Cubic Forms Equivalence over Complex

A Thesis Submitted
in Partial Fulfilment of the Requirements
for the Degree of

Master of Technology

by

Ashutosh Tiwari
Roll No. : 14111006

under the guidance of

Prof. Nitin Saxena

Department of Computer Science and Engineering

Indian Institute of Technology Kanpur

June, 2016

CERTIFICATE

It is certified that the work contained in the thesis entitled "*Cubic Forms Equivalence over Complex*", by "*Ashutosh Tiwari*", has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

Dr. Nitin Saxena
Deptt. of Computer Science & Engineering
Indian Institute of Technology
Kanpur-208016.

Abstract

We consider the problem of cubic forms equivalence over complex. Two polynomials $f(x_1, \ldots, x_n)$ and $g(x_1, \ldots, x_n)$ of total degree d with coefficients in a field $\mathbb{F}$ are said to be equivalent and denoted by $f \sim g$ over a field $\mathbb{F}$ if there exists an invertible linear transformation τ over $\mathbb{F}$ sending each x_i to a linear combination of $x_1, \ldots, x_n$ such that:

$$f(\tau(x_1), \ldots, \tau(x_n)) = g(x_1, \ldots, x_n)$$

This problem has a **PSPACE** algorithm over an algebraically closed field like $\mathbb{C}$ by using Hilberts Nullstellensatz and over $\mathbb{Q}$ this problem is not even known to be computable.

This problem is at least as hard as Graph-Isomorphism problem and also a fairly general case of ring isomorphism commutative $\mathbb{F}$-algebra isomorphism reduces to cubic forms equivalence. The thesis aims to find an alternative approach and algorithm to test cubic forms equivalence.

We completely classify the irreducible trivariate trinomial case of cubic forms equivalence. We give an explicit classification of the polynomials of this type over $\mathbb{C}$. We also give an alternative approach for testing cubic forms equivalence. This reduces the problem of cubic forms equivalence to equivalence of first order derivative vector spaces under an invertible linear transformation. In case of trivariate quadnomial cubic forms, we show that there exists infinitely many equivalence classes over $\mathbb{C}$.

Acknowledgments

I am greatly indebted to my thesis advisor Prof. Nitin Saxena, for his guidance, teaching and helping me all the times. His methodology of teaching, his insights on various mathematical problems motivated me to pursue my research in Theoretical Computer Science. I will never cease to be amazed by clarity and the precision with which he approached mathematics. In addition to his encyclopedic knowledge of the field, he is very patient and understanding advisor. He never hesitated in clearing my doubts regardless how basic they were and he always listened to every idea very enthusiastically. He afforded me total freedom in my research, while providing structure and guidance in the form of regular meetings every week. I spent several months running around in circles, but my enthusiasm never flagged, owing to his support and encouragement. I consider myself fortunate to work under his guidance and he will always remain as a source of great inspiration.

I would like to thank Prof. Manindra Agrawal, Prof. Surendra Baswana and other faculty members for their effort in teaching their respective courses. They always cleared my doubts despite of their busy schedules. Their lectures were so motivating and interesting that even a very complex problem appeared very simple. They always tried to create a friendly atmosphere so that the students can clear any doubt without any hesitation. This makes IIT Kanpur's Computer Science and Engineering Department stand out over others.

I would like to thank my colleague Sumanta Gosh, Amit Kumar Sinhababu, Vishwas Bhargav and Kirtan Padh for having interesting discussion over different topics which always helped me in better understanding of the problem.

In last I would like to thank my friend Gaurav Kumar for always helping me and mentally supporting me throughout my stay at IITK. I also want to express my gratitude to all my friends who were always there to cheer me up in the time of crisis.

This work would not have been possible without the constant support and motivation provided by my family. I thank them for always believing in me and supporting my decisions.

Finally I would like to thank the beautiful place IIT Kanpur.....without it nothing would have been possible.

Ashutosh Tiwari

June, 2016

Dedicated to

My family who are my greatest asset

He who would learn to fly one day must first

learn to stand and walk and run and climb and dance;

one cannot fly into flying.

– Friedrich Nietzsche

Contents

Chapter 1

Introduction

1.1 Overview

The general problem of polynomial equivalence is defined as given two polynomials $f(x_1, \ldots, x_n)$ and $g(x_1, \ldots, x_n)$ of total degree d over any field $\mathbb{F}$, we say that the given two polynomials f and g are equivalent and denoted by $f \sim g$, if there exists an invertible linear transformation τ over $\mathbb{F}$ which sends each x_i to a linear combination of $x_1, \ldots, x_n$ over $\mathbb{F}$ such that:

$$f(\tau(x_1), \ldots, \tau(x_n)) = g(x_1, \ldots, x_n)$$

We assume that the polynomials f and g are given in input as *expanded* form:

$$\sum_{0 \le i_1 + \ldots + i_n \le d} a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n}$$

Example 1.1.1. Suppose $f(x, y) = x^2 - y^2$ and $g(x, y) = 4xy$ are polynomials over $\mathbb{Q}$. Then the map $\tau : \begin{cases} x \mapsto x + y \\ y \mapsto x - y \end{cases}$ applied on f gives g that is $f(\tau(x), \tau(y)) = g(x, y)$. Thus $f \sim g$ over $\mathbb{Q}$.

Example 1.1.2. Consider $f = x^2$ and $g = bx^2$, where b is not square of any number. Then f and g are not equivalent over $\mathbb{Q}$ but they are equivalent over $\mathbb{R}$ as $\tau : x \mapsto \sqrt{b}x$ is an equivalence.

We will specially work with cubic forms. We will vary the number of variables keeping the degree fixed to 3. We first show our result for bivariate cubic forms equivalence and then we will move to trivariate cubic forms equivalence.

1.2 The Problem

Let us closely look at polynomial equivalence problem over a field $\mathbb{F}$ to understand it properly. It is defined as:

Given two polynomials $f(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ of total degree d over a field $\mathbb{F}$. We say that polynomials f and g are equivalent if there exists an invertible linear transformation τ over the field $\mathbb{F}$ which sends each x_i to a linear combination of $x_1, x_2, \ldots, x_n$ over $\mathbb{F}$ such that

$$f(\tau(x_1), \tau(x_2), \ldots, \tau(x_n)) = g(x_1, x_2, \ldots, x_n)$$

Now comparing the coefficients of various terms on both sides we will get different equations. We have to solve these equations over the field $\mathbb{F}$. These equations will have degree $\leq d$. It means that we have to solve a non-linear system of equations over the field $\mathbb{F}$. In general solving a non-linear system of equations has different complexity over different rings. Solving non-linear system of equations over $\mathbb{Z}$ is undecidable and over the field $\mathbb{Q}$ it is open. This problem is similar to Hilbert's *tenth problem* (H10). The main difference is that H10 problem aims for integer solution but our problem can have complex solution also. The complexity of solving non-linear system of equations over the various fields is listed as below:

Field	**Complexity**
Finite Field ($\mathbb{F}$)	NP $\cap$ coAM
Rationals ($\mathbb{Q}$)	OPEN
Reals ($\mathbb{R}$)	PSPACE
Complex ($\mathbb{C}$)	PSPACE

1.3 Current Status

Cubic forms equivalence problem has different complexity over different fields. The current status of this problem over various fields is listed below:

1. Over the finite field $\mathbb{F}$, this problem is in NP $\cap$ coAM.
2. Over the field $\mathbb{Q}$, this problem is not even known to be computable.
3. Over the field $\mathbb{R}$, this problem is in PSPACE.
4. Over the field $\mathbb{C}$, this problem is in PSPACE (assuming GRH it is in Σ_2).

Let $\mathbb{F}$ be a finite field of size p. Given a linear transformation τ on the variables $x_1, \ldots, x_n$, it is easy to check whether $f(\tau(x_1), \ldots, \tau(x_n)) = g(x_1, \ldots, x_n)$ by substituting for τ in f and doing the computation in time $poly(n, \log p)$. Thus cubic forms equivalence over $\mathbb{F}$ is in NP. The first one is due to the work of Babai & Szemerédi 1984[BS84]. They showed that this problem is in AM.
Over the field $\mathbb{R}$, we see equivalence as a matrix $\mathcal{M}$ in n^2 unknowns and solve the system of equations. These systems can be solved in PSPACE as the existential theory of the reals is in PSPACE (see [BPR06, Remark 13.9]).
Over the field $\mathbb{C}$, we consider the equivalence as a matrix $\mathcal{M}$ in n^2 unknowns and solve the system of equations. This system of equations can be solved in PSPACE by using Hilberts Nullstellensatz (Brownawell 1987) [Bro87]. Assuming Generalized Riemann Hypothesis, Hilberts Nullstellensatz can be solved in Σ_2 [Koi96]

1.4 Contribution of the Thesis

The first thing we approach in this thesis is bivariate cubic forms equivalence over $\mathbb{C}$. We give an algorithm to check the equivalence in this case. We find an alternative way to handle this problem. We solve this problem by reducing cubic forms equivalence to equivalence of first order derivative vector spaces under an invertible linear transformation. There we give a conjecture for equivalence of first order derivative vector spaces and proved this in the case of bivariate cubic forms over $\mathbb{C}$.

Then after completely solving the bivariate case we move to the trivariate cubic forms equivalence over $\mathbb{C}$. This problem seems to be harder than the previous case because in case of trivariate cubic forms there are two types of polynomials - one that is reducible over $\mathbb{C}$ and other that is irreducible over $\mathbb{C}$. The reducible case is very easy and we have given an algorithm to check the equivalence of two cubic forms equivalence if at least one of the input polynomial is factorizable.

Then the remaining case was trivariate irreducible cubic forms over $\mathbb{C}$. We decided to first handle irreducible trivariate trinomial case. There we give a complete classification of irreducible trivariate trinomial cubic forms into four equivalence classes and we proved our derivative vector space conjecture in this case.

Finally we move to the irreducible trivariate quadnomial cubic forms. In this case we chose the most intuitive polynomial with four monomials. It is a symmetric polynomial and using the determinant of the Hessian matrix for this polynomial, we proved that in the case of trivariate quadnomial cubic forms there exists infinitely many equivalence classes over $\mathbb{C}$. Finally we give a conjecture for equivalence of two symmetric polynomials.

1.5 Organization of the Thesis

Chapter 2 and 3 give a survey on various aspects of cubic forms equivalence problem. Chapter 2 focuses on known results on cubic forms equivalence and its complexity. Chapter 3 covers the problem Polynomial Decomposition over a fixed finite field and in this chapter we show that cubic forms equivalence is a special case of this problem and hence it is solved over a fixed finite field. The chapters 4, 5 and 6 span the results. We finally conclude in chapter 7 summarizing our work and stating the possible future directions this thesis seems to suggest.

Chapter 2

Cubic Form Equivalence known results

Cubic forms equivalence problem is a well studied problem in mathematics (for example see Harrison 1975 [Har75]; Harrison and Pareigis 1988 [HP88]; Manin 1986 [Man86]; Rupprecht 2003 [Rup03]). Agrawal and Saxena showed that higher degree forms equivalence problem reduces to the cubic forms equivalence case. So the cubic forms equivalence problem is the most important restricted case of polynomial equivalence problem. They also showed that a fairly general case of ring isomorphism - commutative $\mathbb{F}$-algebra isomorphism - reduces to cubic forms equivalence. They further showed that Graph Isomorphism problem reduces to the $\mathbb{F}$-algebra isomorphism problem. This shows that Graph Isomorphism problem reduces to the cubic forms equivalence problem.

2.1 Basic Definitions

Definition 2.1. (**Cubic forms equivalence**). Let $f(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ be two homogeneous degree 3 polynomials. These two polynomials are said to be equivalent and denoted by $f \sim g$ if there exists an invertible linear transformation τ sending each variable x_i to a linear combination of $x_1, x_2, \ldots, x_n$ such that:

$$f(\tau(x_1), \tau(x_2), \ldots, \tau(x_n)) = g(x_1, x_2, \ldots, x_n)$$

The polynomials f and g are assumed to be given as sum of monomials.

Definition 2.2. (**Basis Representation of a Ring**) A ring R can have infinite elements but it should be finite dimensional that is the additive group of R should be decomposable as:

$$(R, +) \cong (R_1, +) \oplus \ldots \oplus (R_n, +)$$

where $R_1, \ldots, R_n$ are special rings, namely $\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$ or a field. Thus there are 'basis' elements $b_1, \ldots, b_n \in R$ such that $(R, +) = (R_1, +)b_1 \oplus \ldots \oplus (R_n, +)b_n$ and hence to describe R it is sufficient to give the products $b_i \cdot b_j$ as a linear combination of b_k's.

Definition 2.3. (**$\mathbb{F}$-algebra**). In the basis representation of a ring R if the component rings of the additive group are fields, say $R_1 = \ldots = R_n = \mathbb{F}$, then R is called an $\mathbb{F}$-algebra. It is an $\mathbb{F}$-vector space that affords multiplication.

The upper bound of the general polynomial equivalence problem depends on the base field. The following theorem gives a upper bound for the polynomial equivalence problem over various fields.

Theorem 2.4. *For any fixed $d \in \mathbb{Z}, d > 0$, where d is the degree of polynomial then the problem of polynomial equivalence satisfies:*

1. *For a finite field, this problem is in $NP \cap coAM$.*
2. *Over $\mathbb{R}$, this problem is in PSPACE.*
3. *For an algebraically closed field like $\mathbb{C}$, this problem is in PSPACE.*

For the proof of above theorem refer to the [AS06, Theorem 2.1]. Over $\mathbb{R}$ it is in PSPACE due to the result that the existential theory of the reals is in PSPACE [BPR06, Remark 13.9].

2.2 F-algebra Isomorphism and Cubic Forms Equivalence

In this section we will see the reduction of $\mathbb{F}$-algebra isomorphism in cubic forms equivalence and reduction of cubic forms equivalence to $\mathbb{F}$-algebra isomorphism in some cases. Here we will assume that $\mathbb{F}$-algebra is given in the form of basis elements.

Theorem 2.5. *Let $\mathbb{F}$ be a field that has the d^{th} roots for every element in the field then the equivalence of homogeneous polynomial of degree d over $\mathbb{F}$ is many-one polynomial time reducible to $\mathbb{F}$-algebra isomorphism.*

For the proof of this theorem see [AS06, Theorem 2.3].

Theorem 2.6. *Commutative $\mathbb{F}$-algebra isomorphism is many-one polynomial time reducible to cubic polynomial equivalence*

For the proof of this theorem see [AS06, Theorem 2.7].

Theorem 2.7. *Commutative $\mathbb{F}$-algebra isomorphism is many-one polynomial time reducible to Local $\mathbb{F}$-algebra isomorphism.*

For the proof of this theorem see [AS06, Theorem 3.1].

Theorem 2.8. *Commutative $\mathbb{F}$-algebra isomorphism is many-one polynomial time reducible to $\mathbb{F}$-cubic form equivalence.*

For the proof of this theorem see [AS06, Theorem 3.10].

2.3 Cubic Forms Equivalence and Graph Isomorphism

In this section we will see that graph isomorphism problem reduces to the cubic forms equivalence problem.

Lemma 2.9. *Graph Isomorphism is many-one polynomial time reducible to $\mathbb{F}$-algebra Isomorphism.*

For the proof of this theorem see [AS06, Lemma 6.13].

Now this lemma together with theorem 2.7 gives us the following reduction:

$$\text{Graph Isomorphism } \leq_m^P \mathbb{F}\text{- algebra Isomorphism} \leq_m^P \text{Cubic Form Equivalence}$$

Hence Graph Isomorphism problem is the lower bound on the complexity of the cubic forms equivalence problem. Current state of the Graph Isomorphism problem is given by following theorem:

Theorem 2.10. *Graph Isomorphism problem can be solved in quasi-Polynomial time.*

For the proof of this theorem see [Bab15].
Now since the graph Isomorphism problem is solved in quasi-Polynomial time, following question is very interesting:

Problem 1. Can Cubic Form Equivalence be solved in quasi-Polynomial time ?

2.4 Cubic Forms Equivalence over $\mathbb{C}$

Let us understand the complexity of cubic forms equivalence over the $\mathbb{C}$. Let $f(\overline{x})$ and $g(\overline{x})$ be two cubic forms whose equivalence we want to check. Now apply a general τ on f and write the equations by comparing the coefficients. We want to solve these equations over $\mathbb{C}$. Let these equations be $g_1(\overline{x}), g_2(\overline{x}), \ldots, g_m(\overline{x})$. Now we want to check that

$$\exists \overline{x} \in \mathbb{C}^n, g_1(\overline{x}) = g_2(\overline{x}) = \ldots = g_m(\overline{x}) = 0?$$

Hilbert gave the following theorem for the simultaneous zeros of set of polynomials over the algebraically closed field (here we will take field to be $\mathbb{C}$). This theorem is known as Hilbert's Nullstellensatz. For detailed proof of this theorem see [DACO07].

