ON THE COMPLEXITY OF CUBIC FORMS

Manindra Agrawal and Nitin Saxena

Abstract. We study the equivalence problem of cubic forms. We lower bound its complexity by that of $\mathbb{F}$-algebra isomorphism problem and hence by the graph isomorphism problem (for all fields $\mathbb{F}$). For finite fields we upper bound the complexity of cubic forms by NP $\cap$ coAM. We also study the cubic forms obtained from $\mathbb{F}$-algebras and show that they are regular and indecomposable.

Keywords. cubic forms, algebras, graphs, isomorphism, equivalence, complexity.

Subject classification. Computer Science, Algebra.

1. Introduction

Suppose we are given two polynomials $f(x_1,\ldots,x_n)$ and $g(x_1,\ldots,x_n)$ of total degree d with coefficients in a field $\mathbb{F}$. We say that f is *equivalent* to g, denoted by $f \sim g$, if there is an invertible linear transformation τ sending each x_i to a linear combination of $x_1,\ldots,x_n$ such that:

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

The polynomials f, g are assumed to be provided in the input in *expanded* form:

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

Example 1.1. Suppose $f(x,y) = x^2+y^2$ and $g(x,y) = 2x^2+2y^2$ 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, i.e., $\tau \circ f(x,y) = g(x,y)$. Thus, $f \sim g$ over rationals. $\Diamond$

Example 1.2. Consider $f(x) = x^2$ and $g(x) = 2x^2$. Then f and g are not equivalent over $\mathbb{Q}$ but they are equivalent over $\mathbb{R}$ as $\tau : x \mapsto \sqrt{2}x$ is an equivalence. $\Diamond$

The computational problem of *polynomial equivalence* is to check whether two input polynomials $f, g \in \mathbb{F}[\overline{x}]$ are equivalent, in time polynomial in the size of the input. We treat the degree d as a constant while the number of variables n varies. We show in this paper that this easily defined problem is apparently harder than commutative $\mathbb{F}$-algebra isomorphism ($\mathbb{F}$-algebras given in the basis form) and hence (by Lemma 6.13) as a corollary the graph isomorphism problem too reduces to polynomial equivalence. Also, in the other direction most cases of polynomial equivalence reduce to the commutative $\mathbb{F}$-algebra isomorphism problem.

Previous research on polynomial equivalence has primarily focussed on a restricted case – when f, g are homogeneous polynomials called *forms*. The most celebrated case is perhaps when f, g are *quadratic forms* – homogeneous polynomials of degree 2. The classification of quadratic forms is known due to the works of Minkowski (1885), Hasse (1921) and Witt (Witt & Kersten 1998). The classification theorem of quadratic forms is effective in the sense that it gives algorithms for deciding and finding quadratic forms equivalence over "interesting" fields like finite fields, $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$.

In this work we focus on polynomial equivalence for homogeneous polynomials of degree 3 – *cubic forms*. This case of polynomial equivalence seems to be significantly harder than quadratic forms equivalence as we show that a fairly general case of ring isomorphism – commutative $\mathbb{F}$-algebra isomorphism – reduces to cubic forms equivalence. This reduction (together with Lemma 6.13) implies that graph isomorphism reduces to cubic forms equivalence too. Moreover, we also give evidence that the problem of equivalence for higher degree forms reduces to that of cubic forms. Thus, cubic forms seem to be the most important restricted case of polynomial equivalence. Cubic forms equivalence has been well studied in mathematics (for instance see Harrison 1975; Harrison & Pareigis 1988; Manin 1986; Rupprecht 2003). Over the last ten years, it has been found to be useful in computer science as well: Courtois *et al.* (1998); Patarin (1996) propose a cryptosystem based on the hardness of the cubic forms equivalence over finite fields. Graph isomorphism is ofcourse a well studied open problem in computer science, see Köbler *et al.* (1993). Thus, this fundamental connection of isomorphism problems with cubic forms we find interesting and intriguing.

In Section 2 we prove upper and lower bounds for the polynomial equivalence problem over various fields. In Section 3 we lower bound the cubic forms case of polynomial equivalence by algebra isomorphism. In Section 4 we present some known results about quadratic and cubic forms equivalence. Finally, in Section 5 we study properties of the cubic forms we get out of algebras. Some of the standard results about rings useful to us have been collected in the Appendix.

Preliminary versions of this paper were presented in Agrawal & Saxena (2005, 2006).

2. The Complexity of Polynomial Equivalence

For a given field $\mathbb{F}$ and degree d let us define the language for the problem of polynomial equivalence over $\mathbb{F}$ as:

$$\text{polyEquiv}_{d,\mathbb{F}} := \{(f,g) \mid f,g \text{ are polynomials of total degree } d \text{ over } \mathbb{F} \text{ and } f \sim g\}$$

2.1. Upper Bounds. The complexity of polynomial equivalence depends upon the base field. In this section we give upper bounds on polynomial equivalence for various “interesting” fields.

Theorem 2.1. *For any fixed $d \in \mathbb{Z}^{>0}$, the problem of polynomial equivalence satisfies:*

1) *For a finite field $\mathbb{F}$, polyEquiv$_{d,\mathbb{F}} \in$ NP $\cap$ coAM.*

2) *When $\mathbb{F} = \mathbb{R}$, polyEquiv$_{d,\mathbb{F}} \in$ EEXP.*

3) *For an algebraically closed field $\mathbb{F}$ (eg. $\mathbb{C}$), polyEquiv$_{d,\mathbb{F}} \in$ PSPACE.*

Proof (1). Let $\mathbb{F}$ be a finite field of size q. Given a linear transformation τ on the variables $x_1,\ldots,x_n$, it is easy to check whether $f(\tau x_1,\ldots,\tau x_n) = g(x_1,\ldots,x_n)$ simply by substituting for τ in f and doing the computations in time $poly(n^d, \log q)$. Thus, polynomial equivalence over $\mathbb{F}$ is in NP.

Let us now see an AM protocol for $\overline{\text{polyEquiv}_{\mathbb{F}}}$. Suppose $f,g \in \mathbb{F}[x_1,\ldots,x_n]$ are two given polynomials. We call an invertible linear transformation $\phi \in (\mathbb{F}^{n\times n})^*$ an *automorphism of f* if $f(\phi\overline{x}) = f(\overline{x})$. Let us define a set $C(f)$ as:

$$C(f) := \left\{(f(\tau\overline{x}),\phi) \mid \tau,\phi \in \left(\mathbb{F}^{n\times n}\right)^* \text{ and } \phi \text{ is an automorphism of } f(\tau\overline{x})\right\}$$

If s is the number of invertible $n \times n$ matrices over $\mathbb{F}$ then observe that the size of the set $C(f)$ is:

$$\begin{aligned}\#C(f) &= (\text{number of polynomials } \sim f(\overline{x})) \cdot \#Aut(f) \\ &= \frac{s}{\#Aut(f)} \cdot \#Aut(f) \\ &= s\end{aligned}$$

Similarly, we have the set $C(g)$ and we define $C(f,g) = C(f) \cup C(g)$. It is a simple exercise to show that given $\mathbb{F}_q$ and n we can compute the number s of $n \times n$ invertible matrices over $\mathbb{F}_q$ in polynomial time. Now let us see how $\#C(f,g)$ behaves:

$$\begin{aligned}f \not\sim g &\Rightarrow C(f) \cap C(g) = \emptyset \Rightarrow \#C(f,g) = 2s. \\ f \sim g &\Rightarrow C(f) = C(g) \Rightarrow \#C(f,g) = s.\end{aligned}$$

Thus, the set $C(f,g)$ is larger by a factor of 2 when $f \not\sim g$. Also, membership in $C(f,g)$ can be clearly decided in polynomial time. Both these properties of $C(f,g)$ together give us a standard AM protocol (Babai & Szemerédi 1984) to decide whether $f \not\sim g$ and hence, $\overline{polyEquiv_{d,\mathbb{F}}}$ is in AM. □

PROOF (2). When $\mathbb{F} = \mathbb{R}$, we consider the equivalence as a matrix A over $\mathbb{R}$ in n^2 unknowns $((a_{i,j}))$ and then solve the system of equations that we get from:

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

This system of equations can be solved in EEXP due to the result of Tarski on the decidability of first-order equations over reals (Davenport & Heintz 1988). □

PROOF (3). When $\mathbb{F}$ is an algebraically closed field, we consider the equivalence as a matrix A over $\mathbb{F}$ in n^2 unknowns $((a_{i,j}))$ and then solve the system of equations that we get from:

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

This system of equations can be solved over $\mathbb{F}$ in PSPACE by using Hilbert's Nullstellensatz (Brownawell 1987). □

REMARK 2.2. *When $\mathbb{F} = \mathbb{Q}$, it is not yet known if the problem is decidable.*

2.2. Reduction to $\mathbb{F}$-algebra Isomorphism (in some cases). At the first glance, the problem of polynomial equivalence does not appear to be related to the problems of ring isomorphism. But in this section we exhibit a connection of polynomial equivalence to the ring isomorphism problem. We show that the problem of polynomial equivalence restricted to homogeneous polynomials reduces to the ring isomorphism problem for most cases.

THEOREM 2.3. *Suppose $\mathbb{F}$ is a field having d^{th} roots, i.e. $\forall \alpha \in \mathbb{F}$, $\alpha^{\frac{1}{d}} \in \mathbb{F}$. Then equivalence of homogeneous polynomials of degree d over $\mathbb{F}$ is many-one polynomial time reducible to $\mathbb{F}$-algebra isomorphism.*

PROOF. Suppose f, g are homogeneous polynomials of degree d in n variables over $\mathbb{F}$. Then construct a commutative $\mathbb{F}$-algebra R_f from f as:

$$R_f := \mathbb{F}[x_1, \ldots, x_n] / (f, \mathcal{I}_{d+1})$$

where, the ideal $\mathcal{I}_{d+1}$ is generated by all the monomials of degree $d+1$. We claim that the rings R_f and R_g are isomorphic iff $f \sim g$.

Suppose ψ is an equivalence that sends f to g. Then ψ easily extends to an isomorphism from R_f to R_g.

Conversely, suppose ϕ is an isomorphism from $R_f \to R_g$. Then $\phi(f)$ has to map to 0 in R_g thus, there is a $c \in \mathbb{F}$ such that:

$$\phi(f) = cg(\overline{x}) + (\text{terms of degree } d+1 \text{ or more}) \tag{2.4}$$

Since, $x_i^{d+1} = 0$ in R_f, $\phi(x_i)$ cannot have a constant term otherwise $\phi(x_i)^{d+1} \neq 0$. Let us denote the linear part of $\phi(x_i)$ by $\psi(x_i)$. Hence, for all $i \in [n]$:

$$\phi(x_i) = \psi(x_i) + (\text{quadratic and higher degree terms})$$

Since, f is homogeneous of degree d, the degree d terms of $\phi(f)$ are exactly those in $\psi(f)$. Thus:

$$\phi(f) = \psi(f) + (\text{terms of degree } d+1 \text{ or more}) \tag{2.5}$$

The Equations (2.4) and (2.5) imply that $\psi(f) = cg$. Now since $\mathbb{F}$ has d^{th} roots and g is homogeneous of degree d we further get:

$$f(\psi(x_1), \ldots, \psi(x_n)) = g(c^{\frac{1}{d}} x_1, \ldots, c^{\frac{1}{d}} x_n)$$

Thus, $f \sim g$.

Hence, $R_f \cong R_g$ iff $f \sim g$. □

Remark 2.6. *If one slightly generalizes the definition of polynomial equivalence as $f \sim g$ iff there is a $\tau \in \mathbb{F}^{n\times n}$ and a $c \in \mathbb{F}$ such that $f(\tau(\overline{x})) = c \cdot g(\overline{x})$ then this theorem works for all fields $\mathbb{F}$.*

2.3. A Lower Bound: Reduction from $\mathbb{F}$-algebra Isomorphism. Here, we will show that a fairly general case of the ring isomorphism problem – commutative $\mathbb{F}$-algebra isomorphism – reduces to the equivalence problem of polynomials having total degree 3 (called cubic polynomials).

An isomorphism of $\mathbb{F}$-algebras has to preserve all the multiplicative relations, which are $\sim n^2$ if there are n basis elements. On the other hand an equivalence of polynomials has to satisfy only one equation. It is interesting that there is a way to combine the various multiplicative relations of a commutative $\mathbb{F}$-algebra into one polynomial such that its equivalence gives an $\mathbb{F}$-algebra isomorphism.

Theorem 2.7. *Commutative $\mathbb{F}$-algebra Isomorphism $\leq_m^P$ cubic polynomial equivalence.*

Proof. Let R be a commutative $\mathbb{F}$-algebra with additive basis $b_1, \ldots, b_n$ over $\mathbb{F}$. Furthermore, multiplication in R is defined as: for all $1 \leq i \leq j \leq n$,

$$b_i \cdot b_j = \sum_{k=1}^{n} a_{i,j,k} b_k, \quad \text{where, } a_{i,j,k} \in \mathbb{F}$$

Let us define a polynomial that *captures* the multiplicative relations defining ring R:

$$f_R(\overline{z}, \overline{b}) := \sum_{1\leq i\leq j\leq n} z_{i,j} \left(b_i b_j - \sum_{1\leq k\leq n} a_{i,j,k} b_k \right) \tag{2.8}$$

Note that here $\overline{z} = (z_{1,1}, \ldots, z_{n,n})$ and $\overline{b} = (b_1, \ldots, b_n)$ are formal variables and f_R is a polynomial in $\mathbb{F}[\overline{z}, \overline{b}]$. Similarly, for another commutative $\mathbb{F}$-algebra R' the polynomial would be:

$$f_{R'}(\overline{z}, \overline{b}) := \sum_{1\leq i\leq j\leq n} z_{i,j} \left(b_i b_j - \sum_{1\leq k\leq n} a'_{i,j,k} b_k \right)$$

An isomorphism from R to R' easily gives an equivalence from f_R to $f_{R'}$:

Claim 2.9. *If $R \cong R'$ then $f_R \sim f_{R'}$.*

Proof of Claim 2.9. Let ϕ be an isomorphism from R to R'. Note that ϕ sends each b_i to a linear combination of b's and for all $i \leq j \in [n]$: $\phi(b_i)\phi(b_j) - \sum_{1 \leq k \leq n} a_{i,j,k}\phi(b_k) = 0$ in R'. This implies that there exist constants $c_{i,j,k,\ell} \in \mathbb{F}$ such that:

$$\phi(b_i)\phi(b_j) - \sum_{1 \leq s \leq n} a_{i,j,s}\phi(b_s) = \sum_{1 \leq k \leq \ell \leq n} c_{i,j,k,\ell} \left(b_k b_\ell - \sum_{1 \leq s \leq n} a'_{k,\ell,s} b_s \right)$$

This immediately suggests that the linear transformation τ that sends:

$$\begin{array}{lr} \text{for all } 1 \leq i \leq n, & b_i \mapsto \phi(b_i) \\ \text{for all } 1 \leq k \leq \ell \leq n, & \left(\sum_{1 \leq i \leq j \leq n} c_{i,j,k,\ell} z_{i,j} \right) \mapsto z_{k,\ell} \end{array}$$

makes f_R equal to $f_{R'}$. The linear transformation τ is an invertible map because $\tau \mid_{\overline{b}} = \phi$ is invertible and $\tau \mid_{\overline{z}}$ has a range space of full dimension implying that $\tau \mid_{\overline{z}}$ is invertible too. □

The converse, i.e., getting an $\mathbb{F}$-algebra isomorphism from a polynomial equivalence, is more involved to show.

Claim 2.10. *If $f_R \sim f_{R'}$ then $R \cong R'$.*

Proof of Claim 2.10. Let ϕ be a linear transformation such that

(2.11)
$$\sum_{1 \leq i \leq j \leq n} \phi(z_{i,j}) \left(\phi(b_i)\phi(b_j) - \sum_{1 \leq k \leq n} a_{i,j,k}\phi(b_k) \right) = \sum_{1 \leq i \leq j \leq n} z_{i,j} \left(b_i b_j - \sum_{1 \leq k \leq n} a'_{i,j,k} b_k \right)$$

By comparing the cubic terms on both sides we get:

$$\sum_{1 \leq i \leq j \leq n} \phi(z_{i,j})\phi(b_i)\phi(b_j) = \sum_{1 \leq i \leq j \leq n} z_{i,j} b_i b_j \tag{2.12}$$

We aim to show that $\phi(b_i)$ has no z's, *i.e.*, $\phi(b_i)$ is a linear combination of only b's. We will be relying on the following property of the RHS of Equation (2.12): if τ is an invertible linear transformation on the z's then for all $1 \leq i \leq j \leq n$, the coefficient of $z_{i,j}$ in $\sum_{1 \leq i \leq j \leq n} \tau(z_{i,j}) b_i b_j$ is nonzero.

