Equivalence of $\mathbb{F}$-algebras and cubic forms

Manindra Agrawal and Nitin Saxena *
Department of Computer Science
IIT Kanpur, India
{manindra,nitinsa}@cse.iitk.ac.in

September 15, 2005

Abstract

We study the isomorphism problem of two "natural" algebraic structures – $\mathbb{F}$-algebras and cubic forms. We prove that the $\mathbb{F}$-algebra isomorphism problem reduces in polynomial time to the cubic forms equivalence problem. This answers a question asked in [AS05]. For finite fields $\mathbb{F}$ with $3 \not| (\#\mathbb{F} - 1)$, this result implies that the two problems are infact equivalent. This result also has the following interesting consequence:

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

1 Introduction

For a field $\mathbb{F}$, $\mathbb{F}$-*algebras* are commutative rings of finite dimension over $\mathbb{F}$. One of the fundamental computational problems about $\mathbb{F}$-algebras is to decide, given two such algebras, if they are isomorphic. When $\mathbb{F}$ is an algebraically closed field, it follows from Hilbert's Nullstellensatz [Bro87] that the problem can be decided in **PSPACE**. When $\mathbb{F} = \mathbb{R}$, the problem is in **EEXP** due to the result of Tarski on the decidability of first-order equations over reals [DH88]. When $\mathbb{F} = \mathbb{Q}$, it is not yet known if the problem is decidable. When $\mathbb{F}$ is a finite field, the problem is in $\mathbf{NP} \cap \text{co}\mathbf{AM}$ [KS05]. In all of the above results, we assume that an $\mathbb{F}$-algebra is presented by specifying the product of its basis elements over $\mathbb{F}$.

$\mathbb{F}$-*Cubic Forms* are homogeneous degree 3 polynomials over field $\mathbb{F}$. We call two such forms *equivalent* if an invertible linear transformation on the variables makes one equal to the other. The problem of equivalence of $\mathbb{F}$-cubic forms has a very similar complexity to that of $\mathbb{F}$-algebra isomorphism for different $\mathbb{F}$. This follows from the result of [AS05] showing that $\mathbb{F}$-cubic form equivalence reduces, in polynomial time, to $\mathbb{F}$-algebra isomorphism (in case $\mathbb{F}$ is a finite field, the result holds for $3 \not| (\#\mathbb{F} - 1)$ due to technical reasons).

Both the problems have been well studied in mathematics (for instance see [McD74, Har75, MH74, Rup03]). Over the last ten years, these problems have been found to be useful in computer science as well: [Pat96, CGP98] proposes a cryptosystem based on the hardness of the cubic form equivalence over finite fields, [AS05] show that the Graph Isomorphism problem reduces to both $\mathbb{F}$-algebra isomorphism and $\mathbb{F}$-cubic form equivalence for any $\mathbb{F}$. Therefore, the two problems are of an intermediate complexity but seemingly harder than Graph Isomorphism.

Of the two problems, cubic form equivalence might appear to be an easier problem because, for example, the reduction from Graph Isomorphism to $\mathbb{F}$-algebra isomorphism is simple while

*This work was done while the authors were visiting National University of Singapore. Second author was partially supported by Infosys Technologies Limited, Bangalore.

the reduction to $\mathbb{F}$-cubic form equivalence is very involved. In this paper, we show that this is not the case by exhibiting a reduction from $\mathbb{F}$-algebra isomorphism to $\mathbb{F}$-cubic form equivalence. Apart from showing that the two problems are essentially equivalent, this has other interesting implications. For example, this suggests that $\mathbb{Q}$-algebra isomorphism is decidable because $\mathbb{Q}$-cubic form equivalence appears to be decidable due to the rich structure they possess.

Our reduction is a two step process. We first reduce $\mathbb{F}$-algebras to local $\mathbb{F}$-algebras of a special form. Then we use the properties of these local algebras to show that a "natural" construction of $\mathbb{F}$-cubic forms works.