Theorem 2.11. $Z_{\mathbb{C}}(g_1, \ldots, g_m) = \phi \Leftrightarrow 1 \in \langle g_1, \ldots, g_m \rangle_{\mathbb{C}[\overline{x}]}$

Here $Z_{\mathbb{C}}(g_1, \ldots, g_m)$ means simultaneous zeros of the polynomials $g_1(\overline{x}), \ldots, g_m(\overline{x})$ over the field $\mathbb{C}$. In other words this problem is reduced to the problem of ideal-membership, where the ideal is generated by these equations. For checking whether 1 is present in this ideal we have to solve the following algebraic problem

$$\exists \quad ? \quad h_1, \ldots, h_m \in \mathbb{C}[\overline{x}], 1 = \sum_{i=1}^{m} h_i g_i$$

Now we know that $\deg(g_i) \leq d$, where d is the total degree of the polynomials. Since we know the polynomials g_i's, the above equation is linear in terms of the h_i's. Brownawell gave the degree bound on the degree of the polynomials h_i's. It is known as Brownawell's degree bound [Bro87]. He showed that $\deg(h_i) \leq 2^{poly(n,d)}$.

Now the cubic forms equivalence reduces to the problem of finding polynomials h_i's with $\deg(h_i) \leq 2^{poly(n,d)}$ such that it satisfies the following equation

$$\sum_{i=1}^{m} h_i g_i = 1$$

Cook and Fontes showed that linear algebra is in logspace [CF12]. Hence the complexity of cubic forms equivalence problem over the algebraically closed field is **PSPACE**.

2.4.1 Cubic Forms Equivalence over $\mathbb{C}$ assuming GRH

In this subsection we will study the complexity of the cubic forms equivalence over $\mathbb{C}$ assuming Generalized Riemann Hypothesis. We know from the previous section that complexity of cubic forms equivalence over $\mathbb{C}$ is **PSPACE** due to the Hilbert's Nullstellensatz.

Pascal [Koi96] showed that assuming Generalized Riemann Hypothesis, Hilbert Nullstellensatz is in Σ_2. Hence cubic forms equivalence over $\mathbb{C}$ assuming GRH is in Σ_2.

This inspires us to ask the following question :

Problem 2 Can cubic forms equivalence problem be solved in **P** over $\mathbb{C}$?

Chapter 3

Polynomial Decomposition

3.1 Introduction

Linear Fourier analysis over a finite field $\mathbb{F}_p$ studies the structure of the exponentials of linear functions that is functions of the form $\omega^{l(x)}$ where $l : \mathbb{F}_p^n \to \mathbb{F}_p$ is a linear function and $\omega = e^{\frac{2\pi i}{p}}$ is the p^{th} root of the unity. Fourier analysis over finite field has many application in theoretical computer science like coding theory, computational learning theory, influence of variables in boolean functions, probabilistically checkable proofs, cryptography, communication complexity,and quantum computing.

Higher-order Fourier analysis over the finite field studies the structure of the exponentials of low-degree polynomial that is functions of the form $\omega^{Q(x)}$ where $Q : \mathbb{F}_p^n \to \mathbb{F}_p$ is a polynomial of bounded degree.

A new algorithmic application of higher- order Fourier analysis is Polynomial decomposition.

3.2 Polynomial Decomposition

3.2.1 Over a Finite Field of Prime order p

Definition 3.1. Given a $k > 0, k \in \mathbb{Z}$, a vector of positive integers $\delta = (\delta_1, \delta_2, \dots, \delta_k)$ and a function $\Gamma : \mathbb{F}_p^k \to \mathbb{F}_p$, we say that a function $P : \mathbb{F}_p^n \to \mathbb{F}_p$ is (k, δ, Γ)-structured if there exist polynomials $P_1, P_2, \dots, P_k : \mathbb{F}_p^n \to \mathbb{F}_p$ with each $deg(P_i) \leq \delta_i$ such that for all $x \in \mathbb{F}_p^n$,

$$P(x) = \Gamma(P_1(x), P_2(x), \dots, P_k(x)).$$

The polynomials $P_1, \dots, P_k$ are said to form a (k, δ, Γ)-decomposition.

Example 3.2.1. A n-variate polynomial over the field $\mathbb{F}_p$ of total degree d factors nontrivially exactly when it is $(2, (d-1, d-1), \text{prod})$-structured where $\text{prod}(a, b) = a \cdot b$.

First it was showed that every degree-structural property is in randomized polynomial time for finite field of prime order with the help of the following theorem:

Theorem 3.2. *If $p > d$, then for any fixed k, δ and Γ, there is a randomized algorithm which which given a polynomial $P : \mathbb{F}_p^n \to \mathbb{F}_p$ of degree d runs in time $O(n^{d+1})$ and has the following behaviour:*

1. *If P is (k, δ, Γ)-structured, with probability $\frac{2}{3}$, it finds a (k, δ, Γ)-decomposition of P.*
2. *Otherwise, it always outputs* ***NO****.*

For the proof of this theorem refer to [Bha14, Theorem 3.1].
The above theorem was then derandomized using the existing pseudorandom generators of low-degree polynomials to yield the following theorem:

Theorem 3.3. *For every positive integer k, every vector of positive integers $\delta = (\delta_1, \delta_2, \dots, \delta_k)$ and every function $\Gamma : \mathbb{F}_p^k \to \mathbb{F}_p$, there is a deterministic algorithm $\mathcal{A}_{k,\delta,\Gamma}$ that takes as input a polynomial $P : \mathbb{F}_p^n \to \mathbb{F}_p$ of degree $d < p$, runs in time polynomial in n, and output a (k, δ, Γ)-decomposition of P if one exists while otherwise returning* ***NO****.*

For the proof of this theorem refer to [Bha14, Theorem 1.2].

This problem was solved for finite field of prime order p, satisfying $d < p$ by Bhattacharya [Bha14] and later for all d and finite field of prime order by Bhattacharya, Hatami and Tulsiani [BHT15].

3.2.2 Over a fixed Finite Field

Consider the the following family of properties of functions over a fixed finite field $\mathbb{K}$.

Definition 3.4. Given a $k > 0, k \in \mathbb{Z}$, a vector of positive integers $\delta = (\delta_1, \delta_2, \ldots, \delta_k)$ and a function $\Gamma : \mathbb{K}^k \to \mathbb{K}$, we say that a function $P : \mathbb{K}^n \to \mathbb{K}$ is (k, δ, Γ)-structured if there exist polynomials $P_1, P_2, \ldots, P_k : \mathbb{K}^n \to \mathbb{K}$ with each $\deg(P_i) \leq \delta_i$ such that for all $x \in \mathbb{K}^n$,

$$P(x) = \Gamma(P_1(x), P_2(x), \ldots, P_k(x)).$$

The polynomials $P_1, \ldots, P_k$ are said to form a (k, δ, Γ)-decomposition.

First it was showed that every degree-structural property is in randomized polynomial time for a fixed finite field with the help of the following theorem:

Theorem 3.5. *Let $k \in \mathbb{N}$. For every $\delta = (\delta_1, \ldots, \delta_k) \in \mathbb{N}^k$ and every function $\Gamma : \mathbb{K}^k \to \mathbb{K}$, there is a randomized algorithm $\mathcal{A}$ that on input $P : \mathbb{K}^n \to \mathbb{K}$ of degree d, runs in time $\mathrm{poly}_{q,k,\delta}(n^{d+1})$, where $q = |\mathbb{K}| = p^r$ for some prime p and non-zero r and outputs a (k, δ, Γ)-decomposition of P if one exists while otherwise returning **NO**.*

The proof of this theorem can be found in [BB15, Theorem 5.2].

Then this theorem was derandomized to give a deterministic polynomial time algorithm. The following theorem shows this result:

Theorem 3.6. *For every finite field $\mathbb{K}$, positive integers k and d, every vectors of positive integers $\delta = (\delta_1, \delta_2, \ldots, \delta_k)$ and every function $\Gamma : \mathbb{K}^k \to \mathbb{K}$, there is a deterministic algorithm $\mathcal{A}_{\mathbb{K},d,k,\delta,\Gamma}$ that takes as input a polynomial $P : \mathbb{K}^n \to \mathbb{K}$ of degree d that runs in time polynomial in n, and outputs a (k, δ, Γ)-decomposition of P if one exists while otherwise returning **NO**.*

The proof of this theorem can be found in [BB15, Theorem 1.4]. So currently we have deterministic polynomial time algorithm for polynomial decomposition problem over a fixed finite field.

3.3 Polynomial Decomposition and Polynomial Equivalence

Now we will see how polynomial decomposition and cubic forms equivalence problems are related. In the previous section we have seen that there is a deterministic polynomial time algorithm for the polynomial decomposition problem over a fixed finite field. Now if we add some extra conditions on the polynomial decomposition problem then it will be cubic forms equivalence and since we have solved the polynomial decomposition problem over fixed finite field it will also solve the cubic forms equivalence problem over fixed finite field under these restrictions.

Now remember the definition of the (k, δ, Γ)-decomposition. There we have polynomials $P_1, P_2, \ldots, P_k : \mathbb{K}^n \to \mathbb{K}$ with each $\deg(P_i) \leq \delta_i$ such that for all $x \in \mathbb{K}^n$

$$P(x) = \Gamma(P_1(x), P_2(x), \ldots, P_k(x)) \tag{3.1}$$

and the polynomial equivalence problem for $f(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ is defined as:

Let τ be an invertible linear transformation which sends each x_i to a linear combination of $x_1, x_2, \ldots, x_n$ such that

$$\tau(f(\overline{x})) = g(\overline{x})$$

or equivalently it can be written as

$$f(\tau(x_1), \tau(x_2), \ldots, \tau(x_n)) = g(x_1, x_2, \ldots, x_n) \tag{3.2}$$

When we compare equation (3.1) and (3.2) then it is easy to see that by putting the following restrictions on polynomial decomposition problem it will become cubic forms equivalence problem:

1. Take $\Gamma : \mathbb{K}^n \to \mathbb{K}$ as the polynomial $f(\overline{x})$

2. Take $k = n$ and change the definition of our polynomials P_i's such that it is linear in the variables $x_1, x_2, \ldots, x_n$ and the matrix corresponding to this is invertible

3. Take polynomial P as $g(\overline{x})$

Since in the polynomial decomposition problem, k and the field was fixed and for cubic forms equivalence we have to take $k = n$, it means that n is fixed in our cubic forms equivalence in this case. The following problem is very interesting:

Problem 1. Can this method be generalized for any n and over any field ?

The current state of cubic forms equivalence over a finite field is NP $\cap$ coAM. Over field of zero characteristics like $\mathbb{R}$ and $\mathbb{C}$, cubic forms equivalence is decidable but over $\mathbb{Q}$ it is not even known to be computable.

Chapter 4

Bivariate Cubic Forms Equivalence

In the last chapter, we saw (section 3.3) that cubic forms equivalence problem is a special case of polynomial decomposition problem. Over any finite field of prime order $\mathbb{F}_p$ or over a fixed finite field, polynomial decomposition problem is solved in deterministic polynomial time. But we can not use this method over any field of zero characteristic as there are two problems - one the number of variables n is fixed and second we do not know how to define probability over infinite space. We need a new approach to solve cubic forms equivalence over field of zero characteristic.

4.1 Derivative Vector Space

In order to solve cubic forms equivalence problem over zero-characteristic fields we will use a new approach. Using this approach we will solve bivariate cubic forms equivalence problem over $\mathbb{C}$.

Definition 4.1. Derivative Space : Let $f(x_1, \ldots, x_n)$ be any n-variate polynomial over any field $\mathbb{F}$. Then the derivative space of f denoted by Df is defined as below:

$$Df = \langle \partial_{x_i} f \mid i \in [n] \rangle_{\mathbb{F}}$$

Now we will use the derivative spaces of the two polynomials f and g to show that f and g are equivalent.

Lemma 4.2. *Let $f(x_1, \ldots, x_n)$ and $g(x_1, \ldots, x_n)$ be two n-variate, cubic homogeneous polynomials over a field $\mathbb{F}$ such that $char(\mathbb{F}) \nmid 6$. Let τ be an invertible linear transformation over $\mathbb{F}$ which makes f and g equivalent. Then the same τ makes Df and Dg equivalent. That is*

$$\tau(f) = g \Longrightarrow \tau(Df) = Dg.$$

Proof. To prove this theorem let us define shifting of a polynomial. For a given polynomial $f(\overline{x})$, the shifted polynomial is defined as below

$$F(\overline{x}, \overline{t}) = f(\overline{x} + \overline{t}) - f(\overline{x}) - f(\overline{t}).$$

The benefit of shifting is that the terms involving only x_i's and t_i's will cancel out and the remaining terms will have x_i's and t_j's for some i and j. Hence $deg_{\overline{x}}F = deg_{\overline{t}}F = 2$, but the overall degree of each monomial will be 3.

Now we will shift our polynomials $f(\overline{x})$ and $g(\overline{x})$ to $F(\overline{x}, \overline{t})$ and $G(\overline{x}, \overline{t})$. As $F(\overline{x}, \overline{t})$ and $G(\overline{x}, \overline{t})$ are $2n$-variate polynomials, the invertible linear transformation which will be applied on these polynomials will have the following structure

$$\tau' = \begin{bmatrix} \tau & P \\ P & \tau \end{bmatrix}$$

where P is a $n \times n$ zero matrix and $\tau = [a_{ij}], i, j \in [1, n]$. The same invertible linear transformation τ which will be applied to x_i's is extended to the t_i's. It is easy to see that $\tau'(F(\overline{x}, \overline{t})) = F(\tau\overline{x}, \tau\overline{t})$. Now consider the following observations

Observation 1:

$$f(\tau\overline{x}) = g(\overline{x}) \Longrightarrow F(\tau\overline{x}, \tau\overline{t}) = G(\overline{x}, \overline{t}).$$

Proof. We know that

$$F(\tau\overline{x}, \tau\overline{t}) = G(\overline{x}, \overline{t}) \Leftrightarrow f(\tau\overline{x} + \tau\overline{t}) - f(\tau\overline{x}) - f(\tau\overline{t}) = g(\overline{x} + \overline{t}) - g(\overline{x}) - g(\overline{t}).$$

Now putting $[\bar{t} = \bar{x}]$ in the above equality we get

$$\xrightarrow{[\bar{t}=\bar{x}]} f(2.\tau\bar{x}) - 2f(\tau\bar{x}) = g(2\bar{x}) - 2g(\bar{x}).$$

$$\Longrightarrow 6.f(\tau\bar{x}) = 6.g(\bar{x}) \Longrightarrow f(\tau\bar{x}) = g(\bar{x}) \text{ (if } 6 \neq 0).$$

□

Now we will define some notations. We will use $F^{\boxed{\bar{x}}}(\bar{x}, \bar{t})$ to denote the part of F which is non-linear in $\bar{x}$ but linear in $\bar{t}$ and similarly $F^{\boxed{\bar{t}}}(\bar{x}, \bar{t})$ to denote the part of F which is non-linear in $\bar{t}$ but linear in $\bar{x}$.

Claim : The coefficients of the t_i's in $F^{\boxed{\bar{x}}}(\bar{x}, \bar{t})$ is the partial derivative of the f with respect to x_i's.

