the concept of *graph states*, and their associated labeled graphs.

Definition. A *graph state* is the code space related to the group with a generating matrix of the form $\begin{pmatrix} Id_n & | & M \end{pmatrix}$, where M is a symmetric matrix with zero diagonal. We assign to such a graph state a labeled graph, with labels coming from the matrix M, i.e., with label M_{ij} for the edge $\{ij\}$.

Theorem 5. *Every stabilizer state is equivalent to a graph state with respect to the local Clifford group.*

Proof. Consider a stabilizer state with generating matrix A. By lemma 4, A is a full-rank matrix and its rows are orthogonal. Moreover, since by lemma 6 we can apply a linear transformation of determinant one on any pair of columns i and $(n+i)$, we may assume that the first $n \times n$ block of A is invertible. Then, we apply an invertible matrix U such that the first block of UA is identity. Using the fact that the rows of UA are orthogonal, we conclude that the second block of UA is symmetric. Notice

that, even though this symmetric matrix may have non-zero diagonal entries, but by applying the determinant one linear operations on pair of columns, we end up with a matrix with an identity in the first block, and a symmetric matrix with zero diagonal in the second block.

□

Similar to the binary case in [10], we want to describe the action of the local Clifford group as operations on graphs.

Definition. Let G be a labeled graph on vertex set $\{1, 2, \cdots, n\}$, such that the label of the edge $\{i, j\}$ is the $ij-$th entry of matrix M, where M is a symmetric matrix over $\mathbf{F}_p$ with zero diagonal. For every vertex v, and $0 \neq b \in \mathbf{F}_p$, define the operator $\circ_b v$ on the graph as follows; $G \circ_b v$ is the graph on the same vertex set, with label matrix $I(v,b)MI(v,b)$, where $I(v,b) = diag(1, 1, \cdots, b, \ldots, 1)$, b being on the $v-$th entry.

Also, for any vertex w and number $a \in \mathbf{F}_p$, define the operator $*_a w$ on the graph as follows; $G *_a w$ is the graph on the same vertex set, with label matrix M', where $M'_{jk} = M_{jk} + aM_{vj}M_{vk}$ for $j \neq k$, and $M'_{jj} = 0$ for all j.

Theorem 6. *Two graph states G and H with label matrices M and N over $\mathbf{F}_p$, are equivalent under local Clifford group if and only if there exists a sequence of $*$ and $\circ$ operators acting on one of them to obtain the other one.*

Proof. Let $A = \begin{pmatrix} Id_n & | & M \end{pmatrix}$ and $B = \begin{pmatrix} Id_n & | & N \end{pmatrix}$ be the generating matrices of these two graph states. If these two states are equivalent, by lemma 6, there exist matrices U and $Y = \begin{pmatrix} E & F \\ E' & F' \end{pmatrix}$ satisfying the conditions mentioned in lemma 6, such that $B = UAY$.

For every i, let

$$Y_i = \begin{pmatrix} E_i & F_i \\ E'_i & F'_i \end{pmatrix},$$

where

$$E_i = diag(1, \cdots, 1, e_i, 1, \cdots, 1, 1),$$

$$F_i = diag(0, \cdots, 0, f_i, 0, \cdots, 0),$$

$$E'_i = diag(0, \cdots, 0, e'_i, 0, \cdots, 0),$$

$$F'_i = diag(1, \cdots, 1, f'_i, 1, \cdots, 1).$$

Then Y_i's commute mutually, and $Y = Y_1 Y_2 \cdots Y_n$. We call Y *trivial* if $E = Id_n$ and $E' = 0$.

We prove the theorem by induction on the number of non-trivial matrices Y_i's. If all Y_i's are trivial, then $AY = \begin{pmatrix} Id_n & | & D \end{pmatrix}$, for some matrix D. Therefore $U = Id_n$, as well as $Y = Id_{2n}$ and $A = B$. Thus, suppose that at least one of the Y_i's is non-trivial.

We consider two cases;

Case (i). $e_{i_0} \neq 0$ for some i_0, where Y_{i_0} is non-trivial. Let $AY_{i_0} = \begin{pmatrix} V & | & D \end{pmatrix}$. Therefore,

$$V = \begin{pmatrix} 1 & 0 & \cdots & e'_{i_0} M_{1 i_0} & \cdots & 0 \\ 0 & 1 & & \vdots & & 0 \\ \vdots & & \ddots & \vdots & & \vdots \\ \vdots & & & e_{i_0} & & \vdots \\ \vdots & & & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & e'_{i_0} M_{n i_0} & \cdots & 1 \end{pmatrix}$$

In order to invert V, one should multiply the i_0-th row by $e_{i_0}^{-1}$, and then multiply it by $-e'_{i_0} M_{j i_0}$ and finally add it to $j-$th row, for any $j \neq i_0$.

Therefore, $V^{-1} AY_{i_0} = \begin{pmatrix} Id_n & | & V^{-1} D \end{pmatrix}$. Also, the jk entry of $V^{-1} D$, for $j \neq k$ and both unequal to i_0, is

$$(V^{-1} D)_{jk} = M_{jk} - e'_{i_0} e_{i_0}^{-1} M_{ij} M_{ik},$$

and the $i_0 j$ entry is

$$(V^{-1} D)_{i_0 j} = e_{i_0}^{-1} M_{ij}.$$

$V^{-1}D$ may have non-zero entries on its diagonal. But there exists a trivial matrix Y', such that $V^{-1}AY_{i_0}Y'$ is equal to $V^{-1}AY_{i_0}$, except on the entries of the diagonal of the second block, which are all zero for the matrix $V^{-1}AY_{i_0}Y'$. Therefore $V^{-1}AY_{i_0}Y'$ is the generating matrix of a graph state, and by the above equalities, this graph state is

$$G *_{i_0} (-e_{i_0}^{-1}e'_{i_0}) \circ_{i_0} e_{i_0}^{-1}$$

On the other hand, we have

$$B = UAY = UV(V^{-1}AY_{i_0}Y')(Y'^{-1}Y''),$$

where Y'' is equal to the multiplication of all Y_j's except Y_{i_0}. We now observe that $V^{-1}AY_{i_0}Y'$ is a graph obtained from G, via operations $*$ and $\circ$. Also the number of non-trivial terms in $Y'^{-1}Y''$ is less than this number in Y, and therefore by induction, the claim is proved.

Case (ii). $e_i = 0$ for all i's that Y_i is non-trivial. Suppose that Y_{i_0} is non-trivial. If for every non-trivial Y_j, $M_{i_0 j} = 0$, then the i_0-th row of the first block of AY is zero and hence, it would not be invertible and the first block of UAY can not be the identity. Thus, there exists an i_1, such that Y_{i_1} is non-trivial and $M_{i_0 i_1} \neq 0$. Then the first block of the matrix $AY_{i_0}Y_{i_1}$ is

$$V = \begin{pmatrix} 1 & \cdots & e'_{i_0}M_{1i_0} & e'_{i_1}M_{1i_1} & \cdots & 0 \\ 0 & \ddots & \vdots & \vdots & & 0 \\ \vdots & & 0 & e'_{i_1}M_{i_0 i_1} & & \vdots \\ \vdots & & e'_{i_0}M_{i_1 i_0} & 0 & & \vdots \\ 0 & & \vdots & \vdots & \ddots & 0 \\ 0 & \cdots & e'_{i_0}M_{ni_0} & e'_{i_1}M_{ni_1} & \cdots & 1 \end{pmatrix}$$

In order to invert V, one should multiply the i_0-th and the i_1-th rows by $(e'_{i_1}M_{i_0 i_1})^{-1}$ and $(e'_{i_0}M_{i_1 i_0})^{-1}$, respectively, and then multiply the i_1-th row by $-e'_{i_0}M_{ji_0}$ and add it to the $j-$th row, for any j. And the same process for the i_0-th row. No-

tice that $e_{i_0}f'_{i_0} - e'_{i_0}f_{i_0} = 1$ and $e_{i_0} = 0$,therefore $e'_{i_0}f_{i_0} = -1$ and consequently, e'_{i_0} is non-zero. Also the same is true for e'_{i_1}. After this, one should switch the rows i_0 and i_1. By this process we get a matrix with the identity in the first block as well as a symmetric matrix on the second block. But the diagonal elements of this block may be non-zero. By multiplying by an appropriate trivial matrix Y', we get

$$A' = V_{-1}AY_{i_0}Y_{i_1}Y' = \left(Id_n \quad | \quad M'\right),$$

where M' is the matrix of a graph G' such that

$$M'_{jk} = M_{jk} - M^{-1}_{i_0i_1}M_{i_0j}M_{i_1k} - M^{-1}_{i_0i_1}M_{i_1j}M_{i_0k}.$$

Now, one can see that

$$G' = G \circ_{(-M^{-1}_{i_0i_1})} i_0 *_1 i_0 *_{(-1)} i_1 *_1 i_0 \circ_{(e'^{-1}_{i_0}M^{-1}_{i_0i_1})} i_0 \circ_{(e'^{-1}_{i_1})} i_1.$$

We have $B = UV^{-1}A'Y'^{-1}Y''$, where Y'' is equal to the multiplication of all Y_j's, except Y_{i_0} and Y_{i_1}. Also the number of non-trivial terms in $Y'^{-1}Y'$ is strictly less than this number in Y, and therefore, by induction, the claim is proved.

The other direction of the theorem is an immediate consequence of the first direction. □

2.4 Local measurement of Pauli group

The theorem 6 tells us that the action of the local Clifford group can be translated into operations on graphs. We do the same process for local measurement of Pauli group. Suppose that the stabilizer group of a state is generated by $g_1, g_2, \cdots, g_n$ and we measure $h \in \mathcal{G}_n$. Assume that $g_i^{-1}hg_i = \omega^{c_i}h$. If c_i's are all zero then h commutes with all of g_i's, and therefore the outcome of the measurement is the state itself, with the unchanged stabilizer group. Otherwise, there exists at least one non-zero c_i. By changing the set of generators for stabilizer group we can assume that c_1 is non-zero,

and $c_i = 0$, $i = 2, \cdots, n$. Therefore $\omega^{-c}h, g_2, \cdots, g_n$ is a set of generators for the state after the measurement, in which c is the outcome of measurement. We use this idea to translate the local Pauli measurement to operations on graphs. In order to do so, we need the following definition.

Definition. Suppose that G is a labeled graph on $\mathbf{F}_p$. If v is a vertex of G, define $d(v)G$ to be a graph on the same vertex set, but all edges connected to v have zero labels.

Theorem 7. *Suppose that we have a graph state with label matrix M and we measure the operator $X_i(a)$ on the $i-$th qudit. Then if $M_{ij} = 0$ for all $j = 1, \cdots, n$ then the state remains unchanged, and if $M_{ij} \neq 0$ for some j, then the state after the measurement is equivalent to*

$$d(i)\big(G \circ_{(M_{ij}^{-2})} i \circ_{(-M_{ij})} j \circ_{(M_{ij}^{-2})} i\big).$$

Proof. If $M_{ij} = 0$ for all j, then $X_i(a)$ commutes with the stabilizer group, and therefore, that the state remains unchanged after the measurement. Thus, let us suppose that $M_{ij} \neq 0$ for some j, and let $\alpha = M_{ij}$. Now $U\begin{pmatrix} Id_n & | & M \end{pmatrix}$ is also a generating matrix for the graph state, where

$$U = \begin{pmatrix} 1 & 0 & \cdots & -\alpha^{-1}M_{1i} & \cdots & 0 \\ 0 & 1 & & -\alpha^{-1}M_{2i} & & 0 \\ \vdots & & \ddots & \vdots & & \vdots \\ \vdots & & & 1 & & \vdots \\ \vdots & & & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & -\alpha^{-1}M_{ni} & \cdots & 1 \end{pmatrix}$$

(non-zero off-diagonal entries are on $j-$th column). Now, we observe that $X_i(a)$ commutes with all of the rows of $U\begin{pmatrix} Id_n & | & M \end{pmatrix}$, except the $j-$th one. Hence, if we replace the $j-$th row by

$$(0, \cdots, 0, a, 0, \cdots, 0 \mid 0, \cdots, 0),$$

we obtain the generating matrix for the new state. On the other hand, every stabilizer state is equivalent to a graph state under the local Clifford group, and if we apply this process to the new generating matrix we end up with the generating matrix $\Big(Id_n \mid M'\Big)$, where M' is the matrix of the the graph

$$d(i)\big(G \circ_{(M_{ij}^{-2})} i \circ_{(-M_{ij})} j \circ_{(M_{ij}^{-2})} i\big).$$

□

The changes occurred by measuring the operator $X_i(a)Z_i(b)$ on a graph state is presented in the following theorem.

Theorem 8. *Consider a graph state with label matrix M, and suppose that one measures the operator $X_i(a)Z_i(b)$ on the $i-th$ qudit, where a and b are non-zero numbers. Then the state after measurement is equivalent to $d(i)\big(G \circ_{(ab^{-1})} i\big)$.*

Proof. First, suppose that $M_{ij} = 0$ for each j. In this case $X_i(a)Z_i(b)$ commutes with all of the generators, except the $i-$th one. Now, if we replace it by

$$(0, \cdots, 0, a, 0, \cdots, 0 \mid 0, \cdots, 0, b, 0, \cdots, 0),$$

where a and b both locate on the $i-$th entry, then, using the local Clifford group, we obtain the same generating matrix and the same graph. Also, notice that in this case, $d(i)\big(G \circ_{(ab^{-1})} i\big)$ is the same as G.

Therefore, let us assume that $M_{ij} \neq 0$ for some j, and let $\alpha = M_{ij}$. Clearly, $(U + \alpha a^{-1} b \delta_{ij}) \Big(Id_n \mid M\Big)$ is also a generating matrix for the stabilizer group, where

$$U = \begin{pmatrix} 1 & 0 & \cdots & -\alpha^{-1}M_{1i} & \cdots & 0 \\ 0 & 1 & & -\alpha^{-1}M_{2i} & & 0 \\ \vdots & & \ddots & \vdots & & \vdots \\ \vdots & & & 1 & & \vdots \\ \vdots & & & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & -\alpha^{-1}M_{ni} & \cdots & 1 \end{pmatrix}$$

(once again, non-zero off-diagonal entries are on $j-$th column). It is easy to check that all of the rows of $(U + \alpha a^{-1} b \delta_{ij}) \left(Id_n \mid M \right)$, except the $j-$th row, commute with $X_i(a)Z_i(b)$. Therefore, if we replace it by a row equivalent to $X_i(a)Z_i(b)$ we get a generator for the new state. Applying the algorithm to get a graph state from this state, we obtain that the new graph is $d(i)\big(G \circ_{(ab^{-1})} i\big)$. □

Finally, measuring the operator $Z_i(b)$ has some effects on the graph states, described below in details.

Theorem 9. *Suppose that G is a graph state with label matrix M and we measure the operator $Z_i(b)$ on the $i-$th qudit, where b is non-zero. The state after this measurement is equivalent to $d(i)G$.*

Proof. Consider the generating matrix $\left(Id_n \mid M \right)$ of the graph state. We know that all of the rows of this matrix, except the $i-$th one, are orthogonal to the row-representation of $Z_i(b)$, which is $(0, \cdots, 0 \mid 0, \cdots, 0, b, 0, \cdots, 0)$. Therefore, after the measurement, the stabilizer group is in fact the group generated by the rows of $\left(Id_n \mid M \right)$, except the $i-$th one and $Z_i(b)$. Therefore, the stabilizer state, after deleting the $i-$th qudit, is $d(i)G$. □

Chapter 3

An Efficient Algorithm to Recognize Locally Equivalent Graphs

3.1 Isotropic systems and locally equivalent graphs

We have studied the action of local Clifford groups on graphs when the order of the field is a prime number, and translated it into combinatorial operations $*$ and $\circ$. We consider these two operators in general, when the order of the field is a power of some prime number, and investigate the properties of these operations on arbitrary graphs.

Assume that p is an odd prime number, and $\mathbf{F}_q$ is the field of q elements with characteristic p. Suppose that G is a graph on n vertices. We call G a labeled graph on $\mathbf{F}_q$, if labels of its edges form an $n \times n$ symmetric matrix $G = (g_{ij})$ with zero diagonal over $\mathbf{F}_q$, where g_{ij} is the label of edge ij. We restate a few definitions and notations from the previous chapter.

