ON THE IMAGE CONJECTURE

ARNO VAN DEN ESSEN, DAVID WRIGHT, AND WENHUA ZHAO

Abstract. The Image Conjecture was formulated by the third author, who showed that it implied his Vanishing Conjecture, which is equivalent to the famous Jacobian Conjecture. We prove various cases of the Image Conjecture and show that how it leads to another fascinating and elusive assertion that we here dub the Factorial Conjecture. Various cases of the Factorial Conjecture are proved.

1. Introduction

The notion of a Mathieu subspace was introduced by coauthor Wenhua Zhao in [7], inspired by a conjecture of Olivier Mathieu ([3]), which was shown by Mathieu to imply the famed Jacobian Conjecture. The third author then formulated the Image Conjecture (Conjecture 2.1) upon noticing the resemblance of Mathieu's conjecture with his own Vanishing Conjecture, which he had shown to be equivalent to the Jacobian Conjecture ([6]). He proved that the Image Conjecture, for characteristic zero, implies the Vanishing Conjecture. This connection makes the Image Conjecture a matter of intrigue. The reader is referred to [1] for more details on this story.

We begin by defining a Mathieu subspace. Let k be a field and A a commutative k-algebra. Consider the following two conditions relating to a k-vector subspace $\mathcal{M}$ of A and an element f of A:

$$f^m \in \mathcal{M} \text{ for all } m \geq 1, \tag{M1}$$

and

$$\text{for any } g \in A, \text{ we have } f^m g \in \mathcal{M} \text{ for } m \gg 0. \tag{M2}$$

We will refer to these conditions by their labels (M1) and (M2) throughout this paper.

Definition 1.1. A sub-k-vector space $\mathcal{M}$ of A is called a *Mathieu subspace* if, for all $f \in A$, (M1) implies (M2).

2000 *Mathematics Subject Classification.* Primary: 14R15, 13N10: Secondary: 13A99, 13F20.

Key words and phrases. Mathieu subspace, Jacobian Conjecture, Vanishing Conjecture, Image Conjecture, regular sequence.

The research of the third author was partially supported by NSA Grant H98230-10-1-0168.

It is not difficult to verify that in the definition of Mathieu subspace the condition (M1) can be replaced by

$$\text{(M1}'\text{)} \qquad f^m \in \mathcal{M} \text{ for all } m \gg 0,$$

and although (M1) appeared in the original definition of Mathieu subspace given in [7], the authors have of late been stating the definition using (M1′), for the purpose of comparison with the definition of an ideal. A proof of the equivalence of the two definitions has been given in Proposition 2.1 of [9].

We list some basic facts about Mathieu subspaces, which we leave to the reader to verify:

(1) A and $\{0\}$ are Mathieu subspaces.
(2) If $\mathcal{M}$ is a Mathieu subspace and $1 \in \mathcal{M}$, then $\mathcal{M} = A$.
(3) Any ideal in A is a Mathieu subspace.
(4) The sum $\mathcal{M} + \mathcal{N}$ of two Mathieu subspaces is not necessarily a Mathieu subspace. (Hint: Use basic facts 2 and 3. Or, see Example 4.12 in [7].)

In the next section we will state the Image Conjecture, for which the notion of a Mathieu subspace is needed, and prove some special cases. Before we proceed, one more definition is in order.

Definition 1.2. For any ring A and variables $z_1, \ldots, z_n$, let $\mathcal{L} : A[z_1, \ldots, z_n] \to A$ be the A-linear map defined by $\mathcal{L}(z^i) = i!$ (meaning $\mathcal{L}(z_1^{\ell_1} \cdots z_n^{\ell_n}) = \ell_1! \cdots \ell_n!$).

Many of the results surrounding the conjecture involve this curious map $\mathcal{L}$, which will be at the heart of the Factorial Conjecture, introduced and discussed in Section 4.

2. The Image Conjecture

The Image Conjecture, formulated by the third author in [8][1], goes as follows:

Conjecture 2.1 (Image Conjecture). *Let k be a field and A be a k-algebra, and let $B = A[z_1, \ldots, z_n]$ be the polynomial ring in n variables over A. For $a_1, \ldots, a_n \in A$ a regular sequence, the image of the A-linear map $B^n \to B$ defined by $\mathcal{D} = (\partial_{z_1} - a_1, \ldots, \partial_{z_n} - a_n)$ is a Mathieu subspace in B.*

We will begin by showing the Image Conjecture is true when k has positive characteristic. We are most interested, though, in the case when k has characteristic zero, from which the Jacobian Conjecture would follow. For the characteristic zero case we have only a partial result for $n = 1$ (Theorem 2.8 below); beyond that the Image Conjecture remains a mystery.

Theorem 2.2. *Let A be an $\mathbb{F}_p$-algebra, and let $B = A[z_1, \ldots, z_n]$ be the polynomial ring in n variables over A. For $a_1, \ldots, a_n \in A$ a regular sequence, the image of the A-linear map $B^n \to B$ defined by $\mathcal{D} = (\partial_{z_1} - a_1, \ldots, \partial_{z_n} - a_n)$ is a Mathieu subspace in B.*

[1]The formulation in [8] assumes A is a $\mathbb{Q}$-algebra; however it is more general in its assumption about $\mathcal{D}$. See Conjecture 1.3 in [8].

Remark 2.3. The theorem fails if we drop the hypothesis that $a_1, \dots, a_n$ forms a regular sequence. This can be seen in the case $n = 1$, $A = \mathbb{F}_p$ (or any field of characteristic p), and $a_1 = 0$. In that case $1 = \partial_z z \in \operatorname{Im} \mathcal{D}$, but $z^{p-1} \notin \operatorname{Im} \mathcal{D}$, so $\operatorname{Im} \mathcal{D}$ is not a Mathieu subspace by item 2 in the Introduction. (This is Example 2.7 in [8]).

Before proving Theorem 2.2 we need some preliminary results, the first of which is a well-known fact about regular sequences.

Lemma 2.4. *Let A be a ring and let $a_1, \dots, a_n$ be a regular sequence A. If $g_1, \dots, g_n \in A$ are such that $\sum_{i=0}^n a_i g_i = 0$, then for each pair (i, j) with $1 \le i, j \le n$ and $i \ne j$ there exists an element $g_{ij} \in A$ such that $g_{ij} = -g_{ji}$ for each pair and $g_i = \sum_{j \ne i} g_{ij} a_j$.*

Proof. This follows from the exactness of the Koszul complex for the sequence $(a_1, \dots, a_n)$ (see [4], §18.D). □

For the rest of this section A, B, $a_1, \dots, a_n$, and $\mathcal{D}$ will be as in Theorem 2.2, and $\mathfrak{a}$ will denote the ideal $Aa_1 + \cdots + Aa_n$ of A. We will write z^r for the monomial $z_1^{r_1} \cdots z_n^{r_n}$. For the very next result A does not need to be an $\mathbb{F}_p$-algebra.

Lemma 2.5. *Let $g \in B = A[z]$ be of degree d, with g_d its degree d homogeneous summand. If $g \in \operatorname{Im} \mathcal{D}$, then all coefficients of g_d belong to the ideal $\mathfrak{a}$.*

Proof. Being in the image of $\mathcal{D}$, g has the form

$$g = \sum_{i=1}^{n} (\partial_{z_i} - a_i) h_i \tag{1}$$

for some $h_1, \dots, h_n \in B$. For $1 \le i \le n$ and any integer $m \ge 0$ we will denote by $h_{i,m}$ the degree m homogeneous summand of h_i. Let e be the maximum of the degrees of $h_1, \dots, h_n$. Since $\deg g = d$, it is clear from (1) that not all of $h_1, \dots, h_n$ can have degree strictly less than d, so we have $e \ge d$. If $e = d$ it follows from (1) that $g_d = -\sum_{i=1}^n a_i h_{i,d}$, and hence that all its coefficients belong to $\mathfrak{a}$, and we are done.

