Constructing (almost) rigid rings and a UFD having infinitely generated Derksen and Makar-Limanov invariant

David Finston and Stefan Maubach*

June 11, 2013

Abstract

An example is given of a UFD which has infinitely generated Derksen invariant. The ring is “almost rigid” meaning that the Derksen invariant is equal to the Makar-Limanov invariant. Techniques to show that a ring is (almost) rigid are discussed, among which is a generalization of Mason’s abc-theorem.


1 Introduction and tools

The Derksen invariant and Makar-Limanov invariant are useful tools to distinguish nonisomorphic algebras. They have been applied extensively in the context of affine algebraic varieties. Both invariants rely on locally nilpotent derivations: for $R$ a commutative ring and $A$ a commutative $R$-algebra, an $R$-linear mapping $D : A \to A$ is an $R$-derivation if $D$ satisfies the Leibniz rule: $D(ab) = aD(b) + bD(a)$. The derivation $D$ is locally nilpotent if for each $a \in A$ there is some $n \in \mathbb{N}$ such that $D^n(a) = 0$. When $k$ is a field of characteristic 0 a locally nilpotent $k$-derivation $D$ of the $k$-algebra $A$ gives rise to an algebraic action of the additive group of $k$, $G_a(k)$, on $A$ via:

$$\exp(tD)(a) \equiv \sum_{i=0}^{\infty} \frac{t^i}{i!} d^i(a).$$

for $t \in k, a \in A$. Conversely, an algebraic action $\sigma$ of $G_a(k)$ on $A$ yields a locally nilpotent derivation via:

$$\frac{\sigma(t, a) - a}{t} \bigg|_{t=0}.$$
In this case, the kernel of $D$ denoted by $A^D$ coincides with the ring of $G_\alpha(k)$ invariants in $A$.

The Makar-Limanov invariant of the $R$-algebra $A$, denoted $ML_R(A)$, is defined as the intersection of the kernels of all locally nilpotent $R$-derivations of $A$, while the Derksen invariant, $D_R(A)$ is defined as the smallest algebra containing the kernels of all nonzero locally nilpotent $R$-derivations of $A$. The subscript $R$ will be suppressed when it is clear from the context.

In [9] the question was posed of whether the Derksen invariant of a finitely generated algebra over a field could be infinitely generated. In [14] an example is given of an infinitely generated Derksen invariant of a finitely generated $C$-algebra. In fact, this example is of a form described in this paper as an “almost-rigid ring”: a ring for which the Derksen invariant is equal to the Makar-Limanov invariant. Despite its simplicity and the simplicity of the argument, this example has a significant drawback in that it is not a UFD. In this paper we provide a UFD example having infinitely generated invariants (it is again an almost-rigid ring).

The paper is organized as follows. Section 1 consists of basic notions and examples associated with rigidity and almost rigidity. In section 2, the focus is on rigid and almost rigid rings, with techniques to prove rigidity or almost rigidity. In section 3, certain rings are shown to be UFDs, and these are used in section 4 to give the UFD examples having infinitely generated Makar-Limanov and Derksen invariants.

**Notations:** If $R$ is a ring, then $R^{[n]}$ denotes the polynomial ring in $n$ variables over $R$ and $R^*$ denotes the group of units of $R$. The $R$ module of $R$-derivations of an $R$-algebra $A$ is denoted by $Der_R(A)$ and the set of locally nilpotent $R$-derivations by $LND_R(A)$ (the $R$ will be suppressed when it is clear from the context). We will use the letter $k$ for a field of characteristic zero, and $K$ for an algebraic closure. The symbol $\partial_X$ denotes the derivative with respect to $X$. When the context is clear, $x, y, z, \ldots$ will represent residue classes of elements $X, Y, Z, \ldots$ modulo an ideal.

Let $A$ be an $R$-algebra which is an integral domain. Well-known facts that we need are included in the following:

**Lemma 1.1.** Let $D \in LND_R(A)$.

1. Then $D(A^*) = 0$.
2. If $D(ab) = 0$ where $a, b$ are both nonzero, then $D(a) = D(b) = 0$.
3. If $\tilde{D} \in Der_R(A)$ and $f \in A$ satisfy $f \tilde{D} \in LND_R(A)$, then $\tilde{D} \in LND_R(A)$ and $f \in A^D$.