Definition. Let G be a labeled graph with labels forming a symmetric matrix $G = (g_{ij})$ on $\mathbf{F}_q$. For vertex v of G and a number $a \in \mathbf{F}_q$, define $G *_a v$ to be a graph with the label matrix $G' = (g'_{ij})$ such that for all i, $g'_{vi} = g_{vi}$, and for i, j inequal to v,

$$g'_{ij} = g_{ij} + a g_{vi} g_{vj},$$

and moreover, G' is symmetric with zero diagonal.

Also for a non-zero number $b \in \mathbf{F}_q$ define $G \circ_b v$ to be a graph with the label matrix $G' = (g'_{ij})$ such that for all i, $g'_{iv} = bg_{iv}$, and $g'_{ij} = g_{ij}$ if i, j are inequal to v, and again, G' is symmetric with zero diagonal.

Two graphs G and G' are called *locally equivalent* if there exists a sequence of the above operations, acting on G to obtain G'. Notice that these operations are invertible, so that this relation is an equivalency relation.

Let $\mathbf{F}_q^n$ be the $n-$ dimensional vector space over $\mathbf{F}_q$. For vectors

$$X = (x_1, \cdots, x_n), Y = (y_1, \cdots, y_n),$$

consider the standard bilinear form

$$\langle X, Y \rangle = \sum_{i=1}^{n} x_i y_i.$$

$\langle ., . \rangle$ is a non-degenerate, symmetric bilinear form. Using this form, we define a non-degenerate anti-symmetric bilinear form on $\mathcal{V} = \mathbf{F}_q^{2n}$, the $2n-$dimensional vector space over the field $\mathbf{F}_q$. For vectors (X, X') and (Y, Y') in $\mathcal{V}$, set

$$\langle (X, X'), (Y, Y') \rangle = (X, X') \cdot \Lambda \cdot (Y, Y')^T,$$

where

$$\Lambda = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$

In other words,

$$\langle (X, X'), (Y, Y') \rangle = \langle X, Y' \rangle - \langle X', Y \rangle.$$

Due to the nature of anti-symmetric forms, we are now in the situation of introducing a geometrically known concept, *isotropic systems.*

Definition. A subspace $\mathcal{W}$ of $\mathcal{V}$ is called an *isotropic system* , if it is an $n-$dimensional subspace and $\langle (X, X'), (Y, Y') \rangle = 0$, for any $(X, X'), (Y, Y') \in \mathcal{W}$. In fact, since

$dim\mathcal{W} = n$ and $\langle .,. \rangle$ is a non-degenerate bilinear form, we have

$$\mathcal{W} = \{V \in \mathcal{V} : \langle V, W \rangle = 0, \forall W \in \mathcal{W}\}. \tag{3.1}$$

For every graph G, define

$$\mathcal{W}_G = \{X \cdot \begin{pmatrix} I & | & G \end{pmatrix} : X \in \mathbf{F}_q^n\},$$

where $\begin{pmatrix} I & | & G \end{pmatrix}$ is a matrix with two $n \times n$ blocks which the first one is identity. Since the matrix G is symmetric,

$$\begin{pmatrix} I & | & G \end{pmatrix} \cdot \Lambda \cdot \begin{pmatrix} G & | & -I \end{pmatrix}^T = G^T - G = 0,$$

and one can easily conclude that $\mathcal{W}_G$ forms an isotropic system which is called the *isotropic system associated to* G.

Definition. *Suppose that A is a $2n \times 2n$ matrix*

$$A = \begin{pmatrix} Z & T \\ X & Y \end{pmatrix},$$

consisting of four diagonal matrices $X = diag(x_1, \cdots, x_n), Y = diag(y_1, \cdots, y_n)$, $Z = diag(z_1, \cdots, z_n)$ and $T = diag(t_1, \cdots, t_n)$. A is called normal if

$$Y \cdot Z - X \cdot T = I.$$

Notice that every normal matrix is invertible, its inverse is normal as well, and in addition the multiplication of normal matrices is again normal. In particular, when $Z = I$ and $X = 0$, A is called trivial.

For an isotropic system $\mathcal{W}$ and a normal matrix A, define $\mathcal{W} \cdot A = \{W \cdot A : W \in \mathcal{W}\}$. One can verify that $\mathcal{W} \cdot A$ is also an isotropic system.

Two isotropic systems $\mathcal{W}$ and $\mathcal{W}'$ are called *locally equivalent* if there exists a normal matrix A such that $\mathcal{W}' = \mathcal{W} \cdot A$. By the above properties, it is clear that this

is an equivalency relation. The importance of this relation is clear once we state the following theorem.

Theorem 10. *Two graphs G and H on the same vertex sets are locally equivalent if and only if their associated isotropic systems are locally equivalent.*

Proof. For the *only if* part, it is sufficient to show that the systems $\mathcal{W}_G, \mathcal{W}_{G*_a i}$, and also the systems $\mathcal{W}_G, \mathcal{W}_{G\circ_b i}$ are locally equivalent. First, note that the rows of $\begin{pmatrix} I & | & G *_a i \end{pmatrix}$ form a basis for $\mathcal{W}_{G*_a i}$. Let

$$A = \begin{pmatrix} Z & T \\ X & Y \end{pmatrix},$$

where $X = diag(0, \cdots, 0, -a, 0, \cdots, 0), Y = I, Z = I$ and $T = 0$. We just need to check that the rows of $\begin{pmatrix} I & | & G \end{pmatrix} \cdot A$ are orthogonal to the rows of $\begin{pmatrix} I & | & G *_a i \end{pmatrix}$. Consider the $j-$th row of $\begin{pmatrix} I & | & G \end{pmatrix} \cdot A$, and the $k-$th row of $\begin{pmatrix} I & | & G *_a i \end{pmatrix}$. If $j \neq i$, and $k \neq i$, the product of these two rows is $(g_{jk} + a g_{ik} g_{ij} - a g_{ij} g_{ik}) - (g_{jk}) = 0$. If $j = i$ and $k \neq i$, it is $(g_{ik}) - (g_{ik}) = 0$, and finally, if $j \neq i$, and $k = i$ then this product is again $(g_{ij}) - (g_{ij}) = 0$. Also the $i-$th row of these matrices are equal, and therefore according to the definition of the inner product, these rows are orthogonal to each other, and thus, $\mathcal{W}_G$ and $\mathcal{W}_{G*_a i}$ are locally equivalent.

Similarly, for $\mathcal{W}_G, \mathcal{W}_{G\circ_b i}$, let

$$B = \begin{pmatrix} Z' & T' \\ X' & Y' \end{pmatrix},$$

where $X' = 0$, $T' = 0$ and

$$Y' = diag(1, \cdots, 1, b, 1, \cdots, 1), Z' = diag(1, \cdots, 1, b^{-1}, 1, \cdots, 1)$$

. Similar to the previous case, one can easily check that the rows of $\begin{pmatrix} I & | & G \end{pmatrix} \cdot B$ and $\begin{pmatrix} I & | & G \circ_b i \end{pmatrix}$ are orthogonal, and therefore, $\mathcal{W}_G, \mathcal{W}_{G\circ_b i}$ are locally equivalent.

To prove the *if* part, suppose that $\mathcal{W}_G$ and $\mathcal{W}_H$ are locally equivalent. Then there

exists a normal matrix

$$A = \begin{pmatrix} Z & T \\ X & Y \end{pmatrix},$$

where

$$X = diag(x_1, \cdots, x_n), Y = diag(y_1, \cdots, y_n),$$

$$Z = diag(z_1, \cdots, z_n), T = diag(t_1, \cdots, t_n),$$

such that the rows of $\begin{pmatrix} I & | & G \end{pmatrix} \cdot A$ form a basis for the isotropic system $\mathcal{W}_H$. Therefore there exists an invertible matrix U such that $U \cdot \begin{pmatrix} I & | & G \end{pmatrix} \cdot A = \begin{pmatrix} I & | & H \end{pmatrix}$.

For every i, let

$$A_i = \begin{pmatrix} Z_i & T_i \\ X_i & Y_i \end{pmatrix},$$

where

$$Z_i = diag(1, \cdots, 1, z_i, 1, \cdots, 1), T_i = diag(0, \cdots, 0, t_i, 0, \cdots, 0),$$

$$X_i = diag(0, \cdots, 0, x_i, 0, \cdots, 0), Y_i = diag(1, \cdots, 1, y_i, 1, \cdots, 1).$$

The matrices A_i's all commute and $A = A_1 A_2 \cdots A_n$.

We prove the theorem by an induction on the number of non-trivial matrices A_i. If all A_i's are trivial then A is also trivial, and we have

$$\begin{pmatrix} I & | & G \end{pmatrix} \cdot A = \begin{pmatrix} I & | & G \end{pmatrix} \cdot \begin{pmatrix} I & T \\ 0 & Y \end{pmatrix} = \begin{pmatrix} I & | & T + GY \end{pmatrix}.$$

Therefore we have $U \cdot \begin{pmatrix} I & | & T + GY \end{pmatrix} = \begin{pmatrix} I & | & H \end{pmatrix}$. Looking at the first blocks in this equation we get $U = I$, and $T + GY = H$. The diagonal of H is zero, and hence $T = 0$. Also A is a normal matrix and therefore, $A = I$ and $G = H$. Hence, suppose that at least one of A_i's is non-trivial.

Let us consider two cases:

Case(i). $z_{i_0} \neq 0$ for some i_0, where A_{i_0} is non-trivial. Let $\begin{pmatrix} I & | & G \end{pmatrix} A_{i_0} = \begin{pmatrix} V & | & D \end{pmatrix}$. Then

$$V = \begin{pmatrix} 1 & 0 & \cdots & x_{i_0} g_{1 i_0} & \cdots & 0 \\ 0 & 1 & & \vdots & & 0 \\ \vdots & & \ddots & \vdots & & \vdots \\ \vdots & & & z_{i_0} & & \vdots \\ \vdots & & & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & x_{i_0} g_{n i_0} & \cdots & 1 \end{pmatrix}.$$

In order to invert V, we should multiply the i_0-th row by $z_{i_0}^{-1}$, and then by $-x_{i_0} g_{j i_0}$ and add it to the $j-$th row, for any $j \neq i_0$.

Thus $V^{-1}\left(I \mid G\right) A_{i_0} = \left(I \mid V^{-1}D\right)$, and the $jk-$th entry of $V^{-1}D$, for j inequal to k, i_0, is

$$(V^{-1}D)_{jk} = g_{jk} - z_{i_0}^{-1} x_{i_0} g_{i_0 j} g_{i_0 k}.$$

Also for $j \neq i_0$,

$$(V^{-1}D)_{j i_0} = (V^{-1}D)_{i_0 j} = z_{i_0}^{-1} g_{i_0 j}.$$

The matrix $V^{-1}D$ may have non-zero entries on its diagonal. But, by elementary linear algebra, there exists a trivial matrix A', such that $V^{-1}\left(I \mid G\right) A_{i_0} A'$ is equal to $V^{-1}\left(I \mid G\right) A_{i_0}$ except for the entries on the diagonal of the second block, which are zero. Therefore the rows of $V^{-1}\left(I \mid G\right) A_{i_0} A'$ span an isotropic system associated to some graph, and by the mentioned equalities, this graph is nothing but $G *_{(-z_{i_0}^{-1} x_{i_0})} i_0 \circ_{(z_{i_0}^{-1})} i_0$.

On the other hand, we have

$$\left(I \mid H\right) = U\left(I \mid G\right) A = UV(V^{-1}\left(I \mid G\right) A_{i_0} A')(A'^{-1} A''),$$

where A'' is equal to the multiplication of all A_j's, except A_{i_0}.

Now $V^{-1}\left(I \mid G\right) A_{i_0} A'$ is an isotropic system, associated to the graph

$$G *_{(-z_{i_0}^{-1} x_{i_0})} i_0 \circ_{z_{i_0}} i_0.$$

Also the number of non-trivial terms in $A'^{-1} A''$ is strictly less than the number of

non-trivial terms in A, and therefore, by induction, we obtain the desired result.

Case(ii). $z_i = 0$ for all i's, where A_i is non-trivial. Notice that, in this case $x_i \neq 0$ for any i, where A_i is non-trivial, since A is a normal matrix and $y_i z_i - x_i t_i = 1$. Now, suppose that A_{i_0} is non-trivial. If for every non-trivial A_j, $g_{i_0 j} = 0$, then the i_0-th row of the first block of $\begin{pmatrix} I & | & G \end{pmatrix} A$ is zero. Hence, it is not invertible and the first block of $U \begin{pmatrix} I & | & G \end{pmatrix} A$ can not be identity. Thus, there exists an i_1, such that A_{i_1} is non-trivial and $g_{i_0 i_1} \neq 0$. Therefore, the first block of $\begin{pmatrix} I & | & G \end{pmatrix} A_{i_0} A_{i_1}$ is

$$V = \begin{pmatrix} 1 & \cdots & x_{i_0} g_{1 i_0} & x_{i_1} g_{1 i_1} & \cdots & 0 \\ 0 & \ddots & \vdots & \vdots & & 0 \\ \vdots & & 0 & x_{i_1} g_{i_0 i_1} & & \vdots \\ \vdots & & x_{i_0} g_{i_1 i_0} & 0 & & \vdots \\ 0 & & \vdots & \vdots & \ddots & 0 \\ 0 & \cdots & x_{i_0} g_{n i_0} & x_{i_1} g_{n i_1} & \cdots & 1 \end{pmatrix}.$$

In order to invert V, one has to multiply the i_0-th and the i_1-th rows by $(x_{i_1} g_{i_0 i_1})^{-1}$ and $(x_{i_0} g_{i_1 i_0})^{-1}$ respectively, and then multiply the row i_1 by $-x_{i_0} g_{j i_0}$ and add it to the $j-$th row, for any j. Also, exactly the same process for row i_0 must be done. After this, we should change the rows i_0 and i_1. By this process we get a matrix with identity in the first block and a symmetric matrix on the second block. But the diagonal elements of this block may be non-zero. In order to handle this issue, by multiplying by an appropriate trivial matrix A', we get

$$V^{-1} \begin{pmatrix} I & | & G \end{pmatrix} A_{i_0} A_{i_1} A' = \begin{pmatrix} I & | & G' \end{pmatrix},$$

where $G' = (g'_{jk})$ is the graph with entries

$$g'_{jk} = g_{jk} - g_{i_0 i_1}^{-1} g_{i_0 j} g_{i_1 k} - g_{i_0 i_1}^{-1} g_{i_1 j} g_{i_0 k},$$

for all $j, k \neq i_0, i_1$, and

$$g'_{i_0 j} = x_{i_0}^{-1} g_{i_0 i_1}^{-1} g_{i_1 j},$$

$$g'_{i_1 j} = x_{i_1}^{-1} g_{i_0 i_1}^{-1} g_{i_0 j},$$

for all $j \neq i_0, i_1$. Moreover

$$g_{i_0 i_1} = -x_{i_0}^{-1} x_{i_1}^{-1} g_{i_0 i_1}^{-1}.$$

Therefore,

$$G' = G \circ_{(-g_{i_0 i_1}^{-1})} i_0 *_1 i_0 *_{(-1)} i_1 *_1 i_0 \circ_{(x_{i_0}^{-1} g_{i_0 i_1}^{-1})} i_0 \circ_{(x_{i_1}^{-1})} i_1.$$

We have $\begin{pmatrix} I & | & H \end{pmatrix} = UV \begin{pmatrix} I & | & G' \end{pmatrix} A'^{-1} A''$, where A'' is equal to the multiplication of all A_j's, except A_{i_0} and A_{i_1}. Also the number of non-trivial terms in $A'^{-1}A''$ is strictly less than this number in A, and therefore by induction, the result is proved.

□

3.2 System of equations and normal matrices

Let G and H be two graphs, and g, h be their neighborhood functions respectively, meaning that $g(i)$ is a vector such that its $j-$th coordinate, g_{ij}, is the label of the edge ij in G. The same holds for the graph H and the function h. Using theorem 10 and relation (3.1) in the definition of isotropic systems, one obtains that G and H are locally equivalent if there exists a normal matrix

$$A = \begin{pmatrix} Z & T \\ X & Y \end{pmatrix},$$

such that rows of $\begin{pmatrix} I & | & G \end{pmatrix} \cdot A$ are all orthogonal to the rows of $\begin{pmatrix} I & | & H \end{pmatrix}$. This condition is equivalent to the following:

$$\langle X, g(i) \times h(j) \rangle - \langle Y, g(i) \times e_j \rangle + \langle Z, e_i \times h(j) \rangle - \langle T, e_i \times e_j \rangle = 0, \tag{3.2}$$

for any two vertices i, j, where $u \times v$, for vectors u and v of the same size, is a vector of their size, whose $k-$th coordinate is the product of the $k-$th coordinates of u and

v. Also e_i is a vector whose all coordinates are zero except the $i-$th, which is one. Here in the latter formula, and later on, we look at the diagonal $n \times n$ matrices as vectors of size n when necessary.

