On the centers of higher degree forms

Nitin Saxena[a*]

[a]Department of Computer Science, IIT Kanpur, India
nitinsa@cse.iitk.ac.in

Let Θ be a symmetric d-linear form on a vector space V of dimension n over a field K. Its center, $\mathrm{Cent}(V, \Theta)$, is the analog of the space of symmetric matrices for a bilinear form. If $d > 2$, the center is a commutative subalgebra of $\mathrm{End}_K(V)$. It was conjectured in [4] that the center has dimension at most n and a proof was given for $n \leq 5$. We construct counter examples to this conjecture. We give an infinite family of *cubic* forms $\{(V_r, \Theta_r)\}_{r\geq 3}$ such that for any $\epsilon \in (0, 1)$ there exists $r_0(\epsilon)$ having the property:

$$\text{for all } r \geq r_0(\epsilon),\ \dim_K \mathrm{Cent}(V_r, \Theta_r) > (1 + \epsilon) \cdot \dim_K V_r$$

1. Preliminaries

We first collect the definitions related to d-linear forms following [4]. Suppose V is a vector space over a field K. A symmetric 2-linear form $\Theta : V \times V \to K$ has a geometrical interpretation as an inner product on V. The 2-linear form Θ induces a quadratic form $\phi : V \to K$ defined by: $\phi(v) = \Theta(v, v)$ and conversely a quadratic form ϕ induces a 2-linear form: $2\Theta(u, v) = \phi(u + v) - \phi(u) - \phi(v)$ when char $K \neq 2$. These concepts can be generalized to higher dimensions d.

Definition 1.1. A *d-linear space* over K is a pair (V, Θ) where V is a finite dimensional K-vector space and $\Theta : V \times \cdots \times V \to K$ is a symmetric d-linear form. That is, Θ is K-linear in each of its slots and it is invariant under all permutations of the slots.

When char $K = 0$ or char $K > d$, these d-linear spaces are in one-one correspondence to d-homogeneous polynomials in $K[x_1, \ldots, x_n]$ where $n := \dim_K V$. This can be seen by fixing a K-basis $e_1, \ldots, e_n$ of V and defining $\phi(v) := \Theta(v, \ldots, v)$ where $v = x_1e_1 + \ldots + x_ne_n$, then ϕ is a d-homogeneous polynomial in $K[x_1, \ldots, x_n]$.

Two d-linear spaces (V, Θ), (V', Θ') are *isomorphic* if there is an invertible linear map $t : V \to V'$ such that $\Theta'(tv_1, \ldots, tv_d) = \Theta(v_1, \ldots, v_d)$ for every $v_1, \ldots, v_d \in V$.

A notion of *decomposability* of d-linear spaces can be defined as follows:

Definition 1.2. The *orthogonal sum* $(V_1, \Theta_1) \perp (V_2, \Theta_2)$ of two spaces is the d-linear space on $V_1 \oplus V_2$ with form $\Theta_1 \perp \Theta_2$ defined as:

$$(\Theta_1 \perp \Theta_2)(u_1 + v_1, \ldots, u_d + v_d) := \Theta_1(u_1, \ldots, u_d) + \Theta_2(v_1, \ldots, v_d)$$

*This work was done while the author was visiting School of Computing, National University of Singapore.

where, $u_i \in V_1$ and $v_i \in V_2$. A d-linear space (V, Θ) is *decomposable* if $(V, \Theta) \cong (V_1, \Theta_1) \perp (V_2, \Theta_2)$ for some *nonzero* spaces $(V_1, \Theta_1), (V_2, \Theta_2)$.

On the level of homogeneous polynomials the sum $\Theta_1 \perp \Theta_2$ corresponds to $(\phi_1 \perp \phi_2)(X_1, X_2) = \phi_1(X_1) + \phi_2(X_2)$ where X_1, X_2 are disjoint set of variables.
A d-homogeneous polynomial ϕ whose number of variables cannot be reduced by a linear change of variables corresponds to a *regular* d-linear space (V, Θ).

