DENSITY OF REAL AND COMPLEX DECOMPOSABLE UNIVARIATE POLYNOMIALS

JOACHIM VON ZUR GATHEN[1], GUILLERMO MATERA[2,3]

Abstract. We estimate the density of tubes around the algebraic variety of decomposable univariate polynomials over the real and the complex numbers.

1. Introduction

For two univariate polynomials $g, h \in F[x]$ of degrees d, e, respectively, over a field F, their *composition*

$$f = g(h) = g \circ h \in F[x] \tag{1.1}$$

is a polynomial of degree $n = de$. If such g and h exist with degree at least 2, then f is called *decomposable* (or *composed, composite*, a *composition*).

Since the foundational work of Ritt, Fatou, and Julia in the 1920s on compositions over $\mathbb{C}$, a substantial body of work has been concerned with structural properties (e.g., [8], [7], [21, 22], [27]), with algorithmic questions (e.g., [1], [20], [3]), and with enumeration over finite fields, exact and approximate (e.g., [16], [15], [4], [11], [28]).

This paper presents analogs for the case of the real or complex numbers of the latter counting results. What does counting mean here? The dimensions and degrees of its irreducible components as algebraic varieties? These quantities turn up in our argument, but we bound here the *density* of these components. Any proper algebraic subvariety X of $\mathbb{R}^n$ has volume and density 0. However, we can bump up the dimension of X to n by taking an ϵ-tube U_ϵ around X, replacing each point in X by a hypercube $(-\epsilon, \epsilon)^{\operatorname{codim} X}$ for "small" positive ϵ. If this is done properly, U_ϵ has dimension n. Its volume may be infinite, and we make it finite by intersecting with a hypercube $(-B, B)^n$ for some "large" positive B. Then the *density* of X in $(-B, B)^n$ is this finite volume divided by the volume $(2B)^n$ of the large hypercube. A similar approach works in the complex case.

Date: August 20, 2016.

Key words and phrases. Polynomial composition, real polynomials, complex polynomials, volume, tubes.

JvzG acknowledges the support of the B-IT Foundation and the Land Nordrhein-Westfalen. GM is partially supported by the grants UNGS 30/3084 and PIP 11220090100421 CONICET.

Let X be an equidimensional real or complex algebraic variety embedded in a k-dimensional affine space with codimension m, and consider the ϵ-neighborhood $\{y\colon |x-y| < \epsilon\}$ of some point x in the space. This is a real hypercube or a complex polycylinder, respectively. We also use the corresponding notion for a projective space. There are several notions for forming an ϵ-tube around X, namely, as the union of all

- k-dimensional ϵ-neighborhoods of $x \in X$,
- m-dimensional ϵ-neighborhoods in the direction normal to $x \in X$,
- m-dimensional ϵ-neighborhoods in a fixed direction around $x \in X$.

Singular points may be disregarded. The first two tubes comprise the points in the affine space whose distance to X in a normal direction is less than ϵ. Thus the two notions coincide, at least for smooth varieties. The ratio to the volume in the third notion is locally $\cos\alpha$, where α is the angle between the two m-dimensional linear spaces, namely the normal space (at a nonsingular point) and the space in the chosen fixed direction.

The present paper uses exclusively the third notion, the others are included here only for perspective.

Weyl [26], answering a question posed by Hotelling [19], proved fundamental results on tubes around manifolds. Since then, the topic has been studied in topology and differential geometry and is the subject of the textbook of Gray [17], which includes many further references. The first notion and generalizations of it are commonly used.

For algebraic varieties and the first notion, Demmel [6] and Beltrán & Pardo [2] show upper bounds of the form $c \cdot \deg X \cdot (\epsilon/B)^{2m}$ on the density of complex ϵ-tubes inside the B-neighborhood of 0, where c does not depend on ϵ or $B > \epsilon$. In the real case, $2m$ is replaced by m. Often it is sufficient to consider $B = 1$. Lower bounds, with various values for c, are also available. [24] uses the third notion and shows in his Theorem 4A an upper bound of $k(\epsilon/B)^2$ for the hypersurface of monic squareful univariate polynomials of degree k in $\mathbb{C}^k$. These papers investigate the condition number which is large for inputs at which (iterative) numerical methods behave badly, such as the matrices close to singular ones for matrix inversion or the (univariate) polynomials close to squareful ones for Newton's root finding method. These hypersurfaces are also the topic of [23].

Yet another notion is the $2d$-dimensional volume of a d-dimensional variety in a complex affine space. Demmel [6], Section 7, provides bounds on this volume.

We study the density of tubes around the (affine closed, usually reducible) variety of decomposable univariate polynomials. An isomorphism with an affine space (Theorem 2.2) suggests a preferred (constant) direction in which to attach ϵ-neighborhoods, thus following the third one of the recipes sketched above.

Cheung, Ng & Tsang [5] also consider decomposable polynomials. They bound the density of a hypersurface containing them, using the third notion. This provides, by necessity, a weaker bound than ours.

This paper is organized as follows. Section 2 presents a decomposition algorithm which is central for our approach, and results on the dimensions and degrees of various varieties of decomposable polynomials. Section 3 discusses bounds on the growth of coefficients in the decomposition algorithm mentioned above. These bounds are asymptotically optimal in a certain sense. Section 4 defines our tubes over $\mathbb{R}$ and presents upper and lower bounds for the resulting density (Theorem 4.6). Section 5 considers the analogous problem over $\mathbb{C}$. Section 6 takes up the above discussion of other notions of tubes and of related work, with some more detail.

2. The Newton-Taylor decomposition algorithm

It is well known that we may assume all three polynomials in (1.1) to be monic (leading coefficient 1) and original (constant coefficient 0, so that the graph contains the origin). All other compositions can be obtained from this special case by composing (on the left and on the right) with linear polynomials (polynomials of degree 1); see, e.g., von zur Gathen [12].

Thus we consider for a proper divisor d of n and $e = n/d$

$$\begin{aligned} P_n(F) &= \{f \in F[x] \colon \deg f = n, f \text{ monic original}\}, \\ \gamma_{n,d} &\colon P_d(F) \times P_e(F) \to P_n(F) \text{ with } \gamma_{n,d}(g,h) = g \circ h, \\ C_{n,d}(F) &= \{f \in P_n(F) \colon \exists g,h \in P_d(F) \times P_e(F) \;\; f = g \circ h\} \\ &= \operatorname{im} \gamma_{n,d}, \\ C_n(F) &= \bigcup_{\substack{d \mid n \\ d \notin \{1,n\}}} C_{n,d}(F). \end{aligned} \tag{2.1}$$

$P_n(F)$ is an $(n-1)$-dimensional vector space over F and $C_n(F)$ is the algebraic variety of decomposable polynomials. We drop the argument F when it is clear from the context. When n is prime, then $C_n(F)$ is empty, and in the following we always assume n to be composite.

We recall the decomposition algorithm from von zur Gathen [10]. It computes $\gamma_{n,d}^{-1}(f)$ for $f \in C_{n,d}$ by taking the reverse $\tilde{f} = x^n \cdot f(x^{-1})$ of f and computing its dth root $\tilde{h}$ modulo x^e, via Newton iteration with initial value 1. Thus $\tilde{h}^d \equiv \tilde{f} \bmod x^e$, $\deg \tilde{h} < e$, and $\tilde{h}(0) = 1$. Then the reverse $h = x^e \cdot \tilde{h}(x^{-1})$ of $\tilde{h}$ is monic original of degree e

and is the unique candidate for the right component. The Newton iteration is well-defined unless $\mathrm{char}(F)$ divides d. Like any polynomial of degree at most $n = de$, f has a (unique) generalized Taylor expansion $f = \sum_{0\le j\le d} G_j h^j$ around h, with all $G_j \in F[x]$ of degree less than e. Then $f \in C_{n,d}$ if and only if all G_j are constants, and if so, indeed $f = g \circ h$ with $g = \sum_{0\le j\le d} G_j x^j$. We call this the Newton-Taylor (NT) method for decomposing. This computation expresses each coefficient of g and h as a polynomial in the coefficients of f, as illustrated in Example 2.1. It can be executed with $O(n \log^2 n \,\mathrm{loglog}\, n)$ operations in F. For more details on the computer algebra machinery, see Section 3, the cited article, and von zur Gathen & Gerhard [14], Sections 9.2 and 9.4.