Let $\mathbf{F}_q^{4n}$ be the space of the vectors of the form (X, Y, Z, T) associated with the following symmetric bilinear form

$$((X, Y, Z, T), (X', Y', Z', T')) \mapsto$$

$$\langle (X, Y, Z, T), (X', Y', Z', T') \rangle = \langle X, X' \rangle - \langle Y, Y' \rangle + \langle Z, Z' \rangle - \langle T, T' \rangle.$$

Moreover, for any pair of vertices i, j, we define the following function, so called *Lambda Function*, which plays a key role in the whole section.

$$\lambda(i, j) = \Big(g(i) \times h(j), g(i) \times e_j, e_i \times h(j), e_i \times e_j \Big),$$

and

$$\lambda(G, H) = Span\{\lambda(i, j) : \ i, j\}$$

.

Using the bilinear form, one can rewrite the original problem in the following way:

Given the graphs G and H on the same vertex set of size n, there exists an efficient algorithm (polynomial in n) to verify whether or not there exists a vector (X, Y, Z, T) orthogonal to $\lambda(G, H)$ satisfying $Y \times Z - X \times T = I$.

We now develop some more technical tools to attack this problem. For $\phi = (X, Y, Z, T) \in \mathbf{F}_q^{4n}$, let

$$\phi^1 = (-Z, -T, -X, -Y),$$

$$\phi^2 = (Y, X, T, Z),$$

and for $\alpha \in \mathbf{F}_q^{4n}$, $a \in \mathbf{F}_q$ and $l = 1, 2$ define

$$\phi *_{l,a} \alpha = \phi - a\phi^l \times \alpha,$$

and for any subspace N of $\mathbf{F}_q^{4n}$,

$$N *_{l,a} \alpha = \{\phi *_{l,a} \alpha : \phi \in N\}.$$

Lemma 7. *Let $\alpha \in \mathbf{F}_q^{4n}$ be such that $\alpha \times \alpha^l = 0$ for $l = 1, 2$. For $\phi, \psi \in \mathbf{F}_q^{4n}$, and any subspace N of $\mathbf{F}_q^{4n}$, the following properties hold:*

(i) *$\phi \to \phi *_{l,a} \alpha$ is bijective.*

(ii) $\langle \phi *_{l,a} \alpha, \psi *_{l,a} \alpha^l \rangle = \langle \phi, \psi \rangle$.

(iii) $(N *_{l,a} \alpha)^\perp = N^\perp *_{l,a} \alpha^l$.

Proof. For (i), by a simple induction one can check that after k times iteration we get $\phi *_{l,a} \alpha \cdots *_{l,a} \alpha = \phi - ka\phi^l \times \alpha$. Therefore after p iteration we end up with the identity map, and hence $\phi \to \phi *_{l,a} \alpha$ is a bijection.

For (ii), using the facts that $\langle \phi \times \psi'^l, \psi^l \rangle = -\langle \phi^l \times \psi', \psi \rangle$ and $\langle \phi, \psi \times \psi' \rangle = \langle \phi \times \psi', \psi \rangle$, we have

$$\langle \phi *_{l,a} \alpha, \psi *_{l,a} \alpha^l \rangle = \langle \phi, \psi \rangle - a\langle \phi, \psi^l \times \alpha^l \rangle - a\langle \phi^l \times \alpha, \psi \rangle + a^2 \langle \phi^l \times \alpha, \psi^l \times \alpha^l \rangle$$

$$= \langle \phi, \psi \rangle - a\langle \phi \times \alpha^l, \psi^l \rangle - a\langle \phi^l \times \alpha, \psi \rangle + a^2 \langle \phi^l \times \alpha \times \alpha^l, \psi^l \rangle = \langle \phi, \psi \rangle.$$

(iii) is a direct consequence of (ii). □

In the next two theorems, we study the effect of local operations on the set $\lambda(G, H)^\perp$, and observe that this set is well-behaved under these types of operators.

Theorem 11. *Let G and H be two graphs on the same vertex set with neighborhood functions g and h, respectively. For every vertex i,*

(i) $\lambda(G *_a i, H) = \lambda(G, H) *_{1,a} (-g(i) \times g(i), -g(i) \times g(i), -e_i, -e_i)$.

(ii) $\lambda(G, H *_a i) = \lambda(G, H) *_{2,a} (h(i) \times h(i), e_i, h(i) \times h(i), e_i)$.

And more importantly,

(iii) $\lambda(G *_a i, H)^{\perp} = \lambda(G, H)^{\perp} *_{1,a} (e_i, e_i, g(i) \times g(i), g(i) \times g(i))$.

(iv) $\lambda(G, H *_a i)^{\perp} = \lambda(G, H)^{\perp} *_{2,a} (e_i, h(i) \times h(i), e_i, h(i) \times h(i))$.

Proof. The proof of part (ii) is similar to the proof of part (i). Also parts (iii) and (iv) are immediate consequences of (i), (ii) and the third part of lemma 7. Hence we just need to prove the first part.

Suppose that g' is the neighborhood function of $G *_a i$. Then we have

$$g'(j) = g(j) + ag_{ij}g(i) - ag_{ij}^2 e_j.$$

The space $\lambda(G *_a i, H)$ is generated by $\lambda'(j,k)$'s, where

$$\lambda'(j,k) = \Big(g'(j) \times h(k), g'(j) \times e_k, e_j \times h(k), e_j \times e_k\Big)$$

$$= \lambda(j,k) + ag_{ij}\Big(g(i) \times h(k), g(i) \times e_k, 0, 0\Big) - ag_{ij}^2\Big(e_j \times h(k), e_j \times e_k, 0, 0\Big)$$

$$= \lambda(j,k) + ag_{ij}\Big(\lambda(i,k) - (0, 0, e_i \times h(k), e_i \times e_k)\Big) - ag_{ij}^2\Big(e_j \times h(k), e_j \times e_k, 0, 0\Big).$$

Set $\lambda''(j,k) = \lambda'(j,k) - ag_{ij}\lambda'(i,k)$. It is easy to check that $\lambda''(j,k)$'s also generate the space $\lambda(G *_a i, H)$, and we have

$$\lambda''(j,k) = \lambda(j,k) + ag_{ij}\lambda(i,k) - ag_{ij}\Big(0, 0, e_i \times h(k), e_i \times e_k\Big)$$

$$-ag_{ij}^2\Big(e_j \times h(k), e_j \times e_k, 0, 0\Big) - ag_{ij}\lambda(i,k)$$

$$= \lambda(j,k) - a\Big(0, 0, g(j) \times e_i \times h(k), g(j) \times e_i \times e_k\Big)$$

$$-a\Big(g(i) \times g(i) \times e_j \times h(k), g(i) \times g(i) \times e_j \times e_k, 0, 0\Big)$$

$$= \lambda(j,k) - a\Big(e_j \times h(k), e_j \times e_k, g(j) \times h(k), g(j) \times e_k\Big) \times \Big(g(i) \times g(i), g(i) \times g(i), e_i, e_i\Big)$$

$$= \lambda(j,k) *_{1,a} \Big(- g(i) \times g(i), -g(i) \times g(i), -e_i, -e_i\Big).$$

Therefore $\lambda(G *_a i, H) = \lambda(G, H) *_{1,a} (-g(i) \times g(i), -g(i) \times g(i), -e_i, -e_i)$.

□

For any $0 \neq b \in \mathbf{F}_q$ and vertex i, define

$$f_{b,i} = I + (b-1)e_i = (1, \cdots, 1, b, 1, \cdots, 1).$$

Theorem 12. *Let G and H be two graphs on the same vertex sets with neighborhood functions g and h, respectively. For every vertex i,*

(i) *The map $\phi \longrightarrow \phi \times (f_{b_1,i}\ , f_{b_2,i}\ , f_{b_3,i}\ , f_{b_4,i})$ is bijective, for non-zero elements $b_1, b_2, b_3, b_4 \in \mathbf{F}_q$.*

(ii) $\lambda(G \circ_b i, H)^{\perp} = \lambda(G, H)^{\perp} \times (f_{b^{-1},i}\ , f_{b^{-1},i}\ , f_{b,i}\ , f_{b,i})$.

(iii) $\lambda(G, H \circ_b i)^{\perp} = \lambda(G, H)^{\perp} \times (f_{b^{-1},i}\ , f_{b,i}\ , f_{b^{-1},i}\ , f_{b,i})$.

Proof. The proof of (i) is straight forward. To prove (ii), notice that g', the neighborhood function of $G \circ_b i$, is given by $g'(j) = g(j) \times f_{b,i}$ if $j \neq i$, and $g'(i) = bg(i)$. Hence, if $\langle \phi, \lambda(j,k) \rangle = 0$, then

$$\langle \phi \times (f_{b^{-1},i}\ , f_{b^{-1},i}\ , f_{b,i}\ , f_{b,i}), \lambda'(j,k) \rangle = 0,$$

where $\lambda'(j,k) = \Big(g'(j) \times h(k), g'(j) \times e_k, e_j \times h(k), e_j \times e_k\Big)$. Part (iii) is similar to (ii).

□

We now define the *determinant function* for a vector in $\mathbf{F}^{4n}$. For a vector $\phi = (X, Y, Z, T)$, set

$$det\, \phi = Y \times Z - X \times T.$$

Some straight forward computations easily lead to the proof of the following lemma.

Lemma 8.

(i) $det\, \phi = det\, \phi *_{1,a} (e_i, e_i, g(i) \times g(i), g(i) \times g(i))$.

(ii) $det\, \phi = det\, \phi *_{2,a} (e_i, g(i) \times g(i), e_i, g(i) \times g(i))$.

(iii) $\det\ \phi = det\, \phi \times (f_{b^{-1},i}, f_{b^{-1},i}, f_{b,i}, f_{b,i})$.

(iv) $\det \phi = det\,\phi \times (f_{b^{-1},i}, f_{b,i}, f_{b^{-1},i}, f_{b,i})$.

□

Note that the functions we see on the right hand side of parts (i) to (iv) in this lemma is exactly the ones appear in theorems 11 and 12, and hence this lemma states the determinant function is invariant under the action of $*$ and $\circ$.

In the new setting, the problem of verifying whether or not two graphs G, H are locally equivalent, is equivalent to finding a vector $\phi \in \mathbf{F}_q^{4n}$ such that $\phi \in \lambda(G,H)^{\perp}$ and $det\,\phi = I$. Let $\Lambda(G,H) = \lambda(G,H)^{\perp}$, and $\sigma(G,H)$ be the set of solutions, i.e., vectors $\phi \in \Lambda(G,H)$ satisfying $det\,\phi = I$.

To sum up, theorems 11, 12 together with lemma 8, give the following picture; if graphs G_1, G_2 are locally equivalent, as well as the graphs H_1, H_2, then there exists a (linear) bijection β, such that

$$\Lambda(G_2,H_2) = \beta(\Lambda(G_1,H_1)),$$

$$\sigma(G_2,H_2) = \beta(\sigma(G_1,H_1)).$$

Even though the function β depends on G_1, G_2, H_1 and H_2, but it gives us useful information on the locally equivalent graphs, namely, if two graphs G and H are locally equivalent, then roughly speaking, the relative linear position of $\sigma(G,H)$ inside $\Lambda(G,H)$ is exactly the same as the relative linear position of $\sigma(G,G)$ inside $\Lambda(G,G)$. For instance, once we prove that for every graph G, $\sigma(G,G)$ is a *large* subset of $\Lambda(G,G)$, in the sense that it contains a linear subspace of small co-dimension, then the same must be true for $\sigma(G,H)$ inside $\Lambda(G,H)$, when G and H are locally equivalent.

3.3 Internal solutions

As seen already, we have shown that in fact for locally equivalent graphs G_1 and G_2, and again locally equivalent graphs H_1 and H_2, there exists a linear bijection β, such that

$$\Lambda(G_2,H_2) = \beta(\Lambda(G_1,H_1)),$$

$$\sigma(G_2, H_2) = \beta(\sigma(G_1, H_1)).$$

In this section and the next one, we show that in fact $\sigma(G, G)$ is a *large* subset of $\Lambda(G, G)$, in the sense that it contains a linear subspace of co-dimension ≤ 5. Consequently, by existence of the bijection β, the same must be true for $\sigma(G, H)$ inside $\Lambda(G, H)$ when G and H are locally equivalent.

Definition. *Internal solutions for a graph G are vectors (X, Y, Z, T) in $\sigma(G, G)$.*

Using the condition 3.2, now we can assume that there is just one graph involved instead of two. We rewrite the condition 3.2 in this particular case, i.e., assuming that $G = H$.

$$\langle X, g(i) \times g(j) \rangle = (Y(j) - Z(i))g_{ij}, \text{ for every } i \neq j, \tag{3.3}$$

$$\langle X, g(i) \times g(i) \rangle = T(i), \text{ for every } i. \tag{3.4}$$

Lemma 9. *Assume that the graph G is connected. Then, for every (X, Y, Z, T) $\in \Lambda(G, G)$, the function $Y + Z$ on the vertices is constant, i.e., $Y + Z = aI$ for some number a.*

Proof. Assume that i, j are two adjacent vertices in G. The condition (3.3) implies that

$$\langle X, g(i) \times g(j) \rangle = (Y(j) - Z(i))g_{ij},$$

$$\langle X, g(i) \times g(j) \rangle = (Y(i) - Z(j))g_{ji}.$$

Therefore $Y(i) + Z(i) = Y(j) + Z(j)$, for any two adjacent vertices. Connectivity of G implies the desired conclusion.

□

From now on, we assume that G is a connected graph. Lemma 9 gives us a partitioning of the set $\Lambda(G, G)$, as follows:

$$\Lambda_a(G, G) = \{(X, Y, Z, T) \in \Lambda(G, G) : Y + Z = aI\}.$$

Notice that for any $a \in \mathbf{F}_q$, $(0, aI, aI, 0) \in \Lambda_{2a}(G, G)$, and $\Lambda_{2a}(G, G) = \Lambda_0(G, G) + (0, aI, aI, 0)$. Therefore, since q is an odd number, all $\Lambda_a(G, G)$'s are just shifts of $\Lambda_0(G, G)$.

Definition. Consider a connected graph, G. We call ij an edge of G if $g_{ij} \neq 0$. For an even cycle C in G consisting of (ordered) vertices $i_1, i_2, \cdots i_{2l}$, let

$$v(C) = \sum_{k=1}^{2l} (-1)^k g_{i_k i_{k+1}}^{-1} g(i_k) \times g(i_{k+1}).$$

We define $\nu(G)$, called the *bineighborhood space* of G, to be the subspace generated by the vectors $g(i) \times g(j)$ for i, j satisfying $g_{ij} = 0$, as well as by $v(C)$'s for even cycles C, i.e.,

$$\nu(G) = Span\{\{v(C) : \ C \text{ even cycle}\} \cup \{g(i) \times g(j) : \ g_{ij} = 0\}\}.$$

Theorem 13. *For $X \in \mathbf{F}_q^n$, there exist Y, Z and T such that $(X, Y, Z, T) \in \Lambda_0(G, G)$ if and only if X is orthogonal to $\nu(G)$. Moreover, if G has an odd cycle, for every $X \in \nu(G)^\perp$, there exists a unique (X, Y, Z, T) in $\Lambda_0(G, G)$.*

Proof. Fix a vector X, and assume that there exists some $(X, Y, Z, T) \in \Lambda_0(G, G)$. For any two vertices i, j with $g_{ij} = 0$, $\langle X, g(i) \times g(j) \rangle = (Y(i) + Y(j)) g_{ij} = 0$. Moreover, if $i_1, i_2, \cdots, i_{2l}$ is a cycle then we have

$$\langle X, (-1)^k g_{i_k i_{k+1}}^{-1} g(i_k) \times g(i_{k+1}) \rangle = (-1)^k (Y(i_k) + Y(i_{k+1})).$$

By summing up all of these equalities for $k = 1, 2, \cdots, 2l$ we get that X is orthogonal to $\nu(C)$ (for every cycle C) and hence, to the whole space $\nu(G)$.