Definition 1.3. (V, Θ) is said to be *regular* if $\Theta(v, V, \ldots, V) = 0$ implies $v = 0$. The expression $\Theta(v, V, \ldots, V) = 0$ is a shorthand for: $\forall v_2, \ldots, v_d \in V,\ \Theta(v, v_2, \ldots, v_d) = 0$.

The notion of symmetric matrices for bilinear forms generalizes to the *center* for higher dimensional forms.

Definition 1.4. The *center* $\mathrm{Cent}(V, \Theta)$ of a d-linear space (V, Θ) is defined as:

$$\{t \in \ \mathrm{End}_K(V) \mid \Theta(tv_1, v_2, \ldots, v_d) = \Theta(v_1, tv_2, v_3, \ldots, v_d) \text{ for all } v_1, \ldots, v_d \in V\}.$$

The following properties of the center were first proved in [2]:

Lemma 1.5. *Suppose (V, Θ) is a regular d-linear space where $d \geq 3$.*

(1) Cent(V, Θ) is a commutative K-subalgebra of End$_K V$.

(2) (V, Θ) is indecomposable if and only if Cent(V, Θ) is local.

The following property of the center (see page 1277 of [3]) is useful in computing the structure. We provide the proof for the sake of completeness.

Lemma 1.6. *Let (V, Θ) be a d-linear space and let $n :=$ dim$_K V$. Then*

$$Cent(V, \Theta) \cong \left\{M \in K^{n \times n} | (JM)^T = JM\right\}$$

where $J = \left(\frac{\partial^2 f}{\partial x_i \partial x_j}\right)$ is the Hessian matrix of the d-homogeneous polynomial $f(x_1, \ldots, x_n)$ corresponding to (V, Θ).

Proof. Let us fix a K-basis $\{e_i\}_{1 \leq i \leq n}$ of V such that e_i is an $n \times 1$ vector having all zeros except a 1 at the i-th position. Suppose $t \in \mathrm{Cent}(V, \Theta)$ then by definition for all $1 \leq i, j \leq n$:

$$\forall v_3, \ldots, v_d \in V,\ \Theta(te_i, e_j, v_3, \ldots, v_d) = \Theta(e_i, te_j, v_3, \ldots, v_d) \tag{1}$$

Let M be a matrix whose i-th column is equal to te_i, for all $1 \leq i \leq n$. Thus, LHS of equation (1) is

$$\Theta\left(\left(\sum_{l=1}^{n} M_{li} e_l\right), e_j, v_3, \ldots, v_d\right) = \sum_{l=1}^{n} M_{li} \Theta(e_l, e_j, v_3, \ldots, v_d)$$

Now $\Theta(e_l, e_j, v_3, \ldots, v_d)$ is a $(d-2)$-linear form treating the first 2 arguments fixed and the last $(d-2)$ taking values from V. It can be easily verified that this $(d-2)$-linear form corresponds to the $(d-2)$-homogeneous polynomial:

$$\frac{1}{d(d-1)} \cdot \frac{\partial^2 f}{\partial x_l \partial x_j}$$

Thus, the LHS of equation (1) corresponds to the following $(d-2)$-homogeneous polynomial:

$$\frac{1}{d(d-1)} \cdot \sum_{l=1}^{n} M_{li} \frac{\partial^2 f}{\partial x_l \partial x_j} = \frac{1}{d(d-1)} \cdot \sum_{l=1}^{n} M_{li} J_{jl} = \frac{1}{d(d-1)} \cdot (JM)_{ji}$$

Similarly, the RHS of equation (1) corresponds to $\frac{1}{d(d-1)} \cdot (JM)_{ij}$. Since equation (1) holds for all i, j we get $(JM)^T = JM$. □

It was conjectured in [4] that if $d \geq 3$ and (V, Θ) is a regular d-linear space over the field K then $\dim_K \mathrm{Cent}(V, \Theta) \leq \dim_K V$. In this paper we construct an infinite family of *cubic* forms (*i.e.* for $d = 3$) which are exceptions to the conjecture. In these counter examples the lower bound on the fraction $\frac{\dim_K \mathrm{Cent}(V,\Theta)}{\dim_K V}$ can be made arbitrarily close to 2.