Suppose $\phi(b_{i_0})$ has z's, i.e.,

$$\phi(b_{i_0}) = \sum_j c_{i_0,j} b_j + \sum_{j,k} c_{i_0,j,k} z_{j,k}$$

We can apply an invertible linear transformation τ on z*'s* in Equation (2.12) such that τ maps $\sum_{j,k} c_{i_0,j,k} z_{j,k}$ to $z_{1,1}$. Then apply an evaluation map *val* that substitutes $z_{1,1}$ by $\left(-\sum_j c_{i_0,j} b_j\right)$. Now $val \circ \tau \circ \phi(b_{i_0}) = 0$ and thus, Equation (2.12) becomes:

$$(2.13) \quad \sum_{\substack{1\le j\le k\le n\\ j,k\ne i_0}} val \circ \tau \circ \phi(z_{j,k} b_j b_k) \;=\; \sum_{\substack{1\le j\le k\le n\\ (j,k)\ne(1,1)}} z_{j,k}(\text{quadratic } b\text{'s}) + (\text{cubic } b\text{'s})$$

Notice that the LHS of Equation (2.12) had $\binom{n+1}{2}$ summands while the LHS of Equation (2.13) has at most $\left\{\binom{n+1}{2} - n\right\}$ summands. These summands on the LHS of Equation (2.13) are of two kinds: those that have a nonzero occurrence of a z-variable and those that are cubic in b's. So we repeat this process of applying invertible linear transformations on z*'s* and fixing z*'s* in Equation (2.13) so that for all $1 \le j \le k \le n,\ j,k \ne i_0,\ val \circ \tau \circ \phi(z_{j,k} b_j b_k)$ either maps to zero or to a cubic in b*'s*. Thus, after $\left\{1 + \binom{n+1}{2} - n\right\}$ z-fixings the LHS of Equation (2.12) is a cubic in b*'s* while the RHS still has $\binom{n+1}{2} - \left\{1 + \binom{n+1}{2} - n\right\} = (n-1)$ unfixed z*'s*, which is a contradiction.

Since $\phi(b_i)$'s have no z*'s* and there are no cubic b*'s* in the RHS of Equation (2.11) we can ignore the b*'s* in $\phi(z_{j,k})$*'s*. Thus, now $\phi(z_{j,k})$*'s* are linear combinations of z*'s* and $\phi(b_i)$*'s* are linear combinations of b*'s*. Again looking at Equation (2.11), this means that $\left(\phi(b_i)\phi(b_j) - \sum_{1\le s\le n} a_{i,j,s}\phi(b_s)\right)$ is a linear combination of $\left(b_k b_\ell - \sum_{1\le s\le n} a'_{k,\ell,s} b_s\right)$ for $1 \le k \le \ell \le n$; implying that $\left(\phi(b_i)\phi(b_j) - \sum_{1\le s\le n} a_{i,j,s}\phi(b_s)\right) = 0$ in ring R'. This combined with the fact that $\phi|_{\bar b}$ is an invertible linear transformation on $\bar b$ means that ϕ induces an isomorphism from ring R to R'. □

The above two claims complete the proof. □

3. Another Lower Bound: 𝔽-algebra Isomorphism reduces to Cubic Forms Equivalence

We had seen in Theorem 2.7 how to construct non homogeneous cubic polynomials that capture the multiplicative relations of a given 𝔽-algebra. Now what happens if we homogenize those cubic polynomials, does an equivalence between such cubic forms give us isomorphism between the original $\mathbb{F}$-algebras?

In this section we first give a reduction from commutative $\mathbb{F}$-algebra isomorphism to local commutative $\mathbb{F}$-algebra isomorphism. Then from these local commutative $\mathbb{F}$-algebras we construct cubic forms (obtained by homogenizing Equation (2.8)) and prove that an equivalence between these cubic forms induces an isomorphism between the local commutative $\mathbb{F}$-algebras. Thus, cubic forms equivalence problem is at least as hard as the isomorphism problem of commutative $\mathbb{F}$-algebras. Consequently, for any field $\mathbb{F}$, cubic forms equivalence problem is at least as hard as the graph isomorphism problem (by Lemma 6.13).

3.1. Commutative $\mathbb{F}$-algebras reduce to local $\mathbb{F}$-algebras.

An $\mathbb{F}$-algebra is *local* if it cannot be broken into simpler $\mathbb{F}$-algebras, *i.e.*, if it cannot be written as a direct product of algebras. Given a commutative $\mathbb{F}$-algebra this direct product decomposition can be done by factoring polynomials over the field $\mathbb{F}$. Any non-unit r in a finite dimensional local commutative $\mathbb{F}$-algebra is *nilpotent*, i.e., there is an m such that $r^m = 0$. For more details on local rings refer the appendix or the text by McDonald (1974).

In this section we give a many-to-one reduction from commutative $\mathbb{F}$-algebra isomorphism to local commutative $\mathbb{F}$-algebra isomorphism. Moreover, the local commutative $\mathbb{F}$-algebras that we construct have basis elements most of whose products vanish. We exploit the properties of this local $\mathbb{F}$-algebra to give a reduction from commutative $\mathbb{F}$-algebra to cubic forms in the next subsection.

THEOREM 3.1. *Commutative $\mathbb{F}$-algebra isomorphism $\leq_m^P$ Local $\mathbb{F}$-algebra isomorphism.*

PROOF. Given two $\mathbb{F}$-algebras R and S, Theorem 2.7 constructs two cubic polynomials p and q respectively such that p, q are equivalent iff R, S are isomorphic. These polynomials live in $\mathbb{F}[z_{1,1}, \ldots, z_{n,n}, b_1, \ldots, b_n]$ and look like:

$$p(\overline{z}, \overline{b}) := \sum_{1 \leq i \leq j \leq n} z_{i,j} \left(b_i b_j - \sum_k a_{i,j,k} b_k \right)$$

$$q(\overline{z}, \overline{b}) := \sum_{1 \leq i \leq j \leq n} z_{i,j} \left(b_i b_j - \sum_k a'_{i,j,k} b_k \right)$$

Let

$$p_3(\overline{z}, \overline{b}) := \sum_{1 \leq i \leq j \leq n} z_{i,j} b_i b_j \quad \text{and} \quad p_2(\overline{z}, \overline{b}) := - \sum_{1 \leq i \leq j \leq n} \left(z_{i,j} \sum_k a_{i,j,k} b_k \right) \tag{3.2}$$

Similarly define $q_3(\overline{z}, \overline{b})$ and $q_2(\overline{z}, \overline{b})$ from q. Thus, $p = p_3 + p_2$ and $q = q_3 + q_2$, where p_3, q_3 are homogeneous of degree 3 and p_2, q_2 are homogeneous of degree 2.

Using p, q we construct the following commutative $\mathbb{F}$-algebras:

$$\begin{aligned} R' &:= \mathbb{F}[\overline{z}, \overline{b}, u] / \left\langle p_3, up_2, u^2, \mathcal{I} \right\rangle \\ S' &:= \mathbb{F}[\overline{z}, \overline{b}, u] / \left\langle q_3, uq_2, u^2, \mathcal{I} \right\rangle \end{aligned} \tag{3.3}$$

where, $\mathcal{I}$ is the ideal generated by all possible products of 4 variables (with repetition) from the set:

$$\{z_{1,1}, \ldots, z_{1,n}, \ldots, z_{n,1}, \ldots, z_{n,n}, b_1, \ldots, b_n, u\}$$

Note that all the variables in R', S' are nilpotent and hence the two rings are *local* commutative $\mathbb{F}$-algebras (see the appendix). The following claim tells us that it is enough to consider the isomorphism problem for these local structures. Recall that $R \cong S$ iff p, q are equivalent polynomials.

Claim 3.4. *$p(\overline{z}, \overline{b}), q(\overline{z}, \overline{b})$ are equivalent polynomials iff $R' \cong S'$.*

Proof of Claim 3.4. If p, q are equivalent then the same equivalence, extended by sending $u \mapsto u$, gives an isomorphism from R' to S'.

Conversely, say ϕ is an isomorphism from R' to S'. Our intention is to show that the *linear part* of ϕ, i.e., ignoring the quadratic or higher degree terms in $\phi(v)$, where variable $v \in \{z_{1,1}, \ldots, z_{n,n}, b_1, \ldots, b_n, u\}$, induces an equivalence from p to q. Note that since $\overline{z}, \overline{b}, u$ are nilpotents in R', therefore $\forall i \leq j \in [n], k \in [n]$, $\phi(z_{i,j}), \phi(b_k), \phi(u)$ can have no constant term.

Let us see where ϕ sends u. Since, $\phi(u)^2 = 0$ in S', while for all i, j: $z_{i,j}^2$ and b_i^2 are nonzero in S', thus, we deduce that the linear part of $\phi(u)$ can have no $\overline{z}$, $\overline{b}$'s. Further, as ϕ is an isomorphism $\phi(u)$ should have at least one linear term. Thus,

$$\phi(u) \; = \; c \cdot u + \text{(terms of degree 2 or more)}, \text{ where } c \in \mathbb{F}^*. \tag{3.5}$$

Now by the definition of ϕ there are $c_1, c_2 \in \mathbb{F}$ such that:

$$\phi(p_3) \; = \; c_1 \cdot q_3 + c_2 \cdot uq_2 + (\text{linear terms in } \overline{z}, \overline{b}, u) \cdot u^2 + (\text{terms of degree 4 or more})$$

By substituting $u = 0$ we get,

$$\phi(p_3) \mid_{u=0} \; = \; c_1 q_3 + \text{(terms of degree 4 or more)} \tag{3.6}$$

Also, there are $d_1, d_2 \in \mathbb{F}$ such that:

$$\phi(up_2) \;=\; d_1 \cdot q_3 + d_2 \cdot uq_2 + (\text{linear terms in } \overline{z}, \overline{b}, u) \cdot u^2 + (\text{terms of degree 4 or more})$$

Using Equation (3.5) we deduce that $d_1 = 0$. Thus,

$$\phi(up_2) \;=\; d_2 \cdot uq_2 + (\text{linear terms in } \overline{z}, \overline{b}, u) \cdot u^2 + (\text{terms of degree 4 or more})$$

As $c \neq 0$ in Equation (3.5), we deduce that there is a $d_2' \in \mathbb{F}$:

$$u\phi(p_2) \;=\; d_2' \cdot uq_2 + (\text{linear terms in } \overline{z}, \overline{b}, u) \cdot u^2 + (\text{terms of degree 4 or more})$$

Factoring out u and substituting $u = 0$ gives us:

$$\phi(p_2) \mid_{u=0} \;=\; d_2' \cdot q_2 + (\text{terms of degree 3 or more}) \tag{3.7}$$

Let ψ be the linear part of $\phi \mid_{u=0}$, that is:

$$\begin{aligned} \text{for all } i \leq j,\ \psi(z_{i,j}) \;&:=\; \text{linear terms of } \phi(z_{i,j}) \text{ other than } u, \text{ and} \\ \text{for all } i,\ \psi(b_i) \;&:=\; \text{linear terms of } \phi(b_i) \text{ other than } u \end{aligned}$$

By comparing degree 3 and degree 2 terms on both sides of Equations (3.6) and (3.7) respectively, we get:

$$\psi(p_3) \;=\; c_1 q_3 \tag{3.8}$$

$$\psi(p_2) \;=\; d_2' q_2 \tag{3.9}$$

Note that since ϕ is an isomorphism, ψ has to be an invertible map and thus, $\psi(p_3), \psi(p_2) \neq 0$. As a result c_1 and d_2' are both non-zero. Consider the map $\psi' := (\frac{d_2'}{c_1}) \circ \psi$. The above two equations give us: $\psi'(p_3 + p_2) = \frac{d_2'^3}{c_1^2} \cdot (q_3 + q_2)$. Denote $\frac{d_2'^3}{c_1^2}$ by c. Thus,

$$\psi'(p(\overline{z}, \overline{b})) = c \cdot q(\overline{z}, \overline{b})$$

Now we can get rid of the extra factor of c by defining a map ψ'':

$$\begin{aligned} \forall i, j,\ \psi''(z_{i,j}) \;&:=\; \frac{1}{c}\psi'(z_{i,j}) \\ \forall i,\ \psi''(b_i) \;&:=\; \psi'(b_i) \end{aligned}$$

It follows that $\psi''(p) = \frac{1}{c}\psi'(p) = q$ and thus, $p(\overline{z}, \overline{b})$, $q(\overline{z}, \overline{b})$ are equivalent under the map ψ''. □

Thus, $R \cong S$ iff $R' \cong S'$ and hence it is sufficient to study $\mathbb{F}$-algebra isomorphism over local commutative $\mathbb{F}$-algebras of the form occurring in Equation (3.3). □

3.2. Local commutative $\mathbb{F}$-algebras reduce to Cubic Forms. Here, we show that local commutative $\mathbb{F}$-algebra isomorphism reduces to cubic forms equivalence. This result when combined with the last subsection shows that cubic forms equivalence is at least as hard as the commutative algebra isomorphism and graph isomorphism.

We construct cubic forms from the rings of Equation (3.3) and then heavily use the properties of the underlying local commutative $\mathbb{F}$-algebra to study the equivalences of these cubic forms. The reduction that we exhibit in the following theorem holds for *any* field $\mathbb{F}$.

THEOREM 3.10. *Commutative $\mathbb{F}$-algebra isomorphism $\leq_m^P$ $\mathbb{F}$-cubic forms equivalence.*

PROOF. Given commutative $\mathbb{F}$-algebras R, S we will construct cubic forms ϕ_R, ϕ_S such that the cubic forms are equivalent iff the algebras are isomorphic. The construction involves first getting the local $\mathbb{F}$-algebras R', S' (as in Theorem 3.1) and then the cubic forms out of these local commutative algebras.

Let $b_1, \ldots, b_n$ be the additive basis of R over $\mathbb{F}$. Let the multiplication in the algebra be defined as:

$$\text{for all } i, j \in [n] : \ b_i \cdot b_j = \sum_{k=1}^{n} a_{i,j,k} b_k, \text{ where } a_{i,j,k} \in \mathbb{F}$$

Consider the following local ring R' constructed from R:

$$R' := \mathbb{F}[\overline{z}, \overline{b}, u] / \langle p_3, up_2, u^2, \mathcal{I} \rangle \tag{3.11}$$

where, $p_3(\overline{z}, \overline{b}) := \sum_{1 \leq i \leq j \leq n} z_{i,j} b_i b_j$ and $p_2(\overline{z}, \overline{b}) := \sum_{1 \leq i \leq j \leq n} z_{i,j} \left(\sum_{k=1}^{n} a_{i,j,k} b_k \right)$. $\mathcal{I}$ is the set of all possible products of 4 variables (with repetition) from $\{z_{1,1}, \ldots, z_{n,n}, b_1, \ldots, b_n, u\}$.

Similarly, construct S' from S and we know from Theorem 3.1 that $R \cong S$ iff $R' \cong S'$. Now we move on to constructing cubic forms from these local commutative algebras R' and S'.

A natural set of generators of the ring R' is: $\{1\} \cup \{z_{i,j}\}_{1 \leq i \leq j \leq n} \cup \{b_i\}_{1 \leq i \leq n} \cup \{u\}$. For simplicity let us call them $1, x_1, \ldots, x_g, u$ respectively, where $g := \binom{n+1}{2} + n$. A natural additive basis of R' over $\mathbb{F}$ is:

$$\{1\} \cup \{x_i\}_{1 \leq i \leq g} \cup \{u\} \cup \{x_i x_j\}_{1 \leq i \leq j \leq g} \cup \{u x_i\}_{1 \leq i \leq g} \cup \{x_i x_j x_k\}_{1 \leq i \leq j \leq k \leq g}$$
$$\cup \{u x_i x_j\}_{1 \leq i \leq j \leq g} \text{ minus one term each from } p_3 \text{ and } up_2$$

(3.12)

For simplicity denote the elements of this additive basis by $1, c_1, \ldots, c_d$ respectively, where,

$$d := g+1+\binom{g+1}{2}+g+\binom{g+2}{3}+\binom{g+1}{2}-2 = 2g+2\binom{g+1}{2}+\binom{g+2}{3}-1$$

Finally, we construct a cubic form ϕ_R using R' as follows:

$$\phi_R(\overline{y}, \overline{c}, v) := \sum_{1\le i\le j\le d} y_{i,j}c_ic_j - v\sum_{1\le i\le j\le d} y_{i,j}\left(\sum_{k=1}^{d}\tilde{a}_{i,j,k}c_k\right) \tag{3.13}$$

where $\forall i, j,\ c_i \cdot c_j = \sum_{k=1}^{d} \tilde{a}_{i,j,k}c_k$ in R', for some $\tilde{a}_{i,j,k} \in \mathbb{F}$.

Observe that the v terms in this cubic form are "few" because most of the $\tilde{a}$ are zero. This property is useful in analysing the equivalence of such forms. Let us first bound the number of v terms in ϕ_R.

Claim 3.14. *The number of nonzero v terms in RHS of Equation (3.13) is less than $(3d-6)$.*

Proof of Claim 3.14. The number of nonzero v terms in RHS of Equation (3.13) is:

$$\le\ \#\{(k,\ell) \mid 1\le k\le \ell\le d,\ c_kc_\ell \ne 0 \text{ in } R'\}+3\left[\#(\text{terms in } p_3) + \#(\text{terms in } p_2)\right]$$

The first expression above accounts for all the relations in R' of the form $c_kc_\ell = c_m$. The second expression takes care of the relations that arise from $p_3 = 0$ and $up_2 = 0$. The factor of 3 above occurs because a term $x_ix_jx_k$ in p_3, up_2 can create v terms in at most 3 ways: from $(x_i)\cdot(x_jx_k)$ or $(x_j)\cdot(x_ix_k)$ or $(x_k)\cdot(x_ix_j)$.

$$\begin{aligned}\le\ & \#\left\{(k,\ell) \mid k\le\ell,\ c_k, c_\ell \in \{x_i\}_{1\le i\le g}\right\} + \#\left\{(k,\ell) \mid\ c_k \in \{x_i\}_{1\le i\le g}, c_\ell = u\right\}\\ & +\#\left\{(k,\ell) \mid\ c_k \in \{x_i\}_{1\le i\le g}, c_\ell \in \{x_ix_j\}_{1\le i\le j\le g}\right\}\\ & +\#\left\{(k,\ell) \mid\ c_k \in \{x_i\}_{1\le i\le g}, c_\ell \in \{ux_i\}_{1\le i\le g}\right\}\\ & +\#\left\{(k,\ell) \mid\ c_k = u, c_\ell \in \{x_ix_j\}_{1\le i\le j\le g}\right\} + 3\left[\#(\text{terms in } p_3) + \#(\text{terms in } p_2)\right]\end{aligned}$$

$$\le\ \left[\binom{g+1}{2} + g + g\cdot\binom{g+1}{2} + g^2 + \binom{g+1}{2}\right]+3\left[\binom{n+1}{2} + \binom{n+1}{2}\cdot n\right]$$

Note that the dominant term in the above expression is $\frac{g^3}{2}$ while in that of d it is $\frac{g^3}{6}$. Thus, the above expression should be around $3d$. Exact computation gives the following bound:

$$< \ (3d - 6)$$

□

Construct a cubic form ϕ_S from ring S in a way similar to that of Equation (3.13).

$$\phi_S(\overline{y}, \overline{c}, v) := \sum_{1 \le i \le j \le d} y_{i,j} c_i c_j - v \sum_{1 \le i \le j \le d} y_{i,j} \left(\sum_{k=1}^{d} \tilde{e}_{i,j,k} c_k \right) \tag{3.15}$$

where $\forall i, j, \ c_i \cdot c_j = \sum_{k=1}^{d} \tilde{e}_{i,j,k} c_k$ in S' for some $\tilde{e}_{i,j,k} \in \mathbb{F}$.