For the other direction, suppose that $X \in \nu(G)^\perp$. For any vertex i, set $T(i) = \langle X, g(i) \times g(i) \rangle$, and $Z = -Y$. In the case that G has an odd cycle, Y would be uniquely determined by (3.3) on the vertices of that odd cycle. Since G is connected, then one can determine the function Y on the rest of the vertices, and since $X \in \nu(G)^\perp$

there is no ambiguity in the definition of Y.

In the case that G contains no odd cycles, we can fix $Y(i)$ for some arbitrarily chosen vertex i, and then determine the other components in terms of $Y(i)$ and once again, since $X \in \nu(G)^{\perp}$ and there is no odd cycle, there is no ambiguity in its definition.

□

Even though the determinant is a quadratic function and not a linear one, but in this setting, the set $\Lambda(G,G)$ satisfies some property that helps us study this set more deeply, as stated in the following theorem.

The problem of verifying locally equivalent graphs on one or two vertices is a trivial problem, and hence, from now on we assume that the number of vertices of G is more than 2.

Theorem 14. *For every $\phi \in \Lambda(G,G)$, the determinant of ϕ is constant.*

Proof. First, notice that one may restrict himself to study the case $\phi \in \Lambda_0(G,G)$, since there exists a vector $(X,Y,-Y,T) \in \Lambda_0(G,G)$ and $a \in \mathbf{F}_q$ such that $\phi = (X,Y,-Y,T) + a(0,I,I,0)$, and $det\,\phi = det(X,Y,-Y,T) + a^2 I$. Hence suppose that $\phi = (X,Y,-Y,T) \in \Lambda_0(G,G)$.

If G has at most two vertices, the proof is clear. Let us assume that $n \geq 3$, and i_1, i_2 are two adjacent vertices in G. Showing that $(det\,\phi)_{i_1} = (det\,\phi)_{i_2}$ gives us the desired result. By lemma 8, local complementing operations, $*$ and $\circ$, do not change the determinant, therefore we can assume that i_1 and i_2 have a common neighbor j_0 by applying one $*$ operator if needed. One has

$$g_{rs}(Y(r) + Y(s)) = \langle X, g(r) \times g(s) \rangle,$$

for each pair of inequal $r, s \in \{j_0, i_1, i_2\}$. Consequently,

$$Y(i_1) = \frac{1}{2}\Big[g_{i_1 i_2}^{-1}\langle X, g(i_1) \times g(i_2)\rangle + g_{i_1 j_0}^{-1}\langle X, g(i_1) \times g(j_0)\rangle$$
$$-g_{i_2 j_0}^{-1}\langle X, g(i_2) \times g(j_0)\rangle\Big],$$

and

$$Y(i_2) = \frac{1}{2}\Big[g^{-1}_{i_1 i_2}\langle X, g(i_1)\times g(i_2)\rangle + g^{-1}_{i_2 j_0}\langle X, g(i_2)\times g(j_0)\rangle$$
$$-g^{-1}_{i_1 j_0}\langle X, g(i_1)\times g(j_0)\rangle\Big].$$

On the other hand, $T(r) = \langle X, g(r)\times g(r)\rangle$, for any vertex r. Hence, in order to prove $(det\,\phi)_{i_1} = (det\,\phi)_{i_2}$, we should show that

$$-\frac{1}{4}\Big[g^{-1}_{i_1 i_2}\langle X, g(i_1)\times g(i_2)\rangle + g^{-1}_{i_1 j_0}\langle X, g(i_1)\times g(j_0)\rangle$$
$$-g^{-1}_{i_2 j_0}\langle X, g(i_2)\times g(j_0)\rangle\Big]^2 - X(i_1)\langle X, g(i_1)\times g(i_1)\rangle$$

$$= -\frac{1}{4}\Big[g^{-1}_{i_1 i_2}\langle X, g(i_1)\times g(i_2)\rangle + g^{-1}_{i_2 j_0}\langle X, g(i_2)\times g(j_0)\rangle$$
$$-g^{-1}_{i_1 j_0}\langle X, g(i_1)\times g(j_0)\rangle\Big]^2 - X(i_2)\langle X, g(i_2)\times g(i_2)\rangle,$$

or equivalently

$$g^{-1}_{i_1 i_2}\langle X, g(i_1)\times g(i_2)\rangle\Big[g^{-1}_{i_2 j_0}\langle X, g(i_2)\times g(j_0)\rangle - g^{-1}_{i_1 j_0}\langle X, g(i_1)\times g(j_0)\rangle\Big]$$
$$= X(i_1)\langle X, g(i_1)\times g(i_1)\rangle - X(i_2)\langle X, g(i_2)\times g(i_2)\rangle.$$

Let

$$C_j = g^{-1}_{i_2 j}\langle X, g(i_2)\times g(j)\rangle - g^{-1}_{i_1 j}\langle X, g(i_1)\times g(j)\rangle,$$

for any j adjacent to both i_1 and i_2. Since X is orthogonal to the cycle j_0, i_1, j, i_2, for any j adjacent to i_1, i_2, we have $C_{j_0} = C_j$. On the other hand if either $g_{i_1 j}$ or $g_{i_2 j}$ is zero, then

$$g_{i_1 j} g_{i_2 j} X(j) C_{j_0} = 0,$$

and

$$X(j)(g_{i_1 j}\langle X, g(i_2)\times g(j)\rangle - g_{i_2 j}\langle X, g(i_1)\times g(j)\rangle) = 0,$$

because, for instance if $g_{i_1 j} = 0$, then X is orthogonal to $g(i_1) \times g(j)$.

Therefore we have

$$\langle X, g(i_1) \times g(i_2)\rangle \Big[g^{-1}_{i_2 j_0} \langle X, g(i_2) \times g(j_0)\rangle - g^{-1}_{i_1 j_0} \langle X, g(i_1) \times g(j_0)\rangle \Big] =$$

$$\Big(\sum_{j \neq i_1, i_2} g_{i_1 j} g_{i_2 j} X(j) \Big) \Big[g^{-1}_{i_2 j_0} \langle X, g(i_2) \times g(j_0)\rangle - g^{-1}_{i_1 j_0} \langle X, g(i_1) \times g(j_0)\rangle \Big] =$$

$$\sum_{j \neq i_1, i_2} g_{i_1 j} g_{i_2 j} X(j) \Big[g^{-1}_{i_2 j_0} \langle X, g(i_2) \times g(j_0)\rangle - g^{-1}_{i_1 j_0} \langle X, g(i_1) \times g(j_0)\rangle \Big] =$$

$$\sum_{j \neq i_1, i_2} g_{i_1 j} g_{i_2 j} X(j) \Big[g^{-1}_{i_2 j} \langle X, g(i_2) \times g(j)\rangle - g^{-1}_{i_1 j} \langle X, g(i_1) \times g(j)\rangle \Big] =$$

$$\sum_{j \neq i_1, i_2} X(j) \Big[g_{i_1 j} \langle X, g(i_2) \times g(j)\rangle - g_{i_2 j} \langle X, g(i_1) \times g(j)\rangle \Big] =$$

$$\sum_{j \neq i_1, i_2} \sum_{k=1}^{n} g_{i_1 j} g_{i_2 k} g_{kj} X(j) X(k) - g_{i_2 j} g_{i_1 k} g_{kj} X(j) X(k) =$$

$$0 + \sum_{j \neq i_1, i_2} \sum_{k = i_1, i_2} g_{i_1 j} g_{i_2 k} g_{kj} X(j) X(k) - g_{i_2 j} g_{i_1 k} g_{kj} X(j) X(k) =$$

$$\sum_{j=1}^{n} g_{i_1 i_2} g^2_{i_1 j} X(i_1) X(j) - \sum_{j=1}^{n} g_{i_1 i_2} g^2_{i_2 j} X(i_2) X(j) =$$

$$g_{i_1 i_2} \Big[X(i_1) \langle X, g(i_1) \times g(i_1)\rangle - X(i_2) \langle X, g(i_2) \times g(i_2)\rangle \Big],$$

which completes the proof. □

3.4 Linearity of the kernel of *det* function

Using theorem 14, we may give another partitioning of the set $\Lambda(G, G)$ as follows,

$$\Lambda^{\alpha}(G, G) = \{\phi \in \Lambda(G, G) : det\, \phi = \alpha I\},$$

and combining with the previous partitioning, we set

$$\Lambda^{\alpha}_{a}(G, G) = \Lambda_a(G, G) \cap \Lambda^{\alpha}(G, G).$$

Notice that Λ_0 is a linear subspace since it is the kernel of a linear map. But generally the determinant function is not a linear function when q is not a power of 2. Here, due to the nature and strength of theorem 14, we will show that despite of not being a linear function, the kernel of the determinant exhibit some linear properties. More precisely, we show that $\Lambda_0^0(G,G)$ is a linear subspace if $dim\,\Lambda(G,G) \geq 5$.

In order to provide a proof for that, for any

$$\phi = (X, Y, -Y, T), \phi' = (X', Y', -Y', T') \in \Lambda_0(G,G),$$

let us define

$$\Psi(\phi, \phi') = 2Y \times Y' + X \times T' + X' \times T.$$

Notice that $\Psi(\phi, \phi')$ is constant, because *det* is a constant function and

$$\Psi(\phi, \phi') = det\,\phi + det\,\phi' - det\,(\phi + \phi').$$

Also to prove the linearity of $\Lambda_0^0(G,G)$, one can sufficiently show that $\Psi(\phi, \phi') = 0$ for any $\phi, \phi' \in \Lambda_0^0(G,G)$. The following series of lemmas provide us with the necessary tools.

Lemma 10. *Suppose that* $\phi_i = (X_i, Y_i, -Y_i, T_i) \in \Lambda_0(G,G)$ *for* $i = 1, 2$, *and morever,* $\phi_1 \in \Lambda_0^0(G,G)$. *Also suppose that* $\Psi(\phi_1, \phi_2) = aI$ *for some* $0 \neq a \in \mathbf{F}_q$. *Then on every vertex, either* X_1 *or* X_2 *is non-zero.*

Proof. Assume that $X_1(i) = 0$, for some vertex $i \in \{1, 2, \cdots, n\}$. Since $det\,\phi_1 = 0$, one has $-Y_1(i)^2 - X_1(i)T_1(i) = 0$ and therefore, $Y_1(i) = 0$. Hence the $i-$th component of $\Psi(\phi_1, \phi_2)$ is $X_2(i)T_1(i) = a \neq 0$ and thus $X_2(i) \neq 0$.

□

Lemma 11. *Let* $\phi_i = (X_i, Y_i, -Y_i, T_i) \in \Lambda_0^0(G,G)$ *for* $i = 1, 2$, *and* $\psi = (U, V, -V, W) \in \Lambda_0^0(G,G)$. *Moreover, assume that* $\Psi(\phi_1, \phi_2) = aI$ *for some* $0 \neq a \in \mathbf{F}_q$, *and* $\Psi(\phi_1, \psi) = 0$. *Then* $Supp(U) \subseteq Supp(X_1)$, *in the sense that if* U *is non-zero on some vertex, then so is* X_1.

Proof. For any $r \in \mathbf{F}_q$, we have $\Psi(\phi_1, r\psi + \phi_2) = aI \neq 0$. Therefore by lemma 10, $Supp(X_1) \cup Supp(rU + X_2) = \{1, 2, \cdots, n\}$. Now suppose that $X_1(i) = 0$ for some $i \in \{1, 2, \cdots, n\}$, and $U(i) \neq 0$. There exists some $r_0 \in \mathbf{F}_q$ such that $r_0 U(i) + X_2(i) = 0$. Thus $i \notin Supp(X_1) \cup Supp(r_0 U + X_2)$, which contradicts the earlier statement.

□

The third lemma is the following:

Lemma 12. *Suppose that $\phi_i = (X_i, Y_i, -Y_i, T_i) \in \Lambda_0^0(G, G)$ for $i = 1, 2$, such that $Supp(X_1)$ and $Supp(X_2)$ are minimal subsets of $\{1, 2, \cdots, n\}$ with $\Psi(\phi_1, \phi_2) \neq 0$. If $\psi = (U, V, -V, W) \in \Lambda_0^0(G, G)$ and $\Psi(\phi_1, \psi) = 0$, then either $\psi = 0$ or $U = -a^{-1}cX_1$, where $\Psi(\phi_1, \phi_2) = aI$ and $\Psi(\phi_2, \psi) = cI$.*

Proof. First assume that $c = 0$. In this case we have $\Psi(r\psi + \phi_1, \phi_2) = aI$, for any $r \in \mathbf{F}_q$. If $U(i) \neq 0$ for some $i \in \{1, 2, \cdots n\}$, then there exists $r_0 \in \mathbf{F}_q$ such that $r_0 U(i) + X_1(i) = 0$. Thus, using lemma 11, $Supp(U) \subseteq Supp(X_1)$ and hence $Supp(r_0 U + X_1)$ is a proper subset of $Supp(X_1)$. Moreover, $\Psi(r_0\psi + \phi_1, \phi_2) = aI$ and $det(r_0\psi + \phi_1) = r_0^2 det\ \psi + det\ \phi_1 - r_0\Psi(\psi, \phi_1) = 0$. Then $r_0\psi + \phi_1 \in \Lambda_0^0(G, G)$, which contradict the minimality of ϕ_1, ϕ_2. Therefore $U = 0$.

Now assume that $c \neq 0$. Once again, by lemma 11, $Supp(U) \subseteq Supp(X_1)$ and $Supp(X_1) \subseteq Supp(U)$. Suppose that $U(i) \neq 0$ for some $i \in \{1, \cdots, n\}$. There exists some $r_0 \in \mathbf{F}_q$ such that $r_0 U(i) + X_1(i) = 0$, and also, $\Psi(r_0\psi + \phi_1, \phi_2) = (r_0 c + a)I$. By the minimality of ϕ_1 and ϕ_2, one concludes that $r_0 c + a = 0$. Therefore $-ac^{-1}U(i) + X_1(i) = 0$ for any i satisfying $U(i) \neq 0$. Therefore $U = -a^{-1}cX_1$.

□

Finally, the last lemma we need is a fact in number theory.

Lemma 13. *Given a 3×3 matix A with entries in $\mathbf{F}_q$, there exists a non-zero vector $\mathbf{x} \in \mathbf{F}_q^3$ so that $\mathbf{x}^T \cdot A \cdot \mathbf{x} = 0$.*

Proof. There are many ways to prove this lemma, and one straight forward computational way is as follows. Let us rewrite the matrix equation as a degree two numeric

equation,

$$ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2fyz = 0.$$

In the case that $abc = 0$ then there exists a solution to the equation, for instance $(1, 0, 0)$ when $a = 0$. Thus, we assume that $abc \neq 0$.

Solving the latter equation in terms of z using *the square root of delta* formula, we obtain that the problem is equivalent to this one: *does delta have a square root?* In other words, it is equivalent to finding a non-trivial solution to the following equation,

$$\alpha x^2 + \beta y^2 + 2\gamma xy = t^2,$$

where $\alpha = e^2 - ac, \beta = f^2 - bc$ and $\gamma = ef - cd$.

Once again, if $\alpha = 0$ then $(x, y, t) = (1, 0, 0)$ is a solution, and if not, by solving it in terms of x, we get the next equation,

$$\theta y^2 = s^2 - \alpha t^2,$$

where $\theta = \gamma^2 - \alpha\beta$.

We set $y = 1$. Changing $s, t \in \mathbf{F}_q$, each of the functions $s^2 - \theta$ and αt^2 obtains $(q + 1)/2$ different elements. Therefore there is at least one solution (y, s, t), where $y = 1$. □

Now we have all the necessary tools in hand, to provide a proof for the linearity of $\Lambda_0^0(G, G)$.

Theorem 15. *Suppose that* $dim\, \Lambda_0(G, G) \geq 5$. *then* $\Psi \equiv 0$ *on* $\Lambda_0^0(G, G)$, *or equivalently,* $\Lambda_0^0(G, G)$ *is a linear subspace.*

Proof. First of all, we can assume that G has an odd cycle. Because we already know that by local complementation, the linear properties of $\Lambda(G, G)$, the determinant and so the function Ψ, do not change. Under this assumption, as we observed in theorem 13, if $\phi_i = (X_i, Y_i, -Y_i, T_i) \in \Lambda_0(G, G)$, $i = 1, 2$, and $X_1 = X_2$, then $\phi_1 = \phi_2$.

