Forum of Mathematics, Sigma (2026), **Vol. 14**:e52 1–23
doi:10.1017/fms.2026.10202

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

A new bound on cofactors of sparse polynomials

Ido Nahshon[1] and Amir Shpilka[2]

[1]Blavatnik School of Computer Science and AI, Tel Aviv University, Tel Aviv, Israel; E-mail: ido.nahshon39@gmail.com.
[2]Blavatnik School of Computer Science and AI, Tel Aviv University, Tel Aviv, Israel; E-mail: shpilka@tauex.tau.ac.il (Corresponding author).

Received: 24 May 2025; **Revised:** 21 January 2026; **Accepted:** 21 January 2026

2020 Mathematics Subject Classification: *Primary* – 11C08; *Secondary* – 68W30, 12D05

Abstract

We prove that for polynomials $f, g, h \in \mathbb{Z}[x]$ satisfying $f = gh$ and $f(0) \neq 0$, the ℓ_2-norm of the cofactor h is bounded by

$$\|h\|_2 \leq \sqrt{\frac{\|g\|_0}{\deg g}} \cdot \|f\|_1 \cdot \left(\widetilde{O}\left(\frac{\|g\|_0^{2.5} \cdot \deg^2 f}{\sqrt{\deg g}}\right)\right)^{\|g\|_0 - 1},$$

where $\|g\|_0$ is the number of nonzero coefficients of g (its sparsity). We also obtain similar results for polynomials over $\mathbb{C}$. These bounds are an improvement over the bounds presented in an earlier conference version of this paper [NS24].

This result significantly improves upon previously known exponential bounds (in $\deg f$) for general polynomials. It further implies that, under exact division, the polynomial division algorithm runs in quasi-linear time with respect to the input size and the number of terms in the quotient h. This resolves a long-standing open problem concerning the exact divisibility of sparse polynomials.

In particular, our result demonstrates a quadratic separation between the runtime (and representation size) of exact and nonexact divisibility by sparse polynomials. Notably, prior to our work, it was not even known whether the representation size of the quotient polynomial could be bounded by a sub-quadratic function of its number of terms, or even by a subquadratic function of $\deg f$.

Contents

1. Introduction

Let $f, g, h \in \mathbb{C}[x]$ be polynomials such that $f = gh$. Classical results of Gel'fond, Mahler and Mignotte provide upper bounds on the height of h (ℓ_∞ norm of its vector of coefficients) given information on the coefficients of g and f [Gel60, Mah62, Mig74, Mig88]. These results were used by Gel'fond in the study of transcendence and are widely used in computer algebra to prove upper bounds on the running time of algorithms, such as in the polynomial factorization algorithm of Lenstra, Lenstra, and Lovász [LLL82].

The first of these bounds was proved by Gel'fond [Gel60] (see also [Mah62] and [BG06, Lemma 1.6.11]).

Theorem 1.1 (Gel'fond's Lemma). *Let $f, g, h \in \mathbb{C}[x]$ such that $f = gh$. Then,*

$$\|h\|_\infty \leq 2^{\deg f} \frac{\|f\|_\infty}{\|g\|_\infty}. \tag{1}$$

Improved bounds were provided by Mahler [Mah62] and consequently by Mignotte [Mig74].

Theorem 1.2 (Mignotte's Bound [Mig74, Theorem 2]). *Let $f, g, h \in \mathbb{Z}[x]$ such that $f = gh$. Then,*

$$\|h\|_1 \leq 2^{\deg h} \|f\|_2 \tag{2}$$

Discussions about this classical inequality can be found in [Mig88, Section 2] and [Mig12, Chapter 4]. This bound is also known to be quite tight; for any $d \in \mathbb{N}$ there exists $h \in \mathbb{Z}[x]$ of degree d and $f \in \mathbb{Z}[x]$ such that

$$\|h\|_1 \geq \Omega\left(\frac{2^d}{d^2 \log d}\right) \|f\|_2.$$

When $\|h\|_0$ is guaranteed to be small relative to its degree, tighter bounds can be obtained. For instance, Giorgi, Grenet and Perret du Cray established the following bound by a straightforward induction on the polynomial division algorithm [GGPdC21].

Lemma 1.3 (Lemma 2.12 in [GGPdC21]). *Let $f, g, h \in \mathbb{Z}[x]$ satisfy $f = gh$. Then*

$$\|h\|_\infty \leq \|f\|_\infty (\|g\|_\infty + 1)^{\frac{\|h\|_0 + 1}{2}}. \tag{3}$$

While the bound given in (2) is close to being tight, in this paper we ask whether one can get an improvement if the factor g is sparse. For example, Khovanskiĭ's theory asserts that when studying real roots of polynomial equations, results analogous to Bézout's theorem can be obtained, where the number of monomials in the equations takes the place of the degree in Bézout's theorem [Kho91].

Besides being a self-motivated question, bounding the norm of cofactors of sparse polynomials has important applications in computer algebra which we discuss next.

1.1. The sparse representation

The sparse representation of polynomials is widely used in computer algebra as it is the most natural and succinct representation when polynomials are far from being "dense," that is, when most of their coefficients are zero, or, equivalently, when they are supported on a small number of monomials [vzGG13, DST93]. In this representation, a polynomial is described by a list of coefficient and degree

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

pairs that correspond to its terms with nonzero coefficients. For example, a polynomial $f \in R[x]$ over the ring R with t nonzero coefficients, $f = \sum_{i=1}^{t} c_i x^{e_i}$, is represented as $\{(c_i, e_i) \mid i = 1 \dots t\}$. Particularly interesting cases are when $R = \mathbb{Z}$ or R is a finite field. When working over the integers, the size of the sparse representation of a polynomial $f \in \mathbb{Z}[x]$, denoted $\text{size}(f)$, is

$$\text{size}(f) = \|f\|_0(\log_2 \|f\|_\infty + \log_2 \deg f),$$

where $\|f\|_0$ and $\|f\|_\infty$ are the number of nonzero coefficients in f, and the maximal coefficient of f (in absolute value), respectively.[1] This makes the sparse representation especially useful for applications involving polynomials with high degree where most of the coefficients are zero. In particular, it is used by computer algebra systems and libraries such as Maple [MP13], Mathematica [Wol99], Sage [S+08], and Singular [Sch03].

In the sparse representation, the degree could be exponentially larger than the representation size. Algorithms that run in polynomial time in terms of the sparse-representation size (i.e., number of terms, their bit complexity and the logarithm of the degree) are called sparse polynomial algorithms.

Although the basic arithmetic of sparse polynomials is fairly straightforward [Joh74], the sparse representation poses many challenges in designing efficient algorithms, and many seemingly simple problems are known to be NP-hard. For example, Plaisted proved that determining whether $x^n - 1$ divides a product of sparse polynomials (such that the size of the input is $\text{poly}(\log n)$) is NP-complete [Pla77, Pla84]. Other NP-hard problems concerning sparse polynomials include: deciding whether there exists a common divisor of two polynomials and testing whether a polynomial has a cyclotomic factor [Pla77].

