Derivations in Univariate Polynomial Subalgebras of Finite Codimension

Erik Leffler
Advisors: Anna Torstensson, Victor Ufnarovski

October 19, 2021

Abstract

In this text we continue the work of describing subalgebras of $\mathbb{K}[x]$ of finite codimension that was started in "Describing subalgebras of $\mathbb{K}[x]$ using derivatives" [2]. In the referenced paper, the authors present how such subalgebras can be described by conditions on the values in certain points and proceed to develop a large theoretical framework to understand the nature of such conditions. The authors state and prove a Main Theorem regarding the form that such conditions can exhibit. They also propose a Main Conjecture, a sharpening of the Main Theorem. After having restated the required theory from "Describing subalgebras of $\mathbb{K}[x]$ using derivatives" [2], we will present a proof of the Main Conjecture.

Contents

1 Introduction

Let $\mathbb{K}$ be an algebraically closed field of characteristic 0. Throughout this text we shall be concerned with univariate polynomial subalgebras $A \subset \mathbb{K}[x]$ of finite codimension. Usually such subalgebras would be described in terms of a basis. For example, one might be interested in the subalgebra A that is generated by the polynomials x^3, x^4 and x^5. Then A consists of all polynomials where the first, and second degree terms are all 0. In [2], an entire theory is developed around the concept of describing such subalgebras in a new way, by the use of equations. For example, the same subalgebra A can be written using conditions as follows,

$$A = \{f \in \mathbb{K}[x] \mid f'(0) = f''(0) = 0\}.$$

Another less obvious example, let $B = \langle x^3 - x, x^2 \rangle$. This algebra can be written using conditions as,

$$B = \{f \in \mathbb{K}[x] \mid f(1) = f(-1)\}.$$

That these representations are equivalent may be unclear to the reader as of now. However, once we have presented the necessary theory from [2], it will be an easy thing to see.

In [2] the authors postulate a main conjecture regarding the possible forms subalgebra conditions can exhibit. In this text we shall present a proof of this conjecture. But before we can even state, let alone prove, the conjecture we need to restate some of the theory that is developed in the paper.

In the remainder of this text, whenever we speak of an algebra, we mean a univariate polynomial algebra over the scalar field $\mathbb{K}$.

2 Background

We begin our journey by introducing some useful terminology regarding the basis of an algebra.

2.1 Type and SAGBI Basis

2.1.1 Type of an Algebra

If $A \subset \mathbb{K}[x]$ is a subalgebra, the set $S = \{\deg(f) \mid f \in A\}$ of degrees of the polynomials forms a numerical semigroup. Every numerical semigroup has a unique finite minimal set of generators. This minimal generator set of S will prove to be a useful property. Thus we introduce a new definition.

Definition 1. We define the *type* of a subalgebra $A \subseteq \mathbb{K}[x]$, written $T(A)$, as the minimal generator set of the numerical semigroup $S = \{\deg f \mid f \in A\}$ of degrees in A. We write $T(A)$ as a tuple and omit 0 as all subalgebras need to contain the scalar field.

For example, let $A = \langle x^3, x^5 \rangle$. Then any polynomial in A will have a leading term comprised of factors x^3, x^5. Hence $T(A) = \langle 3, 5 \rangle$. To deal with the subtleties of more complicated examples, we need to define SAGBI bases.

2.1.2 SAGBI bases in Algebras of Univariate Polynomials

With the type defined we can now easily define what a SAGBI basis is. In a multivariate setting, the definition of a SAGBI basis requires some care and setup. Thankfully, in the univariate case the concept of a SAGBI basis is quite simple, and we restrict our definitions accordingly.

Definition 2. A SAGBI basis of a subalgebra $A \subset \mathbb{K}[x]$ is a subset $G \subseteq A$ of polynomials such that for each degree $d \in T(A)$, there is a polynomial p of degree $\deg p = d$ in G.

Note that a SAGBI basis may contain redundant polynomials. If it does not we call it a minimal SAGBI basis. Throughout this text, most if not all SAGBI bases will be minimal.

Let G be a SAGBI basis for A. Then for any polynomial $q \in A$, we can find polynomials $p_1, p_2, \ldots, p_n \in G$ such that $\deg\left(\prod p_i\right) = \deg q$ (due to the fact G contains a generating set for the numerical semigroup of degrees). Hence there exists some scalar α such that

$$\deg\left(q - \alpha \prod p_i\right) < \deg q.$$

We may repeat these steps, each time obtaining a polynomial of lesser degree until we find ourselves left with 0. This process is called subduction and shows that a SAGBI basis in fact generates its algebra.

2.2 Subalgebra Conditions

2.2.1 Derivations and Equality Conditions

In the introduction we said that any subalgebra A can be represented by a set of conditions. In this section we shall elaborate on what these conditions are. In general, these conditions will be represented as kernels of different linear functions from an algebra A to the scalar field $\mathbb{K}$. Such functions are called linear functionals. Only two different families of linear functionals are required. The first are called derivations.