When f is known to be in $C_{n,d}$ and h has been calculated from its e highest coefficients, then only the coefficients of f at powers x^i with d dividing i are needed to compute g. We let $N = \{1, 2, \ldots, n-1\}$ be the support of a general $f \in P_n$. The NT method only uses the coefficients f_i of f at x^i for those $i \in N$ which are in the *Newton-Taylor set*

$$\mathrm{NT}_d = \{n-1, \ldots, n-e+1\} \cup \{i \in N : e \mid i\}.$$

We also take the complement $\mathrm{cNT}_d = N \setminus \mathrm{NT}_d$. Then

$$\begin{aligned} \#\mathrm{NT}_d &= n/d - 1 + d - 1 = d + n/d - 2, \\ m_d = \#\mathrm{cNT}_d &= n - d - n/d + 1. \end{aligned} \tag{2.2}$$

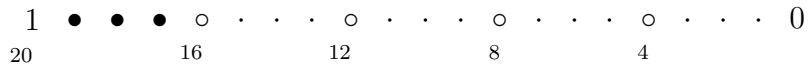

FIGURE 1. The Newton-Taylor set for $n = 20$ and $d = 5$.

Example 2.1. For $n = 20$, $d = 5$, and $e = 4$, we have $NT_5 = \{19, 18, 17, 16, 12, 8, 4\}$ and $\#NT_5 = d + n/d - 2 = 7$. The leading and trailing coefficients of any $f \in P_{20}$ are fixed as 1 and 0, respectively. The bullets and open circles in Figure 1 are positions of coefficients used in the Newton and Taylor algorithms, respectively. Using the binomial expansion (also known to Newton) instead of the Newton iteration and $u = f_{19}x + f_{18}x^2 + f_{17}x^3$, we find

$$\begin{aligned} \tilde{h} &= 1 + h_3 x + h_2 x^2 + h_1 x^3 \equiv (1+u)^{1/5} \\ &= \sum_{\ell \ge 0} \binom{1/5}{\ell} u^\ell \equiv 1 + \frac{1}{5}u - \frac{2}{25}u^2 + \frac{6}{125}u^3 \bmod x^4, \\ h &= x^4 + h_3 x^3 + h_2 x^2 + h_1 x \\ &= x^4 + \frac{f_{19}}{5} \cdot x^3 + \frac{-2f_{19}^2 + 5f_{18}}{25} \cdot x^2 + \frac{6f_{19}^3 - 20 f_{18} f_{19} + 25 f_{17}}{125} \cdot x. \end{aligned}$$

Now

$$g_4 = f_{16} - \frac{1}{125}\,(21f_{19}^4 - 90f_{18}f_{19}^2 + 50f_{18}^2 + 100f_{17}f_{19})$$

is the coefficient of x^{16} in $f - h^5$. Similarly, g_j for $j = 3, 2, 1$ is determined as the coefficient of x^{4j} in $f - \sum_{j<k\le 5} g_k h^k$. These four coefficients of g have degrees 4, 8, 12, and 16, respectively, in the NT_5-coefficients of f.

To complete the picture, one can express the twelve cNT_5-coefficients of $f \in C_{20,5}$ as polynomials in the seven NT-coefficients. The polynomials have the following degrees at x^{15}, x^{14}, x^{13}, $x^{11}, \ldots$: $5, 5, 7, 9, 10, 11, 13, 14, 15, 17, 18, 19$. The Bézout number, that is, the product of these degrees, is much larger than the bound in Theorem 2.2 below.

Using these facts, we give a geometric description of $C_{n,d}$.

Theorem 2.2. *Let d be a proper divisor of n and assume that $\mathrm{char}(F)$ does not divide d. Then $C_{n,d}(F) = \mathrm{im}\,\gamma_{n,d}$ is a closed irreducible algebraic subvariety of $P_n(F)$ of dimension $d + n/d - 2$ and codimension m_d. The Newton-Taylor method provides a polynomial section $\nu_{n,d}\colon C_{n,d} \to P_d(F) \times P_{n/d}(F)$ of $\gamma_{n,d}$. Furthermore, $\gamma_{n,d}$ and $\nu_{n,d}$ are defined over $\mathbb{Z}$ and $\mathbb{Z}[d^{-1}]$, respectively. For $f = \sum_{1\le i\le n} f_i x^i \in C_{n,d}$, $\nu_{n,d}(f)$ depends only on the coefficients f_i with $i \in NT_d$. The degree of $C_{n,d}$ is at most $d^{d+n/d-2}$.*

Proof. Let $e = n/d$. To show that $C_{n,d}$ is closed and irreducible, we embed $P_n(F) = \{(f_{n-1}, \ldots, f_1) \in \mathbb{A}^{n-1}(F)\}$ in $\mathbb{P}^{n-1}(F)$ via

$$(f_{n-1}, \ldots, f_1) \mapsto \bar f = (1 : f_{n-1} : \ldots : f_1).$$

The projective version $\bar\gamma_{n,d}$ of $\gamma_{n,d}$ is then

$$\begin{aligned}\bar\gamma_{n,d}((g_d : g_{d-1} : \ldots : g_1), (h_e : h_{e-1} : \ \ldots : h_1))\\ = \sum_{1\le j\le d} g_j h_e^{d-j} \bar h^j \in \mathbb{P}^{n-1}(F),\end{aligned}$$

where $\bar h = \sum_{1\le \ell\le e} h_\ell x^\ell$ and, with a slight abuse of notation, $\bar h^j$ stands for the (projective) vector of n coefficients of the polynomial $\bar h^j$. This vector is homogeneous in the variables h_ℓ of degree j.

The scalar extension of $\bar\gamma_{n,d}$ to $\mathbb{P}^{d-1}(\overline{F}) \times \mathbb{P}^{e-1}(\overline{F}) \to \mathbb{P}^{n-1}(\overline{F})$ is well–defined, where $\overline{F}$ is an algebraic closure of F. As this extension is a closed mapping which is defined over F, we conclude that $\bar\gamma_{n,d}$ is also a closed mapping. In particular, $\bar C_{n,d} = \mathrm{im}\ \bar\gamma_{n,d}$ is closed in $\mathbb{P}^{n-1}(F)$.

We now show that $\bar C_{n,d}(F) \cap \mathbb{A}^{n-1}(F) = C_{n,d}(F)$. The inclusion $C_{n,d}(F) \subseteq \bar C_{n,d}(F) \cap \mathbb{A}^{n-1}(F)$ is clear. For the other inclusion, we take some $f \in \bar C_{n,d}(F) \cap \mathbb{A}^{n-1}(F)$ and $\bar g \in \mathbb{P}^{d-1}(F)$ and $\bar h \in \mathbb{P}^{e-1}(F)$ with $\bar f = \bar g \circ \bar h$. Since $f \in \mathbb{A}^{n-1}(F) = P_n(F)$, the leading coefficient of $\bar f$ (at x^n) is nonzero. We normalize $\bar f$ so that this coefficient equals 1. The

coefficient of $\bar{g} \circ \bar{h} = \sum_{1 \le j \le d} g_j h_e^{d-j} \bar{h}^j$ at x^n equals $g_d \cdot \mathrm{lc}(\bar{h}^d) = g_d \cdot h_e^d$. It follows that $g_d h_e \neq 0$. After normalizing $\bar{g}$ and $\bar{h}$ by dividing by their leading coefficients, we obtain polynomials $g \in P_d(F)$ and $h \in P_e(F)$ with $f = g \circ h$. This shows the desired inclusion and the claim that $C_{n,d}$ is closed in P_n. Furthermore, as $P_d(F) \times P_e(F)$ is irreducible, it follows that $C_{n,d} = \mathrm{im}\ \gamma_{n,d}$ is also irreducible.