In section 2 we give an overview of the reduction. In section 3 we reduce general $\mathbb{F}$-algebra isomorphism to the isomorphism problem for local $\mathbb{F}$-algebras and in section 4 we reduce $\mathbb{F}$-algebra isomorphism problem to $\mathbb{F}$-cubic form equivalence.

2 The Basics

An $\mathbb{F}$-algebra R is a commutative ring containing field $\mathbb{F}$. We assume that R is specified in terms of its additive generators over $\mathbb{F}$, say $b_1, \ldots, b_n$. Thus, $R = \mathbb{F}b_1 \oplus \ldots \oplus \mathbb{F}b_n$. To completely specify R, the product of pairs of basis elements is given in terms of a linear combination of b's. Thus, a's $\in \mathbb{F}$ are given in the input such that:

$$\forall i, j, \quad b_i b_j = \sum_{1 \le k \le n} a_{ij,k} b_k \tag{1}$$

Let S be another $\mathbb{F}$-algebra with basis elements $b_1, \ldots, b_n$ satisfying:

$$\forall i, j, \quad b_i b_j = \sum_{1 \le k \le n} a'_{ij,k} b_k$$

To specify an isomorphism ψ from R to S it is sufficient to describe $\psi(b_i)$, for each i, as a linear combination of $b_1, \ldots, b_n$ in S.

The isomorphism problem for these $\mathbb{F}$-algebras is related to polynomial equivalence problem over $\mathbb{F}$ because we can combine equations (1), by using new variables $\overline{z}$ for various i, j, to construct:

$$f_R(\overline{z}, \overline{b}) := \sum_{1 \le i \le j \le n} z_{ij} \left(b_i b_j - \sum_{1 \le k \le n} a_{ij,k} b_k \right) \tag{2}$$

In the above expression we consider z_{ij} and b_i as formal variables and thus f_R is a degree-3 or cubic polynomial. Similarly, construct $f_S(\overline{z}, \overline{b})$ from S. It was shown in [AS05] that equivalence of the polynomials f_R and f_S is sufficient to decide whether R and S are isomorphic. If ϕ is an isomorphism from R to S then it is easy to see that there is a linear invertible map τ on $\overline{z}$ such that: $f_R(\tau\overline{z}, \phi\overline{b}) = f_S(\overline{z}, \overline{b})$. More work is needed to show that if f_R is equivalent to f_S then infact $R \cong S$. The main idea being that any equivalence ψ from f_R to f_S will map b_i's to a linear combination of $\overline{b}$'s and hence ψ becomes our natural candidate for an isomorphism from R to S (for details see [AS05]).

The question we resolve in this paper is whether there is a way to construct *homogeneous* cubic polynomials, *i.e.* cubic forms over $\mathbb{F}$ (henceforth referred to as $\mathbb{F}$-*cubic forms*), such that their equivalence implies the isomorphism of R and S. The cubic form we construct looks like:

$$g_R(\overline{z}, \overline{b}, v) := \sum_{1 \le i \le j \le n} z_{ij} \left(b_i b_j - v \cdot \sum_{1 \le k \le n} a_{ij,k} b_k \right) \tag{3}$$

Here v is a new formal variable. We reduce $\mathbb{F}$-algebra isomorphism to $\mathbb{F}$-cubic form equivalence by first constructing special $\mathbb{F}$-algebras R', S' from R, S (in section 3) and then showing that equivalence of $g_{R'}, g_{S'}$ implies the isomorphism of R, S (in section 4). The idea again is to show that any equivalence ψ from $g_{R'}(\overline{z}, \overline{b}, v)$ to $g_{S'}(\overline{z}, \overline{b}, v)$ sends b_i's to a linear combination of $\overline{b}$'s and thus ψ leads us to an isomorphism from R to S.

3 Local $\mathbb{F}$-algebra Isomorphism Problem

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 an $\mathbb{F}$-algebra this direct product decomposition can be done by factoring polynomials over the field $\mathbb{F}$. Any non-unit r in a local $\mathbb{F}$-algebra is *nilpotent* i.e., there is an m such that $r^m = 0$ (see [McD74]).