Definition 3. Let $\alpha \in \mathbb{K}$. An α-derivation over some subalgebra $A \subseteq \mathbb{K}[x]$ is a linear functional $D \mid A \to \mathbb{K}$ such that for any $f, g \in A$ we have

$$D(fg) = D(f)g(\alpha) + f(\alpha)D(g).$$

Note that the name is parameterized and that an α-derivation need not be the same thing as a β-derivation if $\alpha \neq \beta$.

Right away we see that $D(f) = f'(\alpha)$ is an α-derivation in any subalgebra as $D(fg) = (fg)'(\alpha) = f'(\alpha)g(\alpha) + f(\alpha)g'(\alpha)$. That D is linear is immediately clear. We can find more interesting examples if we consider the kernel of D, namely $A = \{f \in \mathbb{K} \mid f'(\alpha) = 0\}$ (that A in fact is an algebra will be proved shortly). In this algebra both $D_2(f) = f''(\alpha)$ and $D_3(f) = f'''(\alpha)$ are α-derivations since

$$\begin{aligned} D_2(fg) &= f''(\alpha)g(\alpha) + 2f'(\alpha)g'(\alpha) + f(\alpha)g''(\alpha) \\ &= f''(\alpha)g(\alpha) + f(\alpha)g''(\alpha), \\ D_3(fg) &= f'''(\alpha)g(\alpha) + 3f''(\alpha)g'(\alpha) + 3f'(\alpha)g''(\alpha) + f(\alpha)g'''(\alpha) \\ &= f'''(\alpha)g(\alpha) + f(\alpha)g'''(\alpha). \end{aligned}$$

Moreover, any linear combination of D_2, D_3 is an α-derivation. In fact, the set of α-derivations forms a vector space over the same scalar field $\mathbb{K}$ as the algebra they act upon. To see this, let D_1, D_2 be α-derivations. Then

$$\begin{aligned} (\beta_1 D_1 + \beta_2 D_2)(fg) &= \beta_1 D_1(fg) + \beta_2 D_2(fg) \\ &= \beta_1(D_1(f)g(\alpha) + f(\alpha)D_1(g)) + \beta_2(D_2(f)g(\alpha) + f(\alpha)D_2(g)) \\ &= (\beta_1 D_1 + \beta_2 D_2)(f)g(\alpha) + f(\alpha)(\beta_1 D_1 + \beta_2 D_2)(g). \end{aligned}$$

We move on and define the second type of linear functional.

Definition 4. An equality condition over a subalgebra $A \subseteq \mathbb{K}[x]$ is a function $E \mid A \to \mathbb{K}$ of the form

$$E(f) = c(f(\alpha) - f(\beta))$$

for some scalars $c, \alpha \neq \beta \in \mathbb{K}$.

We call these equality conditions as any polynomial p in the kernel of $E(f) = c(f(\alpha) - f(\beta))$ satisfies $p(\alpha) = p(\beta)$.

Note that the kernel of any α-derivation or equality condition is a subalgebra. As both functionals are linear, we only need to show closure under multiplication. Let $A \subseteq \mathbb{K}[x]$ be a subalgebra of finite codimension, D be an α-derivation over A, and $E(f) = f(\beta_1) - f(\beta_2)$ be an equality condition. Then if $f, g \in \ker(D)$ we have $D(fg) = f(\alpha)D(g) + D(f)g(\alpha) = 0 + 0$ whence $fg \in \ker(D)$. If instead $f, g \in \ker(E)$ we have $E(fg) = f(\alpha)g(\alpha) - f(\beta)g(\beta)$. But $f, g \in \ker(E)$ so $f(\alpha) = f(\beta)$ and the same for g. Hence $E(fg) = 0$ and $fg \in \ker(E)$.

It will be useful to have some lemmas regarding linear functionals under our belt so we include these here.

Lemma 5. Let V be a vector space over the field $\mathbb{K}$ and let $f : V \to \mathbb{K}$ be a linear functional. Then $\ker(f)$ is either trivial or has codimension 1.

Proof. If $f = 0$ then $\ker(f)$ is trivial so let $f \neq 0$. Then there exist some $v_0 \in V$ such that $f(v_0) = 1$. Now for any $v \in V$ we have $f(f(v)v_0) = f(v)f(v_0) = f(v)$, hence $v - f(v)v_0 \in \ker(f)$. It follows that any $v \in V$ may be written as $v = f(v)v_0 + u$ for some $u \in \ker(f)$. In other words, $\ker(f) + \langle v_0 \rangle = V$ and we are done. □

Lemma 6. Let f, g be two non-trivial linear functionals from V to $\mathbb{K}$. If $\ker(f) = \ker(g)$, then $f = cg$ for some $c \in \mathbb{K}$.

Proof. Let $v_0 \in V$ such that $f(v_0) = 1$. As above, we may write any $v \in V$ as $v = f(v)v_0 + u$ for some $u \in \ker(f)$. Looking at g we get $g(v) = g(v_0)f(v) + g(u) = g(v_0)f(v)$ as the functionals share the same kernel. Hence for any $v \in V$, $g(v) = g(v_0)f(v)$ and the statement of the lemma holds with $c = g(v_0)$. □

Finally, we reformulate the two previous lemmas in a way that will be more applicable later on when we tackle the Main Conjecture.