We prove the degree estimate. The existence of the section $\nu_{n,d}$ implies that $\dim C_{n,d} = d + e - 2$. Let $H_1, \ldots, H_{d+e-2}$ be hyperplanes of $P_n(F)$ with $\#(C_{n,d} \cap H_1 \cap \cdots \cap H_{d+e-2}) = \deg C_{n,d}$. Let $\mathcal{S} = C_{n,d} \cap H_1 \cap \cdots \cap H_{d+e-2}$. Then $\#S = \deg C_{n,d}$ and

$$\gamma_{n,d}^{-1}(\mathcal{S}) = \gamma_{n,d}^{-1}(H_1) \cap \cdots \cap \gamma_{n,d}^{-1}(H_{d+e-2}).$$

The polynomial map $\gamma_{n,d}$ consists of $n-1$ integer polynomials in the coefficients of g and h, all of total degree at most d. Furthermore, for each $i \le d+e-2$ there exists a linear combination w_i of the polynomials which define the coordinates of $\gamma_{n,d}$ so that $\gamma_{n,d}^{-1}(H_i) = \{w_i = 0\}$. Therefore, $\deg \gamma_{n,d}^{-1}(H_i) \le d$ and, by the Bézout inequality (see, e.g., Heintz [18], Fulton [9], Vogel [25]), it follows that $\deg \gamma_{n,d}^{-1}(\mathcal{S}) \le d^{d+e-2}$. Let $\gamma_{n,d}^{-1}(\mathcal{S}) = \bigcup_{1 \le j \le k} X_j$ be the decomposition of $\gamma_{n,d}^{-1}(\mathcal{S})$ into irreducible components. Since $\gamma_{n,d}(\gamma_{n,d}^{-1}(\mathcal{S})) = \mathcal{S}$ and each irreducible component X_j of $\gamma_{n,d}^{-1}(\mathcal{S})$ is mapped by $\gamma_{n,d}$ to a point of $\mathcal{S}$, we deduce that

$$\deg C_{n,d} = \#\mathcal{S} \le k \le \sum_{1 \le j \le k} \deg X_j = \deg \gamma_{n,d}^{-1}(\mathcal{S}) \le d^{d+e-2}.$$

The Newton and Taylor algorithms are integral algorithms, except that divisions by d occur in Newton iteration. □

This precise description of $C_{n,d}$, with the section $\nu_{n,d}$, is the basis for our bounds on the real and complex densities that we consider.

The convex function $d + n/d$ of d assumes its maximum among the proper divisors of n at $d = \ell$ and $d = n/\ell$, where ℓ is the least prime number dividing n; see von zur Gathen [12]. Thus the two "large" components of C_n are $C_{n,\ell}$ and $C_{n,n/\ell}$, unless $n = \ell^2$, when they coincide. We will deal with the other components of smaller dimension at the end of Section 4.

We also want to show that the sum of the two "large" densities bounds the density of C_n from below. To this end, it suffices to prove that the intersection of the two components has small dimension. Since both are irreducible, it suffices to show that they are distinct. This follows easily from Ritt's Second Theorem. In fact, the following geometric variant of the normal form for Ritt's Theorem in von zur Gathen [13] provides precise bounds.

Theorem 2.3. *Let n, d, and $e = n/d$ be as above, with $e > d \ge 2$ in addition, $i = \gcd(d, e)$, $s = \lfloor e/d \rfloor$ and F a field of characteristic either*

0 or coprime to n. Then $X = C_{n,d}(F) \cap C_{n,e}(F)$ is a closed algebraic subvariety of $P_n(F)$.

When $d \geq 3i$, then X has exactly two irreducible components, one of dimension $2i + s - 1$ and another one of dimension $2i$, and the intersection of the two is irreducible of dimension $2i-1$. When $d \leq 2i$, then X is irreducible. It has dimension $d + e/d - 3/2$ if $d = 2i$, and dimension $2d + e/d - 3$ if $d = i$.

In all cases, $\dim X < \dim C_{n,d}(F) = \dim C_{n,e}(F)$.

Proof. We first assume that $d \geq 2i$. Theorem 6.3 from von zur Gathen [13] provides, expressed in geometric language, two polynomial functions

$$\alpha_{\exp}\colon P_i \times F^s \times F \times P_i \to P_n,$$
$$\alpha_{\mathrm{trig}}\colon P_i \times F \times F \times P_i \to P_n,$$

so that $X = \operatorname{im} \alpha_{\exp} \cup \operatorname{im} \alpha_{\mathrm{trig}}$. Here *exp* stands for exponential and *trig* for trigonometric collisions. More precisely,

$$\alpha_{\exp}(u, w, a, v) = u \circ (x^{d(e-sd)/i^2} w^{d/i}(x^{d/i}))^{[a]} \circ v,$$
$$\alpha_{\mathrm{trig}}(u, z, a, v) = u \circ T_{n/i^2}(x, z)^{[a]} \circ v.$$

Here T_n is the *Dickson polynomial* of degree n, closely related to the Chebyshev polynomial and satisfying $T_n(x, 0) = x^n$. The monic (but possibly not original) polynomial $w = \sum_{0 \leq i \leq s} w_i x^i$ of degree s corresponds to the vector $(w_{s-1}, \ldots, w_0) \in F^s$, with $w_s = 1$. The *original shift* $p^{[a]}$ of a polynomial $p \in F[x]$ by $a \in F$ is $(x - p(a)) \circ p \circ (x + a)$. Furthermore, $\alpha_{\exp}$ and α_{trig} are injective, $\dim \operatorname{im} \alpha_{\exp} = 2i + s - 1$, and $\dim \operatorname{im} \alpha_{\mathrm{trig}} = 2i$. If $d = 2i$ then $\operatorname{im} \alpha_{\mathrm{trig}} \subseteq \operatorname{im} \alpha_{\exp}$. Otherwise we have $d \geq 3i$ and

$$\begin{aligned} \operatorname{im} \alpha_{\exp} \cap \operatorname{im} \alpha_{\mathrm{trig}} &= P_i \circ (x^{n/i^2})^{[F]} \circ P_i \\ &= \{u \circ ((x + a)^{n/i^2} - a^{n/i^2}) \circ v\colon u, v \in P_i, a \in F\} \end{aligned}$$

has dimension $2i - 1$. For the dimension inequality in this case, we have $2i + s - 1 \leq d + e/2 - 1 \leq d + e - 3$.

When $d = i$, the same Theorem 6.3 shows that $C_{n,d} \cap C_{n,e} = P_i \circ P_{e/d} \circ P_i$ is irreducible of dimension $2i+s-3 = 2d+e/d-3 < d+e-2 = \dim C_{n,d}$. For more details, see the cited paper. □

The main point here is that the dimension of this intersection is less than the dimension of its two arguments.

3. Bounding the height of f, g, and h

For the lower bounds of Theorems 4.5 and 5.1 below, we analyze the coefficient growth in the Newton-Taylor method. We start by making more explicit the form of f, g, and h in terms of the Newton-Taylor coefficients of $f = g \circ h$. Recall that $n = d \cdot e$ are the degrees.

Following the approach of Section 2. we consider $u = \sum_{1\le i<e} u_i x^i = \sum_{1\le i<e} f_{n-i} x^i \equiv \tilde{f} - 1 \bmod x^e$ and $v = \sum_{0\le \ell<e} v_\ell x^\ell$ with $v^d \equiv 1 + u \bmod x^e$ and $v(0) = 1$. The binomial expansion, as in Example 2.1, says that

$$v = (1+u)^{1/d} = \sum_{0\le \ell<e} \binom{1/d}{\ell} u^\ell \bmod x^e. \tag{3.1}$$

Then we call $h = x^e \cdot v(x^{-1})$ the *reverse* of v. This differs slightly from the usual reverse $x^{\deg v} \cdot v(x^{-1})$, since $\deg v < e$.

The Taylor iteration determines the coefficients of $g = \sum_{1\le j\le d} g_j x^j$ as follows. We have $g_d = 1$, and for $j = d-1, d-2, \ldots, 1$, g_j is the coefficient of x^{ej} in $f - \sum_{j<k\le d} g_k h^k$. Finally, $f = \sum_{1\le i\le n} f_i x^i = g \circ h = \sum_{1\le j\le d} g_j h^j$.

We first determine the "degrees" of h, g, and f in terms of the NT-coefficients of f. More precisely, if we consider the coefficients f_i with $i \in \mathrm{NT}_d$ as variables, then the coefficients of f (with $i \in \mathrm{cNT}_d$), g, and h are polynomials over $R = \mathbb{Z}[d^{-1}]$ in these variables. In order to make this rigorous, we introduce the generic polynomial $F^{\mathrm{NT}_d} = \sum_{i\in \mathrm{NT}_d} F_i x^i$ in the set $\boldsymbol{F}^{\mathrm{NT}_d} = \{F_i \colon i \in \mathrm{NT}_d\}$ of indeterminates.

