A NOTE ON TRIANGULAR DERIVATIONS OF $k[X_1, X_2, X_3, X_4]$

Daniel Daigle and Gene Freudenburg

(Communicated by Wolmer V. Vasconcelos)

Abstract. For a field $k$ of characteristic zero, and for each integer $n \geq 4$, we construct a triangular derivation of $k[X_1, X_2, X_3, X_4]$ whose ring of constants, though finitely generated over $k$, cannot be generated by fewer than $n$ elements.

1. Introduction

Let $k$ be a field of characteristic zero. If $R$ is a finitely generated $k$-algebra, we write $\#(R) = s$ to indicate that $R$ can be generated by $s$ elements but not by $s - 1$. The purpose of this note is to show:

Theorem. Given any integer $n \geq 3$, there exists a triangular derivation $\Delta$ of the polynomial ring $k[X_1, X_2, X_3, X_4]$ whose kernel satisfies $\#(\ker \Delta) = n \leq \# (\ker \Delta) \leq n + 1$.

Equivalently, the theorem asserts that, given $n \geq 3$, there exists a triangular action of $G_a = (k, +)$ on $A^4$ whose ring of invariants satisfies $\#(O(A^4)^{G_a}) \leq n + 1$. The theorem is proved by constructing $\Delta$ explicitly for $n \geq 4$ (for $n = 3$, just use a partial derivative).

In contrast to our present result, the well-known theorem of Miyanishi [2] states that, for any locally nilpotent $k$-derivation $D$ of $k[X_1, X_2, X_3]$, $\#(\ker D) = 2$. At the other extreme, the authors recently found a triangular derivation of the ring $k[X_1, X_2, X_3, X_4, X_5]$ whose kernel is not finitely generated as a $k$-algebra [1]. It is not known whether such kernels in dimension four are always finitely generated, even for triangular derivations.

2. Preliminaries

A triangular derivation of $k[X_1, \ldots, X_n]$ is a $k$-derivation $\Delta : k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]$ satisfying $\Delta(X_i) \in k[X_1, \ldots, X_{i-1}]$ for all $i = 1, \ldots, n$.

An element of a submonoid $\Gamma$ of $(\mathbb{N}, +)$ is primitive if it is positive and cannot be written as the sum of two positive elements of $\Gamma$. It is easy to see that the set of primitive elements in $\Gamma$ is a finite set which generates $\Gamma$ and which is contained in every generating set.

The support of an element $f = \sum_{i=0}^{\infty} a_i X^i$ of the power series ring $k[[X]]$ is $\text{Supp}(f) = \{ i \in \mathbb{N} | a_i \neq 0 \}$. Given a submonoid $\Gamma$ of $(\mathbb{N}, +)$, the elements $f$ of $\text{Supp}(f)$ are primitive.
\( k[[X]] \) satisfying \( \text{Supp}(f) \subseteq \Gamma \) form a subalgebra of \( k[[X]] \) which we denote \( k[[\Gamma]] \).

We observe:

If \( g_1, \ldots, g_r \in k[[\Gamma]] \) and \( P \in k[[T_1, \ldots, T_r]] \) satisfy \( \text{ord}(g_i) \geq 1 \) for all \( i \) and \( \text{ord}(P) \geq 2 \), then no primitive element of \( \Gamma \) belongs to the support of \( P(g_1, \ldots, g_r) \).

Indeed, let \( \gamma \in \text{Supp}(P(g_1, \ldots, g_r)) \); then \( \gamma \) must be in the support of some monomial \( g_1^{i_1} \cdots g_r^{i_r} \) with \( i_1 + \cdots + i_r \geq 2 \), so \( \gamma \) is the sum of \( i_1 + \cdots + i_r \) elements of \( \bigcup_{i=1}^r \text{Supp}(g_i) \subseteq \Gamma \setminus \{0\} \) and hence is not primitive.

**Lemma 1.** Let \( \Gamma \) be a submonoid of \( (\mathbb{N},+) \), let \( e_1 < \cdots < e_h \) be the primitive elements of \( \Gamma \), let \( R = k[X^{e_1}, \ldots, X^{e_h}] \) and let \( T \) be an indeterminate over \( R \). Then:

\[
\#(R) = h \quad \text{and} \quad #(R[T]) = h + 1.
\]

**Proof.** Given \( f \in R[T] \), let \( f(0) \in k[X] \) be the result of evaluating \( f \) at \( T = 0 \), and let \( \text{ord}(f) \in \mathbb{N} \cup \{\infty\} \) be the \( X \)-order of \( f(0) \), i.e., the largest \( s \geq 0 \) such that \( X^s \) divides \( f(0) \) in \( k[X] \). Note that \( #(R) = h \) is a consequence of \( #(R[T]) = h + 1 \), so it suffices to prove the latter.