## 2 (Almost) rigid rings

As defined in [8] page 196, [3], or [2], a rigid ring is a ring which has no locally nilpotent derivations except the zero derivation. Examples include the rings $R := \mathbb{C}[X, Y, Z]/(X^a + Y^b + Z^c)$ with $a, b, c \geq 2$ and pairwise relatively prime [6], and
coordinate rings of Platonic $\mathbb{C}^*$ fiber spaces \cite{13}. We define an almost rigid ring here as a ring whose set of locally nilpotent derivations is, in some sense, one-dimensional.

**Definition 2.1.** An $R$-algebra $A$ is called almost-rigid if there is a nonzero $D \in \text{LND}(A)$ such that $\text{LND}(A) = A^D D$.

For a field $F$ any derivation $D$ of $F[X]$ has the form $D = f(X) \partial_X$. Thus the simplest almost-rigid algebra is $F[X]$. Other examples include the algebras

$$\mathbb{C}[X, Y, Z, U, V]/(X^a + Y^b + Z^c, X^mV - Y^nU - 1)$$

with $a, b, c$ pairwise relatively prime given in \cite{6} as counterexamples to a cancellation problem. Clearly an almost-rigid algebra has its Derksen invariant equal to its Makar-Limanov invariant. The following lemma is useful in determining rigidity.

**Lemma 2.2.** Let $D$ be a nonzero locally nilpotent derivation on a domain $A$ containing $\mathbb{Q}$. Then $A$ embeds into $K[S]$ where $K$ is some algebraically closed field of characteristic zero, in such a way that $D = \partial_S$ on $K[S]$.

**Proof.** The proof uses some well-known facts about locally nilpotent derivations. Since $D \neq 0$ is locally nilpotent, we can find an element $p$ such that $D^2(p) = 0, D(p) \neq 0$. Set $q := D(p)$ (and thus $q \in A^D$) and observe that $D$ extends uniquely to a locally nilpotent derivation $\tilde{D}$ of $\tilde{A} := A[q^{-1}]$. Since $\tilde{D}$ has the slice $s := p/q$ (a slice is an element $s$ such that $\tilde{D}(s) = 1$) we have (see prop.1.3.21 in \cite{5}) $\tilde{A} = \tilde{A}^D[s]$ and $\tilde{D} = \partial_s$. Denote by $k$ the quotient field of $\tilde{A}^D (= \text{quotient field of } A^D)$ noting that $D$ extends uniquely to $k[s]$. One can embed $k$ into its algebraic closure $K$, and the derivation $\partial_s$ on $K[s]$, restricted to $A \subseteq K[s]$, equals $D$. \qed

As an application, we have

**Example 2.3.** Let $R := \mathbb{C}[x, y] = \mathbb{C}[X, Y]/(X^a + Y^b + 1)$ where $a, b \geq 2$. Then $R$ is rigid.

**Proof.** Suppose $D \in \text{LND}(R), D \neq 0$. Using lemma 2.2 we see $D$ as $\partial_S$ on $K[S] \supseteq R$. Now the following lemma ("mini-Mason’s") shows that $x, y$ both must be constant polynomials in $S$. But that means $D(x) = D(y) = 0$, so $D$ is the zero derivation, contradiction. So the only derivation on $R$ is the zero derivation, i.e. $R$ is rigid. \qed

Versions of the following lemma can be found as lemma 9.2 in \cite{5}, and lemma 2 in \cite{11}. Here we give it the appellation “mini-Mason’s” as it can be seen as a very special case of Mason’s very useful original theorem. (Note that Mason’s theorem is the case $n = 3$ of theorem 2.5.)

**Lemma 2.4.** (Mini-Mason) Let $f, g \in K[S]$ where $K$ is algebraically closed and of characteristic zero. Suppose that $f^a + g^b \in K^*$ where $a, b \geq 2$. Then $f, g \in K$. 

3
Proof. Note that $\gcd(f, g) = 1$. Taking derivative with respect to $S$ gives $af'' - bg'' = 0$. So $f$ divides $gg'$, so $f$ divides $g'$. Same reason, $g$ divides $f'$. This can only be if $f' = g' = 0$. ■

Mason’s theorem provides a very useful technique in constructing rigid rings (see [6] for an example). With appropriate care, a generalization of Mason’s theorem provides more examples. In this paper, we will use [1, Theorem 2.1], which is a corollary of a generalization of Mason’s theorem (see [1, Theorem 1.5]).