Since all three polynomials are monic, we also set $F_n = G_d = H_e = 1 \in \mathbb{Z}$; these are not indeterminates. We imitate the above equations, but now in the new indeterminates rather than the coefficients of f.

$$\begin{aligned}
U &= \sum_{1\le i<e} U_i x^i = \sum_{0\le i<e} F_{n-i} x^i, \\
V &= \sum_{0\le \ell<e} \binom{1/d}{\ell} U^\ell \bmod x^e, \\
H &= \sum_{1\le \ell\le e} H_\ell x^\ell = \text{ reverse of } V, \\
G &= \sum_{1\le j\le d} G_j x^j, \text{ where} \\
&\qquad G_j = F_{ej} - (\text{coefficient of } x^{ej} \text{ in } \sum_{j<k\le d} G_k H^k), \\
F &= \sum_{1\le i\le n} F_i x^i = \sum_{1\le j\le d} G_j H^j = G \circ H.
\end{aligned} \tag{3.2}$$

All five quantities are polynomials in $R[x, \boldsymbol{F}^{\mathrm{NT}_d}]$, where $R = \mathbb{Z}[d^{-1}]$; for V, this follows from the formula for linear Newton iteration, which involves division only by d. F, G, and H are monic original, and each of their coefficients H_ℓ, G_j, and F_i is a polynomial in $R[\boldsymbol{F}^{\mathrm{NT}_d}]$. The G_j are well-defined for $j = d, d-1, \ldots, 1$, and all F_i that occur in the first and fourth equation have $i \in \mathrm{NT}_d$. It is convenient to express the

degrees under consideration using the (unusual) grading $\operatorname{gr}(F_i) = n - i$ for $i \in \mathrm{NT}_d$.

Proposition 3.1. *The polynomials are homogeneous of the following grades.*

(i) $\operatorname{gr} U_i = i$ *for* $1 \le i < e$,
(ii) $\operatorname{gr} V_\ell = \ell$ *for* $0 \le \ell < e$,
(iii) $\operatorname{gr} H_\ell = e - \ell$ *for* $1 \le \ell \le e$,
(iv) $\operatorname{gr} G_j = n - ej$ *for* $1 \le j \le d$,
(v) $\operatorname{gr} F_i = n - i$ *for* $1 \le i \le n$ *with* $i \notin NT_d$.

Proof. (ii) We have $V_0 = 1$, and for $\ell \ge 1$, V_ℓ is the coefficient of x^ℓ in the sum defining V. Since U is divisible by x, this coefficient is a sum of terms $U_{m_1} U_{m_2} \cdots U_{m_r}$ with $r \le \ell$, positive integers $m_1, \dots, m_r$, and $m_1 + m_2 + \cdots + m_r = \ell$, where we leave out the binomial coefficients. In particular, $\operatorname{gr} V_\ell = \ell$ or $V_\ell = 0$. Furthermore, F_{n-1}^ℓ occurs in U_1^ℓ and in V with nonzero coefficient $\binom{1/d}{\ell}$.

(iii) In the reverse $H = x^e \cdot V(x^{-1})$ of V, we have $\operatorname{gr} H_\ell = e - \ell$.

(iv) The claim is shown by downward induction on j from d to 1. For $j = d$, we have $G_d = 1$, of grade 0. For $j < d$, the contribution of $\boldsymbol{F}^{\mathrm{NT}_d}$ to G_j has grade $n - ej$. A summand $G_k H^k$ contributes terms of the form

$$G_k \cdot H_{\ell_1} \cdots H_{\ell_k}$$

with positive integers $\ell_1, \dots, \ell_k$ and $\ell_1 + \cdots + \ell_k = ej$. The grade of such a term equals the sum of the grades of its factors, which by induction is $n - ek + (e - \ell_1) + \cdots + (e - \ell_k) = n - ej$. Finally, F_{ej} occurs in G_j with nonzero coefficient 1.

(v) F_i is the coefficient of x^i in $\sum_{1 \le j \le d} G_j H^j$. Similarly as for (iv), a summand $G_j H^j$ contributes terms of the form

$$G_j \cdot H_{m_1} \cdots H_{m_j}$$

with $m_1 + \cdots + m_j = i$. The grade of such a term is $n - ej + (e - m_1) + \cdots (e - m_j) = n - i$. Furthermore, as F_{ej} occurs only in the summand $G_j H^j$, cancelation cannot occur unless $H^j = 0$ for every j. □

For a polynomial $f = \sum_i f_i x^i \in \mathbb{C}[x]$ with all $f_i \in \mathbb{C}$, we consider its height (or infinity norm) $\|f\| = \max_i |f_i|$. For $f \in C_{n,d}$, we denote as $f^{\mathrm{NT}_d} \in \mathbb{C}^{m_d}$ the vector of those coefficients of f whose index is in NT_d, and by $\|f^{\mathrm{NT}_d}\|$ its norm. Proposition 3.1 (v) implies that $\|f\| = O(\|f^{\mathrm{NT}_d}\|^n)$. Next we bound the coefficient implicit in this estimate. We start by considering u and v.

Lemma 3.2. *Let* $d, e \ge 2$ *be integers,* $0 \le \ell < e$, $A \ge 2$ *a real number,* $u, v \in \mathbb{C}[x]$ *with* $u(0) = 0$, $v(0) = 1$, $\deg u, \deg v < e$, $\|u\| \le A$, *and* $v^d \equiv (1 + u) \bmod x^e$. *Then the following hold.*

(i) $\|u^\ell\| \le (eA)^\ell$,
(ii) $v_0 = 1$ *and* $|v_\ell| \le (eA)^\ell$ *for* $\ell \ge 1$.

Proof. (i) Since $u = \sum_{1 \le i < e} u_i x^i$ is a sum of at most $e-1$ summands, the expansion of u^ℓ contains not more than $(e-1)^\ell < e^\ell$ summands, each of which is absolutely at most A^ℓ.

(ii) Equation (3.1) holds for v, and v_ℓ is the coefficient of x^ℓ in

$$v = (1+u)^{1/d} = \sum_{0 \le m < e} \binom{1/d}{m} u^m = 1 + \frac{u_1}{d} x + O(x^2). \tag{3.3}$$

Now $\binom{1/d}{0} = 1$, and for $m \ge 1$ we have

$$\begin{aligned} \left|\binom{1/d}{m}\right| &= \left|\frac{(1/d)\cdot(1/d-1)\cdots(1/d-m+1)}{m!}\right| \\ &= \left|\frac{1\cdot(1-d)\cdots(1-(m-1)d)}{d^m \cdot m!}\right| < \frac{d\cdot 2d\cdots(m-1)d}{d^m\cdot m!} = \frac{1}{dm}. \end{aligned}$$

For $C \ge 4$, we have $\sum_{1 \le m \le \ell} C^m/m \le 2C^\ell/\ell$, as follows by induction on $\ell \ge 1$. Since $d, e \ge 2$ and u^m with $m > \ell$ does not contribute to v_ℓ, we also have

$$|v_\ell| \le \sum_{1 \le m \le \ell} \frac{1}{dm} \|u^m\| \le \frac{1}{2} \sum_{1 \le m \le \ell} \frac{1}{m} (eA)^m \le \frac{(eA)^\ell}{\ell}.$$

□

Proposition 3.3. *Let $d, e \ge 2$ be integers, $f, g, h \in \mathbb{C}[x]$ be monic original polynomials of degrees $n = de$, d, e, respectively, $f = g \circ h$, and $\|f^{NT}\| \le A$ with $A \ge 2$. Then the following hold.*

(i) $|h_\ell| \le (eA)^{e-\ell}$ *for* $1 \le \ell \le e$,
(ii) $|g_j| \le e^{(d-j)(d+j+1)/2} (eA)^{n-ej}$ *for* $1 \le j \le d$,
(iii) $|f_i| \le 2e^{d(d+1)/2} (eA)^{n-i}$ *for* $1 \le i \le n$ *with* $i \notin NT_d$.

Proof. Since h is the reverse of v, Lemma 3.2 (ii) implies the claim (i).