Assume that \( #(R[T]) \neq h + 1 \); then \( R[T] \) can be generated by \( h \) elements, say \( R[T] = k[f_1, \ldots, f_h] \). We begin by showing that, replacing if necessary the generating set \( \{f_1, \ldots, f_h\} \) by another one with the same cardinality \( h \), we may arrange that \( \text{ord}(f_j) = e_j \) for all \( j = 1, \ldots, h \). To see this, consider an integer \( i \) satisfying \( 1 \leq i \leq h \) and

\[
\text{ord}(f_j) = e_j, \quad \text{for all } j < i
\]

(this certainly holds for \( i = 1 \)). Observe that every element of \( \Gamma \) strictly less than \( e_i \) belongs to the monoid generated by \( \{e_1, \ldots, e_{i-1}\} \); hence, replacing each \( f_j \) (with \( j \geq i \)) by \( f_j \) plus a suitable polynomial in \( (f_1, \ldots, f_{i-1}) \), we may arrange that \( \text{ord}(f_j) \geq e_i \) for all \( j \geq i \). After relabelling, we obtain that \( f_1, \ldots, f_h \) satisfy

\[
e_i \leq \text{ord}(f_i) \leq \text{ord}(f_{i+1}) \leq \cdots \leq \text{ord}(f_h).
\]

Since \( X^{e_i} \in R[T] \), we may write

\[X^{e_i} = \lambda_1 f_1 + \cdots + \lambda_h f_h + P(f_1, \ldots, f_h),\]

where \( \lambda_j \in k \), \( P \in k[T_1, \ldots, T_h] \) (the \( T_j \) are indeterminates) and where every monomial occurring in \( P(T_1, \ldots, T_h) \) has degree at least two. Now \( P(f_1, \ldots, f_h|_{T=0} = P(f_1(0), \ldots, f_h(0)) = \sum \mu_j X^{\gamma_j} \), where \( \mu_j \in k \) and \( \gamma_j \in \Gamma \), but none of these \( \gamma_j \) can be a primitive element of \( \Gamma \) by (1). It follows that \( \lambda_j = 0 \) for all \( j < i \); also, \( \text{ord}(f_i) = e_i \), so we arranged that \( (2) \) holds for a larger value of \( i \). Thus we may arrange that

\[
\text{ord}(f_j) = e_j \quad \text{for all } j = 1, \ldots, h.
\]

Since \( T \in R[T] \), we may write

\[T = \lambda'_1 f_1 + \cdots + \lambda'_h f_h + P'(f_1, \ldots, f_h),\]

where \( \lambda'_j \in k \), \( P' \in k[T_1, \ldots, T_h] \), and where every monomial occurring in \( P'(T_1, \ldots, T_h) \) has degree at least two. Evaluating \( (3) \) at \( T = 0 \) shows that \( \lambda'_j = 0 \) for all \( j \) (as before, \( P'(f_1(0), \ldots, f_h(0)) \) can’t produce a term \( X^{e_i} \), by (1)). On
the other hand, each $f_j$ evaluated at $X = 0$ is an element of $T_k[T]$. Thus, evaluating the equation $T = P'(f_1, \ldots, f_h)$ at $X = 0$ yields $T = T^2 Q(T)$ for some $Q(T) \in k[T]$. This is a contradiction, so #$\langle R[T]\rangle = h + 1$ cannot be false.

Lemma 2. Let $h, p, q$ be positive integers. If $\gcd(p, q) = 1$, then the ideal

$$(T_0^q - T_1^p, T_1^q - T_2^p, \ldots, T_{h-1}^q - T_h^p)$$

of $k[T_0, \ldots, T_h]$ is prime.

