ISRAEL JOURNAL OF MATHEMATICS **219** (2017), 917–928
DOI: 10.1007/s11856-017-1502-2

THE GAUSSIAN MOMENTS CONJECTURE AND THE JACOBIAN CONJECTURE

BY

Harm Derksen*

Department of Mathematics, University of Michigan
530 Church Street, Ann Arbor, MI 48109-1043, USA
e-mail: hderksen@umich.edu

AND

Arno Van den Essen

Department of Mathematics, Radboud University
P. O. Box 9010, Postvak 59, 6500 GL Nijmegen, The Netherlands
e-mail: A.vandenEssen@math.ru.nl

AND

Wenhua Zhao**

Department of Mathematics, Illinois State University
300 S. School Street, Normal, IL 61761, USA
e-mail: wzhao@ilstu.edu

ABSTRACT

We first propose what we call the Gaussian Moments Conjecture. We then show that the Jacobian Conjecture follows from the Gaussian Moments Conjecture. Note that the the Gaussian Moments Conjecture is a special case of [11, Conjecture 3.2]. The latter conjecture was referred to as the Moment Vanishing Conjecture in [7, Conjecture A] and the Integral Conjecture in [6, Conjecture 3.1] (for the one-dimensional case). We also give a counter-example to show that [11, Conjecture 3.2] fails in general for polynomials in more than two variables.

* Partially supported by NSF grant DMS 1302032.
** Partially supported by the Simons Foundation Grant-278638.
Received July 21, 2015 and in revised form May 31, 2016

1. Introduction

For a random variable X we denote its expected value by $\mathbb{E}(X)$. Suppose that $X = (X_1, \ldots, X_n)$ is a random vector with a multi-variate normal distribution. We make the following conjecture:

Conjecture 1.1 (Gaussian Moments Conjecture **GMC**(n)): *Suppose that $P(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$ is a complex-valued polynomial such that the moments $\mathbb{E}(P(X)^m)$ are equal to 0 for all $m \geq 1$. Then for every polynomial $Q(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$ we have $\mathbb{E}(P(X)^m Q(X)) = 0$ for $m \gg 0$.*

By using translations and linear maps, we can normalize the random vector X such that $X_1, \ldots, X_n$ are independent, with mean 0 and variance 1.

The Gaussian Moments Conjecture is a special case of [11, Conjecture 3.2]. Furthermore, because of Proposition 3.3 and relation (3.2) in [11], the Gaussian Moments Conjecture is the special case of [11, Conjecture 3.1] for Hermite polynomials. Note that [11, Conjecture 3.2] was later referred to as the Moment Vanishing Conjecture in [7, Conjecture A], and the Integral Conjecture in [6, Conjecture 3.1] (for the one-dimensional case). Unfortunately, this conjecture is false in general, as can be seen from the following

Proposition 1.2: *Let $B = \{(x, y) \in \mathbb{R}^2 \,|\, y \geq 0,\, x^2 + y^2 \leq 1\}$, $P(x, y) = (x + iy)^2$ and $Q(x, y) = x + iy$. Then $\int_B P(x, y)^m \, dxdy = 0$ for all $m \geq 1$, but $\int_B Q(x, y)P(x, y)^m \, dxdy \neq 0$ for all $m \geq 1$.*

Proof. For each $m \geq 1$, by using the polar coordinates (r, θ) we have

$$\int_B P(x, y)^m \, dxdy = \int_0^1 \int_0^\pi r^{2m} e^{2mi\theta} r \, dr d\theta = 0;$$

$$\int_B Q(x, y)P(x, y)^m \, dxdy = \int_0^1 \int_0^\pi r^{2m+1} e^{(2m+1)i\theta} r \, dr d\theta = \frac{2i}{(2m + 3)(2m + 1)} \neq 0. \qquad \blacksquare$$

Remark 1.3: Note that Conjecture 3.2 in [11] is still open for univariate polynomials. It is also open for the (whole) disks or squares centered at the origin for polynomials in two variables.