2. The Counter Example

The following theorem summarizes the construction of the counter examples.

Theorem 2.1. *Let $r \geq 3$. Consider the cubic polynomial:*

$$f(\overline{z}, \overline{b}) := \sum_{1 \leq i \leq j \leq r} z_{i,j} b_i b_j \ .$$

Let (V, Θ) be the 3-linear space corresponding to f over a field K with char$(K) \neq 2, 3$. Then

(1) (V, Θ) is regular and indecomposable.

(2) $n := dim_K V = r + \frac{r(r+1)}{2}$ and $dim_K Cent(V, \Theta) \geq r^2 + 1$. Thus,

$$\frac{dim_K Cent(V, \Theta)}{dim_K V} \geq 2 - \frac{6r-2}{r^2+3r} > 1 \ .$$

Proof. Let $s := \frac{r(r+1)}{2}$. We will use lemma 1.6 to compute the structure of $\mathrm{Cent}(V, \Theta)$. As in the proof of lemma 1.6, let $J = \left(\frac{\partial^2 f}{\partial x_i \partial x_j}\right)$ be the Hessian matrix of f. Fix a K-basis of V as $e_i =$ (an $n \times 1$ vector with i-th entry 1 and the rest zeros) and for any $t \in \mathrm{End}_K(V)$ define a corresponding matrix M whose i-th column is te_i for all $1 \leq i \leq n$. Note that the following relation holds: for any $v \in V$, $tv = Mv$. We will show that if $t \in \mathrm{Cent}(V, \Theta)$ then M is of a very special form:

Claim 2.1.1. *If $t \in Cent(V,\Theta)$ then for some $c \in K,\ A \in K^{s\times r}$*

$$M = cI + \begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix} .$$

Consequently, (V,Θ) is indecomposable and $Cent(V,\Theta) \cong K \oplus \mathcal{N}$ where $\mathcal{N}$ is a commutative nil algebra in which product of any two elements vanish.

Proof of Claim 2.1.1. From the definition, $t \in$ Cent(V,Θ) iff

$$\Theta\left(M\begin{pmatrix} z_{1,*} \\ b_{1,*}\end{pmatrix}, \begin{pmatrix} z_{2,*} \\ b_{2,*}\end{pmatrix}, \begin{pmatrix} z_{3,*} \\ b_{3,*}\end{pmatrix}\right) = \Theta\left(\begin{pmatrix} z_{1,*} \\ b_{1,*}\end{pmatrix}, M\begin{pmatrix} z_{2,*} \\ b_{2,*}\end{pmatrix}, \begin{pmatrix} z_{3,*} \\ b_{3,*}\end{pmatrix}\right) \qquad (2)$$

where for all $1 \le i \le 3$, $z_{i,*}$ represents the column vector (having s entries):

$$\begin{pmatrix} z_{i,1,1} & z_{i,1,2} & \cdots & z_{i,r-1,r} & z_{i,r,r}\end{pmatrix}^T$$

and similarly $b_{i,*}$ represents the column vector (having r entries):

$$\begin{pmatrix} b_{i,1} & \cdots & b_{i,r}\end{pmatrix}^T$$

Remember that Θ is the natural 3-linear form obtained from f, so we intend to associate the $z_{i,j,k}$ component to the $z_{j,k}$ variable of f and the $b_{i,j}$ component to the b_j variable. In equation form this yields:

$$\Theta(v,v,v) = f(\overline{z},\overline{b}) = \sum_{1\le i\le j\le r} z_{i,j}b_ib_j$$

$$\text{where } v := z_{1,1}e_1 + z_{1,2}e_2 + \ldots + z_{r-1,r}e_{s-1} + z_{r,r}e_s + b_1e_{s+1} + \ldots + b_re_n\ .$$