Proof. Consider the ideals $p = (T_0^q - T_1^p, \ldots, T_{h-1}^q - T_h^p)$ of $k[T_0, \ldots, T_h]$ and $p' = (T_0^q - T_1^p, \ldots, T_{h-2}^q - T_{h-1}^p)$ of $k[T_0, \ldots, T_{h-1}]$. By induction, we may assume that $p'$ is prime. This allows us to identify $R' = k[T_0, \ldots, T_{h-1}]$ with $k[X_0, \ldots, X_{h-1}]$, where $X$ is an indeterminate and $e_j = p^{h-j}q^j$. Let $K'$ be the field of fractions of $R'$ and note that $K' = k(X^p)$. Since $k[T_0, \ldots, T_h]/p \cong k(X^p)/(T_h^p - \theta^q)$, where $\theta = T_{h-1} + p' \in R'$, it suffices to show that $T_h^p - \theta^q$ is an irreducible element of $K'[T_h]$; for this, it’s enough to verify that $(\theta^q)^i/p \notin K'$ for all $i = 1, \ldots, p - 1$. But $\theta = X^{qh-1}$, so $(\theta^q)^i/p = X^{iqh} \notin k(X^p)$ for all $i = 1, \ldots, p - 1$.

The following is a well-known fact about extracting roots in a power series ring.

Lemma 3. Let $q$ be a positive integer, $R$ a domain containing $\mathbb{Q}$, $W$ an indeterminate over $R$ and $\sigma$ an element of $R[[W]]$ with constant term equal to 1 (i.e., $\sigma = 1 + s_1 W + s_2 W^2 + \cdots$ where $s_i \in R$). Then there exists a unique $\rho \in R[[W]]$ satisfying $\rho^q = \sigma$ and having constant term equal to 1.

Lemma 4. Let $h \geq 2$ be an integer and $p, q$ prime numbers such that $p^2 < q$. Then there exist $f_0, \ldots, f_h \in k[W, X]$ satisfying:

(i) $f_j(0, X) = X^{p^{h-j}q^j}$ for all $j$ such that $0 \leq j \leq h$;

(ii) $f_{j+1} \equiv \frac{f_j^{q-1} - p}{W}$ (mod $W^{h-j}$) for all $j$ such that $0 < j < h$;

(iii) $f_h^p - f_h = 0$.

Proof. Define $f_h = X^{qh}$ and $f_{h-1} = X^{p^{h-1}q}$. Suppose that $f_h, \ldots, f_i \in k[W, X]$ have been defined (where $0 < i < h$) and satisfy (i)–(iii) and

$$X^{p^{h-j}q^j} \mid f_j \quad (i \leq j \leq h).$$

Note that the assumption $p^2 < q$ implies that $f_i^p + W f_{i+1}$ is divisible by $X^{p^{h-i+1}q^i}$; define

$$\sigma = \frac{f_i^p + W f_{i+1}}{X^{p^{h-i+1}q^i}} \in k[W, X] \subset k[X][[W]]$$

and note that $\sigma$ has the form $\sigma = 1 + s_1 W + s_2 W^2 + \cdots$ (with $s_j \in k[X]$). By Lemma 3 we may consider $\rho = 1 + r_1 W + r_2 W^2 + \cdots \in k[X][[W]]$ (with $r_j \in k[X]$) such that $\rho^q = \sigma$. Then $\tilde{f}_{i-1} := X^{p^{h-i+1}q^i-1} \rho \in k[X][[W]]$ satisfies

$$\frac{\tilde{f}_{i-1}^q - f_i^p}{W} = f_{i+1} \quad \text{and} \quad X^{p^{h-i+1}q^i} \mid \tilde{f}_{i-1}$$

so, if $f_{i-1} \in k[W, X]$ is a suitable truncation of $\tilde{f}_{i-1}$, then $f_h, \ldots, f_{i-1}$ satisfy (i)–(iii) and (4). So we are done by induction.
3. The examples

Given an integer \( h \geq 2 \), we construct a triangular derivation \( \Delta : \mathbb{k}[W, X, Y, Z] \to \mathbb{k}[W, X, Y, Z] \) whose kernel satisfies \( h + 2 \leq \#(\ker \Delta) \leq h + 3 \).

Choose prime numbers \( p, q \) satisfying \( p^2 < q \); consider \( f_0, \ldots, f_h \in \mathbb{k}[W, X] \) as in Lemma 4 and define \( F_0 = f_0 + YW^{h+1}, \quad F_1 = f_1 + ZW^h \) and

\[
F_{i+1} = F_i^{p+1} - F_i^p \left( \frac{i}{W} \right) \quad (1 \leq i \leq h).
\]

Let \( A = \mathbb{k}[W, F_0, \ldots, F_{h+1}] \). We have to prove the following two claims:

(5) \( h + 2 \leq \#(A) \leq h + 3 \);

(6) \( A \) is the kernel of some triangular derivation

\[ \Delta : \mathbb{k}[W, X, Y, Z] \to \mathbb{k}[W, X, Y, Z] \].