Lemma 7. Let A be a subalgebra of $\mathbb{K}[x]$ and L_1, L_2 be two linear functionals over A. If $L_2(f) = 0$ for all $f \in \ker(L_1)$, then $L_2 = cL_1$ for some $c \in \mathbb{K}$.

Proof. If $L_2 = 0$ then the statement holds with $c = 0$. If $L_1 = 0$, then $\ker(L_1) = V$ so $L_2(f) = 0$ for all $f \in V$ whence $L_2 = 0$. So assume that both derivations are non-trivial. By Lemma 5, both $\ker(L_1)$ and $\ker(L_2)$ have codimension 1 in A, and as $\ker(L_1) \subset \ker(L_2)$ we have $\ker(L_1) = \ker(L_2)$. Now applying Lemma 6 yields the statement of the lemma. □

2.2.2 Subalgebras of Codimension 1

In this section we will completely classify all subalgebras of codimension 1. This will serve as an important base case for an inductive proof later on.

Let $A \subseteq \mathbb{K}[x]$ be a subalgebra of codimension 1. First note that any subalgebra that contains x also must contain all polynomials in x and therefore be all of $\mathbb{K}[x]$. Hence A can't contain any polynomials of degree 1. By our codimension assumption, it follows that A can be generated by a second and third degree polynomial.

Theorem 8. Let $A \subseteq \mathbb{K}[x]$ be a subalgebra of codimension 1. Then A is the kernel of either $D(f) = cf'(\alpha)$ or $E(f) = cf(\beta_1) - cf(\beta_2)$ in $\mathbb{K}[x]$ for some scalars α, $\beta_1 \neq \beta_2$ and c.

Proof. As A has codimension 1, there exist a SAGBI basis of the form $g_2(x) = x^2 + a_2x$, $g_3(x) = x^3 + a_3x$ (the second degree term in g_3 can be annihilated by subtraction of kg_2 for some suitable scalar k). We now wish to show that there either exist some β_1, β_2 such that

$$g_2(\beta_1) - g_2(\beta_2) = g_3(\beta_1) - g_3(\beta_2) = 0,$$

or there exist an α such that

$$g_2'(\alpha) = g_3'(\alpha) = 0$$

This would be enough since the kernels of both E and D are subalgebras and would therefore need to include A if they contain g_2, g_3. That A would be equal to whichever kernel can be seen by noting that neither kernel can include linear polynomials and would therefore have codimension of at least 1.

We are now ready for the proof. The symmetry line of g_2 is given by $x = -a_2/2$ which means that for any scalar b we have $g_2(-a_2/2 + b) - g_2(-a_3/2 - b) = 0$. Thus we need to find a non-zero value of b such that

$$\begin{aligned} 0 &= g_3(-a_2/2 + b) - g_3(-a_2/2 - b) \\ &= (-a_2/2 + b)^3 + a_3(-a_2/2 + b) - (-a_2/2 - b)^3 - a_3(-a_2/2 - b) \\ &= \frac{3a_2^2 b}{2} + 2b^3 + 2a_3 b, \end{aligned}$$

and as $b \neq 0$ we get

$$3a_2^2 + 4b^2 + 4a_3 = 0 \Rightarrow b^2 = \frac{3a_2^2 + 4a_3}{4}.$$

We can always find such b since our field $\mathbb{K}$ is algebraically complete. However, we need $b \neq 0$, which corresponds to $3a_2^2 \neq -4a_3$. But if $3a_2^2 = -4a_3$ we have

$$\begin{aligned} g_3'(-a_2/2) &= \frac{3a_2^2}{4} + a_3 \\ &= -a_3 + a_3 \\ &= 0, \end{aligned}$$

whence $g_2'(-a_2/2) = g_3'(-a_2/2) = 0$ and we are done. □

2.2.3 Conditions Can Represent Subalgebras of Finite Codimension

The workhorse underpinning this entire theory is a theorem proved in [1]. We shall state it here without proof.

Theorem 9. Any subalgebra $A \subseteq \mathbb{K}[x]$ of finite codimension $n > 1$ is contained in some subalgebra $B \subseteq \mathbb{K}[x]$ of codimension $n-1$ where A is the kernel of some derivation or equality condition in B.

We can use Theorem 9 inductively over codimension to show that any subalgebra $A \subseteq \mathbb{K}[x]$ of finite codimension can be written as the intersection of kernels of derivations and equality conditions. Here Theorem 8 serves as a base case.

2.3 The Spectrum of a Subalgebra

Before we begin with the mathematics in this section, we introduce some terminology that will aid our ease of expression. We say that the scalar α categorizes a derivation D if D is an α-derivation. We say that the scalars β_1, β_2 define an equality condition E if $E(f) = c(f(\beta_1) - f(\beta_2))$ for some scalar c.

We now define another important property of univariate polynomial subalgebras.