**Theorem 2.5.** Let $f_1, f_2, \ldots, f_n \in K[S]$ where $K$ is an algebraically closed field containing $\mathbb{Q}$. Assume

$$
\sum_{i=1}^{n} f_i^{d_i} = 0.
$$

Additionally, assume that for every $1 \leq i_1 < i_2 < \ldots < i_s \leq n$,

$$
\sum_{i=i_1}^{i_s} f_i^{d_i} = 0 \implies \gcd\{f_{i_1}, f_{i_2}, \ldots, f_{i_s}\} = 1.
$$

Then

$$
\sum_{i=1}^{n} \frac{1}{d_i} \leq \frac{1}{n - 2}
$$

implies that all $f_i$ are constant.

**Example 2.6.** Let $R := \mathbb{C}[X_1, X_2, \ldots, X_n]/(X_1^{d_1} + X_2^{d_2} + \ldots + X_n^{d_n})$ where $d_1^{-1} + d_2^{-1} + \ldots + d_n^{-1} \leq \frac{1}{n - 2}$. Then $R$ is a rigid ring.

The proof will follow from the more general

**Lemma 2.7.** Let $A$ be a finitely generated $\mathbb{Q}$ domain. Consider a subset $F = \{F_1, F_2, \ldots, F_m\}$ of $A$ and positive integers $d_1, \ldots, d_n$ satisfying: 1) $P := F_1^{d_1} + F_2^{d_2} + \ldots + F_m^{d_m}$ is a prime element of $A$ and 2) No nontrivial subsum of $F_1^{d_1}, F_2^{d_2}, \ldots, F_m^{d_m}$ lies in $(P)$ (e.g. the $F_i$ are linearly independent). Additionally, assume that

$$
d_1^{-1} + d_2^{-1} + \ldots + d_n^{-1} \leq \frac{1}{n - 2}.
$$

Set $R := A/(P)$ and let $D \in \text{LND}(R)$. With $f_i \in R$ equal to the residue class of $F_i$, we have $D(f_i) = 0$ for all $1 \leq i \leq n$.

**Proof.** Suppose $D \in \text{LND}(R)$ where $D \neq 0$. Using lemma 2.2 with $K$ an algebraic closure of the quotient field of $R^D$, we realize $D$ as $\partial S$ on $K[S] \supseteq R$. In particular, $f_1(S)^{d_1} + f_2(S)^{d_2} + \ldots + f_m(S)^{d_m} = 0$. By hypothesis there cannot be a subsum $f_{i_1}^{d_{i_1}} + f_{i_2}^{d_{i_2}} + \ldots + f_{i_s}^{d_{i_s}} = 0$. Applying the above theorem 2.5 we find that all $f_i$ are constant. ■

This lemma also helps in constructing almost-rigid rings not of the form $R^{[1]}$ with $R$ rigid.
Example 2.8. [13] Define
\[ R := \mathbb{C}(a, b) = \mathbb{C}[A, B]/(A^3 - B^2) \]
and
\[ S := R[X, Y, Z]/(Z^2 - a^2(aX + bY)^2 - 1). \]
Then \( LN D(S) = S^D D \) where \( D := b\partial_X - a\partial_Y \).

The following is an example of a rigid unique factorization domain. The proof of UFD property is deferred to the next section.

Example 2.9. Let \( n \geq 3 \), and in \( \mathbb{C}[X_1, X_2, \ldots, X_n, Y_1, Y_2, \ldots, Y_n] \) set
\[ P := X_1^{d_1} + X_2^{d_2} + \ldots + X_n^{d_n} + L_2^{e_2} + L_3^{e_3} + \ldots + L_n^{e_n} \]
where \( L_i := X_iY_1 - X_1Y_i \) and
\[ d_1^{-1} + d_2^{-1} + \ldots + d_n^{-1} + e_2^{-1} + e_3^{-1} + \ldots + e_n^{-1} \leq 1/(2n - 1 - 2). \]
Let
\[ R := \mathbb{C}[X_1, X_2, \ldots, X_n, Y_1, Y_2, \ldots, Y_n]/(P) \]
and denote by \( x_i, y_i, l_i \) the images of \( X_i, Y_i, L_i \) in \( R \). Then \( R \) is an almost-rigid UFD, and \( LN D(R) = R^D D \) where \( D(x_i) = 0, D(y_i) = x_i. \)