Proof. We know from the definition of the partial derivative

$$\frac{\partial f(x_1, \ldots, x_n)}{\partial x_i} = \lim_{t \to 0} \frac{f(x_1, \ldots, x_i + t, \ldots, x_n) - f(x_1, \ldots, x_i, \ldots, x_n)}{t}.$$

Now as $f(\bar{x})$ was a cubic homogeneous polynomial, there will be no linear term in $\bar{t}$ in $f(\bar{t})$. So the linear term in $\bar{t}$ will only be contributed by $f(\bar{x} + \bar{t}) - f(\bar{x})$. Now to find out the coefficient of t_i in $F^{\boxed{\bar{x}}}(\bar{x}, \bar{t})$ put $t_i = t$ and every other t_j's to zero. It shows that coefficient of t_i is nothing but $\lim_{t \to 0} \frac{f(x_1, \ldots, x_i + t, \ldots, x_n) - f(x_1, \ldots, x_i, \ldots, x_n)}{t}$ in $F^{\boxed{\bar{x}}}(\bar{x}, \bar{t})$, which is nothing but the partial derivative of $f(x_1, \ldots, x_n)$ with respect to x_i. Hence the coefficients of the t_i's in $F^{\boxed{\bar{x}}}(\bar{x}, \bar{t})$ is the partial derivative of the f with respect to x_i's. □

Observation 2:

$$\tau'(F(\bar{x}, \bar{t})) = G(\bar{x}, \bar{t}) \Leftrightarrow \tau'(F^{\boxed{\bar{x}}}(\bar{x}, \bar{t})) = G^{\boxed{\bar{x}}}(\bar{x}, \bar{t}) \text{ and } \tau'(F^{\boxed{\bar{t}}}(\bar{x}, \bar{t})) = G^{\boxed{\bar{t}}}(\bar{x}, \bar{t})$$

Proof. We can write $F(\bar{x}, \bar{t}) = F^{\boxed{\bar{x}}}(\bar{x}, \bar{t}) + F^{\boxed{\bar{t}}}(\bar{x}, \bar{t})$ by the definition of $F(\bar{x}, \bar{t})$ and similarly we can also write $G(\bar{x}, \bar{t}) = G^{\boxed{\bar{x}}}(\bar{x}, \bar{t}) + G^{\boxed{\bar{t}}}(\bar{x}, \bar{t})$.

$$\tau'(F(\bar{x}, \bar{t})) = G(\bar{x}, \bar{t}) \Leftrightarrow \tau'(F^{\boxed{\bar{x}}}(\bar{x}, \bar{t}) + F^{\boxed{\bar{t}}}(\bar{x}, \bar{t})) = G^{\boxed{\bar{x}}}(\bar{x}, \bar{t}) + G^{\boxed{\bar{t}}}(\bar{x}, \bar{t})$$

$$\implies F(\tau\overline{x}, \tau\overline{t})) = G(\overline{x}, \overline{t}) \Leftrightarrow F^{[\overline{x}]}(\tau\overline{x}, \tau\overline{t}) + F^{[\overline{t}]}(\tau\overline{x}, \tau\overline{t}) = G^{[\overline{x}]}(\overline{x}, \overline{t}) + G^{[\overline{t}]}(\overline{x}, \overline{t})$$

Since we know that τ is a linear transformation so it will send linear part in $\overline{t}$ of F to linear part in $\overline{t}$ of G (respectively linear part in $\overline{x}$ of F to linear part in $\overline{x}$ of G). Hence

$$\tau'(F^{[\overline{x}]}(\overline{x}, \overline{t})) = G^{[\overline{x}]}(\overline{x}, \overline{t}) \text{ and } \tau'(F^{[\overline{t}]}(\tau\overline{x}, \tau\overline{t})) = G^{[\overline{t}]}(\overline{x}, \overline{t})$$

In fact here we do not require both conditions, $\tau'(F^{[\overline{x}]}(\overline{x}, \overline{t})) = G^{[\overline{x}]}(\overline{x}, \overline{t})$ suffices both conditions. □

From Observation 1 and 2, we get that

$$f(\tau\overline{x}) = g(\overline{x}) \Longrightarrow \tau'(F^{[\overline{x}]}(\overline{x}, \overline{t})) = G^{[\overline{x}]}(\overline{x}, \overline{t}) \tag{4.1}$$

Assume that the polynomials f and g are equivalent that is $f(\tau\overline{x}) = g(\overline{x})$, then from equation (4.1) we get that

$$\tau'(F^{[\overline{x}]}(\overline{x}, \overline{t})) = G^{[\overline{x}]}(\overline{x}, \overline{t}) \implies F^{[\overline{x}]}(\tau\overline{x}, \tau\overline{t}) = G^{[\overline{x}]}(\overline{x}, \overline{t}) \tag{4.2}$$

Now comparing the coefficient of t_i's for each $i \in [n]$ after applying τ in the above equation, we get that the following equations for each $i \in [n]$

$$\sum_{j=1}^{n} a_{ji}\tau(\partial_{x_j} f) = \partial_{x_i} g, \forall j \in [1, n], \text{ where } \tau = [a_{ij}], i, j \in [1, n].$$

Since τ is an invertible linear transformation, we can write above equations as

$$\sum_{j=1}^{n} a_{ji}.\partial_{x_j} f = \tau^{-1}(\partial_{x_i} g), \text{ for each } i \in [n] \tag{4.3}$$

Using observation 1 and 2, and equation (4.3) it is clear that

$$\tau(f) = g \Longrightarrow \tau(Df) = Dg$$

□

Conjecture 1 : We conjecture that the converse of above lemma is also true. That is

$$\tau(Df) = Dg \Longrightarrow \tau(f) = g.$$

4.2 Bivariate Cubic Forms

In this section we will see the bivariate cubic forms equivalence problem. Given two cubic forms $f(x, y)$ and $g(x, y)$, we have to check whether they are equivalent over $\mathbb{C}$. For this we will prove the following theorem for bivariate cubic forms.

Theorem 4.3. *Any bivariate cubic form over $\mathbb{C}$ can be categorized in one of the following three classes.*

1. *One having three distinct factors and is equivalent to $xy(x + y)$.*

2. *One having two distinct factors and is equivalent to x^2y.*

3. *One having one distinct factor and is equivalent to x^3.*

Proof. We know that over $\mathbb{C}$ any bivariate cubic forms factorizes into smaller degree polynomials. This is possible because we can convert our bivariate homogeneous polynomial to univariate case, factorize it and then again convert it to the bivariate case. We will use this fact and prove the above theorem by finding an invertible linear transformation which makes a polynomial in a class equivalent to its corresponding polynomial called pivot polynomial for that class.

Case 1 : Here we will show that all bivariate cubic forms having three distinct factors over $\mathbb{C}$ are equivalent to $xy(x + y)$. For this consider a general bivariate cubic form having three distinct factors as follows

$$f = (ax + by)(cx + dy)(ex + hy)$$

where the variables a, b, c, d, e and h are such that f has three distinct factors over $\mathbb{C}$. Now we will show that f will be equivalent to $xy(x + y)$. We will show it in two steps with two different τ's. In first step we will show $f \sim xy(\alpha x+\beta y)$ for some α, β. Consider the following transformation

$$(ax + by) \mapsto x \text{ and}$$

$$(cx + dy) \mapsto y$$

This will give us τ_1 which is described below

$$\tau_1 = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

Since f has three distinct factors so $ad - bc \neq 0$, which means that determinant of this τ_1 is not zero. Applying τ_1 on f, we get the following

$$\tau_1(f) = f' = xy(\alpha x + \beta y)$$

where $\alpha = \frac{de-ch}{ad-bc}$ and $\beta = \frac{ah-be}{ad-bc}$. Since f has three distinct factors, α and β exits and neither is zero.

In the second step we will use τ_2 which will send f' to required polynomial $xy(x + y)$. τ_2 is described as below

$$\tau_2 = \begin{bmatrix} \alpha^{-\frac{2}{3}}\beta^{\frac{1}{3}} & 0 \\ 0 & \alpha^{\frac{1}{3}}\beta^{-\frac{2}{3}} \end{bmatrix}$$

Also since $\alpha \neq 0, \beta \neq 0$, the determinant of τ_2 is non-zero. Applying τ_2 on f', we will get the following

$$\tau_2(f') = xy(x + y)$$

The single τ which sends f to $xy(x + y)$ is given as below:

$$\tau = \begin{pmatrix} \alpha^{-\frac{2}{3}}\beta^{\frac{1}{3}} & 0 \\ 0 & \alpha^{\frac{1}{3}}\beta^{-\frac{2}{3}} \end{pmatrix} \times \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

Hence any f having three distinct factors over $\mathbb{C}$ is equivalent to $xy(x + y)$.

Case 2 : Here we will prove that any bivariate cubic form having two distinct factors over $\mathbb{C}$ is equivalent to x^2y.

Now consider a general bivariate cubic form having two distinct factors over $\mathbb{C}$ as follows

$$f = (ax + by)^2(cx + dy)$$

where variables a, b, c and d are such that the polynomial f has two distinct factors. Now apply the following τ on x^2y to make it equal to f

$$\tau = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

τ will not be invertible if $ad = bc$ but it is not possible as if we take $ad = bc$ then the above f will not have two distinct factors. Hence $f \sim x^2y$.

Case 3 : Here in this case we will prove that any bivariate cubic form having one distinct factor over $\mathbb{C}$ is equivalent to x^3.

Now consider a general bivariate cubic form which has only one distinct factor over $\mathbb{C}$ given as below

$$f = (ax + by)^3$$

Now we will show that f is equivalent to x^3. Here both a and b cannot be simultaneously zero otherwise f will be zero. So there can be at most three possibilities - one in which $a \neq 0, b \neq 0$ and second in which $a \neq 0, b = 0$. In both these cases we will use the following transformation on x^3 to make $x^3 \sim f$.

$$\tau = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$$

Last possibility is when $a = 0, b \neq 0$. We know that $x^3 \sim y^3$ (Apply $x \mapsto y, y \mapsto x$ on x^3), we will use the following transformation on y^3 to make it equivalent to f.

$$\tau = \begin{bmatrix} 1 & 0 \\ a & b \end{bmatrix}$$

In this case also $x^3 \sim y^3 \sim f$. Hence all bivariate cubic forms having one distinct factor over $\mathbb{C}$ is equivalent to x^3 and y^3. $\square$

4.3 Algorithm for Bivariate Cubic Forms Equivalence over $\mathbb{C}$

In this section we will present an algorithm to check the equivalence of two bivariate cubic forms over $\mathbb{C}$. Using theorem 4.3, we have three equivalence classes in the case of bivariate cubic forms and the pivot polynomials of these classes are as below.

1. $xy(x+y)$
2. xy^2
3. x^3

Now we will give an algorithm to check equivalence of two bivariate cubic forms over $\mathbb{C}$.

Algorithm 1 Bivariate cubic forms equivalence

Input: Two bivariate cubic forms f and g.
Output: "Yes" or "No", depending on whether f and g are equivalent over $\mathbb{C}$.
1: Factor both the cubic forms over $\mathbb{C}$.
2: Count the number of distinct factors in each cubic form.
3: If number of distinct factors are same for both cubic forms then output "Yes" else output "No".

The time complexity of this algorithm is same as the time complexity of factoring a bivariate homogeneous polynomial over $\mathbb{C}$ which is polytime using Kaltofen's factoring algorithm for constant degree (deg $= 3$).

To see the correctness of the algorithm, suppose if it outputs "YES" then it means that the two input polynomials are equivalent to the same pivot polynomial and hence are equivalent. Suppose it outputs "NO" then it means that the two input polynomials are equivalent to two different pivot polynomials having different number of distinct factors and we know that these two pivot polynomials cannot be equivalent to each other. Hence the two given input polynomials cannot be equivalent to each other.

4.4 Conjecture-1 in Case of Bivariate Cubic Forms

Now we will prove our conjecture 1 in case of bivariate cubic forms.

Lemma 4.4. *Conjecture-1 is true in case of bivariate cubic forms.*

Proof. To prove conjecture-1, we will use contrapositive that is

$$\tau(f) \neq g \Longrightarrow \tau(Df) \neq Dg, \text{ for any } \tau.$$

Since we are using f and g such that $f \nsim g$ and we know that in case of bivariate cubic forms there are three equivalence classes so if we take f and g from different equivalence classes and show that there does not exist any invertible linear transformation τ which will make Df and Dg equivalent then it will prove our conjecture in case of bivariate cubic forms.

Case 1 : In this case we are going to take the following polynomials
$f = xy(x+y)$ and $g = xy^2$.
Then we have Df and Dg as

$$Df = \langle 2xy + y^2, x^2 + 2xy \rangle_{\mathbb{C}} \textit{ and}$$

$$Dg = \langle y^2, 2xy \rangle_{\mathbb{C}}$$

Now let us take a general invertible linear transformation τ over $\mathbb{C}$ as follows

$$\tau = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Now if we are able to find out the values of a, b, c and d such that τ is invertible then converse is false otherwise true for this case.
Since Dg has no term of x^2, the coefficient of x^2 in each component of $\tau(Df)$ should be zero. Writing equations for coefficient of x^2 in each component of $\tau(Df)$ and making it equal to zero, we get

$$c^2 + 2ac = 0 \tag{4.4}$$

$$a^2 + 2ac = 0 \tag{4.5}$$

Equation (4.4) gives us either $c = 0$ or $c = -2a$. Equation (4.5) gives us either $a = 0$ or $a = -2c$. Using these there can be four combinations of the values of a and c. We will see it one by one and show that in each case τ is not invertible.

1. Here we will take $a = -2c$ and $c = -2a$. It will give us $a = 0$ which implies that $c = 0$ also. Hence τ is not invertible. So this is not possible.
2. Here we will take $a = 0$ and $c = -2a$. Using $a = 0$, it is clear that $c = 0$. Hence in this case also τ is not invertible. So this is not possible.
3. Here we will take $a = -2c$ and $c = 0$. Using $c = 0$, it is clear that $a = 0$. Hence in this case also τ is not invertible. So this is not possible.
4. Here we will take $a = 0$ and $c = 0$. In this case also τ is not invertible. So this is not possible.

Hence in this case there does not exist any invertible linear transformation τ such that $Df \sim Dg$. So converse is true in this case.

Case 2 : In this case we will take the following polynomials
$f = xy(x + y)$ and $g = x^3$. Then we have Df and Dg as

$$Df = \langle 2xy + y^2, x^2 + 2xy\rangle_{\mathbb{C}} \text{ and}$$

$$Dg = \langle x^2\rangle_{\mathbb{C}}$$

Now let us take a general linear invertible transformation τ over $\mathbb{C}$ as follows

$$\tau = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Now if we are able to find out the values of a, b, c and d such that τ is invertible then converse is false otherwise true for this case.

Since Dg has no term of y^2, the coefficient of y^2 in each component of $\tau(Df)$ should be zero. Writing equations for coefficient of y^2 in each component of $\tau(Df)$ and making it equal to zero, we get

$$d^2 + 2bd = 0 \tag{4.6}$$

$$b^2 + 2bd = 0 \tag{4.7}$$

From equation (4.6) we get that either $d = 0$ or $d = -2b$ and from equation (4.7) we get that either $b = 0$ or $b = -2d$. It is same as Case 1. In all four combinations we know that τ is not invertible. So converse is true in this case.

Case 3 : In this case we will take the following polynomials
$f = xy^2$ and $g = x^3$. Then we have Df and Dg as

$$Df = \langle y^2, 2xy\rangle_{\mathbb{C}} \text{ and}$$

$$Dg = \langle x^2\rangle_{\mathbb{C}}$$

Now let us take a general linear invertible transformation τ over $\mathbb{C}$ as follows

$$\tau = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Now if we are able to find out the values of a, b, c and d such that τ is invertible then converse is false otherwise true for this case.
Applying τ on Df and making it equal to Dg, we get the following

$$< (cx + dy)^2, 2(ax + by)(cx + dy) > = < x^2 >$$

Now comparing first component on left side with linear combination of components on right side, we get

$$c^2x^2 + d^2y^2 + 2cdxy = \lambda_1 x^2$$

Comparing coefficients on both sides, we get the following equations

$$c^2 = \lambda_1 \tag{4.8}$$

$$d^2 = 0 \tag{4.9}$$

$$cd = 0 \tag{4.10}$$

Now comparing second component on left side with linear combination of components on right side, we get

$$2acx^2 + 2bdy^2 + 2(ad + bc)xy = \lambda_2 x^2$$

Comparing coefficients on both sides, we get the following equations

$$2ac = \lambda_2 \tag{4.11}$$

$$2bd = 0 \tag{4.12}$$

$$ad + bc = 0 \tag{4.13}$$

From equation (4.8) and (4.9) we get $c = \pm\lambda_1$ and $d = 0$ respectively. From (4.11) we get $a = \pm\frac{\lambda_2}{2\lambda_1}$. Now from (4.13) and above values we get $bc = 0$ and as $c \neq 0$, we get $b = 0$. So we get $b = 0$ and $d = 0$ which makes τ non-invertible. So converse is true in this case.

Hence we proved that converse is true in case of bivariate cubic forms. □

This proof motivates us to give the following corollary.

Corollary 4.5. *Conjecture-1 is also true for any n-variate cubic form, where $n \geq 2$, which completely factorizes into three factors.*

Proof. We will give an idea for this. We can apply the same proof of Lemma 4.4, if the polynomial completely factorizes. The main idea in this is that we can treat the remaining $n - 2$ variables as constants by pushing these $n - 2$ variables in the function field. Now we can use the same analysis to show that conjecture-1 is true in this case. □

Chapter 5

Trivariate Cubic Forms

We have seen an algorithm for bivariate cubic forms equivalence over $\mathbb{C}$. The basic property that we exploit there is that every bivariate cubic form factorizes over $\mathbb{C}$. Since we are dealing with cubic forms there can be at most three distinct factors. We proved there that all bivariate cubic forms having same number of distinct factors are equivalent. Now we will move to trivariate cubic forms equivalence problem. We cannot exploit the same property here as not all the trivariate cubic forms are factorizable over $\mathbb{C}$. But the idea will work for all those trivariate cubic forms which will completely factorize over $\mathbb{C}$. Here we will first prove the result for trivariate cubic forms which will factorize over $\mathbb{C}$ then we will give our attention to those trivariate cubic forms which are irreducible over $\mathbb{C}$. Finally in this chapter we will give a complete classification of irreducible trivariate trinomial cubic forms over $\mathbb{C}$.

5.1 Preliminaries

5.1.1 Factorizable Trivariate Cubic Forms

In this section we will deal with those trivariate cubic froms which will factorize over $\mathbb{C}$. Since we are dealing with cubic forms there can be at most three distinct factors and we will use the number of distinct factors to decide equivalence for these cubic forms.

Theorem 5.1. *Any trivariate cubic form over $\mathbb{C}$ will be in one of the following four classes*

1. *One having three distinct factors and is equivalent to xyz.*
2. *One having two distinct factors and is equivalent to x^2y.*
3. *One having one distinct factor and is equivalent to x^3.*
4. *Irreducible Polynomial over $\mathbb{C}$.*

Proof. We will first show that all the trivariate cubic forms which factorizes into smaller degree factors are equivalent to the respective class polynomial based on the number of distinct factors then we will show that irreducible polynomial will not be equivalent to any factorisable trivariate cubic form.