Now suppose that Ψ is not zero, and let $\phi_i = (X_i, Y_i, -Y_i, T_i) \in \Lambda_0^0(G, G)$, $i = 1, 2$, such that X_1, X_2 are minimal elements of $\{1, 2, \cdots, n\}$ (in the sense of lemma

12) satisfying $\Psi(\phi_1, \phi_2) = aI$, where $0 \neq a \in \mathbf{F}_q$. Since $dim\, \Lambda_0(G,G) \geq 5$, there exist elements $\psi_j = (U_j, V_j, -V_j, W_j) \in \Lambda_0(G,G)$, $j = 1,2,3$, independent of ϕ_1 and ϕ_2. Set $\Psi(\phi_1, \psi_j) = b_j$ and $\Psi(\phi_2, \psi_j) = c_j$ for $j = 1,2,3$, and also define $\omega_j = a\psi_j - c_j\phi_1 - b_j\phi_2$, for $j = 1,2,3$. One can easily verify that $\Psi(\phi_i, \omega_j) = 0$, for every $i = 1,2$ and $j = 1,2,3$. Using lemma 13, we can find a non-trivial solution of $det\,(r_1\omega_1 + r_2\omega_2 + r_3\omega_3) = 0$, where $r_1, r_2, r_3 \in \mathbf{F}_q$. Thus, $r_1\omega_1 + r_2\omega_2 + r_3\omega_3 \in \Lambda_0^0(G,G)$ and $\Psi(\phi_i, r_1\omega_1 + r_2\omega_2 + r_3\omega_3) = 0$, $i = 1,2$. Therefore, by lemma 12 the first coordinate of $r_1\omega_1 + r_2\omega_2 + r_3\omega_3$ is zero and also by theorem 13, we conclude that $r_1\omega_1 + r_2\omega_2 + r_3\omega_3 = 0$, which is a contradiction. Hence, $\Psi(\phi_1, \phi_2) = 0$ for every $\phi_1, \phi_2 \in \Lambda_0^0(G,G)$, and $\Lambda_0^0(G,G)$ is a linear subspace.

□

We can say much more about this subspace. Having constant determinant as well as its linearity, makes it a significantly helpful to study $\sigma(G,G)$ whose description is our main goal in this section. In fact, the following lemmas tell us that this linear space, $\Lambda_0^0(G,G)$, is really a *large* subspace in the whole space $\Lambda(G,G)$.

Lemma 14. *The codimention of* $\Lambda_0^0(G,G)$ *in* $\Lambda_0(G,G)$ *is at most two, provided that* $dim\, \Lambda_0(G,G) \geq 5$.

Proof. Consider three independent vectors $\phi_1, \phi_2, \phi_3 \in \Lambda_0(G,G)$. For numbers c_1, c_2 and c_3,

$$det\,(c_1\phi_1 + c_2\phi_2 + c_3\phi_3) = c_1^2 det\,(\phi_1) + c_2^2 det\,(\phi_2) + c_3^2 det\,(\phi_3)$$

$$+c_1c_2\Psi(\phi_1, \phi_2) + c_1c_3\Psi(\phi_1, \phi_3) + c_2c_3\Psi(\phi_2, \phi_3).$$

By lemma 13, there exists $(c_1, c_2, c_3) \neq 0$ such that $det\,(c_1\phi_1 + c_2\phi_2 + c_3\phi_3) = 0$ which means that $c_1\phi_1 + c_2\phi_2 + c_3\phi_3 \in \Lambda_0^0(G,G)$. Thus, the codimension of $\Lambda_0^0(G,G)$ inside $\Lambda_0(G,G)$ is at most two. □

Since q is an odd number, the translation of $\Lambda_0(G,G)$ by the vectors $(0, aI, aI, 0)$, for different values $a \in \mathbf{F}_q$, gives the whole space $\Lambda(G,G)$. Therefore, codimension of $\Lambda_0(G,G)$ in $\Lambda(G,G)$ is one. Also, $\Lambda_0^0(G,G) + (0, I, I, 0) = \Lambda_2^1(G,G)$. On the other

hand, by the definition of σ, $\sigma(G,G) \supseteq \Lambda_2^1(G,G)$. Therefore we conclude the following corollary:

Corollary 1. *There exists an affine linear subspace inside $\sigma(G,G)$, whose codimention in the whole space $\Lambda(G,G)$ is at most 3, provided that $\Lambda(G,G)$ has dimension not less than 5. Putting these together, in general the codimension of this affine subspace is at most 5.*

Having the mentioned property in hand, together with the β function introduced earlier, we can now give the desired description of $\sigma(G,H)$ for equivalent graphs G and H, which creates the foundations of our algorithm determining whether two graphs are equivalent or not.

Theorem 16. *If the connected graphs G and H, defined on the same vertex sets, are locally equivalent, then the codimension of some affine linear subset of $\sigma(G,H)$ inside $\Lambda(G,H)$ is at most 5.*

3.5 The algorithm

We now have all the tools to describe in details and provide the proofs for an efficient algorithm to determine whether two graphs are equivalent or not. The algorithm is the following.

Suppose that G and H are two connected graphs (notice that by local complementation a connected graph remains connected), with neighborhood functions g and h. Consider the linear system of equations:

$$\langle X, g(i) \times h(j) \rangle - \langle Y, g(i) \times e_j \rangle + \langle Z, e_i \times h(j) \rangle - \langle T, e_i \times e_j \rangle = 0, \tag{3.5}$$

for any two vertices i, j, and for X, Y, Z and T in $\mathbf{F}_q^n$, together with the equation

$$Y \times Z - X \times T = I. \tag{3.6}$$

Assume that $\mathcal{B}$ is an arbitrary basis for $\Lambda(G, H)$, the set of solutions to the linear equation (3.5), which can be computed efficiently. According to the corollary 1 and theorem 16 in the previous section, if there exist solutions to (3.5) and (3.6), then there exists an affine subset, denoted by Γ, in $\Lambda(G, H)$ with $codim \leq 5$, whose elements all satisfy both (3.5) and (3.6). The following lemma takes the advantage of this property.

Lemma 15. *For any basis $\mathcal{B}$ of a linear space Λ, and every affine subspace Γ of Λ of codim ≤ 5, there exists a vector $u \in \Gamma$, which is a linear combination of at most five elements of $\mathcal{B}$.*

Proof. Consider the set $\Gamma' = \{u - v : u, v \in \Gamma\}$ which is a subspace of Λ, and the *canonical projection* $p : \Lambda \rightarrow \Lambda/\Gamma'$. The set $p(\mathcal{B})$ generates Λ/Γ', and therefore there exists a basis $\{p(b_1), \cdots, p(b_k)\}$ for Λ/Γ', where $k = dim\,(\Lambda) - dim\,(\Gamma') \leq 5$. Since Γ is affine, $\Gamma \in \Lambda/\Gamma'$ and hence can be written as the linear combination of $p(b_i)$'s, which means that there exists a vector $u \in \Gamma$ which is a linear combination of at most five elements of $\mathcal{B}$.

□

By this lemma, we can now consider all of the linear combinations of every 5 elements of $\mathcal{B}$, and check whether or not it satisfies the condition (3.6). If at least one of them satisfies (3.6), then the answer is *positive*, and is *negative* otherwise.

Notice that solving this problem for the *unconnected* graphs is an immediate consequence of solving it for the connected graphs, since the local operators preserves the connectivity.

The described algorithm is efficient. In fact, notice that by using a pivoting method, a base $\mathcal{B}$ can be computed in $O(n^4)$ time because there are $O(n^2)$ linear equations in (3.5). This number must be added to and hence will be dominated by the time to check the equation (3.6) for all of the linear combination of five elements of this basis, which is $O(n^5)$, (in the case that $dim\Lambda(G, H) \leq 5$, we check all of the possibilities). Thus the algorithm takes $O(n^5)$ time and the overall complexity is polynomial in n, and hence it is efficient.

Chapter 4

Enumerating the Classes of Local Equivalency in Graphs

4.1 Isotropic systems and graphic presentations

Assume that q is a power of p, which is an odd prime number and $\mathbf{F}_q$ is the finite field with q elements. Also let $\mathbf{K} = \mathbf{F}_q^2$ denote a two-dimensional vector space over $\mathbf{F}_q$ associated with the bilinear form $\langle .,. \rangle$ satisfying $\langle (x,y),(x',y') \rangle = xy' - x'y$ for $(x,y),(x',y') \in \mathbf{K}$. For a set V of n elements, define $\mathbf{K}^V$ to be the $2n-$dimensional vector space over $\mathbf{F}_q$ equipped with the bilinear form

$$\langle A, A' \rangle = \sum_{v \in V} \langle A(v), A'(v) \rangle.$$

For $X, Y \in \mathbf{F}_q^V$, let $X \times Y$ be a vector in $\mathbf{F}_q^V$ such that $(X \times Y)(v) = X(v)Y(v)$. Also for $v \in V$ and $(x,y) \in \mathbf{K}$, let $E_{v,(x,y)}$ be a vector in $\mathbf{K}^V$ where its coordinates are all zero except the $v-$th one which is equal to (x,y), i.e., $E_{v,(x,y)}(w) = \delta_{vw}(x,y)$ for every $w \in V$. Also for any vector $A \in \mathbf{K}^V$, let $A_v = E_{v,A(v)}$.

For simplicity, we denote a vector A in $\mathbf{K}^V$ by its presentation as $A = (X,Y)$ where $X, Y \in \mathbf{F}_q^V$. Therefore, $A(v) = (X(v), Y(v))$. Also for $X \in \mathbf{F}_q^V$ let *diag* X be

an $n \times n$ diagonal matrix where $(diag\ X)_{vv} = X(v)$, and for the $2n \times 2n$ matrix

$$D = \begin{pmatrix} diag\ X & diag\ Y \\ diag\ X' & diag\ Y' \end{pmatrix},$$

define

$$det\ D = diagX\ diagY' - diagX'\ diagY,$$

being an $n \times n$ diagonal matrix. Therefore $\langle A, A' \rangle = tr(det\ D)$ where tr is the usual trace function. Note that the usual determinant of D is equal to $det(det\ D)$, which is the multiplication of diagonal entries of $det\ D$.

Definition. *An isotropic system $\mathcal{L}$ is an $n-$dimensional subspace of $\mathbf{K}^V$ where $|V| = n$, such that $\langle A, B \rangle = 0$ for every $A, B \in \mathcal{L}$. In other words, $\mathcal{L}$ is a subspace which is orthogonal to itself with respect to this bilinear form.*

Note that $\langle ., . \rangle$ is non-degenerate and since $\mathcal{L}$ has dimension n, therefore

$$\mathcal{L} = \{A \in \mathbf{K}^V : \langle A, B \rangle = 0,\ \forall B \in \mathcal{L}\}.$$

In fact, if we fix a set of generators $\{A_1 = (X_1, Y_1), \cdots A_n = (X_n, Y_n)\}$ for $\mathcal{L}$ and construct the $n \times 2n$ matrix

$$\mathcal{B} = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{pmatrix} = \left(\begin{array}{c|c} X_1 & Y_1 \\ X_2 & Y_2 \\ & \vdots \\ X_n & Y_n \end{array}\right), \tag{4.1}$$

then $\mathcal{L}$ is an isotropic system if and only if $\mathcal{B}$ is a full-rank matrix (and hence $\dim \mathcal{L} = n$) and

$$\mathcal{B} \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \mathcal{B}^T = 0,$$

because the $ij-$th entry of this matrix is

$$X_i Y_j^T - Y_i X_j^T = \langle A_i, A_j \rangle.$$

We will shortly prove that every isotropic system can be defined based on graphs. To start with, we introduce these graph-based isotropic systems. Suppose that $G = (V, E)$ is a simple labeled graph (without loops and multiple edges) where the label of each edge comes from $\mathbf{F}_q$. Thus, we can represent the graph by an $n \times n$ matrix $G = (g_{vw})$, where n is equal to $|V|$, the number of vertices in the graph, and for every $v, w \in V$, g_{vw} is equal to the label of the edge vw. G is a symmetric matrix with zero diagonal. Assume that $A = (X, Y)$ and $B = (Z, T)$ are in $\mathbf{K}^V$ such that $diagZ\ diagY - diagX\ diagT = cI$ where I is the identity matrix and $c \in \mathbf{F}_q$ is a non-zero constant. Denote by $\mathcal{L}$ the vector space generated by all vectors $g(v)(diagX \mid diagY) + B_v$ for $v \in V$, where $g(v)$ denotes the $v-$th row of G. In fact, the rows of the matrix

$$(I \mid G) \cdot D \tag{4.2}$$

form a basis for $\mathcal{L}$, where

$$D = \begin{pmatrix} diag\ Z & diag\ T \\ diag\ X & diag\ Y \end{pmatrix}.$$

In order to prove that $\mathcal{L}$ is an isotropic system, first note that $(I \mid G)$ is a full-rank matrix. Also the determinant of D is c^n which is non-zero, and hence D is full-rank as well, and since D is a square matrix, $(I \mid G) \cdot D$ is also full rank. On the other hand, we need to show that the rows of $(I \mid G) \cdot D$ are orthogonal to each other, or equivalently,

$$(I \mid G) \cdot D \cdot \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \cdot \big((I \mid G) \cdot D\big)^T = 0.$$

We have

$$(I \mid G)D \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \big((I \mid G)D\big)^T$$

$$= (I \mid G) \begin{pmatrix} diag\ Z & diag\ T \\ diag\ X & diag\ Y \end{pmatrix} \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \begin{pmatrix} diag\ Z & diag\ X \\ diag\ T & diag\ Y \end{pmatrix} \begin{pmatrix} I \\ G \end{pmatrix}$$

$$= (I \mid G) \begin{pmatrix} diag\ Z & diag\ T \\ diag\ X & diag\ Y \end{pmatrix} \begin{pmatrix} diag\ T & diag\ Y \\ -diag\ Z & -diag\ X \end{pmatrix} \begin{pmatrix} I \\ G \end{pmatrix}$$

$$= (I \mid G) \begin{pmatrix} 0 & cI \\ -cI & 0 \end{pmatrix} \begin{pmatrix} I \\ G \end{pmatrix} = c(I \mid G) \begin{pmatrix} G \\ -I \end{pmatrix} = c(G - G) = 0.$$

Therefore $\mathcal{L}$ is an isotropic system.

Definition. *Suppose that $\mathcal{L}$ is an $n-$dimensional isotropic system for which there exists a graph G and vectors $A = (X, Y)$ and $B = (Z, T)$ in K^V such that $\det D(A, B) = cI$ for some $0 \neq c \in \mathbf{F}_q$, where*

$$D(A, B) = \begin{pmatrix} diagZ & diagT \\ diagX & diagY \end{pmatrix},$$

and $(I \mid G) \cdot D(A, B)$ is a basis for $\mathcal{L}$. We call (G, A, B) a graphic presentation of $\mathcal{L}$ and G a fundamental graph for $\mathcal{L}$.

Theorem 17. *Every isotropic system $\mathcal{L}$ has a graphic presentation.*

Proof. We have already shown that every subspace which addmits a graphic presentation is an isotropic system. Hence, it is sufficient to prove that every isotropic system has a basis of the form (4.2).