The following claim is what we intend to prove now.

Claim 3.16. *$\phi_R(\overline{y}, \overline{c}, v)$ is equivalent to $\phi_S(\overline{y}, \overline{c}, v)$ iff $R' \cong S'$ iff $R \cong S$.*

Proof of Claim 3.16. The part of this claim that needs to be proved is $\phi_R \sim \phi_S \Rightarrow R' \cong S'$. Suppose ψ is an equivalence from $\phi_R(\overline{y}, \overline{c}, v)$ to $\phi_S(\overline{y}, \overline{c}, v)$. We will show how to extract from ψ an isomorphism from R' to S'.

We have the following starting equation to analyze:

$$\sum_{1 \le i \le j \le d} \psi(y_{i,j}) \psi(c_i) \psi(c_j) - \psi(v) \sum_{1 \le i \le j \le d} \psi(y_{i,j}) \left(\sum_{k=1}^{d} \tilde{a}_{i,j,k} \psi(c_k) \right)$$

$$= \sum_{1 \le i \le j \le d} y_{i,j} c_i c_j - v \sum_{1 \le i \le j \le d} y_{i,j} \left(\sum_{k=1}^{d} \tilde{e}_{i,j,k} c_k \right) \tag{3.17}$$

The main property of this huge equation that we would like to show is: $\psi(c_i)$ *consists of only $\overline{c}$ terms.* Thus, $\psi(c_i)$ has enough information to extract a ring isomorphism from R' to S'. In the rest of the proof we will "rule out" the unpleasant cases of $\psi(c_i)$ having $\overline{y}, v$ terms and $\psi(v)$ having $\overline{y}$ terms.

Let for every $i \in [d]$, $\psi(c_i) = \sum_j \alpha_{i,j} c_j + \sum_{j,k} \beta_{i,j,k} y_{j,k} + \gamma_i v$ where α, β, γ's $\in \mathbb{F}$. For obvious reasons we will call the expression $\sum_{j,k} \beta_{i,j,k} y_{j,k}$ as the *$\overline{y}$ part of $\psi(c_i)$*. $\overline{y}$ parts of $\psi(v)$ and $\psi(y_{i,j})$ are defined similarly. We will show that the rank of the $\overline{y}$ part of $\psi(c_1), \ldots, \psi(c_d), \psi(v)$ is less than 3.

Assume that for some i, j, k the $\overline{y}$ parts of $\psi(c_i), \psi(c_j), \psi(c_k)$ are linearly independent over $\mathbb{F}$. By a *term* on LHS of Equation (3.17) we mean expressions of the form $\psi(y_{\ell,s})\psi(c_\ell)\psi(c_s)$ or $\psi(v)\psi(y_{\ell,s})\psi(c_t)$, where $\ell, s, t \in [d]$. Let T_0 be the set of all terms on LHS of Equation (3.17). There are at least $d + (d-1) + (d-2) = (3d-3)$ terms on LHS of Equation (3.17) that have an occurrence of $\psi(c_i), \psi(c_j)$ or $\psi(c_k)$, denote this set of terms by T_1 and the set of the remaining terms by T_2. Let us build a maximal set Y of linearly independent $\overline{y}$ parts and a set T of corresponding terms as follows:
Start with keeping $\overline{y}$ parts of $\psi(c_i), \psi(c_j), \psi(c_k)$ in Y and setting $T = T_1$. Successively add a new $\overline{y}$ part to Y that is linearly independent from the elements already in Y and that occurs in a term $t \in T_0 \setminus T$, also, add t to T. When Y has grown to its maximal size, it is easy to see that:

$$\begin{aligned}
\#Y &\leq 3 + \#T_2 \quad [\because \text{ initially, } \#Y = 3 \text{ and there are } \#T_2 \text{ terms outside } T] \\
&= 3 + \left[\binom{d+1}{2} + \#(\text{terms having } \psi(v)) - \#T_1\right] \\
&< 3 + \left[\binom{d+1}{2} + (3d-6) - (3d-3)\right] \quad [\text{by Claim 3.14 and } \because \#T_1 \geq (3d-3)] \\
&= \binom{d+1}{2} \\
&= \#\left\{y_{i,j}\right\}_{1 \leq i \leq j \leq d}
\end{aligned}$$

Now apply an invertible linear transformation τ on the $\overline{y}$ variables in Equation (3.17) such that all the $\overline{y}$ parts in Y are mapped to distinct *single* $\overline{y}$ variables, let $\tau(Y)$ denote the set of these variables. By substituting suitable linear forms, having only $\overline{c}, v$'s, to variables in $\tau(Y)$ we can make all the terms in $\tau(T)$ zero and the rest of the terms, *i.e.* $\tau(T_0 \setminus T)$, will then have no occurrence of $\overline{y}$ variables (as Y is the *maximal* set of linearly independent $\overline{y}$ parts). Thus, LHS of Equation (3.17), after applying τ and the substitutions, is completely in terms of $\overline{c}, v$ while RHS still has at least one free $\overline{y}$ variable (as we fixed only $\#\tau(Y) < \#\left\{y_{i,j}\right\}_{1 \leq i \leq j \leq d}$ $\overline{y}$ variables and as τ is an invertible linear transformation). This contradiction shows that the $\overline{y}$ part of $\psi(c_i), \psi(c_j), \psi(c_k)$ cannot be linearly independent, for any i, j, k. Using a similar argument it can be shown that the $\overline{y}$ part of $\psi(c_i), \psi(c_j), \psi(v)$ cannot be linearly independent, for any i, j. Thus, the rank of the $\overline{y}$ part of $\psi(c_1), \ldots, \psi(c_d), \psi(v)$ is ≤ 2. For concreteness let us assume that the rank is *exactly* 2, the proof we give below will easily go through even when the rank is 1.

Again let Y be a maximal set of linearly independent $\overline{y}$ parts occurring in $\left\{\psi(y_{i,j})\right\}_{1 \leq i \leq j \leq d}$ with the extra condition that $\overline{y}$ parts in Y are also linearly independent from those occurring in $\psi(c_1), \ldots, \psi(c_d), \psi(v)$. As we have assumed the rank of the $\overline{y}$ part of $\psi(c_1), \ldots, \psi(c_d), \psi(v)$ to be 2 we get $\#Y = \binom{d+1}{2} - 2$. Let $(i_1, j_1), (i_2, j_2)$ be the two tuples such that the $\overline{y}$ parts of $\psi(y_{i_1,j_1}), \psi(y_{i_2,j_2})$ do not appear in Y. To make things easier to handle let us apply an invertible linear transformation τ_1 on the variables in Equation (3.17) such that:

- the $\overline{y}$ parts of $\tau_1 \circ \psi(c_1), \ldots, \tau_1 \circ \psi(c_d), \tau_1 \circ \psi(v)$ are all linear combinations of only y_{i_1,j_1} and y_{i_2,j_2}.
- for all (i,j) other than (i_1, j_1) and (i_2, j_2), the $\overline{y}$ part of $\tau_1 \circ \psi(y_{i,j})$ is equal to $y_{i,j}$.
- τ_1 is identity on $\overline{c}, v$.

For clarity let $\psi' := \tau_1 \circ \psi$. Rest of our arguments will be based on comparing the coefficients of $y_{i,j}$, for $(i,j) \neq (i_1, j_1), (i_2, j_2)$, on both sides of the equation:

$$\sum_{1 \le i \le j \le d} \psi'(y_{i,j}) \left(\psi'(c_i c_j) - \psi'(v) \sum_{k=1}^{d} \tilde{a}_{i,j,k} \psi'(c_k) \right)$$

$$= \sum_{1 \le i \le j \le d} y_{i,j} (\text{quadratic terms in } \overline{c}, v) \tag{3.18}$$

For any c_i, choose distinct basis elements c_j, c_k and c_ℓ satisfying $c_i c_j = c_i c_k = c_i c_\ell = 0$ in R' (note that there is an ample supply of such j, k, ℓ), such that by comparing coefficients of $y_{i,j}, y_{i,k}, y_{i,\ell}$ (assumed to be other than y_{i_1,j_1}, y_{i_2,j_2}) on both sides of Equation (3.18) we get:

$$\psi'(c_i c_j) + (e_{i,j,1} E_1 + e_{i,j,2} E_2) = (\text{quadratic terms in } \overline{c}, v)$$

$$\psi'(c_i c_k) + (e_{i,k,1} E_1 + e_{i,k,2} E_2) = (\text{quadratic terms in } \overline{c}, v)$$

$$\psi'(c_i c_\ell) + (e_{i,\ell,1} E_1 + e_{i,\ell,2} E_2) = (\text{quadratic terms in } \overline{c}, v) \tag{3.19}$$

where, $e_{i,j,1}, e_{i,j,2}, e_{i,k,1}, e_{i,k,2}, e_{i,\ell,1}, e_{i,\ell,2} \in \mathbb{F}$ and

$$E_1 = \psi'(c_{i_1} c_{j_1}) - \psi'(v) \sum_{k=1}^{d} \tilde{a}_{i_1,j_1,k} \psi'(c_k)$$

$$E_2 = \psi'(c_{i_2} c_{j_2}) - \psi'(v) \sum_{k=1}^{d} \tilde{a}_{i_2,j_2,k} \psi'(c_k)$$

Now there exist $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}$ (not all zero) such that Equations (3.19) can be combined to get rid of E_1, E_2 and get:

$$\psi'(c_i)\,(\lambda_1\psi'(c_j) + \lambda_2\psi'(c_k) + \lambda_3\psi'(c_\ell)) = (\text{quadratic terms in } \overline{c}, v)$$

This equation combined with the observation that both $\psi'(c_i)$ and $(\lambda_1\psi'(c_j) + \lambda_2\psi'(c_k) + \lambda_3\psi'(c_\ell))$ are non-zero (as ψ' is invertible) implies that:

$$\forall i, \quad \psi'(c_i) = (\text{linear terms in } \overline{c}, v) \tag{3.20}$$

This means that the $\overline{y}$-variables are only in $\psi'(y_{i,j})$'s and possibly $\psi'(v)$. Again apply an invertible linear transformation τ_2 on the $\overline{y}$-variables in Equation (3.18) such that $\tau_2 \circ \psi'(v)$ has only y_{i_0,j_0} in the $\overline{y}$ part and the $\overline{y}$ part of $\tau_2 \circ \psi'(y_{i,j})$ is equal to $y_{i,j}$ for all (i,j) except possibly (i_0,j_0). For clarity let $\psi'' := \tau_2 \circ \psi'$. Our equation now is:

$$\sum_{1\le i\le j\le d} \psi''(y_{i,j}) \left(\psi''(c_ic_j) - \psi''(v)\sum_{k=1}^{d} \tilde{a}_{i,j,k}\psi''(c_k)\right)$$

$$= \sum_{1\le i\le j\le d} y_{i,j}(\text{quadratic terms in } \overline{c}, v) \tag{3.21}$$

By comparing coefficients of $y_{i,j}$ (other that y_{i_0,j_0}) on both sides of the above equation we get:

$$\left(\psi''(c_ic_j) - \psi''(v)\sum_{k=1}^{d} \tilde{a}_{i,j,k}\psi''(c_k)\right) + e\cdot\left(\psi''(c_{i_0}c_{j_0}) - \psi''(v)\sum_{k=1}^{d} \tilde{a}_{i_0,j_0,k}\psi''(c_k)\right)$$

$$= (\text{quadratic terms in } \overline{c}, v), \qquad \text{for some } e \in \mathbb{F}.$$

Pick i,j such that $\sum_{k=1}^{d} \tilde{a}_{i,j,k}c_k \neq 0$ in R'. Now if $\psi''(v)$ has a nonzero y_{i_0,j_0} term then by comparing coefficients of y_{i_0,j_0} on both sides of the above equation we deduce:

$$\sum_{k=1}^{d} \tilde{a}_{i,j,k}\psi''(c_k) + e\cdot\sum_{k=1}^{d} \tilde{a}_{i_0,j_0,k}\psi''(c_k) = 0 \tag{3.22}$$

But again we can pick i,j suitably so that $\left(\sum_{k=1}^{d} \tilde{a}_{i,j,k}c_k\right) \notin \left\{0,\ -e\cdot\sum_{k=1}^{d} \tilde{a}_{i_0,j_0,k}c_k\right\}$ and hence avoiding Equation (3.22) to hold. Thus, proving that $\psi''(v)$ has no y_{i_0,j_0} term. So we now have:

$$\psi''(v) = (\text{linear terms in } \overline{c}, v)$$

and

$$\forall i, \quad \psi''(c_i) = (\text{linear terms in } \overline{c}, v) \tag{3.23}$$

Since, $\overline{y}$-variables are present only in $\psi''(y_{i,j})$'s, comparing coefficients of $y_{i,j}$'s on both sides of Equation (3.21) gives:

$$\forall i,j, \;\; \psi''(c_ic_j) - \psi''(v)\sum_{k=1}^{d} \tilde{a}_{i,j,k}\psi''(c_k) = (\text{quadratic terms in } \overline{c}) - v(\text{linear terms in } \overline{c}) \tag{3.24}$$

Using this equation we will prove now that $\psi''(c_i)$ has only $\overline{c}$-variables.

Consider a c_i such that $c_i^2 = 0$ in R', then from Equation (3.24):

$$\psi''(c_i)^2 = (\text{quadratic terms in } \overline{c}) - v(\text{linear terms in } \overline{c}) \tag{3.25}$$

Now if $\psi''(c_i)$ has a nonzero v term then there will be a v^2 term above on LHS which is absurd. Thus, $\psi''(c_i)$ has only $\overline{c}$-variables when $c_i^2 = 0$ in R'. When $c_i^2 \neq 0$ then $c_i^2 = \sum_{k=1}^{d} \tilde{a}_{i,i,k}c_k$ in R' where the c_k's with nonzero $\tilde{a}_{i,i,k}$ satisfy $c_k^2 = 0$. This happens because the way $\overline{c}$'s are defined in Equation (3.12) the expression of c_i^2 will have only quadratic or cubic terms in $\overline{x}$ and the square of these terms would clearly be zero in R'. Thus, again if $\psi''(c_i)$ has a v term then there will be an uncancelled v^2 term on LHS of the equation:

$$\psi''(c_i)^2 - \psi''(v)\sum_{k=1}^{d} \tilde{a}_{i,i,k}\psi''(c_k) = (\text{quadratic terms in } \overline{c}) - v(\text{linear terms in } \overline{c})$$

Thus, we know at this point that $\psi''(v)$ has only $\overline{c}, v$ terms and $\psi''(c_i)$ has only $\overline{c}$ terms. Since, τ_1, τ_2 act only on $\overline{y}$'s we have what we intended to prove in the beginning (recall Equation (3.17)):

$$\psi(v) = (\text{linear terms in } \overline{c}, v)$$

and

$$\forall i, \quad \psi(c_i) = (\text{linear terms in } \overline{c}) \tag{3.26}$$

We have now almost extracted a ring isomorphism from the cubic form equivalence ψ, just few technicalities are left which we resolve next.

Apply an invertible linear transformation τ_3 on the $\overline{y}$-variables in Equation (3.17) such that the $\overline{y}$ part of $\tau_3 \circ \psi(y_{i,j})$ is equal to $y_{i,j}$ for all $i \leq j \in [d]$.

Of course, we assume that τ_3 is identity on the $\overline{c}, v$ variables. So, on comparing coefficients of $y_{i,j}$ on both sides of the Equation (3.17) after applying τ_3 we get: (3.27)

$$\forall i,j, \quad \tau_3 \circ \psi(c_i c_j) - \tau_3 \circ \psi(v) \sum_{k=1}^{d} \tilde{a}_{i,j,k} \tau_3 \circ \psi(c_k) = \sum_{i \leq j} \lambda_{i,j} \left(c_i c_j - v \sum_{k=1}^{d} \tilde{e}_{i,j,k} c_k \right)$$

for some $\lambda_{i,j} \in \mathbb{F}$.