The surveys of Davenport and Carette [DC09] and of Roche [Roc18] give a good picture of known results and open questions concerning sparse polynomials.

One of the long-standing open problems concerns exact divisibility of sparse polynomials. There are two versions to this problem. The decision problem asks, given two sparse polynomials f and g, to decide whether g divides f. The search problem, or the exact division problem, asks to compute the quotient polynomial f/g when it is known that g divides f.

The two problems are closely related but also differ in what we can hope to achieve. In the decision problem, the output is a single bit, allowing us to analyze the complexity in terms of the input size. Conversely, in the search (exact division) problem, the output size depends on the number of monomials in f/g, and thus may require an exponential number of bits (compared to the size of the input) to represent.

There are two quantities that affect the complexity of the exact division problem. The first, mentioned above, is the number of terms of the quotient f/g. It is easy to find examples in which f/g has exponentially many monomials. The second quantity is the height of the quotient f/g.

Prior to this work the only bounds on the height were exponential in $\deg h$, as in Equations (1),(2) and(3) (see also [Mig12]). In particular, Davenport and Carette note that even in the case where g exactly divides f, we need to perform $\Omega(\|f/g\|_0 \cdot \|g\|_0)$ operations on coefficients, and the number of bits required to represent a coefficient may be as large as $\deg f$ [DC09, Section III.B]. Therefore, in terms of the input size and $\|f/g\|_0$ the only provable bounds on the running time of the exact division algorithm were of the form

$$\Omega(\|f/g\|_0 \cdot \|g\|_0 \cdot \deg f/g). \tag{4}$$

1.2. Our results

Our main result gives a new bound on the ℓ_2-norm of f/g, for $f, g \in \mathbb{C}[x]$ such that g divides f. This result improves the classical bounds of Gel'fond [Mah62] and Mignotte [Mig74] when the factor g is

[1] As we think of $\|f\|_0$ as being considerably smaller than $\log_2 \|f\|_\infty$ and $\log_2 \deg f$, we do not pay attention to the case where bit lengths of coefficients vary.

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

sparse. In what follows we assume without loss of generality that $f(0) \neq 0$ as we can always remove powers of x that divide the polynomials without affecting their coefficients. In the general case, $\deg g$ should be replaced by $\deg g - \mathrm{ord}_0 g$ throughout.

Theorem 1.4. *Let $f, g, h \in \mathbb{C}[x]$ such that $f = gh$ and $f(0) \neq 0$. Define $L(n) = n \log n$, and let*

$$M \geq \max\left\{ \begin{array}{c} \min\{|LC(g)|, |TC(g)|\} \cdot \sqrt{e}\left(\frac{\|g\|_0}{4e}\right)^{\frac{\|g\|_0-1}{2}} (\deg g)^{\frac{\|g\|_0}{2}} \\ \max\{|LC(g)|, |TC(g)|\} \cdot \deg g \end{array} \right\}. \tag{5}$$

where $LC(g)$ and $TC(g)$ are respectively the leading coefficient and the trailing coefficient of g and e is the basis of the natural log. Then

$$\|h\|_2 \leq \frac{\sqrt{2}\,\|f\|_1}{M}\left(2\|g\|_0 \cdot L(12\|g\|_0 \deg g + 2\deg f)^2\right)^{\|g\|_0-1}. \tag{6}$$

Remark 1.5. We note that in (6) there must appear a term that inversely depends on $|\mathrm{LC}(g)|$ or on $|\mathrm{TC}(g)|$ since if $hg = f$ then for every constant c we also have $(c \cdot h) \cdot (g/c) = f$. This scales $\|h\|_2$ by a factor of c.

The following is an immediate corollary.

Corollary 1.6. *Let*

- *$f, g, h \in \mathbb{Z}[x]$ such that $f = gh$ and $f(0) \neq 0$, or*
- *$f, g, h \in \mathbb{C}[x]$ such that $f = gh$, $f(0) \neq 0$, and $|LC(g)|, |TC(g)| \geq 1$.*

Then, it holds that

$$\begin{aligned} \|h\|_2 &\leq \sqrt{\frac{\|g\|_0}{\deg g}} \cdot \|f\|_1 \cdot \left(\widetilde{O}\left(\frac{\|g\|_0^{2.5} \cdot \deg^2 g + \sqrt{\|g\|_0} \cdot \deg^2 f}{\sqrt{\deg g}}\right)\right)^{\|g\|_0-1} \\ &\leq \sqrt{\frac{\|g\|_0}{\deg g}} \cdot \|f\|_1 \cdot \left(\widetilde{O}\left(\frac{\|g\|_0^{2.5} \cdot \deg^2 f}{\sqrt{\deg g}}\right)\right)^{\|g\|_0-1}. \end{aligned}$$

In terms of bit representation size we have

$$\log_2 \|h\|_\infty \leq \log_2 \|h\|_2 \leq \log_2 \|f\|_\infty + O\big(\|g\|_0 \cdot \log_2 \deg f\big). \tag{7}$$

If all we know is that one among $\mathrm{LC}(g)$, $\mathrm{TC}(g)$ is large then, using the estimate $\mathrm{M} \geq \max\{\mathrm{LC}(g), \mathrm{TC}(g)\} \cdot \deg g$, we obtain the following bound.

Corollary 1.7. *Let $f, g \in \mathbb{C}[x]$ such that $f = gh$ and g is monic. Then it holds that*

$$\|h\|_2 \leq \frac{\|f\|_1}{\deg g} \cdot \widetilde{O}\left(\|g\|_0^3 \deg^2 f\right)^{\|g\|_0-1}.$$

Unlike the bounds in Equations (1), (2) and (3), our bound on the height of h is not exponential in the degree or number of coefficients of h, but rather in the sparsity of the factor g, which for sparse polynomials may be exponentially smaller. Thus, when $\|g\|_0$ is small, this gives an exponential improvement over the bounds of Gel'fond and Mignotte (Theorems 1.1, 1.2). In addition, Theorem 1.4 gives an exponential separation between exact and nonexact division since $\log_2 \|h\|_\infty$ can be as large as $\Omega(\deg f \cdot \log_2 \|g\|_\infty)$ when allowing nonzero remainder. As noted in [DC09, Section III.A], for division with remainder, this coefficient growth is intrinsic.

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

Observation 1.8. Let $f, g \in \mathbb{C}[x]$ and let q, r be the quotient and the remainder of f divided by g, respectively. For any $\|f\|_\infty$, $\|g\|_\infty$, $\deg f$, and $\deg g$, there exists f and g of sparsity 2 such that $\|r\|_\infty = \|f\|_\infty \|g\|_\infty^{\deg f - \deg g + 1}$.

Proof. Let $d_1, d_2 \in \mathbb{N}$ and $a \in \mathbb{C}$ with $|a| \geq 1$. We conclude the claim by noting that

$$x^{d_1} \bmod (x^{d_2+1} - ax^{d_2}) = a^{d_1 - d_2} x^{d_2}. \qquad \square$$

Theorem 1.4 also provides the following guarantee regarding the performance of the polynomial division algorithm in the exact case.