Consider an arbitrary basis for $\mathcal{L}$ and put them in the rows of an $n \times 2n$ matrix $\mathcal{B}$ to get a matrix of the form (4.1). Notice that if we change the $v-$th column of the first block of $\mathcal{B}$ with $v-$th column of second block, we come up with a basis for another isotropic system and it is equivalent to multiplying this matrix with a $2n \times 2n$ matrix D_1 which consists of four $n \times n$ diagonal matrices (in fact, just two of these matrices are non-zero). Among all such matrices $\mathcal{B}D_1$, choose the one in which the rank of its first block is the maximum possible, namely r. Now note that in K^V, changing the order of coordinates is equivalent to changing the order of columns of $\mathcal{B}$ in the first and the second blocks. In fact, it is equivalent to multiplying $\mathcal{B}$ by a

$2n \times 2n$ permutation matrix from the right hand side, i.e., by a matrix in the form

$$\Pi = \begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix}, \tag{4.3}$$

where π is a permutation matrix over n elements. Next, we find a permutation π such that in $\mathcal{B}D_1\Pi$ the first r columns of the first block are linearly independent. Then there exists an invertible matrix U such that

$$U\mathcal{B}D_1\Pi = \left(\begin{array}{cc|cc} I_r & \alpha & \beta & \gamma \\ 0 & \zeta & \eta & \theta \end{array}\right).$$

Due to the properties of the matrix D_1 and the maximality assumption, we have $\zeta = 0$ and $\theta = 0$. Now notice that the rows of the matrix $U\mathcal{B}D_1\Pi$ form a basis for an isotropic system and because of the orthogonality assumption, we conclude that $\eta = 0$. Therefore the rank of whole matrix is r. But this is a basis for an isotropic system of dimension n. Hence $r = n$, and we have

$$U\mathcal{B} = (I_n \mid \beta)\Pi^{-1}D_1^{-1} = (\pi^{-1} \mid \beta\pi^{-1})D_1^{-1}.$$

Therefore, $\pi U\mathcal{B} = (I \mid \pi\beta\pi^{-1})D_1^{-1}$. The matrix $\pi\beta\pi^{-1}$ may have non-zero diagonal entries, but by multiplying $(I \mid \pi\beta\pi^{-1})$ by a $2n \times 2n$ matrix with four diagonal blocks, one can obtain a matrix with the identity matrix as the first block, and the second block is the same as before, except that the diagonal entries are all zero. Considering this multiplication, we end up with $\pi U\mathcal{B} = (I \mid G')D'$, where D' is the described $2n \times 2n$ matrix with four diagonal blocks. Note that both matrices π and U are invertible, so that the rows of $\pi U\mathcal{B}$ are still a basis for $\mathcal{L}$. Let

$$D' = \begin{pmatrix} diagZ' & diagT' \\ diagX' & diagY' \end{pmatrix}$$

and by taking into the account of the orthogonality assumption, we conclude that

$$0 = (I \mid G')D' \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} D'^T (I \mid G')^T$$

$$= (I \mid G') \begin{pmatrix} diagZ' & diagT' \\ diagX' & diagY' \end{pmatrix} \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \begin{pmatrix} diagZ' & diagX' \\ diagT' & diagY' \end{pmatrix} \begin{pmatrix} I \\ G'^T \end{pmatrix}$$

$$= (I \mid G') \begin{pmatrix} 0 & detD' \\ -detD' & 0 \end{pmatrix} \begin{pmatrix} I \\ G'^T \end{pmatrix} = detD'\ G'^T - G'\ detD'.$$

Therefore $detD'G'^T = G'\ detD'$. It means that the matrix $G = G'\ detD'$ is symmetric. Moreover, it has a zero diagonal since G' does. We have

$$\pi U\mathcal{B} = (I \mid G) \begin{pmatrix} I & 0 \\ 0 & detD'^{-1} \end{pmatrix} D'$$

$$= (I \mid G) \begin{pmatrix} diagZ' & diagT' \\ detD'^{-1}diagX' & detD'^{-1}diagY' \end{pmatrix}.$$

Hence if we define

$$D = \begin{pmatrix} diagZ' & diagT' \\ detD'^{-1}diagX' & detD'^{-1}diagY' \end{pmatrix},$$

then $\pi U\mathcal{B} = (I \mid G)D$ and $det\ D = I$. This is a basis of the form (4.2), and the proof is complete.

□

4.2 Fundamental graphs for isotropic systems

In the previous section we proved that every isotropic system has a fundamental graph. But this fundamental graph is not unique. In order to study these different fundamental graphs for an isotropic system, we present a couple of definitions.

Definition. *Let G be a graph over the vertex set V. For $v \in V$ and a number $r \in \mathbf{F}_q$, define $G *_r v$ to be a graph (more precisely, a symmetric matrix with zero diagonal) $G' = (g'_{uw})$ such that for every w, $g'_{vw} = g_{vw}$, and also for every u, w inequal to v,*

$$g'_{uw} = g_{uw} + r g_{vu} g_{vw}.$$

Moreover, for a non-zero number $s \in \mathbf{F}_q$, define $G \circ_s v$ to be a graph $G' = (g'_{uw})$ such that for each u, $g'_{uv} = s g_{uv}$, and also for each u, w inequal to v, $g'_{uw} = g_{uw}$.

Two graphs G and G' are called locally equivalent if there exists a sequence of the above operations, acting on G to obtain G'.

Notice that these operations are invertible, so that it is an equivalency relation. The following theorem is already proved in chapter 3.

Theorem 18. *Two graphs G and G' are locally equivalent if and only if there exists an invertible $n \times n$ matrix U and a $2n \times 2n$ matrix D with four diagonal blocks satisfying $detD = I$ and $U(I \mid G)D = (I \mid G')$.*

□

For a non-zero number $c \in \mathbf{F}_q$, let $G' = cG$ be the usual product of a matrix G and a constant c, i.e., $g'_{vw} = c g_{vw}$ for any v, w.

Theorem 19. *For any two fundamental graphs for an isotropic system, there exists a non-zero $c \in \mathbf{F}_q$ such that cG and G' are locally equivalent. Conversely, if for some non-zero number c, the graphs cG and G' are locally equivalent, then there is an isotropic system such that G and G' are its fundamental graphs.*

Proof. Suppose that (G, A, B) and (G', A', B') are two graphic presentations for the isotropic system $\mathcal{L}$. It means that the rows of each of the matrices $(I \mid G)D(A, B)$ and $(I \mid G')D(A', B')$ form a basis for $\mathcal{L}$. Therefore there exists an invertible matrix U such that

$$U(I \mid G)D(A, B) = (I \mid G')D(A', B').$$

Hence

$$U(I \mid G)D(A, B)D(A', B')^{-1} = (I \mid G').$$

Note that both $detD(A,B)$ and $detD(A',B')$ are (non-zero) constant numbers, and $detD(A',B')^{-1}$ is also a constant. Therefore there exists a non-zero number $c \in \mathbf{F}_q$ such that $det\big(D(A,B)D(A',B')^{-1}\big) = cI$. Now let

$$D = \begin{pmatrix} I & 0 \\ 0 & c^{-1}I \end{pmatrix} D(A,B)D(A',B')^{-1}.$$

Then $detD = I$ and we have

$$U(I \mid G) \begin{pmatrix} I & 0 \\ 0 & cI \end{pmatrix} D = (I \mid G').$$

Therefore $U(I \mid cG)D = (I \mid G')$ and the first part of the conclusion follows from theorem 18.

Conversely, suppose that cG and G' are locally equivalent. Therefore, there exist matrices U and D such that U is invertible, $detD = I$ and $U(I \mid cG)D = (I \mid G')$. Also, suppose that A and B are two vectors such that $D = D(A,B)$. Therefore (G, cA, B) and (G', A', B') are two graphic presentations for the same isotropic system, where A', B' are defined so that $D(A',B') = I_{2n}$. More precisely, $A'(v) = (0,1)$ and $B'(v) = (1,0)$ for each v. □

Having this theorem in hand, we can now study the classes of local equivalency of graphs by investigating different graphic presentations of an isotropic system.

4.3 Eulerian vectors and local complementation

We call a vector $A \in \mathbf{K}^V$ *complete* if $A(v)$ is non-zero for all $v \in V$. Assume that $A \in \mathbf{K}^V$ is complete. We define $\hat{A}$ to be the vector subspace generated by vectors A_v for all $v \in V$, i.e., $\hat{A} = \langle A_v : v \in V \rangle$. In fact, if $A = (X,Y)$ then $\hat{A}$ is the vector space generated by rows of $(diagX, diagY)$.

Definition. *Let $\mathcal{L}$ be an isotropic system and $A \in \mathbf{K}^V$ be a complete vector. We call A an Eulerian vector for $\mathcal{L}$ if $\hat{A} \cap \mathcal{L} = 0$.*

Lemma 16. *Suppose that $\mathcal{L}$ is an isotropic system and (G, A, B) is a graphic presentation for $\mathcal{L}$. Then A is an Eulerian vector for $\mathcal{L}$.*

Proof. By definition of the graphic presentation we know that $detD(A, B)$ is a non-zero constant. Therefore, $A(v)$ is non-zero for any v. In fact, the $v-$th entry of the diagonal of $detD(A, B)$ is $\langle B(v), A(v)\rangle$, so that $A(v)$ should be non-zero and hence A is complete. To lead to a contradiction, suppose that $\hat{A} \cap \mathcal{L}$ is non-zero. Therefore, if $A = (X, Y)$ then there exists a non-zero vector $S \in \mathbf{F}_q^n$ such that $S(diagX|diagY) \in \mathcal{L}$. S is non-zero, hence at least one of its coordinates , say $v-$th, is non-zero. By considering the orthogonality condition, we have

$$0 = \langle S(diagX|diagY), g(v)(diagX|diagY) + B_v\rangle$$

$$= \sum_{w \in V} S(w) g_{vw} \langle (X(w), Y(w)), (X(w), Y(w))\rangle + \langle S(diagX|diagY), B_v\rangle$$

$$= S(v)\langle A(v), B(v)\rangle.$$

As we assumed, $S(v)$ is non-zero and also $\langle A(v), B(v)\rangle$ is non-zero since $detD(A, B)$ is so, which is a contradiction.

□

Corollary 2. *Every isotropic system has an Eulerian vector.*

Proof. By theorem 17, every isotropic system has a graphic presentation (G, A, B) and by lemma 16, A is an Eulerian vector for the isotropic system.

□

Let $\mathcal{L}$ be an isotropic system and A an Eulerian vector for $\mathcal{L}$. Therefore $\mathcal{L} \cap \hat{A} = 0$. If A' is a vector which is equal to A at any coordinate except the $v-$th one, at which it is equal to a non-zero multiple of $A(v)$, then $\hat{A'} = \hat{A}$, and therefore A' is also an Eulerian vector for $\mathcal{L}$.

This observation gives us the motivation of defining $\mathbf{K}^*$ to be $\mathbf{K}\backslash\{0\}$ under the equivalency relation $(x, y) \sim (x', y')$ iff $r(x, y) = (x', y')$ (and hence $\mid \mathbf{K}^* \mid = q + 1$). Now by the above discussion if we replace each coordinate of A with something

equivalent to that coordinate, we obtain another Eulerian vector. The set of Eulerian vectors of an isotropic system has even more useful properties.

Definition. *We say that a subset $\sum \subseteq \mathbf{K}^V$ of complete vectors has the switching property if*

(i) *Similar to Eulerian vectors, for each $A \in \sum$, one can replace each coordinate of A by its (scalar) multiple and it still remains in this subset.*

(ii) *In addition, for each $A \in \sum$ and $v \in V$, $A - A_v + rE_{v,(x,y)}$ is still in $\sum$ for each non-zero $r \in \mathbf{F}_q$ and every $(x,y) \in \mathbf{K}^*$ except one (x,y). In other words, in a set with switching property and a vector A in this set, we can replace a coordinate of A with exactly q elements of $\mathbf{K}^*$ so that it still remains in $\sum$.*

We will observe shortly that switching at the vertex v is equivalent to a local complementation operation on this vertex.

Theorem 20. *The set of Eulerian vectors of an isotropic system has the switching property.*

Proof. Assume that A is an Eulerian vector for the isotropic system $\mathcal{L}$, and to lead to a contradiction, suppose that (x_i, y_i), $i = 1, 2$, are two different vectors in $\mathbf{K}^*$ and $A_i = A - A_v + E_{v,(x_i,y_i)}$, $i = 1, 2$, are not Eulerian (we know that all of these vectors $A - A_v + E_{v,(x,y)}$, $(x,y) \in \mathbf{K}^*$ can not be Eulerian, since if so, for every $c \in \mathcal{L}$, $c(v) = 0$ and the dimension of $\mathcal{L}$ could not be equal to n). Therefore there exist non-zero vectors $C_i \in \hat{A}_i \cap \mathcal{L}$ for $i = 1, 2$. The $v-$th coordinate of C_i can not be zero, because otherwise, $C_i \in \hat{A} \cap \mathcal{L}$, which is not possible since A is Eulerian. Therefore, the $v-$th coordinate of C_i is a non-zero multiple of (x_i, y_i), $i = 1, 2$. Now notice that (x_1, y_1) and (x_2, y_2) are different elements of $\mathbf{K}^*$, thus they are linearly independent and there exist $r_1, r_2 \in \mathbf{F}_q$ such that $A(v) = r_1(x_1, y_1) + r_2(x_2, y_2)$. Therefore $r_1 C_1 + r_2 C_2$ is a non-zero vector in $\hat{A} \cap \mathcal{L}$, which is a contradiction.

□

Theorem 21. *For every isotropic system $\mathcal{L}$ and a graphic presentation (G, A, B) of it, A is an Eulerian vector. Conversely, for every Eulerian vector A, there exists a graphic presentation (G, A, B). Also this graphic presentation is unique up to a (non-*

zero) constant, i.e., if (G', A, B') *is another graphic presentation for* $\mathcal{L}$ *then there exists a non-zero number* $c \in \mathbf{F}_q$ *such that* $G' = cG$ *and* $B' = cB$.

Proof. The first part of the theorem was already proved in lemma 16. For the second part, suppose that $A = (X, Y)$ is an Eulerian vector of the isotropic system $\mathcal{L}$. By the switching property, for every $v \in V$, there exists some $(z_v, t_v) \in \mathbf{K}$ such that $(z_v, t_v) \nsim A(v)$ (meaning that (z_v, t_v) and $A(v)$ are not scalar multiples of each other) and there is a vector of the form $C_v + E_{v,(z_v,t_v)}$ in $\mathcal{L}$, where C_v is in $\hat{A}$ and $C_v(v) = 0$. Since $(z_v, t_v) \nsim A(v)$, hence $\langle (z_v, t_v), A(v) \rangle \neq 0$ and by considering an scalar multiple (if necessary) of (z_v, t_v), we may assume that

$$\langle (z_v, t_v), A(v) \rangle = 1. \tag{4.4}$$

We know that $C_v \in \hat{A}$ and $C_v(v) = 0$, thus there exists a matrix $G = (g_{uw})$ over $\mathbf{F}_q$ such that $g_{vv} = 0$ and $C_v = g(v)(diagX|diagY)$, for every v. Here, by $g(v)$ we mean the $v-$th row of G.

Now, Let $B = (Z, T)$ be the vector in $\mathbf{K}^V$ with $Z(v) = z_v$ and $T(v) = t_v$ for every $v \in V$. Due to the equation (4.4), we observe that $detD(A, B) = I$ and also $D(A, B)$ is an invertible matrix. Using this notation, the rows of $(I \mid G)D(A, B)$ are all in $\mathcal{L}$. Since this matrix is a full-rank one, its rows form a basis for $\mathcal{L}$. Therefore, once we show that G is the matrix for a graph, we will end up with the presentation (G, A, B) for $\mathcal{L}$.

To show that G is a graph, first note that $g_{vv} = 0$ by its definition. For proving that G is symmetric, consider again the orthogonality assumption. We have

$$0 = (I \mid G) \begin{pmatrix} diagZ & diagT \\ diagX & diagY \end{pmatrix} \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \begin{pmatrix} diagZ & diagX \\ diagT & diagY \end{pmatrix} \begin{pmatrix} I \\ G^T \end{pmatrix}$$

$$= (I \mid G) \begin{pmatrix} diagZ & diagT \\ diagX & diagY \end{pmatrix} \begin{pmatrix} diagT & diagY \\ -diagZ & -diagX \end{pmatrix} \begin{pmatrix} I \\ G^T \end{pmatrix}$$

$$= (I \mid G) \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \begin{pmatrix} I \\ G^T \end{pmatrix} = G^T - G.$$

Therefore $G^T = G$ and (G, A, B) is a graphic presentation of $\mathcal{L}$.

For the uniqueness, suppose that (G', A, B') is another graphic presentation for $\mathcal{L}$ such that $detD(A, B') = cI$. It means that $(I \mid G')D(A, B')$ is also a basis for $\mathcal{L}$. Let $B' = (Z', T')$ and by considering the orthogonality assumption, once again we have

$$0 = (I \mid G) \begin{pmatrix} diagZ & diagT \\ diagX & diagY \end{pmatrix} \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \begin{pmatrix} diagZ' & diagX \\ diagT' & diagY \end{pmatrix} \begin{pmatrix} I \\ G' \end{pmatrix}$$

$$= (I \mid G) \begin{pmatrix} detD(B', B) & detD(A, B) \\ -detD(A, B') & 0 \end{pmatrix} \begin{pmatrix} I \\ G' \end{pmatrix}$$

$$= (I \mid G) \begin{pmatrix} detD(B', B) + G' \\ -cI \end{pmatrix} = detD(B', B) + G' - cG.$$

Therefore, $detD(B', B) + G' - cG = 0$ and since $detD(B', B)$ is a diagonal matrix and the diagonals of G and G' are both equal to zero, we have $detD(B', B) = 0$ and $G' = cG$. Hence it just remains to show $B' = cB$. Because of the equation

$$0 = detD(B', B) = diagZ\ diagT' - diagZ'\ diagT,$$

for any v there exists a $c_v \in \mathbf{F}_q$ such that $(Z'(v), T'(v)) = c_v(Z(v), T(v))$. Therefore $D(A, B')_{vv} = c_v D(A, B)_{vv}$. On the other hand $detD(A, B) = I$ and $detD(A, B') = cI$, so that $c_v = c$ for any v. Hence $B' = cB$.