Substitute $v = 1$ in the expression for $\tau_3 \circ \psi(v) = \gamma_{v,v} v + \sum_i \alpha_{v,i} c_i$ and denote the result by m. Observe that $\gamma_{v,v} \neq 0$ and $\forall i,\ c_i$ is a nilpotent element in S' and hence m is a *unit* in the ring S'. On substituting $v = 1$ in Equation (3.27) we get:

$$\forall i,j, \quad \tau_3 \circ \psi(c_i) \cdot \tau_3 \circ \psi(c_j) - m \cdot \sum_{k=1}^{d} \tilde{a}_{i,j,k} \tau_3 \circ \psi(c_k) = 0 \ \text{ in } S'$$

If we define $\Psi := \frac{\tau_3 \circ \psi}{m}$ then we get:

$$\forall i,j, \quad \Psi(c_i)\Psi(c_j) - \sum_{k=1}^{d} \tilde{a}_{i,j,k} \Psi(c_k) = 0 \ \text{ in } S' \tag{3.28}$$

Now observe that if for some λ_i's $\in \mathbb{F}$, $\Psi(\sum_{i=1}^{d} \lambda_i c_i) = 0$ in S' then $\tau_3 \circ \psi(\sum_{i=1}^{d} \lambda_i c_i) = 0$ in S'. Since $\tau_3 \circ \psi$ is an invertible linear map from R' to equi-dimensional S' this means that $\sum_{i=1}^{d} \lambda_i c_i = 0$ in R'. Therefore, Ψ is a *bijection* from R' to S'. Together with Equation (3.28) this tells us that Ψ is an isomorphism from R' to S'. □

This completes the reduction from commutative $\mathbb{F}$-algebra isomorphism to cubic form equivalence. □

4. Equivalence of Forms: Known results

The last two sections indicate that the problem of cubic forms equivalence is quite an interesting special case of polynomial equivalence. Not much is known about the structure of cubic forms. On the other hand, structure of quadratic forms is well understood. We collect in this section the main ideas that have been around to understand forms equivalence. The notions of regularity and decomposability of cubic forms given here will be used to study our cubic forms (that appeared in Equation (3.13)) in the next section.

4.1. Quadratic Forms Equivalence.

In this subsection we sketch the classification theorem known for quadratic forms. As a byproduct we also get algorithms for solving quadratic forms equivalence over finite fields, $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$. The detailed proofs can be found in Serre (1973), we present the main ideas here simply for their beauty.

Here we will assume that char $\mathbb{F} \neq 2$. Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a quadratic form and let V be the vector space $\mathbb{F}^n$. Observe that the map $\Theta : V \times V \to \mathbb{F}$ defined as $\Theta(u, v) = \frac{f(u+v)-f(u)-f(v)}{2}$ is symmetric and *bilinear*, i.e., $\Theta(u, v) = \Theta(v, u)$ and $\Theta(u + u', v) = \Theta(u, v) + \Theta(u', v)$. Also, f is recoverable from Θ as $f(u) = \Theta(u, u)$. Thus, there is a $1 - 1$ correspondence from quadratic forms to symmetric bilinear maps on the underlying vector space and this connection is quite fruitful in classifying quadratic forms.

4.1.1. The Algorithm.

Suppose we are given two nonzero quadratic forms $f, g \in \mathbb{F}[x_1, \ldots, x_n]$. We will show how to check $f \sim g$ over $\mathbb{F}$.

Step 0:(Base case) If $f = a_i x_i^2$ and $g = b_j x_j^2$ then $f \sim g$ iff $\frac{a_i}{b_j}$ is a square in $\mathbb{F}$.

Step 1:(Diagonalization) Let us express f as a matrix product:

$$\begin{aligned} f(x_1, \ldots, x_n) &= \sum_{i=1}^{n} a_{i,i} x_i^2 + \sum_{1 \le i < j \le n} 2a_{i,j} x_i x_j \\ &= (x_1 \ \ldots \ x_n)\, A\, (x_1 \ \ldots \ x_n)^{\mathrm{T}} \end{aligned}$$

where, A is a symmetric matrix with $a_{i,j}$ as the $(i, j)^{\text{th}}$ and $(j, i)^{\text{th}}$ entries. Since A is a symmetric matrix over a field we can apply Gaussian elimination to get an invertible matrix C such that CAC^{T} is diagonal, say diag$[b_1 \ \ldots \ b_n]$. Then we have,

$$\begin{aligned} f\left((x_1 \ \ldots \ x_n)C\right) &= (x_1 \ \ldots \ x_n) CAC^{\mathrm{T}} (x_1 \ \ldots \ x_n)^{\mathrm{T}} \\ &= \sum_{i=1}^{n} b_i x_i^2 \end{aligned}$$

Thus, from now on we can assume that the input quadratic forms f, g are given as sums of squares. Note that in this step we needed char $\mathbb{F} \neq 2$.

Step 2:(Root-finding) Let $f = \sum_{i=1}^{n} a_i x_i^2$ and $g = \sum_{i=1}^{n} b_i x_i^2$, where a_i, b_i's are nonzero in $\mathbb{F}$. Find a root $(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}^n$ of the diagonal quadratic equation:

$$\sum_{i=1}^{n} a_i x_i^2 = b_n \tag{4.1}$$

Step 3:(Witt's decomposition) Let Θ be the symmetric bilinear map corresponding to f. Using simple linear algebra compute the subspace:

$$U := \left\{ u \in \mathbb{F}^n \mid \Theta\left((\alpha_1 \cdots \alpha_n)^T, u \right) = 0 \right\}$$

Now Witt's theorem states that subspace U and the "orthogonal" vector $(\alpha_1 \cdots \alpha_n)^T$ span the full space V:

$$V = \mathbb{F} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \oplus U$$

This means that any $v \in V$ can be written as $\lambda(\alpha_1 \cdots \alpha_n)^T + u$, where $\lambda \in \mathbb{F}$ and $u \in U$. Thus,

$$\begin{aligned} f(v) &= \Theta(v, v) \\ &= \Theta\left(\lambda(\alpha_1 \cdots \alpha_n)^T + u, \lambda(\alpha_1 \cdots \alpha_n)^T + u \right) \\ &= \lambda^2 \Theta\left((\alpha_1 \cdots \alpha_n)^T, (\alpha_1 \cdots \alpha_n)^T \right) + \Theta(u, u) \\ &= \lambda^2 f\left((\alpha_1 \cdots \alpha_n)^T \right) + f(u) \\ &= \lambda^2 b_n + f(u) \end{aligned}$$

This simply means that $f \sim b_n x_n^2 + f_1(x_1, \ldots, x_{n-1})$ for some quadratic form $f_1 \in \mathbb{F}[x_1, \ldots, x_{n-1}]$.

Step 4:(Witt's cancellation) So, we now have $f(x_1, \ldots, x_n) \sim b_n x_n^2 + f_1(x_1, \ldots, x_{n-1})$ and $g(x_1, \ldots, x_n) = b_n x_n^2 + \sum_{i=1}^{n-1} b_i x_i^2$. Witt's cancellation lemma says that:

$$b_n x_n^2 + f_1(x_1, \ldots, x_{n-1}) \;\sim\; b_n x_n^2 + \sum_{i=1}^{n-1} b_i x_i^2$$

$$\text{iff}$$

$$f_1(x_1, \ldots, x_{n-1}) \;\sim\; \sum_{i=1}^{n-1} b_i x_i^2$$

So, now we can recursively do steps 0-3 on these smaller quadratic forms of rank $n-1$.

Observe that steps 0, 1 and 3 are 'easy' to do, so the only part that needs explanation is step 2 – solving diagonal quadratic equations.

4.1.2. Solving diagonal quadratic equations. Here we are interested in solving Equation (4.1) in step 2. We will show how to find roots when $\mathbb{F}$ is a finite field, $\mathbb{C}, \mathbb{R}$ and $\mathbb{Q}$.

Suppose $\mathbb{F}$ is a finite field, say $\mathbb{F}_q$. If $n=1$ we need to solve $a_1x_1^2 = b_n$ which is just finding square-roots. If $n \geq 2$ a classic theorem of Weil (see Bach 1996) states that for a random choice of $x_1, \ldots, x_{n-1} \in \mathbb{F}_q$ there exists an $x_n \in \mathbb{F}_q$ satisfying the Equation (4.1). Thus, in all the cases we can find roots of the Equation (4.1) over $\mathbb{F}_q$ in randomized polynomial time.

Suppose $\mathbb{F}$ is $\mathbb{R}$ or $\mathbb{C}$ then it is easily seen that roots of the Equation (4.1) can be found in deterministic polynomial time.

Suppose $\mathbb{F} = \mathbb{Q}$. If $n=1$ then solving $a_1x_1^2 = b_n$ is just finding square-roots over rationals. The first nontrivial case is $n=2$ when we need to solve $a_1x_1^2 + a_2x_2^2 = b_n$. We can first pre-process the equation by clearing the denominators of a_1, a_2, b_n and then taking the square parts of the integer coefficients 'in' x_1, x_2 to get an equation: $ax^2 + by^2 = z^2$ where a, b are *square-free* integers and we want *coprime* $x, y, z \in \mathbb{Z}$. We now demonstrate an algorithm, due to Legendre, to solve this equation. We just need to define the *norm* of elements in the number field $\mathbb{Q}(\sqrt{a})$. Elements of $\mathbb{Q}(\sqrt{a})$ are of the form $(\alpha + \beta\sqrt{a})$ for some $\alpha, \beta \in \mathbb{Q}$ and we define the norm function $N : \mathbb{Q}(\sqrt{a}) \to \mathbb{Q}$ as: $N(\alpha + \beta\sqrt{a}) = \alpha^2 - a\beta^2$. Observe that it is a multiplicative function.

Wlog assume $|a| < |b|$. If $ax^2 + by^2 = z^2$ has a solution then for any prime $p|b$, p cannot divide x (otherwise $p|z \Rightarrow p^2|by^2 \Rightarrow p|y \Rightarrow x, y, z$ are not coprime). Thus, a is a square mod p. As a is a square mod p for every prime $p|b$ we get that a is a square mod b. Thus, there is a $t \in \mathbb{Z}$ such that $|t| \leq \frac{|b|}{2}$ and $a = t^2 (\text{mod } b)$. Let $b' \in \mathbb{Z}$ be such that:

$$t^2 = a + bb' \quad \text{over } \mathbb{Z} \tag{4.2}$$

Now we claim that $ax^2 + by^2 = z^2$ has a solution iff $ax^2 + b'y^2 = z^2$ has a solution. This happens because (say) if $ax^2 + by^2 = z^2$ has a solution then:

$$b = N\left(\frac{z + x\sqrt{a}}{y}\right)$$

Also, from Equation (4.2):

$$\begin{aligned} bb' &= N(t+\sqrt{a}) \\ \Rightarrow b' &= N\left(\frac{yt+y\sqrt{a}}{z+x\sqrt{a}}\right) \end{aligned}$$

Which on rationalizing the denominator effectively gives an integral solution of $ax^2+b'y^2=z^2$. Conversely, if $ax^2+b'y^2=z^2$ has a solution then $ax^2+by^2=z^2$ can be shown to have solutions in the exact same way as above.

Now notice that the equation $ax^2+b'y^2=z^2$ is a “smaller” equation, for:

$$\begin{aligned} |a|+|b'| &= |a|+\left|\frac{t^2-a}{b}\right| \\ &\le |a|+\left|\frac{t^2}{b}\right|+\left|\frac{a}{b}\right| \\ &< |a|+\frac{|b|}{4}+1 \\ &< |a|+|b| \end{aligned}$$

Thus, the above procedure can be repeatedly applied till we reach the equation $\pm x^2 \pm y^2 = z^2$ or $\pm x^2 = z^2$ which are trivial to solve over integers.

The interesting thing to note in the above algorithm is that it constructively shows that the equation $ax^2+by^2+cz^2=0$ has a solution over $\mathbb{Q}$ iff it has a solution over $\mathbb{R}$ and mod p for all primes p. This property is famously known as the *local-global principle.*

Rational root-finding for diagonal quadratic equations when $n>2$ uses the above algorithm and the ‘tool’ of local-global principle.

This completes the sketch of algorithms for quadratic forms equivalence and we collect the results in the following theorem.

Theorem 4.3 (Hasse, Witt et al). *(i) Over finite fields, quadratic forms equivalence can be decided in P and found in ZPP.*

(ii) Over $\mathbb{R}$ and $\mathbb{C}$, quadratic forms equivalence can be decided and found in P.

(iii) Over $\mathbb{Q}$, quadratic forms equivalence can be done in EXP.

4.2. Cubic Forms Equivalence. Unlike quadratic forms the theory of cubic forms is still in its infancy. We collect here some known notions useful in "pre-processing" a given cubic form (Harrison 1975).

Let $f(x_1, \ldots, x_n)$ be a cubic form over $\mathbb{F}$. In this section we will assume that characteristic of $\mathbb{F}$ is not 2 or 3. Let $V = \mathbb{F}^n$. We say that a map $\Theta : V \times V \times V \to \mathbb{F}$ is *symmetric* if for any permutation π on $\{1, 2, 3\}$ and any $v_1, v_2, v_3 \in V$, $\Theta(v_1, v_2, v_3) = \Theta(v_{\pi(1)}, v_{\pi(2)}, v_{\pi(3)})$. Θ is said to be 3-*linear* if it is linear in all the 3 arguments, where linear in the first argument means that: for all $u, u', v, w \in V$, $\Theta(u + u', v, w) = \Theta(u, v, w) + \Theta(u', v, w)$. Now the claim is that we can define a symmetric 3-linear map on V from any given cubic form $f(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le k \le n} a_{i,j,k} x_i x_j x_k$. Let $\overline{x}_1 = \begin{pmatrix} x_{1,1} \\ \vdots \\ x_{n,1} \end{pmatrix}$, $\overline{x}_2, \overline{x}_3$ be vectors in $V = \mathbb{F}^n$. Define a map Θ from the cubic form f as:

$$\Theta\left(\overline{x}_1, \overline{x}_2, \overline{x}_3\right) = \Theta\left(\begin{pmatrix} x_{1,1} \\ \vdots \\ x_{n,1} \end{pmatrix}, \begin{pmatrix} x_{1,2} \\ \vdots \\ x_{n,2} \end{pmatrix}, \begin{pmatrix} x_{1,3} \\ \vdots \\ x_{n,3} \end{pmatrix}\right)$$
$$= \frac{1}{6} \sum_{\alpha} D_\alpha(f) \cdot x_{\alpha(1),1} x_{\alpha(2),2} x_{\alpha(3),3}$$

where α ranges over all maps from $\{1, 2, 3\} \to \{1, 2, \ldots, n\}$ and the coefficient $D_\alpha(f)$ is given as:

$$D_\alpha(f) := \frac{\partial^3 f(x_1, \ldots, x_n)}{\partial x_{\alpha(1)} \partial x_{\alpha(2)} \partial x_{\alpha(3)}}$$

It is easily seen that this map Θ is symmetric 3-linear and moreover:

$$\Theta\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = f(x_1, \ldots, x_n)$$

Thus, we have a $1-1$ correspondence between the cubic forms and the symmetric 3-linear maps on the underlying vector space (compare this with a similar observation for quadratic forms in Section 4.2).

Example 4.4. Let $f(x,y) = x^3+x^2y$ be a cubic form. Then the corresponding symmetric 3-linear map Θ on $V = \mathbb{F}^2$ is defined as:

$$\Theta\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} x_3 \\ y_3 \end{pmatrix}\right) = x_1x_2x_3 + \frac{1}{3}x_1x_2y_3 + \frac{1}{3}x_1x_3y_2 + \frac{1}{3}x_2x_3y_1$$

and verify that:

$$\Theta\left(\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix}\right) = f(x,y)$$

◊

4.2.1. Regularity. The first thing we would like to ensure about a given cubic form f is that there should not be "extra" variables in f, i.e., there is no invertible linear transformation τ such that $f(\tau x_1, \ldots, \tau x_n)$ has less than n variables. Such a cubic form is called *regular*.

Example 4.5. The cubic form $f(x) = x^3$ is regular while $f(x,y) = (x+y)^3$ is not regular as the invertible map:

$$\tau : \begin{cases} x+y & \mapsto x \\ y & \mapsto y \end{cases}$$

reduces the number of variables of f. ◊

By *regularizing* a given cubic form f we mean finding an invertible linear transformation that applied on f makes it regular.

Proposition 4.6 (Harrison). *A given cubic form can be regularized in deterministic polynomial time.*

Proof. Suppose $f \in \mathbb{F}[x_1, \ldots, x_n]$ is a given cubic form and $\Theta(\cdot,\cdot,\cdot)$ is its corresponding symmetric 3-linear map on $V = \mathbb{F}^n$. Suppose $f(x_1, \ldots, x_n)$ is not regular and its regularized form is $f^{reg}(x_1, \ldots, x_m)$ in smaller number of variables $1 \leq m < n$. Further, let Θ^{reg} be the symmetric 3-linear map corresponding to f^{reg} and A be the invertible matrix in $\mathbb{F}^{n\times n}$ such that for all $\overline{x}_1, \overline{x}_2, \overline{x}_3 \in V$:

$$\Theta(A\overline{x}_1, A\overline{x}_2, A\overline{x}_3) = \Theta^{reg}\left(\begin{pmatrix} x_{1,1} \\ \vdots \\ x_{m,1} \end{pmatrix}, \begin{pmatrix} x_{1,2} \\ \vdots \\ x_{m,2} \end{pmatrix}, \begin{pmatrix} x_{1,3} \\ \vdots \\ x_{m,3} \end{pmatrix}\right)$$

Now observe that the RHS above is independent of the last coordinates, i.e. $x_{n,1}, x_{n,2}, x_{n,3}$. Thus, if we fix $\overline{x}_1$ to be $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ then for all $\overline{x}_2, \overline{x}_3 \in V$:

$$\Theta\left(A\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}, A\overline{x}_2, A\overline{x}_3\right) = \Theta^{reg}\left(0, \begin{pmatrix} x_{1,2} \\ \vdots \\ x_{m,2} \end{pmatrix}, \begin{pmatrix} x_{1,3} \\ \vdots \\ x_{m,3} \end{pmatrix}\right) = 0$$

As A is invertible $v := A\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \neq 0$ and we have $\Theta(v, \cdot, \cdot) = 0$.