If $e > d$ then it follows from (1) that $\sum_{i=1}^n a_i h_{i,e} = 0$. We appeal to Lemma 2.4, replacing A with B (which is innocent, since $a_1, \dots, a_n$ is a regular sequence in B as well), which asserts the existence of polynomials $p_{ij,e} \in B$, for $i \ne j$, such that $p_{ij,e} = -p_{ji,e}$ and $h_{i,e} = \sum_{j \ne i} p_{ij,e} a_j$. Since each $h_{i,e}$ is homogeneous of degree e, we can replace $p_{ij,e}$ by its degree e homogeneous summand and assume $p_{ij,e}$ homogeneous of degree e as well.

More generally, we claim that for $m \ge d + 1$ we have, for each pair i, j with $i \ne j$, a polynomial $p_{ij,m}$, homogeneous of degree m and 0 if $m > e$, such that $p_{ij,m} = -p_{ji,m}$ and

$$h_{i,m} = \sum_{j \ne i} (p_{ij,m} a_j - \partial_{z_j} p_{ij,m+1}) . \tag{2}$$

Note that the preceding paragraph established exactly this for $m = e$, with $p_{ij,e+1} = 0$ as required. Suppose inductively that the polynomials have been found for larger values of m. Reading equation (1) in degree m gives

$$0 = \sum_{i=1}^{n} (\partial_{z_i} h_{i,m+1} - a_i h_{i,m}) \tag{3}$$

$$
\begin{aligned}
&= \sum_{i=1}^{n} \left(\partial_{z_i} \left(\sum_{j \neq i} (p_{ij,m+1} a_j - \partial_{z_j} p_{ij,m+2}) \right) - a_i h_{i,m} \right) \\
&= \sum_{i=1}^{n} \left(\partial_{z_i} \left(\sum_{j \neq i} p_{ij,m+1} a_j \right) - a_i h_{i,m} \right) - \sum_{i \neq j} \partial_{z_i} \partial_{z_j} p_{ij,m+2} \\
&= \sum_{i=1}^{n} \left(\partial_{z_i} \left(\sum_{j \neq i} p_{ij,m+1} a_j \right) - a_i h_{i,m} \right) \quad (\text{since } \partial_{z_i} \partial_{z_j} p_{ij,m+2} = -\partial_{z_j} \partial_{z_i} p_{ji,m+2}) \\
&= -\sum_{i=1}^{n} a_i \left(h_{i,m} + \sum_{j \neq i} \partial_{z_j} p_{ij,m+1} \right) \quad (\text{this uses } p_{ij,m+1} = -p_{ji,m+1}) \,. \qquad (4)
\end{aligned}
$$

From this equation, Lemma 2.4 provides polynomials $p_{ij,m} \in B$ with $p_{ij,m} = -p_{ji,m}$ such that $h_{i,m} + \sum_{j \neq i} \partial_{z_j} p_{ij,m+1} = \sum_{j \neq i} p_{ij,m} a_j$, which, solving for $h_{i,m}$, yields (2).

Finally, we complete the proof by reading (1) in degree d, which gives g_d as the right side of (3) with $m = d$, and hence (following the same reasoning) g_d is equal to (4), with $m = d$. This shows the coefficients of g_d lie in $\mathfrak{a}$. $\square$

We now will need to assume that A is an $\mathbb{F}_p$-algebra.

Corollary 2.6. *Let $f = \sum c_r z^r \in B$ with $c_r \in A$. If $f^p \in \operatorname{Im} \mathcal{D}$, then $c_r^p \in \mathfrak{a}$ for all r.*

Proof. The proof will be by induction on the number d of non-zero homogeneous summands of f. Write $f = f_1 + \cdots + f_d$ where f_i are non-zero homogeneous summands with $\deg f_i < \deg f_j$ when $i < j$. Then $f^p = f_1^p + \cdots + f_d^p$, and since $f^p \in \operatorname{Im} \mathcal{D}$ Lemma 2.5 says that all coefficients of f_d^p belong to $\mathfrak{a}$, and this proves the case $d = 1$. In any case f_d^p is the sum of monomials of the form $ca_i z^{pr}$ with $c \in A$, $r = (r_1, \ldots, r_n)$, $r_1 + \cdots + r_d = \deg f_d$. Since $ca_i z^{pr} = (\partial_i - a_i)(-cz^{rp}) \in \operatorname{Im} \mathcal{D}$, it follows that $f_d^p \in \operatorname{Im} \mathcal{D}$, so $f^p - f_d^p = f_1^p + \cdots + f_{d-1}^p \in \operatorname{Im} \mathcal{D}$, and the proof is complete by induction. $\square$

Lemma 2.7. *For all $r = (r_1, \ldots, r_n)$ we have $a_i^p z^r \in \operatorname{Im} \mathcal{D}$.*

Proof. Since $\partial_i^p = 0$ on B, we have $(-a_i)^p z^r = (\partial_i - a_i)^p z^r \in \operatorname{Im} \mathcal{D}$. $\square$

With these facts the proof of Theorem 2.2 follows quickly.

Proof of Theorem 2.2. We will show, more strongly, that if $f \in B$ with $f^p \in \operatorname{Im} \mathcal{D}$, then for any $g \in B$ we have $f^m g \in \operatorname{Im} \mathcal{D}$ when $m \geq p^2$. Let $f = \sum c_r z^r$ be such that $f^p \in \operatorname{Im} \mathcal{D}$. By Corollary 2.6 we have $c_r^p \in \mathfrak{a}$, hence $c_r^{p^2} \in Aa_1^p + \cdots + Aa_n^p$, for all r. Since $f^{p^2} = \sum c_r^{p^2} z^{p^2 r}$, it follows that for every $g \in B$ all coefficients of $f^m g$ belong to $Aa_1^p + \cdots + Aa_n^p$ if $m \geq p^2$. Therefore $f^m g \in \operatorname{Im} \mathcal{D}$ by Lemma 2.7. $\square$

For characteristic zero, the Image Conjecture is not even completely solved in the case $n = 1$. However, the theorem below solves a weak version of this case. Here z represents only one variable.

Theorem 2.8. *If A is a $\mathbb{Q}$-algebra and if $a \in A$ is a non-zero-divisor such that Aa is a radical ideal, then the image of $\mathcal{D} = \partial_z - a$ is a Mathieu subspace in $B = A[z]$.*

Remark 2.9. The proof of this theorem will appeal to a result from Section 4, namely Theorem 4.9, which says that if $f \in \mathbb{C}[z]$ (z representing one variable) and $\mathcal{L}(f^m) = 0$ for all $m \geq 0$, then $f = 0$. An easy use of the Lefschetz principle shows that the same holds replacing $\mathbb{C}$ by an arbitrary field of characteristic zero.

In the case where a is a unit in A it can be shown rather easily that $\operatorname{Im} \mathcal{D} = B$, hence is a Mathieu subspace. Just note that $\partial_z - a$ has the inverse map $(\partial_z - a)^{-1} = [-a(1 - a^{-1}\partial_z)]^{-1} = -a^{-1} \sum_{i=0}^{\infty} a^{-i}\partial_z^i$, which makes sense because ∂_z is locally nilpotent.

Therefore we make some preparations in the case a is not a unit, in which case $I = \cap_{i=1}^{\infty} Aa^i \neq A$. For $c \in A - I$ there exists a unique integer $m \geq 0$ such that $c \in Aa^m - Aa^{m+1}$. Setting $m = \infty$ if $c \in I$, we call m the a-order of c and denote it by $v_a(c)$. Since a is a non-unit in B as well, v_a extends to elements of B which do not lie in $\cap_{i=1}^{\infty} Ba^i$. It is clear that an element f of B of the form cz^i, then $v_a(f) = v_a(c)$.