Proof. An elementary argument shows that \( R \) is a domain: View
\[ P \in \mathbb{C}[X_1, X_2, \ldots, X_n, Y_1, Y_2, \ldots, Y_n-1][Y_n]. \]
The residue of \( P \) modulo \( (Y_1, Y_2, \ldots, Y_{n-1}) \) has the same degree in \( Y_n \) as \( P \) and is clearly irreducible.

That any \( 2n - 1 \) element subset of \( \{ x_i^{d_i}, t_i^{e_i} : 1 \leq i \leq n \} \) is algebraically independent over \( \mathbb{Q} \) modulo \( (P) \) is also elementary: Suppose that \( \sum_{i=1}^{n} X_i^{d_i} + \sum_{i=1}^{n} L_i^{e_i} \) is divisible by \( P \). Lemma [27] yields that for any \( E \in LN D(R) \) we have \( E(x_i) = 0 \), and \( E(l_i) = 0 \). So \( x_1E(y_i) = x_iE(y_1) \). Since \( R \) is a UFD, we can write \( E(y_i) = \alpha x_i \) for some \( \alpha \in R \). So \( E = \alpha D \) where \( D \) is as in the statement. ■

3 Factoriality of Brieskorn-Catalan-Fermat rings for \( n \geq 5 \)

Because of their resemblance to rings arising in Fermat’s last theorem, the Catalan conjecture, and to the coordinate rings of Brieskorn hypersurfaces, we will call the rings \( \mathbb{C}[X_1, X_2, \ldots]/(X_1^{d_1} + X_2^{d_2} + \ldots + X_n^{d_n}) \) Brieskorn-Catalan-Fermat (BCF) rings. Our examples depend on the factoriality of certain BCF rings. While the next observation is undoubtedly well known, a proof is included since we could not find an explicit one in the literature.
**Theorem 3.1.** If \( n \geq 5 \) and \( d_i \geq 2 \) for all \( 1 \leq i \leq n \), then \( \mathbb{C}[X_1, X_2, \ldots]/(X_1^{d_1} + X_2^{d_2} + \ldots + X_n^{d_n}) \) is a UFD.

The result follows from the next two theorems:

**Theorem 3.2.** (Corollary 10.3 of [10]) Let \( A = A_0 + A_1 + \ldots \) be a graded noetherian Krull domain such that \( A_0 \) is a field. Let \( m = A_1 + A_2 + \ldots \). Then \( Cl(A) \cong Cl(A_m) \), where \( Cl \) is the class group.

**Theorem 3.3.** ([10]) A local noetherian ring \((A, m)\) with characteristic \( A/m = 0 \) and an isolated singularity is a UFD if its depth is \( \geq 3 \) and the embedding codimension is \( \leq \dim(A) - 3 \).

**Proof.** (of theorem 3.1) Write

\[
A : = \mathbb{C}[x_1, x_2, \ldots, x_n] = \mathbb{C}[X_1, X_2, \ldots]/(X_1^{d_1} + X_2^{d_2} + \ldots + X_n^{d_n}).
\]

Note that by giving appropriate positive weights to the \( X_i \), the ring \( A \) is graded, and \( m := A_1 + A_2 + \ldots = (x_1, x_2, \ldots, x_n), A_0 = \mathbb{C} \). \( A \) now satisfies the requirements of 3.2, so it is equivalent to show that \( A_m \) is a UFD (note that “\( A \) is a UFD” is equivalent to “\( Cl(A) = \{0\} \)” ). Now \( A_m \) has only one singularity, namely at the point \( m \). The ring \( A \) is defined by one homogeneous equation, and therefore, by definition, a complete intersection. Being a complete intersection implies that the ring \( A \) is Cohen-Macauley and that its depth is the same as its Krull dimension. So, the depth of \( A \) is \( n - 1 \) which is \( \geq 3 \) since \( n \geq 5 \). Now, one can see \( A \) as a subring of the polynomial ring localized at the maximal ideal \((X_1, X_2, \ldots, X_n)\). \( A \) has codimension 1 in this ring, so its embedding codimension is 1. \( \dim(A) - 3 = n - 4 \), so, if \( n \geq 5 \), we have that the embedding codimension of \( A \) equals 1 \( \leq \dim(A) - 3 \). So, if \( n \geq 5 \), the criteria of 3.3 are met, and \( A_m \) is a UFD.