Remark 1.4: The function $X_1^2 + X_2^2$ has an exponential distribution and, more generally, $X_1^2 + \cdots + X_{2k}^2$ has a χ^2 distribution. So, if the Gaussian Moments

Conjecture is true for all $n \geq 1$, then the conjecture is also true when we replace the Gaussian distributions by exponential or χ^2 distributions. The Moments Conjecture for exponential distributions is equivalent to [5, Conjecture 4.1], which is a weaker form of the Factorial Conjecture ([5, Conjecture 4.2]).

One of the main open conjectures in affine algebraic geometry is the notorious Jacobian Conjecture, which was first proposed by O. H. Keller [8] in 1939. See also [1] and [3].

Conjecture 1.5 (Jacobian Conjecture $\mathbf{JC}(n)$): *If $F : \mathbb{C}^n \to \mathbb{C}^n$ is a polynomial map that is locally invertible, then it is globally invertible.*

The main result of this paper is:

Theorem 1.6: *If $\mathbf{GMC}(n)$ is true for all $n \geq 1$, then $\mathbf{JC}(n)$ is true for all $n \geq 1$.*

Acknowledgment. The main results of the paper were obtained when the authors organized and attended the two-week International Short-School/Conference on Affine Algebraic Geometry and the Jacobian Conjecture, which was supported by and held at Chern Institute of Mathematics, Tianjin, China from July 14–25, 2014. The authors are very grateful to the institute for support and hospitality.

2. Background

Suppose that A is a unital commutative $\mathbb{C}$-algebra.

Definition 2.1: A **Mathieu–Zhao space** (or **MZ space**) is a $\mathbb{C}$-linear subspace $V \subseteq A$ with the property that $f^m \in V$ for all $m \geq 1$ implies that for every $g \in A$, $f^m g \in V$ for $m \gg 0$.

Observe that in this definition we have changed the name **Mathieu subspace**, which was introduced by the third author in [11, 12], to Mathieu–Zhao space or MZ space. This follows a suggestion of the second author in [4]. For some more general studies of this new notion, see [12].

With the definition above we can now reformulate our main conjecture as follows.

Conjecture 2.2 (**GMC**(n), reformulation): *The subspace*

$$\{P(x_1,\dots,x_n)\in\mathbb{C}[x_1,\dots,x_n]\mid \mathbb{E}(P(X_1,\dots,X_n))=0\}$$

is an MZ space of $\mathbb{C}[x_1,\dots,x_n]$.

Suppose that G is a complex reductive algebraic group acting regularly on an affine variety Z. Then G also acts on the ring $\mathbb{C}[Z]$ of polynomial functions on Z. Let $K\subseteq G$ be a maximal compact subgroup. Then K is Zariski dense in G. The Reynolds operator $\mathcal{R}_Z:\mathbb{C}[Z]\to\mathbb{C}[V]^K$ is the averaging operator:

$$\mathcal{R}_Z(f)=\int_{g\in K} g\cdot f\,d\mu,$$

where $d\mu$ is the Haar measure on K, normalized such that $\int_K d\mu=1$.

Conjecture 2.3 (Mathieu Conjecture **MC**(Z)): *The kernel* $\operatorname{Ker}(\mathcal{R}_Z)$ *of the Reynolds operator is an MZ space of* $\mathbb{C}[Z]$.

This conjecture is equivalent to the conjecture $C(\mathbb{C}[Z])$ of [9] (see [9, Corollary 1.3]). The group G acts on its own coordinate ring, and **MC**(G) implies **MC**(Z) ([9, Corollary 1.7]). The following theorem was proven in [9, Theorem 5.5]:

Theorem 2.4 (Mathieu): *If* **MC**$(\mathrm{SL}_n(\mathbb{C})/\mathrm{GL}_{n-1}(\mathbb{C}))$ *is true for all* $n\geq 1$, *then* **JC**(n) *is true for all* $n\geq 1$.

For later purposes, here we also point out that J. Duistermaat and W. van der Kallen [2] in 1998 had proved the Mathieu conjecture for the case of tori, which can be re-stated in terms of MZ spaces as follows.

Theorem 2.5 (Duistermaat and van der Kallen): *Let* $x=(x_1,x_2,\dots,x_n)$ *be* n *commutative free variables and* M *the subspace of the Laurent polynomial algebra* $\mathbb{C}[x_1^{-1},\dots,x_n^{-1},x_1,\dots,x_n]$ *consisting of the Laurent polynomials with no constant term. Then* M *is an MZ space of* $\mathbb{C}[x_1^{-1},\dots,x_n^{-1},x_1,\dots,x_n]$.