For (ii), we have $g_d = 1$ and

$$g_j = \text{ coefficient of } x^{ej} \text{ in } f - \sum_{j < k \le d} g_k h^k$$

for $1 \le j < d$. Since $ej \in \mathrm{NT}_d$, the required coefficient of f occurs in f^{NT}. We first bound the coefficient of x^i in $h^k = (\sum_{1 \le \ell \le e} h_\ell x^\ell)^k$ for $1 \le i \le n$. It is the sum of terms $h_{m_1} \cdots h_{m_k}$ with integers $1 \le m_1, \ldots, m_k \le e$ and $m_1 + \cdots + m_k = i$. By (i), each such term is bounded in absolute value by $(eA)^{(e-m_1)\cdots(e-m_k)} = (eA)^{ek-i}$. Since h is a sum of e monomials, there are at most e^k such terms that contribute to the coefficient in question. Except for $i = n$ and $k = d$, the choice $m_1 = \cdots = m_k = e$ does not contribute. Thus the absolute value of this coefficient of x^i is at most

$$(e^k - 1)(eA)^{ek-i}. \tag{3.4}$$

For $1 \le j < d$, we have with $i = ej$ that

$$|g_j| \le A + \sum_{j<k\le d} |g_k|(e^k - 1)(eA)^{ek-ej}. \tag{3.5}$$

In (ii), we claim that

$$|g_j| \le b_j (eA)^{n-ej} \tag{3.6}$$

with $b_j = e^{(d-j)(d+j+1)/2}$. We have $g_d = b_d = 1$ and $b_{d-1} = e^d$. First, we show that $\sum_{j<k\le d} b_k(e^k - 1) < b_j$ by downward induction for $j = d-1, \dots, 1$. For $j = d-1$, we have $e^d - 1 < e^d = b_{d-1}$. For $j < d-1$, we find

$$\begin{aligned}\sum_{j<k\le d} b_k(e^k - 1) &= \sum_{j+1<k\le d} b_k(e^k - 1) + b_{j+1}(e^{j+1} - 1) \\ &< b_{j+1} + b_{j+1}(e^{j+1} - 1) = b_j.\end{aligned}$$

We will absorb the lonely term A in (3.5) into the summand for $k = d-1$. First, we note that

$$\frac{2}{e-1} + 2 \le (2e)^e, \tag{3.7}$$

since $e \ge 2$. (In fact, (3.7) holds for $e \ge 1.55$.) This implies that

$$\frac{A}{(e^{d-1} - 1)(eA)^{n-ej}} + \frac{A}{(eA)^e} \le 1 \tag{3.8}$$

for $j < d$, since (3.7) is the special case $d = 2$, $j = d-1$, $A = 2$ of (3.8), the left hand side of (3.8) is monotonically decreasing in d and A and increasing in j, and the special case takes the extreme values of d, j, and A under our assumptions. In turn, this means that

$$\frac{A}{(e^{d-1} - 1)(eA)^{n-ej}} + (A + (e^d - 1)(eA)^e)(eA)^{-e} \le e^d = b_{d-1}.$$

By (3.5), we have $|g_{d-1}| \le A + (e^d - 1)(eA)^e$, and thus

$$\begin{aligned}&A + |g_{d-1}|(e^{d-1} - 1)(eA)^{n-e-ej} \\ &\le (e^{d-1} - 1)(eA)^{n-ej}\Big(\frac{A}{(e^{d-1} - 1)(eA)^{n-ej}} \\ &\quad + (A + (e^d - 1)(eA)^e)(eA)^{-e}\Big) \\ &\le b_{d-1}(e^{d-1} - 1)(eA)^{n-ej}.\end{aligned} \tag{3.9}$$

We finally prove (3.6) by downward induction for $j = d, d-1, \dots, 1$, using (3.5) and (3.9). The cases where $j \in \{d, d-1\}$ are clear. For

$j < d-1$, we separate the summands for $k \in \{d, d-1\}$ and find

$$\begin{aligned}
|g_j| &\le A + \sum_{j<k\le d} |g_k|(e^k-1)(eA)^{ek-ej} \\
&= A + (e^d-1)(eA)^{n-ej} + |g_{d-1}|(e^{d-1}-1)(eA)^{n-e-ej} \\
&\quad + \sum_{j<k\le d-2} |g_k|(e^k-1)(eA)^{ek-ej} \\
&\le \sum_{j<k\le d} b_k (eA)^{n-ek}(e^k-1)(eA)^{ek-ej} \\
&= (eA)^{n-ej} \sum_{j<k\le d} b_k(e^k-1) < b_j (eA)^{n-ej}.
\end{aligned}$$

(iii) Since f_i is the coefficient of x^i in $\sum_{1\le j\le d} g_j h^j$, we find from (3.4) that

$$\begin{aligned}
|f_i| &\le \sum_{1\le j\le d} e^{(d-j)(d+j+1)/2}(eA)^{n-ej} \cdot e^j (eA)^{ej-i} \\
&= e^{d(d+1)/2}(eA)^{n-i} \sum_{1\le j\le d} e^{-j(j-1)/2}.
\end{aligned}$$

The exponents in the sum are pairwise different, so that its value is at most the complete geometric sum, of value $e/(e-1) \le 2$. □

According to Proposition 3.1, all f_i (with $i \in \mathrm{cNT}_d$), g_j, and h_ℓ are homogeneous of grades $n-i$, $n-ej$, and $e-\ell$, respectively. This implies that the exponents of A in Proposition 3.3 cannot be improved. However, the exponents of e are less precisely determined.

Corollary 3.4. *Let $A, B \ge 2$ and $f = g \circ h \in C_{n,d}$ with g and h monic original of degrees d and e, respectively, and $\|f^{NT}\| \le A \le B^{1/n}/e^{1+(d+1)/2e}$. Then the following bounds hold.*

(i) $\|h\| \le (eA)^{e-1}$,
(ii) $\|g\| \le e^{(d(d+1)/2-1}(eA)^{n-e}$,
(iii) $\|f\| \le 2e^{d(d+1)/2}(eA)^{n-1} < e^{d(d+1)/2}(eA)^n \le B$.

4. Density estimates for $C_{n,d}(\mathbb{R})$ and $C_n(\mathbb{R})$

In this section we consider the set $P_n(\mathbb{R})$ of monic original polynomials of composite degree n with real coefficients and the subsets $C_n(\mathbb{R})$ and $C_{n,d}(\mathbb{R})$ of $P_n(\mathbb{R})$ for a proper divisor d of n. Our aim is to obtain density estimates on tubes around $C_{n,d}(\mathbb{R})$ and $C_n(\mathbb{R})$. We drop the field $F = \mathbb{R}$ from our notation in this section.

We identify P_n with $\mathbb{R}^{n-1}$ by mapping $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x \in P_n$ to $(a_{n-1}, \ldots, a_1) \in \mathbb{R}^{n-1}$. As shown above, $C_{n,d}$ is an affine real variety of dimension $d + n/d - 2$. In particular, $C_{n,d}$ has codimension at least $n/2$, and thus its (standard Lebesgue) volume is 0. For a meaningful

concept, we take a specific ϵ-tube around $C_{n,d}$. Namely, for each $f = \sum_{1\le i\le n} f_i x^i \in C_{n,d}$ and $\epsilon > 0$, we define the ϵ-neighborhood of f as

$$U_\epsilon(f) = \big\{u = \sum_{1\le i\le n} u_i x^i \in P_n(\mathbb{R})\colon u_i = f_i \text{ for } i \in \mathrm{NT}_d, \\ |u_i - f_i| < \epsilon \text{ for } i \in \mathrm{cNT}_d\big\}.$$

Thus $U_\epsilon(f)$ is an open m_d-dimensional hypercube $(-\epsilon,\epsilon)^{m_d}$ in P_n. Around each coefficient f_i with $i \in \mathrm{cNT}_d$ we have a real interval of length 2ϵ. We also set

$$U_\epsilon(C_{n,d}) = \bigcup_{f\in C_{n,d}} U_\epsilon(f). \tag{4.1}$$

In order to have finite volumes, we take a bound $B > 0$ on the coefficients and consider the $(n-1)$-dimensional hypercube

$$P_{n,B} = \big\{f = \sum_{1\le i\le n} f_i x^i \in P_n\colon |f_i| < B \text{ for } 1 \le i < n\big\}$$

around P_n and its intersection with the ϵ-tube

$$U_{\epsilon,B}(C_{n,d}) = U_\epsilon(C_{n,d}) \cap P_{n,B}.$$

Our main purpose is to obtain estimates on the density $\mathrm{den}_{\epsilon,B}(C_{n,d})$ of the ϵ-tube in $P_{n,B}$, namely

$$\mathrm{den}_{\epsilon,B}(C_{n,d}) = \frac{\mathrm{vol}\,(U_{\epsilon,B}(C_{n,d}))}{\mathrm{vol}(P_{n,B})} = \frac{\mathrm{vol}\,(U_{\epsilon,B}(C_{n,d}))}{(2B)^{n-1}}. \tag{4.2}$$

In a slightly different model of our situation, we might allow arbitrary leading coefficients in our polynomials, rather than just 1. It would then be sufficient to just consider the unit hypercube with $B = 1$ and scale the resulting density. However, our approach is overall more convenient and allows an easier comparison with previous work; see Section 6.