In this section we give a many-to-one reduction from $\mathbb{F}$-algebra isomorphism to local $\mathbb{F}$-algebra isomorphism. Moreover, the local $\mathbb{F}$-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 $\mathbb{F}$-algebra to cubic forms in the next section.

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

Proof. Given two $\mathbb{F}$-algebras R and S, [AS05] constructs two cubic polynomials p and q respectively such that p, q are equivalent iff R, S are isomorphic. These polynomials look like (as in equation (2))):

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

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

Let

$$p_3(\overline{z}, \overline{b}) = \sum_{1 \leq i \leq j \leq n} z_{ij} b_i b_j \quad \text{and} \quad p_2(\overline{z}, \overline{b}) = - \sum_{1 \leq i \leq j \leq n} \left(z_{ij} \sum_k a_{ij,k} b_k \right). \tag{4}$$

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 $\mathbb{F}$-algebras:

$$\begin{aligned} R' &:= \mathbb{F}[\overline{z}, \overline{b}, u] / \left\langle p_3, up_2, u^2, \mathcal{I} \right\rangle \\ S' &:= \mathbb{F}[\overline{z}, \overline{b}, u] / \left\langle q_3, uq_2, u^2, \mathcal{I} \right\rangle \end{aligned} \tag{5}$$

where, $\mathcal{I}$ is the ideal generated by all possible products of 4 variables.

Note that all the variables in R', S' are nilpotent and hence the two rings are *local* $\mathbb{F}$-algebras (see [McD74]). 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 3.1.1. *$p(\overline{z}, \overline{b}), q(\overline{z}, \overline{b})$ are equivalent polynomials* iff *$R' \cong S'$.*

Proof of Claim 3.1.1. 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 induces an equivalence from p to q. Note that since $\overline{z}, \overline{b}, u$ are nilpotents in R', therefore $\forall i \leq j \in [n], k \in [n],\ \phi(z_{ij}), \phi(b_i), \phi(u)$ can have no constant term.

Let us see where ϕ sends u. Since $\phi(u)^2 = 0$ in S' while for all i, j: $z_{ij}^2,\ b_i^2 \neq 0$, the linear part of $\phi(u)$ can have no $\overline{z},\ \overline{b}$'s. Thus,

$$\phi(u) \ = \ c \cdot u + (\text{terms of degree 2 or more}), \text{ where } c \in \mathbb{F}. \tag{6}$$

Now by the definition of ϕ:

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

By substituting $u = 0$ we get,

$$\phi(p_3) \mid_{u=0} = \ c_1 q_3 + (\text{terms of degree 4 or more}) \tag{7}$$

Also,

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

Using eqn (6) we deduce that $d_1 = 0$. Thus,

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

Again using eqn (6) we deduce:

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

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

$$\phi(p_2) \mid_{u=0} = \ d_2' \cdot q_2 + (\text{terms of degree 3 or more}) \tag{8}$$

Let ψ be the linear part of ϕ after substituting $u = 0$, that is:

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

By comparing degree 3 and degree 2 terms on both sides of equations (7) and (8) respectively, we get:

$$\psi(p_3) \ = \ c_1 q_3 \tag{9}$$
$$\psi(p_2) \ = \ d_2' q_2 \tag{10}$$

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'':

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

It follows that $\psi''(p) = q$ and thus $p(\overline{z}, \overline{b}), q(\overline{z}, \overline{b})$ are equivalent. □

Thus, $R \cong S$ iff $R' \cong S'$ and hence it is sufficient to study $\mathbb{F}$-algebra isomorphism over local $\mathbb{F}$-algebras of the form (5). □

4 Cubic Form Equivalence

Given two cubic forms $f(\overline{x}), g(\overline{x})$ (homogeneous degree 3 polynomials over a field $\mathbb{F}$) the equivalence problem is to determine whether there is an invertible linear transformation (over the field $\mathbb{F}$) on the variables that makes the two forms equal. When field $\mathbb{F}$ is finite, cubic form equivalence is in $\mathbf{NP} \cap \text{co}\mathbf{AM}$. For an infinite field $\mathbb{F}$ we expect the problem to be *decidable* but it is still open for $\mathbb{F} = \mathbb{Q}$.