Let $\partial_i=\frac{\partial}{\partial z_i}$ be the partial derivative with respect to z_i. Define

$$\mathcal{E}_n:\mathbb{C}[w,z]=\mathbb{C}[w_1,\dots,w_n,z_1,\dots,z_n]\to\mathbb{C}[z]$$

such that

$$\mathcal{E}_n(P(w)Q(z))=P(\partial)Q(z)\in\mathbb{C}[z].$$

Zhao made the following conjecture in [10]:

CONJECTURE 2.6 (Special Image Conjecture $\mathbf{SIC}(n)$): *$\mathrm{Ker}(\mathcal{E}_n)$ is an MZ space of $\mathbb{C}[w,z]$.*

Zhao proved the following result ([10, Theorem 3.6, Theorem 3.7]):

THEOREM 2.7 (Zhao): *If $\mathbf{SIC}(n)$ is true for all $n \geq 1$, then $\mathbf{JC}(n)$ is true for all $n \geq 1$.*

3. Reduction of the Jacobian Conjecture to the Gaussian Moments Conjecture

We define the linear map

$$\mathcal{F}_n : \mathbb{C}[w,z] = \mathbb{C}[w_1,\ldots,w_n,z_1,\ldots,z_n] \to \mathbb{C}$$

by setting

$$\mathcal{F}_n(P) = \mathcal{E}_n(P)\mid_{z=0} .$$

For $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n$, set $z^\alpha = z_1^{\alpha_1}\cdots z_n^{\alpha_n}$ and $\alpha! = \alpha_1!\alpha_2!\cdots\alpha_n!$. Then we have

$$\mathcal{F}_n(w^\alpha z^\beta) = \begin{cases} \alpha! & \text{if } \alpha = \beta; \\ 0 & \text{if } \alpha \neq \beta. \end{cases}$$

PROPOSITION 3.1: *If $\mathrm{Ker}(\mathcal{F}_n)$ is an MZ space of $\mathbb{C}[w,z]$, then $\mathrm{Ker}(\mathcal{E}_n)$ is an MZ space of $\mathbb{C}[w,z]$, i.e., $\mathbf{SIC}(n)$ is true.*

Proof. Assume that $P^m \in \mathrm{Ker}(\mathcal{E}_n)$ for $m \geq 1$. Then for each $\alpha \in \mathbb{C}^n$ we have

$$\mathcal{E}_n(P^m(w,z))\mid_{z=\alpha} = \mathcal{E}_n(P^m(w,z+\alpha))\mid_{z=0} = \mathcal{F}_n(P^m(w,z+\alpha)) = 0.$$

Hence $P^m(w,z+\alpha) \in \mathrm{Ker}(\mathcal{F}_n)$ for all $m \geq 1$. Since $\mathrm{Ker}(\mathcal{F}_n)$ is an MZ space of $\mathbb{C}[w,z]$, for any $Q \in \mathbb{C}[w,z]$ and $\alpha \in \mathbb{C}^n$ we have $Q(w,z+\alpha)P(w,z+\alpha)^m \in \mathrm{Ker}(\mathcal{F}_n)$ for all $m \gg 0$. Therefore, for all $m \gg 0$ we have

$$\mathcal{E}_n(Q(w,z)P(w,z)^m)\mid_{z=\alpha} = \mathcal{F}_n(Q(w,z+\alpha)P(w,z+\alpha)^m) = 0.$$

Define $Z_N \subseteq \mathbb{C}^n$ to be the zero set of all $\mathcal{E}_n(Q(w,z)P(w,z)^m)$ with $m \geq N$. Clearly, Z_N is Zariski closed for all N, and $\bigcup_{N=1}^\infty Z_N = \mathbb{C}^n$. It follows that $Z_N = \mathbb{C}^n$ for some integer N, because a countable union of Zariski closed proper subsets cannot be the whole affine space. So for $m \geq N$, $\mathcal{E}_n(Q(w,z)P(w,z)^m)$ is the zero function. ∎