Example 4.1. For perspective, we calculate the density of the linear subspace $L = \mathbb{R}^k \times \{0\}^{n-k} \subseteq \mathbb{R}^n$. For $x \in L$, we take $U_\epsilon(x) = \{(x_1,\dots,x_k)\} \times (-\epsilon,\epsilon)^{n-k}$ and have, for $B > \epsilon$,

$$U_\epsilon(L) = \mathbb{R}^k \times (-\epsilon,\epsilon)^{n-k}, \\ \mathrm{den}_{\epsilon,B}(L) = \frac{\mathrm{vol}\,\big((-B,B)^k \times (-\epsilon,\epsilon)^{n-k}\big)}{(2B)^n} = \Big(\frac{\epsilon}{B}\Big)^{n-k}. \tag{4.3}$$

Let $\chi\colon P_{n,B} \to \{0,1\}$ be the characteristic function of $U_{\epsilon,B}(C_{n,d}) \subseteq P_{n,B}$. Then the density is

$$\mathrm{den}_{\epsilon,B}(C_{n,d}) = \frac{1}{(2B)^{n-1}} \int_{P_{n,B}} \chi(a)\,\mathrm{d}a.$$

For a subset $S \subseteq N$ of cardinality s, we consider the projection $\pi^S\colon \mathbb{R}^{n-1} \to \mathbb{R}^s$ onto the coordinates in S: $\pi^S(a_{n-1},\dots,a_1) = (a_i\colon i \in$

S). Furthermore, for a subset $C \subseteq P_n$, we write C^S for $\pi^S(C)$. By reordering the coordinates, we can express the hypercube $P_{n,B}$ as the Cartesian product $P_{n,B} = P_{n,B}^{\mathrm{NT}_d} \times P_{n,B}^{\mathrm{cNT}_d}$. According to Fubini's theorem we have

$$\begin{aligned} \mathrm{vol}\big(U_{\epsilon,B}(C_{n,d})\big) &= \int_{P_{n,B}} \chi(a)\,\mathrm{d}a \\ &= \int_{P_{n,B}^{\mathrm{NT}_d}} \Big(\int_{P_{n,B}^{\mathrm{cNT}_d}} \chi(a^{\mathrm{NT}_d}, a^{\mathrm{cNT}_d})\,\mathrm{d}a^{\mathrm{cNT}_d} \Big)\,\mathrm{d}a^{\mathrm{NT}_d}. \end{aligned} \tag{4.4}$$

Here $(a^{\mathrm{NT}_d}, a^{\mathrm{cNT}_d})$ are the coordinates of $a \in P_{n,B}$ in the product representation, and a^{NT_d} refers to a point in $P_{n,B}^{\mathrm{NT}_d}$.

Lemma 4.2. *Let $0 < \epsilon < B$ and $b \in P_{n,B}^{NT_d}$.*

(i) *We have*

$$\int_{P_{n,B}^{cNT_d}} \chi(b,c)\,\mathrm{d}c \le (2\epsilon)^{m_d},$$

where c ranges over $P_{n,B}^{cNT_d}$.

(ii) *Let $f \in C_{n,d}$ be the unique element with $\pi^{NT_d}(f) = b$. If $U_\epsilon(f) \subseteq P_{n,B}$, then equality holds in* (i).

Proof. The existence and uniqueness of f follow from the section $\nu_{n,d}\colon C_{n,d} \to P_d \times P_{n/d}$ (Theorem 2.2). For any $c \in P_{n,B}^{\mathrm{cNT}_d}$, we have

$$\chi(b,c) = 1 \iff (b,c) \in U_{\epsilon,B}(C_{n,d}) \iff (b,c) \in U_\epsilon(f) \cap P_{n,B}.$$

Therefore

$$\int_{P_{n,B}^{\mathrm{cNT}_d}} \chi(b,c)\,\mathrm{d}c \le \int_{U_\epsilon(f)} \mathrm{d}c = (2\epsilon)^{m_d}.$$

If $U_\epsilon(f) \subseteq P_{n,B}$, then equality holds. This shows both claims. □

We derive the following upper bound on the density of $C_{n,d}$.

Proposition 4.3. *With notation and assumptions as above, we have*

$$\mathrm{den}_{\epsilon,B}(C_{n,d}) \le \left(\frac{\epsilon}{B}\right)^{m_d}.$$

Proof. Combining (4.4) and Lemma 4.2, we obtain

$$\begin{aligned} \mathrm{vol}\left(U_{\epsilon,B}(C_{n,d})\right) &= \int_{P_{n,B}} \chi(a)\,\mathrm{d}a \\ &= \int_{P_{n,B}^{\mathrm{NT}_d}} \left(\int_{P_{n,B}^{\mathrm{cNT}_d}} \chi(a_{\mathrm{NT}_d}, a^{\mathrm{cNT}_d}) \mathrm{d}a^{\mathrm{cNT}_d} \right) \mathrm{d}a^{\mathrm{NT}_d} \\ &\le \int_{P_{n,B}^{\mathrm{NT}_d}} (2\epsilon)^{m_d} \mathrm{d}a^{\mathrm{NT}_d} = (2\epsilon)^{m_d} (2B)^{n-1-m_d}. \end{aligned}$$

Using (4.2), it follows that

$$\operatorname{den}_{\epsilon,B}(C_{n,d}) \leq \frac{(2\epsilon)^{m_d}(2B)^{n-1-m_d}}{(2B)^{n-1}} = \Big(\frac{\epsilon}{B}\Big)^{m_d}.$$

□

Now we derive a lower bound. We set

$$\alpha_{n,d} = (d/n)^{1+d(d+1)/2n} \tag{4.5}$$

and $A_B = \alpha_{n,d}B^{1/n}$. From Corollary 3.4 (iii), we know that if $B \geq (2/\alpha_{n,d})^n$ and $f \in C_{n,d}$ is such that $f^{\mathrm{NT}_d} \in P^{\mathrm{NT}_d}_{n,A_{B-\epsilon}}$, then $U_\epsilon(f) \subset U_{\epsilon,B}(C_{n,d})$.

Proposition 4.4. *With notation and assumptions as above, and assuming that $B - \epsilon \geq (2/\alpha_{n,d})^n$, we have*

$$\operatorname{den}_{\epsilon,B}(C_{n,d}) \geq \Big(\frac{\epsilon}{B}\Big)^{m_d}\left(\frac{\alpha_{n,d}(B-\epsilon)^{1/n}}{B}\right)^{d+\frac{n}{d}-2}.$$

Proof. We let

$$V = \bigcup_{\{f\in C_{n,d}: f^{\mathrm{NT}_d}\in P^{\mathrm{NT}_d}_{n,A_{B-\epsilon}}\}} U_\epsilon(f) \subseteq U_{\epsilon,B}(C_{n,d})$$

and $\chi_\epsilon\colon P_{n,B} \to \{0,1\}$ be the characteristic function of V. Since $V \subseteq U_{\epsilon,B}(C_{n,d})$, it follows that $\chi_\epsilon(a) \leq \chi(a)$ for every $a \in P_{n,B}$. Using Lemma 4.2(ii), we find

$$\begin{aligned}\int_{P_{n,B}} \chi(a)\,\mathrm{d}a &\geq \int_{P_{n,B}} \chi_\epsilon(a)\,\mathrm{d}a \\ &= \int_{P^{\mathrm{NT}_d}_{n,A_{B-\epsilon}}} \Big(\int_{P^{\mathrm{cNT}_d}_{n,B}} \chi_\epsilon(a^{\mathrm{NT}_d}, a^{\mathrm{cNT}_d})\,\mathrm{d}a^{\mathrm{cNT}_d}\Big)\mathrm{d}a^{\mathrm{NT}_d} \\ &= \int_{P^{\mathrm{NT}_d}_{n,A_{B-\epsilon}}} (2\epsilon)^{m_d}\mathrm{d}a^{\mathrm{NT}_d} = (2\epsilon)^{m_d}\big(2A_{B-\epsilon}\big)^{n-1-m_d}.\end{aligned}$$

Dividing by $\operatorname{vol}(P_{n,B}) = (2B)^{n-1}$ and using (2.2) yields the claimed bound. □

We summarize the results of Propositions 4.3 and 4.4 as follows.