Here we show that $\mathbb{F}$-algebra isomorphism reduces to cubic form equivalence. This improves the result of [AS05] that graph isomorphism reduces to cubic form equivalence. The proof involves the use of similar cubic forms as constructed in [AS05] but here we heavily use the properties of the intermediate local $\mathbb{F}$-algebras to study the equivalences of these cubic forms.

Theorem 4.1. *$\mathbb{F}$-algebra isomorphism $\leq_m^P$ $\mathbb{F}$-cubic form equivalence.*

Proof. Given $\mathbb{F}$-algebras $R,\ S$ we will construct cubic forms $\phi_R,\ \phi_S$ 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 thm 3.1) and then the cubic forms out of these local algebras (similar to [AS05]).

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

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

Consider the following local ring R' constructed from R:

$$R' \ := \ \mathbb{F}[\overline{z}, \overline{b}, u] / \left\langle p_3, up_2, u^2, \mathcal{I} \right\rangle \tag{11}$$

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

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

A natural set of generators of the ring R' is: $\{1\} \cup \{z_{ij}\}_{1 \leq i \leq j \leq n} \cup \{b_i\}_{1 \leq i \leq n} \cup \{u\}$. 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 and up_2. (12)

For simplicity denote 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:

$$\phi_R(\overline{y}, \overline{c}, v) := \sum_{1 \leq i \leq j \leq d} y_{ij} c_i c_j - v \sum_{1 \leq i \leq j \leq d} y_{ij} \left(\sum_{k=1}^{d} \tilde{a}_{ij,k} c_k \right) \tag{13}$$

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

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 bound the number of v terms in ϕ_R.

Claim 4.1.1. *The number of surviving v terms in the rhs of eqn (13) is $< (3d-6)$.*

Proof of Claim 4.1.1. The number of surviving v terms in the rhs of eqn (13) is:

$$\leq \#\left\{(k,l) \mid 1 \leq k \leq l \leq d,\ c_k c_l \neq 0 \text{ in } R'\right\} + 3\left[\#(\text{terms in } p_3) + \#(\text{terms in } p_2)\right]$$

The first expression above accounts for all the relations in R' of the form $c_k c_l = c_m$. 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 $x_i x_j x_k$ in p_3, up_2 can create v terms in atmost 3 ways: from $(x_i)\cdot(x_j x_k)$ or $(x_j)\cdot(x_i x_k)$ or $(x_k)\cdot(x_i x_j)$.

$$\begin{aligned}
\leq\ & \#\left\{(k,l) \mid k \leq l,\ c_k, c_l \in \{x_i\}_{1\leq i\leq g}\right\} + \#\left\{(k,l) \mid\ c_k \in \{x_i\}_{1\leq i\leq g}, c_l = u\right\} \\
& + \#\left\{(k,l) \mid\ c_k \in \{x_i\}_{1\leq i\leq g}, c_l \in \{x_i x_j\}_{1\leq i\leq j\leq g}\right\} \\
& + \#\left\{(k,l) \mid\ c_k \in \{x_i\}_{1\leq i\leq g}, c_l \in \{u x_i\}_{1\leq i\leq g}\right\} \\
& + \#\left\{(k,l) \mid\ c_k = u, c_l \in \{x_i x_j\}_{1\leq i\leq j\leq g}\right\} + 3\left[\#(\text{terms in } p_3) + \#(\text{terms in } p_2)\right] \\
\leq\ & \left[\binom{g+1}{2} + g + g\cdot\binom{g+1}{2} + g^2 + \binom{g+1}{2}\right] + 3\left[\binom{n+1}{2} + \binom{n+1}{2}\cdot n\right]
\end{aligned}$$

Note that the dominant term in the above expression is $\frac{g^3}{2}$ while in that of d it is $\frac{g^3}{6}$. Computation gives the following bound:

$$< (3d-6)$$

□

Construct a cubic form ϕ_S from ring S in a way similar to that of eqn (13).

$$\phi_S(\overline{y}, \overline{c}, v) := \sum_{1\leq i\leq j\leq d} y_{ij} c_i c_j - v \sum_{1\leq i\leq j\leq d} y_{ij} \left(\sum_{k=1}^{d} \tilde{e}_{ij,k} c_k\right) \tag{14}$$

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

The following claim is what we intend to prove now.