The following lemma of Nagata is a very useful tool in proving factoriality.

**Lemma 3.4.** (Nagata) Let \( A \) be a domain, and \( x \in A \) is prime. If \( A[x^{-1}] \) is a UFD, then \( A \) is a UFD.

**Lemma 3.5.** \( R \) as in example 2.9 is a UFD.

**Proof.** Note that \( X_2^{d_2} + X_3^{d_3} + \ldots + X_n^{d_n} + (X_2Y_1)^{e_2} + (X_3Y_1)^{e_3} + \ldots + (X_nY_1)^{e_n} \) is irreducible for any \( d_i \geq 1, e_i \geq 1 \), so \( R/(x_1) \) is a domain. Using 3.4 it is enough to show that \( R[x_1^{-1}] \) is a UFD. Define \( m_i := y_i - \frac{x_i}{x_1}y_1 \) for \( 2 \leq i \leq n \), and

\[
S := \mathbb{C}[x_1, x_2, \ldots, x_n, m_2, m_3, \ldots, m_n].
\]

Then \( R[x_1^{-1}] = S[x_1^{-1}][Y_1] \) where \( Y_1 \) is algebraically independent over \( S[x_1^{-1}] \). It is now enough to prove that \( S \) is a UFD. But this follows from theorem 3.1 since \( n \geq 3 \).
4  A UFD having infinitely generated invariants

4.1 Definitions

Definition 4.1. In \( \mathbb{C}[7] = \mathbb{C}[X, Y, Z, S, T, U, V] \), let \( L_1 := Y^3S - X^3T, L_2 := Z^3S - X^3U, L_3 := Y^2Z^2S - XV \). Define \( P := X^{d_1} + Y^{d_2} + Z^{d_3} + L_1^{d_4} + L_2^{d_5} + L_3^{d_6} \) where the \( d_i \geq 2 \) are integers. Set
\[
A := \mathbb{C}[x, y, z, t, u, v] = \mathbb{C}[X, Y, Z, S, T, U, V] \left( P \right),
\]
and let \( R \) be the subring \( \mathbb{C}[x, y, z] \).

The elements \( s, t, u, v \) in \( A \) form a regular sequence; in particular they are algebraically independent.

Definition 4.2.
\[
E := X^3 \partial_S + Y^3 \partial_T + Z^3 \partial_U + X^2Y^2Z^2 \partial_V.
\]

Note that \( E \) is locally nilpotent and \( P \in \ker(E) \). Thus \( E \) induces a well defined element of \( LND(A) \) denoted by \( D \).

4.2 The factoriality of \( A \)

For a 5-tuple of positive integers \( d = (d_1, d_2, \ldots, d_5) \), define \( Q(d) := Y^{d_2} + Z^{d_3} + (Y^3S)^{d_4} + (Z^3S)^{d_5} + (Y^2Z^2S)^{d_6} \)

Proposition 4.3. If \( Q(d) \) is irreducible in \( \mathbb{C}[Y, Z, S] \) then \( A \) is a UFD.

Proof. Assume that \( Q(d) \) is irreducible. Note that \( A/(x) \cong \mathbb{C}[Y, Z, S, T, U, V]/(Q(d)) \) so that \( x \) is prime. By Nagata’s lemma \[3.4\] it is enough to show that \( A[x^{-1}] \) is a UFD. Now define
\[
M_1 := T - \frac{Y^3}{X^3}S, M_2 := U - \frac{Z^3}{X^3}S, M_3 := V - \frac{Y^2Z^2}{X}S,
\]
write \( m_i \) for the image of \( M_i \) in \( A[x^{-1}] \), and let
\[
B = \mathbb{C}[x, y, z, m_1, m_2, m_3][x^{-1}].
\]