□

Using this theorem, if we denote by $\epsilon(\mathcal{L})$ the number of Eulerian vectors of the isotropic system $\mathcal{L}$, we conclude the following corollary.

Corollary 3. *The number of graphic presentations of an isotropic system is equal to* $(q-1)\epsilon(\mathcal{L})$.

The following theorem, explains the relationship between the *switching property*

and *local complementation.*

Theorem 22. *Suppose that (G, A, B) is a graphic presentation for the isotropic system $\mathcal{L}$, and $v \in V$.*

(i) *If $r \in \mathbf{F}_q$, then $(G *_r v, A + rB_v, B + rg(v)^2 \times A)$ is also a graphic presentation of $\mathcal{L}$. Therefore switching A at v is equivalent to a local complementation operator.*

(ii) *If $s \in \mathbf{F}_q$ is non-zero, then $(G \circ_s v, A + (s^{-1} - 1)A_v, B + (s - 1)B_v)$ is also a graphic presentation of $\mathcal{L}$.*

Proof. We prove first part, and the second part is similar. It is easy to check that $detD(A + rB_v, B + rg(v)^2 \times A)$ is constant. Hence, it is sufficient to show that all of the rows of $(I \mid G *_r v)D(A + rB_v, B + rg(v)^2 \times A)$ are in $\mathcal{L}$. Let $G' = G *_r v$ and $w \in V$, $w \neq v$. We have $g'(w) = g(w) + rg_{vw}g(v) - rg_{vw}^2\delta_w$, thus the $w-$th row of $(I \mid G')D(A + rB_v, B + rg(v)^2 \times A)$ is equal to

$$g'(w) \times (A + rB_v) + (B_w + rg_{vw}^2 A_w)$$

$$= (g(w) + rg_{vw}g(v) - rg_{vw}^2\delta_w) \times (A + rB_v) + (B_w + rg_{vw}^2 A_w)$$

$$= g(w) \times A + rg_{vw}g(v) \times A - rg_{vw}^2 A_w + rg_{vw}B_v + B_w + rg_{vw}^2 A_w$$

$$= \big(g(w) \times A + B_w\big) + rg_{vw}\big(g(v) \times A + B_v\big),$$

which is in $\mathcal{L}$. Also for the $v-$th row, $g'(v) = g(v)$ and

$$g(v) \times (A + rB_v) + (B_v + rg^2(v) \times A_v) = g(v) \times A + B_v$$

which is an element of $\mathcal{L}$.

□

4.4 Index of an isotropic system

We are now in the position of introducing the notion of *index* for an isotropic system.

Theorem 23. *For any isotropic system $\mathcal{L}$, there exists a number $\lambda(\mathcal{L})$ such that for any fundamental graph G for $\mathcal{L}$, there are exactly $\lambda(\mathcal{L})$ pairs (A, B) such that (G, A, B) is a graphic presentation of $\mathcal{L}$. This number is called the index of the isotropic system $\mathcal{L}$.*

Proof. Suppose that G is a fundamental graph of $\mathcal{L}$, and there exist exactly k graphic presentations of the form (G, A_i, B_i), $i = 1, \cdots, k$ for $\mathcal{L}$. It is sufficient to show that for any other fundamental graph H for $\mathcal{L}$, there are also k graphic presentation with H as its fundamental graph. Since G and H are fundamental graphs of the same isotropic system, by theorems 18 and 19, there exist invertible matrices U and D, such that D consists of four diagonal blocks and $detD = cI$ for some non-zero $c \in \mathbf{F}_q$, and moreover,

$$U(I \mid H)D = (I \mid G). \tag{4.5}$$

Since (G, A_i, B_i) is a graphic presentation for $\mathcal{L}$ for $i = 1, \cdots, k$, the rows of the matrix $(I \mid G)D(A_i, B_i)$ form a basis for $\mathcal{L}$. Now using (4.5), we conclude that the rows of $U(I \mid H)D\ D(A_i, B_i)$ and hence the rows of $(I \mid H)D\ D(A_i, B_i)$ form bases for $\mathcal{L}$. Now notice that $detD\ D(A_i, B_i)$ is a constant. Therefore it gives us a graphic presentation of $\mathcal{L}$ with fundamental graph H, for $i = 1, \cdots, k$. Also since the matrices U, D and $D(A_i, B_i)$ are invertible, the described k presentations are different. Moreover, for any presentation with fundamental graph H, we can convert it to a presentation with fundamental graph G. Therefore for any fundamental graph of $\mathcal{L}$, there exist exactly $\lambda(\mathcal{L}) = k$ graphic presentations with this graph as a fundamental graph.

□

Theorem 24. *Assume that $\mathcal{L}$ is an isotropic system admitting G as a fundamental graph. Then $\lambda(\mathcal{L})$ is equal to the number of matrices of the form $D(A, B)$, with non-zero constant determinant, and*

$$(I \mid G)D(A, B)\begin{pmatrix} G \\ -I \end{pmatrix} = 0. \tag{4.6}$$

In fact, $\lambda(\mathcal{L}) = \lambda(G)$, meaning that the index of an isotropic system just depends on any arbitrary fundamental graph.

Proof. As in the proof of theorem 23, suppose that (G, A_i, B_i), $i = 1, \cdots, k$, are all graphic presentations of $\mathcal{L}$ with fundamental graph G. Using the orthogonality assumption we have

$$0 = (I \mid G)D(A_1, B_1)\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} D(A_i, B_i)^T \begin{pmatrix} I \\ G \end{pmatrix}$$

$$= (I \mid G)D(A_1, B_1)\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} D(A_i, B_i)^T \begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix}\begin{pmatrix} G \\ -I \end{pmatrix}.$$

On the other hand, the matrix

$$\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} D(A_i, B_i)^T \begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix}$$

consists of four diagonal matrices and has non-zero constant determinant, and also

$$D(A_1, B_1)\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} D(A_i, B_i)^T \begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix}$$

satisfies all of these properties. Therefore, for each i, where $i = 1, \cdots, k$, we find a solution of (4.6). Conversely, since all of the above equations can be inverted, for each solution $D(A, B)$ we can find one of the graphic presentations (G, A_i, B_i).

□

Corollary 4. *For an isotropic system that admits G as a fundamental graph, the number of its graphic presentations is equal to $\lambda(G)$ times the number of graphs that are locally equivalent to cG for some non-zero $c \in \mathbf{F}_q$.*

In chapter 3, the solutions of (4.6) with determinant I are called *internal solutions*, and some significant properties are proved for these solutions.

For a graph G, we call a pair vw an *edge* if $g_{vw} \neq 0$. Suppose that C is an even cycle (a cycle with an even number of vertices) consisting of vertices $v_1, v_2, \cdots, v_{2l}$. Set

$$\nu(C) = \sum_{i=1}^{2l} (-1)^i g_{v_i v_{i+1}} g(v_i) \times g(v_{i+1}).$$

Definition. *Suppose that G is a graph. The bineighborhood space of G, denoted by $\nu(G)$, is a subspace of $\mathbf{F}_q^V$ defined by*

$$\nu(G) = span\{\{\nu(C) : C \text{ even cycle}\} \cup \{g(v) \times g(w) : g_{vw} = 0\}\}.$$

We assume that the graphs we consider are connected, and restate a couple of theorems from chapter 3, which will be used shortly.

Lemma 17. *If $D(A, B)$, where $A = (X, Y)$ and $B = (Z, T)$, satisfies (4.6) then $Y + Z$ is a scalar multiple of $(1, 1, \cdots, 1)$. On the other hand, for any such vectors A, B, the matrix $D(A, B) + cI_{2n}$ satisfies (4.6) for each $c \in \mathbf{F}_q$.*

□

Theorem 25. *Suppose that $D(A, B)$ satisfies (4.6) and $A = (X, Y)$. Then $X \in \nu(G)^\perp$.*

On the other hand for any $X \in \nu(G)^\perp$,

(i) *if G has an odd cycle, then there exists a unique Y and a unique T such that $D(A, B)$ satisfies (4.6), where $A = (X, Y)$ and $B = (-Y, T)$.*

(ii) *if G does not have an odd cycle, then there exist exactly q pairs of Y_i, T_i, $i = 1, \cdots, q$, such that $D(A_i, B_i)$ satisfies (4.6), where $A = (X, Y_i)$ and $B = (-Y_i, T_i)$.*

□

Theorem 26. *If $D(A, B)$ satisfies (4.6) for some vectors A and B, then it has a constant determinant.*

□

Having all of these theorems in hand, we conclude the following statement.

Theorem 27. (i) *If G has an odd cycle, then for any $X \in \nu(G)^{\perp}$ there are exactly q (A,B)'s, where the first component of A is X and $D(A,B)$ satisfies (4.6). Among all of these q solutions, either all of them or $q-2$ of them have non-zero constant determinant.*

(ii) *If G has no odd cycle, then for any $X \in \nu(G)^{\perp}$ there are exactly q^2 (A,B)'s where the first component of A is X and $D(A,B)$ satisfies (4.6). Among all of these q^2 solutions, at least $q(q-2)$ of them have non-zero constant determinant.*

Proof. Suppose that G has an odd cycle, and fix some $X \in \nu(G)^{\perp}$. By lemma 17 and theorem 25 there are $A_0 = (X, Y_0)$ and $B_0 = (-Y_0, T)$ such that $D(A_0, B_0)$ satisfies (4.6) and any other solution $D(A,B)$ of (4.6), where the first component of A is X, is of the form $D(A,B) = D(A_0,B_0) + cI_{2n}$, for any $c \in \mathbf{F}_q$. Hence there are q solutions with this property. Notice that $detD(A,B) = detD(A_0,B_0) + c^2 I$, and by theorem 26, $detD(A_0,B_0) = d_0 I$ is constant. Therefore depending on whether $-d_0 \in \mathbf{F}_q$ is a perfect square or not, there are either $q-2$ or q different values of $c \in \mathbf{F}_q$ such that $d_0 + c^2$ is non-zero. The proof of (ii) is exactly the same. The only difference is that in this case there are q solutions of the form $A = (X,Y)$, $B = (-Y,T)$ for (4.6). □

We can now give an estimation on $\lambda(G)$ for a graph G.

Corollary 5. *If a graph G has an odd cycle then*

$$(q-2)q^{dim\,\nu(G)^{\perp}} \leq \lambda(G) \leq q^{dim\,\nu(G)^{\perp}+1},$$

and if not

$$(q-2)q^{dim\,\nu(G)^{\perp}+1} \leq \lambda(G) \leq q^{dim\,\nu(G)^{\perp}+2}.$$

4.5 The number of graphs locally equivalent to a fixed graph

In this section we plan to compute $l(G)$, the number of graphs which are locally equivalent to a graph G. Once again, we assume that the graphs we consider are

connected.

Lemma 18. *$l(G) = l(cG)$ for any non-zero $c \in \mathbf{F}_q$.*

Proof. Clearly, for any graph H locally equivalent to G, cH is locally equivalent to cG.

□

Lemma 19. *If $c \in \mathbf{F}_q$ is a non-zero perfect square, then G and cG are locally equivalent.*

Proof. Suppose that $c = d^2$, and apply the operation $\circ_d v$ on G for all $v \in V$, and the resulted graph is cG.

□

Theorem 28. *The number of graphs locally equivalent to some non-zero scalar multiple of the graph G is either equal to $l(G)$ or $2l(G)$.*

Proof. Suppse that cG is locally equivalent to G for any non-zero c. Then for any graph locally equivalent to cG for some c, it is also locally equivalent to G. Therefore $l(G)$ is the number of graphs that are locally equivalent to cG for some c.

Next, suppose that there exists a non-zero c_0 such that c_0G is not locally equivalent to G. Notice that by lemma 19, c_0 is not a perfect square. Assume that H is a graph that is locally equivalent to cG, for some c. If c is a perfect square, then by lemma 19, H is also locally equivalent to G. On the other hand if c is not a perfect square, then ${c_0}^{-1}c$ is a perfect square. Hence ${c_0}^{-1}H$ is locally equivalent to G. Therefore, for any such H, it is locally equivalent to either G or c_0G. Also by lemma 18, $l(c_0G) = l(G)$. Therefore, in this case, the number of graphs locally equivalent to cG for some c, is $2l(G)$.

□

Using theorem 28, we can relate $l(G)$ to the number of graphs that are locally equivalent to cG for some non-zero c. Since this number appears in counting the number of graphic presentations of an isotropic system, we can obtain some useful

information about $l(G)$. For this purpose, fix an isotropic system $\mathcal{L}$ admitting G as a fundamental graph.

Theorem 29. *The number of graphs locally equivalent to cG for some non-zero $c \in \mathbf{F}_q$ is equal to*

$$\frac{(q-1)\epsilon(\mathcal{L})}{\lambda(\mathcal{L})}.$$

Proof. By corollary 3, the number of graphic presentations of $\mathcal{L}$ is equal to $(q-1)\epsilon(\mathcal{L})$. On the other hand, by corollary 4, the number of graphic presentations is equal to $\lambda(\mathcal{L})$ times the number of graphs that are locally equivalent to cG, for some non-zero c. By letting these two values be equal, one obtains the described conclusion.

□

The following corollary is a direct consequence of theorems 28 and 29.

Corollary 6. *Either $l(G)$ or $2l(G)$ is equal to*

$$\frac{(q-1)\epsilon(\mathcal{L})}{\lambda(\mathcal{L})}.$$

Using corollaries 5 and 6, giving a bound for $\epsilon(\mathcal{L})$ can lead us to a bound for $l(G)$.

Remark. *In [5],[6] and [7], it has been shown that in the binary case, $l(G) = \frac{\epsilon(\mathcal{L})}{\lambda(\mathcal{L})}$.*

4.6 The number of Eulerian vectors

In this chapter, we include the binary case. To be precise, we assume that q is either 2 or a power of an odd prime number. In addition, we do *not* assume the connectivity of graphs. In order to compute the number of Eulerian vectors of an isotropic system, $\epsilon(\mathcal{L})$, we use a well-known polynomial, so called *Tutte-Martin polynomial* which is defined as follows:

$$\mathcal{M}(\mathcal{L};t) = \sum_{C:complete} (t-q)^{\,dim(\mathcal{L}\cap\hat{C})},$$

where the summation is over all complete vectors $C \in \mathbf{K}^V$. By the definition of Eulerian vector, $\epsilon(\mathcal{L}) = \mathcal{M}(\mathcal{L}; q)$. In order to compute $\mathcal{M}(\mathcal{L}; t)$, we give a recursion formula for this polynomial.

Definition. *Let $\mathcal{L}$ be an isotropic system, $v \in V$ and $x \in \mathbf{K}^*$ (or $x = 0$). Define*

$$\mathcal{L}_x^v = \{C \in \mathcal{L} : \langle C(v), x\rangle = 0\} = \{C \in \mathcal{L} : C(v) \sim x \text{ or } C(v) = 0\},$$

and

$$\mathcal{L}|_x^v = \text{projection of } \mathcal{L}_x^v \text{ on } \mathbf{K}^{V-\{v\}}.$$

Also let $\mathcal{L}_0^v = \{C \in \mathcal{L} : C(v) = 0\}$, and for $C \in \mathbf{K}^V$, we set $C|^v$ to be the projection of C in $\mathbf{K}^{V-\{v\}}$.

Lemma 20. *$\mathcal{L}|_x^v$ is an isotropic system.*

Proof. First notice that $\mathcal{L}_x^v$ is a subspace of $\mathcal{L}$ and is self-orthogonal. On the other hand the $v-$th coordinate of each vector in $\mathcal{L}_x^v$ is either 0 or equivalent to x. Then the $v-$th coordinate of any two vectors in $\mathcal{L}_x^v$ are orthogonal, and hence if we delete the $v-$th coordinate, all of the vectors remain orthogonal to each other. In other words, $\mathcal{L}|_x^v$ is again self-orthogonal. Thus, it remains to show $dim\, \mathcal{L}|_x^v = n - 1$.