In the following proposition $\mathcal{D}$ is as in Theorem 2.8. Here A can be any commutative ring, not necessarily a $\mathbb{Q}$-algebra.

Proposition 2.10. *Let $a \in A$ be a non-zero-divisor. Let $f = b_0 + b_1 z + \cdots + b_d z^d \in A[z]$.*

i) *If $f \in \operatorname{Im} \mathcal{D}$, then $b_d \equiv 0 \mod a$ and*

$$d!b_d + (d-1)!b_{d-1}a + (d-2)!b_{d-2}a^2 + \cdots + b_0 a^d \equiv 0 \mod a^{d+1}. \tag{5}$$

ii) *Conversely, let A be either a $\mathbb{Q}$-algebra or an $\mathbb{F}_p$-algebra such that $d < p$. If f satisfies* (5)*, then $f \in \operatorname{Im} \mathcal{D}$.*

Proof. For *i)* we can assume $b_d \neq 0$. If $d = 0$ the two statements coincide and are easy to prove. Assume $d \geq 1$ and $g \in \operatorname{Im} \mathcal{D}$, so that $f = (\partial_z - a)(c_0 + c_1 z + \cdots + c_d z^d)$. (Note that the polynomial on the inside must have the same degree as that of f, since a is not a zero-divisor.) In particular $b_d = -ac_d$, establishing the first assertion of *i)*, and therefore $f - (\partial_z - a)(c_d z^d) = b_0 + \cdots + b_{d-2}z^{d-2} + (b_{d-1} - dc_d)z^{d-1} \in \operatorname{Im} \mathcal{D}$. By induction on d we have $(d-1)!(b_{d-1} - dc_d) + (d-2)!b_{d-2}a + \cdots + b_0 a^{d-1} \equiv 0 \mod a^d$. Multiplying by a and using $b_d = -ac_d$ gives (5).

For *ii)*, note that the hypothesis and (5) imply that $b_d = -ac_d$ for some $c_d \in A$. If $d = 0$ all is clear. If $d \geq 1$ we again have $f - (\partial_z - a)(c_d z^d) = b_0 + \cdots + b_{d-2}z^{d-2} + (b_{d-1} - dc_d)z^{d-1}$, so $f \in \operatorname{Im} \mathcal{D}$ if and only if $b_0 + \cdots + b_{d-2}z^{d-2} + (b_{d-1} - dc_d)z^{d-1} \in \operatorname{Im} \mathcal{D}$. By induction it suffices to show $(d-1)!(b_{d-1} - dc_d) + (d-2)!b_{d-2}a + \cdots + b_0 a^{d-1} \equiv 0 \mod a^d$, or equivalently (since a is a non-zero-divisor), that $(d-1)!(b_{d-1}a - dac_d) + (d-2)!b_{d-2}a^2 + \cdots + b_0 a^d \equiv 0 \mod a^{d+1}$. Since $ac_d = -b_d$, this is precisely the hypothesis. □

Now we return to our assumption that A is a $\mathbb{Q}$-algebra.

Lemma 2.11. *An element of B of the form cz^i lies in the image of $\mathcal{D}$ if and only if $v_a(c) \geq i + 1$.*

Proof. This is immediate from Proposition 2.10. □

Corollary 2.12. *Let $f = c_0 + c_1z + \cdots + c_dz^d \in B$. If $v_a(c_i) \geq i+1$ for $0 \leq i \leq d$, then for each $g \in B$ we have $gf^m \in \operatorname{Im} \mathcal{D}$ for $m \gg 0$.*

Proof. Let $N = \deg g$ and let $m \geq N+1$. Note that each term cz^j in f^m satisfies $v_a(c) \geq j+m$. Hence each term cz^j of gf^m satisfies $v_a(c) \geq j+m-N \geq j+1$. By Lemma 2.11 each term of gf^m, and hence gf^m itself, lies in $\operatorname{Im} \mathcal{D}$. □

Lemma 2.13. *Let $f = c_0 + c_1z + \cdots + c_dz^d \in B$ be such that $v_a(c_i) \geq i$ for $0 \leq i \leq d$, and, for some $t \leq d$, $v_a(c_t) \geq t+1$. Let $\tilde{f} = f - c_tz^t$. If $f^m \in \operatorname{Im} \mathcal{D}$ for some $m \geq 1$, then $\tilde{f}^m \in \operatorname{Im} \mathcal{D}$.*

Proof. Writing $\tilde{f}^m = f^m + h$ one easily sees that the terms of h satisfy the hypothesis of Lemma 2.11, and so we have $h \in \operatorname{Im} \mathcal{D}$. Since $f^m \in \operatorname{Im} \mathcal{D}$, it follows that $\tilde{f}^m \in \operatorname{Im} \mathcal{D}$. □

Proof of Theorem 2.8. Let $f = c_0 + c_1z + \cdots + c_dz^d \in B$ be such that $f^m \in \operatorname{Im} \mathcal{D}$ for all $m \geq 1$. We will show that $v_a(c_i) \geq i+1$ for $0 \leq i \leq d$, which implies $\operatorname{Im} \mathcal{D}$ is a Mathieu subspace by virtue of Corollary 2.12.

Suppose, to the contrary, that $v_a(c_i) \leq i$ for some i. Let t be the maximum of the numbers $i - v_a(c_i)$, which, by our assumption is non-negative. Let $h = a^tf$. Then for each term cz^i of h we have $v_a(c_i) \geq i$, and equality holds for at least one i. Clearly $h^m \in \operatorname{Im} \mathcal{D}$ for all $m \geq 1$. Using Lemma 2.13 to remove the terms for which equality does not hold, we arrive at a polynomial $f = c_0 + c_1z + \cdots + c_dz^d \in B$ with $f^m \in \operatorname{Im} \mathcal{D}$ for all $m \geq 1$ having the property that $v_a(c_i) = i$ when $c_i \neq 0$. We have $c_i = a^ib_i$ with $b_i \in A$, and when $b_i \neq 0$ we have $b_i \notin Aa$. Letting $p = \sum b_iz^i$ we then have $f = p(az)$.

For any $g(z) \in B$, if g has degree $\leq N$ for some integer $N \geq 0$, it follows from Proposition 2.10 that $g(az) \in \operatorname{Im} \mathcal{D}$ if and only if $a^N\mathcal{L}(g) \equiv 0 \mod a^{N+1}$ ($\mathcal{L}$ as in Definition 1.2). Noting that $f^m = p^m(az)$ and $\deg p^m \leq md$ we thereby conclude $a^{md}\mathcal{L}(p^m) \equiv 0 \mod a^{md+1}$ for all $m \geq 1$. Since a is not a zero-divisor, we get $\mathcal{L}(p^m) \equiv 0 \mod a$ for all $m \geq 1$. Let s be the smallest of all i such that $b_i \neq 0$. Then $b_s \notin Aa$. We are assuming Aa is a radical ideal, hence it is the intersection of the prime ideals containing it. Therefore there is a prime ideal $\mathcal{P}$ in A containing Aa but not containing b_s. Letting $\bar{p}$ be the image of p in $k[z]$ where k is the fraction field of $A/\mathcal{P}$, we have $\bar{p} \neq 0$ and $\mathcal{L}(\bar{p}^m) = 0$. But this contradicts Theorem 4.9 (see Remark 2.9). □

3. Specific version of the Image Conjecture relevant to the Vanishing and Jacobian Conjectures

The following specific version of the Image Conjecture, from [8], is of special interest. For this we let $\xi = (\xi_1, \ldots, \xi_n)$ and $z = (z_1, \ldots, z_n)$ be two sets of commuting indeterminates, and we consider the commuting operators $\mathcal{D}_i = \xi_i - \partial_{z_i}$, $1 \leq i \leq n$, on the polynomial ring $A = \mathbb{C}[\xi, z]$. We consider the map $\mathcal{D} = (\mathcal{D}_1, \ldots, \mathcal{D}_n) : A^n \to A$.