We begin by showing that

(7) \( F_j = f_j + b_j W^{h+1-j} \quad (0 \leq j \leq h+1) \),

where \( b_j \in \mathbb{k}[W, X, Y, Z] \) and \( b_j(0, X, Y, Z) \notin \mathbb{k}[X] \), and where we define \( f_{h+1} = 0 \).

We proceed by induction and note that the assertion is clear for \( j \leq 1 \). Assume that (7) holds for \( 0 \leq j \leq i \), for some \( i \) such that \( 1 \leq i \leq h \). Then \( F_i = f_i + b_i W^{h+1-i} \) and \( F_{i+1} = f_{i+1} + b_{i+1} W^{h+2-i} \), so

\[
F_{i+1} - F_i = (f_{i+1} - f_i + b_{i+1} W^{h+2-i} - b_i W^{h+1-i}) - b_i W^{h+1-i} + \varepsilon_1 W^{h+2-i}
\]

for some \( \varepsilon_1 \in \mathbb{k}[W, X, Y, Z] \). Write \( \frac{F_{i+1} - F_i}{W} = f_{i+1} + \varepsilon_2 W^{h-i}, \) with \( \varepsilon_2 \in \mathbb{k}[W, X] \); then dividing \( (F_{i+1} - F_i) \) by \( W \) gives

\[
F_{i+1} = (f_{i+1} + \varepsilon_2 W^{h-i}) - p f_i^{p-1} b_i W^{h+1-i} + \varepsilon_1 W^{h+2-i}
\]

which proves (7). (In particular, the \( F_i \)'s are polynomials.)

Let \( \pi : \mathbb{k}[W, X, Y, Z] \to \mathbb{k}[X, Y, Z] \) be the surjective \( \mathbb{k} \)-homomorphism defined by

\[
W \mapsto 0, \quad X \mapsto X, \quad Y \mapsto Y, \quad Z \mapsto Z.
\]

Then (7) implies that \( \pi(A) = \mathbb{k}[X^{e_0}, \ldots, X^{e_h}, \tau] \), where \( e_i = p^{h-i} q^i \) and where \( \tau \) is transcendental over \( \mathbb{k}(X) \). Let \( R = \mathbb{k}[X^{e_0}, \ldots, X^{e_h}] \); since \( R[\tau] \) is a homomorphic image of \( A, \#(A) \geq \#(R[\tau]) \); since \( \#(R[\tau]) = h + 2 \) by Lemma 1, (5) holds. Define a derivation \( \Delta : \mathbb{k}[W, X, Y, Z] \to \mathbb{k}[W, X, Y, Z] \) by

\[
\Delta = \begin{vmatrix}
\frac{\partial}{\partial X} & \frac{\partial}{\partial Y} & \frac{\partial}{\partial Z} \\
\frac{\partial F_0}{\partial X} & \frac{\partial F_0}{\partial Y} & \frac{\partial F_0}{\partial Z} \\
\frac{\partial F_1}{\partial X} & \frac{\partial F_1}{\partial Y} & \frac{\partial F_1}{\partial Z}
\end{vmatrix}.
\]

Then \( \Delta Y = -W^{h+1} \frac{\partial f_0}{\partial X}, \quad \Delta X = -W^h \frac{\partial f_0}{\partial X}, \quad \Delta X = W^{2h+1} \) and \( \Delta W = 0 \), so \( \Delta \) is a triangular derivation of \( \mathbb{k}[W, X, Y, Z] \). It is clear that \( \mathbb{k}[W, F_0, F_1] \subseteq \ker \Delta \), so \( A \subseteq \ker \Delta \); let us now argue that \( \ker \Delta \subseteq A_W \). Write \( B = \mathbb{k}[W, X, Y, Z] \); since

\[
B_W \supseteq A_W[X] \supseteq \mathbb{k}[W, W^{-1}, X, F_0, F_1] = \mathbb{k}[W, W^{-1}, X, Y, Z] = B_W,
\]

\( B_W \) is a polynomial ring over \( A_W \). On the other hand, \( (\ker \Delta)_W \) contains \( A_W \) and is the kernel of the nonzero derivation \( \Delta_W : B_W \to B_W \), so \( (\ker \Delta)_W = A_W \) and
we have shown that \( A \subseteq \ker \Delta \subseteq AW \). So, in order to prove (9), there remains only to prove

\[
A \cap WB = WA.
\]