PROPOSITION 3.2: *If $\mathbf{GMC}(2n)$ is true, then $\mathrm{Ker}(\mathcal{F}_n)$ is an MZ space of $\mathbb{C}[w,z]$.*

Proof. Let $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ be $2n$ independent random variables with the normal distribution and with mean 0 and variance 1. Define complex-valued random variables W_j, Z_j and real-valued random variables R_j and T_j by

$$W_j = \frac{X_j - Y_j i}{\sqrt{2}} = R_j e^{-iT_j} \quad \text{and} \quad Z_j = \frac{X_j + Y_j i}{\sqrt{2}} = R_j e^{iT_j}.$$

Then $R_1, \ldots, R_n, T_1, \ldots, T_n$ are independent, and for every $1 \le j \le n$, R_j^2 has an exponential distribution with mean 1 and $\mathbb{E}(R_j^{2k}) = k!$. Now consider

$$\mathbb{E}(W^\alpha Z^\beta) = \mathbb{E}(R^{\alpha+\beta} e^{i\sum_j(\beta_j-\alpha_j)T_j}) = \prod_{j=1}^n (\mathbb{E}(R^{\alpha_j+\beta_j})\mathbb{E}(e^{i(\beta_j-\alpha_j)T_j})).$$

If $\beta \neq \alpha$, then $\beta_j \neq \alpha_j$ for some j, whence $\mathbb{E}(e^{i(\beta_j-\alpha_j)T_j}) = 0$ and $\mathbb{E}(W^\alpha Z^\beta) = 0$. If $\alpha = \beta$, then we have

$$\mathbb{E}(W^\alpha Z^\alpha) = \mathbb{E}(R^{2\alpha}) = \prod_j \mathbb{E}(R_j^{2\alpha_j}) = \prod_j \alpha_j! = \alpha!.$$

It follows that $\mathbb{E}(W^\alpha Z^\beta) = \mathcal{F}_n(w^\alpha z^\beta)$ for all $\alpha, \beta \in \mathbb{N}^n$. By linearity, we get $\mathbb{E}(Q(W,Z)) = \mathcal{F}_n(Q(w,z))$ for every polynomial $Q(w,z) \in \mathbb{C}[w,z]$. It follows readily from **GMC**$(2n)$ that $\operatorname{Ker} \mathcal{F}_n$ is an MZ space of $\mathbb{C}[w,z]$. ∎

Now we can prove our main result Theorem 1.6:

Proof of Theorem 1.6. It follows directly from Proposition 3.1, Proposition 3.2 and Theorem 2.7. ∎

4. Some special cases of the Gaussian Moments Conjecture

We view $\mathbb{C}[x_1, \ldots, x_n]$ as the coordinate ring of $V \cong \mathbb{C}^n$, where V is viewed as the standard representation of $\mathrm{O}(n)$.

PROPOSITION 4.1: *For homogeneous polynomials $P(x)$,* **GMC**(n) *follows from* **MC**(V).

Proof. Let $\Phi : \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}$ be given by $\Phi(P(x)) = \mathbb{E}(P(X))$. Any linear map $\mathbb{C}[x_1, \ldots, x_n]_d \to \mathbb{C}$ is determined by an element of $S^d(V)$. Since Φ is invariant under the action of $O(n)$ it is given by an element of $S^d(V)^{\mathrm{O}(n)}$. But $S^d(V)^{\mathrm{O}(n)}$ is at most one dimensional and is spanned by the restriction of the Reynolds operator $\mathcal{R}_V$. So up to a constant, $\Phi(P(x)^m)$ is equal to $\mathcal{R}_V(P(x)^m)$. If $\mathbb{E}(P(X)^m) = 0$ for $m \geq 1$, then $\mathcal{R}_V(P(X)^m) = 0$ for $m \geq 1$. If $Q(x)$ is homogeneous, then $\mathcal{R}_V(P(x)^m Q(x)) = 0$ for $m \gg 0$. So $\mathbb{E}(P(X)^m Q(X)) = 0$ for $m \gg 0$. If $Q(X)$ is non-homogeneous then $\mathbb{E}(P(X)^m Q(X)) = 0$ for $m \gg 0$, because $\mathbb{E}(P(X) Q_d(X)) = 0$ for $m \gg 0$ for every homogeneous summand $Q_d(x)$ of $Q(x)$. ∎