Conjecture 3.1 (Special Image Conjecture)**.** *The image of $\mathcal{D}$ is a Mathieu subspace.*

In [8] it is shown that the above conjecture implies the Jacobian Conjecture.[2] More specifically, it is shown that it suffices to show that

[2]One has to prove the conjecture for all $n \geq 1$, which then implies the Jacobian Conjecture for all $n \geq 1$.

Theorem 3.2 ([8], Theorem 3.7)**.** *The following two statements are equivalent:*

1. *For any $f \in \mathbb{C}[\xi, z]$ of the form $(\xi_1^2 + \cdots + \xi_n^2)P$ with $P \in \mathbb{C}[z]$ and P is homogeneous of degree four, then $f^m \in \operatorname{Im}\mathcal{D}$ for all $m \geq 1$ implies that, for each $g \in \mathbb{C}[z]$, $f^m g \in \operatorname{Im}\mathcal{D}$ for all $m \gg 0$.*
2. *The Jacobian Conjecture holds in all dimensions $n \geq 1$.*

We now give a realization of the image of $\mathcal{D}$ that is established in [8]. Let $\mathcal{E}$ be the $\mathbb{C}$-linear map from $\mathbb{C}[\xi, z]$ to $\mathbb{C}[z]$ defined by sending a monomial $\xi_1^{\alpha_1} \cdots \xi_n^{\alpha_n} z_1^{\beta_1} \cdots z_n^{\beta_n}$ to $\partial_{z_1}^{\alpha_1} \cdots \partial_{z_n}^{\alpha_n} z_1^{\beta_1} \cdots z_n^{\beta_n}$. Then:

Theorem 3.3 ([8], Theorem 3.1)**.** $\operatorname{Im}\mathcal{D} = \operatorname{Ker}\mathcal{E}$.

This obviously makes it much easier to determine whether an element lies in $\operatorname{Im}\mathcal{D}$, as $\mathcal{E}$ is easy to apply.

We now set $\mathcal{M} = \operatorname{Im}\mathcal{D}$ ($= \operatorname{Ker}\mathcal{E}$) and make a number of observations, letting $A = \mathbb{C}[\xi, z]$ as above, first noting that, by Theorem 3.3, condition (M1) coincides with

$$\mathcal{E}(f^m) = 0 \text{ for all } m \geq 1$$

in this context.

We define a multi-grading on the polynomial ring $\mathbb{C}[\xi, z]$ by setting the multi-degree of a monomial $\xi_1^{i_1} \cdots \xi_n^{i_n} z_1^{j_1} \cdots z_n^{j_n}$ to be $(j_1 - i_1, \ldots, j_n - i_n)$. We also have the ordinary grading on $\mathbb{C}[\xi, z]$ by which $\xi_1, \ldots, \xi_n$ each have degree -1 and $z_1, \ldots, z_n$ each have degree 1. The motivation for these choices is the map $\mathcal{E}$, which preserves $z_1, \ldots, z_n$ but converts $\xi_1, \ldots, \xi_n$ to operators which lower degree by one. In the discussion below, "multi-degree" refers to the former; "degree" refers to the latter. With $\mathbb{C}[z]$ viewed as a subring of $A = \mathbb{C}[\xi, z]$, these gradings restrict to give a multi-grading and a grading on $\mathbb{C}[z]$. Note that the map $\mathcal{E} : A \to \mathbb{C}[z]$ preserves both the multi-degree and the degree of a monomial.

1. Condition (M2) is satisfied if it holds whenever g is a monomial in A.
2. We can write any $f \in A$ as a sum of terms of the form $z_1^{r_1} \cdots z_n^{r_n} Q$ where Q has multi-degree $(0, \ldots, 0)$, and $(r_1, \ldots, r_n) \in \mathbb{Z}^n$. These terms are just the multi-homogeneous summands of f. Any $Q(\xi, z)$ of multi-degree $(0, \ldots, 0)$ can be written in the form $q(U_1, \ldots, U_n)$ where $U_i = \xi_i z_i$ for $i = 1, \ldots, n$.
3. If f is multi-homogeneous of multi-degree $(r_1, \ldots, r_n)$, in other words if f has the form $z_1^{r_1} \cdots z_n^{r_n} q(U_1, \ldots, U_n)$, then:
   (a) If $r_1, \ldots, r_n \geq 0$ then $\mathcal{E}(f) = c z_1^{r_1} \cdots z_n^{r_n}$ for some $c \in \mathbb{C}$ (since $\mathcal{E}$ preserves multi-degree).
   (b) If $r_i < 0$ for some i then $\mathcal{E}(f) = 0$.

   Note that if (b) holds for f then it holds for f^m for any $m \geq 1$, hence (M1) holds for f. Moreover it's easy to see that, for any $g \in A$, (b) holds for all multi-homogeneous terms of $f^m g$, for $m \gg 0$, so (M2) holds for f as well.
4. For any $f \in A$, let N_f be the convex polyhedron (Newton polyhedron) in $\mathbb{R}^n$ determined by the finite set of points $(r_1, \ldots, r_n)$ which are multi-degrees of the nonzero terms $z_1^{r_1} \cdots z_n^{r_n} q(U)$ (as above) appearing in f.

(5) Note that if $f \in A$ is such that there exists i such that the multi-degree of all multi-homogeneous summands of f have negative i-coordinate, then again we have $\mathcal{E}(f^m) = 0$ for all $m \geq 1$ and $\mathcal{E}(f^m g) = 0$ for all $g \in A, m \gg 0$, hence f satisfies (M1) and (M2). This condition simply says that N_f lies in the half space $\{(x_1, \dots, x_n) \in \mathbb{R}^n \,|\, x_i < 0\}$.

(6) More generally, if there exists a hyperplane $H \subset \mathbb{R}^n$ through the origin such that the strictly positive n-tant $\{(x_1, \dots, x_n) \in \mathbb{R}^n \,|\, x_1, \dots, x_n > 0\}$ and N_f lie strictly on opposite sides of H, then $\mathcal{E}(f^m) = 0$ for all $m \geq 1$ and $\mathcal{L}(f^m g) = 0$ for all $g \in A, m \gg 0$, hence f satisfies (M1) and (M2). This can be seen as follows: There is a nonzero vector $v = (v_1, \dots, v_n) \in \mathbb{R}^n$ such that $v_1, \dots, v_n \geq 0$ and such that $H = \{x \in \mathbb{R}^n \,|\, (x \cdot v) = 0\}$ (usual inner product). Then $(v \cdot r) < 0$ for all $r \in N_f$. It follows that for all terms $z_1^{s_1} \cdots z_n^{s_n} q(U_1, \dots, U_n)$ of f^m, where $m \geq 1$, we must have $(v \cdot s) < 0$, where $s = (s_1, \dots, s_n)$ (in other words all points on the Newton polyhedron of f^m lies below H). Therefore we must have $s_i < 0$ for some i, from which it follows that $\mathcal{E}(f^m) = 0$. Similarly, if $g \in A$ then for sufficiently large m, all points in the Newton polyhedron of $f^m g$ are below H, so that $\mathcal{E}(f^m g) = 0$.