More interestingly, we will now see that the converse holds too, i.e., if there is a nonzero $v \in V$ such that $\Theta(v, \cdot, \cdot) = 0$ then f is not regular. Consider the following equation in the variables $x_{1,1}, x_{2,1}, \ldots, x_{n,1}$:

$$\text{for all } \overline{x}_2, \overline{x}_3 \in V,\ \Theta\left(\overline{x}_1, \overline{x}_2, \overline{x}_3\right) = 0 \tag{4.7}$$

If we compare the coefficient of $x_{i,2}x_{j,3}$ on both sides of the equation we get a linear equation and hence as i, j vary over all of $\{1, 2, \ldots, n\}$ we get a system of homogeneous linear equations, say:

$$M\begin{pmatrix} x_{1,1} \\ \vdots \\ x_{n,1} \end{pmatrix} = 0$$

Now, if there is a nonzero $v \in V$ such that $\Theta(v, \cdot, \cdot) = 0$ then it means that $Mv = 0$ and hence, $\text{rank}(M) < n$. Now, by applying Gaussian elimination on M we get invertible matrices C, D such that the last $(n - \text{rank}(M))$ columns of $DMC =: M'$ are zero. Thus, the elements of the column vector $M(C\overline{x}_1) = (D^{-1}M')\overline{x}_1$ are independent of $x_{\text{rank}(M)+1,1}, \ldots, x_{n,1}$. In other words, $\Theta\left(C\overline{x}_1, \overline{x}_2, \overline{x}_3\right)$ is independent of the last $(n - \text{rank}(M))$ coordinates of $\overline{x}_1$. Now since Θ is symmetric 3-linear and C is an invertible linear transformation, the system of equations in the variables $\overline{x}_2$ that we get from the following equality:

$$\text{for all } \overline{x}_1, \overline{x}_3 \in V,\ \Theta\left(C\overline{x}_1, \overline{x}_2, \overline{x}_3\right) = 0$$

is equivalent to the system: $M\overline{x}_2 = 0$. Thus, as before, $M(C\overline{x}_2)$ is independent of the last $(n - \text{rank}(M))$ coordinates of $\overline{x}_2$ implying that $\Theta\left(C\overline{x}_1, C\overline{x}_2, \overline{x}_3\right)$ is independent of the last $(n-\text{rank}(M))$ coordinates of $\overline{x}_1$ and that of $\overline{x}_2$. Repeating this same argument again, we deduce: $\Theta\left(C\overline{x}_1, C\overline{x}_2, C\overline{x}_3\right)$ is independent of the last $(n - \text{rank}(M))$ coordinates of $\overline{x}_1, \overline{x}_2, \overline{x}_3$.

Thus, $f\left(C\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\right) = \Theta\left(C\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}, C\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}, C\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\right)$ is independent of

$x_{\text{rank}(M)+1}, \ldots, x_n$ and regular over the variables $x_1, \ldots, x_{\text{rank}(M)}$.

Note that all the steps in the above discussion require simple linear algebra and hence can be executed in deterministic polynomial time. □

4.2.2. Decomposability. Cubic forms do not satisfy the nice property of diagonalization unlike quadratic forms, for example: x^3+x^2y cannot be written as a sum of cubes. But there is a notion of decomposability of cubic forms into simpler cubic forms. We call a cubic form $f(x_1, \ldots, x_n)$ *decomposable* if there is an invertible linear transformation τ, an $i \in [n]$ and cubic forms g, h such that:

$$f(\tau x_1, \ldots, \tau x_n) = g(x_1, \ldots, x_i) + h(x_{i+1}, \ldots, x_n)$$

This is also denoted by: $f \sim g \oplus h$.

Example 4.8. The cubic form $f_1(x, y) = x^3 + y^3$ is decomposable while the cubic form $f_2(x, y) = x^3 + xy^2$ is indecomposable. ♢

It is interesting that given a cubic form f the decomposition of f can be found algorithmically. To show this we need the notion of centre of a cubic form that captures the symmetries of the underlying 3-linear map.

Definition 4.9. *Let f be a cubic form and Θ be the corresponding symmetric 3-linear map on the space V. The* center, *Cent*(f), *of the cubic form f is defined as:*

$$\left\{M \in \mathbb{F}^{n\times n} \mid \textit{for all } v_1, v_2, v_3 \in V,\ \Theta(Mv_1, v_2, v_3) = \Theta(v_1, Mv_2, v_3)\right\}$$

Example 4.10. Let $f(x)$ be the cubic form x^3 then $\text{Cent}(f) = \mathbb{F}$. If $f(x, y) = x^3 + y^3$ then $\text{Cent}(f) \cong \text{Cent}(x^3) \times \text{Cent}(y^3) \cong \mathbb{F} \times \mathbb{F}$. ♢

The following properties of the center were first proved by Harrison (1975):

Lemma 4.11. *Suppose $f(x_1, \ldots, x_n)$ is a regular cubic form and Θ is the corresponding symmetric 3-linear map on $V = \mathbb{F}^n$.*

(1) Cent(f) is a commutative $\mathbb{F}$-algebra.

(2) f is indecomposable if and only if Cent(f) is indecomposable.

Proof (1). Suppose $M_1, M_2 \in \mathrm{Cent}(f)$ then $M_1 + M_2$ is also in the centre and it is routine to show that $(\mathrm{Cent}(f), +)$ is an abelian group.

To see that $M_1 \cdot M_2 \in \mathrm{Cent}(f)$ observe that for any $u, v, w \in V$:

$$\begin{aligned}\Theta(M_1 \cdot M_2 u, v, w) &= \Theta(M_2 u, v, M_1 w) \;\; [\because M_1 \in \mathrm{Cent}(f)]\\ &= \Theta(u, M_2 v, M_1 w) \;\; [\because M_2 \in \mathrm{Cent}(f)]\\ &= \Theta(u, M_1 \cdot M_2 v, w) \;\; [\because M_1 \in \mathrm{Cent}(f)]\end{aligned}$$

Thus, by definition $M_1 \cdot M_2$ is in $\mathrm{Cent}(f)$. Multiplication in $\mathrm{Cent}(f)$ is associative simply because it is matrix multiplication. To see commutativity observe that:

$$\begin{aligned}\Theta(M_1 \cdot M_2 u, v, w) &= \Theta(M_2 u, v, M_1 w) \;\; [\because M_1 \in \mathrm{Cent}(f)]\\ &= \Theta(u, M_2 v, M_1 w) \;\; [\because M_2 \in \mathrm{Cent}(f)]\\ &= \Theta(M_1 u, M_2 v, w) \;\; [\because M_1 \in \mathrm{Cent}(f)]\\ &= \Theta(M_2 \cdot M_1 u, v, w) \;\; [\because M_2 \in \mathrm{Cent}(f)]\end{aligned}$$

Thus, $\Theta\left((M_1 \cdot M_2 - M_2 \cdot M_1)u, \cdot, \cdot\right) = 0$. As f is regular this means that $(M_1 \cdot M_2 - M_2 \cdot M_1)u = 0$ (refer the proof of the Proposition 4.6). Since, this happens for all $u \in V$ we have that $(M_1 \cdot M_2 - M_2 \cdot M_1) = 0$ implying that $M_1 \cdot M_2 = M_2 \cdot M_1$.

Also, $\mathbb{F}$ is clearly contained in $\mathrm{Cent}(f)$. Thus, $\mathrm{Cent}(f)$ is a commutative $\mathbb{F}$-algebra. □

Proof (2). Here, we need a property of local commutative rings proved in the appendix: a finite dimensional commutative algebra R is decomposable iff there is a nontrivial idempotent element, i.e., there is a $r \in R \setminus \{0, 1\}$, $r^2 = r$.

If the cubic form f decomposes as $f_1 \oplus f_2$ then it is easy to show that $\mathrm{Cent}(f)$ decomposes as $\mathrm{Cent}(f_1) \times \mathrm{Cent}(f_2)$.

Conversely, suppose $\mathrm{Cent}(f)$ is decomposable. Then there is a matrix $M \in \mathrm{Cent}(f)$ such that $M^2 = M$ but $M \neq 0, I$. Now we want to decompose f using M.

Firstly, observe that if there is a $v \in MV \cap (I-M)V$ then $Mv = (I-M)v = 0$ and by adding the two we get $v = 0$. Next, observe that for any $u, v, w \in V$:

$$\begin{aligned}\Theta(Mu, (I-M)v, w) &= \Theta(u, M(I-M)v, w) \quad [\because M \in \mathrm{Cent}(f)]\\ &= 0 \quad [\because M^2 = M]\end{aligned}$$

Thus, for any $v_1 \in MV, v_2 \in (I-M)V$, $\Theta(v_1, v_2, \cdot) = 0$ or in other words: $MV, (I-M)V$ are *orthogonal* subspaces of V with respect to Θ. This means that for any $v \in V$ if we express v as $v = v_1 + v_2$, where $v_1 \in MV, v_2 \in (I-M)V$, then:

$$\begin{aligned}f(v) &= \Theta(v, v, v)\\ &= \Theta(v_1 + v_2, v_1 + v_2, v_1 + v_2)\\ &= \Theta(v_1, v_1, v_1) + \Theta(v_2, v_2, v_2) \quad [\because \Theta \text{ is linear and } v_1, v_2 \text{ are orthogonal}]\end{aligned}$$

If f_1 is the cubic form corresponding to Θ acting on MV and f_2 is the cubic form corresponding to Θ acting on $(I-M)V$ then the above equation says that: $f \sim f_1 \oplus f_2$. □

Note that given a cubic form f we can compute the center in terms of a basis over $\mathbb{F}$ as it just requires linear algebra computations. Thus, the above lemma gives a method of decomposing the cubic form if we can decompose its centre.

Proposition 4.12 (Harrison). *Cubic form decomposition can be done in polynomial time given an oracle of polynomial factoring over* $\mathbb{F}$.

Proof. Suppose f is a cubic form. Assume wlog that f is regular as otherwise we can regularize f by applying Proposition 4.6. Now compute its centre, $\mathrm{Cent}(f)$, in deterministic polynomial time. As $\mathrm{Cent}(f)$ is a commutative $\mathbb{F}$-algebra we can find the decomposition of $\mathrm{Cent}(f)$, using polynomial factoring over $\mathbb{F}$ (see Remark 6.11), into local commutative rings. In particular, if $\mathrm{Cent}(f)$ is decomposable we can compute a nontrivial decomposition:

$$\mathrm{Cent}(f) = R_1 \times R_2$$

from where we get a nontrivial idempotent, for example, the element of $\mathrm{Cent}(f)$ corresponding to $(0, 1)$ (where 0 is the zero of R_1 and 1 is the unity of R_2). Now, the proof of Lemma 4.11 outlines a way of decomposing f using this nontrivial idempotent of $\mathrm{Cent}(f)$. □

5. Our Cubic Forms

The cubic forms that we worked with in this paper were of a special form. They owe their origin to local commutative $\mathbb{F}$-algebras. Suppose R is such an $\mathbb{F}$-algebra and $\mathcal{M}$ is its unique maximal ideal (refer Lemma 6.12 to see the form of these maximal ideals). Let $b_1, \ldots, b_n$ be a basis of $\mathcal{M}$ over $\mathbb{F}$ and the multiplication in R is defined as:

$$\text{for all } 1 \leq i \leq j \leq n,\ b_i \cdot b_j = \sum_{1 \leq k \leq n} a_{i,j,k} b_k, \quad \text{where, } a_{i,j,k}\text{'s are in } \mathbb{F} \tag{5.1}$$

Now if we combine these multiplicative relations by considering b_i*'s* as formal variables, homogenizing variable u and 'fresh' formal variables $z_{j,k}$*'s* then we get the following cubic form f from $\mathcal{M}$:

$$f(u, \bar{b}, \bar{z}) = \sum_{1 \leq i \leq j \leq n} z_{i,j} \left(b_i b_j - u \sum_{1 \leq k \leq n} a_{i,j,k} b_k \right)$$

These are more involved versions of *hyperbolic* cubic forms: $\sum_{1 \leq i \leq j \leq n} z_{i,j} b_i b_j$ (Keet 1993). If R_1, R_2 are two $\mathbb{F}$-algebras with maximal ideals $\mathcal{M}_1, \mathcal{M}_2$ and the corresponding cubic forms f_1, f_2 then the proof of Claim 2.9 essentially says that an isomorphism from R_1 to R_2 gives an equivalence from f_1 to f_2.

In this section we show that these cubic forms are regular and indecomposable over any field $\mathbb{F}$ of char $\neq 2, 3$.

Theorem 5.2. *Let $\mathbb{F}$ be a field with char $\neq 2, 3$. Let $\mathcal{M}$ be a maximal ideal of a local commutative $\mathbb{F}$-algebra R such that $\mathcal{M}^2 \neq 0$. The multiplicative relations of $\mathcal{M}$ are given by Equation (5.1) and additionally $b_{n-1}^2 = 0,\ b_n \mathcal{M} = 0$. Define a cubic form f as:*

$$f(u, \bar{b}, \bar{z}) = \sum_{1 \leq i \leq j \leq n} z_{i,j} \left(b_i b_j - u \sum_{1 \leq k \leq n} a_{i,j,k} b_k \right)$$

Then,

(1) f is regular.

(2) f is indecomposable.

Proof (1). As $\mathcal{M}^2 \neq 0$ note that f above is not u-free. Let Θ be the symmetric 3-linear map corresponding to f. Define the vector space $V := \mathbb{F}^m$, where $m := 1+n+\binom{n+1}{2}$. Let us fix the notation for specifying the coordinates of a vector v_i in V as:

$$(u_i, b_{1,i}, \ldots, b_{n,i}, z_{1,1,i}, \ldots, z_{1,n,i}, z_{2,2,i}, \ldots, z_{2,n,i}, \ldots, z_{n,1,i}, \ldots, z_{n,n,i})^{\mathrm{T}}$$

or more compactly as:

$$\begin{pmatrix} u_i \\ \overline{b}_i \\ \overline{z}_i \end{pmatrix}$$

If f is not regular then there is a nonzero $v \in V$ such that $\Theta(v, \cdot, \cdot) = 0$. So consider the following equation in the variables $u_1, \overline{b}_1, \overline{z}_1$:

$$\text{(5.3)} \qquad \text{for all } \begin{pmatrix} u_2 \\ \overline{b}_2 \\ \overline{z}_2 \end{pmatrix}, \begin{pmatrix} u_3 \\ \overline{b}_3 \\ \overline{z}_3 \end{pmatrix} \in V,\ \Theta\left(\begin{pmatrix} u_1 \\ \overline{b}_1 \\ \overline{z}_1 \end{pmatrix}, \begin{pmatrix} u_2 \\ \overline{b}_2 \\ \overline{z}_2 \end{pmatrix}, \begin{pmatrix} u_3 \\ \overline{b}_3 \\ \overline{z}_3 \end{pmatrix}\right) = 0$$

Therefore, by considering the coefficient of $z_{i,i,3}$ in the above equation we get:

$$\text{(5.4)} \qquad \frac{b_{i,1}b_{i,2}}{3} - \frac{u_1}{6}\sum_{1\le k\le n} a_{i,i,k}b_{k,2} - \frac{u_2}{6}\sum_{1\le k\le n} a_{i,i,k}b_{k,1} \ = \ 0$$

and by considering the coefficient of $z_{i,j,3}$, for $1 \le i < j \le n$, we get:

$$\text{(5.5)} \qquad \frac{b_{i,1}b_{j,2}}{6} + \frac{b_{j,1}b_{i,2}}{6} - \frac{u_1}{6}\sum_{1\le k\le n} a_{i,j,k}b_{k,2} - \frac{u_2}{6}\sum_{1\le k\le n} a_{i,j,k}b_{k,1} \ = \ 0$$

If $u_1 = 0$ then the coefficient of $b_{i,2}$ in Equation (5.4) gives: $b_{i,1} = 0$. As i varies over $[1 \ldots n]$ we get: $\begin{pmatrix} u_1 \\ \overline{b}_1 \end{pmatrix} = 0$.

If $u_1 \neq 0$ then considering the coefficient of $b_{k,2}$ in Equation (5.4) we get: $a_{i,i,k} = 0$ for all $k \in [n]\setminus\{i\}$. Thus, in the ideal $\mathcal{M}$: $b_i^2 = a_{i,i,i}b_i$ or $b_i(b_i - a_{i,i,i}) = 0$. This implies that $a_{i,i,i} = 0$ for otherwise $(b_i - a_{i,i,i})$ is invertible (as b_i is in the unique maximal ideal $\mathcal{M}$) forcing $b_i = 0$. Thus, in the ideal $\mathcal{M}$: $b_i^2 = 0$ for all $i \in [n]$. Similarly, considering the coefficient of $b_{k,2}$ in Equation (5.5) we get: $a_{i,j,k} = 0$ for all $k \in [n] \setminus \{i, j\}$. Thus, in the ideal $\mathcal{M}$: $b_ib_j = a_{i,j,i}b_i + a_{i,j,j}b_j$. Multiplying this equation by b_i and using $b_i^2 = 0$ we get: $a_{i,j,j}b_ib_j = 0$ and symmetrically, $a_{i,j,i}b_ib_j = 0$. So if $b_ib_j \neq 0$ then $a_{i,j,i} = a_{i,j,j} = 0$ and hence $b_ib_j = 0$. Thus, in the ideal $\mathcal{M}$: $b_ib_j = 0$ for all $1 \le i \le j \le n$. But this contradicts the hypothesis that $\mathcal{M}^2 \neq 0$.