Proposition 4.2: *Suppose that X is a Gaussian Random Variable, and $P(x) \in \mathbb{C}[x]$ is a univariate polynomial such that $\mathbb{E}(P(X)^m) = 0$ for $m \geq 1$. Then $P(x) = 0$. In particular,* **GMC**(n) *is true for $n = 1$.*

Proof. As observed in the beginning of this paper, **GMC**(n) is a special case of the Image Conjecture for Hermite polynomials. For $n = 1$ the case of Hermite polynomials is proved in Corollary 4.3 of [6]. ∎

For a different proof of **GMC**(1), see Proposition 4.7 and Remark 4.8 of this section.

Proposition 4.3: *Let $P \in \mathbb{C}[x_1, \ldots, x_n, y_1, \ldots, y_n]$ be such that for each $1 \leq k \leq n$, $P(x, y)$ as a polynomial in x_k and y_k is homogeneous. Then* **GMC**$(2n)$ *holds for P.*

Proof. For each $1 \leq k \leq n$, let d_k be the degree of f as a polynomial in x_k and y_k.

Making the change of variables for x_i and y_i $(1 \leq i \leq n)$:

$$x_i = r_i \cos\theta_i \quad \text{and} \quad y_i = r_i \sin\theta_i,$$

we see that $P = (r_1^{d_1} r_2^{d_2} \cdots r_n^{d_n}) F$ for some polynomial F in $\cos\theta_i$ and $\sin\theta_i$ $(1 \leq i \leq n)$, which is independent of r_i $(1 \leq i \leq n)$.

Let $S^n := (S^1)^{\times n}$, where S^1 is the unit circle in $\mathbb{C}$. Denote by $d\mu_n$ the measure of $d\theta_1 d\theta_2 \cdots d\theta_n$, which is a Haar measure of the torus S_n. Then F can be viewed as an S^n-finite function over the torus S^n. Furthermore, for any $m \geq 1$ we have

$$\begin{aligned}\mathbb{E}(P^m(X,Y)) &= \int_{r_1=0}^{1} \cdots \int_{r_n=0}^{1} (r_1^{md_1+1} \cdots r_n^{md_n+1}) \left(\int_{S^n} F^m d\mu_n \right) dr_1 \cdots dr_n \\ &= A_m \int_{S^n} F^m d\mu_n,\end{aligned} \tag{4.1}$$

for some nonzero constant A_m.

Hence, if $\mathbb{E}(P^m) = 0$ when $m \gg 0$, then so is $\int_{S^n} F^m d\mu$. Since $d\mu_n$ is a Haar measure of the torus S^n, applying the Duistermaat–van der Kallen Theorem

2.5 to F we see that for each polynomial G in $\cos\theta_i$ and $\sin\theta_i$ $(1 \le i \le n)$, we have $\int_{S^n} F^m G\, d\mu_n = 0$ when $m \gg 0$.

Now for each monomial $M(x, y)$ in x_i and y_i $(1 \le i \le n)$, by Eq. (4.1) with P^m replaced by $P^m M$, we see that $\mathbb{E}(P^m M) = 0$ when $m \gg 0$. Hence for each polynomial $Q(x, y)$, we also have $\mathbb{E}(P^m Q) = 0$ when $m \gg 0$. Therefore **GMC**$(2n)$ holds for P. ∎

Since every homogeneous polynomial in two variables satisfies the condition of Proposition 4.3, we immediately have the following:

Corollary 4.4: **GMC**(2) *holds for all homogeneous polynomials* P.

By a similar argument as in the proof of Proposition 4.3, we have also the following case of Conjecture 3.2 in [11]:

Corollary 4.5: *Let B be the unit disk in $\mathbb{R}^2$ centered at the origin with the Lebesgue measure $dxdy$. Let $P \in \mathbb{C}[x, y]$ be such that P is homogeneous and $\int_B P^m\, dxdy = 0$ for all $m \gg 0$. Then for every $Q \in \mathbb{C}[x, y]$ we have $\int_B P^m Q\, dxdy = 0$ for all $m \gg 0$.*

In the rest of this section we point out that some results proved in [5] for the Factorial Conjecture ([5, Conjecture 4.2]) can also be proved similarly for **GMC**(n).

