Infinitude of equivalence classes of Cubic forms over Complex

Vishwas Bhargava

July 10, 2016

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

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

A homogeneous cubic polynomial is called a *cubic form*. The problem of *deciding* whether two cubic forms are equivalent has a **PSPACE** algorithm over an algebraically closed field like $\mathbb{C}$ by using Hilberts Nullstellensatz and over $\mathbb{Q}$ this problem is not even known to be computable.

This problem is at least as hard as Graph-Isomorphism problem and also a fairly general case of ring isomorphism commutative $\mathbb{F}$-algebra isomorphism reduces to cubic forms equivalence.

In Cubic form equivalence over $\mathbb{C}$ following facts are easy to see :

- Bivariate cubic forms have finitely many equivalence classes.
- Trivariate trinomials have finitely many equivalence classes.(This can be seen just by scaling of variables.)

Now a natural question which comes to mind is are there infintely many equivalence(which looks believable) and can we prove it ? I gave an elementary prove of the same. The proof is elementary yet beautiful.

Motivating Polynomial

Consider the following polynomial family $f_k(x, y, z) = x^3 + y^3 + z^3 + kxyz$ When we apply an invertible linear transformation on this polynomial family it looks that at least one monomial will be introduced and so I conjectured

that $f_{k_1} \nsim f_{k_2}$ for $k_1 \neq k_2$, and this conjecture stood tall on computational verification for k upto 35000. This family has some nice properties firstly it is a symmetric polynomial family and second is stated below.

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

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

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

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

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

After simplifying it we get that

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

It tells us that

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

$$k = -3a'b' \tag{2}$$

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

Hessian Matrix and Polynomial Equivalence

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

Definition 0.0.1. (**Hessian Matrix**) For a polynomial $f(\overline{x}) \in \mathbb{F}[\overline{x}]$, the Hessian matrix $H_f(\overline{x}) \in (\mathbb{F}[\overline{x}])^{n \times n}$ is defined as follows:

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

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

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

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

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

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

Theorem. *[Kayal, 2011] Let $f(\overline{x}) \in \mathbb{F}[\overline{x}]$ be a n-variate polynomial and $\tau \in \mathbb{F}^{n \times n}$ be a linear transformation. Let $F(\overline{x}) \stackrel{def}{=} f(\tau \cdot \overline{x})$. Then,*

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

In particular,

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

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

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

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

$$\frac{\partial F(\overline{x})}{\partial x_i} = \sum_{k=1}^{n} a_{ki} \frac{\partial f(\tau \cdot \overline{x})}{\partial x_k} \tag{3}$$

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

$$\frac{\partial^2 F(\overline{x})}{\partial x_i \cdot \partial x_j} = \sum_{k=1}^{n} a_{ki} \cdot \left(\sum_{l=1}^{n} a_{lj} \frac{\partial^2 f(\tau \cdot \overline{x})}{\partial x_k \cdot \partial x_l} \right) \tag{4}$$

$$\frac{\partial^2 F(\overline{x})}{\partial x_i \cdot \partial x_j} = \sum_{k \in [n], l \in [n]} a_{ki} \cdot \frac{\partial^2 f(\tau \cdot \overline{x})}{\partial x_k \cdot \partial x_l} \cdot a_{lj} \tag{5}$$

Putting these equations in the matrix form we will get

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

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

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

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

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

□

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

Lemma 0.0.1. If $f(\overline{x}), g(\overline{x}) \in \mathbb{F}[\overline{x}]$ are two n-variate polynomials then over $\mathbb{F} = \mathbb{C}$, we have

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

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

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

which is nothing but

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

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

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

for some τ'. □

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

Lemma 0.0.2. There will always exist a polynomial f_k such that $H^{-1}(f_m) = f_k$.

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

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

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

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

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

$H(f_k) = f_m$ if

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

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

$$k^3 + 3mk^2 + 108 = 0 \tag{6}$$

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

Theorem 1. *In case of trivariate quadnomial cubic forms equivalence over $\mathbb{C}$ there exists infinitely many equivalence classes.*

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

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

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

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

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

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

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

Now the polynomial $H^{-1}(f_k) = f_m$, where m is the root of the equation $m^3 + 3km^2 + 108 = 0$.
Now from the lemma 5.5 we can say that

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

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

$$H^{-1}(f_{-3}) \nsim H^{-1}(f_k) \text{ except } H^{-1}(f_{-3}) \tag{7}$$

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

$$H^{-1}(H^{-1}(f_{-3})) \nsim H^{-1}(H^{-1}(f_k)) \text{ except } H^{-1}(H^{-1}(f_{-3})) \tag{8}$$

$$\implies H^{-2}(f_{-3}) \nsim H^{-2}(f_k) \tag{9}$$

Using the inverse of Hessian repeatedly we will get an infinite sequence $H^{-i}(f_{-3}), i \geq 0, i \in \mathbb{Z}$, if we solve the equation $m^3 + 3km^2 + 108 = 0$ with $k = -3$ as initial value of k. Now take one root of the above equation and assume it as new value of k. Continue the same process with the new k. This sequence will go infinite times if we can show that in this process k can never repeat. We will show that this sequence is infinite later.
Now we can say that we got infinitely many equivalence classes if any polynomial in the sequence $H^{-i}(f_{-3})$ is not equivalent to the other polynomial except itself. For the sake of contradiction assume that in this sequence two different polynomials are equivalent that is $f_{k_1} \sim f_{k_2}$ for some $k_1 \neq k_2$. From the sequence construction we can say that $f_{k_1} = H^{-i}(f_{-3})$ for some i and $f_{k_2} = H^{-j}(f_{-3})$ for some $j \neq i$. Now we know that from lemma 5.5 that

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

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

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

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

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

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

$$m = 0.160864727636919 + 2.42255290483452i$$

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

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

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

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

which shows

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

taking absolute value of both sides, we get

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

by the triangular inequality, we can write

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

rearranging the variables, we get

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

Now if we can show that $\left|\frac{108}{m_{i+1}^2}\right| \leq 1$ then it shows that in the next iteration the absolute value of m_{i+1} gets nearly tripled of the previous value m_i, suggesting that it will be a geometric progression and hence every time the value of k will be different (nearly triple) of the previous value, hence this process will go infinite times and it will never repeat.
We will show that $\left|\frac{108}{m_{i+1}^2}\right| \leq 1$ by induction.
Base Case : For the above equation we know that $m_2 = -18.3217294552738$, hence $\left|\frac{108}{m_{i+1}^2}\right| \leq 1$.
Induction Hypothesis : Let us assume that this is true for m_i for some i, that is we have $\left|\frac{108}{m_i^2}\right| \leq 1$.
Induction step : Here we have to show that $\left|\frac{108}{m_{i+1}^2}\right| \leq 1$. From the inductive hypothesis, we know that $\left|\frac{108}{m_i^2}\right| \leq 1 \implies |108| \leq |m_i^2| \implies 108 \leq m_i^2 \implies 6\sqrt{3} \leq |m_i|$. Since m_{i+1} is the new root of the above equation and m_i is the new k at that time so we can write

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

we can write it as

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

now take the absolute value of both sides, we get

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

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

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

after rearranging it, it will be

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

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

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

Bibliography

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