Theorem 1.9. *When the division is exact, the bit complexity*[2] *of the (deterministic) polynomial division algorithm for polynomials $f, g \in \mathbb{Z}[x]$ is*

$$\widetilde{O}(\|f/g\|_0 \cdot \|g\|_0 \cdot (\log \|g\|_\infty + \log \|f\|_\infty + \|g\|_0 \log \deg f)).$$

Note that when $\|g\|_0 = \mathsf{poly}(\log \|f/g\|_0)$ or $\|g\|_0 = \mathsf{poly}(\log(\|g\|_\infty \cdot \|f\|_\infty \cdot \deg f))$, the bound in Theorem 1.9 is $\widetilde{O}(\|f/g\|_0(\log \deg f + \log H))$ where H is an upper bound on the heights of f and g.

Finally, we recall the following result of Giorgi et al. [GGPdCR22, Theorem 1.3], specialized to the case of univariate polynomials.

Theorem 1.10 [GGPdCR22, Theorem 1.3]. *There exists a Monte Carlo randomized algorithm that, given two sparse polynomials $f, g \in \mathbb{Z}[x]$ such that g divides f, and a bound T on the sparsity of the quotient f/g, computes the sparse representation of f/g with probability at least $2/3$. The algorithm requires*

$$\widetilde{O}((\|f\|_0 + \|g\|_0 + T)\,(\log \deg f + \log H))$$

bit operations, where H is an upper bound on the heights of the polynomials f, g, and f/g.

In combination with Theorem 1.4, we derive the corollary below.

Corollary 1.11. *There exists a randomized algorithm that, given two sparse polynomials $f, g \in \mathbb{Z}[x]$, such that g divides f, the algorithm outputs the quotient polynomial f/g, with probability at least $2/3$. The running time of the algorithm is*

$$\widetilde{O}((\|f\|_0 + \|g\|_0 + \|f/g\|_0) \cdot (\log \|g\|_\infty + \log \|f\|_\infty + \|g\|_0 \log \deg f)).$$

While Corollary 1.11 speaks about a randomized algorithm and not a deterministic one as in subsection 1.9, it has the advantage of having the term $(\|f\|_0 + \|g\|_0 + \|f/g\|_0)$, whereas Theorem 1.9 has $\|f/g\|_0 \cdot \|g\|_0$, which in the relevant case is larger by a factor of $\Omega(\|g\|_0)$.

1.3. Proof outline and comparison to [NS24]

We explain the ideas behind the proof of Theorem 1.4 as all the other results mentioned above are simple corollaries of it. We first discuss the overall idea that led to the result of [NS24] and then the improvement obtained in this paper.

The proof of Theorem 1.4 starts, as in [GR11, Theorem 2.9], by considering the discrete Fourier transform of the coefficient vector of h. Parseval's identity gives

$$\|h\|_2^2 = \frac{1}{p} \sum_{0 \leq i < p} \left|h(\omega^i)\right|^2, \tag{8}$$

[2]Bit complexity measures the running time of an algorithm as the total number of elementary operations on bits.

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

where ω is a primitive p-th root of unity for a prime $p > \deg h$. Hence, $\|h\|_2 \le |h(\theta)|$ for some p-th root of unity θ. Since $|g(\theta)| \cdot |h(\theta)| = |f(\theta)| \le \|f\|_1$,

$$\|h\|_2 \le |h(\theta)| \le \frac{\|f\|_1}{|g(\theta)|}.$$

Hence, it suffices to lower bound the values of g at roots of unity in order to upper bound $\|h\|_2$. As g may vanish at 1, the above approach cannot be applied directly. To overcome this, we observe that if $p > 2\deg f$ then the contribution of $h(1)$ to the overall sum in (8) is not too large. Consequently, we can upper bound $\|h\|_2$ by a similar expression, except that now θ is a primitive root of unity.

Consider the restriction of g to the unit circle, $\tilde{g}(x) = g(e^{ix}) : [0, 2\pi) \to \mathbb{C}$. We prove by induction on the sparsity of g that outside the neighborhood of a small set of bad points $B(g) \subset [0, 2\pi)$ (intuitively, these are zeros of g and points at which g' attains unusually small values), $g(e^{ix})$ attains large values. Indeed, when $\deg g = 1$ this is relatively simple to show as g must be of the form $x - \alpha$ (after rescaling) and since primitive roots of unity of relatively prime orders are somewhat far from each other, we can find many primes p so that the values of g on primitive p-th roots of unity are not too small.

For higher degrees, we note that if the derivative of g is not small in a large enough region then g is large on most of that region. Thus, by moving further away from the bad set for the derivative of g, $B(g')$ in which g' attains unusually small values, we get that on this set g always attains large values. We then prove by a simple pigeonhole principle that there exists a prime p such that all primitive p-th roots of unity are far away from the bad set and conclude the result. This is the approach behind the proof of the main result in [NS24].

Theorem 1.12 [NS24, Theorem 1.5]. *Let $f, g \in \mathbb{C}[x]$ such that $f = gh$ and g is monic. Then it holds that*

$$\|h\|_2 \le \|f\|_1 \cdot \widetilde{O}\left(\|g\|_0^3 \deg^2 f\right)^{\|g\|_0 - 1}.$$

Note that this is similar to Corollary 1.6, except that it is larger by a factor of $\deg g$. We next explain how to regain that factor and more strongly, the additional factor of M appearing in Theorem 1.4.

Improvement over [NS24].
To get the improved result, we note that in the sketch above, every time that we take a derivative of g, its leading coefficient grows by a factor equivalent to the degree. Intuitively, this should help increase the value of the derivative, and this is the source of the improvement. Note that for linear factors the proof considered monic polynomials, and this is also the inductive assumption that we make. Thus, the coefficient of the top monomial will contribute a multiplicative factor to the value of g, when we make g monic. This is sufficient to obtain the extra factor of $\deg g$ in Corollary 1.6 compared to [NS24, Theorem 1.5] (see Theorem 1.12).

One may notice, however, that after taking derivatives we need to remove all powers of x that divide the polynomial, so that the next derivative will reduce the sparsity. This can cause an abrupt drop in the degree, which will not give us the saving of roughly $(\deg g)^{O(\|g\|_0)}$ (see (5)). This can happen only if most of the monomials have degrees close to $\deg g$. In this case however, if we consider $g_{\mathrm{rev}}(x) = x^{\deg g} g(1/x)$, then this makes most of the monomials of degrees that are considerably smaller than the top degree, thus allowing us to gain large factors in every derivative. On the other hand, once we move to g_{rev}, it may not be monic, and in fact, it may have a small leading term which will *cost* us a large factor in the bound. Balancing these two cases leads to the bound of (5), and is the main technical part of subsection 3.4.

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

2. Preliminaries

In this section, we set our notation, and state some basic facts that we shall later use.

2.1. General notation

Let R be a unique factorization domain (UFD) and let $g, f \in R[x]$ be two polynomials. We say that g divides f, and denote it with $g \mid f$, when there is a polynomial $h \in R[x]$ such that $g \cdot h = f$. We denote $g \nmid f$ when this is not the case.