Case 1 : In this case we will show that any trivariate cubic form which factorizes and has three distinct factors is equivalent to xyz. For this consider a general trivariate cubic form having three distinct factors as

$$f(x, y, z) = (ax + by + cz)(dx + ey + kz)(gx + hy + iz)$$

where the constants $a, b, c, d, e, k, g, h, i$ are such that f has three distinct factors. Now we will show that it is equivalent to

$$g(x, y, z) = xyz$$

For this we will apply τ on g make it equal to f. consider the following mapping

$$\tau = \begin{bmatrix} a & b & c \\ d & e & k \\ g & h & i \end{bmatrix}$$

Now we have to show that τ is invertible. Since the elements of τ are coefficients of x, y and z in three distinct factors of f so we cannot write any row or column of τ as a linear combination of any other two rows or columns which means τ is invertible.

Case 2 : In this case we will show that any trivariate cubic form having two distinct factors over $\mathbb{C}$ is equivalent to x^2y which by permutation of variables is equivalent to x^2z, y^2x, y^2z, z^2x and z^2y. Now consider the general polynomial having two distinct factors as below

$$f(x, y, z) = (ax + by + cz)^2(dx + ey + kz)$$

where coefficients a, b, c, d, e, k are such that f has two distinct factors. We will show that it is equivalent to

$$g(x, y, z) = x^2y$$

We will apply τ on g and make it equal to f by using following transformation

$$\tau = \begin{bmatrix} a & b & c \\ d & e & k \\ 0 & 0 & 1 \end{bmatrix}$$

We know that we cannot write a, b, c as a linear combination of d, e, k since they are coefficients of x, y, z in two distinct factors hence we cannot write any row or column of τ as a linear combination of any other two rows or columns which means τ is invertible.

Case 3 : In this case we will show that any trivariate cubic form having one distinct factor over $\mathbb{C}$ is equivalent to x^3 which by permutation of variables is equivalent to y^3 and z^3. Now consider the general polynomial having one distinct factor as below

$$f(x, y, z) = (ax + by + cz)^3$$

We will show that it is equivalent to

$$g(x, y, z) = x^3$$

We will apply τ on g and make it equal to f by using following transformation if $a \neq 0$.

$$\tau = \begin{bmatrix} a & b & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

If $a = 0$ but $b \neq 0$ then we will use the following transformation to make it equivalent to y^3 which is equivalent to x^3.

$$\tau = \begin{bmatrix} 1 & 0 & 0 \\ a & b & c \\ 0 & 0 & 1 \end{bmatrix}$$

Similarly if $a = 0, b = 0$ but $c \neq 0$ then we will use following transformation to make it equivalent to z^3 which is equivalent to x^3.

$$\tau = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & b & c \end{bmatrix}$$

Clearly in this case τ is invertible.

Case 4 : In this case we will show that irreducible trivariate cubic forms are not equivalent to any factorizable trivariate cubic form. Suppose this is not true and f is a irreducible trivariate cubic form which is equivalent to some factorizable trivariate cubic form g. But in the earlier cases we have shown that any trivariate factorizable cubic form will be equivalent to a pivot polynomial depending on the number of distinct factors which implies that f factorizes which contradicts the irreducibility of f. Hence any irreducible trivariate cubic form cannot be equivalent to any trivariate factorizable cubic form. $\square$

5.1.2 Algorithm for Factorisable Trivariate Cubic Forms Equivalence

Theorem 5.1 in above section gives us an algorithm for checking equivalence of two trivariate cubic forms where at least one polynomial factorizes over $\mathbb{C}$. The algorithm is given as follows:

Algorithm 2 Factorizable trivariate cubic forms equivalence

Input: Two trivariate cubic forms f and g where at least one polynomial factorizes over $\mathbb{C}$.

Output: "YES" or "NO" depending on whether f and g are equivalent.

1: Factorize the input polynomials f and g.
2: If both are irreducible polynomials over $\mathbb{C}$ then OUTPUT - "Cannot say anything".
3: If one polynomial factorizes but not second then OUTPUT - "NO".
4: Otherwise count the number of distinct factors in both polynomials.
5: If number of distinct factors in both polynomials are same then OUTPUT - "YES" otherwise OUTPUT - "NO".

Correctness : We know from theorem 5.1 that if one of the given polynomial is irreducible but second factorizes then they cannot be equivalent. If both the polynomials factorizes then we are counting the number of distinct factors as they are classified in a class depending on the number of distinct factors and are equivalent to pivot polynomial of that class. So if they have same number of distinct factors then they will be equivalent to the same pivot polynomial which will make them equivalent and if the number of distinct factors are not same then they will be equivalent to different pivot polynomials and hence they will not be equivalent.

Time Complexity : The time complexity of this algorithm is same as time complexity of factoring a multivariate polynomial over $\mathbb{C}$ which is polytime using Kaltofen's algorithm for constant degree.

Corollary 5.2. *This algorithm is also applicable in case of n- variate cubic forms where $n \geq 2$ and at least one polynomial is factorizable over $\mathbb{C}$.*

Now we will deal with irreducible trivariate cubic forms equivalence which is the most important case. Before proceeding to that we will see the relation between determinant of Hessian matrix of polynomials and their equivalence.

5.2 Hessian Matrix and Polynomial Equivalence

In this section we will see the relation between polynomial equivalence and determinant of Hessian matrix. Hessian matrix gives us a new way of checking equivalence over $\mathbb{C}$. We will first define what is Hessian matrix for a polynomial then we will see some results for equivalence using determinant of Hessian matrix.

Definition 5.3. (**Hessian Matrix**) For a polynomial $f(\overline{x}) \in \mathbb{F}[\overline{x}]$, the Hessian matrix $H_f(\overline{x}) \in (\mathbb{F}[\overline{x}])^{n\times n}$ is defined as follows:

$$H_f(\overline{x}) \stackrel{def}{=} \begin{bmatrix} \frac{\partial^2 f}{\partial x_1 \cdot \partial x_1} & \cdots & \frac{\partial^2 f}{\partial x_1 \cdot \partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n \cdot \partial x_1} & \cdots & \frac{\partial^2 f}{\partial x_n \cdot \partial x_n} \end{bmatrix}$$

We denote the determinant of Hessian matrix $H_f(\overline{x})$ for polynomial f as $H(f)$.

$$H(f(\overline{x})) = \det(H_f(\overline{x}))$$

Let f be a homogeneous n-variate polynomial of degree d, then it is easy to see that

$$\deg(H(f)) = (d-2)n$$

The most interesting property of the Hessian matrix of a polynomial is the effect that a linear transformation of the variables has on it.

Lemma 5.4. *[Kay11] Let $f(\overline{x}) \in \mathbb{F}[\overline{x}]$ be a n-variate polynomial and $\tau \in \mathbb{F}^{n\times n}$ be a linear transformation. Let $F(\overline{x}) \stackrel{def}{=} f(\tau \cdot \overline{x})$. Then,*

$$H_F(\overline{x}) = \tau^T \cdot H_f(\tau \cdot \overline{x}) \cdot \tau$$

In particular,

$$H(F(\overline{x})) = \det(\tau)^2 H(f(\tau \cdot \overline{x}))$$

Proof. To prove this we will use chain rule of derivatives. Let us assume that τ is as follows

$$\tau = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

We have for all $1 \le i \le n$

$$\frac{\partial F(\overline{x})}{\partial x_i} = \sum_{k=1}^{n} a_{ki} \frac{\partial f(\tau \cdot \overline{x})}{\partial x_k} \tag{5.1}$$

Therefore for all $1 \leq i, j \leq n$, we have

$$\frac{\partial^2 F(\overline{x})}{\partial x_i \cdot \partial x_j} = \sum_{k=1}^{n} a_{ki} \cdot \left(\sum_{l=1}^{n} a_{lj} \frac{\partial^2 f(\tau \cdot \overline{x})}{\partial x_k \cdot \partial x_l} \right) \tag{5.2}$$

$$\frac{\partial^2 F(\overline{x})}{\partial x_i \cdot \partial x_j} = \sum_{k \in [n], l \in [n]} a_{ki} \cdot \frac{\partial^2 f(\tau \cdot \overline{x})}{\partial x_k \cdot \partial x_l} \cdot a_{lj} \tag{5.3}$$

Putting these equations in the matrix form we will get

$$H_F(\overline{x}) = \tau^T \cdot H_f(\tau \cdot \overline{x}) \cdot \tau$$

Now taking determinant both side of the above equation, we will get

$$H(F(\overline{x})) = \det(\tau^T \cdot H_f(\tau \cdot \overline{x}) \cdot \tau)$$

We know that for two square $n \times n$ matrices A and B, $\det(A \cdot B) = \det(A) \cdot \det(B)$ and $\det(A) = \det(A^T)$. Hence we get

$$H(F(\overline{x})) = \det(\tau)^2 H(f(\tau \cdot \overline{x}))$$

□

Now using the above lemma, we will give another lemma which will help in cubic forms equivalence.

Lemma 5.5. *If $f(\overline{x}), g(\overline{x}) \in \mathbb{F}[\overline{x}]$ are two n-variate polynomials then over $\mathbb{F} = \mathbb{C}$, we have*

$$\tau(f) = g \implies \tau'(H(f)) = H(g) \text{ for some } \tau'.$$

Proof. Let us suppose that we have $\tau(f) = g$. Now we will show that $\tau'(H(f)) = H(g)$. Using the previous lemma we know that

$$H(\tau(f)) = \det(\tau)^2 \cdot \tau(H(f))$$

which is nothing but

$$H(g) = \det(\tau)^2 \cdot \tau(H(f))$$

Since we are over $\mathbb{C}$, we can always find a τ_1 which will make f and $c \cdot f$ equivalent. Hence our τ' is nothing but a combination of τ and τ_1. More precisely $\tau' = \tau_1\tau$. It proves that

$$\tau(f) = g \implies \tau'(H(f)) = H(g)$$

for some τ'. □

Now using this lemma we will show that $f = x^3 + y^3 + z^3$ has only trivial automorphism that is a variable can only be scaled by either $1, \omega$ or ω^2.

Lemma 5.6. *The polynomial $f = x^3 + y^3 + z^3$ has only trivial automorphism.*

Proof. To prove this we want to find an invertible linear transformation τ such that $\tau(f) = f$. Using the previous lemma we know that

$$\tau(f) = f \implies \tau(H(f)) = H(f)$$

Now for f computing the value of $H(f)$

$$H(f) = \det \begin{bmatrix} 6x & 0 & 0 \\ 0 & 6y & 0 \\ 0 & 0 & 6y \end{bmatrix}$$

That is $H(f) = 216xyz$. We want a τ which makes $216xyz$ equivalent to $216xyz$. We know that this is only possible by scaling of the variables. So we get the information about τ that τ is only scaling of the variables. So τ has the following form

$$\tau = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}$$

Now applying τ on f and making it equal to f, we get

$$a^3x^3 + b^3y^3 + c^3z^3 = x^3 + y^3 + z^3$$

Now comparing the coefficients on both sides we get

$$a^3 = 1, b^3 = 1, c^3 = 1 \implies a, b, c = 1, \omega, \omega^2$$

which proves the lemma. □

5.3 Irreducible Trivariate Trinomial Cubic Forms

In this section we will deal with the irreducible trivariate trinomial cubic forms. Here we will show that all irreducible trivariate trinomial cubic forms are classified into 4 equivalence classes. Before proceeding to prove it, we need to define some notations.

Trivariate Trinomial Representation : We will denote a general trivariate trinomial cubic form by the following notation

$$f = k_1\overline{x}^{e_1} + k_2\overline{x}^{e_2} + k_3\overline{x}^{e_3}$$

where $\overline{x}$ is a vector representing variables, e_i is a vector representing exponent of the respective variable and $|e_i| = 3$ and k_1, k_2 and k_3 are non-zero coefficient.

Now we will prove an important theorem which we will use in our irreducible trivariate trinomial cubic forms classification.

Theorem 5.7. *All irreducible trivariate trinomial cubic forms having same support that is trinomial of the following type:*

$$f = k_1\overline{x}^{e_1} + k_2\overline{x}^{e_2} + k_3\overline{x}^{e_3}.$$

$$\exists\tau \text{ such that } \tau(k_1\overline{x}^{e_1} + k_2\overline{x}^{e_2} + k_3\overline{x}^{e_3}) = k_1'\overline{x}^{e_1} + k_2'\overline{x}^{e_2} + k_3'\overline{x}^{e_3}$$

for any $k_1, k_2, k_3 \neq 0$*, and* $k_1', k_2', k_3' \neq 0$*. Also* τ *only scales the variables.*

Proof. We will show that an invertible linear transformation τ which only scales the variables of f will give us a system of equations that can be solved, which will prove the theorem.

Assume that τ sends $\overline{x}$ to $\overline{\alpha}.\overline{x}$ i.e.

$$\overline{x} \mapsto \overline{\alpha}.\overline{x}$$

where $\overline{\alpha}$ is a vector denoting scaling of the respective variables in $\overline{x}$. Apply this τ on the f

$$\tau(f) = k_1\overline{\alpha}^{e_1}\overline{x}^{e_1} + k_2\overline{\alpha}^{e_2}\overline{x}^{e_2} + k_3\overline{\alpha}^{e_3}\overline{x}^{e_3} = k_1'\overline{x}^{e_1} + k_2'\overline{x}^{e_2} + k_3'\overline{x}^{e_3}$$

Comparing the coefficients on both sides, we get the following equations

$$\begin{aligned}\overline{\alpha}^{e_1} &= \frac{k_1'}{k_1}\\ \overline{\alpha}^{e_2} &= \frac{k_2'}{k_2}\\ \overline{\alpha}^{e_3} &= \frac{k_3'}{k_3}\end{aligned}$$

Taking log on both sides we get the following equations

$$\begin{aligned}e_{11}\log\alpha_1 + e_{12}\log\alpha_2 + e_{13}\log\alpha_3 &= \log\frac{k_1'}{k_1}\\ e_{21}\log\alpha_1 + e_{22}\log\alpha_2 + e_{23}\log\alpha_3 &= \log\frac{k_2'}{k_2}\\ e_{31}\log\alpha_1 + e_{32}\log\alpha_2 + e_{33}\log\alpha_3 &= \log\frac{k_3'}{k_3}\end{aligned}$$

Writing these equations in the matrix form we get the following equation

$$\begin{pmatrix} e_{11} & e_{12} & e_{13}\\ e_{21} & e_{22} & e_{23}\\ e_{31} & e_{32} & e_{33}\end{pmatrix}\begin{pmatrix}\log\alpha_1\\ \log\alpha_2\\ \log\alpha_3\end{pmatrix} = \begin{pmatrix}\log\frac{k_1'}{k_1}\\ \log\frac{k_2'}{k_2}\\ \log\frac{k_3'}{k_3}\end{pmatrix}$$

Now we will have a solution for $\overline{\alpha}$ if the matrix

$$\mathcal{M} = \begin{pmatrix} e_{11} & e_{12} & e_{13}\\ e_{21} & e_{22} & e_{23}\\ e_{31} & e_{32} & e_{33}\end{pmatrix}$$

is invertible. Remember that vector $\overline{e_i}, i \in [1,3]$ was the exponent for the respective variable in the trinomial. Since in trinomial each monomial should be different we have the following constraints on the matrix

1. Each row has sum 3 because each monomial is cubic.
2. No two rows are same, otherwise the polynomial will not have three distinct monomials.
3. No column will be a zero vector, otherwise the polynomial will become bivariate.
4. In each column at least one value will be zero, otherwise the polynomial will be factorizable.
5. Each entry $e_{ij}, i, j \in [3]$ in the matrix will satisfy the following property, as each monomial is cubic.
$$0 \leq e_{ij} \leq 3 \text{ and } e_{ij} \in \mathbb{Z}$$

Using these constraints we will show that determinant of the matrix is not zero, hence it is an invertible matrix. Now consider the following operations

$$\begin{bmatrix} e_{11} & e_{12} & e_{13} \\ e_{21} & e_{22} & e_{23} \\ e_{31} & e_{32} & e_{33} \end{bmatrix} \xrightarrow[C_3 \leftarrow C_1+C_2+C_3]{\text{Replacing } C_3 \text{ by}} \begin{bmatrix} e_{11} & e_{12} & 3 \\ e_{21} & e_{22} & 3 \\ e_{31} & e_{32} & 3 \end{bmatrix} \xrightarrow[R_1 \leftarrow R_1-R_3, R_2 \leftarrow R_2-R_3]{\text{Replacing } R_1, R_2 \text{ by}} \begin{bmatrix} e_{11}-e_{31} & e_{12}-e_{32} & 0 \\ e_{21}-e_{31} & e_{22}-e_{32} & 0 \\ e_{31} & e_{32} & 3 \end{bmatrix}$$

In the above operations the determinant of the matrix is not changed. Now calculating the determinant of the above matrix with respect to last column, we get $det(\mathcal{M}) = 3[(e_{11} - e_{31})(e_{22} - e_{32}) - (e_{21} - e_{31})(e_{12} - e_{32})]$. Now $det(\mathcal{M})$ will be zero if $(e_{11} - e_{31})(e_{22} - e_{32}) - (e_{21} - e_{31})(e_{12} - e_{32}) = 0$. We will show that this is not possible. From the given constraints, we know that every column can have one or two zeros. We will take these two cases and show that in both cases $det(\mathcal{M})$ is non-zero.