Definition 10. Let $A \subseteq \mathbb{K}[x]$ be a subalgebra of finite codimension. Then a scalar α belongs to the spectrum of A, $\mathrm{Sp}(A)$, if either $f'(\alpha) = 0$ for all $f \in A$ or there exist some $\beta \neq \alpha$ such that $f(\alpha) = f(\beta)$ for all $f \in A$.

A quick aside. This definition is not entirely complete without Lemma 15. The lemma depends on the current definition though so we need to state things in this order. But for now, the reader should accept that in the kernel of any α-derivation, we have either $f'(\alpha) = 0$ for all f or $f(\alpha) = f(\beta)$ for all f and some scalar β. Hence the spectrum will contain any scalars that define equality conditions or categorizes derivations by which the algebra can be described.

For example, if $A = \{f \in \mathbb{K}[x] \mid f(-1) = f(1), f'(1) - 2f'(-1) = 0, f'(3) = 0\}$, then $\{-1, 1, 3\} \subseteq \mathrm{Sp}(A)$ Again, it will be easy to see that A is, in fact, an algebra once the reader has finished this section.

Note that if we create a new subalgebra by adding a condition to A, the resulting spectrum will be a superset of the old one. This is important enough to warrant its own lemma.

Lemma 11. If $A, B \subseteq \mathbb{K}[x]$ are two subalgebras of finite codimension and $A \subseteq B$, then $\mathrm{Sp}(B) \subseteq \mathrm{Sp}(A)$.

Proof. Any condition that holds in B also holds in A. □

Now in the previous example we wrote $\{-1, 1, 3\} \subseteq \mathrm{Sp}(A)$, but in fact, equality holds and $\{-1, 1, 3\} = \mathrm{Sp}(A)$. This can be seen by applying the following theorem.

Theorem 12. Let $A \subseteq \mathbb{K}[x]$ be a subalgebra of finite codimension and let D be an α-derivation over A. If $\lambda \notin \mathrm{Sp}(A) \cup \{\alpha\}$ we have $\lambda \notin \mathrm{Sp}(\ker D)$. Also let $E(f) = f(\alpha) - f(\beta)$. Then if $\lambda \notin \mathrm{Sp}(A) \cup \{\alpha, \beta\}$ we have $\lambda \notin \mathrm{Sp}(A)$.

A proof can be found in [2].

This theorem along with the previous lemma essentially state that there are no "ghost" elements in the spectrum of a subalgebra. If A is obtained as the kernel of a set of derivations and equality conditions, the spectrum consists of exactly the scalars that define the equality conditions and categorize the derivations.

There is also a natural and important equivalence relation that we can define on the spectrum.

Definition 13. Let $A \subseteq \mathbb{K}[x]$ be a subalgebra of finite codimension. Then two spectral elements $\alpha, \beta \in \mathrm{Sp}(A)$ are said to belong to the same cluster if $f(\alpha) = f(\beta)$ for all $f \in A$. If this is the case, we write $\alpha \sim \beta$ and say that α is equivalent to β.

So basically, two spectral elements α, β are equivalent in a subalgebra if they define one of the equality conditions that hold in the subalgebra.

An interesting property of equivalent spectral elements is that they share the same derivation space. To see this, let $\alpha \sim \beta$ be equivalent spectral elements in some subalgebra $A \subseteq \mathbb{K}[x]$ of finite codimension and let D be an α-derivation. Then $D(fg) = D(f)g(\alpha) + f(\alpha)D(g)$, but since $\alpha \sim \beta$ we have $f(\alpha) = f(\beta)$ and $g(\alpha) = g(\beta)$. Hence $D(fg) = D(f)g(\beta) + f(\beta)D(g)$ and D is a β-derivation as well. So for example, if $f(1) = f(-1)$ for all f in some algebra, we have that $D(f) = f'(1) - 2f'(-1)$ is both a 1-derivation and a -1-derivation. Now it should be easy to see that $\{f \in \mathbb{K}[x] \mid f(-1) = f(1), f'(1) - 2f'(-1) = 0, f'(3) = 0\}$ is an algebra.

2.4 The Main Theorem and the Main Conjecture

In this section we will deepen our understanding of derivations by proving our prior claim that all derivations are linear combinations of derivatives evaluated at elements in the spectrum. We will also state the Main Conjecture. First, we need one more definition.

Definition 14. An α-derivation D over a subalgebra $A \subseteq \mathbb{K}[x]$ of finite codimension is called *trivial* if $\alpha \notin \mathrm{Sp}(A)$.

All trivial derivations are fully characterized in the following lemma.

Lemma 15. Let $A \subseteq \mathbb{K}[x]$ be a subalgebra of finite codimension and D be a trivial α-derivation over A. Then $D(f) = cf'(\alpha)$ for some scalar c.

The proof is complicated and we therefore direct the interested reader to [2].

Now, there are a couple of theorems we need before we can deal with the Main Theorem. The first one shows that every subalgebra of finite codimension contains a particularly useful ideal.