Since \( D(s) = x^3, \frac{x}{s} \) is a slice for the extension of \( D \) to \( A[x^{-1}] = B[s] \), with \( s \) transcendental over \( B \). Consider \( C := \mathbb{C}[X, Y, Z, M_1, M_2, M_3]/(X^{d_1} + Y^{d_2} + Z^{d_3} + \left( M_1^{d_4} + M_2^{d_5} + M_3^{d_6} \right)) \). This ring is a UFD by theorem \[3.1\] so \( C[x^{-1}] = B \) is also a UFD, from which we deduce that \( B[s] = A[x^{-1}] \) is a UFD. \( \blacksquare \)

The polynomial \( Q(d) \) is irreducible for infinitely many positive integer choices of the \( d_i \); take for example \( \gcd(d_2, d_3) = 1 \) and \( d_2 \geq \max(3d_4, 2d_6) \).
4.3 A is not finitely generated

In this section, we assume that $d_1, \ldots, d_6$ are such that $Q(d)$ is irreducible (i.e. $A$ is a UFD), and such that $d_1 + d_2 + \ldots + d_6 \leq \frac{1}{4}$ (note that by necessity $d_1, d_2, d_3 \geq 4$).

The following lemma shows that $A$ is an almost-rigid ring.

**Lemma 4.4.** Any locally nilpotent derivation on $A$ is a multiple of $D$.

**Proof.** Let $\Delta$ be a nonzero LND on $A$. By lemma 2.7 since we assumed $\sum_{i=1}^{6} d_i \leq \frac{1}{4}$, we see that $x, y, z, l_1, l_2, l_3$ must be in $A^\Delta$. So $\Delta(l_1) = 0$, so $x^3 \Delta(t) = y^3 \Delta(s)$, and thus $\Delta(S) = x^2 \alpha$ for some $\alpha \in A$ (since $A$ is a UFD). Using $\Delta(l_1) = \Delta(l_2) = \Delta(l_3) = 0$ this yields $\Delta(T) = y^3 \alpha, \Delta(U) = z^3 \alpha, \Delta(V) = x^2 y^2 z^2 \alpha$, i.e. $\Delta = \alpha D$. ■

**Lemma 4.5.** $A^D \subset (x, y, z) A + R$.

**Proof.** Let

$$J : = (X^3, Y^3, Z^3, X^2 Y^2 Z^2)(X, Y, Z)C[x, y, z],$$

$$H : = (x, y, z) A \supseteq J := (x^3, y^3, z^3, x^2 y^2 z^2) H.$$  

Both $J$ and $H$ are $D$ stable ideals of $A$. Denote by $\bar{D}$ the locally nilpotent derivation induced by $D$ on $\bar{A} := A/J, \bar{H} := H/J$, and $\bar{D}$ the image of $D$ in $\bar{A}$. Note that $\bar{D}(\bar{H}) = 0$. We will prove that $A^D \subseteq \bar{H} + \bar{R}$, which will imply that $A^D + J \subseteq H + J + R$, and the required result then follows since $J \subseteq H$.

To that end assume there exists $h \in \bar{A}^D$ with $h \notin \bar{H} + \bar{R}$. Note that since $P \in J$ we have

$$\bar{A} \cong (C[7]/(P))/((J/(P)) \cong C[7]/J.$$  

With $\bar{x}, \bar{y}, \bar{z}, \bar{s}, \bar{t}, \bar{u}, \bar{v}$ denoting as usual the images of $S, T, U, V$ in $\bar{A}$, we have $\bar{A} = \bar{R}[\bar{s}, \bar{t}, \bar{u}, \bar{v}]$, a polynomial ring over $\bar{R}$.

Assign degree 0 to elements of $\bar{R}$, weights $wt(\bar{s}) >> wt(\bar{u}) >> wt(\bar{t}) >> wt(\bar{s})$, and well order monomials $s^{\alpha} \bar{t} u \bar{v}^d$ in $\bar{A}$ lexicographically. By assumption there exists a monomial $M$ of lowest order appearing in $h$ which is not in $\bar{H} + \bar{R}$. Say $M := rs^d \bar{t} u \bar{v}^d$ where $r \in \bar{R} \setminus \bar{H}$.