Case 1 : In this case assume that there are two zeros in the first column. Without loss of generality assume that $e_{11} = 0, e_{21} = 0$, otherwise we can exchange row and make it $e_{11} = 0, e_{21} = 0$ which will multiply determinant by a non-zero value only. Now putting these values in $det(\mathcal{M})$, we get that $det(\mathcal{M}) = 3e_{31}(e_{12} - e_{22})$. Now e_{12} cannot be equal to e_{22}, otherwise it will give $e_{13} = e_{23}$ making two rows same. Similarly e_{31} cannot be equal to 0, otherwise the first column will be zero. Hence $det(\mathcal{M})$ is non-zero in this case.

Case 2 : In this case assume that there is one zero in the first column. Without loss of generality assume that $e_{11} = 0$, otherwise we can exchange two rows and make it $e_{11} = 0$ which will multiply determinant by a non-zero value only. Now putting this value in $det(\mathcal{M})$, we get that $det(\mathcal{M}) = 3[-e_{31}(e_{22} - e_{32}) - (e_{21} - e_{31})(e_{12} - e_{22})] = 3[-e_{31}e_{22} - e_{21}e_{12} + e_{21}e_{32} + e_{31}e_{12}] = 3[e_{21}(e_{32} - e_{12}) + e_{31}(e_{12} - e_{22})]$. Now we know that e_{21} and e_{31} can't be simultaneously zero, otherwise the complete column will be zero and if one of them is zero then it will reduce to case 1, which means in this case both are non-zero. If e_{21} and e_{31} are equal then the expression for determinant will be $\det(\mathcal{M}) = -3e_{31}(e_{22} - e_{32})$. Now e_{22} can't be equal to e_{32}, otherwise the second and third row will be equal. We can assume without loss of generality that $e_{21} > e_{31} > 0$. Now for determinant to be equal to zero, we must have

$$e_{21}(e_{32} - e_{12}) = e_{31}(e_{22} - e_{12}). \tag{5.4}$$

As we have assumed that $e_{21} > e_{31} > 0$, then for above equation to be true $e_{32} - e_{12} < e_{22} - e_{12} \implies e_{32} < e_{22}$. Now e_{21} can't have value 3, otherwise e_{22} will have value 0 implying that e_{32} is negative, which is not allowed. Also e_{21} can't have value 1, otherwise e_{31} will be zero and this case reduces to case 1. So only possible value of e_{21} is 2 and e_{31} will have value 1. Now e_{22} can't have value 0, otherwise e_{32} will be negative, which is not allowed and as e_{21} is 2, e_{22} can't have value greater than 1, hence e_{22} will have value 1 and e_{32} will have value 0. Now putting these possible values in the equation (5.4), we get that

$$-2e_{12} = 1 - e_{12} \implies e_{12} = -1$$

which is not possible. Hence in this case also, determinant is non-zero.

In all the cases we have shown that matrix $\mathcal{M}$ will be invertible under above constraints. We will have a solution for the $\overline{\alpha}$. This shows that

$$\exists \tau \text{ such that } \tau(k_1\overline{x}^{e_1} + k_2\overline{x}^{e_2} + k_3\overline{x}^{e_3}) = k'_1\overline{x}^{e_1} + k'_2\overline{x}^{e_2} + k'_3\overline{x}^{e_3}$$

for any $k_1, k_2, k_3 \neq 0$, and $k'_1, k'_2, k'_3 \neq 0$. Also τ is only scaling the variables. $\square$

This theorem can be generalized and can be proved using the same method. Here we are giving the statement of generalized theorem in following corollary.

Corollary 5.8. *For all the degree-n, irreducible n-variate, n-nomials having same support that is polynomial of following types*

$$f = k_1\overline{x}^{e_1} + k_2\overline{x}^{e_2} + \ldots + k_n\overline{x}^{e_n} \text{ where } |e_i| = n, \forall i \in [1, n]$$

$$\exists\tau \text{ such that } \tau(k_1\overline{x}^{e_1} + k_2\overline{x}^{e_2} + \ldots + k_n\overline{x}^{e_n}) = k'_1\overline{x}^{e_1} + k'_2\overline{x}^{e_2} + \ldots + k'_n\overline{x}^{e_n}$$

for any $k_1, k_2, \ldots, k_n \neq 0$, and $k'_1, k'_2, \ldots, k'_n \neq 0$. Also τ is only scaling the variables.

Using the theorem 5.7 we will classify irreducible trivariate trinomial cubic forms into finite classes.

Theorem 5.9. *Irreducible trivarite trinomial cubic forms are completely classified into 4 classes.*

Proof. For proving this we will first count number of irreducible trivariate trinomial cubic forms. Since there are 10 trivariate cubic monomials like $x^3, y^3, z^3, x^2y, x^2z, y^2x, y^2z, z^2x, z^2y$ and xyz, total number of trivariate trinomial cubic forms will be $\binom{10}{3}$. Out of which 12 are bivariate cubic forms like $x^3 + x^2y + xy^2$ and 51 are factorizable trivariate cubic forms like x^3+xy^2+xyz. So remaining 57-cubic forms are irreducible trivariate trinomial which are classified in following 4-classes.
Using theorem 5.7 we know that any irreducible trivariate trinomial cubic form $f = a_1\overline{x}^{e_1} + a_2\overline{x}^{e_2} + a_3\overline{x}^{e_3}$, such that $|e_i| = 3, \forall i \in [1, 3]$ is equivalent to $f' = \overline{x}^{e_1} + \overline{x}^{e_2} + \overline{x}^{e_3}$. So without loss of generality we will only consider those irreducible trivariate trinomial cubic forms whose coefficients are 1.

Class-1	**Class-2**	**Class-3**	**Class-4**
$x^3+y^3+z^3$	$x^3+y^3+x^2z$	x^3+y^3+xyz	$x^3+y^2x+z^2y$
$x^3+y^3+z^2x$	$x^3+y^3+y^2z$	x^3+z^3+xyz	$x^3+y^2z+z^2x$
$x^3+y^3+z^2y$	$x^3+z^3+x^2y$	$x^3+x^2y+z^2y$	$y^3+x^2y+z^2x$
$x^3+z^3+y^2x$	$x^3+z^3+z^2y$	$x^3+x^2z+y^2z$	$y^3+x^2z+z^2y$
$x^3+z^3+y^2z$	$x^3+x^2y+y^2z$	x^3+y^2z+xyz	$z^3+x^2y+y^2z$
$x^3+y^2z+z^2y$	$x^3+x^2z+z^2y$	x^3+z^2y+xyz	$z^3+x^2z+y^2x$
$y^3+z^3+x^2y$	$x^3+y^2x+y^2z$	y^3+z^3+xyz	
$y^3+z^3+x^2z$	$x^3+z^2x+z^2y$	$y^3+x^2z+y^2z$	
$y^3+x^2z+z^2x$	$y^3+z^3+y^2x$	y^3+x^2z+xyz	
$z^3+x^2y+y^2x$	$y^3+z^3+z^2x$	$y^3+y^2x+z^2x$	
$x^2y+y^2z+z^2x$	$y^3+x^2y+x^2z$	y^3+z^2x+xyz	
$xy^2+yz^2+zx^2$	$y^3+x^2z+y^2x$	$z^3+x^2y+z^2y$	
	$y^3+y^2z+z^2x$	z^3+x^2y+xyz	
	$y^3+z^2x+z^2y$	$z^3+y^2x+z^2x$	
	$z^3+x^2y+x^2z$	z^3+y^2x+xyz	
	$z^3+x^2y+z^2x$	$x^2y+x^2z+y^2z$	
	$z^3+y^2x+y^2z$	$x^2y+x^2z+z^2y$	
	$z^3+y^2x+z^2y$	$x^2y+z^2x+z^2y$	
		$x^2z+y^2x+y^2z$	
		$y^2x+y^2z+z^2x$	
		$y^2x+z^2x+z^2y$	

Now first we will show that all the polynomials in same class are equivalent by giving some argument or by giving an invertible linear transformation τ. Then we will show that polynomial in one class is not equivalent to polynomial of some other class.

Class - 1 Polynomials : Here we will show why all polynomials in class-1 are equivalent.

1) $x^3+y^3+z^3 \sim x^3+y^3+z^2x$: Here we can orthogonally decompose the variables in two parts one containing x, z and other containing y. Since y is not interfering with x, z in the final transformation we will send $y \mapsto y$. Now we have to show that $x^3+z^3 \sim x^3+z^2x$. Using theorem 4.3 it is easy to see that both are equivalent as both have three distinct

factors over $\mathbb{C}$ and both are equivalent to $xz(x+z)$.

2) $x^3+y^3+z^3 \sim x^3+y^3+z^2y$: Here we will orthogonally decompose variables into two parts one containing x and other containing y, z. Now using the similar argument it is easy to show that $x^3+y^3+z^3 \sim x^3+y^3+z^2y$.

3) $x^3+y^3+z^2x \sim x^3+z^3+y^2x$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto x, y \mapsto z, z \mapsto y$$

4)$x^3+y^3+z^2y \sim x^3+z^3+y^2z$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto x, y \mapsto z, z \mapsto y$$

5) $x^3+y^3+z^3 \sim x^3+y^2z+z^2y$: Here we will orthogonally decompose variables into two parts one containing x and other containing y, z. Now we will send $x \mapsto x$ and we have to show that $y^3+z^3 \sim y^2z+z^2y$. Since both the polynomials have three distinct factors over $\mathbb{C}$, both are equivalent to $yz(y+z)$ using theorem 4.3. Hence both the polynomials are equivalent.

6) $x^3+z^3+y^2x \sim y^3+z^3+x^2y$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto x, z \mapsto z$$

7) $x^3+z^3+y^2z \sim y^3+z^3+x^2z$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto x, z \mapsto z$$

8) $x^3+y^2z+yz^2 \sim y^3+x^2z+z^2x$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto x, z \mapsto z$$

9) $x^3 + y^2z + z^2y \sim z^3 + x^2y + y^2x$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto z, y \mapsto x, z \mapsto y$$

10) $x^3 + y^3 + z^3 \sim x^2y + y^2z + z^2x$: It is the most non-trivial equivalence in this class. For this equivalence apply following transformation on the polynomial on the left side:

$$x \mapsto x + y + z$$

$$y \mapsto \omega^{\frac{2}{3}}(x + \omega y + \omega^2 z)$$

$$z \mapsto \omega^{\frac{1}{3}}(x + \omega^2 y + \omega z)$$

Using this transformation $x^3 + y^3 + z^3 \sim 9x^2y + 9y^2z + 9z^2x \sim x^2y + y^2z + z^2x$(using theorem 4.3).

11) $x^2y+y^2z+z^2x \sim xy^2+yz^2+zx^2$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto x, y \mapsto z, z \mapsto y$$

Class - 2 Polynomials : Here we will show why all polynomials in class - 2 are equivalent.

1) $x^3 + y^3 + x^2z \sim x^3 + y^3 + y^2z$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto x, z \mapsto z$$

2) $x^3 + y^3 + y^2z \sim x^3 + z^3 + z^2y$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto x, y \mapsto z, z \mapsto y$$

3) $x^3 + y^3 + y^2z \sim x^3 + x^2y + y^2z$: This is the first non-trivial equivalence in this

class. Apply the following transformation on the polynomial on the right side to see the equivalence:

$$x \mapsto x - \frac{1}{3}y, y \mapsto y, z \mapsto \frac{1}{3}x + \frac{25}{27}y + z$$

4) $x^3 + x^2y + y^2z \sim x^3 + x^2z + z^2y$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto x, y \mapsto z, z \mapsto y$$

5) $x^3 + x^2y + y^2z \sim x^3 + y^2x + y^2z$: This is the second non-trivial equivalence in this class. Apply the following transformation on the polynomial on the right side to see the equivalence:

$$x \mapsto x + \frac{1}{3}y, y \mapsto y, z \mapsto -\frac{4}{3}x - \frac{10}{27}y + z$$

6) $x^3 + y^2x + y^2z \sim x^3 + z^2x + z^2y$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto x, y \mapsto z, z \mapsto y$$

7) $x^3 + y^3 + x^2z \sim y^3 + z^3 + y^2x$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto z, z \mapsto x$$

8) $y^3 + z^3 + y^2x \sim y^3 + z^3 + z^2x$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto x, y \mapsto z, z \mapsto y$$

9) $x^3 + y^2x + y^2z \sim y^3 + x^2y + x^2z$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto x, z \mapsto z$$

10) $x^3 + x^2y + y^2z \sim y^3 + x^2z + y^2x$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto x, z \mapsto z$$

11) $x^3 + x^2z + z^2y \sim y^3 + y^2z + z^2x$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto x, z \mapsto z$$

12) $x^3 + y^2x + y^2z \sim y^3 + z^2x + z^2y$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto z, z \mapsto x$$

13) $x^3 + y^3 + x^2z \sim x^3 + z^3 + x^2y$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto x, y \mapsto z, z \mapsto y$$

14) $x^3 + z^2x + z^2y \sim z^3 + x^2y + x^2z$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto z, y \mapsto y, z \mapsto x$$

15) $x^3 + x^2z + z^2y \sim z^3 + x^2y + z^2x$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto z, y \mapsto y, z \mapsto x$$

16) $x^3 + y^2x + y^2z \sim z^3 + y^2x + y^2z$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto z, y \mapsto y, z \mapsto x$$

17) $x^3 + x^2y + y^2z \sim z^3 + y^2x + z^2y$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto z, y \mapsto y, z \mapsto x$$

Class - 3 Polynomials :: Here we will show that why all polynomials in class - 3 are equivalent.

1) $x^3 + y^3 + xyz \sim x^3 + z^3 + xyz$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto x, y \mapsto z, z \mapsto y$$

2) $x^3 + y^3 + xyz \sim x^3 + x^2y + z^2y$: To see this equivalence apply the following transformation on the polynomial on the left side

$$x \mapsto \frac{1}{2}(x - iz), y \mapsto \frac{1}{2}(x + iz), z \mapsto 3x + 4y$$

3) $x^3 + x^2y + z^2y \sim x^3 + x^2z + y^2z$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto x, y \mapsto z, z \mapsto y$$

4) $x^3 + y^3 + xyz \sim x^3 + y^2z + xyz$: To see this equivalence apply the following transformation on the polynomial on the left side

$$x \mapsto \theta y, y \mapsto \theta^2(x + y), z \mapsto 3x - z$$

where θ is the 6^{th} primitive root of unity.

5) $x^3 + y^2z + xyz \sim x^3 + z^2y + xyz$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto x, y \mapsto z, z \mapsto y$$

6) $x^3 + y^3 + xyz \sim y^3 + z^3 + xyz$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto z, z \mapsto x$$

7) $x^3 + x^2z + y^2z \sim y^3 + x^2z + y^2z$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto x, z \mapsto z$$

8) $x^3 + y^2z + xyz \sim y^3 + x^2z + xyz$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto x, z \mapsto z$$

9) $x^3 + z^2y + xyz \sim y^3 + z^2x + xyz$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto x, z \mapsto z$$

10) $x^3 + x^2y + z^2y \sim y^3 + y^2x + z^2x$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto x, z \mapsto z$$

11) $x^3 + x^2z + y^2z \sim z^3 + x^2y + z^2y$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto z, y \mapsto x, z \mapsto y$$

12) $x^3 + y^2z + xyz \sim z^3 + x^2y + xyz$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto z, y \mapsto x, z \mapsto y$$

13) $x^3 + x^2z + y^2z \sim z^3 + y^2x + z^2x$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto z, y \mapsto y, z \mapsto x$$

14) $x^3 + z^2y + xyz \sim z^3 + y^2x + xyz$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto z, y \mapsto x, z \mapsto y$$

15) $x^3 + y^3 + xyz \sim x^2y + x^2z + z^2y$: To prove this equivalence we will use lemma 5.5, which says that $f \sim g \implies H(f) \sim H(g)$, where $H(f)$ is the determinant of Hessian matrix. Now consider $f = x^3 + y^3 + xyz$ and $g = x^3 + x^2y + z^2y$. We know that $f \sim g$, then by lemma 5.5, we have that $H(f) \sim H(g)$. Now let us find the value of $H(f)$ and $H(g)$.

$$H(f) = \det \begin{bmatrix} 6x & z & y \\ z & 6y & x \\ y & x & 0 \end{bmatrix}$$

after taking the determinant we get that $H(f) = -6x^3 - 6y^3 + 2xyz$. Now from the theorem 5.7, we know that $-6x^3 - 6y^3 + 2xyz \sim x^3 + y^3 + xyz$. It shows that $H(f) \sim x^3 + y^3 + xyz$. Now let us find the value of $H(g)$, which is as below

$$H(g) = \det \begin{bmatrix} 6x + 2y & 2x & 0 \\ 2x & 0 & 2z \\ 0 & 2z & 2y \end{bmatrix}$$

after taking the determinant we get that $H(g) = -24xz^2 - 8yz^2 - 8x^2y$. Now again using theorem 5.7, we can write that $-24xz^2 - 8yz^2 - 8x^2y \sim xz^2 + yz^2 + x^2y$. It shows that $H(g) \sim xz^2 + yz^2 + x^2y$ and $xz^2 + yz^2 + x^2y \sim x^2y + x^2z + z^2y$ by exchanging the variable x and z on the left side. So finally we have $H(g) \sim x^2y + x^2z + z^2y$. So the complete picture is

$$x^3 + y^3 + xyz \sim H(f) \sim H(g) \sim x^2y + x^2z + z^2y$$

which shows that $x^3 + y^3 + xyz \sim x^2y + x^2z + z^2y$.