Theorem 4.5. *Let $0 < \epsilon < B$ be as in Proposition 4.4 and let d be a proper divisor of n. Then we have the following bounds on the density of the ϵ-tube around $C_{n,d}(\mathbb{R})$:*

$$c_d(\epsilon,B)\cdot\Big(\frac{\epsilon}{B}\Big)^{n-d-\frac{n}{d}+1} \leq \operatorname{den}_{\epsilon,B}(C_{n,d}(\mathbb{R})) \leq \Big(\frac{\epsilon}{B}\Big)^{n-d-\frac{n}{d}+1},$$

where $c_d(\epsilon,B) = \Big(\frac{(B-\epsilon)^{\frac{1}{n}}}{B}\big(\frac{d}{n}\big)^{1+\frac{d(d+1)}{2n}}\Big)^{d+\frac{n}{d}-2}$.

We thus have good bounds on the irreducible components of C_n in (2.1). How to get such bounds for C_n itself? In Theorem 4.5, we consider ϵ-tubes around $C_{n,d}$ of a direction and a dimension that varies with d. For C_n, it seems appropriate to consider ϵ-tubes of the same dimension for all d, as follows.

We let ℓ be the least prime number dividing the composite integer n. If $n = \ell^2$, then $C_n = C_{n,\ell}$ has just one component. Otherwise, Theorem 2.2 shows that $C_n(\mathbb{R}) \subseteq \mathbb{R}^{n-1}$ has two "large" components, namely $C_{n,\ell}$ and $C_{n,n/\ell}$, each of dimension $\ell + n/\ell - 2 = \dim C_n$. As a consequence, for the density of C_n we consider ϵ–tubes of the same dimension $m_\ell = n - 1 - \dim C_n$ around each component of C_n. For a proper divisor $d \notin \{\ell, n/\ell\}$ of n, we have $\dim C_{n,d} < \dim C_n$ and thus $\dim C_{n,d} + m_\ell < n - 1$. Then any m_ℓ–dimensional ϵ–tube around $C_{n,d}$ has volume and density equal to zero. Furthermore, Theorem 2.3 implies that the sum of the two "large" densities bounds the density of C_n from below. In other words, we define $\mathrm{vol}_{\epsilon,B}(C_n) = \mathrm{vol}(U_{\epsilon,B}(C_{n,\ell}) \cup U_{\epsilon,B}(C_{n,n/\ell}))$ and $\mathrm{den}_{\epsilon,B}(C_n) = \mathrm{vol}_{\epsilon,B}(C_n)/\mathrm{vol}(P_{n,B})$. Setting

$$\delta_n = \begin{cases} 1 & \text{if } n = \ell^2, \\ 2 & \text{otherwise,} \end{cases} \tag{4.6}$$

we obtain the following result.

Theorem 4.6. *Let $0 < \epsilon < B$ be such that $B - \epsilon \geq (2/\alpha_{n,d})^n$ and let ℓ be the least prime number dividing the composite integer n. Then*

$$\delta_n c_\ell(\epsilon, B) \left(\frac{\epsilon}{B}\right)^{n-\ell-n/\ell+1} \leq \mathrm{den}_{\epsilon,B}(C_n(\mathbb{R})) \leq \delta_n \left(\frac{\epsilon}{B}\right)^{n-\ell-n/\ell+1}.$$

The approximation factor $c_\ell(\epsilon, B)$ in the lower bound tends to a constant smaller than 1, depending only on n, when ϵ/B gets small compared to n.

5. Density estimates for $C_{n,d}(\mathbb{C})$ and $C_n(\mathbb{C})$

In this section, we take $F = \mathbb{C}$ and consider the real volume on $P_n(\mathbb{C})$ as a $(2n-2)$-dimensional real vector space. We discuss briefly the density estimates we obtain for $C_{n,d}(\mathbb{C})$. The approach is similar to that of Section 4; therefore, we merely sketch the proofs and summarize the results we obtain. We drop the field $F = \mathbb{C}$ from our notation.

As in (4.1), we take an ϵ-tube around $C_{n,d}$, namely given $f = \sum_{1 \leq i \leq n} f_i x^i \in C_{n,d}$ and $\epsilon > 0$, we define the (complex) ϵ-neighborhood of f as

$$U_\epsilon(f) = \Big\{ u = \sum_{1 \leq i \leq n} u_i x^i \in P_n \colon u_i = f_i \text{ for } i \in \mathrm{NT}_d, \\ |u_i - f_i| < \epsilon \text{ for } i \in \mathrm{cNT}_d \Big\}.$$

Thus $U_\epsilon(f)$ is an open m_d-dimensional complex polycylinder in P_n, of real dimension $2m_d$. Around each coefficient f_i with $i \in \mathrm{cNT}_d$, we have a real circle of radius ϵ and area $\pi\epsilon^2$. For $B > 0$, we set

$$U_\epsilon(C_{n,d}) = \bigcup_{f \in C_{n,d}} U_\epsilon(f),$$
$$P_{n,B} = \Big\{ f = \sum_{1 \le i \le n} f_i x^i \in P_n \colon |f_i| < B \text{ for } 1 \le i < n \Big\},$$
$$U_{\epsilon,B}(C_{n,d}) = U_\epsilon(C_{n,d}) \cap P_{n,B}.$$

Then $\mathrm{vol}(P_{n,B}) = (\pi B^2)^{n-1}$. Let $\chi \colon P_{n,B} \to \{0,1\}$ be the characteristic function of $U_{\epsilon,B}(C_{n,d})$. As before, we express the polycylinder $P_{n,B}$ as the Cartesian product $P_{n,B} = P_{n,B}^{\mathrm{NT}_d} \times P_{n,B}^{\mathrm{cNT}_d}$ and apply Fubini's theorem to obtain

$$\mathrm{vol}\left(U_{\epsilon,B}(C_{n,d})\right) = \int_{P_{n,B}^{\mathrm{NT}_d}} \Big(\int_{P_{n,B}^{\mathrm{cNT}_d}} \chi(a^{\mathrm{NT}_d}, a^{\mathrm{cNT}_d})\, \mathrm{d}a^{\mathrm{cNT}_d} \Big)\, \mathrm{d}a^{\mathrm{NT}_d}. \tag{5.1}$$

For an arbitrary element $b \in P_{n,B}^{\mathrm{NT}_d}$, there exists a unique $f \in C_{n,d}$ with $\pi^{\mathrm{NT}_d}(f) = b$ by Theorem 2.2. Then the function $\chi(b, f^{\mathrm{cNT}_d})$ takes the value 1 on an m_d-dimensional complex polycylinder of radius ϵ whose center is the vector of coefficients of f corresponding to indices in cNT_d. As a consequence, we have

$$\mathrm{vol}\left(U_{\epsilon,B}(C_{n,d})\right) = \int_{P_{n,B}^{\mathrm{NT}_d}} (\pi\epsilon^2)^{m_d} \mathrm{d}a^{\mathrm{NT}_d} \le (\pi\epsilon^2)^{m_d} (\pi B^2)^{n-1-m_d}.$$

This yields the complex analog of the upper bound of Proposition 4.3:

$$\mathrm{den}_{\epsilon,B}(C_{n,d}) = \frac{\mathrm{vol}(U_{\epsilon,B}(C_{n,d}))}{(\pi B^2)^{n-1}} \le \big(\frac{\epsilon}{B}\big)^{2m_d}.$$

On the other hand, for a lower bound we consider as in Proposition 4.4 the characteristic function $\chi_\epsilon \colon P_{n,B} \to \{0,1\}$ of the set

$$V = \bigcup_{f \in C_{n,d} \cap P_{n,A_{B-\epsilon}}} U_\epsilon(f) \subseteq U_{\epsilon,B}(C_{n,d})$$

for $\epsilon < B$, where $A_{B-\epsilon} = \alpha_{n,d}(B-\epsilon)^{\frac{1}{n}}$ and $\alpha_{n,d}$ is defined as in (4.5), and argue as before to obtain

$$\mathrm{vol}(U_{\epsilon,B}(C_{n,d})) \ge \mathrm{vol}(V) \ge (\pi\epsilon^2)^{m_d} (\pi(\alpha_{n,d}(B-\epsilon)^{\frac{1}{n}})^2)^{d+\frac{n}{d}-2},$$

provided that $B - \epsilon \ge (2/\alpha_{n,d})^n$.