(7) If $f \in A$ and N_f has an extremal point $(r_1, \dots, r_n)$ corresponding to the term $z^r q(U) = z_1^{r_1} \cdots z_n^{r_n} q(U_1, \dots, U_n)$, then the point $(mr_1, \dots, mr_n)$ lies on the Newton polyhedron of f^m (from the term $z^{mr} q(U)^m = z_1^{mr_1} \cdots z_n^{mr_n} q(U_1, \dots, U_n)^m$), and in fact is an extremal point. Thus if f satisfies (M1), so does the multi-homogeneous summand $z^r q(U)$.

(8) We suspect that it cannot happen that a nonzero multi-homogeneous element $z^r q(U)$ with $r_1, \dots, r_n \geq 0$ satisfies (M1). If this suspicion is true, then by the last item, the Newton polyhedron of an $f \in A$ satisfying (M1) cannot have an extremal point in the closed positive n-tant $\{(x_1, \dots, x_n) \in \mathbb{R}^n \,|\, x_1, \dots, x_n \geq 0\}$.

(9) To address the problem in the previous item, note that if a multi-homogeneous element $f = z_1^{r_1} \cdots z_n^{r_n} q(U_1, \dots, U_n)$ satisfies (M1), i.e., $\mathcal{E}(f^m) = 0$ for all $m \geq 1$, then so does $\xi_1^{r_1} \cdots \xi_n^{r_n} f = U_1^{r_1} \cdots U_n^{r_n} q(U)$, which has multi-degree $(0, \dots, 0)$. Thus we need to show that if $h \in \mathbb{C}[U_1, \dots, U_n]$ and if $\mathcal{E}(h^m) = 0$ for all $m \geq 1$, then $h = 0$. This will be Conjecture 4.2 below.

Recall that $U_i = \xi_i z_i$. One sees that for a monomial $U^\ell = U_1^{\ell_1} \cdots U_n^{\ell_n}$ we have $\mathcal{E}(U^\ell) = \ell! = \ell_1! \cdots \ell_n!$. Thus the map $\mathcal{E}$ restricted to $\mathbb{C}[U_1, \dots, U_n]$ is precisely the map $\mathcal{L}$ of Definition 1.2. In the conjectures below $U = (U_1, \dots, U_n)$ can be taken to be any system of variables (forgetting ξ and z for the moment), and $\mathcal{L} : \mathbb{C}[U_1, \dots, U_n] \to \mathbb{C}$ the $\mathbb{C}$-linear map sending U^ℓ to $\ell!$.

4. The Factorial Conjecture

It follows from the discussion of the preceding section that the following assertion, which draws interest merely by virtue of its simplicity, is necessary for the Image Conjecture to hold.

Conjecture 4.1. *The kernel of $\mathcal{L} : \mathbb{C}[U_1, \dots, U_n] \to \mathbb{C}$ is a Mathieu subspace.*

As per items 8 and 9 above, we propose the stronger assertion, which we dub the Factorial Conjecture:

Conjecture 4.2 (Factorial Conjecture)**.** *Let $f \in \mathbb{C}[U_1, \ldots, U_n]$ be such that $\mathcal{L}(f^m) = 0$ for all $m \geq 1$. Then $f = 0$.*

As seen above, this conjecture would imply that the Newton polyhedron of any $f \in A = \mathbb{C}[\xi, z]$ satisfying (M1) has no extremal points in the closed positive n-tant.

The Factorial Conjecture looks innocent on first glance; one would think it is either easy to prove or else a counterexample should be findable. However no proof or counterexample has yet been given. The authors believe it to be true and will devote quite a bit of effort below in showing that the condition $\mathcal{L}(f^m) = 0$ for all $m \geq 1$ implies $f = 0$ in various situations. In this case we say "the Factorial Conjecture holds for f".

As a first observation, let us note that the Factorial Conjecture holds for $f = cM$ where $c \in \mathbb{C}$ and M is a monomial in $\mathbb{C}[U]$, since the condition $\mathcal{L}(f) = 0$ obviously implies $c = 0$. More strongly we have:

Proposition 4.3. *The Factorial Conjecture holds for $f \in \mathbb{C}[U_1, \ldots, U_n]$ of the form $c_1M_1 + c_2M_2$, where M_1, M_2 are monomials and $c_1, c_2 \in \mathbb{C}$. More strongly, $\mathcal{L}(f) = \mathcal{L}(f^2) = 0$ implies $f = 0$ in this case.*

The proof will involve the following observation.

Remark 4.4. The one-variable formula $\int_0^\infty U^k e^{-U} dU = k!$ (easily proved inductively using integration by parts) leads to the multi-variable formula

$$\int_{D_n} U^k e^{-U} dU = k!$$

where $U^k = U_1^{k_1} \cdots U_n^{k_n}$ and $k! = k_1! \cdots k_n!$, $dU = dU_1 \cdots dU_n$, and D_n is the non-negative n-tant $U_1 \geq 0, \ldots, U_n \geq 0$ in $\mathbb{R}^n$. It follows that for $f \in \mathbb{C}[U_1, \ldots, U_n]$, $\mathcal{L}(f)$ can be realized as

$$\mathcal{L}(f) = \int_{D_n} f(U) e^{-U} dU \tag{6}$$

(which, incidentally, gives a way to calculate $\mathcal{L}(f)$ using a symbolic algebra program such as Maple). Letting $\langle\ ,\ \rangle$ be the Hermitian inner product defined on $\mathbb{C}[U]$ by

$$\langle f, g \rangle = \int_{D_n} f(U) \overline{g(U)} e^{-U} dU \tag{7}$$

we note that this restricts to a positive definite form on $\mathbb{R}[U]$, and that $\mathcal{L}(f^2) = \langle f, f \rangle$, which must be strictly positive if $f \in \mathbb{R}[U]$ and $f \neq 0$.

Proof of Proposition 4.3. We have $\mathcal{L}(f) = c_1L_1 + c_2L_2 = 0$ with $L_1, L_2 \in \mathbb{Z} - \{0\}$, so $c_2 = -c_1L_1/L_2$ and $f = c_1h$ where $h = M_1 - (L_1/L_2)M_2 \in \mathbb{Q}[U] - \{0\}$. From Remark 4.4 we have $0 = \mathcal{L}(f^2) = \langle f, f \rangle = c_1\bar{c_1}\langle h, h \rangle$, which shows $c_1 = 0$, since $\langle h, h \rangle > 0$. By symmetry we have $c_2 = 0$, so $f = 0$. □

Now we make two remarks that will be important in several of the proofs that follow.[3] The first remark shows that to prove the Factorial Conjecture we may assume f has coefficients which are algebraic numbers.

Remark 4.5 (Algebraic reduction)**.** Given a collection of monomials $M_1, \ldots, M_d \in \mathbb{C}[U]$ (where U represents $U_1, \ldots, U_n$), we consider whether there exists $f \neq 0$ of the form $\sum_{i=1}^d c_i M_i$ which satisfy $\mathcal{L}(f^m) = 0$ for all $m \geq 1$. Thinking of of $c_1, \ldots, c_d$ as indeterminates, we note that $\mathcal{L}(f^m)$ is a homogeneous polynomial of degree m in $\mathbb{Z}[c_1, \ldots, c_d]$. By the Nullstellensatz, the existence of a nonzero solution is equivalent to saying the polynomials $\mathcal{L}(f^m)$ generate a homogeneous ideal in $\mathbb{Q}[c_1, \ldots, c_d]$ whose radical is strictly contained in the ideal generated by the indeterminates $c_1, \ldots, c_d$, which, in turn, is equivalent to the existence of a nonzero solution over $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$. Similarly, if f has the form $h + \sum_{i=1}^d c_i M_i$ where h is a nonzero polynomial in $\mathbb{Q}[U]$ not involving the monomials $M_1, \ldots, M_d$, then consider the ideal generated by the (non-homogeneous) polynomials $\mathcal{L}(f^m)$ in $\mathbb{Q}[c_1, \ldots, c_d]$. The existence of a solution over $\mathbb{C}$ is equivalent to saying this ideal is not all of $\mathbb{Q}[c_1, \ldots, c_d]$, which is equivalent to the existence of a solution over $\overline{\mathbb{Q}}$.