16) $x^2y+x^2z+z^2y \sim x^2y+x^2z+y^2z$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto x, y \mapsto z, z \mapsto y$$

17) $x^2y+x^2z+z^2y \sim x^2y+z^2x+z^2y$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto z, y \mapsto y, z \mapsto x$$

18) $x^2y+x^2z+z^2y \sim x^2z+y^2x+y^2z$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto z, z \mapsto x$$

19) $x^2y+x^2z+z^2y \sim y^2x+y^2z+z^2x$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto x, z \mapsto z$$

20) $x^2y+x^2z+z^2y \sim y^2x+z^2x+z^2y$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto z, y \mapsto x, z \mapsto y$$

Class - 4 Polynomials : Here we will show why all polynomials in class - 4 are equivalent.

1) $x^3 + y^2x + z^2y \sim x^3 + y^2z + z^2x$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto x, y \mapsto z, z \mapsto y$$

2) $x^3 + y^2x + z^2y \sim y^3 + x^2y + z^2x$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto x, z \mapsto z$$

3) $x^3 + y^2x + z^2y \sim y^3 + x^2z + z^2y$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto y, y \mapsto z, z \mapsto x$$

4) $x^3 + y^2x + z^2y \sim z^3 + x^2y + y^2z$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto z, y \mapsto y, z \mapsto x$$

5) $x^3 + y^2x + z^2y \sim z^3 + x^2z + y^2x$: Here it is easy to see by symmetry. Use following τ on the polynomial on the left side:

$$x \mapsto z, y \mapsto x, z \mapsto y$$

Now we will show why polynomials in one class are not equivalent to the polynomials in other class. Since polynomials in one class are equivalent to each other, we will take one polynomial from a class and we will show that it is not equivalent to a polynomial in all the other classes.

Class - 1 and Class - 2 : Here we will show why polynomials in class - 1 and class - 2 are not equivalent to each other. We will take one polynomial from class - 1 and one polynomial from class - 2 and show that they are not equivalent under any invertible linear transformation τ. We will denote polynomial from class - 1 by f and polynomial from class - 2 by g.

Let us take the first polynomial from both the classes that is

$$f = x^3 + y^3 + z^3 \text{ and } g = x^3 + y^3 + x^2z$$

To prove that these two polynomials are inequivalent we will use our theorem $\tau(f) = g \implies \tau(Df) = Dg$. If we can prove that $\tau(Df) \neq Dg$ for a general τ then we have proved $f \nsim g$ (by contrapositive).

Consider the derivative space of both polynomials Df and Dg.

$$Df = \langle x^2, y^2, z^2 \rangle \text{ and}$$

$$Dg = \langle 3x^2 + 2xz, y^2, x^2 \rangle$$

Let us apply a general τ on Df as defined below

$$\tau = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix}$$

Since in the image(Dg), z^2 is not present which implies that coefficient of z^2 should be zero in $\tau(Df)$ in all three components. Writing three equations related to coefficients of z^2 in three components we get the following equations

$$a_3^2 = 0 \implies a_3 = 0 \tag{5.5}$$

$$b_3^2 = 0 \implies b_3 = 0 \tag{5.6}$$

$$c_3^2 = 0 \implies c_3 = 0 \tag{5.7}$$

which implies that the last column of τ is zero resulting into non-invertible transformation. Hence there is no invertible linear transformation which will make $Df \sim Dg$. We conclude that $Df \nsim Dg \implies f \nsim g$.

Class - 1 and Class - 3 : Here we will show why polynomials in class - 1 and class - 3 are not equivalent to each other. We will take one polynomial from class - 1 and one polynomial from class - 3 and show that they are not equivalent under any invertible linear transformation τ. We will denote polynomial from class - 1 by f and polynomial from class - 3 by g.

Let us take the first polynomial from both the classes that is

$$f = x^3 + y^3 + z^3 \text{ and } g = x^3 + y^3 + xyz$$

To prove that these two polynomials are inequivalent we will use our theorem $\tau(f) = g \implies \tau(Df) = Dg$. If we can prove that $\tau(Df) \neq Dg$ for a general τ then we have proved $f \nsim g$ (by contrapositive).

Consider the derivative space of both polynomials Df and Dg.

$$Df = \langle x^2, y^2, z^2 \rangle \text{ and}$$

$$Dg = \langle 3x^2 + yz, 3y^2 + xz, xy \rangle$$

Let us apply a general τ on Df as defined below

$$\tau = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix}$$

Since in the image(Dg), z^2 is not present which implies that coefficient of z^2 should be zero in $\tau(Df)$ in all three components. Writing three equations related to coefficients of z^2 in three components we get the following equations

$$a_3^2 = 0 \implies a_3 = 0 \tag{5.8}$$

$$b_3^2 = 0 \implies b_3 = 0 \tag{5.9}$$

$$c_3^2 = 0 \implies c_3 = 0 \tag{5.10}$$

which implies that the last column of τ is zero resulting into non-invertible transformation. Hence there is no invertible linear transformation which will make $Df \sim Dg$. We conclude that $Df \nsim Dg \implies f \nsim g$.

Class - 1 and Class - 4 : Here we will show why polynomials in class - 1 and class - 4 are not equivalent to each other. We will take one polynomial from class - 1 and one polynomial from class - 4 and show that they are not equivalent under any invertible linear transformation τ. We will denote polynomial from class - 1 by f and polynomial from class - 4 by g.

Let us take the first polynomial from both the classes that is

$$f = x^3 + y^3 + z^3 \text{ and } g = x^3 + y^2x + z^2y$$

To prove that these two polynomials are inequivalent we will use our theorem - $f \sim g \implies H(f) \sim H(g)$. If we can prove that $H(f) \nsim H(g)$ for a general τ then we have proved $f \nsim g$ (by contrapositive).

Let us calculate the values $H(f)$ *and* $H(g)$.

$$H(f) = \det \begin{bmatrix} 6x & 0 & 0 \\ 0 & 6y & 0 \\ 0 & 0 & 6z \end{bmatrix} \; and \; H(g) = \det \begin{bmatrix} 6x & 2y & 0 \\ 2y & 2x & 2z \\ 0 & 2z & 2y \end{bmatrix}$$

Calculating the determinant of above matrices, we get

$$H(f) = f' = 216xyz \; and \; H(g) = g' = 24x^2y - 24xz^2 - 8y^3$$

Now to prove that f' *and* g' are inequivalent, we will use our theorem - $f' \sim g' \implies Df' \sim Dg'$. If we can prove that $Df' \nsim Dg'$ for a general τ then we have proved $f' \nsim g'$ (by contrapositive). Let us calculate Df' and Dg'.

$$Df' = \langle yz, xz, xy \rangle \text{ and}$$

$$Dg' = \langle 2xy - z^2, x^2 - y^2, xz \rangle$$

Let us apply a general τ on Dg' as defined below

$$\tau = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix}$$

Since in the Df', z^2 is not present which implies that coefficient of z^2 should be zero in

$\tau(Dg')$ in all three components. Writing three equations related to coefficients of z^2 in three components we get the following equations

$$2a_3b_3 - c_3^2 = 0 \tag{5.11}$$

$$a_3^2 - b_3^2 = 0 \tag{5.12}$$

$$a_3c_3 = 0 \tag{5.13}$$

Equation (5.13) implies that either $a_3 = 0$ or $c_3 = 0$. First let us take $a_3 = 0$, then from equation (5.11), we get that $c_3 = 0$ and from equation (5.12), we get that $b_3 = 0$. This shows that last column of τ is zero which is not possible.

In second case let us take $c_3 = 0$, then from equation (5.11), we get that $a_3b_3 = 0 \implies a_3 = 0 \text{ } or \text{ } b_3 = 0$. In both cases using equation (5.12), we get that last column of τ is zero, resulting into a non-invertible transformation.

Hence $Df' \nsim Dg' \implies f' \nsim g'$. Here f' and g' were nothing but $H(f)$ and $H(g)$, so we have showed that $H(f) \nsim H(g) \implies f \nsim g$.

Class - 2 and Class - 3 : Here we will show why polynomials in class - 2 and class - 3 are not equivalent to each other. We will take one polynomial from class - 2 and one polynomial from class - 3 and show that they are not equivalent under any invertible linear transformation τ. We will denote polynomial from class - 2 by f and polynomial from class - 3 by g.

Let us take the first polynomial from both the classes that is

$$f = x^3 + y^3 + x^2z \text{ and } g = x^3 + y^3 + xyz$$

To prove that these two polynomials are inequivalent we will use our theorem $\tau(f) = g \implies \tau(Df) = Dg$. If we can prove that $\tau(Df) \neq Dg$ for a general τ then we have proved $f \nsim g$ (by contrapositive).

Consider the derivative space of both polynomials Df and Dg.

$$Df = \langle 3x^2 + 2xz, y^2, x^2 \rangle = \langle xz, y^2, x^2 \rangle \text{ and}$$

$$Dg = \langle 3x^2 + yz, 3y^2 + xz, xy \rangle$$

Let us apply a general τ on Df as defined below

$$\tau = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix}$$

Since in the image(Dg), z^2 is not present which implies that coefficient of z^2 should be zero in $\tau(Df)$ in all three components. Writing three equations related to coefficients of z^2 in three components we get the following equations

$$a_3 c_3 = 0 \tag{5.14}$$

$$b_3^2 = 0 \Longrightarrow b_3 = 0 \tag{5.15}$$

$$a_3^2 = 0 \Longrightarrow a_3 = 0 \tag{5.16}$$

Using above values our new τ is given as below

$$\tau = \begin{bmatrix} a_1 & a_2 & 0 \\ b_1 & b_2 & 0 \\ c_1 & c_2 & c_3 \end{bmatrix}$$

Applying τ on first component and making it equal to the linear combination of components of Dg we get following equation

$$(a_1 x + a_2 y)(c_1 x + c_2 y + c_3 z) = \lambda_1(3x^2 + yz) + \lambda_2(3y^2 + xz) + \lambda_3(xy) \tag{5.17}$$

Similarly applying τ on second component and making it equal to the linear combination of components of Dg we get the following equation

$$(b_1 x + b_2 y)^2 = \lambda_4(3x^2 + yz) + \lambda_5(3y^2 + xz) + \lambda_6(xy) \tag{5.18}$$

Now comparing the coefficient of various terms of the above equation we get the following equations

$$
\begin{aligned}
b_1^2 &= 3\lambda_4 \\
b_2^2 &= 3\lambda_5 \\
2b_1b_2 &= \lambda_6 \\
0 &= \lambda_4 \\
0 &= \lambda_5
\end{aligned}
$$

which implies that $b_1^2 = 0 \implies b_1 = 0$ and $b_2^2 = 0 \implies b_2 = 0$, which implies that the second row of τ is zero resulting into non-invertible transformation. Hence there is no invertible linear transformation which will make $Df \sim Dg$. We can conclude that $Df \nsim Dg \implies f \nsim g$.

Class - 2 and Class - 4 : Here we will show why polynomials in class - 2 and class - 4 are not equivalent to each other. We will take one polynomial from class - 2 and one polynomial from class - 4 and show that they are not equivalent under any invertible linear transformation τ. We will denote polynomial from class - 2 by f and polynomial from class - 4 by g.

Let us take the first polynomial from both the classes that is

$$f = x^3 + y^3 + x^2z \text{ and } g = x^3 + y^2x + z^2y$$

To prove that these two polynomials are inequivalent we will use our theorem $\tau(f) = g \implies \tau(Df) = Dg$. If we can prove that $\tau(Df) \neq Dg$ for a general τ then we have proved $f \nsim g$ (by contrapositive).

Consider the derivative space of both polynomials Df and Dg.

$$Df = \langle 3x^2 + 2xz, y^2, x^2 \rangle = \langle xz, y^2, x^2 \rangle \text{ and}$$

$$Dg = \langle 3x^2 + y^2, z^2 + 2xy, yz \rangle$$

Let us apply a general τ on Dg as defined below

$$\tau = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix}$$

Since in the Df, z^2 is not present so we will apply τ on Dg and try to make it equivalent to Df. In Df there is no term of z^2 so the coefficient of z^2 in all the three components of $\tau(Dg)$ should be zero. Writing three equations related to coefficients of z^2 in three components we get the following equations

$$3a_3^2 + b_3^2 = 0 \tag{5.19}$$

$$c_3^2 + 2a_3b_3 = 0 \tag{5.20}$$

$$b_3c_3 = 0 \tag{5.21}$$

Equation (5.21) implies that either $b_3 = 0$ or $c_3 = 0$. Taking the first case that is $b_3 = 0$, then using equation (5.20) we get $c_3 = 0$ and using equation (5.19) we get $a_3 = 0$, which implies that $a_3 = b_3 = c_3 = 0$ resulting into a non-invertible τ.

Taking the second case that is $c_3 = 0$ then using equation (5.20) we will get either $a_3 = 0$ or $b_3 = 0$. In both the conditions along with equation (5.19) we get that $a_3 = b_3 = c_3 = 0$ which makes the last column of τ zero resulting into a non-invertible τ.

In both cases we have observed that $\nexists \tau$ such that $\tau(Dg) = Df \implies Df \nsim Dg \implies f \nsim g$.

Class - 3 and Class - 4 : Here we will show why polynomials in class - 3 and class - 4 are not equivalent to each other. We will take one polynomial from class - 3 and one polynomial from class - 4 and show that they are not equivalent under any invertible linear transformation τ. We will denote polynomial from class - 3 by f and polynomial from class - 4 by g.

Let us take the first polynomial from both the classes that is

$$f = x^3 + y^3 + xyz \text{ and } g = x^3 + y^2x + z^2y$$

To prove that these two polynomials are inequivalent we will use our theorem $\tau(f) =$

$g \implies \tau(Df) = Dg$. If we can prove that $\tau(Df) \neq Dg$ for a general τ then we have proved $f \nsim g$ (by contrapositive).

Consider the derivative space of both polynomials Df and Dg.

$$Df = \langle 3x^2 + yz, 3y^2 + xz, xy \rangle \text{ and}$$

$$Dg = \langle 3x^2 + y^2, z^2 + 2xy, yz \rangle$$

Let us apply a general τ on Dg as defined below

$$\tau = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix}$$

Since in the Df, z^2 is not present so we will apply τ on Dg and try to make it equivalent to Df. In Df there is no term of z^2 so the coefficient of z^2 in all the three components of $\tau(Dg)$ should be zero. Writing three equations related to coefficients of z^2 in three components we get the following equations

$$3a_3^2 + b_3^2 = 0 \tag{5.22}$$

$$c_3^2 + 2a_3b_3 = 0 \tag{5.23}$$

$$b_3c_3 = 0 \tag{5.24}$$

Equation (5.24) implies that either $b_3 = 0$ or $c_3 = 0$. Taking the first case that is $b_3 = 0$, then using equation (5.23) we get $c_3 = 0$ and using equation (5.22) we get $a_3 = 0$, which implies that $a_3 = b_3 = c_3 = 0$ making τ non-invertible.

Taking the second case that is $c_3 = 0$ then using equation (5.23) we will get either $a_3 = 0$ or $b_3 = 0$. In both the conditions along with equation (5.22) we get that $a_3 = b_3 = c_3 = 0$ which makes the last column of τ zero resulting into a non-invertible τ.

In both cases we have observed that $\nexists \tau$ such that $\tau(Dg) = Df \implies Df \nsim Dg \implies f \nsim g$. This completes the proof of our main result. $\square$

Following corollary shows that conjecture-1 is true in the case of trivariate trinomial cubic forms.

Corollary 5.10. *Conjecture-1 is true in the case of trivariate trinomial cubic forms.*

Proof. In the case of trivariate trinomials, we have two types of polynomials - one which factorizes over $\mathbb{C}$ and one which is irreducible over $\mathbb{C}$. Conjecture-1 is true in the case of factorizable trivariate trinomials and it can be seen with the help of *corollary 4.5.* The proof for Conjecture-1 in case of irreducible trivariate trinomials is given in the previous theorem. There we took two polynomials which are not equivalent and we showed that there is no invertible linear transformation τ which makes their first order derivative spaces equivalent. $\square$

Following corollary shows that there are finitely many equivalence classes in the case of trivariate trinomial cubic forms.