Thus, a solution of Equation (5.3) must satisfy: $\begin{pmatrix} u_1 \\ \overline{b}_1 \end{pmatrix} = 0$. Using this we can now expand Equation (5.3) as:

$$\text{for all } \begin{pmatrix} u_2 \\ \overline{b}_2 \\ \overline{z}_2 \end{pmatrix}, \begin{pmatrix} u_3 \\ \overline{b}_3 \\ \overline{z}_3 \end{pmatrix} \in V, \quad \begin{aligned} \sum_{1\le i\le j\le n} z_{i,j,1} \Bigg(& \frac{b_{i,2}b_{j,3}}{6} + \frac{b_{j,2}b_{i,3}}{6} - \frac{u_2}{6} \sum_{1\le k\le n} a_{i,j,k} b_{k,3} \\ & - \frac{u_3}{6} \sum_{1\le k\le n} a_{i,j,k} b_{k,2} \Bigg) \\ & = 0 \end{aligned}$$

The above equation clearly means that: $z_{i,j,1} = 0$ for all $1 \le i \le j \le n$. Thus, $\begin{pmatrix} u_1 \\ \overline{b}_1 \\ \overline{z}_1 \end{pmatrix} = 0$ and hence f is regular. □

Proof (2). We compute the center of f and then show that it is an indecomposable $\mathbb{F}$-algebra which means, by Lemma 4.11, that f is indecomposable.

Let Θ be the symmetric 3-linear map corresponding to f. Define the vector space $V := \mathbb{F}^m$, where $m := 1 + n + \binom{n+1}{2}$. Let us fix the notation of specifying the coordinates of a vector v_i in V as:

$$(u_i, b_{1,i}, \ldots, b_{n,i}, z_{1,1,i}, \ldots, z_{1,n,i}, z_{2,2,i}, \ldots, z_{2,n,i}, \ldots, z_{n,1,i}, \ldots, z_{n,n,i})^{\mathrm{T}}$$

or more compactly as:

$$\begin{pmatrix} u_i \\ \overline{b}_i \\ \overline{z}_i \end{pmatrix}$$

Recall that Cent(f) consists of matrices $M \in \mathbb{F}^{m\times m}$ such that:

$$\forall \begin{pmatrix} u_1 \\ \overline{b}_1 \\ \overline{z}_1 \end{pmatrix}, \begin{pmatrix} u_2 \\ \overline{b}_2 \\ \overline{z}_2 \end{pmatrix}, \begin{pmatrix} u_3 \\ \overline{b}_3 \\ \overline{z}_3 \end{pmatrix} \in V, \qquad \begin{aligned} & \Theta\left(M \begin{pmatrix} u_1 \\ \overline{b}_1 \\ \overline{z}_1 \end{pmatrix}, \begin{pmatrix} u_2 \\ \overline{b}_2 \\ \overline{z}_2 \end{pmatrix}, \begin{pmatrix} u_3 \\ \overline{b}_3 \\ \overline{z}_3 \end{pmatrix} \right) \\ = \; & \Theta\left(\begin{pmatrix} u_1 \\ \overline{b}_1 \\ \overline{z}_1 \end{pmatrix}, M \begin{pmatrix} u_2 \\ \overline{b}_2 \\ \overline{z}_2 \end{pmatrix}, \begin{pmatrix} u_3 \\ \overline{b}_3 \\ \overline{z}_3 \end{pmatrix} \right) \end{aligned} \tag{5.6}$$

Consider the matrix M in block form as: $\begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix}$ such that M_{11} is $(n+1) \times (n+1)$ and M_{22} is $\binom{n+1}{2} \times \binom{n+1}{2}$. We prove properties of these block matrices in the subsequent claims.

Claim 5.7. $M_{12} = 0$.

Proof of Claim 5.7. Substitute $\begin{pmatrix} u_1 \\ \overline{b}_1 \end{pmatrix} = \begin{pmatrix} u_3 \\ \overline{b}_3 \end{pmatrix} = 0$ in Equation (5.6) to get:

$$\forall \begin{pmatrix} 0 \\ \overline{z}_1 \end{pmatrix}, \begin{pmatrix} u_2 \\ \overline{b}_2 \\ \overline{z}_2 \end{pmatrix}, \begin{pmatrix} 0 \\ \overline{z}_3 \end{pmatrix} \in V, \quad \Theta\left(\begin{pmatrix} M_{12}\overline{z}_1 \\ M_{22}\overline{z}_1 \end{pmatrix}, \begin{pmatrix} u_2 \\ \overline{b}_2 \\ \overline{z}_2 \end{pmatrix}, \begin{pmatrix} 0 \\ \overline{z}_3 \end{pmatrix} \right) = 0$$

If $M_{12} \neq 0$ then we can assign $\overline{z}_1 = v_1 \in \mathbb{F}^{\binom{n+1}{2} \times \binom{n+1}{2}}$ such that $M_{12}v_1 \neq 0$ and:

$$\forall \begin{pmatrix} u_2 \\ \overline{b}_2 \\ \overline{z}_2 \end{pmatrix}, \begin{pmatrix} 0 \\ \overline{z}_3 \end{pmatrix} \in V, \quad \Theta\left(\begin{pmatrix} M_{12}v_1 \\ M_{22}v_1 \end{pmatrix}, \begin{pmatrix} u_2 \\ \overline{b}_2 \\ \overline{z}_2 \end{pmatrix}, \begin{pmatrix} 0 \\ \overline{z}_3 \end{pmatrix} \right) = 0 \tag{5.8}$$

Notice that we can now run the proof of the regularity of f, as equations similar to Equation (5.4) and Equation (5.5) can be obtained by comparing the coefficients of $z_{i,i,3}, z_{i,j,3}$ in the Equation (5.8), to deduce $M_{12}v_1 = 0$. This contradiction shows that $M_{12} = 0$. □

Thus, an $M \in \mathrm{Cent}(f)$ looks like: $M = \begin{pmatrix} M_{11} & 0 \\ M_{21} & M_{22} \end{pmatrix}$. Let τ be a linear transformation on V induced by M, i.e.,

$$M \begin{pmatrix} u_i \\ \overline{b}_i \\ \overline{z}_i \end{pmatrix} = \begin{pmatrix} \tau(u_i) \\ \tau(b_{1,i}) \\ \vdots \\ \tau(b_{n,i}) \\ \tau(z_{1,1,i}) \\ \vdots \\ \tau(z_{n,n,i}) \end{pmatrix}$$

Claim 5.9. *There is an $\alpha \in \mathbb{F}$ such that $M_{11} = \alpha \cdot I$.*

Proof of Claim 5.9. To understand M more let us substitute: $\overline{z}_1 = \overline{z}_2 =$

$0, \begin{pmatrix} u_3 \\ \bar{b}_3 \end{pmatrix} = 0$ in the Equation (5.6):

$$\begin{aligned}
\forall \begin{pmatrix} u_1 \\ \bar{b}_1 \\ 0 \end{pmatrix}, \begin{pmatrix} u_2 \\ \bar{b}_2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \bar{z}_3 \end{pmatrix} \in V, \qquad & \Theta\left(\begin{pmatrix} M_{11} \begin{pmatrix} u_1 \\ \bar{b}_1 \end{pmatrix} \\ M_{21} \begin{pmatrix} u_1 \\ \bar{b}_1 \end{pmatrix} \end{pmatrix}, \begin{pmatrix} u_2 \\ \bar{b}_2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \bar{z}_3 \end{pmatrix} \right) \\
= \; & \Theta\left(\begin{pmatrix} u_1 \\ \bar{b}_1 \\ 0 \end{pmatrix}, \begin{pmatrix} M_{11} \begin{pmatrix} u_2 \\ \bar{b}_2 \end{pmatrix} \\ M_{21} \begin{pmatrix} u_2 \\ \bar{b}_2 \end{pmatrix} \end{pmatrix}, \begin{pmatrix} 0 \\ \bar{z}_3 \end{pmatrix} \right)
\end{aligned} \tag{5.10}$$

In the above equation comparing the coefficient of $z_{i,j,3}$, for $1 \leq i \leq j \leq n$, gives:

$$\begin{aligned}
& \frac{\tau(b_{i,1})b_{j,2}}{6} + \frac{\tau(b_{j,1})b_{i,2}}{6} - \frac{\tau(u_1)}{6} \sum_{1 \leq k \leq n} a_{i,j,k} b_{k,2} - \frac{u_2}{6} \sum_{1 \leq k \leq n} a_{i,j,k} \tau(b_{k,1}) \\
= \; & \frac{b_{i,1}\tau(b_{j,2})}{6} + \frac{b_{j,1}\tau(b_{i,2})}{6} - \frac{u_1}{6} \sum_{1 \leq k \leq n} a_{i,j,k} \tau(b_{k,2}) - \frac{\tau(u_2)}{6} \sum_{1 \leq k \leq n} a_{i,j,k} b_{k,1}
\end{aligned} \tag{5.11}$$

We have $b_n \mathcal{M} = 0$ in R thus, $b_n^2 = 0$ in R and so $a_{n,n,k} = 0$ for all $k \in [n]$. Thus, the Equation (5.11) for $(i,j) = (n,n)$ is simply:

$$\frac{\tau(b_{n,1})b_{n,2}}{3} = \frac{b_{n,1}\tau(b_{n,2})}{3}$$

Since, the above equation holds for all $\begin{pmatrix} u_1 \\ \bar{b}_1 \\ 0 \end{pmatrix}, \begin{pmatrix} u_2 \\ \bar{b}_2 \\ 0 \end{pmatrix} \in V$ we deduce that there is an $\alpha \in \mathbb{F}$ such that $\tau(b_{n,1}) = \alpha \cdot b_{n,1}$.

Note that $b_i b_n = 0$ in R, for any $i \in [n]$, so $a_{i,n,k} = 0$ for all $k \in [n]$. Thus, Equation (5.11) for $(i,j) = (i,n)$, where $1 \leq i < n$, becomes:

$$\begin{aligned}
& \frac{\tau(b_{i,1})b_{n,2}}{6} + \frac{\tau(b_{n,1})b_{i,2}}{6} = \frac{b_{i,1}\tau(b_{n,2})}{6} + \frac{b_{n,1}\tau(b_{i,2})}{6} \\
\Rightarrow \quad & \frac{\tau(b_{i,1})b_{n,2}}{6} + \frac{\alpha b_{n,1}b_{i,2}}{6} = \frac{\alpha b_{i,1}b_{n,2}}{6} + \frac{b_{n,1}\tau(b_{i,2})}{6} \qquad [\because \tau(b_{n,1}) = \alpha \cdot b_{n,1}] \\
\Rightarrow \quad & \left(\tau(b_{i,1}) - \alpha b_{i,1}\right) b_{n,2} = b_{n,1} \left(\tau(b_{i,2}) - \alpha b_{i,2}\right)
\end{aligned}$$

Since, the above equation holds for all $\begin{pmatrix} u_1 \\ \bar{b}_1 \\ 0 \end{pmatrix}, \begin{pmatrix} u_2 \\ \bar{b}_2 \\ 0 \end{pmatrix} \in V$ we deduce that there is a $\beta \in \mathbb{F}$ such that

$$\tau(b_{i,1}) - \alpha b_{i,1} = \beta \cdot b_{n,1} \quad \text{for all } i \in [n-1] \tag{5.12}$$

Since, $b_{n-1}^2 = 0$ in R, we have $a_{n-1,n-1,k} = 0$ for all $k \in [n]$ and thus, Equation (5.11) for $(i,j) = (n-1, n-1)$ becomes:

$$\frac{\tau(b_{n-1,1})b_{n-1,2}}{3} = \frac{b_{n-1,1}\tau(b_{n-1,2})}{3}$$

Since, the above equation holds for all $\begin{pmatrix} u_1 \\ \bar{b}_1 \\ 0 \end{pmatrix}, \begin{pmatrix} u_2 \\ \bar{b}_2 \\ 0 \end{pmatrix} \in V$ we deduce that there is a $\gamma \in \mathbb{F}$ such that $\tau(b_{n-1,1}) = \gamma \cdot b_{n-1,1}$. This together with Equation (5.12) gives:

$$\begin{aligned} & \tau(b_{n-1,1}) = \gamma \cdot b_{n-1,1} = \alpha \cdot b_{n-1,1} + \beta \cdot b_{n,1} \\ \Rightarrow \quad & \gamma = \alpha \text{ and } \beta = 0 \end{aligned}$$

Finally, this together with Equation (5.12) gives us a nice form for τ:

$$\tau(b_{i,1}) = \alpha \cdot b_{i,1} \quad \text{for all } i \in [n] \tag{5.13}$$

Now choose $i \leq j \in [n]$ such that $b_i b_j \neq 0$ in R so that there is a $k \in [n]$ such that $a_{i,j,k} \neq 0$. Plugging Equation (5.13) in Equation (5.11) we get:

$$\begin{aligned} & \frac{\tau(u_1)}{6} \sum_{1 \leq k \leq n} a_{i,j,k} b_{k,2} + \frac{\alpha u_2}{6} \sum_{1 \leq k \leq n} a_{i,j,k} b_{k,1} = \frac{\alpha u_1}{6} \sum_{1 \leq k \leq n} a_{i,j,k} b_{k,2} + \frac{\tau(u_2)}{6} \sum_{1 \leq k \leq n} a_{i,j,k} b_{k,1} \\ \Rightarrow \quad & (\tau(u_1) - \alpha u_1) \sum_{1 \leq k \leq n} a_{i,j,k} b_{k,2} = (\tau(u_2) - \alpha u_2) \sum_{1 \leq k \leq n} a_{i,j,k} b_{k,1} \end{aligned}$$

If $b_i b_j \neq 0$ in R then there is a $k \in [n]$ such that $a_{i,j,k} \neq 0$ and as the above equation holds for all $\begin{pmatrix} u_1 \\ \bar{b}_1 \\ 0 \end{pmatrix}, \begin{pmatrix} u_2 \\ \bar{b}_2 \\ 0 \end{pmatrix} \in V$ we deduce that there is a $\gamma \in \mathbb{F}$ such that:

$$\tau(u_1) - \alpha u_1 = \gamma \cdot \sum_{1 \leq k \leq n} a_{i,j,k} b_{k,1} \quad \text{where } r := \sum_{1 \leq k \leq n} a_{i,j,k} b_{k,1} \neq 0$$

If $\gamma \neq 0$ then since the LHS of the above equation is independent of i, j we will have that for all $i \leq j \in [n]$ either $b_i b_j = 0$ or r. Thus, $r^2 = c \cdot r$ for some $c \in \mathbb{F}$. As r is a nonzero element of the maximal ideal $\mathcal{M}$ this implies that $r = 0$. This contradiction means that $\gamma = 0$ and hence:

$$\tau(u_1) = \alpha u_1$$

This together with Equation (5.13) gives:

$$\begin{aligned} M_{11}\begin{pmatrix} u_1 \\ \overline{b}_1 \end{pmatrix} &= \begin{pmatrix} \tau(u_1) \\ \tau(b_{1,1}) \\ \vdots \\ \tau(b_{n,1}) \end{pmatrix} = \begin{pmatrix} \alpha u_1 \\ \alpha b_{1,1} \\ \vdots \\ \alpha b_{n,1} \end{pmatrix} \\ \Rightarrow \quad M_{11} &= \alpha \cdot I \end{aligned} \tag{5.14}$$

□

CLAIM 5.15. *$M_{22} = \alpha \cdot I$, where α is the same as in the last claim.*

Proof of Claim 5.15. Let us start by substituting: $\begin{pmatrix} u_1 \\ \overline{b}_1 \end{pmatrix} = 0, \overline{z}_2 = \overline{z}_3 = 0$ in the Equation (5.6):

(5.16)

$$\begin{aligned}
&\Theta\left(\begin{pmatrix} 0 \\ M_{22}\overline{z}_1 \end{pmatrix}, \begin{pmatrix} u_2 \\ \overline{b}_2 \\ 0 \end{pmatrix}, \begin{pmatrix} u_3 \\ \overline{b}_3 \\ 0 \end{pmatrix}\right) = \Theta\left(\begin{pmatrix} 0 \\ \overline{z}_1 \end{pmatrix}, \begin{pmatrix} M_{11}\begin{pmatrix} u_2 \\ \overline{b}_2 \end{pmatrix} \\ M_{21}\begin{pmatrix} u_2 \\ \overline{b}_2 \end{pmatrix} \end{pmatrix}, \begin{pmatrix} u_3 \\ \overline{b}_3 \\ 0 \end{pmatrix}\right) \\
\Rightarrow \quad &\Theta\left(\begin{pmatrix} 0 \\ M_{22}\overline{z}_1 \end{pmatrix}, \begin{pmatrix} u_2 \\ \overline{b}_2 \\ 0 \end{pmatrix}, \begin{pmatrix} u_3 \\ \overline{b}_3 \\ 0 \end{pmatrix}\right) = \Theta\left(\begin{pmatrix} 0 \\ \overline{z}_1 \end{pmatrix}, \begin{pmatrix} \alpha\begin{pmatrix} u_2 \\ \overline{b}_2 \end{pmatrix} \\ M_{21}\begin{pmatrix} u_2 \\ \overline{b}_2 \end{pmatrix} \end{pmatrix}, \begin{pmatrix} u_3 \\ \overline{b}_3 \\ 0 \end{pmatrix}\right) \\
\Rightarrow \quad &\Theta\left(\begin{pmatrix} 0 \\ M_{22}\overline{z}_1 \end{pmatrix}, \begin{pmatrix} u_2 \\ \overline{b}_2 \\ 0 \end{pmatrix}, \begin{pmatrix} u_3 \\ \overline{b}_3 \\ 0 \end{pmatrix}\right) = \Theta\left(\begin{pmatrix} 0 \\ \overline{z}_1 \end{pmatrix}, \begin{pmatrix} \alpha\begin{pmatrix} u_2 \\ \overline{b}_2 \end{pmatrix} \\ 0 \end{pmatrix}, \begin{pmatrix} u_3 \\ \overline{b}_3 \\ 0 \end{pmatrix}\right) \\
\Rightarrow \quad &\Theta\left(\begin{pmatrix} 0 \\ (M_{22} - \alpha I)\overline{z}_1 \end{pmatrix}, \begin{pmatrix} u_2 \\ \overline{b}_2 \\ 0 \end{pmatrix}, \begin{pmatrix} u_3 \\ \overline{b}_3 \\ 0 \end{pmatrix}\right) = 0
\end{aligned}$$