It is easy to see that the proof of (9) reduces to that of the following: if \( T_0, \ldots, T_{h+1} \) are indeterminates and \( \psi \in k[T_0, \ldots, T_{h+1}] \), then \( \psi(T_0, \ldots, T_{h+1}) \in WB \) implies \( \psi(F_0, \ldots, F_{h+1}) \in WA \). Write \( \psi = \sum_{n \geq 0} \psi_n T_{h+1} \) with \( \psi_n \in k[T_0, \ldots, T_h] \). Then

\[
0 = \pi(\psi(F_0, \ldots, F_{h+1})) = \sum_{n \geq 0} \psi_n(X^{c_0}, \ldots, X^{c_h})\tau^n,
\]

where \( \tau = \pi(F_{h+1}) \) is transcendental over \( k(X) \), and consequently \( \psi_n \in \ker \varphi \) for all \( n \), where \( \varphi : k[T_0, \ldots, T_h] \to k[X] \) is the \( k \)-homomorphism which maps \( T_i \) to \( X^{c_i} \). By Lemma 2, \( \ker \varphi = (T_0^q - T_1^q, \ldots, T_{h-1}^q - T_h^q) \), so \( \psi_n = \sum_{j=1}^h \alpha_j(T_{j-1}^q - T_j^q) \) for some \( \alpha_j \in k[T_0, \ldots, T_h] \). Then

\[
\psi_n(F_0, \ldots, F_h) = \sum_{j=1}^h \alpha_j(F_0, \ldots, F_h)(F_{j-1}^q - F_j^q)
= \sum_{j=1}^h \alpha_j(F_0, \ldots, F_h)WF_{j+1} \in WA.
\]

So (9) holds and, consequently, \( \ker(\Delta) = A \). So (5) and (6) are proved.

Example. We exhibit a triangular derivation \( \Delta \) of \( k[W, X, Y, Z] \) whose kernel cannot be generated by five elements over \( k \). Let \( p = 2 \), \( q = 5 \) and \( h = 4 \) and, following the proof of Lemma 1, successively define \( f_1, f_2, f_3, f_4, f_0 \) by

\[
f_4 = X^{625}, \quad f_3 = X^{250}, \quad f_2 = X^{100} + \frac{1}{5} X^{225} W,
\]

\[
f_1 = X^{40} + \left( \frac{2}{25} X^{165} + \frac{1}{5} X^{90} \right) W + \left( -\frac{3}{625} X^{290} - \frac{8}{125} X^{215} - \frac{2}{25} X^{140} \right) W^2
\]

and

\[
f_0 = X^{16} + \left( \frac{2}{25} X^{66} + \frac{1}{5} X^{36} + \frac{4}{125} X^{141} \right) W
+ \left( -\frac{42}{5125} X^{191} - \frac{32}{15625} X^{116} - \frac{42}{15625} X^{266} + \frac{9}{625} X^{161} - \frac{8}{125} X^{86} - \frac{2}{25} X^{56} \right) W^2
+ \left( \frac{438}{5125} X^{241} + \frac{68}{15625} X^{166} + \frac{665}{15625} X^{316} + \frac{328}{15625} X^{211} + \frac{132}{3125} X^{136}
+ \frac{36}{625} X^{106} - \frac{72}{15625} X^{286} - \frac{28}{3125} X^{181} + \frac{6}{125} X^{76} + \frac{244}{1953125} X^{391} \right) W^3.
\]

Define \( \Delta \) as in (8) or, equivalently, by

\[
\Delta W = 0, \quad \Delta X = W^9, \quad \Delta Y = -W^4 \frac{\partial f_0}{\partial X} \quad \text{and} \quad \Delta Z = -W^5 \frac{\partial f_1}{\partial X}.
\]

Then, by (5) and (6), we have \( 6 \leq \#(\ker \Delta) \leq 7. \)

\[\text{Note that the } f_j \text{'s are not unique.}\]
REFERENCES


Department of Mathematics and Statistics, University of Ottawa, Ottawa, Canada K1N 6N5

E-mail address: daniel@mathstat.uottawa.ca

Department of Mathematics, University of Southern Indiana, Evansville, Indiana 47712

E-mail address: freudenb@usi.edu