Let us compare the coefficient of $z_{3,i,i}$ on both sides of equation (2) to get:

$$\frac{1}{3}\tau(b_{1,i})b_{2,i} = \frac{1}{3}b_{1,i}\tau(b_{2,i}) \text{ where } \tau(.) \text{ is the effect of } M.$$

As this equation holds for all values of $z_{1,*},\ b_{1,*},\ z_{2,*},\ b_{2,*}$ we obtain that $\tau(b_{1,i}) = c_ib_{1,i}$ for some $c_i \in K$. Now compare the coefficients of $z_{3,i,j}$ for $i < j$ on both sides of equation (2):

$$\frac{1}{6}(\tau(b_{1,i})b_{2,j} + \tau(b_{1,j})b_{2,i}) = \frac{1}{6}(b_{1,i}\tau(b_{2,j}) + b_{1,j}\tau(b_{2,i}))$$
$$\Rightarrow c_ib_{1,i}b_{2,j} + c_jb_{1,j}b_{2,i} = c_jb_{1,i}b_{2,j} + c_ib_{1,j}b_{2,i}\ .$$

This forces $c_i = c_j$ and hence $c_1 = \cdots = c_r =: c \in K$. Thus, the last r rows of $(M - cI)$ are zero.

Note that equation (2) holds if we substitute $(M - cI)$ instead of M. We will keep using $\tau(.)$ as the effect of $(M - cI)$. Let us compare coefficients of $b_{3,j}$ on both sides of this modified form of equation (2):

$$\frac{1}{3}(\tau(z_{1,j,j})b_{2,j} + z_{2,j,j}\tau(b_{1,j})) + \frac{1}{6}\sum_{\substack{i=1\\ i\ne j}}^{r}(\tau(z_{1,i,j})b_{2,i} + z_{2,i,j}\tau(b_{1,i}))$$

$$= \frac{1}{3}(\tau(z_{2,j,j})b_{1,j} + z_{1,j,j}\tau(b_{2,j})) + \frac{1}{6}\sum_{\substack{i=1\\ i\neq j}}^{r}(\tau(z_{2,i,j})b_{1,i} + z_{1,i,j}\tau(b_{2,i})) \ .$$

This expression can be considerably simplified by observing that the last r rows of $(M-cI)$ are zero and hence $\tau(b_{*,*}) = 0$:

$$\frac{1}{3}\tau(z_{1,j,j})b_{2,j} + \frac{1}{6}\sum_{\substack{i=1\\ i\neq j}}^{r}\tau(z_{1,i,j})b_{2,i} = \frac{1}{3}\tau(z_{2,j,j})b_{1,j} + \frac{1}{6}\sum_{\substack{i=1\\ i\neq j}}^{r}\tau(z_{2,i,j})b_{1,i} \ .$$

Again, as this equation holds for all values of $z_{1,*},\ b_{1,*},\ z_{2,*},\ b_{2,*}$ we deduce that $\tau(z_{1,i,j})$ is only a linear combination of $b_{1,k}$'s and has no $z_{1,*}$. Thus,

$$(M - cI) = \begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix}_{n\times n} \quad \text{where } A \in K^{s\times r} \ .$$

Since the product of any two such matrices is zero we immediately get the structure of Cent(V,Θ) as claimed. Thus, Cent(V,Θ) is a local ring and by lemma 1.5 we also deduce that Θ is an indecomposable cubic form. □

Now we are ready to estimate the dimension of Cent(V,Θ). By lemma 1.6:

- $\begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix} \in \text{Cent}(V,\Theta)$ if and only if $J \cdot \begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix}$ is a symmetric matrix.
- J in block form looks like $\begin{pmatrix} 0 & B^T \\ B_{r\times s} & Z_{r\times r} \end{pmatrix}$.