Let $f = \sum_i f_i x^i$,. We shall use the following notation: $\|f\|_0$ denotes the sparsity of f (the number of nonzero f_i's); $\|f\|_p = (\sum_i |f_i|^p)^{1/p}$; if $R \subseteq \mathbb{C}$ then $\|f\|_\infty = \max_i |f_i|$ is the height of f; $\mathrm{ord}_\alpha f$ denotes the multiplicity of a root α in f, in particular, $\mathrm{ord}_0 f = \max\left\{i : x^i \mid f\right\}$; $\mathrm{LC}(f) \in R$ denotes the leading coefficient in f, that is, the coefficient of the highest degree term in f. Similarly, $\mathrm{TC}(f) \in R$, the trailing coefficient of f, denotes the coefficient of the smallest degree term in f.

For a polynomial g we denote $g_0 \triangleq (g/x^{\mathrm{ord}_0 g})$ and $g_{\mathrm{rev}} \triangleq x^{\deg g} \cdot g(1/x)$. For example, if $g = \sum_{i=1}^s c_i \cdot x^{n_i}$ then $g_0 = \sum_{i=1}^s c_i \cdot x^{n_i - n_1}$ and $g_{\mathrm{rev}} = \sum_{i=1}^s c_i \cdot x^{n_s - n_i}$. Observe that $(g_{\mathrm{rev}})_0 = (g_0)_{\mathrm{rev}}$ and that $g_0 = (g_{\mathrm{rev}})_{\mathrm{rev}}$.

We denote the derivative of g by g'.

For any real or complex-valued function f, we define $V(f)$ to be the set of zeros of f, that is, $V(f) = \{\alpha \mid f(\alpha) = 0\}$, over the corresponding field. For a complex-valued function f we denote by $\Re f$ and $\Im f$ the real and imaginary parts of f, respectively.

For an integer $k \in \mathbb{N}$, we denote $[k] = \{1, \ldots, k\}$. Throughout this paper, log refers to the natural logarithm. We use π to denote the mathematical constant, while $\pi(\cdot)$ refers to the prime counting function.

2.2. Useful facts

The following facts are simple and well known but for completeness we provide their proof.

Claim 2.1 (Discrete Parseval's Identity). *Let $f \in \mathbb{C}[x]$ and let $n > \deg f$. Then,*

$$\|h\|_2^2 = \frac{1}{n} \sum_{0 \le i < n} \left|h(\omega^i)\right|^2$$

where $\omega \in \mathbb{C}$ is a primitive n-th root of unity.

Proof. Recall that the $n \times n$ Discrete Fourier Transform (DFT) matrix is

$$\frac{1}{\sqrt{n}} \left(\omega^{jk}\right)_{0 \le j,k < n}$$

where $\omega \in \mathbb{C}$ is a primitive n-th root of unity. Since the DFT matrix is unitary, applying it to the coefficient vector of h we conclude that

$$\|h\|_2^2 = \sum_{0 \le i \le \deg h} |h_i|^2 = \frac{1}{n} \sum_{0 \le i < n} \left|h(\omega^i)\right|^2. \qquad \square$$

Claim 2.2. Let $f \in \mathbb{C}[x]$. Then $\|f\|_2 \le \|f\|_1 \le \sqrt{\deg f + 1}\|f\|_2$.

Proof. The first inequality is immediate from definition and the second follows from the Cauchy-Schwartz inequality. $\square$

Claim 2.3. Let $f \in \mathbb{C}[x]$ and let $x \in \mathbb{C}$ such that $|x| = 1$. Then $|f(x)| \le \|f\|_1$.

Proof. This is a consequence of the triangle inequality. $\square$

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

Claim 2.4. For all $0 \le t < 1$,

$$(1-t) \ge e^{-\frac{t}{1-t}}$$

Proof. Take the logarithm of both side and observe that the derivative is nonnegative (and that at $t = 0$ there is an equality). □

2.2.1. Complex analysis

For general facts about complex analysis, see [Ahl21, Tit02]. For the definition of harmonic functions, see [Ahl21, Chapter 4.6] and [ABW13].

Claim 2.5. Let $f : \mathbb{C} \to \mathbb{R}$ be a harmonic function. If $f(\omega) = 0$ for every ω such that $|\omega| = 1$, then $f = 0$.

We give the proof of this well known fact for completeness.

Proof. Let,

$$D = \{\omega \in \mathbb{C} : |\omega| \le 1\}$$

be the unit disc. From the Maximum Modulus Principle for harmonic functions (see [Ahl21, Chapter 4.6.2, Theorem 21]) and compactness of D we get that $f(\omega) = 0$ for all $\omega \in D$. It follows that f must vanish everywhere [ABW13, Theorem 1.27]. □

Claim 2.6. Let $f \in \mathbb{C}[x]$ be a polynomial. If $\Re f$ (or equivalently, $\Im f$, $\Re f + \Im f$ or $\Re f - \Im f$) is nonzero, then it has at most $2 \deg f$ roots on the unit circle.

Proof. Let $S \subseteq \mathbb{C}$ be the set of roots of $\Re f$ on the unit circle. We can write $\Re f(x+iy) = u(x,y)$ where $u : \mathbb{R}^2 \to \mathbb{R}$ is a bi-variate polynomial of total degree $\deg f$. Hence,

$$|S| = |V(u) \cap V(x^2 + y^2 - 1)|.$$

Since f is analytic, $\Re f$ is harmonic. Claim 2.5 implies that $\Re f$ does not vanish on the unit circle. Thus, from the irreducibility of $x^2 + y^2 - 1$, we deduce that $V(u)$ and $V(x^2 + y^2 - 1)$ have no component in common. From Bézout's theorem (see, e.g., [Har92, Theorem 18.3]) we conclude that

$$|S| \le \deg u \cdot \deg (x^2 + y^2 - 1) = 2 \deg f.$$ □

Claim 2.7. If $|x - y| \le \frac{1}{2}$, then $\left|e^{2\pi i x} - e^{2\pi i y}\right| \ge 4|x - y|$.

Proof. Since

$$\left|e^{2\pi i x} - e^{2\pi i y}\right| = \left|e^{2\pi i (x-y)} - 1\right|,$$

we may assume without loss of generality that $y = 0$. Let $t = 2\pi x$. Since $|x| \le \frac{1}{2}$, we have $|t| \le \pi$. If $|t| \le \pi/2$, then

$$\left|e^{it} - 1\right| = \sqrt{(1 - \cos(t))^2 + \sin^2(t)} \ge |\sin(t)| \ge \tfrac{2}{\pi}|t|,$$

where the last inequality follows from the fact that $\sin(t)$ is concave on $[0, \pi]$ and convex on $[-\pi, 0]$. If $\pi/2 \le |t| \le \pi$, then

$$\left|e^{it} - 1\right| = \sqrt{(1 - \cos(t))^2 + \sin^2(t)} \ge |1 - \cos(t)| \ge \tfrac{2}{\pi}|t|,$$

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

where the last inequality follows from the fact that $1-\cos(t)$ is positive and concave on both $[\frac{\pi}{2}, \frac{3\pi}{2}]$ and $[-\frac{3\pi}{2}, -\frac{\pi}{2}]$. Substituting $t = 2\pi x$, we obtain

$$\left|e^{2\pi i x} - 1\right| \geq \frac{2}{\pi} \cdot 2\pi|x| = 4|x|. \qquad \square$$

2.2.2. Number theory

Fact 2.8 [RS62, Corollary 1]. Let $\pi(n) = |\{p \leq n : p \text{ is prime}\}|$ be the prime-counting function. Then $\pi(n) \geq \frac{n}{\log n}$ for $n \geq 17$.