Theorem 16. Let $A \subseteq \mathbb{K}[x]$ be subalgebra of finite codimension n and spectrum $\mathrm{Sp}(A) = \{\alpha_1, \alpha_2, \ldots, \alpha_s\}$. Then there exist an integer $N > 1$ such that $p(x)\pi(x)^N \in A$ for all $p \in \mathbb{K}[x]$ where $\pi(x) = \prod_{\alpha_i \in \mathrm{Sp}(A)}(x - \alpha_i)$

Proof. We use induction on the codimension n to prove this. If $n = 1$, then by Theorem 8, we know that either $\pi(x) = (x - \alpha), N = 2$ or $\pi(x) = (x - \beta_1)(x - \beta_2), N = 1$ will work (here we used the same scalars as in Theorem 8).

We now let $n > 1$ and consider the induction step. Let A be obtained from B as the kernel of some equality condition or derivation L. Let $\pi_B(x) = \prod_{\alpha_i \in \mathrm{Sp}(B)}(x - \alpha_i)$, and N_B be the integer that is guaranteed by the induction hypothesis.

We consider first the case when L is an equality condition, $L(f) = f(\alpha) - f(\beta)$. If both $\alpha, \beta \in \mathrm{Sp}(B)$ we have $L(p\pi_B) = 0$ for any polynomial $p(x) \in \mathbb{K}[x]$ hence $p\pi_B^{N_B} \in A$ and the theorem statement holds with $N = N_B$. If instead only one element belongs to the spectrum of B, say $\alpha \in \mathrm{Sp}(B)$ but $\beta \in \mathrm{Sp}(B)$. Then $\pi_A = (x - \beta)\pi_B$ so by the induction hypothesis we have $p\pi_A^{N_B} = p(x - \beta)^{N_B}\pi_B^{N_B} \in B$ for any $p \in \mathbb{K}[x]$ and this in conjunction with the fact that $L(p\pi_A^{N_B}) = 0$ yields the theorem statement with $N = N_B$. Finally, consider the case where neither element is in the spectrum of B, $\alpha, \beta \notin \mathrm{Sp}(B)$. Then as before the induction hypothesis yields $p\pi_A^{N_B} = p(x-\beta)^{N_B}(x-\alpha)^{N_B}\pi_B^{N_B} \in B$ and this case is proved in an identical manner.

Now let L be an α-derivation. If L is non-trivial, then define q to be the polynomial we get by removing the $(x-\alpha)$ factor from π_B. I.e $q(x) = \pi_B(x)/(x-\alpha)$. Now, for any polynomial $p \in \mathbb{K}[x]$ we have that

$$\begin{aligned} L(p(x)\pi_A^{2N_B}) =& L(p(x)(x-\alpha)^{2N_B}q^{2N_B}(x)) \\ =& L\left(p(x)(x-\alpha)^{N_B}q^{N_B}(x)\right)(\alpha-\alpha)^{N_B}q^{N_B}(\alpha) \\ &+ p(\alpha)(\alpha-\alpha)^{N_B}q^{N_B}(\alpha)L\left((x-\alpha)^{N_B}q^{N_B}\right) \\ =& 0, \end{aligned}$$

hence the statement holds with $N = 2N_B$. If L is trivial in B we get the same result by simply performing the same steps as above but with $L(p\pi_A^{2N_B}) = L(p(x-\alpha)^{2N_B}\pi_B^{2N_B})$ as our starting point.

We have now exhausted all cases and the proof is done. □

Finally, we are ready for the Main Theorem.

Theorem 17 (Main Theorem)**.** Let $A \subseteq \mathbb{K}[x]$ be a subalgebra of finite codimension n and spectrum $\mathrm{Sp}(A) = \{\alpha_1, \alpha_2, \ldots, \alpha_s\}$. Then there exist an integer

N such that A can be written as the intersection of the kernels of n functions of the form

$$D(f) = \sum_{i=0}^{N-1} \sum_{j=1}^{s} c_{ij} f^{(i)}(\alpha_j).$$

Proof. Throughout this proof we shall consider A as a vector space. It follows from Theorem 16 that we can construct a linearly independent set $V_2 = \{x^i \pi^N(x) | i \in \mathbb{N}\}$ that span a subspace of A. Let V_1 be another (minimal) subset of A such that $V = V_1 \cup V_2$ forms a basis for A. As $\operatorname{codim}(A) = n$ and $\operatorname{codim}(\langle V_2 \rangle) = Ns$ (since $\deg(\pi) = s$) we have that $\dim(\langle V_1 \rangle) = Ns - n$.

Now consider the vector space K of linear functions that can be written as

$$D(f) = \sum_{i=0}^{N-1} \sum_{j=1}^{s} c_{ij} f^{(i)}(\alpha_j),$$

and satisfy $D(q) = 0$ for all $q \in V_1$. If D is a function that may be written as above, the system of equations $D(q) = 0 \ \forall q \in V_1$ consists of $Ns - n$ homogeneous linear equations and has Ns degrees of freedom (each of the c_{ij}). Moreover, if q is a polynomial where $\deg(q) = m$, then $q^{(m)} \neq 0$ and $q^{(k)} = 0$ for all $k > m$. As no two elements in V_1 are of the same degree, and they all have degree less than N, the system of equations has full rank. It follows that there are n linearly independent solutions and $\dim(K) = n$.