Corollary 5.11. *Trivariate trinomial cubic forms have finitely many equivalence classes.*

Proof. In the case of trivariate trinomials, we have two types of polynomials - one which factorizes over $\mathbb{C}$ and one which is irreducible over $\mathbb{C}$. Theorem 5.1 showed that there are three equivalence classes in case of factorizable trivariate cubic forms. Theorem 5.8 showed that there are four equivalence classes in case of irreducible trivariate trinomial cubic forms. Combining these two shows that there are finitely many equivalence classes in case of trivariate trinomial cubic forms. $\square$

Now after completely classifying trivariate trinomial cubic forms, we will move to the irreducible trivariate quadnomial cubic forms.

Chapter 6

Infinite Equivalence Classes

In the previous chapter we studied the trivariate trinomial cubic forms. There we showed that trivariate trinomial cubic forms have finitely many equivalence classes like bivariate cubic forms. Now in this chapter we will study the irreducible trivariate quadnomial cubic forms. We will study the symmetric trivariate cubic quadnomial and we will show that in the case of irreducible trivariate quadnomial cubic forms there exists infinitely many equivalence classes over $\mathbb{C}$ and will give a conjecture related to the equivalence of two symmetric cubic forms. We will give some examples which will support the conjecture later in this chapter.

6.1 Preliminaries

Definition 6.1. Symmetric polynomial. Let the group S_n(symmetric group of size n) act on the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ by permuting the variables:

$$\sigma p(x_1, \ldots, x_n) = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)}), \forall \sigma \in S_n \tag{6.1}$$

The polynomials invariant under this action of S_n are called *symmetric polynomials*.

Example 6.1.1. For $n = 3$ the polynomial $x_1^2x_2 + x_2^2x_3 + x_3^2x_1 + x_1x_2^2 + x_2x_3^2 + x_3x_1^2$ is symmetric but $x_1^2x_2 + x_2^2x_3 + x_3^2x_1$ is not.

6.2 Main Results

6.2.1 Infinitely many Equivalence Classes

In this section we will show that in the case of irreducible trivariate quadnomial cubic forms there exists infinitely many equivalence classes. Before proceeding to the proof, we need some results which are given below.

Lemma 6.2. *The polynomial $f(x, y, z) = x^3 + y^3 + z^3 + kxyz$ is factorizable over $\mathbb{C}$ if and only if $k = -3, -3\omega, -3\omega^2$.*

Proof. Let us assume that $f(x, y, z) = x^3 + y^3 + z^3 + kxyz$ is factorizable as $f(x, y, z) = g(x, y, z) \cdot h(x, y, z)$. Then one of the factors will be linear and the other factor will be quadratic.

Claim : The factors g and h will be homogeneous polynomials.

Proof. For the sake of the contradiction assume that they are not homogeneous. We know that

$$f(x, y, z) = x^3 + y^3 + z^3 + kxyz = g(x, y, z) \cdot h(x, y, z).$$

Now as the factors are not homogeneous, consider the lowest degree term in g and after multiplying it with lowest degree term in h, we will get the lowest degree term in f. Similarly we will get highest degree term in f by multiplying the highest degree term in g with highest degree term in h. Clearly the lowest degree term will not cancel out with any other term in $g \cdot h$, so the product $g \cdot h$ will not be a homogeneous polynomial, which is a contradiction as f was a homogeneous polynomial. $\square$

Without loss of generality, we can assume that $g(x, y, z) = (ax+by+cz)$ and $h(x, y, z) = (dx^2 + ey^2 + fz^2 + gxy + hyz + ixz)$ and $a, b, c \neq 0$ and $d, e, f \neq 0$. Otherwise we will not be able to generate x^3, y^3 and z^3. Also we know that coefficient of x^3 is 1, we can take $g(x, y, z) = (x + a'y + b'z)$ and $h(x, y, z) = (x^2 + c'y^2 + d'z^2 + e'xy + f'yz + g'xz)$. So we have

$$f(x, y, z) = x^3 + y^3 + z^3 + kxyz = (x + a'y + b'z)(x^2 + c'y^2 + d'z^2 + e'xy + f'yz + g'xz)$$

Now consider the polynomial $f(x, y, z)$ over function field $\mathbb{C}(y, z)[x]$. The above factorization tells us that $x = -(a'y + b'z)$ is a root of the polynomial $f(x, y, z)$ over function field $\mathbb{C}(y, z)[x]$. This means that

$$-(a'y + b'z)^3 + y^3 + z^3 - k(a'y + b'z)yz = 0.$$

After simplifying it we get that

$$(1 - a'^3)y^3 + (1 - b'^3)z^3 - (3a'b' + k)yz(a'y + b'z) = 0.$$

It tells us that

$$a'^3 = 1 \text{ and } b'^3 = 1 \tag{6.2}$$

$$k = -3a'b' \tag{6.3}$$

Form the equation (6.2), we get that $(a'b')^3 = 1 \implies a'b' = 1, \omega, \omega^2$. Hence the possible values of k for which $f(x, y, z)$ will be factorizable are $-3, -3\omega$ and $-3\omega^2$. □

Notation : We have given a notation $H_f(\overline{x})$ to denote the determinant of Hessian matrix for polynomial $f(\overline{x})$. $H^{-1}(f(\overline{x}))$ will denote the polynomial whose Hessian is $f(\overline{x})$ and $H^{-i}(f(\overline{x}))$ will denote a polynomial on which applying Hessian i-times gives the polynomial $f(\overline{x})$. Also we will use f_k to denote the polynomial $x^3 + y^3 + z^3 + kxyz$.

Lemma 6.3. *There will always exist a polynomial f_k such that $H^{-1}(f_m) = f_k$.*

Proof. To prove it consider the Hessian of the polynomial f_k. It is given as

$$H(f_k) = \det \begin{bmatrix} 6x & kz & ky \\ kz & 6y & kx \\ ky & kx & 6z \end{bmatrix}$$

$$H(f_k) = -6\left[x^3 + y^3 + z^3 - \left(\frac{36}{k^2} + \frac{k}{3}\right)xyz\right]$$

Since we are over $\mathbb{C}$, we can always leave the constant multiple, the expression for Hessian is

$$H(f_k) = x^3 + y^3 + z^3 - \left(\frac{36}{k^2} + \frac{k}{3}\right) xyz.$$

$H(f_k) = f_m$ if

$$-\left(\frac{36}{k^2} + \frac{k}{3}\right) = m.$$

Now $H^{-1}(f_m) = f_k$ will exists if the above equation will have a solution for k for any value of m. The simplified equation is

$$k^3 + 3mk^2 + 108 = 0 \tag{6.4}$$

Since we are over $\mathbb{C}$, this equation will always have a solution for k and hence $H^{-1}(f_m) = f_k$ will always exists. □

Theorem 6.4. *In case of trivariate quadnomial cubic forms equivalence over $\mathbb{C}$ there exists infinitely many equivalence classes.*

Proof. To prove this theorem we will use the polynomial $f_{-3} = x^3 + y^3 + z^3 - 3xyz$ and Hessian matrix. From the lemma 6.2 we know that $x^3 + y^3 + z^3 + kxyz$ is factorizable only when $k = -3, -3\omega, -3\omega^2$. From the theorem 5.1 we know that two trivariate polynomials are equivalent over $\mathbb{C}$ if the number of factors are same. Since $f_k = x^3 + y^3 + z^3 + kxyz$ is irreducible over $\mathbb{C}$ except when $k = -3, -3\omega, -3\omega^2$. This shows that

$$f_{-3} = x^3 + y^3 + z^3 - 3xyz \nsim f_k = x^3 + y^3 + z^3 + kxyz, \forall k \in \mathbb{C}/\{-3, -3\omega, -3\omega^2\} \tag{6.5}$$

Now let us find the Hessian of the polynomial f_k. It is given as

$$H(f_k) = \det \begin{bmatrix} 6x & kz & ky \\ kz & 6y & kx \\ ky & kx & 6z \end{bmatrix}$$

$$H(f_k) = -6\left[x^3 + y^3 + z^3 - \left(\frac{36}{k^2} + \frac{k}{3}\right) xyz\right]$$

Since we are over $\mathbb{C}$, we can always leave the constant multiple, the expression for Hessian is

$$H(f_k) = x^3 + y^3 + z^3 - \left(\frac{36}{k^2} + \frac{k}{3}\right) xyz$$

Now suppose that $H^{-1}(f_k) = f_m$, which means that $H(f_m) = f_k$. Now comparing the coefficients, we get that

$$-\left(\frac{36}{m^2} + \frac{m}{3}\right) = k \implies \frac{108 + m^3}{3m^2} = -k$$

Now the polynomial $H^{-1}(f_k) = f_m$, where m is the root of the equation $m^3 + 3km^2 + 108 = 0$.

Now from the lemma 5.5 we can say that

$$H(f) \nsim H(g) \implies f \nsim g$$

From this result and equation (6.5), we get that

$$H^{-1}(f_{-3}) \nsim H^{-1}(f_k), \forall k \in \mathbb{C}/\{-3, -3\omega, -3\omega^2\} \text{ except } H^{-1}(f_{-3}) \tag{6.6}$$

Again we can apply the same on the equation (6.6), to get that

$$H^{-1}(H^{-1}(f_{-3})) \nsim H^{-1}(H^{-1}(f_k)) \text{ except } H^{-1}(H^{-1}(f_{-3})) \tag{6.7}$$

$$\implies H^{-2}(f_{-3}) \nsim H^{-2}(f_k) \tag{6.8}$$

Using the inverse of Hessian repeatedly we will get an infinite sequence $H^{-i}(f_{-3}), i \geq 0, i \in \mathbb{Z}$, if we solve the equation $m^3 + 3km^2 + 108 = 0$ with $k = -3$ as initial value of k. Now take one root of the above equation and assume it as new value of k. Continue the same process with the new k. This sequence will go infinite times if we can show that in this process k can never repeat. We will show that this sequence is infinite later.

Now we can say that we got infinitely many equivalence classes if any polynomial in the sequence $H^{-i}(f_{-3})$ is not equivalent to the other polynomial except itself. For the sake of contradiction assume that in this sequence two different polynomials are equivalent that is $f_{k_1} \sim f_{k_2}$ for some $k_1 \neq k_2$. From the sequence construction we can say that

$f_{k_1} = H^{-i}(f_{-3})$ for some i and $f_{k_2} = H^{-j}(f_{-3})$ for some $j \neq i$. Now we know that from lemma 5.5 that

$$f \sim g \implies H(f) \sim H(g)$$

We know that $f_{k_1} \sim f_{k_2}$ so, applying Hessian i times on this we get that

$$f_{-3} \sim H^{-(j-i)}(f_{-3})$$

as we know that $j \neq i$, we can say that $H^{-(j-i)}(f_{-3}) \neq f_{-3}$. It shows that f_{-3} is equivalent to some polynomial f_k where $k \neq -3, -3\omega, -3\omega^2$, which is not possible. Hence two different polynomials in this sequence can never be equivalent to each other. So if we can show that the number of polynomials in the above sequence is infinite then our proof will be complete.

Claim : The number of polynomials in the sequence $H^{-i}(f_{-3})$ is infinite.

Proof. To prove this we have to show that the process of selecting a new value of k as new root of the polynomial $m^3 + 3km^2 + 108 = 0$ with $k = -3$ as initial value and continuing the same process repeatedly goes infinite times. In other words in the subsequent step we will always get a new value of k. For the first time we will get $m = -3$ and $m = 6$ as the roots of the equation. We are always going to take the new root which has highest absolute value. For the case when we take $k = 6$ then it has the following roots

$$m = -18.3217294552738, 0.160864727636919 - 2.42255290483452i \text{ and}$$

$$m = 0.160864727636919 + 2.42255290483452i$$

Now consider that in the i^{th} step the selected root was m_i and in the $(i+1)^{th}$ step the selected root will be m_{i+1}. Then our equation will be

$$m_{i+1}^3 + 3m_i m_{i+1}^2 + 108 = 0$$

divide both sides by m_{i+1}^2, we get

$$m_{i+1} + 3m_i + \frac{108}{m_{i+1}^2} = 0$$

which shows

$$m_{i+1} = -(3m_i + \frac{108}{m_{i+1}^2})$$

taking absolute value of both sides, we get

$$|m_{i+1}| = \left|3m_i + \frac{108}{m_{i+1}^2}\right|$$

by the triangular inequality, we can write

$$|m_{i+1}| \leq |3m_i| + \left|\frac{108}{m_{i+1}^2}\right|$$

rearranging the variables, we get

$$|m_{i+1}| - |3m_i| \leq \left|\frac{108}{m_{i+1}^2}\right|$$

Now if we can show that $\left|\frac{108}{m_{i+1}^2}\right| \leq 1$ then it shows that in the next iteration the absolute value of m_{i+1} gets nearly tripled of the previous value m_i, suggesting that it will be a geometric progression and hence every time the value of k will be different (nearly triple) of the previous value, hence this process will go infinite times and it will never repeat. We will show that $\left|\frac{108}{m_{i+1}^2}\right| \leq 1$ by induction.

Base Case : For the above equation we know that $m_2 = -18.3217294552738$, hence $\left|\frac{108}{m_{i+1}^2}\right| \leq 1$.

Induction Hypothesis : Let us assume that this is true for m_i for some i, that is we have $\left|\frac{108}{m_i^2}\right| \leq 1$.

Induction step : Here we have to show that $\left|\frac{108}{m_{i+1}^2}\right| \leq 1$. From the inductive hypothesis, we know that $\left|\frac{108}{m_i^2}\right| \leq 1 \implies |108| \leq |m_i^2| \implies 108 \leq m_i^2 \implies 6\sqrt{3} \leq |m_i|$. Since m_{i+1} is the new root of the above equation and m_i is the new k at that time so we can write

$$m_{i+1}^3 + 3m_i m_{i+1}^2 + 108 = 0$$

we can write it as

$$m_{i+1}^3 + 108 = -3m_i m_{i+1}^2$$

now take the absolute value of both sides, we get

$$|m_{i+1}^3 + 108| = |3m_i m_{i+1}^2|$$

as we know that $6\sqrt{3} \leq |m_i|$, we can write $|m_i| > 6$. Now putting this lower bound on $|m_i|$ in above equation, we get

$$|m_{i+1}^3 + 108| \geq 18|m_{i+1}^2| \implies |m_{i+1}^3| + 108 \geq 18|m_{i+1}^2|$$

after rearranging it, it will be

$$|m_{i+1}^3| - 18|m_{i+1}^2| + 108 \geq 0$$

Now solving the equation $x^3 - 18x^2 + 108 = 0$, we will get $x = -2.30620291582885$, 2.65275181001085 and $x = 17.6534511058180$ as roots. Since we are always going to select the root with the highest absolute value, we can write $|m_{i+1}| > 17.6534511058180 \implies m_{i+1}^2 > 289$, which shows that $\left|\frac{108}{m_{i+1}^2}\right| \leq 1$.
It proves our claim that after first two iterations $\left|\frac{108}{m_{i+1}^2}\right| \leq 1$ will always be true. □

The proof of the above claim combined with the previous argument completes our proof.

□

6.3 Conjecture for Equivalence of Symmetric Polynomials

In this section we will give a conjecture for the equivalence of two symmetric polynomials which we find very interesting. Before giving the conjecture, let us see some definitions.

Definition 6.5. Symmetric τ. An invertible linear transformation τ on n-variables is called symmetric τ, if for some σ which is not identity matrix, the following equation holds

$$\tau\sigma = \sigma\tau.$$

where σ is a $n \times n$ permutation matrix.

Conjecture-2 : If two symmetric polynomials are equivalent then some invertible linear transformation τ which makes them equivalent is a symmetric τ.

We will show some empirical results that support our conjecture-2. We checked this for only one polynomial but having different coefficients. The results showed that τ is a symmetric τ. These examples are as below:

1. In this example we took $f = x^3 + y^3 + z^3 + pxyz$ and $g = x^3 + y^3 + z^3 + (p+1)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following
$$\tau = \begin{bmatrix} a & a & a \\ b & a & c \\ a & b & c \end{bmatrix}$$
where $a = 0.5829297353 - 0.08326252149i$, $b = -0.2193574088 + 0.5464632201i$, $c = -0.3635723264 - 0.4632006986i$ and $p = 1.020917568 - 2.276163511i$.

2. In this example we took $f = x^3 + y^3 + z^3 + pxyz$ and $g = x^3 + y^3 + z^3 + p^2xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following
$$\tau = \begin{bmatrix} a & a & a \\ b & a & c \\ c & a & b \end{bmatrix}$$
where $a = 0.5983343398$, $b = -0.2991671699+0.5181727382i$, $c = -0.2991671699-0.5181727382i$ and $p = 1.668401649$.

3. In this example we took $f = x^3 + y^3 + z^3 + pxyz$ and $g = x^3 + y^3 + z^3 + p^3xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following
$$\tau = \begin{bmatrix} a & a & b \\ b & a & a \\ c & a & c \end{bmatrix}$$

where $a = -0.2725758219 - 0.5496877248i$, $b = -0.3397556229 + 0.5109014487i$, $c = 0.6123314448 + 0.03878627616i$ and $p = 1.251715417 - 0.8166856050i$.

4. In this example we took $f = x^3 + y^3 + z^3 + pxyz$ and $g = x^3 + y^3 + z^3 + 2pxyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following

$$\tau = \begin{bmatrix} a & b & c \\ a & a & a \\ b & a & c \end{bmatrix}$$

where $a = -0.3953181849 - 0.4811118065i$, $b = 0.6143141390 - 0.1017996875i$, $c = -0.2189959540 + 0.5829114940i$ and $p = 1.371885725 - 1.541660830i$.