The following fact is a strengthening of Bertrand's postulate by Ramanujan.

Fact 2.9 [Ram19]. Let $n \in \mathbb{N}$ such that $n \geq 6$. Then, there exist at least two primes in the interval $(n, 2n]$.

3. A Bound on the ℓ_2-norm of the cofactor polynomial

In this section, we prove our main result, Theorem 1.4. We first give the main two claims that are required for the proof and show how they imply the theorem, and then prove the claims in the next sections. To state the claims we require some definitions.

Definition 3.1. For a polynomial $g(x) = \sum_{i=1}^{s} c_i x^{n_i}$ with $n_1 < n_2 < \ldots < n_s$ and $\prod_{i=1}^{s} c_i \neq 0$ we define $d(g) \triangleq \prod_{i=1}^{s-1}(n_s - n_i)$. When $s = 1$ we set $d(g) = 1$.

Intuitively, $d(g)$ captures the coefficient growth when we take derivatives of g (and clear factors of the form x^k).

To obtain an improved bound over the results in [NS24], we introduce the function below.

Definition 3.2. For a polynomial $g \in \mathbb{C}[x]$ we denote

$$\mathrm{M} \triangleq \max\{|\mathrm{LC}(g)| \cdot d(g), |\mathrm{TC}(g)| \cdot d(g_{\mathrm{rev}})\}.$$

We next express our upper bound on the norm of the cofactor in terms of M.

Theorem 3.3. *Let $f, g, h \in \mathbb{C}[x]$ such that $f = gh$. Denote $L(n) = n \log n$. Then,*

$$\|h\|_2 \leq \frac{\sqrt{2}\|f\|_1}{M}\left(2\|g\|_0 \cdot L(12\|g\|_0(\deg g - ord_0 g) + 2\deg f)^2\right)^{\|g\|_0 - 1}.$$

We prove Theorem 3.3 in subsection 3.3. We now state our upper bound on M, which is the source of the improvement over [NS24].

Lemma 3.4. *Let $g \in \mathbb{C}[x]$. Let $M = \max\{|LC(g)| \cdot d(g), |TC(g)| \cdot d(g_{rev})\}$. Then,*

$$M \geq \max\left\{\begin{array}{c} \min\{|LC(g)|, |TC(g)|\} \cdot \sqrt{e}\left(\frac{\|g\|_0}{4e}\right)^{\frac{\|g\|_0 - 1}{2}} (\deg g - ord_0 g)^{\frac{\|g\|_0}{2}} \\ \max\{|LC(g)|, |TC(g)|\} \cdot (\deg g - ord_0 g) \end{array}\right\}.$$

We prove this result in subsection 3.4. Given the bounds above we can prove Theorem 1.4 and Corollary 1.6. We recall their statements.

Theorem 1.4. *Let $f, g, h \in \mathbb{C}[x]$ such that $f = gh$ and $f(0) \neq 0$. Define $L(n) = n \log n$, and let*

$$M \geq \max\left\{\begin{array}{c} \min\{|LC(g)|, |TC(g)|\} \cdot \sqrt{e}\left(\frac{\|g\|_0}{4e}\right)^{\frac{\|g\|_0 - 1}{2}} (\deg g)^{\frac{\|g\|_0}{2}} \\ \max\{|LC(g)|, |TC(g)|\} \cdot \deg g \end{array}\right\}.$$

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

where $LC(g)$ and $TC(g)$ are respectively the leading coefficient and the trailing coefficient of g and e is the basis of the natural log. Then

$$\|h\|_2 \le \frac{\sqrt{2}\,\|f\|_1}{M}\left(2\|g\|_0 \cdot L(12\|g\|_0 \deg g + 2\deg f)^2\right)^{\|g\|_0-1}.$$

Proof of Theorem 1.4. This is exactly the statement of Theorem 3.3 with the lower bound on M established in Lemma 3.4. □

Corollary 1.6. *Let*

- $f, g, h \in \mathbb{Z}[x]$ *such that* $f = gh$ *and* $f(0) \neq 0$, *or*
- $f, g, h \in \mathbb{C}[x]$ *such that* $f = gh$, $f(0) \neq 0$, *and* $|LC(g)|, |TC(g)| \ge 1$.

Then, it holds that

$$\begin{aligned}\|h\|_2 &\le \sqrt{\frac{\|g\|_0}{\deg g}} \cdot \|f\|_1 \cdot \left(\widetilde{O}\left(\frac{\|g\|_0^{2.5} \cdot \deg^2 g + \sqrt{\|g\|_0} \cdot \deg^2 f}{\sqrt{\deg g}}\right)\right)^{\|g\|_0-1} \\ &\le \sqrt{\frac{\|g\|_0}{\deg g}} \cdot \|f\|_1 \cdot \left(\widetilde{O}\left(\frac{\|g\|_0^{2.5} \cdot \deg^2 f}{\sqrt{\deg g}}\right)\right)^{\|g\|_0-1}.\end{aligned}$$

In terms of bit representation size we have

$$\log_2 \|h\|_\infty \le \log_2 \|h\|_2 \le \log_2 \|f\|_\infty + O\left(\|g\|_0 \cdot \log_2 \deg f\right).$$

Proof of Corollary 1.6. By Theorem 3.3

$$\|h\|_2 \le \frac{\sqrt{2}\|f\|_1}{\mathrm{M}}\left(2\|g\|_0 \cdot L(12\|g\|_0(\deg g - \mathrm{ord}_0 g) + 2\deg f)^2\right)^{\|g\|_0-1}, \tag{9}$$

for $L(n) = n\log(n)$. As $g(0) \neq 0$, $\mathrm{ord}_0 g = 0$. Hence,

$$\|g\|_0 L(12\|g\|_0(\deg g - \mathrm{ord}_0 g) + 2\deg f)^2 = \tilde{O}\left(\|g\|_0^3 \deg^2 g + \|g\|_0 \deg^2 f\right). \tag{10}$$

Either of the assumptions in the statement implies that $\mathrm{LC}(g), \mathrm{TC}(g) \ge 1$. Thus, Lemma 3.4 gives

$$\mathrm{M} \ge \sqrt{e}\left(\frac{\|g\|_0}{4e}\right)^{\frac{\|g\|_0-1}{2}} \cdot (\deg g)^{\frac{\|g\|_0}{2}}. \tag{11}$$