Now, note that if $q \in V_2$, then q has roots in every element of the spectrum of multiplicity at least N. Thus if $\alpha_i \in \operatorname{Sp}(A)$ and $k < N$ we have $q^{(k)}(\alpha_i) = 0$. Hence $D(q) = 0$ for all $D \in K$ and $q \in V_2$ as well. It follows that all functions in K annihilate all of A and $A \subseteq \bigcap_{D \in K} \ker(D)$. But as $\dim(K) = n$, repeated application of Lemma 5 over basis elements of K yields $\operatorname{codim}\left(\bigcap_{D \in K} \ker(D)\right) = n$ and thus $A = \bigcap_{D \in K} \ker(D)$. Any basis for K will now provide us with the n conditions that were promised in the theorem statement. □

Now we present another version of the Main Theorem that will be easier to work with in this text.

Corollary 18. Let $A \subseteq \mathbb{K}[x]$ be a subalgebra of finite codimension n and spectrum $\operatorname{Sp}(A) = \{\alpha_1, \alpha_2, \ldots, \alpha_s\}$. Then there exist an integer N such any derivation D over A can be written as

$$D(f) = \sum_{i=0}^{N-1} \sum_{j=1}^{s} c_{ij} f^{(i)}(\alpha_j).$$

Proof. As D is a derivation, $A' = \ker(D)$ is a subalgebra of A. We now adopt the terminology of the previous proof. Let K, K' be the vector spaces of functions of desired form that annihilate A and A' respectively. As $A' \subset A$, we have $K \subset K'$. By Lemma 5 it follows that $\operatorname{codim}(A') = \operatorname{codim}(A) + 1$ and from our results in

the previous proof, $\text{codim}(A) = \dim(K) = n, \text{codim}(A') = \dim(K') = n+1$. Thus K has codimension 1 in K'. Let V be a basis for K. We can complete V with one element, $F \in K'$ to create a basis for K'. As $\ker(D) = \ker(F)$, it follows from Lemma 6 that $D = cF$ for some scalar c whence D adheres to the desired form. □

We will now state the Main Conjecture.

Theorem 19 (Main Conjecture)**.** Let $A \subseteq \mathbb{K}[x]$ be a subalgebra of finite codimension n. Then there exist an integer N such that any non trivial α-derivation D can be written as

$$D(f) = \sum_{i=1}^{N-1} \sum_{\hat{\alpha} \sim \alpha} c_{ij} f^{(i)}(\hat{\alpha}).$$

As you can see, the Main Conjecture is a sharpening of the Main Theorem wherein any derivation only contains derivatives evaluated in one cluster (and no regular $f^{(0)}(\alpha)$ evaluations).

3 Proving the Main Conjecture

We are now ready to prove the Main Conjecture. We begin with two Lemmas that are required for correctness.

Lemma 20. Let A be a subalgebra of $\mathbb{K}[x]$ where $\beta \not\sim \delta$. Then the equality condition $E(f) = f(\beta) - f(\delta)$ is not an α-derivation. Note that α can be non-equivalent to both elements β, δ or equivalent to either one of them (but not both as $\beta \not\sim \delta$).

Proof. As $\beta \not\sim \delta$, we can find $g \in A$ such that $g(\beta) = -1$ and $g(\delta) = 0$. Then $E(g) = E(g^3) = -1, E(g^2) = 1$. Using the previous equlaities, if E were to be an α-derivation we would have

$$1 = E(g^2) = 2g(\alpha)E(g) = -2g(\alpha),$$

but also

$$-1 = E(g^3) = 3g^2(\alpha)E(g) = 3g^2(\alpha),$$

which is impossible. □

Lemma 21. Let A be a subalgebra of $\mathbb{K}[x]$ where $\alpha \not\sim \beta$. If L is some linear functional over A, then $\alpha \sim \beta$ in $\ker(L)$ if and only if L is an equality condition.

Proof. If $\alpha \sim \beta$ in $\ker(L)$, then $\ker(L) \subseteq \ker(f \to f(\alpha) - f(\beta))$, and we have that $L = cf(\alpha) - cf(\beta)$ by Lemma 7. The other implication is immediate. □

The previous two lemmas allow us to add any number of derivation conditions to a subalgebra and be sure that the cluster structure remains unchanged.

We are now ready to start approaching the Main Theorem. Our approach will rely on inductively iterating through an inclusion chain of subalgebras. At each step we will apply the following lemma, which in some regard is a special case of the Main Theorem.

Lemma 22. Let $A \subset \mathbb{K}[x]$ be a subalgebra of finite codimension where $\alpha \not\sim \beta$ and $f^{(i)}(\beta) = 0$ for all $0 < i < m$ and $f \in A$, and there exist some $f \in A$ such that $f^{(m)}(\beta) \neq 0$. Then

$$D(f) = f^{(m)}(\beta) + \sum_{\alpha_i \sim \alpha} \sum_{j=0}^{N} c_{ij} f^{(j)}(\alpha_i)$$

can't be an α-derivation.