We consider two cases:

(i) There exists $C_0 \in \mathcal{L}$ such that $\langle C_0(v), x\rangle \neq 0$. In this case, we have $\mathcal{L}_x^v \neq \mathcal{L}$, and therefore, $dim\mathcal{L}_x^v = n-1$. Notice that $E_{v,x}$ is not orthogonal to C_0, therefore $E_{v,x}$ in not in $\mathcal{L}_x^v$. Therefore the projection of $\mathcal{L}_x^v$ on $\mathbf{K}^{V-\{v\}}$ is injective. Thus, $dim\mathcal{L}|_x^v$ is also $n - 1$.

(ii) For any $C \in \mathcal{L}$, $\langle C(v), x\rangle = 0$. Then $E_{v,x}$ is in $\mathcal{L}$, and for any $C \in \mathcal{L}$, $C(v) = 0$ or $C(v) \sim x$. Thus $\mathcal{L}_x^v = \mathcal{L}$, and $\mathcal{L} = \mathcal{L}_0^v \oplus \langle E_{v,x}\rangle$. It means that, by removing the $v-$th coordinate of $\mathcal{L}_0^v$, we end up with $\mathcal{L}|_x^v$. Therefore, $dim\mathcal{L}|_x^v = dim\mathcal{L}_0^v = n - 1$.

□

Remark. *Let G be a fundamental graph of $\mathcal{L}$ and (G, A, B) be a graphic presentation of $\mathcal{L}$. Then $\mathcal{M}(\mathcal{L}; t)$ just depends on G. In fact, if $\mathcal{L}'$ is another isotropic system*

with graphic presentation (G, A', B')*, then multiplication by the matrix* $D(A,B)^{-1}D(A',B')$ *maps* $\mathcal{L}$ *to* $\mathcal{L}'$*. Also it maps* $\mathcal{L} \cap \hat{C}$ *to* $\mathcal{L}' \cap \hat{C}'$*, where* $C' = CD(A,B)^{-1}D(A',B')$*.*

Using this remark we can talk about the Tutte-Martin polynomial of a graph, $\mathcal{M}(G;t)$. Also if G and H are two locally equivalent graphs, then they are fundamental graphs of the same isotropic system, and therefore $\mathcal{M}(G;t) = \mathcal{M}(H;t)$.

Next, if a vertex v is isolated in G, i.e., v has no neighbor, then $E_{v,B(v)}$ is in $\mathcal{L}$ and $\mathcal{L} = \mathcal{L}_0^v \oplus \langle E_{v,B(v)} \rangle$. This case is actually studied in the second case, in the proof of lemma 20. In this case, as we already mentioned, for all x, $\mathcal{L}|_x^v$ are the same and equal to $\mathcal{L}|_0^v$.

Theorem 30.

$$\mathcal{M}(\mathcal{L};t) = \begin{cases} (q-1)t\mathcal{M}(\mathcal{L}|_0^v;t) & \textit{if } v \textit{ is isolated in } G, \\ (q-1)\sum_{x\in\mathbf{K}^*}\mathcal{M}(\mathcal{L}|_x^v;t) & \textit{otherwise.} \end{cases}$$

Proof. Suppose that v is isolated is G. Then $\mathcal{L} = \mathcal{L}_0^v \oplus \langle E_{v,B(v)} \rangle$, and for any complete vector $C \in \mathbf{K}^V$, we have

$$\mathcal{L} \cap \hat{C} = \left(\mathcal{L}|_0^v \cap \hat{C}|^v\right) \oplus \left(\langle E_{v,B(v)} \rangle \cap \langle E_{v,C(v)} \rangle\right).$$

Therefore

$$\mathcal{M}(\mathcal{L};t) = \sum_{C\in\mathbf{K}^V} (t-q)^{\,dim(\mathcal{L}\cap\hat{C})} = \sum_{C\in\mathbf{K}^V} (t-q)^{\,dim\left(\mathcal{L}|_0^v\cap\hat{C}|^v\right)\oplus\left(\langle E_{v,B(v)}\rangle\cap\langle E_{v,C(v)}\rangle\right)}$$

$$= \sum_{C\in\mathbf{K}^V} (t-q)^{\,dim\,(\mathcal{L}|_0^v\cap\hat{C}|^v)}(t-q)^{\delta_{(B(v)\sim C(v))}}$$

$$= \sum_{C\in\mathbf{K}^{V-\{v\}}} \left((q^2-q)+(q-1)(t-q)\right)(t-q)^{\,dim\,(\mathcal{L}|_0^v\cap\hat{C})} = (q-1)t\mathcal{M}(\mathcal{L}|_0^v;t),$$

where all summations are over the complete vectors.

Now, assume that v is not isolated and g_{vw} is non-zero for some $w \in V$. Hence, there exists a vector $C_1 \in \mathcal{L}$ such that $C_1(v) \sim A(v)$. Also we already know that for some $C_2 \in \mathcal{L}$, we have $C_2(v) \sim B(v)$, and $A(v) \nsim B(v)$. Therefore, the $v-$th

coordinates of vectors in $\mathcal{L}$ cover the whole space $\mathbf{K}$. Thus

$$\mathcal{M}(\mathcal{L};t) = \sum_{C\in\mathbf{K}^V} (t-q)^{dim(\mathcal{L}\cap\hat{C})} = \sum_{x\in\mathbf{K}^*} \sum_{C,C(v)\sim x} (t-q)^{dim(\mathcal{L}\cap\hat{C})}$$

$$= \sum_{x\in\mathbf{K}^*} \sum_{C,C(v)\sim x} (t-q)^{dim(\mathcal{L}^v_x\cap\hat{C})} = \sum_{x\in\mathbf{K}^*} \sum_{C,C(v)\sim x} (t-q)^{dim(\mathcal{L}|^v_x\cap\hat{C}|^v)}$$

$$= \sum_{x\in\mathbf{K}^*} \sum_{C\in\mathbf{K}^{V-\{v\}}} (q-1)(t-q)^{dim(\mathcal{L}|^v_x\cap\hat{C})} = \sum_{x\in\mathbf{K}^*} (q-1)\mathcal{M}(\mathcal{L}|^v_x;t),$$

(once again, all summations are over the complete vectors).

□

Consider a graph G. As usual, by $G-\{v\}$, we mean the graph obtained from G by deleting vertex v.

Lemma 21. *Let $\mathcal{L}$ be an isotropic system with graphic presentation (G,A,B). Then $G-\{v\}$ is a fundamental graph of $\mathcal{L}|^v_{A(v)}$.*

Proof. We already know that the rows of $(I \mid G)D(A,B)$ form a basis for $\mathcal{L}$. The $v-$th coordinate of each row, except the $v-$th row, is either zero or equivalent to $A(v)$. Therefore, the rows of $(I \mid G)D(A,B)$, except the $v-$th row form a basis for $\mathcal{L}^v_{A(v)}$. Thus, by deleting the $v-$th row and the $v-$th column of G, and also the $v-$th coordinates of A and B, we come up with a graphic presentation of $\mathcal{L}|^v_{A(v)}$, meaning that $G-\{v\}$ is a fundamental graph of $\mathcal{L}|^v_{A(v)}$.

□

Theorem 31. **(i)** *If v is an isolated vertex in G, then $G-\{v\}$ is a fundamental graph of $\mathcal{L}|^v_0$.*

(ii) *If w is a neighbor of v in G then q graphs $G*_r v-\{v\}$, $r\in\mathbf{F}_q$, together with $G*_{-g^{-2}_{vw}} w*_1 v-\{v\}$ are fundamental graphs of $\mathcal{L}|^v_x$ for $x\in\mathbf{K}^*$.*

Proof. The part (i) is a direct consequece of lemma 21. To prove (ii), using lemma 21, we should show that for each $x\in\mathbf{K}^*$, there exists an Eulerian vector related to one of these graphs, such that its $v-$th coordinate is x.

Suppose that (G, A, B) is a graphic presentation of $\mathcal{L}$. By theorem 22, for any $r \in \mathbf{F}_q$, $(G *_r v, A + rB_v, B + rg^2(v) \times A)$ is also a graphic presentation of $\mathcal{L}$. The $v-$th coordinate of the Eulerian vector of this presentation is $A(v)+rB(v)$. Therefore, $G*_r v - \{v\}$ is a fundamental graph of $\mathcal{L}|^v_{A(v)+rB(v)}$. Now notice that $\langle A(v), B(v)\rangle \neq 0$, therefore for r varies in $\mathbf{F}_q$, $A(v) + rB(v)$ are all different elements of $\mathbf{K}^*$, and there are q of them. The only element of $\mathbf{K}^*$ not obtained this way is $B(v)$. Consider the fundamental graph $G *_s w *_1 v$, where $s = -g^{-2}_{vw}$. By theorem 22, $A + sB_w + (B_v + sg^2_{vw}A_v)$ is an Eulerian vector for this fundamental graph, and the $v-$th coordinate of this vector is $(sg^2_{vw} + 1)A(v) + B(v) = B(v)$. Thus $G *_s w *_1 v - \{v\}$ is a fundamental graph of $\mathcal{L}|^v_{B(v)}$.

□

Corollary 7. *If v is isolated in G then*

$$\mathcal{M}(G;t) = (q-1)t\mathcal{M}(G - \{v\};t),$$

otherwise, if w is a neighbor of v then

$$\mathcal{M}(G;t) = (q-1)\big[\mathcal{M}(G *_{-g^{-2}_{vw}} w *_1 v;t) + \sum_{r\in\mathbf{F}_q} \mathcal{M}(G *_r v - \{v\};t)\big].$$

The final estimation is the following one, which is valid due to the fact that all of the graphs described in the right hand side of the formula in corollary 7 have $n-1$ vertices. One can observe that the number of these graphs in the right hand side is equal to $q+1$, and hence

$$max_{G:\ |G|=n}|\mathcal{M}(G;t)| \leq (q-1)\cdot max\{t, q+1\}\cdot max_{H:\ |H|=n-1}|\mathcal{M}(H;t)|.$$

Moreover, when the graph G has only one vertex, i.e., $n = 1$, then

$$|\mathcal{M}(G;t)| \leq (q^2-1)\cdot max\{|t-q|, 1\}.$$

Putting together these two statements, we conclude the following corollary.

Corollary 8. *For a graph G with n vertices, the Tutte-Martin polynomial $\mathcal{M}(G;t)$ can be estimated as follows:*

$$|\mathcal{M}(G;t)| \leq (q^2-1)\cdot[(q-1)\cdot max\{t,q+1\}]^{(n-1)}\cdot max\{|t-q|,1\}.$$

By setting $t=q$, we obtain that:

$$\epsilon(G) \leq (q^2-1)^n.$$

We can even derive a lower bound for $\epsilon(G)$ as well.

$$min_{G:|G|=n}\mathcal{M}(G;q) \geq (q-1)\cdot min\{t,q+1\}\cdot min_{H:\ |H|=n-1}|\mathcal{M}(H;q)|.$$

On the other hand, when the graph has just one vertex, $\epsilon(G) \geq 1$, and hence in general,

$$\epsilon(G) \geq (q^2-q)^{n-1}.$$

Thus, the proof of the following theorem is now complete.

Theorem 32. *The number of Eulerian vectors for a graph (or equivalently for an isotropic system) with n vertices satisfies the following property:*

$$(q^2-q)^{n-1} \leq \epsilon(G) \leq (q^2-1)^n.$$

In particular, when the graph is ordinary (binary), i.e., when $q=2$, we have:

$$2^{n-1} \leq \epsilon(G) \leq 3^n.$$

□

4.7 The number of classes of local equivalency

As mentioned earlier, we use the formula given in corollary 6 as well as the estimations for the number of Eulerian vectors given in the previous section, in order to give a bound for $l(G)$, the number of graphs locally equivalent to G.

By corollary 6, if G is connected, then

$$l(G) \leq \frac{(q-1)\epsilon(\mathcal{L})}{\lambda(\mathcal{L})} \leq (q-1)\epsilon(\mathcal{L})$$

Taking into account the estimation of $\epsilon(\mathcal{L}) = \epsilon(G)$ presented in the theorem 32, we come up with an upper bound for $l(G)$, given that the number of graphs with n vertices is exactly $q^{\frac{n^2}{2}-\frac{n}{2}}$.

Theorem 33. **(i)** *The number of graphs locally equivalent to a connected graph is at most* $(q-1)(q^2-1)^n$ *which is bounded above by* q^{2n+1}, *n being the number of vertices of the graph.*

(ii) $C(n)$, *the number of classes of local equivalency of connected graphs with n vertices satisfies:*

$$q^{\frac{n^2}{2}-\frac{5n}{2}-1} \leq C(n) \leq q^{\frac{n^2}{2}-\frac{n}{2}}.$$

In other words,

$$C(n) = q^{\frac{n^2}{2}-O(n)}.$$

In particular, for the usual (binary) graphs, i.e., when $q = 2$, *the number of graphs locally equivalent to a graph is at most* 3^n *and the number of classes of local equivalency is*

$$C(n) = 2^{\frac{n^2}{2}-O(n)}.$$

Chapter 5

conclusion

Studying the local equivalency relation on either binary or non-binary graphs has been the subject of a significant amount of research for a long time. We translated these relations into a system of algebraic equations, and by developing a new combination of the concepts of isotropic systems and internal solutions, we came up with a solution for the problem of verifying efficiently the locally equivalent graphs. What we have precisely shown, is the following. Given two graphs on n vertices with labels coming from a finite field (of odd order), the algorithm we developed in chapter 3 can be used to verify whether these two graphs are equivalent or not, and the number of steps it takes to implement this algorithm is in $poly(n)$, i.e., it is efficient.

In addition, using the algebraic linear and quadratic equations we developed in chapter 3, we came up with estimations on the number of graphs locally equivalent to a fixed graph. Having these bounds in hand, we have shown that (when q is either equal to 2 or is an odd number) the number of inequivalent graph states, i.e., the number of classes of local equivalency, is (computationally) as large as the total number of graphs.

Bibliography

[1] A. Ashikhmin and E. Knill, *Nonbinary quantum stabilizer codes*, IEEE Trans. Info. Theory, 47 (2001), 3065-3072.

[2] M. Bahramgiri, S. Beigi and P. W. Shor, *An efficient algorithm to recognize locally equivalent graphs in non-binary case,* Arxiv: cs-ds/0702057.

[3] M. Bahramgiri and S. Beigi, *Graph states under the action of local Clifford group,* quant-ph/0610267.

[4] M. Bahramgiri and S. Beigi, *Enumerating the local equivalent graphs under the action of local Clifford group,* Arxiv: math-co/0702267.

[5] A. Bouchet, *An efficient algorithm to recognize locally equivalent graphs*, Combinatorica, 11 (1991), 315-329.

[6] A. Bouchet, *Transforming trees by successive local complementations*, J. Graph Theory, 12 (1988), 195-207.

[7] A. Bouchet, *Recognizing locally equivalent graphs*, Discrete Math., 114 (1993), 75-86.

[8] J. Dehaene, E. Hostens and B. De Moor, *Stabilizer states and Clifford operations for systems of arbitrary dimenstions, and modular arithmetic*, quant-ph/0408190.

[9] J. Dehaene, M. Van den Nest and B. De Moor, *An efficient algorithm to recognize local Clifford equivalence of graph states*, quant-ph/0405023.

[10] J. Dehaene, M. Van den Nest and B. De Moor, *Graphical description of the action of local Clifford trasformations on graph states*, quant-ph/0308151.

[11] M. Hein, J. Eisert and H. J. Briegel, *Multi-party entanglement in graph states*, quant-ph/0307130.

[12] M. Hein, W. Dur, J. Eisert, R. Raussendorf, M. Van den Nest and H. J. Briegel, *Entanglement in graph states and its applications*, quant-ph/0602096.

[13] A. Ketkar, A. Klappenecker, S. Kumar and P. K. Sarvepalli, *Nonbinary stabilizer codes over finite fields*, quant-ph/0508070.

[14] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, (2000).

[15] R. Otter, *The number of trees*, Ann. of Math. (2), 49 (1948), 583-599.

[16] D. Schlingemann, *Stabilizer codes can be realized as graph codes*, quant-ph/0111080.