Substituting (10) and (11) into (9) we obtain

$$\begin{aligned}\|h\|_2 &\le \frac{\sqrt{2}\|f\|_1}{\mathrm{M}}\left(2\|g\|_0 \cdot L(12\|g\|_0(\deg g - \mathrm{ord}_0 g) + 2\deg f)^2\right)^{\|g\|_0-1} \\ &\le \frac{\sqrt{2}\|f\|_1\left(\tilde{O}\left(\|g\|_0^3 \deg^2 g + \|g\|_0 \deg^2 f\right)\right)^{\|g\|_0-1}}{\sqrt{e}\left(\frac{\|g\|_0}{4e}\right)^{\frac{\|g\|_0-1}{2}} \cdot (\deg g)^{\frac{\|g\|_0}{2}}}\end{aligned}$$

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

$$= \frac{\|f\|_1}{\sqrt{\deg g}} \left(\frac{\tilde{O}\left(\|g\|_0^3 \deg^2 g + \|g\|_0 \deg^2 f \right)}{\sqrt{\|g\|_0 \deg g}} \right)^{\|g\|_0 - 1}$$

$$= \frac{\|f\|_1}{\sqrt{\deg g}} \left(\tilde{O}\left(\frac{\|g\|_0^{2.5} \deg^2 g + \sqrt{\|g\|_0} \deg^2 f}{\sqrt{\deg g}} \right) \right)^{\|g\|_0 - 1}. \qquad \square$$

The remainder of this section is devoted to proving Theorem 3.3 and Lemma 3.4.

3.1. Evaluations on the unit circle

To prove Theorem 3.3 we use a well known relation between the norm of a polynomial and its values at roots of unity of high orders.

The following lemma uses simple Fourier analysis to bound the norm of the quotient polynomial in a similar fashion to Theorem 2.9 of [GR11].

Lemma 3.5. *Let $f, g, h \in \mathbb{C}[x]$ such that $f = gh$. Then,*

$$\|h\|_2 \leq \sqrt{2} \|f\|_1 \cdot \max_{\substack{1 \neq \omega \in \mathbb{C} \\ \omega^p = 1}} \frac{1}{|g(\omega)|}$$

where p is a prime such that $p > 2 \deg f$ and g does not vanish at any primitive root of unity of order p.

Proof. When g is constant the statement is trivial (see Claim 2.2), so we assume $\deg g > 0$. From Parseval's identity (Claim 2.1) we conclude $\|h\|_2^2 = \frac{1}{p} \sum_{0 \leq i < p} \left| h(\omega^i) \right|^2$, where ω is a primitive p-th root of unity. Claim 2.2 implies that

$$\left| h(\omega^0) \right|^2 = |h(1)|^2 \leq \|h\|_1^2 \leq \|h\|_2^2 (\deg h + 1) \leq \|h\|_2^2 \deg f.$$

By the choice of $p > 2 \deg f$, it follows that

$$\frac{1}{p} \sum_{0 < i < p} \left| h(\omega^i) \right|^2 = \|h\|_2^2 - \frac{\left| h(\omega^0) \right|^2}{p} \geq \|h\|_2^2 - \frac{\deg f}{p} \|h\|_2^2 > \frac{1}{2} \|h\|_2^2.$$

In other words, the average value of $\left| h(\omega^i) \right|^2$ for $0 < i < p$ is larger than $\frac{1}{2} \|h\|_2^2$. Hence, there exists a p-th root of unity $\theta \neq 1$ such that

$$\|h\|_2 < \sqrt{2} |h(\theta)|.$$

Since $f = gh$ we conclude that $|f(\theta)| = |g(\theta)||h(\theta)|$. By Claim 2.3, $|f(\theta)| \leq \|f\|_1$. Hence,

$$\|h\|_2 < \sqrt{2} |h(\theta)| = \sqrt{2} \frac{|f(\theta)|}{|g(\theta)|} \leq \sqrt{2} \frac{\|f\|_1}{|g(\theta)|}.$$

By taking the maximum over all p-th roots of unity $\omega \neq 1$ we get

$$\|h\|_2 \leq \sqrt{2} \|f\|_1 \cdot \max_{\substack{1 \neq \omega \in \mathbb{C} \\ \omega^p = 1}} \frac{1}{|g(\omega)|}$$

as claimed. $\square$

Lemma 3.5 shows that in order to upper bound $\|h\|_2$, we have to *lower bound* the value of g at primitive roots of unity of *some* prime order $p > 2 \deg f$.

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

To build intuition for the proof of Theorem 3.3 we next consider the case where g is a simple linear factor of f, $g(x) = x - \alpha$. The general case is handled in subsection 3.3.

3.2. Linear factors

We first consider the special case where g is linear. We show that there exists a point $\tilde{\alpha}$ on the unit circle such that g attains large values on any point on the unit circle that is far enough from $\tilde{\alpha}$. To conclude, we prove that there exists a prime p such that every p-th root of unity is far from $\tilde{\alpha}$.

Lemma 3.6. *Let $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$. Then, any set of $k+1$ prime numbers P contains $p \in P$ such that $|a/p - \alpha_i| > \frac{1}{2(\max P)^2}$ for every integer $0 < |a| < p$ and $i \in [k]$.*

Proof. Assume for the sake of contradiction that the statement is false. Thus, for every $p \in P$ there exists $i \in [k]$ such that $|a/p - \alpha_i| \leq \frac{1}{2(\max P)^2}$ for some $0 < |a| < p$. By the Pigeonhole Principle, there exists $i \in [k]$ such that for two different primes $p, q \in P$, $0 < |a| < p$ and $0 < |b| < q$ we have

$$|a/p - \alpha_i| \leq \frac{1}{2(\max P)^2} \quad \text{and} \quad |b/q - \alpha_i| \leq \frac{1}{2(\max P)^2}.$$

This, however, leads to a contradiction

$$\frac{1}{(\max P)^2} \geq \left|\frac{a}{p} - \alpha_i\right| + \left|\alpha_i - \frac{b}{q}\right| \geq \left|\frac{a}{p} - \frac{b}{q}\right| = \left|\frac{ap - bq}{pq}\right| \geq 1/pq > \frac{1}{(\max P)^2}. \qquad \square$$

We use this lemma to claim that for any two different primes p_1 and p_2, any point on the unit circle is somewhat far from either all primitive roots of unity of order p_1 or from those of order p_2.