First, we give a proof for the following case of **GMC**(n), which is parallel to [5, Proposition 4.8].

Proposition 4.6: *Let $F(x) \in \mathbb{C}[x_1, x_2, \ldots, x_n]$ be such that $F(0) \ne 0$. Then $\mathbb{E}(F^m(X)) \ne 0$ for infinitely many $m \ge 1$.*

Proof. Let $\Phi : \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}$ be given by $\Phi(P(x)) = \mathbb{E}(P(X))$. Set $(-1)!! := 1$ and $(2k-1)!! := (2k-1)(2k-3)\cdots 3 \cdot 1$ for all $k \ge 1$. Furthermore, for each $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in 2\mathbb{N}^n$, we set $(\alpha - 1)!! := \prod_{i=1}^n (\alpha_i - 1)!!$. Then for each $\alpha \in \mathbb{N}^n$, we have

$$\Phi(x^\alpha) = \begin{cases} (\alpha-1)!! & \text{if } \alpha \in 2\mathbb{N}^n; \\ 0 & \text{otherwise.} \end{cases} \tag{4.2}$$

Now assume that the proposition fails, i.e., there exists $N \ge 1$ such that $\Phi(F^m) = 0$ for all $m \ge N$. Since $F(0) \ne 0$, replacing F by $F/F(0)$ we may assume $F(0) = 1$. Write $F(x) = 1 - \sum_{i=1}^{k} c_i x^{\beta_i}$ with $c_i \in \mathbb{C}$ and $0 \neq \beta_i \in \mathbb{N}^n$ for all $1 \leq i \leq k$.

Note that if $c_i = 0$ for some $1 \leq i \leq k$, i.e., $F(x) = 1$, the proposition obviously holds. So we assume $c_i \neq 0$ for all $1 \leq i \leq k$. Replacing F by F^2 we may also assume that $0 \neq \beta_i \in 2\mathbb{N}$ for at least one $1 \leq i \leq k$.

Furthermore, by a reduction due to Mitya Boyarchenko (see the proof of [7, Theorem 4.1] or [5, Remarks 4.5 and 4.6]), we may also assume that $c_i \in \bar{\mathbb{Q}}$ for all $1 \leq i \leq k$.

Let $B = \mathbb{Z}[c_1, c_2, \ldots, c_k]$ and p be an odd prime such that $p \geq N$ and $\nu_p(c_i) = 0$ for all $1 \leq i \leq k$, where ν_p denotes an extension of the p-valuation of $\mathbb{Z}$ to B.

Since $p \geq N$ and $F^p \equiv 1 - \sum_{i=1}^{k} c_i^p x^{p\beta_i} \pmod{pB}$, we have $\Phi(F^p) = 0$ and

$$1 \equiv \sum_{\substack{1 \leq i \leq k \\ 0 \neq \beta_i \in 2\mathbb{N}^n}} c_i^p (p\beta_i - 1)!! \pmod{pB}. \tag{4.3}$$

Since each $0 \neq \beta_i \in 2\mathbb{N}^n$ in the sum above has at least one nonzero (and even) component, so $(p\beta_i - 1)!!$ is divisible by p. Then applying ν_p to Eq. (4.3) we get $\nu_p(1) \geq 1$, which is a contradiction. ∎

The next proposition is parallel to [5, Proposition 4.10].

Proposition 4.7: *Let $F(x) = c_0 M_0 + \sum_{i=1}^{d} c_i M_i$ with $M_0 = x_1^{k_1} \cdots x_n^{k_n}$ such that $k_1 \geq 1$ and $k_1 \geq k_j$ for all $2 \leq j \leq n$; $c_i \in \mathbb{C}$ $(0 \leq i \leq d)$ with $c_0 \neq 0$; and M_i $(1 \leq i \leq d)$ are monomials in x that are divisible by $x_1^{k_1+1}$. Then $\mathbb{E}(F^m(X)) \neq 0$ for infinitely many $m \geq 1$.*

Proof. Replacing F by $c_0^{-1}F$ we may assume $c_0 = 1$ and replacing F by F^2 we may assume that k_1 is an even positive integer. Then under these assumptions the proof of [5, Proposition 4.10] works through similarly for the linear functional Φ of $\mathbb{C}[x_1, \ldots, x_n]$ given in Eq. (4.2). ∎

Remark 4.8: Note that when $n = 1$ the conditions of Proposition 4.7 hold automatically for all nonzero univariate polynomials $F(x)$. Hence **GMC**(1) also follows directly from Proposition 4.7.