As the above equation holds for all $\begin{pmatrix} 0 \\ \bar{z}_1 \end{pmatrix}, \begin{pmatrix} u_2 \\ \bar{b}_2 \\ 0 \end{pmatrix}, \begin{pmatrix} u_3 \\ \bar{b}_3 \\ 0 \end{pmatrix} \in V$ we deduce:

$$M_{22} = \alpha I$$

□

Thus, any element M in the center of f looks like:

$$\begin{pmatrix} 0 & 0 \\ M_{12} & 0 \end{pmatrix} + \alpha I \quad \text{where, } \alpha \in \mathbb{F}$$

Now if M is idempotent then:

$$\begin{aligned} & M^2 = M \\ \Rightarrow \quad & M(M - I) = 0 \end{aligned}$$

But one of the matrices M or $(M - I)$ will always be invertible and hence $M = 0$ or $M = I$. Thus, Cent(f) is an indecomposable $\mathbb{F}$-algebra and, hence, f is indecomposable by Lemma 4.11. □

6. Discussion

This paper studied the complexity of the problem of polynomial equivalence. Over finite fields this problem is of intermediate complexity and, hence, unlikely to be NP-hard. Over infinite fields we know very little about this general problem! The special case of quadratic forms is completely understood due to the works of Minkowski (1885), Hasse (1921) and Witt (Witt & Kersten 1998). Inspired from quadratic forms, we considered the "slightly" more general case of cubic forms and proved some interesting results. We gave a reduction from commutative $\mathbb{F}$-algebra isomorphism to $\mathbb{F}$-cubic forms equivalence for any field $\mathbb{F}$. Two of its consequences are: Graph isomorphism reduces to the problem of cubic forms equivalence over any field $\mathbb{F}$, and equivalence of higher degree d-forms reduces to cubic forms equivalence over fields $\mathbb{F}$ having d-th roots. Clearly, cubic forms equivalence seems to be the most important special case of the problem of polynomial equivalence.

We hope that the rich structure of cubic forms will eventually give us more insights about the isomorphism problems of commutative $\mathbb{F}$-algebras and graphs. As a first step to understanding cubic forms, we believe that the decidability of cubic forms equivalence over $\mathbb{Q}$ should be resolved.

In the case of quadratic forms over $\mathbb{Q}$ the problem of equivalence reduced to questions of finding $\mathbb{Q}$-roots of a quadratic form. In particular, if two quadratic forms are equivalent over $\mathbb{R}$ and represent the same set of points over $\mathbb{Q}$ then they are equivalent over $\mathbb{Q}$. Here, we show that such a result does not hold for cubic forms, thus, giving evidence that $\mathbb{Q}$-root finding of a cubic form may not be related to the problem of equivalence of cubic forms. Let us define two rings:

$$R := \mathbb{Q}[x]/(x^2 - 1) \quad \text{and} \quad S := \mathbb{Q}[x]/(x^2 - 2)$$

Notice that the $\mathbb{Q}$-algebras R, S are isomorphic over $\mathbb{R}$ but nonisomorphic over $\mathbb{Q}$. Thus, using the construction given in Theorem 3.10 we get two cubic forms $\phi_R(\overline{y}, \overline{c}, v), \phi_S(\overline{y}, \overline{c}, v)$ that are equivalent over $\mathbb{R}$ but nonequivalent over $\mathbb{Q}$. But what are the rational points that these cubic forms represent? If we choose an i such that the coefficient of $y_{i,i}$ in ϕ_R is c_i^2 then:

$$\phi_R(0, \ldots, y_{i,i}, \ldots, 0, \overline{c}, v) = y_{i,i}c_i^2$$

Clearly, there exists such an i (recall the way we constructed ϕ_R) and, hence, ϕ_R represents all points in $\mathbb{Q}$. Similarly, ϕ_S represents all points in $\mathbb{Q}$. This gives us two cubic forms that are equivalent over $\mathbb{R}$, represent the same set of points over $\mathbb{Q}$ but are yet nonequivalent over $\mathbb{Q}$.

Finally, we pose some questions whose answers might unfold more structure of cubic forms:

- What are the invariants of cubic forms (under equivalence)?
- If cubic forms f, g are equivalent over $\mathbb{R}$ and are equivalent modulo p^k, for all primes p (except finitely many primes) and $k \in \mathbb{Z}^{\geq 1}$, then are they equivalent over $\mathbb{Q}$?
- Can we reduce $\mathbb{F}$-cubic forms equivalence problem to that of $\mathbb{F}$-algebra isomorphism, over *all* fields $\mathbb{F}$?
- Does R-algebra isomorphism reduces to R-cubic forms equivalence, where R is a commutative ring?

Appendix: Facts about Rings

A *ring* is a set R equipped with two binary operations $+$ and $\cdot$, called addition and multiplication, such that (a, b, c are general elements in R):

1). $(R, +)$ is an *abelian group* with identity element 0:

- ∘ Associativity: $(a+b)+c = a+(b+c)$
- ∘ Commutativity: $a+b = b+a$
- ∘ Identity: $0+a = a+0 = a$
- ∘ Inverse: $\forall a\ \exists(-a)$ such that $a + -a = -a + a = 0$

2). $(R, \cdot)$ is a *monoid* with identity element 1:

- ∘ Identity: $1 \cdot a = a \cdot 1 = a$
- ∘ Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

3). Multiplication distributes over addition:

- ∘ $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$
- ∘ $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$

If $(R \setminus \{0\}, \cdot)$ is an abelian group too then R becomes a *field.*

Example 6.1. $R_0 := (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a ring, it is a field iff n is prime. $R_1 := R_0[x]/(x^r - 1)$ is a commutative ring but never a field for $r > 1$. The set $R_2 := \left\{A \mid A \in R_0^{2\times 2}\right\}$ is a noncommutative ring under matrix addition and multiplication in R_0. $\Diamond$

We first collect some results related to decomposition of rings into simpler rings. A ring R is said to be *decomposable* if there are subrings R_1, R_2 such that:

- ∘ $R_1 \cdot R_2 = R_2 \cdot R_1 = 0$, i.e., for all $r_1 \in R_1, r_2 \in R_2$, $r_1 \cdot r_2 = r_2 \cdot r_1 = 0$.
- ∘ $R_1 \cap R_2 = \{0\}$.
- ∘ $R = R_1 + R_2$, i.e., for every $r \in R$ there are $r_1 \in R_1, r_2 \in R_2$ such that $r = r_1 + r_2$.

Such a ring decomposition has been denoted by $R = R_1 \times R_2$ in this work. The subrings R_1, R_2 are called *component* rings of R.

Example 6.2. The ring $R := \mathbb{F}[x]/(x^2 - x)$ decomposes as: $R = Rx \times R(1 - x) \cong \mathbb{F} \times \mathbb{F}$. Here, Rx is a short-hand for the set $\{r \cdot x \mid r \in R\}$. Note that $Rx, R(1-x)$ are subrings of R and have $x, (1-x)$ as their (multiplicative) identity elements respectively. ◊

An element $r \in R$ is called an *idempotent* if $r^2 = r$. The following lemma shows how idempotents help in decomposing a commutative ring.

Lemma 6.3. *A commutative ring R decomposes iff R has an idempotent element other than* $0, 1$.

Proof. Suppose $R = R_1 \times R_2$ is a nontrivial decomposition and let the identity element 1 of R be expressible as $1 = s + t$ where $s \in R_1, t \in R_2$. Then by the definition of decomposition we have:

$$\begin{aligned} & 1 \cdot 1 = (s+t) \cdot (s+t) \\ \Rightarrow\quad & 1 = s^2 + t^2 \qquad [\because s \cdot t = 0] \\ \Rightarrow\quad & s + t = s^2 + t^2 \\ \Rightarrow\quad & s - s^2 = t^2 - t \\ \Rightarrow\quad & s - s^2 = 0 \qquad [\because s - s^2 \in R_1 \cap R_2 = \{0\}] \\ \Rightarrow\quad & s \text{ is an idempotent.} \end{aligned}$$

Note that if $s = 0$ then $t = 1$ and then $R_1 = 0$ (as for all $r_1 \in R_1,\ r_1 \cdot R_2 = 0$) and similarly, if $s = 1$ then $R_2 = 0$. As R_1, R_2 are nonzero subrings of R we deduce that $s \neq 0, 1$ and hence s is an idempotent other than $0, 1$.

Conversely, suppose that $s \neq 0, 1$ is an idempotent of R. Then consider the subrings $R \cdot s$ and $R \cdot (1-s)$. Note that $s, (1-s)$ are the identity elements of $Rs, R(1-s)$ respectively. For any two elements $rs \in Rs, r'(1-s) \in R(1-s)$: $rs \cdot r'(1-s) = rr'(s - s^2) = 0$. If $r \in Rs \cap R(1-s)$ then $rs = 0$ and $r(1-s) = 0$ implying that $r = 0$. Finally, we can express any $r \in R$ as: $r = rs + r(1-s)$. Thus, R decomposes as: $R = Rs \times R(1-s)$. □

The following lemma shows that a decomposition of a ring into indecomposable rings is unique.

Lemma 6.4. *Let R be a ring and $R_1, \ldots, R_k$ be indecomposable nonzero rings such that:*

$$R = R_1 \times R_2 \times \cdots \times R_k$$

Then this decomposition is unique upto ordering, i.e. if we have indecomposable nonzero S_j's such that:

$$R = R_1 \times \cdots \times R_k = S_1 \times \cdots \times S_l$$

then $k = l$ and there exists a permutation π such that for all $i \in [k]$, $\quad R_i = S_{\pi(i)}$.

Proof. Assume wlog that $k \geq l$. Let ϕ_1 be a homomorphism of the ring R such that ϕ_1 is identity on S_1 and $\phi_1(S_2) = \cdots = \phi_1(S_l) = 0$. ϕ_1 is well defined simply because $R = S_1 \times \cdots \times S_l$.

Clearly, $\phi_1(R_1), \phi_1(R_2), \cdots, \phi_1(R_k)$ are all subrings of S_1 and:

$$\phi_1(R) = \phi_1(R_1) + \phi_1(R_2) + \cdots + \phi_1(R_k) = S_1$$

Can these subrings have nontrivial intersection? Say, $s_1 \in \phi_1(R_i) \cap \phi_1(R_j)$ for some $i \neq j$ then there are some $s, s' \in S_2 + \cdots + S_l$ such that $s_1 + s \in R_i$ and $s_1 + s' \in R_j$. Let a be the (multiplicative) identity of $R_1 + \cdots + R_{i-1} + R_{i+1} + \cdots + R_k$ and b be the identity of R_i. Then:

$$\begin{aligned}
& (s_1 + s)a = 0 \text{ and } (s_1 + s')b = 0 \;\; [\because R = R_1 \times \cdots \times R_k] \\
\Rightarrow \;\; & (s_1 + s)a + (s_1 + s')b = 0 \\
\Rightarrow \;\; & s_1(a + b) + sa + s'b = 0 \\
\Rightarrow \;\; & s_1 + (sa + s'b) = 0 \;\; [\because 1 = a + b] \\
\Rightarrow \;\; & s_1 = (sa + s'b) = 0 \;\; [\because s_1 \in S_1 \text{ and } sa, s'b \in S_2 + \cdots + S_l] \\
\Rightarrow \;\; & \phi_1(R_i) \cap \phi_1(R_j) = \{0\} \;\text{ for all } i \neq j \in [k]
\end{aligned}$$

Also, for any $r_i \in R_i, r_j \in R_j, \quad r_i r_j = 0$ implying that $\phi_1(r_i) \cdot \phi_1(r_j) = 0$. The properties above together mean that:

$$S_1 = \phi_1(R_1) \times \phi_1(R_2) \times \cdots \times \phi_1(R_k)$$

Since S_1 was assumed to be indecomposable we have that exactly one of the subrings above is nonzero. Wlog say, $\phi_1(R_2) = \cdots = \phi_1(R_k) = 0$ and then it is implied that $\phi_1(R_1) = S_1$.

Similarly, we can define ϕ_i to be a homomorphism of the ring R such that ϕ_i is identity on S_i and $\phi_i(S_j) = 0$ for all $j \in [l] \setminus \{i\}$. Then the above argument says that there is an injective map $\tau : [l] \rightarrow [k]$ such that for all $i \in [l]$:

$$\phi_i(R_{\tau(i)}) = S_i \text{ and } \phi_i(R_j) = 0 \text{ for all } j \in [k] \setminus \{\tau(i)\} \tag{6.5}$$

Now consider an $l \times k$ matrix $D = ((\delta_{i,j}))$ where $\delta_{i,j} = 1$ if $\phi_i(R_j) = S_i$ else $\delta_{i,j} = 0$. Eqn. (6.5) tells us that each row of D has exactly one 1. Now if $k > l$ then D has more columns than rows and hence there is a zero column, say j-th, implying that $\phi_i(R_j) = 0$ for all $i \in [l]$. But this means that $R_j = 0$ which is a contradiction. Hence, $k = l$ and D has exactly one 1 in each row and column, thus making τ a permutation.

So now we have that for any $j \in [k]$, $\phi_{\tau^{-1}(j)}(R_j) = S_{\tau^{-1}(j)}$ and $\phi_i(R_j) = 0$ for all $i \in [k] \setminus \{\tau^{-1}(j)\}$. In other words for any $j \in [k]$, $R_j = S_{\tau^{-1}(j)}$.

This completes the proof of unique decomposition of rings into indecomposable subrings. □

So what is the structure of these indecomposable rings that appear in the decomposition? Here, we sketch the form of indecomposable rings that are finite and commutative.

Lemma 6.6. *Let R be a finite commutative indecomposable ring. Then,*

(i) R has a prime-power characteristic, say p^m for some prime p.

(ii) R can be expressed in the form:

$$R = ((\mathbb{Z}/p^m\mathbb{Z})[z]/(h(z)))\,[y_1, \ldots, y_k]/\,(y_1^{e_1}, \ldots, y_k^{e_k}, h_1(z, y_1, \ldots, y_k), \ldots, \\ \ldots, h_l(z, y_1, \ldots, y_k))$$

where, $h(z)$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$ and h_i's are multivariate polynomials over $\mathbb{Z}/p^m\mathbb{Z}$.

Remark 6.7. *The ring $(\mathbb{Z}/p^m\mathbb{Z})[z]/(h(z))$, where $h(z)$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$, is called* Galois ring. *It is a finite field if $m = 1$.*

Notice that the form of R claimed in (2) above says that the generators $y_1, \ldots, y_k$ of R are nilpotents, *i.e. they vanish when raised by a suitable integer.*

Proof (i). Suppose R is a finite commutative indecomposable ring with characteristic n. If n nontrivially factors as: $n = ab$, where $a, b \in \mathbb{Z}^{>1}$ are coprime, then by Chinese remaindering R factors too:

$$R = aR \times bR$$

(Convince yourself that this is a decomposition.) This contradiction shows that n is a prime power, say $n = p^m$. □

Proof (ii). We assume $m = 1$ for simplicity of exposition. These ideas carry forward to larger m's (McDonald 1974). So suppose that R is an $\mathbb{F}_p$-algebra and is given in terms of basis elements $b_1, \ldots, b_n$. Let $g_1(b_1, \ldots, b_n), \ldots, g_l(b_1, \ldots, b_n)$

be the multivariate polynomials that define the multiplication operation of the ring R. Thus, we have an expression for R as:

$$R \cong \mathbb{F}_p[x_1, \dots, x_n]/(g_1(x_1, \dots, x_n), \dots, g_l(x_1, \dots, x_n)) \tag{6.8}$$

Since, R is of dimension n, $\{1, x_1, x_1^2, \dots, x_1^n\}$ cannot all be linearly independent and hence there is a polynomial $f_1(z) \in \mathbb{F}_p[z]$ of degree atmost n such that $f_1(x_1) = 0$ in R. Further, assume that f_1 is of lowest degree. Now if f_1 nontrivially factors as: $f_1(z) = f_{11}(z)f_{12}(z)$, where f_{11}, f_{12} are coprime, then by Chinese remaindering R decomposes as:

$$R \cong R \cdot f_{11}(x_1) \times R \cdot f_{12}(x_1)$$

As R is assumed to be indecomposable we deduce that f_1 is a power of an irreducible polynomial. Say, $f_1(z) = f_{11}(z)^{e_1}$ where f_{11} is an irreducible polynomial over $\mathbb{F}_p$ of degree d_1. Now we claim that there are $g_1', \dots, g_l' \in \mathbb{F}_{p^{d_1}}[x_1, \dots, x_n]$ such that:

$$R \cong \mathbb{F}_{p^{d_1}}[x_1, \dots, x_n]/(x_1^{e_1}, g_1'(x_1, \dots, x_n), \dots, g_l'(x_1, \dots, x_n)) \tag{6.9}$$

To prove the above claim we need the following fact:

Claim 6.10. *If $f(x)$ is an irreducible polynomial, of degree d, over a finite field $\mathbb{F}_q$ then*

$$S = \mathbb{F}_q[x]/(f(x)^e) \cong \mathbb{F}_{q^d}[u]/(u^e)$$

Proof of Claim 6.10. Consider the ring $S' := (\mathbb{F}_q[x]/(f(x)))[u]/(u^e) \cong \mathbb{F}_{q^d}[u]/(u^e)$. We claim that the map $\phi : S \to S'$ which fixes $\mathbb{F}_q$ and maps $x \mapsto (x + u)$, is an isomorphism.