Remark 4.6 (Extension of primes)**.** Given any $c_1, \ldots, c_d \in \overline{\mathbb{Q}}$, the ring $\mathbb{Q}[c_1, \ldots, c_d]$ has a ring extension $\mathcal{O}$ in $\overline{\mathbb{Q}}$ which is integral over $\mathbb{Z}[1/\ell]$, for some $\ell \in \mathbb{Z}$, and we can take $\mathcal{O}$ to be a Dedekind ring (replacing $\mathcal{O}$ by its integral closure). Hence for all but finitely many primes $p \in \mathbb{Z}$ (specifically, those primes not dividing ℓ), $p\mathbb{Z}$ extends to a prime ideal of $\mathcal{O}$, or, equivalently, $\mathcal{O}$ has a (not necessarily unique) valuation v_p which has positive value at p. We will say "v_p is a valuation lying over p". For $k \in \mathbb{Z}$ it will then be the case that $v_p(k) > 0$ if and only if p divides k in $\mathbb{Z}$.

Proposition 4.7. *The Factorial Conjecture holds for $f \in \mathbb{C}[U_1, \ldots, U_n]$ having the form $f = Mh$ where M is a monomial and h has nonzero constant term.*

Proof. Suppose such an f has the property $\mathcal{L}(f^m) = 0$ for $m \geq 1$. We can assume the constant term of h is 1, and that $h \neq 1$ Then $f = M + c_1 M_1 + \cdots + c_d M_d$ where $M_1, \ldots, M_d$ are monomials properly divisible by M. For any prime $p \in \mathbb{Z}$ we have

$$f^p = M^p + \sum_{i=1}^d c_i^p M_i^p + p \sum_j g_j(c_1, \ldots, c_d) N_j \tag{8}$$

where, for each j, $g_j(c_1, \ldots, c_d) \in \mathbb{Z}[c_1, \ldots, c_d]$ and N_j is a monomial divisible by M^p. Write $M = U^\alpha, M_1 = U^{\alpha_1}, \ldots, M_d = U^{\alpha_d}$, and $N_j = U^{\beta_j}$. Applying $\mathcal{L}$ to (8) yields

$$\mathcal{L}(f^p) = (p\alpha)! + \sum_{i=1}^d c_i^p (p\alpha_i)! + p \sum_j g_j(c_1, \ldots, c_d) \beta_j! = 0\,. \tag{9}$$

We make two observations: Since M properly divides M_i, we have $\alpha < \alpha_i$, so $(p\alpha)!$ divides $(p\alpha_i)!$ in $\mathbb{Z}$ and moreover, p divides $(p\alpha_i)!/(p\alpha)!$ in $\mathbb{Z}$. Secondly, since M^p divides N_j, $(p\alpha)!$

[3] It should be acknowledged that the technique of making reductions using these ideas is due to Mitya Boyarchenko.

divides $(p\beta_j)!$ in $\mathbb{Z}$. Dividing (9) by $(p\alpha)!$, we get

$$1+\sum_{i=1}^{d} c_i^p \frac{(p\alpha_i)!}{(p\alpha)!}+p\sum_j g_j(c_1,\ldots,c_d)\frac{\beta_j!}{(p\alpha)!}=0\,,$$

which shows that p divides 1 in $\mathbb{Z}[c_1,\ldots,c_d]$. However, only finitely many primes can be units in $\mathbb{Z}[c_1,\ldots,c_d]$, so choosing p to avoid this finite set brings us to a contradiction. □

Proposition 4.7 has these two immediate consequences:

Proposition 4.8. *The Factorial Conjecture holds for $f\in\mathbb{C}[U_1,\ldots,U_n]$ having nonzero constant term.*

Proof. Apply Proposition 4.7 with $M=1$. □

Theorem 4.9. *The Factorial Conjecture holds for $n=1$.*

Proof. Any nonzero polynomial in one variable has the form $f=Mh$ of Proposition 4.7. □

The following says something a little different from Proposition 4.7.

Proposition 4.10. *The Factorial Conjecture holds for $f\in\mathbb{C}[U_1,\ldots,U_n]$ of the form $cM_0+\sum_{i=1}^d c_iM_i$ where $M_0=U_1^{k_1}\cdots U_n^{k_n}$ with $k_1\geq 1$ and $k_1\geq k_i$ for $i=2,\ldots,n$, $c,c_1,\ldots,c_d\in\mathbb{C}$ with $c\neq 0$, and $M_1,\ldots,M_d$ are monomials each divisible by $U_1^{k_1+1}$.*

Proof. Assume such an f has the property $\mathcal{L}(f^m)=0$ for $m\geq 1$. We may assume $c=1$ and that $c_1,\ldots,c_d\in\overline{\mathbb{Q}}$, by Remark 4.5. Choose a Dedekind overring $\mathcal{O}$ of $\mathbb{Z}[c_1,\cdots,c_d]$ as in Remark 4.6. Writing

$$\begin{aligned}
f^m &= (M_0+\sum_{i=1}^d c_iM_i)^m\\
&= \sum_{i_0+i_1+\cdots+i_d=m}\binom{m}{i_0,i_1,\ldots,i_d}c_1^{i_1}\cdots c_d^{i_d}M_0^{i_0}M_1^{i_1}\cdots M_d^{i_d}\\
&= M_0^m+\sum_{i=1}^m\sum_{i_1+\cdots+i_d=i}\frac{m!}{(m-i)!i_1!\cdots i_d!}c_1^{i_1}\cdots c_d^{i_d}M_0^{m-i}M_1^{i_1}\cdots M_d^{i_d}\,,
\end{aligned}$$

we have

$$0=\mathcal{L}(f^m)=\mathcal{L}(M_0^m)+\sum_{i=1}^m\sum_{i_1+\cdots+i_d=i}\frac{m!}{(m-i)!i_1!\cdots i_d!}c_1^{i_1}\cdots c_d^{i_d}\mathcal{L}(M_0^{m-i}M_1^{i_1}\cdots M_d^{i_d}) \tag{10}$$

Let us note that, by our assumption about M_0, mk_1+1 does not divide $\mathcal{L}(M_0^m)$ in $\mathbb{Z}$ if mk_1+1 is prime. Also, by our assumptions about $M_1,\ldots,M_d$, mk_1+1 does divide each of the terms $\mathcal{L}(M_0^{m-i}M_1^{i_1}\cdots M_d^{i_d})$ appearing in (10). Using Dirichlet's prime number theorem[4] we can select a prime number p of the form mk_1+1 for which $\mathcal{O}$ has a valuation

[4]which asserts that for any two positive coprime integers a and b, there are infinitely many primes of the form $a+nb$, where $n\geq 0$. See Theorem 66 and Corollary 4.1 in [2].

v_p over p. Viewing (10) as an equation in $\mathcal{O}$, we see that v_p takes on positive values at each summand $\mathcal{L}(M_0^{m-i}M_1^{i_1}\cdots M_d^{i_d})$. For the first term, however, we have $\mathcal{L}(M_0^m)=k_1!\cdots k_n!$, which is not divisible by p in $\mathbb{Z}$ by our assumption, and hence $v_p(\mathcal{L}(M_0^m))=0$. This gives a contradiction, since the sum is 0. ☐

Proposition 4.11. *The Factorial Conjecture holds for $f\in\mathbb{C}[U_1,\dots,U_n]$ a power of a linear homogenous form.*

Proof. We have $f=g^r$ where $g=\sum_{i=1}^n c_iU_i$. We concern ourselves with g for a moment. For $m>0$ an integer we have $g^m=\sum_{i_1+\cdots+i_n=m}\binom{m}{i_1,\dots,i_n}c_1^{i_1}\cdots c_n^{i_n}U_1^{i_1}\cdots U_n^{i_n}$. Thus $\mathcal{L}(g^m)=\sum_{i_1+\cdots+i_n=m}\frac{m!}{i_1!\cdots i_m!}c_1^{i_1}\cdots c_n^{i_n}i_1!\cdots i_m!=m!\sum_{i_1+\cdots+i_n=m}c_1^{i_1}\cdots c_n^{i_n}$. Let us denote by h_m the polynomial $\sum_{i_1+\cdots+i_n=m}c_1^{i_1}\cdots c_n^{i_n}$, viewing $c_1,\dots,c_n$ as indeterminates for the moment.