Proposition 4.9: *Let $d \geq 1$ and $P(x) = \sum_{i=1}^{n} c_i x_i^d \in \mathbb{C}[x_1, \ldots, x_n]$ for some $c_i \in \mathbb{C}$ $(1 \leq i \leq n)$. Assume that $\mathbb{E}(P^m(X)) = 0$ for all $m \gg 0$. Then $P = 0$. In particular,* **GMC**(n) *holds for $P(x)$.*

This proposition can be proved similarly as Proposition 4.16 in [5] if we choose the integer m there to be even, and the prime p to be $(m+2)d-1$ or $(m+1)d-1$, depending on whether d is odd or even, respectively. Note that the components k_i in the proof of Proposition 4.16 in [5] for our case must be even when m is chosen to be even.

5. Moment vanishing polynomials

Let again $X = (X_1, \dots, X_n)$ be a random vector with joint Gaussian distribution. For $n \geq 2$, there exist many polynomials $P(x) \in \mathbb{C}[x]$ for which $\mathbb{E}(P(X)^m) = 0$ for all $m \geq 1$.

Proposition 5.1: *Suppose that* 0 *lies in the closure of the* $\mathrm{O}_n(\mathbb{C})$ *orbit of* $P(x)$. *Then*

(a) $\mathbb{E}(P(X)^m) = 0$ *for all* $m \geq 1$;
(b) *for any polynomial* $Q(x)$, $\mathbb{E}(P(X)^m Q(X))$ *for* $m \gg 0$.

Proof.
(a) Assume that there exists a sequence of orthogonal matrices $A_1, A_2, \dots$ such that $\lim_{k\to\infty} P(A_k(x)) = 0$. Then we also have $\lim_{k\to\infty} P(A_k(x))^m = 0$, and $\mathbb{E}(P(X)^m) = \lim_{k\to\infty} \mathbb{E}(P(A_k(X))^m) = \mathbb{E}(\lim_{k\to\infty} P(A_k(X))^m) = 0$.

(b) A 1-parameter subgroup is a homomorphism $\lambda : \mathbb{C}^\star \to \mathrm{O}_n(\mathbb{C})$ of algebraic groups. We can view λ as an orthogonal matrix with entries in $\mathbb{C}[t, t^{-1}]$. If $P(\lambda(t)(x))$ lies in $t\mathbb{C}[t, x] = t\mathbb{C}[t, x_1, \dots, x_n]$, then $\lim_{t\to 0} P(\lambda(t)x) = 0$ and 0 lies in the closure of the $\mathrm{O}_n(\mathbb{C})$ orbit of $P(x)$. Conversely, the Hilbert–Mumford criterion state, that if 0 lies in the $\mathrm{O}_n(\mathbb{C})$-orbit closure of $P(x)$, then there exists such a 1-parameter subgroup $\lambda : \mathbb{C}^\star \to \mathrm{O}_n(\mathbb{C})$ such that $P(\lambda(t)(x)) \in t\mathbb{C}[t, x]$. If $Q(x) \in \mathbb{C}[x]$, then for large m, $Q(\lambda(t)x))P(\lambda(t)x)^m \in t\mathbb{C}[t, x]$ and

$$\mathbb{E}(Q(X)P(X)^m) = \mathbb{E}(\lim_{t\to 0} Q(\lambda(t)X)P(\lambda(t)X)^m) = \mathbb{E}(0) = 0. \qquad \blacksquare$$