Lemma 3.7. *Let $\alpha \in \mathbb{C}$, and let $p_1, p_2 \in \mathbb{N}$ be two primes. Then for either $p = p_1$ or $p = p_2$ it holds that $|\omega - \alpha| > \frac{1}{(\max\{p_1,p_2\})^2}$ for any primitive p-th root of unity $\omega \neq 1$.*

Proof. First, observe that if α is $\frac{1}{(\max\{p_1,p_2\})^2}$-far from any point on the unit circle, then we are done. So, assume that there exists a point $\tilde{\alpha}$ on the unit circle such that $|\alpha - \tilde{\alpha}| < \frac{1}{(\max\{p_1,p_2\})^2}$. Let $c \in [-\frac{1}{2}, \frac{1}{2})$ such that $\tilde{\alpha} = e^{2\pi i c}$. By Lemma 3.6 with $k = 1$ and $\alpha_1 = c$ either $p = p_1$ or $p = p_2$ satisfies

$$\left|\frac{a}{p} - c\right| > \frac{1}{2(\max\{p_1, p_2\})^2},$$

for any integer $0 < |a| < p$. Let $\omega \neq 1$ be any primitive p-th root of unity. Let $a \in \mathbb{Z}$, $0 < |a| < p$, such that $\omega = e^{2\pi i \frac{a}{p}}$. By the periodicity of $2\pi i x$, we can choose a to satisfy $\left|\frac{a}{p} - c\right| \leq \frac{1}{2}$. By Claim 2.7 it holds that

$$|\omega - \tilde{\alpha}| = \left|e^{2\pi i \frac{a}{p}} - e^{2\pi i c}\right| \geq 4\left|\frac{a}{p} - c\right| > \frac{2}{(\max\{p_1, p_2\})^2}.$$

The triangle inequality implies

$$|\omega - \alpha| \geq |\omega - \tilde{\alpha}| - |\tilde{\alpha} - \alpha| > \frac{1}{(\max\{p_1, p_2\})^2}. \qquad \square$$

The claim about the norm of the cofactor of a linear factor now follows easily.

Proposition 3.8. *Let $f \in \mathbb{C}[x]$ with a root α. Then*

$$\|f/(x - \alpha)\|_2 \leq 16\sqrt{2}\|f\|_1 \deg^2 f < 23\|f\|_1 \deg^2 f.$$

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

Proof. Lemma 3.5 applied to $g = (x - \alpha)$ and $h = f/g$ implies that

$$\|f/(x-\alpha)\|_2 \le \sqrt{2}\|f\|_1 \cdot \max_{\substack{1 \ne \omega \in \mathbb{C} \\ \omega^p = 1}} \frac{1}{|\omega - \alpha|}, \tag{12}$$

for any prime p satisfying $p > 2\deg f$ such that α is not a primitive root of unity of order p. By Fact 2.9, if $\deg f \ge 2$ then the interval $(2\deg f, 4\deg f]$ contains at least two primes[3] p_1, p_2. Lemma 3.7 guarantees that for either $p = p_1$ or $p = p_2$ it holds that the distance of α from any primitive p-th root of unity is larger than $\frac{1}{(\max\{p_1,p_2\})^2} \ge \frac{1}{(4\deg f)^2}$. Hence,

$$\|f/(x-\alpha)\|_2 \le \sqrt{2}\|f\|_1 \cdot \max_{\substack{1 \ne \omega \in \mathbb{C} \\ \omega^p = 1}} \frac{1}{|\omega - \alpha|} \le \sqrt{2}\|f\|_1 \cdot (4\deg f)^2 < 23\|f\|_1 \deg^2 f,$$

as claimed □

3.3. Sparse factors

In this section we prove Theorem 3.3. As discussed in subsection 3.1, we do so by giving a lower bound on the value of g at suitable roots of unity. Similarly to the proof of Proposition 3.8, we will show that g attains large values everywhere, with the possible exception of a small neighborhood of a small number of points. We achieve this using induction on $\|g\|_0$.

We start with two simple claims.

Claim 3.9. Let $f : \mathbb{R} \to \mathbb{R}$ be a continuously differentiable function, and $\delta > 0$. Let $I = [a, b]$ be an interval in which both f and f' do not change sign. That is, each of them is either nonnegative or nonpositive in I. Then, $|f(\beta)| \ge \delta \min_{\alpha \in I} |f'(\alpha)|$ for every $\beta \in [a + \delta, b - \delta]$.

Proof. If $b - a < 2\delta$ there is nothing to prove. Assume without loss of generality that $f \ge 0$ in I, otherwise analyze $-f$. If $f' \ge 0$ in I, then f is nondecreasing in I and so for every $\beta \in [a + \delta, b - \delta]$ it holds that

$$f(\beta) \ge f(\beta) - f(a) = \int_a^\beta f'(y)dy \ge (\beta - a) \min_{\alpha \in I} f'(\alpha) \ge \delta \min_{\alpha \in I} |f'(\alpha)|.$$

Similarly, if $f' \le 0$ in I, then for every $\beta \in [a + \delta, b - \delta]$ it holds that

$$f(\beta) \ge f(\beta) - f(b) = \int_\beta^b -f'(y)dy \ge (b - \beta) \min_{\alpha \in I} |f'(\alpha)| \ge \delta \min_{\alpha \in I} |f'(\alpha)|,$$

as claimed. □

Claim 3.10. Let $f : \mathbb{R} \to \mathbb{C}$ be a continuously differentiable function, $\delta > 0$ and denote $f_1 = \Re f$, $f_2 = \Im f$. Let $I = [a, b]$ be an interval in which each function among $f_1, f_1', f_2, f_2', f_1' - f_2'$ and $f_1' + f_2'$ is either nonnegative or nonpositive. Then, $|f(\beta)| \ge \frac{\delta}{\sqrt{2}} \min_{\alpha \in I} |f'(\alpha)|$ for every $\beta \in [a + \delta, b - \delta]$.

Proof. Our assumption implies that any of the four functions $\pm f_1' \pm f_2'$ has fixed sign in I. Since this also holds for f_1' and f_2' we conclude that $\left|f_1'\right| - \left|f_2'\right|$, which is equal to one of these four functions, is either nonnegative or nonpositive in I, as well. Without loss of generality assume $\left|f_1'\right| \ge \left|f_2'\right|$ in I. For every $\beta \in I$, $f'(\beta) = f_1'(\beta) + i \cdot f_2'(\beta)$. Hence,

$$2\left|f_1'(\beta)\right|^2 \ge \left|f_1'(\beta)\right|^2 + \left|f_2'(\beta)\right|^2 = |f'(\beta)|^2 \ge \min_{\alpha \in I} |f'(\alpha)|^2.$$

Thus, $\left|f_1'(\beta)\right| \ge \frac{1}{\sqrt{2}} \min_{\alpha \in I} |f'(\alpha)|$ for every $\beta \in I$. The result follows by Claim 3.9 and the fact that $|f(\beta)| \ge |f_1(\beta)|$. □

[3]Fact 2.9 only gives $\deg f \ge 3$ but the interval $(4, 8]$ also contains two primes (we avoid the problematic interval $(5, 10]$).

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

In what comes next, we say that two points α and β are δ-far from each other if $|\alpha - \beta| \geq \delta$. Similarly, we say that a point is δ-far from a set S if it is δ-far from every point in S.

We next prove our main lemma that shows that with the exception of a small neighborhood of a small number of points, a sparse polynomial obtains not too small values on the unit circle.