The polynomials $h_1,h_2,\dots\in\mathbb{C}[c_1,\dots,c_n]$ are related to the elementary symmetric polynomials $s_1,\dots,s_n$ (where $s_m=\sum_{1\le i_1<\cdots<i_m\le n}c_{i_1}\cdots c_{i_m}$) in the following way: Let T be an indeterminate, and set $S(T)=\prod_{i=1}^n(1-c_iT)=1-s_1T+s_2T^2-\cdots+(-1)^ns_nT^n$. In $\mathbb{C}[c_1,\dots,c_n][[T]]$ we have $S(T)^{-1}=\prod_{i=1}^n\frac{1}{(1-c_iT)}=\prod_{i=1}^n(1+c_iT+c_i^2T^2+\cdots)=1+h_1T+h_2T^2+\cdots$, and we let $P(T)$ be the latter power series. Now we specialize to $c_1,\dots,c_n\in\mathbb{C}$ and view $S(T)$ and $P(T)$ as elements of $\mathbb{C}[T]$, $\mathbb{C}[[T]]$, respectively.

Returning to $f=g^r$, we see that our hypotheses $\mathcal{L}(f^m)=0$ for $m\ge 1$ says that $h_{mr}=0$ for $m\ge1$. By Theorem 4.13, we must have $S(T)=1$, i.e., $s_1,\dots,s_n$ vanish at $(c_1,\dots,c_n)$. It is well-known (and easily seen) that the only zero of $s_1,\dots,s_n$ is $(0,\dots,0)$, so we must have $g=0$. ☐

Remark 4.12. In the case where f itself is a linear form one can easily see from the proof that, more strongly, $\mathcal{L}(f)=\mathcal{L}(f^2)=\cdots=\mathcal{L}(f^n)=0$ implies $f=0$.

Theorem 4.13 (N. Mohan Kumar)**.** *Let $S(T)\in\mathbb{C}[T]$ with constant term 1, and let $P(T)=1+a_1T+a_2T^2+\cdots$ be it's multiplicative inverse in the power series ring $\mathbb{C}[[T]]$. If there exists an integer $r>0$ such that $a_{mr}=0$ for all $m\ge1$, then $S(T)=1$.*

Proof. We note that $\mathbb{C}[[T]]$ is a free module over $B=\mathbb{C}[[T^r]]$ with basis $\{1,T,\cdots,T^{r-1}\}$, and that $\mathbb{C}[T]$ is free over $A=\mathbb{C}[T^r]$ with the same basis. Accordingly, we write $P(T)=B_0+B_1T+\cdots+B_{r-1}T^{r-1}$ and $S(T)=A_0+A_1T+\cdots+A_{r-1}T^{r-1}$ with $B_0,\dots,B_{r-1}\in B$, and $A_0,\dots,A_{r-1}\in A$. Our assumption about $P(T)$ clearly shows $B_0=1$, since the constant term is the only power of T^r that has non-zero coefficient. Now we tensor $\mathbb{C}[T]$ and $\mathbb{C}[[T]]$ with the rational function field $K=\mathbb{C}(T^r)$, which is the field of fractions of A. This gives the containment $\mathbb{C}[T]\otimes_AK\subset\mathbb{C}[[T]]\otimes_AK$. The first ring is the field $\mathbb{C}(T)$ (since T is algebraic over $\mathbb{C}(T^r)$), which is free over $K=\mathbb{C}(T^r)$ with basis $\{1,T,\cdots,T^{r-1}\}$; the second ring is the field of Laurent power series ring $\mathbb{C}[[T]][T^{-1}]$, which is free with the same basis over $L=\mathbb{C}[[T^r]]\otimes_AK=\mathbb{C}[[T^r]][T^{-r}]$, which is the field of Laurent power series in

T^r. So we have:

$$\begin{array}{ccccccc} S(T) & = & A_0 + A_1T + \cdots + A_{r-1}T^{r-1} & & 1 + B_1T + \cdots + B_{r-1}T^{r-1} & = & P(T) \\ & & \Cap & & \Cap & & \\ & & A \oplus AT \oplus \cdots \oplus AT^{r-1} & \subset & B \oplus BT \oplus \cdots \oplus BT^{r-1} & & \\ & & \cap & & \cap & & \\ \mathbb{C}(T) & = & K \oplus KT \oplus \cdots \oplus KT^{r-1} & \subset & L \oplus LT \oplus \cdots \oplus LT^{r-1} & & \end{array}$$

Since $S(T)$ lies in the field $\mathbb{C}(T) = K \oplus KT \oplus \cdots \oplus KT^{r-1}$, so must its inverse $P(T)$, and this shows that $B_1, \ldots, B_{r-1}$ lie in $K = \mathbb{C}(T^r)$. Let $Q \in \mathbb{C}[T^r]$ be a common denominator for $B_1, \ldots, B_{r-1}$ as rational functions in T^r. Then

$$Q = QP(T)S(T) = (Q + QB_1T + \cdots + QB_{r-1}T^{r-1})S(T)\,.$$

Since $Q, QB_1, \ldots, QB_{r-1}$ all lie in $\mathbb{C}[T^r]$ there is no cancellation amongst summands of $Q + QB_1T + \cdots + QB_{r-1}T^{r-1}$. Hence its degree is at least the degree of Q. This shows the degree of $S(T)$ is zero, i.e., $S(T) = 1$, as desired. □

We have not succeeded in proving that the Factorial Conjecture holds for more general homogeneous polynomials, except in a few situations given below.

Proposition 4.14. *The Factorial Conjecture holds for $f \in \mathbb{C}[U_1, U_2]$ a quadratic homogenous form in two variables.*

Proof. Writing $f = c_{20}U_1^2 + c_{11}U_1U_2 + c_{02}U_2^2$ we have

$$f^m = \sum_{i+j+k=m} \frac{m!}{i!j!k!} c_{20}^i c_{11}^j c_{02}^k U_1^{2i+j} U_2^{j+2k}$$

so that

$$\begin{aligned} \mathcal{L}(f^m) &= \sum_{i+j+k=m} \frac{m!}{i!j!k!} c_{20}^i c_{11}^j c_{02}^k (2i+j)!(j+2k)! \\ &= \sum_{0 \le i+k \le m} \frac{m!}{i!(m-i-k)!k!} c_{20}^i c_{02}^k c_{11}^{m-i-k} (m+i-k)!(m-i+k)! = 0\,. \end{aligned} \tag{11}$$

Let M be the sum of the terms in above where $k = i$, i.e.,

$$M = \sum_{0 \le 2i \le m} \frac{m!}{(i!)^2(m-2i)!} (m!)^2 (c_{20}c_{02})^i c_{11}^{m-2i}\,.$$