Note that $f(x+u)^e = 0$ in the ring S' simply because $f(x+u) - f(x) = u \cdot q(x)$ for some $q(x) \in \mathbb{F}_q[x]$. Thus, ϕ is a ring homomorphism from S to S'. Next we show that the minimum polynomial that $\phi(x)$ satisfies over S' is of degree de, thus the dimension of $\phi(S)$ is the same as that of S' over $\mathbb{F}_q$ and hence ϕ is an isomorphism.

Suppose $g(z) := \sum_{j=0}^{d'} a_j x^j$ is the least degree polynomial over $\mathbb{F}_q$ such that $g(x + u) = 0$ in S'. This means that in S':

$$0 = g(x + u) = g(x) + u \cdot g^{(1)}(x) + u^2 \cdot \frac{g^{(2)}(x)}{2!} + \cdots + u^{e-1} \cdot \frac{g^{(e-1)}(x)}{(e-1)!}$$

where, $\frac{g^{(i)}(x)}{i!} = \sum_{j=i}^{d'} \frac{j(j-1)\cdots(j-i+1)}{i!} a_j x^{j-i}$. But since $1, u, \dots, u^{e-1}$ are linearly independent over $\mathbb{F}_q[x]/(f(x))$. We have:

$$g(x) = g^{(1)}(x) = \cdots = g^{(e-1)}(x) = 0 \text{ over } \mathbb{F}_q[x]/(f(x))$$

Whence we get, $f(z)^e | g(z)$ which by the definition of g means that $g(z) = f(z)^e$. Thus, ϕ is an isomorphism from S to S'. □

From the above claim we now deduce:

$$\begin{aligned} R &\cong \mathbb{F}_p[x_1, \dots, x_n]/(f_{11}(x_1)^{e_1}, g_1(x_1, \dots, x_n), \dots, g_l(x_1, \dots, x_n)) \\ &\cong \mathbb{F}_{p^{d_1}}[u, x_2, \dots, x_n]/(u^{e_1}, g_1'(u, x_2, \dots, x_n), \dots, g_l'(u, x_2, \dots, x_n)) \\ &\cong \mathbb{F}_{p^{d_1}}[x_1, x_2, \dots, x_n]/(x_1^{e_1}, g_1'(x_1, x_2, \dots, x_n), \dots, g_l'(x_1, x_2, \dots, x_n)) \end{aligned}$$

This new ring which we obtained has x_1 as a nilpotent. We can now consider the lowest degree polynomial $f_2(z) \in \mathbb{F}_{p^{d_1}}[z]$ such that $f_2(x_2) = 0$ in R. The above process when repeated on f_2, x_2 in place of f_1, x_1 gives us that there are $d_2, e_2 \in \mathbb{Z}^{\geq 1}$ and $g_1'', \dots, g_l'' \in \mathbb{F}_{p^{d_1 d_2}}[x_1, \dots, x_n]$ such that:

$$R \cong \mathbb{F}_{p^{d_1 d_2}}[x_1, \dots, x_n]/(x_1^{e_1}, x_2^{e_2}, g_1''(x_1, \dots, x_n), \dots, g_l''(x_1, \dots, x_n))$$

Continuing this way we get that there is a $d \in \mathbb{Z}^{\geq 1}$ and polynomials $h_1, \dots, h_l \in \mathbb{F}_{p^d}[x_1, x_2, \dots, x_n]$ such that:

$$R \cong \mathbb{F}_{p^d}[x_1, \dots, x_n]/(x_1^{e_1}, \dots, x_n^{e_n}, h_1(x_1, \dots, x_n), \dots, h_l(x_1, \dots, x_n))$$

□

Remark 6.11. *Note that the above proof can be viewed as an algorithm to decompose a finite dimensional commutative ring, given in basis form, into indecomposable rings. It is indeed a deterministic polynomial time algorithm given oracles to integer and polynomial factorization.*

Let us now see a structural property of commutative indecomposable rings.

Lemma 6.12. *For a field $\mathbb{F}$, consider a ring R of the form:*

$$R = \mathbb{F}[x_1, \dots, x_n]/(x_1^{e_1}, \dots, x_n^{e_n}, h_1(x_1, \dots, x_n), \dots, h_\ell(x_1, \dots, x_n))$$

Then,

(i) R is indecomposable.

(ii) R has a unique maximal ideal $\mathcal{M}$ and $\mathcal{M} =$ set of nilpotents of R.

Proof (i). Any element r of R looks like $a_0 + a_1(\overline{x})x_1 + \cdots + a_n(\overline{x})x_n$ where, $a_0 \in \mathbb{F}$ and $a_1(\overline{x}), \ldots, a_n(\overline{x}) \in \mathbb{F}[x_1, \ldots, x_n]$.

Suppose $a_0 = 0$. Since, $x_1^{e_1} = \cdots = x_n^{e_n} = 0$ we have that:

$$\begin{aligned} r^{e_1+\cdots+e_n} &= (a_1(\overline{x})x_1 + \cdots + a_n(\overline{x})x_n)^{e_1+\cdots+e_n} \\ &= 0 \end{aligned}$$

Suppose $a_0 \neq 0$. Let $r_0 := r - a_0$ and $e := e_1 + \cdots + e_n$. Then we have:

$$\begin{aligned} (a_0 + r_0)(a_0^e - a_0^{e-1}r_0 + \cdots + (-1)^{e-1}a_0r_0^{e-1} + (-1)^e r_0^e) &= a_0^{e+1} - (-r_0)^{e+1} \\ &= a_0^{e+1} \qquad [\because r_0^e = 0] \\ &\in \mathbb{F}^* \\ &\Rightarrow r \in R^* \end{aligned}$$

Thus, every element r of R is either a nilpotent or a unit depending upon whether $a_0 = 0$ or not.

Now suppose R is decomposable. By Lemma 6.3 there has to be a nontrivial idempotent $t \in R$. But we have:

$$\begin{aligned} & t^2 = t \\ \Rightarrow \quad & t(t-1) = 0 \\ \Rightarrow \quad & t = 0 \text{ or } 1 \qquad [\because t \text{ or } (t-1) \text{ is a unit}] \end{aligned}$$

This contradiction shows that R is indecomposable. □

Proof (ii). Define a set $\mathcal{M} := R \setminus R^*$. As shown above $\mathcal{M}$ is the set of nilpotents of R and hence is an ideal. $\mathcal{M}$ is maximal because any element outside it is a unit. $\mathcal{M}$ is unique because it contains all the non-units of R. □

Agrawal & Saxena (2005) showed that the problem of graph isomorphism can be reduced to $\mathbb{F}$-algebra isomorphism for any field $\mathbb{F}$. We tag the proof here for the sake of completeness. The reduction gives a way to construct a local commutative $\mathbb{F}$-algebra out of a given graph.

Lemma 6.13. *Graph Isomorphism $\leq_m^P$ $\mathbb{F}$-algebra Isomorphism.*

Proof. The proof involves constructing a local commutative $\mathbb{F}$-algebra. We associate variables to each vertex (x-variable) and capture the “adjacency” in the graph by defining the edges-polynomial – $\sum_{(u,v) \text{ is an edge}} x_u x_v$ – as zero in the ring.

Let G be an undirected graph with n vertices and no self loops. Choose any field $\mathbb{F}$ of characteristic not equal to 2. Define the following commutative $\mathbb{F}$-algebra:

$$R(G) := \mathbb{F}[x_1, \ldots, x_n]/\mathcal{I}$$

where, ideal $\mathcal{I}$ has the following relations:

- x's are nilpotents of degree 2, i.e., for all $i \in [n]$: $x_i^2 = 0$.
- the edges-polynomial is zero, i.e., $\sum_{\substack{1 \le i < j \le n \\ (i,j) \in E(G)}} x_i x_j = 0$.
- all cubic terms are zero, i.e., for all $i, j, k \in [n]$: $x_i x_j x_k = 0$.

Suppose (i_0, j_0) is an edge in G such that $1 \le i_0 < j_0 \le n$. Then the additive structure of the ring is:

$$(R(G), +) = \mathbb{F} \cdot 1 \oplus \bigoplus_{i \in [n]} \mathbb{F} \cdot x_i \oplus \bigoplus_{\substack{i < j \in [n] \\ (i,j) \ne (i_0, j_0)}} \mathbb{F} \cdot (x_i x_j)$$

Thus, the dimension of the ring over $\mathbb{F}$ is $\binom{n+1}{2}$. Multiplication satisfies the associative law simply because the product of any three *variables* (in any order) is zero. Also, $R(G)$ is a local commutative $\mathbb{F}$-algebra.

Observe that if $G \cong G'$ then any graph isomorphism ϕ induces a natural isomorphism between rings $R(G)$ and $R(G')$. So we only have to prove the converse:

Claim 6.14. *Let G and G' be two undirected graphs having no self-loops. Further, assume that graphs G and G' are not a disjoint union of a clique and a set of isolated vertices. Then, $R(G) \cong R(G')$ implies $G \cong G'$.*

Proof of Claim 6.14. Suppose ϕ is an isomorphism from $R(G) \rightarrow R(G')$. Let

$$\phi(x_i) = c_{i,0} + c_{i,1}x_1 + \ldots + c_{i,n}x_n + \text{(quadratic terms)}. \tag{6.15}$$

where all $c_{i,j}$'s in the coefficients are in $\mathbb{F}$.

By squaring the above we get:

$$0 = \phi(x_i^2) = \phi(x_i)^2 = c_{i,0}^2 + \text{(linear and quadratic terms)}$$

which means that $c_{i,0} = 0$. The next observation about ϕ is that there is at most one nonzero linear term in $\phi(x_i)$. Let $C_i = \{j \in [n] \mid c_{i,j} \neq 0\}$ be of size > 1. Then $\phi(x_i)^2 = 0$ gives:

$$\sum_{j<k \in C_i} (2c_{i,j}c_{i,k})x_jx_k \;=\; 0 \text{ in } R(G')$$

We know that in $R(G')$ the quadratic relations are $x_i^2 = 0$ and $\sum_{\substack{1\le i<j\le n\\(i,j)\in E(G')}} x_ix_j = 0$. This means that the above equation holds only if there is a $\lambda \in \mathbb{F}$:

$$\sum_{\substack{1\le j<k\le n\\ j,k\in C_i}} (2c_{i,j}c_{i,k})x_jx_k = \lambda \cdot \sum_{\substack{1\le i<j\le n\\(i,j)\in E(G')}} x_ix_j = 0$$

This equality interpreted in graph terms means that G' is a union of a clique on C_i and a set of $(n-\#C_i)$ isolated vertices (remember that $2 \neq 0$ in $\mathbb{F}$). This we ruled out in the hypothesis, thus size of $C_i \le 1$. If $\#C_i = 0$ then for any j, $\phi(x_ix_j) = 0$ which contradicts the assumption that ϕ is an isomorphism. Thus, for all $i \in [n]$, $\#C_i = 1$. Define a map $\pi : [n] \to [n]$ such that the nonzero linear term occurring in $\phi(x_i)$ is $x_{\pi(i)}$.

Suppose π is not a permutation on $[n]$ then there are $i \neq j$ such that $\pi(i) = \pi(j)$. But then there will exist $a, b \in \mathbb{F}^*$ such that there is no nonzero linear term in $\phi(ax_i + bx_j)$. Whence, we get that $\phi(ax_ix_k + bx_jx_k) = 0$ for all $k \in [n]$ which contradicts the assumption that ϕ is an isomorphism. Hence, π is a permutation on $[n]$. Now look at the action of ϕ on the edges-polynomial:

$$\begin{aligned} 0 &= \phi\left(\sum_{\substack{1\le i<j\le n\\(i,j)\in E(G)}} x_ix_j\right) \\ &= \sum_{\substack{1\le i<j\le n\\(i,j)\in E(G)}} \phi(x_i)\phi(x_j) \\ &= \sum_{\substack{1\le i<j\le n\\(i,j)\in E(G)}} c_{i,\pi(i)}c_{j,\pi(j)}x_{\pi(i)}x_{\pi(j)} \end{aligned}$$

Since the above is a zero relation in the ring $R(G')$, we get that the polynomial $\sum_{\substack{1\le i<j\le n\\(i,j)\in E(G')}} x_ix_j$ divides the above. Hence, $(\pi(i), \pi(j)) \in E(G')$ if $(i,j) \in E(G)$.

By symmetry this shows that π is an isomorphism from $G \to G'$. □

The theorem follows from the claim. □

REMARK 6.16. *The above reduction does not work for fields $\mathbb{F}$ of characteristic 2. We can modify the ring $R(G)$ slightly to make the reduction go through even when $\mathbb{F}$ is a field of characteristic 2. Define the ring $R(G)$ from a graph G, having n vertices, as:*

$$R(G) := \mathbb{F}[x_1, \ldots, x_n]/\mathcal{I}$$

where, ideal $\mathcal{I}$ has the following relations:

(i) x's are nilpotents of degree 3, i.e., for all $i \in [n]$: $x_i^3 = 0$.

(ii) the modified *edges-polynomial is zero, i.e., $\sum_{\substack{1\le i<j\le n \\ (i,j)\in E(G)}} (x_i^2 x_j + x_i x_j^2) = 0$.*

(iii) all quartic *terms are zero, i.e., for all $i, j, k, l \in [n]$: $x_i x_j x_k x_l = 0$.*

A similar proof as above shows that isomorphism problem for rings like $R(G)$ solves the graph isomorphism problem too.

REMARK 6.17. *Note that even if graph G is rigid (i.e., G has no nontrivial automorphism) the ring $R(G)$ has lots of nontrivial automorphisms, for example, $\phi : x_i \mapsto x_i + x_1 x_2$. Thus, unfortunately, this reduction does not reduce the problem of testing rigidity of graphs to testing rigidity of rings.*

Acknowledgements

This work began while the authors were visiting NUS, Singapore in 2004-05. It was also partially supported by research funding from Infosys Technologies Limited, Bangalore.

The second author would like to thank Susanne Pumpluen for many interesting email discussions on cubic forms.

References

M. AGRAWAL & N. SAXENA (2005). Automorphisms of Finite Rings and Applications to Complexity of Problems. In *22nd Annual Symposium on Theoretical Aspects of Computer Science, 2005*, 1–17.

M. AGRAWAL & N. SAXENA (2006). Equivalence of F-Algebras and Cubic Forms. In *23rd Annual Symposium on Theoretical Aspects of Computer Science, 2006*, 115–126.

L. BABAI & E. SZEMERÉDI (1984). On the complexity of matrix group problems. In *25th Annual IEEE Symposium on Foundations of Computer Science, 1984*, 229–240.

E. Bach (1996). Weil bounds for singular curves. *Applicable Algebra in Engineering, Communication and Computing* **7**, 289–298.

W. D. Brownawell (1987). Bounds for the degrees in the Nullstellensatz. *Annals of Maths* **126**, 577–591.

N. Courtois, L. Goubin & J. Patarin (1998). Improved Algorithms for Isomorphisms of Polynomials. In *EUROCRYPT*, 184–200.

J. H. Davenport & J. Heintz (1988). Real quantifier elimination is doubly exponential. *Journal of Symbolic Computation* **5**(1-2), 29–35.

D. K. Harrison (1975). A Grothendieck ring of higher degree forms. *Journal of Algebra* **35**, 123–128.

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

H. Hasse (1921). Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen. PhD thesis.

A. Keet (1993). Higher degree hyperbolic forms. *Quaestiones Mathematicae* **16**(4), 413–442.

J. Köbler, U. Schöning & J. Torán (1993). *The graph isomorphism problem: its structural complexity.* Birkhauser Verlag, Basel, Switzerland.

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

B. R. McDonald (1974). *Finite Rings with Identity.* Marcel Dekker, New York.

H. Minkowski (1885). Untersuchungen über quadratische Formen, Bestimmung der Anzahl verschiedener Formen, welche ein gegebenes Genus enthält. PhD thesis, Königsberg.

J. Patarin (1996). Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): Two new families of asymmetric algorithms. In *Eurocrypt'96*, 33–48. Springer LNCS 1070.

C. Rupprecht (2003). Cohomological invariants for higher degree forms. PhD Thesis, Universität Regensburg.

J. P. Serre (1973). *A course in arithmetic.* Springer-Verlag, New York, NY.

E. Witt & I. Kersten (1998). *Collected Papers - Gesammelte Abhandlungen.* Springer, 1st edition.

Manuscript received March 2, 2007

Manindra Agrawal
Department of Computer Science
IIT Kanpur, India
manindra@cse.iitk.ac.in

Nitin Saxena
CWI
Amsterdam, The Netherlands
nitin.saxena@cwi.nl