Claim 4.1.2. *$\phi_R(\overline{y}, \overline{c}, v)$ is equivalent to $\phi_S(\overline{y}, \overline{c}, v)$ iff $R' \cong S'$ iff $R \cong S$.*

Proof of Claim 4.1.2. 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:

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

$$= \sum_{1\leq i\leq j\leq d} y_{ij} c_i c_j - v \sum_{1\leq i\leq j\leq d} y_{ij} \left(\sum_{k=1}^{d} \tilde{e}_{ij,k} c_k\right) \tag{15}$$

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, $\psi(c_i) = \sum_j \alpha_{i,j} c_j + \sum_{j,k} \beta_{i,jk} y_{jk} + \gamma_i v$ where α, β, γ's $\in \mathbb{F}$. For obvious reasons we will call the expression $\sum_{j,k} \beta_{i,jk} y_{jk}$ as the $\overline{y}$ *part of* $\psi(c_i)$. $\overline{y}$ parts of $\psi(v)$ and $\psi(y_{ij})$ 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 the lhs of eqn (15) we mean expressions of the form $\psi(y_{ls})\psi(c_l)\psi(c_s)$ or $\psi(v)\psi(y_{ls})\psi(c_t)$ where $l, s, t \in [d]$. Let T_0 be the set of all terms. There are atleast $d + (d-1) + (d-2) = (3d-3)$ terms on the lhs of eqn (15) that have an occurrence of $\psi(c_i), \psi(c_j)$ or $\psi(c_k)$, denote this set of terms by T_1. Let the set of the remaining terms be T_2. Let us build a maximal set Y of linearly independent $\overline{y}$ parts and a set T of 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. It is easy to see (by claim 4.1.1) that:

$$\begin{aligned} \#Y &\leq 3 + \#T_2 \\ &< 3 + \left[\binom{d+1}{2} + (3d-6) - (3d-3) \right] = \binom{d+1}{2} = \#\left\{y_{ij}\right\}_{1 \leq i \leq j \leq d} \end{aligned} \tag{16}$$

Now apply an invertible linear transformation τ on the $\overline{y}$ variables in equation (15) such that all the $\overline{y}$ parts in Y are mapped to *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, the lhs of eqn (15), after applying τ and the substitutions, is completely in terms of $\overline{c}, v$ while the rhs still has atleast one free $\overline{y}$ variable (as we fixed only $\#\tau(Y) < \#\left\{y_{ij}\right\}_{1 \leq i \leq j \leq d}$ $\overline{y}$ 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 $\{\psi(y_{ij})\}_{1 \leq i \leq j \leq d}$ with the extra condition that $\overline{y}$ parts in Y are also linearly independent from that 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 $\overline{y}$ variables in equation (15) such that:

- the $\overline{y}$ parts of $\tau_1 \circ \psi(c_1), \ldots, \tau_1 \circ \psi(c_d), \tau_1 \circ \psi(v)$ have 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 $\tau_1 \circ \psi(y_{ij})$ has *only* y_{ij}.
- 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_{ij}, for $(i, j) \neq (i_1, j_1), (i_2, j_2)$, on both sides of the equation:

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

$$= \sum_{1 \leq i \leq j \leq d} y_{ij} (\text{quadratic terms in } \overline{c}, v) \tag{17}$$