5. In this example we took $f = x^3 + y^3 + z^3 + pxyz$ and $g = x^3 + y^3 + z^3 + (2p+1)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following

$$\tau = \begin{bmatrix} a & b & a \\ a & a & b \\ b & a & a \end{bmatrix}$$

where $a = -0.2119380822 + 0.5684669999i$, $b = 0.5982759042 - 0.1006897368i$ and $p = -2.324782643 - 0.2689156307i$.

6. In this example we took $f = x^3 + y^3 + z^3 + pxyz$ and $g = x^3 + y^3 + z^3 + (2p^2 + 1)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following

$$\tau = \begin{bmatrix} a & b & a \\ b & a & a \\ a & a & b \end{bmatrix}$$

where $a = -0.6460610796 + 0.5330737447i$, $b = 0.7846859448 + 0.2929684349i$ and $p = 2.387157159 - 1.145847805i$.

7. In this example we took $f = x^3 + y^3 + z^3 + pxyz$ and $g = x^3 + y^3 + z^3 + (3p^2 + 2p + 1)xyz$. Then we solved the equations empirically to get an approximate solution

and we found that τ is following

$$\tau = \begin{bmatrix} a & b & a \\ b & a & a \\ a & a & b \end{bmatrix}$$

where $a = -0.6801575740 + 0.6613462505i$, $b = 0.9128214406 + 0.2583606124i$ and $p = 1.850442576 - 1.480505963i$.

8. In this example we took $f = x^3 + y^3 + z^3 + pxyz$ and $g = x^3 + y^3 + z^3 + (3p-1)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following
$$\tau = \begin{bmatrix} a & b & c \\ a & a & a \\ b & a & c \end{bmatrix}$$
where $a = -0.4103859908 - 0.4953164343i$, $b = 0.6341496104 - 0.1077464762i$, $c = -0.2237636196 + 0.6030629105i$ and $p = 1.429743399 - 1.158646446i$.

9. In this example we took $f = x^3+y^3+z^3+pxyz$ and $g = x^3+y^3+z^3+(p^2+p+1)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following
$$\tau = \begin{bmatrix} a & b & a \\ b & a & a \\ a & a & b \end{bmatrix}$$
where $a = -0.6435429841 + 0.4671094610i$, $b = 0.7263001516 + 0.3237698422i$ and $p = 2.832755389 - 1.122000574i$.

10. In this example we took $f = x^3+y^3+z^3+pxyz$ and $g = x^3+y^3+z^3+(p^4+p^2+1)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following
$$\tau = \begin{bmatrix} a & b & c \\ a & a & a \\ a & c & b \end{bmatrix}$$

where $a = -0.3126476687 - 0.5415216471i$, $b = -0.3126476687 + 0.5415216471i$, $c = 0.6252953375 - 8.182889450 \times 10^{-27}i$ and $p = 1.090198913 + 5.777508253 \times 10^{-26}i$.

11. In this example we took $f = x^3 + y^3 + z^3 + p^2xyz$ and $g = x^3 + y^3 + z^3 + p^3xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following
$$\tau = \begin{bmatrix} a & b & c \\ a & a & a \\ b & a & c \end{bmatrix}$$
where $a = -0.4113335008 - 0.4553084554i$, $b = 0.5999754393 - 0.1285710334i$, $c = -0.1886419385 + 0.5838794888i$ and $p = 1.513595608 - 0.5630747230i$.

12. In this example we took $f = x^3+y^3+z^3+p^2xyz$ and $g = x^3+y^3+z^3+(p^2+p+1)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following
$$\tau = \begin{bmatrix} a & b & a \\ b & a & a \\ a & a & b \end{bmatrix}$$
where $a = -0.5621323331 + 0.3212435781i$, $b = 0.5592712660 + 0.3261990917i$ and $p = 2.179127333 - 0.1831624214i$.

13. In this example we took $f = x^3+y^3+z^3+p^2xyz$ and $g = x^3+y^3+z^3+(p^3+p-1)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following
$$\tau = \begin{bmatrix} a & b & c \\ a & a & a \\ b & a & c \end{bmatrix}$$
where $a = -0.4135061507 - 0.4655513224i$, $b = 0.6099323473 - 0.1253311699i$, $c = -0.1964261966 + 0.5908824923i$ and $p = 1.457509600 - 0.5245995318i$.

14. In this example we took $f = x^3+y^3+z^3+p^2xyz$ and $g = x^3+y^3+z^3+(p^4+1)xyz$. Then we solved the equations empirically to get an approximate solution and we

found that τ is following

$$\tau = \begin{bmatrix} a & b & c \\ a & a & a \\ b & a & c \end{bmatrix}$$

where $a = -0.4267408912 - 0.4820996550i$, $b = 0.6308809940 - 0.1285186251i$, $c = -0.2041401027 + 0.6106182801i$ and $p = 1.400554435 - 0.4059208050i$.

15. In this example we took $f = x^3 + y^3 + z^3 + p^2xyz$ and $g = x^3 + y^3 + z^3 + (p^5 + p^3 + 1)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following

$$\tau = \begin{bmatrix} a & b & b \\ c & b & c \\ b & b & a \end{bmatrix}$$

where $a = -0.2608772384 + 0.5682699563i$, $b = 0.6225748376 - 0.5820866245i$, $c = -0.3616975992 - .5100612939i$ and $p = 1.094313778 + 0.5158977149i$.

16. In this example we took $f = x^3 + y^3 + z^3 + p^2xyz$ and $g = x^3 + y^3 + z^3 + p^5xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following

$$\tau = \begin{bmatrix} a & b & a \\ b & a & a \\ a & a & b \end{bmatrix}$$

where $a = -0.6076495467 + 0.5010641997i$, $b = 0.7377590993 + 0.2757078442i$ and $p = 1.624053482 - 0.2624070611i$.

17. In this example we took $f = x^3 + y^3 + z^3 + p^2xyz$ and $g = x^3 + y^3 + z^3 + p^7xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following

$$\tau = \begin{bmatrix} a & a & b \\ c & b & b \\ b & c & b \end{bmatrix}$$

where $a = 0.6145287008 - 0.3320791859i$, $b = -0.2785054493 + 0.5488014255i$, $c = -0.3360232515 - 0.5155935069i$ and $p = 1.150809237 + 0.3005653693i$.

18. In this example we took $f = x^3+y^3+z^3+p^2xyz$ and $g = x^3+y^3+z^3+(p^7+p^5)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following

$$\tau = \begin{bmatrix} a & b & a \\ b & a & a \\ c & c & a \end{bmatrix}$$

where $a = -0.3424875647 + 0.5230847059i$, $b = 0.6242484260 + 0.03506057852i$, $c = -0.2817608613 - 0.5581452844i$ and $p = 1.066264732 - 0.3214068785i$.

19. In this example we took $f = x^3+y^3+z^3+p^2xyz$ and $g = x^3+y^3+z^3+(3p-7)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following

$$\tau = \begin{bmatrix} a & a & b \\ b & a & a \\ b & c & b \end{bmatrix}$$

where $a = 0.6283417711 + 0.07384605592i$, $b = -0.3781234460 + 0.5072369081i$, $c = -0.2502183252 - 0.5810829640i$ and $p = 1.084648155 + 0.5956425801i$.

20. In this example we took $f = x^3+y^3+z^3+p^2xyz$ and $g = x^3+y^3+z^3+(2p+1)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following

$$\tau = \begin{bmatrix} a & a & b \\ a & c & c \\ a & b & a \end{bmatrix}$$

where $a = -0.1310930454 + 0.5836840363i$, $b = -0.4399386805 - 0.4053719257i$, $c = 0.5710317259 - 0.1783121106i$ and $p = 1.333851228 + 1.380225863i$.

21. In this example we took $f = x^3 + y^3 + z^3 + p^3xyz$ and $g = x^3 + y^3 + z^3 + 2pxyz$. Then we solved the equations empirically to get an approximate solution and we

found that τ is following

$$\tau = \begin{bmatrix} a & b & a \\ b & a & a \\ a & a & b \end{bmatrix}$$

where $a = -0.4136445792 + 0.2739353820i$, $b = 0.4440572894 + 0.2212590227i$ and $p = 2.002789875 + 0.2274145768i$.

22. In this example we took $f = x^3 + y^3 + z^3 + p^3xyz$ and $g = x^3 + y^3 + z^3 + p^5xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following

$$\tau = \begin{bmatrix} a & b & c \\ a & a & a \\ b & a & c \end{bmatrix}$$

where $a = -0.4209815231 - 0.4616650740i$, $b = 0.6103044436 - 0.1337481566i$, $c = -0.1893229205 + 0.5954132305i$ and $p = 1.324840927 - 0.2836572704i$.

23. In this example we took $f = x^3 + y^3 + z^3 + p^3xyz$ and $g = x^3 + y^3 + z^3 + (p^3 + 3p + 1)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following

$$\tau = \begin{bmatrix} a & b & a \\ b & a & a \\ a & a & b \end{bmatrix}$$

where $a = -0.6149338933 + 0.3434946448i$, $b = 0.6049420351 + 0.3608010508i$ and $p = 1.609262866 - 0.1645579148i$.

24. In this example we took $f = x^3 + y^3 + z^3 + p^3xyz$ and $g = x^3 + y^3 + z^3 + (p^5 + p^3 + 1)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following

$$\tau = \begin{bmatrix} a & b & c \\ a & a & a \\ b & a & c \end{bmatrix}$$

where $a = -0.4093826479 - 0.5002235666i$, $b = 0.6378976402 - 0.1044239897i$, $c = -0.2285149923 + 0.6046475563i$ and $p = 1.175031524 - 0.2708772074i$.

25. In this example we took $f = x^3+y^3+z^3+p^3xyz$ and $g = x^3+y^3+z^3+(p^2-p+1)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following
$$\tau = \begin{bmatrix} a & b & c \\ a & a & a \\ b & a & c \end{bmatrix}$$
where $a = -0.3156691944 + 0.4320749097i$, $b = 0.5320224454 + 0.05734008666i$, $c = -0.2163532510 - 0.4894149964i$ and $p = 1.364654892 + 0.7572610557i$.

26. In this example we took $f = x^3+y^3+z^3+p^3xyz$ and $g = x^3+y^3+z^3+(3p+9)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following
$$\tau = \begin{bmatrix} a & b & c \\ c & c & c \\ b & a & c \end{bmatrix}$$
where $a = -0.3466841909 - 0.7142871162i$, $b = 0.7919328837 + 0.05690624172i$, $c = -0.4452486928 + 0.6573808745i$ and $p = 0.4007588239 + 0.9619495296i$.

27. In this example we took $f = x^3 + y^3 + z^3 + p^4xyz$ and $g = x^3 + y^3 + z^3 + pxyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following
$$\tau = \begin{bmatrix} a & b & a \\ c & c & a \\ b & a & a \end{bmatrix}$$
where $a = -0.2065888066 - 0.05812786917i$, $b = 0.1536346146 - 0.1498472200i$, $c = 0.05295419191 + 0.2079750892i$ and $p = 1.760192367 - 2.657453138i$.

28. In this example we took $f = x^3+y^3+z^3+p^4xyz$ and $g = x^3+y^3+z^3+(2p+5)xyz$. Then we solved the equations empirically to get an approximate solution and we

found that τ is following

$$\tau = \begin{bmatrix} a & a & a \\ b & a & c \\ b & c & a \end{bmatrix}$$

where $a = -0.2820741302 + 0.5974785849i$, $b = 0.6584686978 - 0.05445592992i$, $c = -0.3763945676 - 0.5430226550i$ and $p = -0.2248388191 - 0.9540677833i$.

29. In this example we took $f = x^3 + y^3 + z^3 + p^4xyz$ and $g = x^3 + y^3 + z^3 + (7p^2 - 5p + 3)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following

$$\tau = \begin{bmatrix} a & b & a \\ b & a & a \\ a & a & b \end{bmatrix}$$

where $a = -0.6198860337 + 0.3424921499i$, $b = 0.6065499193 + 0.3655909777i$ and $p = 1.429395200 - 0.1146188191i$.

30. In this example we took $f = x^3 + y^3 + z^3 + p^4xyz$ and $g = x^3 + y^3 + z^3 + (3p^3 - 2p^2 + p - 1)xyz$. Then we solved the equations empirically to get an approximate solution and we found that τ is following

$$\tau = \begin{bmatrix} a & b & a \\ b & a & a \\ a & a & b \end{bmatrix}$$

where $a = -0.5210713516 + 0.3007062010i$, $b = 0.5209548850 + 0.3009079272i$ and $p = 1.530351606 - 0.02121988271i$.

Chapter 7

Conclusions and Future Directions

7.1 Summary/Conclusion

In this thesis we have obtained the following results related to cubic forms equivalence problem.

- We observed that this problem is a special case of the polynomial decomposition problem. Since polynomial decomposition problem has deterministic polynomial time algorithm over a fixed finite field $\mathbb{F}$, cubic forms equivalence also has the deterministic polytime algorithm over a fixed finite field $\mathbb{F}$ with fixed number of variables.

- We approached bivariate cubic forms equivalence over the field of $\mathbb{C}$. There we gave a polynomial time algorithm to test the equivalence.

- Then we moved to trivariate cubic forms equivalence problem. There we gave an algorithm to test the equivalence in polynomial time if at least one of the polynomials is factorizable over $\mathbb{C}$.

- Then our focus shifted to irreducible trivariate cubic forms equivalence over $\mathbb{C}$. In this case we completely classified the irreducible trivariate trinomial cubic forms into four equivalence classes.

- Finally we moved to irreducible trivariate quadnomial cubic forms equivalence over $\mathbb{C}$. There we showed that it has infinitely many equivalence classes.

7.2 Future Directions

Based on our work, we propose the following directions of work to pursue in order to get efficient algorithms for testing equivalence of two cubic forms:

- Give a general algorithm for testing cubic forms equivalence over $\mathbb{C}$. Then generalising it over all the fields.

- Finding out what are the invariants of cubic forms under equivalence.

- This problem is not even known to be computable on $\mathbb{Q}$. Decide the computability of cubic forms equivalence over $\mathbb{Q}$.

- Proving/disproving conjecture-1 in general over all fields.

- Graph Isomorphism can be solved in quasi-polynomial time. Can cubic forms equivalence problem also be solvable in quasi-polynomial time ?

- Proving/disproving the conjecture-2 in general over all the fields.

Bibliography

[AS06] Manindra Agrawal and Nitin Saxena. Equivalence of $\mathbb{F}$-Algebras and Cubic Forms. In *STACS*, pages 115–126, 2006.

[Bab15] László Babai. Graph Isomorphism in Quasipolynomial Time. *CoRR*, abs/1512.03547, 2015.

[BB15] Arnab Bhattacharyya and Abhishek Bhowmick. Using higher-order Fourier analysis over general fields. *Electronic Colloquium on Computational Complexity (ECCC)*, 22:77, 2015.

[Bha14] Arnab Bhattacharyya. Polynomial Decompositions in Polynomial Time. In *Algorithms - ESA 2014 - 22th Annual European Symposium, Wroclaw, Poland, September 8-10, 2014. Proceedings*, pages 125–136, 2014.

[BHT15] Arnab Bhattacharyya, Pooya Hatami, and Madhur Tulsiani. Algorithmic regularity for polynomials and applications. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2015, San Diego, CA, USA, January 4-6, 2015*, pages 1870–1889, 2015.

[BPR06] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry (Algorithms and Computation in Mathematics)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[Bro87] W. D. Brownawell. Bounds for the degrees in the Nullstellensatz. *Annals of Maths*, 126:577–591, 1987.

[BS84] L. Babai and E. Szemerédi. On the complexity of matrix group problems. In *25th Annual IEEE Symposium on Foundations of Computer Science*, pages 229–240, 1984.

[CF12] Stephen A. Cook and Lila Fontes. Formal Theories for Linear Algebra. *Logical Methods in Computer Science*, 8(1), 2012.

[DACO07] John Little David A. Cox and Donal O'Shea. Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer-Verlag New York, Inc., Secaucus, NJ, USA. 2007.

[Har75] D. K. Harrison. A Grothendieck ring of higher degree forms. *Journal of Algebra*, 35:123–128, 1975.

[HP88] D. K. Harrison and B. Pareigis. Witt rings of higher degree forms. *Communications in Algebra*, 16(6):1275–1313, 1988.

[Kay11] Neeraj Kayal. Efficient algorithms for some special cases of the polynomial equivalence problem. In *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2011, San Francisco, California, USA, January 23-25, 2011*, pages 1409–1421, 2011.

[Koi96] Pascal Koiran. Hilbert's Nullstellensatz is in the Polynomial Hierarchy. *Journal of Complexity*, 12:273–286, 1996.

[Man86] Y. I. Manin. Cubic forms. *Algebra, geometry, arithmetic. North-Holland, New York*, (Translated from Russian)1986.

[Rup03] C. Rupprecht. Cohomological invariants for higher degree forms. PhD Thesis, Universität Regensburg. 2003.