Proof. Let $p, q \in A$ such that $p^{(m)}(\beta) \neq 0$ and $q(\alpha) \neq q(\beta)$. Moreover define

$$f(x) = \frac{p(x) - p(\beta)}{p^{(m)}(\beta)},\ g(x) = \frac{q(x) - q(\alpha)}{q(\beta) - q(\alpha)}.$$

Then $f(\beta) = 0, f^{(m)}(\beta) = 1$ and $g(\alpha) = 0, g(\beta) = 1$. Now let $h = g^{N+1}$. Then

$$\begin{aligned} D(fh) &= (fh)^{(m)}(\beta) + \sum_{\alpha_i \sim \alpha} \sum_{j=0}^{N} c_{ij} (fh)^{(j)}(\alpha_i) \\ &= f(\beta)h^{(m)}(\beta) + h(\beta)f^{(m)}(\beta) + \sum_{\alpha_i \sim \alpha} \sum_{j=0}^{N} c_{ij} \sum_{k=0}^{j} f^{(j-k)}(\alpha_i) h^{(k)}(\alpha_i) \\ &= 0 + 1 + 0 \\ &= 1, \end{aligned}$$

where the sum is zero as $h = g^{N+1}$ has roots in each $\alpha_i \sim \alpha$ of multiplicity at least $N + 1$. Now, if D were to be an α-derivation, we would have

$$\begin{aligned} D(fh) &= D(f)h(\alpha) + f(\alpha)D(h) \\ &= f(\alpha)D(h) \\ &= f(\alpha) \left(h^{(m)}(\beta) + \sum_{\alpha_i \sim \alpha} \sum_{j=0}^{N} c_{ij} h^{(j)}(\alpha_i) \right) \\ &= f(\alpha)h^{(m)}(\beta). \end{aligned}$$

In the remaining segments we will use $f[a]$ to denote polynomial evaluation when the polynomial is a complicated expression. Collecting the above results we get $1 = f(\alpha)h^{(m)}(\beta)$. But we chose f and h independently. Hence for all f, h selected in the way above, we must have $f(\alpha) = a, h^{(m)}(\beta) = b$ for some constants a, b where $ab = 1$. This means that for all $p \in A$ where $p^{(m)}(\beta) \neq 0$, we have

$$\left(\frac{p - p(\beta)}{p^{(m)}(\beta)} \right) [\alpha] = a \Rightarrow p(\alpha) - p(\beta) = a p^{(m)}(\beta), \tag{1}$$

and for all $q \in A$ where $q(\alpha) \neq q(\beta)$, we have

$$\left(\left(\frac{q-q(\alpha)}{q(\beta)-q(\alpha)}\right)^{N+1}\right)^{(m)}[\beta] = b,$$

which yields

$$\begin{aligned} b(q(\beta)-q(\alpha))^{N+1} &= \left((q-q(\alpha))^{N+1}\right)^{(m)}[\beta] \\ &= \left(\sum_{k=0}^{N+1}\binom{N+1}{k}q^k(-q(\alpha))^{N+1-k}\right)^{(m)}[\beta] \\ &= \sum_{k=0}^{N+1}\binom{N+1}{k}(q^k)^{(m)}(\beta)(-q(\alpha))^{N+1-k}. \end{aligned} \tag{2}$$

Now $f \to f(\alpha) - f(\beta)$ is not a β-derivation by Lemma 20, but $f \to af^{(m)}(\beta)$ clearly is (by our assumptions of A). Thus by equation 1, there must exist a polynomial $P(x)$ such that $P^{(m)}(\beta) = 0$ and $P(\alpha) \neq P(\beta)$. If not $f(\alpha) - f(\beta) = af^{(m)}(\beta)$ for all $f \in A$ which is not allowed since a functional can't simultaneously be a derivation and a non-derivation. But now P qualifies for equality 2 and we get

$$b(P(\beta)-P(\alpha))^{N+1} = \sum_{k=0}^{N+1}\binom{N+1}{k}(P^k)^{(m)}(\beta)(-P(\alpha)^{N+1-k}).$$

If we expand $(P^k)^{(m)}(\beta)$ according to Faà di Bruno's formula, we get a sum of terms that all contain some factor $P^{(l)}(\beta)$ where $1 \leq l \leq m$. Thus we get the contradictory equation $b(P(\beta)-P(\alpha))^{N+1} = 0$ and we are done. □

The following lemma will be used at the tip of the inclusion chain.

Lemma 23. Let $A \subseteq \mathbb{K}[x]$ be a subalgebra of finite codimension where M is a set of non-equivalent spectral elements. If D is an α-derivation and

$$D = \sum_{\alpha_i \in M} c_i f(\alpha_i),$$

then all $c_i = 0$ and D is the zero derivation. Note that we allow both $\alpha \in M$ and $\alpha \notin M$.