For any c_i, choose distinct basis elements c_j, c_k and c_l satisfying $c_ic_j = c_ic_k = c_ic_l = 0$ in R' (note that there is an ample supply of such j, k, l), such that by comparing coefficients of y_{ij}, y_{ik}, y_{il} (assumed to be other than $y_{i_1j_1}, y_{i_2j_2}$) on both sides of equation (17) we get:

$$\begin{aligned}
\psi'(c_ic_j) + (e_{ij,1}E_1 + e_{ij,2}E_2) &= (\text{quadratic terms in } \overline{c}, v) \\
\psi'(c_ic_k) + (e_{ik,1}E_1 + e_{ik,2}E_2) &= (\text{quadratic terms in } \overline{c}, v) \\
\psi'(c_ic_l) + (e_{il,1}E_1 + e_{il,2}E_2) &= (\text{quadratic terms in } \overline{c}, v)
\end{aligned} \tag{18}$$

where, $e_{ij,1}, e_{ij,2}, e_{ik,1}, e_{ik,2}, e_{il,1}, e_{il,2} \in \mathbb{F}$ and

$$E_1 = \psi'(c_{i_1}c_{j_1}) - \psi'(v)\sum_{k=1}^{d} \tilde{a}_{i_1j_1,k}\psi'(c_k)$$

$$E_2 = \psi'(c_{i_2}c_{j_2}) - \psi'(v)\sum_{k=1}^{d} \tilde{a}_{i_2j_2,k}\psi'(c_k)$$

Now there exist $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}$ (not all zero) such that equations (18) can be combined to get rid of E_1, E_2 and get:

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

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

$$\forall i, \quad \psi'(c_i) = (\text{linear terms in } \overline{c}, v) \tag{19}$$

This means that the $\overline{y}$-variables are only in $\psi'(y_{ij})$s and possibly $\psi'(v)$. Again apply an invertible linear transformation τ_2 on the $\overline{y}$-variables in equation (17) such that $\tau_2 \circ \psi'(v)$ has only $y_{i_0j_0}$ in the $\overline{y}$ part and except for one tuple (i_0, j_0), the $\overline{y}$ part of $\tau_2 \circ \psi'(y_{ij})$ has *only* y_{ij} for all other (i, j). For clarity let $\psi'' := \tau_2 \circ \psi'$. Our equation now is:

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

$$= \sum_{1\le i\le j\le d} y_{ij}(\text{quadratic terms in } \overline{c}, v) \tag{20}$$

By comparing coefficients of y_{ij} (other that $y_{i_0j_0}$) on both sides of the above equation we get:

$$\left(\psi''(c_ic_j) - \psi''(v)\sum_{k=1}^{d}\tilde{a}_{ij,k}\psi''(c_k)\right) + e\left(\psi''(c_{i_0}c_{j_0}) - \psi''(v)\sum_{k=1}^{d}\tilde{a}_{i_0j_0,k}\psi''(c_k)\right)$$

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

Pick i, j such that $\sum_{k=1}^{d}\tilde{a}_{ij,k}c_k \neq 0$ in R'. Now if $\psi''(v)$ has a nonzero $y_{i_0j_0}$ term then by comparing coefficients of $y_{i_0j_0}$ on both sides of the above equation we deduce:

$$\sum_{k=1}^{d}\tilde{a}_{ij,k}\psi''(c_k) + e\sum_{k=1}^{d}\tilde{a}_{i_0j_0,k}\psi''(c_k) = 0 \tag{21}$$

But again we can pick i, j suitably so that $\left(\sum_{k=1}^{d} \tilde{a}_{ij,k} c_k\right) \notin \left\{0,\ -e\sum_{k=1}^{d} \tilde{a}_{i_0 j_0,k} c_k\right\}$ and hence avoiding equation (21) 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

$$\forall i, \quad \psi''(c_i) = (\text{linear terms in } \overline{c}, v) \tag{22}$$

Since $\overline{y}$-variables are present only in $\psi''(y_{ij})$'s, comparing coefficients of y_{ij}'s on both sides of equation (20) gives:

$$\forall i, j, \quad \psi''(c_i c_j) - \psi''(v)\sum_{k=1}^{d} \tilde{a}_{ij,k}\psi''(c_k) = (\text{quadratic terms in } \overline{c}) - v(\text{linear terms in } \overline{c}) \tag{23}$$

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 (23):

$$\psi''(c_i)^2 = (\text{quadratic terms in } \overline{c}) - v(\text{linear terms in } \overline{c}) \tag{24}$$