By the integrality reduction (Remark 4.5) we can assume c_{20}, c_{11}, c_{02} lie in a ring $\mathcal{O}$ which is Dedekind and integral over $\mathbb{Z}[1/\ell]$ for some $\ell \in \mathbb{Z}$, $\ell \neq 0$. Let $p = 2r + 1 \in \mathbb{Z}$ be an odd prime which corresponds to a valuation in $\mathcal{O}$, and consider the above equations with $m = 2r$. Let us note that p divides all of the summands of (11) except those comprised by M, i.e., those for which $k \neq i$ (for if, say, $i > k$, then $p \,|\, (m+i-k)!$). Thus we have $\mathcal{L}(f^m) \equiv M \mod p$. From Lemma 4.15 below we get

$$0 \equiv M \equiv \sum_{i=0}^{r} \binom{r}{i} c_{11}^{2r-2i}(-4c_{20}c_{02})^i = (c_{11}^2 - 4c_{20}c_{02})^r \mod p$$

Hence p divides $(c_{11}^2 - 4c_{20}c_{02})^r$ in $\mathcal{O}$. This shows that $d = c_{11}^2 - 4c_{20}c_{02}$ has a positive valuation for infinitely many valuations of $\mathcal{O}$, which shows that $d = 0$. Since d is the discriminant of f, we conclude that f is the square of a linear form in $\mathbb{C}[U_1, U_2]$, so we are in the situation of Proposition 4.11, and the proof is complete, modulo the lemma below. □

Lemma 4.15. *For $p = 2r+1 \in \mathbb{Z}$ an odd prime, we have, setting $m = 2r$,*

$$\frac{(m!)^3}{(i!)^2(m-2i)!} \equiv \binom{r}{i}(-4)^i \mod p$$

for $0 \leq i \leq r$.

Proof. We have $m! \equiv -1 \mod p$ by Wilson's Theorem,[5] so it remains to prove that

$$i!(2r-2i)!\frac{r!}{(r-i)!}(-4)^i \equiv -1 \mod p\,. \tag{12}$$

To see this, we begin with the expression on the left:

$$\begin{aligned}
i!(2r-2i)!\frac{r!}{(r-i)!}(-4)^i &= i!(2r-2i)!r(r-1)\cdots(r-i+1)2^i(-2)^i \\
&= i!(2r-2i)!2r(2r-2)\cdots(2r-2i+2)(-2)^i \\
&= \frac{i!(2r)!}{(2r-1)(2r-3)\cdots(2r-2i+1)}(-2)^i \\
&= \frac{i!(p-1)!}{(p-2)(p-4)\cdots(p-2i)}(-2)^i \\
&\equiv \frac{i!(-1)}{(-2)(-4)\cdots(-2i)}(-2)^i
\end{aligned}$$

(going mod p and again appealing to Wilson's Theorem)

$$\equiv \frac{i!(-1)}{(i!)(-2)^i}(-2)^i \equiv -1\,.$$

□

Proposition 4.16. *The Factorial Conjecture holds for $f \in \mathbb{C}[U_1, \ldots, U_n]$ of the form $c_1U_1^d + \cdots + c_nU_n^d$ where $d \geq 1$.*

[5] Wilson's Theorem: An integer $n > 1$ is prime if and only if $(n-1)! \equiv -1 \mod n$. See [5] for a very nice survey on this.

Proof. The case $d = 1$ is covered in Proposition 4.11, so we assume $d \geq 2$ and each of $c_1, \dots, c_n$ is non-zero. Here we only need to assume that $\mathcal{L}(f^m) = 0$ for $m \gg 0$. We consider the powers f^{nm} of f:

$$f^{nm} = \sum_{k_1+\cdots+k_n=nm} \frac{(nm)!}{k_1!\cdots k_n!} c_1^{k_1}\cdots c_n^{k_n} U_1^{k_1 d}\cdots U_n^{k_n d},$$

which yields

$$\begin{aligned} \mathcal{L}(f^{nm}) &= \sum_{k_1+\cdots+k_n=nm} \frac{(nm)!}{k_1!\cdots k_n!} c_1^{k_1}\cdots c_n^{k_n} (k_1 d)!\cdots(k_n d)! \\ &= (nm)! \sum_{k_1+\cdots+k_n=nm} \frac{(k_1 d)!}{k_1!}\cdots\frac{(k_n d)!}{k_n!} c_1^{k_1}\cdots c_n^{k_n} \end{aligned} \tag{13}$$

One term of (13), we'll call it the special term, occurs when $k_1 = \cdots = k_n = m$. For all other summands we have $k_i > m$ for some i (since $\sum k_i = nm$), and we now examine one of these other summands. Without loss of generality, suppose $k_1 > m$ and write

$$\begin{aligned} \frac{(k_1 d)!}{k_1!} = \frac{k_1 d}{k_1}(k_1 d - 1)\cdots(k_1 d - d + 1)\frac{(k_1 - 1)d}{k_1 - 1}(k_1 d - d - 1)\cdots \\ \cdots(2d+1)\frac{2d}{2}(2d-1)\cdots(d+1)\frac{1d}{d}(d-1)\cdots 1\,. \end{aligned}$$

From this one easily sees that $\frac{(k_1 d)!}{k_1!}$ is an integer divisible by $p = (m+1)d - 1$, which, by Dirichlet's prime number theorem, is prime for infinitely many values of m. As in previous arguments, we apply the algebraic reduction (Remark 4.5) and let $\mathcal{O}$ be the Dedekind ring chosen as in Remark 4.6. For all but finitely many such p, $\mathcal{O}$ has a valuation v_p lying over p. The above observation shows then shows that v_p is positive at all the terms of (13) except the special term, and since $\mathcal{L}(f^{nm}) = 0$ it must be positive at the special term as well. Since $p = (m+1)d - 1$ does not divide $\frac{(k_1 d)!}{k_1!}\cdots\frac{(k_n d)!}{k_n!}$ when $k_1 = \cdots = k_n = m$, we must have $v_p(c_1^m \cdots c_n^m) = 0$, and since this holds for infinitely many valuations of $\mathcal{O}$, we conclude $c_1^m \cdots c_n^m = 0$. Therefore $c_i = 0$ for some i, contradicting our assumption. □

References

1. Arno van den Essen, *The amazing Image Conjecture*, `http://arxiv.org/abs/1006.5801`, 2010.
2. A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993. MR 1215934 (94d:11078)
3. Olivier Mathieu, *Some conjectures about invariant theory and their applications*, Algèbre non commutative, groupes quantiques et invariants (Reims, 1995), Sémin. Congr., vol. 2, Soc. Math. France, Paris, 1997, pp. 263–279. MR MR1601155 (2000k:22014)
4. Hideyuki Matsumura, *Commutative algebra*, second ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980. MR MR575344 (82i:13003)
5. Wikipedia, *Wilson's theorem*, `http://en.wikipedia.org/wiki/Wilson's_theorem`.
6. Wenhua Zhao, *Hessian nilpotent polynomials and the Jacobian conjecture*, Trans. Amer. Math. Soc. **359** (2007), no. 1, 249–274 (electronic). MR MR2247890 (2007f:31015)

7. ———, *Generalizations of the image conjecture and the Mathieu conjecture*, J. Pure Appl. Algebra **214** (2010), no. 7, 1200–1216. MR MR2586998
8. ———, *Images of commuting differential operators of order one with constant leading coefficients*, Journal of Algebra **324** (2010), no. 2, 231 – 247.
9. ———, *Mathieu Subspaces of Associative Algebras*, http://arxiv.org/abs/1005.4260, May 2010.

Department of Mathematics, Radboud University, Nijmegen, The Netherlands *E-mail*: essen@math.ru.nl

Department of Mathematics, Washington University in St. Louis, St. Louis, MO 63130 *E-mail*: wright@math.wustl.edu

Department of Mathematics, Illinois State University, Normal, IL 61790 *E-mail*: wzhao@ilstu.edu