First assume $d \neq 0$. Since $\bar{D}(h) = 0$, the nonzero monomial $dx^2 \bar{y}^2 \bar{z}^2 s^d \bar{t} u \bar{v}^{d-1}$ must appear in the $\bar{D}$-derivative of at least one other monomial $N$ occurring in $h$. Notice that then $N$ must also have $\bar{R}$-coefficient not in $\bar{H}$, as otherwise $\bar{D}(N) = 0$ (since $\bar{D}(\bar{H}) = 0$). Since $\bar{D}N$ contains the monomial $dx^2 \bar{y}^2 \bar{z}^2 rs^d \bar{t} u \bar{v}^{d-1}$, $\bar{D}N$ has degree $a + b + c + d - 1$. But the derivation $\bar{D}$ decreases degree by exactly one, so that $N$ must have degree $a + b + c + d$. Since $M$ was the lowest degree polynomial with lowest possible lexicographic ordering, $N$ then must have a higher lexicographic ordering than $s^d \bar{t} u \bar{v}^{d-1}$. But then all (four) terms in $\bar{D}(N)$ will have higher lexicographic ordering than $s^d \bar{t} u \bar{v}^{d-1}$. So, such a monomial $N$ will not exist, which is a contradiction for this case.
The cases where $d = 0, c \neq 0$, and $d = c = 0, b \neq 0$, and $d = c = b = 0, a \neq 0$ go similarly, leading to a contradiction. ($d = c = b = a = 0$ implies $M \in \bar{R}$, which we excluded). So, the assumption that $h \notin \bar{H} + \bar{R}$, was wrong. Thus $h \in \bar{H} + \bar{R}$ as claimed.

**Lemma 4.6.** For each $n \in \mathbb{N}$, there exists $F_n \in A^D$ which satisfies $F_n = xV^n + f_n$ where $f_n \in \sum_{i=0}^{n-1} R[s, t, u]v^i \subset A$.

**Proof.** It is shown in several places, for example [12], [4], or page 231 of [5], that already on $\mathbb{C}[7]$ there exist such $\tilde{F}_n$ which are in the kernel of the derivation $E$ (they are key to the proof that the kernel of $E$ is not finitely generated as a $\mathbb{C}$-algebra, and therefore yields a counterexample to Hilbert’s 14th problem). By taking for $F_n$ the image of $\tilde{F}_n$ in $A$ we obtain the desired kernel elements.

**Corollary 4.7.** $A^D$ is not finitely generated as a $\mathbb{C}$-algebra.

**Proof.** Suppose $A^D = R[g_1, \ldots, g_s]$ for some $g_i \in A$. Since $A^D \subseteq R + (x, y, z)$ by lemma [4.5] we can assume that all $g_i \in (x, y, z)$. Define $\mathcal{F}_n(A) := \sum_{i=0}^{n-1} R[S, T, U]V^i$ which is a subset of $A$. Choose $n$ such that $g_i \in \mathcal{F}_n(A)$ for all $1 \leq i \leq s$. Now $F_n \in \mathcal{F}_n(A) \cap A^D$. Then $F_n = P(g_1, \ldots, g_s)$ for some $P \in R^[[s]]$. Compute modulo $(x, y, z)^2$. Since each $g_i \in (x, y, z)$, we have

$$P(g_1, \ldots, g_n) \equiv r_1g_1 + \ldots + r_ng_n \mod (x, y, z)^2$$

for some $r_i \in R$. So $F_n \in Rg_1 + \ldots + Rg_n + (x, y, z)^2$. In particular, $F_n \in \mathcal{F}_n(A) + (x, y, z)^2$. Notice that $F_n - xV^n \in \mathcal{F}_n(A) \subseteq \mathcal{F}_n(A) + (x, y, z)^2$, so that $xV^n \in \mathcal{F}_n(A) + (x, y, z)^2$. But this is obviously not the case, contradicting the assumption that $A^D = R[g_1, \ldots, g_s]$ for some $g_i \notin R^\circ$. Thus $A^D$ is not finitely generated as an $R$-algebra, a fortiori as a $\mathbb{C}$-algebra. 

Using lemma [4.4] we know that there is only one kernel of a nontrivial LND on $A$, so the following result is obvious.

**Corollary 4.8.** $ML(A) = Der(A) = A^D$ is not finitely generated.

**References**


*Department of mathematics*  
*New Mexico State University*  
*Las Cruces, USA*  
*email: dfinston@nmsu.edu*

*Department of Mathematics*  
*Radboud University Nijmegen*  
*Nijmegen, The Netherlands*  
*email: s.maubach@math.ru.nl*