Finally, in order to obtain a meaningful notion of density of C_n, we consider, as in Section 4, the ϵ–tube $U_{\epsilon,B}(C_n) = U_{\epsilon,B}(C_{n,\ell}) \cup U_{\epsilon,B}\big(C_{n,n/\ell}\big)$ around C_n, where ℓ is the smallest prime divisor of n. Summarizing, we have the following results on the density of these tubes.

Theorem 5.1. *Let $0 < \epsilon < B$, n be a composite integer, and δ_n as in* (4.6).

(i) *Let d be a proper divisor of n and $B - \epsilon \geq (2/\alpha_{n,d})^n$. Then*

$$c'_d(\epsilon, B) \left(\frac{\epsilon}{B}\right)^{2(n-d-\frac{n}{d}+1)} \leq \mathrm{den}_{\epsilon,B}(C_{n,d}(\mathbb{C})) \leq \left(\frac{\epsilon}{B}\right)^{2(n-d-\frac{n}{d}+1)},$$

where $c'_d(\epsilon, B) = \left((B-\epsilon)^{\frac{1}{n}} B^{-1} (\frac{d}{n})^{1+\frac{d(d+1)}{2n}}\right)^{2(d+\frac{n}{d}-2)}$.

(ii) *Let ℓ be the smallest prime divisor of n and $B - \epsilon \geq (2/\alpha_{n,\ell})^n$. Then*

$$\delta_n c'_\ell(\epsilon, B) \left(\frac{\epsilon}{B}\right)^{2(n-\ell-\frac{n}{\ell}+1)} \leq \mathrm{den}_{\epsilon,B}(C_n(\mathbb{C})) \leq \delta_n \left(\frac{\epsilon}{B}\right)^{2(n-\ell-\frac{n}{\ell}+1)}.$$

6. Discussion

For an arbitrary irreducible algebraic subvariety X of $\mathbb{R}^n$ with codimension m, we might attach a hypercube $(-\epsilon, \epsilon)^m$ to each smooth point x of X in the normal direction to X, thus following the second recipe listed in the introduction. The singular points do not contribute to the volume. Then this tube around X has real dimension n. In an analog of Lemma 4.2, the coordinates in NT_d are replaced by local coordinates at the point and those of cNT_d by coordinate functions normal to them. Instead of having a unique f as in the proof of that lemma, we only know that the normal linear space, of complementary dimension, intersects generically in at most $\deg X$ points. The resulting upper bound then is $\deg X \cdot (2\epsilon)^m$.

Our construction in (4.1) of the ϵ-tube around $C_{n,d}$ does not follow this general recipe, since the ϵ-hypercube in the direction of the coordinates from cNT_d is, in general, not normal to $C_{n,d}$. It is not clear whether one can obtain upper and lower bounds as in Theorems 4.6 and 5.1 for other choices of the ϵ-tubes.

Cheung *et al.* [5] also provide bounds on the density of $C_n(\mathbb{C})$. Instead of the precise information provided by the Newton-Taylor method of Section 2, they use the fact that $C_n(\mathbb{C}) \subseteq X$ for a certain hypersurface X and then a specific one-dimensional ϵ-tube around X chosen to suit their argument, following the third of the options listed in the introduction. They show that $\mathrm{den}_{\epsilon,B}(C_n(\mathbb{C})) \leq (n^2 - 2n) \cdot (\epsilon/B)^2$, which is to be compared with our result in Theorem 5.1.

7. Acknowledgements

Many thanks go to Igor Shparlinski for alerting us to the paper of Cheung *et al.* [5].

References

1. David R. Barton and Richard Zippel, *Polynomial decomposition algorithms*, J. Symb. Comput. **1** (1985), 159–168.

2. C. Beltrán and L. M. Pardo. *Estimates on the distribution of the condition number of singular matrices*. Foundations of Computational Mathematics **7**(1) (2007), 87–134.
3. Raoul Blankertz, *A polynomial time algorithm for computing all minimal decompositions of a polynomial*. ACM Communications in Computer Algebra **48**(1) (2014), 13–23.
4. Raoul Blankertz, Joachim von zur Gathen, and Konstantin Ziegler, *Compositions and collisions at degree p^2*, J. Symb. Comput. **59** (2013), 113–145.
5. Wai Shun Cheung, Tuen Wai Ng and Chiu Yin Tsang, *Density estimates on composite polynomials*. Journal of the Australian Mathematical Society **95** (2013), 329–342.
6. James W. Demmel, *The probability that a numerical analysis problem is difficult*. Mathematics of Computation **50**(182) (1988), 449–480.
7. F. Dorey and G. Whaples, *Prime and composite polynomials*, J. Algebra **28** (1974), 88–101.
8. Michael D. Fried and R. E. MacRae, *On the invariance of chains of fields*, Illinois J. Math. **13** (1969), 165–171.
9. W. Fulton, *Intersection Theory*. Springer, Berlin Heidelberg New York, 1984.
10. Joachim von zur Gathen, *Functional decomposition of polynomials: The tame case*, J. Symb. Comput. **9** (1990), no. 3, 281–299.
11. ———, *Counting decomposable univariate polynomials*, Combin. Probab. Comput. **24** (2015), no. 1, 294–328.
12. ———, *Lower bounds for decomposable univariate wild polynomials*, J. Symb. Comput. **50** (2013), 409–430.
13. ———, *Normal form for Ritt's Second Theorem*, Finite Fields Appl. **27** (2014), 41–71.
14. Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, third ed., Cambridge University Press, Cambridge, UK, 2013.
15. Joachim von zur Gathen, Mark Giesbrecht and Konstantin Ziegler, *Composition collisions and projective polynomials. Statement of results*. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation ISSAC '10, Munich, Germany*, Stephen Watt, editor, 2010, 123–130. ACM Press. Preprint available at `http://arxiv.org/abs/1005.1087`.
16. Mark William Giesbrecht, *Some results on the functional decomposition of polynomials*, Masters thesis, Department of Computer Science, University of Toronto. Technical Report 209/88. Available as http://arxiv.org/abs/1004.5433, 1988.
17. Alfred Gray. *Tubes*. Addison-Wesley, 1990.
18. J. Heintz. *Definability and fast quantifier elimination in algebraically closed fields*. Theoretical Computer Science **24**(3) (1983) 239–277.
19. Harold Hotelling, *Tubes and spheres in n-spaces, and a class of statistical problems*. American Journal of Mathematics **61**(2) (1939), 440–460.
20. Dexter Kozen and Susan Landau, *Polynomial decomposition algorithms*, J. Symb. Comput. **7** (1989), 445–456.
21. Andrzej Schinzel, *Selected topics on polynomials*, The University of Michigan Press, Ann Arbor, 1982.
22. ———, *Polynomials with special regard to reducibility*, Cambridge University Press, Cambridge, UK, 2000.
23. Mike Shub and Steve Smale, *Complexity of Bezout's Theorem II. Volumes and probabilities*. In *Computational Algebraic Geometry*, F. Eyssette and A. Galligo, editors, volume 109 of *Progress in Mathematics*, 1993, 267–285. Birkhäuser, Boston MA.

24. Steve Smale, *The fundamental theorem of algebra and complexity theory*. Bulletin of the American Mathematical Society **4** (1981), 1–36.
25. W. Vogel, *Results on Bézout's theorem*, volume 74 of *Tata Inst. Fundam. Res. Lect. Math.* Tata Institute for Fundamental Research, Bombay, 1984.
26. Hermann Weyl, *On the volume of tubes*. American Journal of Mathematics **61**(2) (1939), 461–472.
27. U. Zannier, *Ritt's Second Theorem in arbitrary characteristic*, J. Reine Angew. Math. **445** (1993), no. 175-203, 1993.
28. Konstantin Ziegler (2014). *Tame decompositions and collisions*. J. Symb. Comput. **75** 2016, 244–268.

[1]B-IT, Universität Bonn, D - 53113 Bonn
E-mail address: gathen@bit.uni-bonn.de

[2]Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150 (B1613GSX) Los Polvorines, Buenos Aires, Argentina
E-mail address: gmatera@ungs.edu.ar

[3] National Council of Science and Technology (CONICET), Argentina