Now if $\psi''(c_i)$ has a nonzero v term then there will be a v^2 term above on the 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 $c_i^2 = \sum_{k=1}^{d} \tilde{a}_{ii,k} c_k$ in R' where the c_k's with nonzero $\tilde{a}_{ii,k}$ satisfy $c_k^2 = 0$. This happens because the way $\overline{c}$'s are defined in eqn (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 the lhs of the equation:

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

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 the $\overline{y}$'s we have what we intended to prove from the beginning (recall eqn (15)):

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

and

$$\forall i, \quad \psi(c_i) = (\text{linear terms in } \overline{c}) \tag{25}$$

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 (15) such that the $\overline{y}$ part of $\tau_3 \circ \psi(y_{ij})$ has *only* y_{ij} 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_{ij} on both sides of the eqn (15) after applying τ_3 we get:

$$\forall i, j, \quad \tau_3 \circ \psi(c_i c_j) - \tau_3 \circ \psi(v)\sum_{k=1}^{d} \tilde{a}_{ij,k}\tau_3 \circ \psi(c_k) = \sum_{i \leq j} \lambda_{ij}\left(c_i c_j - v\sum_{k=1}^{d} \tilde{e}_{ij,k} c_k\right) \tag{26}$$

for some $\lambda_{ij} \in \mathbb{F}$.

Substitute $v = 1$ in the expression for $\tau_3 \circ \psi(v) = \gamma_{vv} v + \sum_i \alpha_{vi} c_i$ and denote the result by m. Observe that $\gamma_{vv} \neq 0$ 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 eqn (26) we get:

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

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

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

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 this means that $\sum_{i=1}^{d} \lambda_i c_i = 0$ in R'. Thus, showing that Ψ is an *injective* map from R' to S'. Since R' and S' are of the same dimension over $\mathbb{F}$, Ψ becomes *surjective* too. Thus, Ψ is an isomorphism from R' to S'. □

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

5 Conclusion

In this paper we gave a reduction from $\mathbb{F}$-algebra isomorphism to $\mathbb{F}$-cubic form equivalence for any field $\mathbb{F}$. Thus, cubic form equivalence, in addition to being a natural algebraic problem, is also directly related to isomorphism problems for $\mathbb{F}$-algebras and graphs. We would like to pose the following questions related to cubic forms:

- Is there a subexponential algorithm for $\mathbb{F}$-cubic forms for any field $\mathbb{F}$? Such an algorithm will result in a subexponential time algorithm for Graph Isomorphism.
- Is $\mathbb{Q}$-cubic form equivalence decidable? This will make $\mathbb{Q}$-algebra isomorphism decidable too.

References

[AS05] M. Agrawal, N. Saxena. *Automorphisms of Finite Rings and Applications to Complexity of Problems.* STACS'05, Springer LNCS 3404, 2005, 1-17.

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

[CGP98] N. Courtois, L. Goubin, J. Patarin. *Improved Algorithms for Isomorphism of Polynomials.* Eurocrypt'98, Springer LNCS 1403, 1998, 184-200.

[DH88] J. Davenport, J. Heintz. *Real Quantifier Elimination Is Doubly Exponential.* Journal of Symbolic Computation, 5, 1988, 29-35.

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

[KS05] N. Kayal, N. Saxena. *On the Ring Isomorphism and Automorphism Problems.* IEEE Conference on Computational Complexity, 2005, 2-12.

[Lang] S. Lang. *Algebra.* 3rd edition, Addison Wesley.

[McD74] Bernard R. McDonald. *Finite Rings with Identity.* Marcel Dekker, Inc., 1974.

[MH74] Y. I. Manin, M. Hazewinkel. *Cubic forms: algebra, geometry, arithmetic.* North-Holland Publishing Co., Amsterdam, 1974.

[Pat96] J. Patarin. *Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): Two new families of asymmetric algorithms.* Eurocrypt'96, Springer LNCS 1070, 1996, 33-48.

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

[Sch88] U. Schoning. *Graph isomorphism is in the low hierarchy.* Journal of Computer and System Science, **37**, 1988, 312-323.