Proof. Let $\alpha_1, \alpha_2, \ldots \alpha_n$ be a labeling of the elements in M. Now we define A_i to be the subalgebra of A obtained by adding the set of conditions $f(\alpha) = f(\alpha_1), f(\alpha) = f(\alpha_2), \ldots, f(\alpha) = f(\alpha_i)$. In A_n all elements in M are equivalent to α thus we have that $D(f) = cf(\alpha)$ for some scalar c. This is not an α-derivation for $c \neq 0$, hence $D(f) = 0$ for all $f \in A_n$. Now consider A_{n-1}. In

this subalgebra we have that $A_n = \ker(f \to f(\alpha) - f(\alpha_n)) \subseteq \ker(D)$, hence $D(f) = c(f(\alpha) - f(\alpha_i))$ for all $f \in A_{n-1}$ and some scalar c. By Lemma 20 we know that the $c(f(\alpha) - f(\alpha_i))$ isn't a derivation for non-zero c, and we see that $D(f) = 0$ for all $f \in A_{n-1}$. The step above may be repeated all the way up the inclusion chain until we arrive at the theorem statement. □

Now, the Main Conjecture.

Proof of the Main Conjecture. Let $C_1, C_2, \ldots, C_n$ be the clusters in A, and assume that $\alpha \in C_1$. Let D be a α-derivation over A. By the Main Theorem, we know that we can write

$$D = F + D_1 + D_2 + \ldots + D_n$$

where

$$D_i = \sum_{\alpha_j \in C_i} \sum_{k=1}^{N} c_{ijk} f^{(k)}(\alpha_j),$$

and

$$F = \sum_{\alpha_i \in M} c_i' f(\alpha_i)$$

Now, let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be a labeling of the elements of $\mathrm{Sp}(A)$. We define $A_{i,j}$ to be the subalgebra of A obtained by adding the conditions $f^{(k)}(\alpha_l) = 0$ for all α_l and $1 \leq k \leq i-1$ and also the conditions $f^{(i)}(\alpha_l)$ for all $1 \leq l \leq j$. Note that in each $A_{i,j}$ we have the same cluster structure as in A by Lemma 21. The subalgebras form an inclusion chain

$$A_{N,m} \subseteq A_{N,m-1} \subseteq A_{N,m-2} \subseteq \ldots \subseteq A_{N,1} \subseteq A_{N-1,m} \subseteq \ldots \subseteq A_{1,1} \subseteq A,$$

along which the proof will traverse inductively. An alternative picture of the chain that emphasizes its recursive nature may be seen bellow.

$$\begin{aligned}
A_{1,1} &= A \cap \ker(f \to f^{(1)}(\alpha_1)),\\
A_{1,2} &= A_{1,1} \cap \ker(f \to f^{(1)}(\alpha_2)),\\
&\vdots\\
A_{1,m} &= A_{1,m-1} \cap \ker(f \to f^{(1)}(\alpha_m)),\\
A_{2,1} &= A_{1,m} \cap \ker(f \to f^{(2)}(\alpha_1)),\\
&\vdots\\
A_{N,m} &= A_{N,m-1} \cap \ker(f \to f^{(N)}(\alpha_m)).
\end{aligned}$$

As $A_{i,j} \subseteq A$ we have that D is an α-derivation over each $A_{i,j}$. Moreover, $D_i(f) = 0$ for all $f \in A_{N,m}$ and $1 \leq i \leq n$. Hence $D = F$ in $A_{N,m}$. As we already know from Lemma 23, F has to be the zero derivation so $D(f) = 0$ for all $f \in A_{N,m}$. Now we move one step up along the inclusion chain. If $m > 1$, the algebra one step up along the chain is $A_{N,m-1}$ and if $m = 1$ it is $A_{N-1,m}$. Either way we denote the next algebra by B. In both cases $A_{N,m}$ may be obtained from B as the kernel of $f \to f^{(N)}(\alpha_m)$. Thus $A_{n,M} = \ker(f \to f^{(N)}(\alpha_m)) \subseteq \ker(D)$ in B hence $D(f) = cf^{(N)}(\alpha_m)$ for all $f \in B$. If $\alpha_m \not\sim \alpha$ we invoke Lemma 22 to obtain $c = 0$ and otherwise continue. Repeating the above steps all the way up the inclusion chain we only keep terms in D where derivatives are evaluated at spectral elements equivalent to α. The others are zeroed out by Lemma 22. What remains at the top is that

$$D(f) = \sum_{\alpha_i \sim \alpha} \sum_{j=1}^{N} c_{ij} f^{(j)}(\alpha_i).$$

for all $f \in A$. □

4 Acknowledgments

I want to thank my supervisors Anna Torstensson and Victor Ufnarovski for all their help over the summer and especially for being so generous with their ideas and sharing this research. They suggested which directions to take and which ideas that might be fruitful to explore. Victor also suggested the more direct method of proof presented here. The first proof required a detour via ideal subalgebras.

References

[1] Evgenii Alekseevich Gorin. "Subalgebras of finite codimension". In: *Mathematical notes of the Academy of Sciences of the USSR* 6.3 (1969), pp. 649–652.

[2] Rode Grönkvist, Erik Leffler, Anna Torstensson, and Victor Ufnarovski. "Describing subalgebras of $\mathbb{K}[x]$ using derivatives". In: (2021). arXiv: `2107.11916 [math.RA]`.