Example 5.2: Consider the 1-parameter subgroup $\lambda : \mathbb{C}^\star \to \mathrm{O}_2(\mathbb{C})$ defined by

$$\lambda(t) = \begin{pmatrix} \frac{t+t^{-1}}{2} & \frac{t^{-1}-t}{2i} \\ \frac{t-t^{-1}}{2i} & \frac{t+t^{-1}}{2} \end{pmatrix}.$$

If $P(x_1, x_2) = x_1 + ix_2$, then we have $P(\lambda(t)x) = tP(x)$ and $\lim_{t\to 0} P(\lambda(t)x) = 0$. So 0 lies in the $\mathrm{O}_2(\mathbb{C})$-orbit closure of $P(x_1, x_2)$. By the proposition above, $P(x_1, x_2)$ satisfies the moment vanishing condition. Now, let $Q(x_1, x_2)$ be a polynomial of degree $< d$ and $m \geq d$. Set $R(x_1, x_2) := (x_1 + ix_2)^m Q(x_1, x_2)$. Then $Q(\lambda(t)x)$ has pole order at most $d - 1$, so

$$R(\lambda(t)x) = t^m (x_1 + ix_2)^m Q(\lambda(t)x) \in t\mathbb{C}[t, x_1, x_2],$$

and

$$\lim_{t \to \infty} R(\lambda(t)x) = 0.$$

Hence $\mathbb{E}\big((X_1 + iX_2)^m Q(X)\big) = 0$ for all $m \geq d$.

A similar argument shows that if $2k \leq n$ and $P(x_1, \dots, x_k)$ is a polynomial with constant coefficient 0, then $P(x_1 + ix_2, x_3 + ix_4, \dots, x_{2k-1} + ix_{2k})$ has the vanishing condition.

By Proposition 5.1(b), the Jacobian Conjecture follows from the following (possibly stronger) conjecture:

Conjecture 5.3 (Gaussian Moments Orbit Conjecture): *If* $\mathbb{E}(P(X)^m) = 0$ *for all* $m \geq 1$*, then the* $\mathrm{O}_n(\mathbb{C})$*-orbit closure of* $P(x)$ *contains 0.*

References

[1] H. Bass, E. H. Connell and D. Wright, *The Jacobian conjecture, reduction of degree and formal expansion of the inverse*, Bulletin of the American Mathematical Society **7** (1982), 287–330.

[2] J. J. Duistermaat and W. van der Kallen, *Constant terms in powers of a Laurent polynomial*, Indagationes Mathematicae **9** (1998), 221–231. [MR1691479].

[3] A. van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture*, Progress in Mathematics, Vol. 190, Birkhäuser Verlag, Basel, 2000.

[4] A. van den Essen, *Introduction to Mathieu Subspaces*, Lectures given at the International Conference/Short-School on Affine Algebraic Geometry, held at the Chern Institute of Mathematics, Tianjin, China, 14–25 July, 2014.

[5] A. van den Essen, D. Wright and W. Zhao, *On the Image Conjecture*, Journal of Algebra **340** (2011), 211–224.

[6] A. van den Essen and W. Zhao, *Mathieu subspaces of univariate polynomial algebras*, Journal of Pure and Applied Algebra **217** (2013), 1316–1324.

[7] J.-P. Françoise, F. Pakovich, Y. Yomdin and W. Zhao, *Moment Vanishing Problem and positivity; some examples*, Bulletin des Sciences Mathématiques **135** (2011), 10–32.

[8] O. H. Keller, *Ganze Gremona-Transformationen*, Monatshefte für Mathematik und Physik **47** (1939), 299–306.

[9] O. Mathieu, *Some conjectures about Invariant Theory and their applications*, in *Algèbre non commutative, groupes qunatiques et invariants (Reims, 1995)*, Séminaires et Congrès, Vol. 2, Société Mathématique de France, Paris, 1997, pp. 263–279.

[10] W. Zhao, *Images of commuting differential operators of order one with constant leading coefficients*, Journal of Algebra **324** (2010), 231–247.

[11] W. Zhao, *Generalizations of the Image Conjecture and the Mathieu Conjecture*, Journal of Pure and Applied Algebra **214** (2010), 1200–1216.

[12] W. Zhao, *Mathieu subspaces of associative algebras*, Journal of Algebra **350** (2012), 245–272.