$$\Rightarrow \ J \cdot \begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0_{s\times s} & 0_{s\times r} \\ 0_{r\times s} & B_{r\times s}\cdot A_{s\times r} \end{pmatrix} \ .$$

$$\Rightarrow \ \begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix} \in \text{Cent}(V,\Theta) \text{ iff } B_{r\times s}\cdot A_{s\times r} \text{ is a symmetric matrix.}$$

This gives us the following $\frac{r(r-1)}{2}$ constraints: for all $1 \le i < j \le r,\ (BA)_{ij} = (BA)_{ji}$. Since each nonzero entry of B is from the set $\{b_1, \ldots, b_r, 2b_1, \ldots, 2b_r\}$ we deduce that each constraint $(BA)_{ij} = (BA)_{ji}$ gives at most r linear equations in elements of A. So we have at most $\frac{r(r-1)}{2} \cdot r$ linear equations in elements of A whereas the number of elements in A is sr. Thus, dimension of the solution space for A is at least $sr - \frac{r(r-1)}{2} \cdot r = r^2$. Hence, $\dim_K \text{Cent}(V,\Theta) \ge r^2 + 1$.

The only thing left to prove is that (V,Θ) is regular.

Claim 2.1.2. (V,Θ) *is a regular* 3*-linear space.*

Proof of Claim 2.1.2. Following the notation of equation (2) suppose $v_1 \in V$ is given as: $\begin{pmatrix} z_{1,*} \\ b_{1,*} \end{pmatrix}$. If $z_{1,i,j} \neq 0$ then define $v_2 =$ (a column vector having all zeros except $b_{2,i} = 1$)

and $v_3 =$ (a column vector having all zeros except $b_{3,j} = 1$). Since Θ is induced by f we obtain:

$$\Theta(v_1, v_2, v_3) = \frac{1}{3} z_{1,i,j} \text{ or } \frac{1}{6} z_{1,i,j} \text{ depending on whether } i = j \text{ or not.}$$

If $b_{1,i} \neq 0$ then define $v_2 =$ (a column vector having all zeros except $b_{2,i} = 1$) and $v_3 =$ (a column vector having all zeros except $z_{3,i,i} = 1$). Again we get:

$$\Theta(v_1, v_2, v_3) = \frac{1}{3} b_{1,i}$$

Thus, for all nonzero $v_1 \in V$ one of the above two definitions will give $v_2, v_3 \in V$ such that $\Theta(v_1, v_2, v_3) \neq 0$. By definition this means that (V, Θ) is regular. □

This completes the description of the counter example. □

Interestingly, cubic forms *like* f can capture the graph isomorphism problem. That is, given two (finite) graphs G_1, G_2 we can effectively construct two cubic forms f_{G_1}, f_{G_2} such that:

$$G_1 \cong G_2 \iff f_{G_1} \cong f_{G_2}$$

For further details see sections 6 and 7 of [1].

Finally, we would like to pose the following question: Given a d-linear space (V, Θ) (where $d > 2$)

$$\text{is} \quad \dim_K \mathrm{Cent}(V, \Theta) \leq (d-1) \cdot \dim_K V \ ?$$

Acknowledgement

I would like to thank Susanne Pumpluen for many useful email discussions and for reviewing a preliminary version of the paper.

REFERENCES

1. M. Agrawal and N. Saxena, Automorphisms of Finite Rings and Applications to Complexity of Problems, Proceedings of Symposium of Theoretical Aspects of Computer Science, Lecture Notes in Computer Science (2005) 1-17.
2. D. Harrison, A Grothendieck ring of higher degree forms, Journal of Algebra 35 (1975) 123-138.
3. D. K. Harrison and B. Pareigis, Witt rings of higher degree forms, Communications in Algebra 16(6) (1988) 1275-1313.
4. M. O'Ryan and D. B. Shapiro, Centers of higher degree forms, Linear Algebra Appl. 371 (2003) 301-314.
5. C. Rupprecht, Cohomological invariants for higher degree forms, PhD Thesis, Universität Regensburg (2003).