Lemma 3.11. *Let $g \in \mathbb{C}[x]$ be a monic polynomial. Then, there exists a set $B(g) \subseteq [0, 2\pi)$, satisfying $|B(g)| \leq 12(\|g\|_0 - 1) \cdot (\deg g - ord_0 g)$, such that for every $\delta > 0$, and every $\alpha \in [0, 2\pi)$ which is $(\|g\|_0 - 1)\delta$-far from $B(g)$, it holds that $\left|g(e^{i\alpha})\right| \geq d(g)\left(\frac{\delta}{\sqrt{2}}\right)^{\|g\|_0 - 1}$.*

Proof. We prove the lemma by induction on $s = \|g\|_0$. The claim holds for $s = 1$ since clearly $|g(e^{i\alpha})| = 1$ for any α, when $g(x) = x^m$.

For the inductive step, suppose that the claim holds for s, and let $g \in \mathbb{C}[x]$ be of sparsity $s + 1$. Since $\left|(g/x^{\mathrm{ord}_0 g})(\omega)\right| = |g(\omega)|$ for every ω on the unit circle we can consider $g_0 = (g/x^{\mathrm{ord}_0 g})$ instead of g, which is of degree $\deg g_0 = \deg g - \mathrm{ord}_0 g$.

Let $f : [0, 2\pi) \to \mathbb{C}$ be defined as $f(x) = g_0(e^{ix})$. Denote with

$$\hat{g}(x) = \frac{g_0'(x)}{\deg g_0},$$

the monic polynomial which is a scalar multiple of g_0'. By Claim 3.15, $d(\hat{g}) = d(g_0')$. Let

$$\begin{aligned} H &= \{\Re f, \Re f', \Im f, \Im f', \Re f' - \Im f', \Re f' + \Im f'\} \text{ and} \\ B(g) &= B(\hat{g}) \cup \{\beta \in [0, 2\pi) : h(\beta) = 0 \text{ for a nonzero } h \in H\}. \end{aligned} \tag{13}$$

By Claim 2.6, each nonzero function in H has at most $2 \deg g_0$ zeros in $[0, 2\pi)$. Since $\hat{g}(x)$ is monic and has sparsity s, we conclude by the inductive assumption that

$$|B(g)| \leq 12(s - 1) \deg \hat{g} + 12 \deg g_0 < 12s \deg g_0.$$

Let $I = [a, b] \subseteq [0, 2\pi)$ be an interval that is $(s - 1)\delta$-far from $B(g)$. By the definition of $B(g)$, each functions in the set H, as defined in Equation (13), does not change its sign within I, since any sign change would have to go through a zero of the function. As $f'(x) = ie^{ix} \cdot g_0'(e^{ix})$, Claim 3.10 implies that for every $\beta \in [a + \delta, b - \delta]$ it holds that

$$\begin{aligned} \left|g(e^{i\beta})\right| = \left|g_0(e^{i\beta})\right| = |f(\beta)| &\geq \frac{\delta}{\sqrt{2}} \min_{\alpha \in I} |f'(\alpha)| \\ = \frac{\delta}{\sqrt{2}} \min_{\alpha \in I} \left|g_0'(e^{i\alpha})\right| &= \frac{\delta \cdot \deg g_0}{\sqrt{2}} \min_{\alpha \in I} \left|\hat{g}(e^{i\alpha})\right|. \end{aligned} \tag{14}$$

By definition, $B(\hat{g}) \subseteq B(g)$. As $\|\hat{g}\|_0 = s$ and each $\beta \in I$ is at least $(s - 1)\delta$-far from $B(g)$, we get from the induction hypothesis applied to $\hat{g}$, Equation (14) and Claim 3.15

$$\begin{aligned} \left|g(e^{i\beta})\right| &\geq \frac{\delta \cdot \deg g_0}{\sqrt{2}} \min_{\alpha \in I} \left|\hat{g}(e^{i\alpha})\right| \\ &\geq \frac{\delta \cdot \deg g_0}{\sqrt{2}} \cdot d(\hat{g}) \left(\frac{\delta}{\sqrt{2}}\right)^{s-1} \\ &= \frac{\delta \cdot \deg g_0}{\sqrt{2}} \cdot d(g_0') \left(\frac{\delta}{\sqrt{2}}\right)^{s-1} \\ &= d(g) \left(\frac{\delta}{\sqrt{2}}\right)^{s}. \end{aligned}$$

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

In other words, every β that is $s\delta$ far from the set $B(g)$ satisfies $\left|g(e^{i\beta})\right| \geq d(g)\left(\frac{\delta}{\sqrt{2}}\right)^s$, which proves the step of the induction. □

Corollary 3.12. *Let $g \in \mathbb{C}[x]$ be a polynomial. Then, there exists a set $B(g) \subseteq [0, 2\pi)$, of size $|B(g)| \leq 12(\|g\|_0 - 1)(\deg g - ord_0 g)$, such that for every $\delta > 0$ and every $\alpha \in [0, 2\pi)$ which is $(\|g\|_0 - 1)\delta$-far from $B(g)$, it holds that*

$$\left|g(e^{i\alpha})\right| \geq \max\{|LC(g)| \cdot d(g), |TC(g)| \cdot d(g_{rev})\} \cdot \left(\frac{\delta}{\sqrt{2}}\right)^{\|g\|_0 - 1}.$$

Proof. Let $g_{\text{rev}} = x^{\deg g} g(1/x)$. Since for every α, $\left|g(e^{i\alpha})\right| = \left|g_{\text{rev}}(e^{-i\alpha})\right|$, we can consider either g or g_{rev} in order to prove the claim (replacing $B(g)$ with $B(g_{\text{rev}})$ if required). Note that $g/\text{LC}(g)$ and $g_{\text{rev}}/\text{LC}(g_{\text{rev}}) = g_{\text{rev}}/\text{TC}(g)$ are monic polynomials. From Lemma 3.11 we have (where α is δ-far from either $B(g)$ or $B(g_{\text{rev}})$, respectively)

$$\left|\frac{g(e^{i\alpha})}{\text{LC}(g)}\right| \geq d(g)\left(\frac{\delta}{\sqrt{2}}\right)^{\|g\|_0 - 1} \Rightarrow \left|g(e^{i\alpha})\right| \geq |\text{LC}(g)| \cdot d(g)\left(\frac{\delta}{\sqrt{2}}\right)^{\|g\|_0 - 1}$$
$$\left|\frac{g_{\text{rev}}(e^{i\alpha})}{\text{LC}(g_{\text{rev}})}\right| \geq d(g_{\text{rev}})\left(\frac{\delta}{\sqrt{2}}\right)^{\|g\|_0 - 1} \Rightarrow \left|g(e^{i\alpha})\right| \geq |\text{TC}(g)| \cdot d(g_{\text{rev}})\left(\frac{\delta}{\sqrt{2}}\right)^{\|g\|_0 - 1}.$$ □

Remark 3.13. Lemma 3.11 and Corollary 3.12 strengthen [NS24, Lemma 3.6] that proved the weaker bound $\left|g(e^{i\alpha})\right| \geq \left(\frac{\delta}{\sqrt{2}}\right)^{\|g\|_0 - 1}$. This is also reflected in Lemma 3.14 that improves upon [NS24, Lemma 3.7] by the same factor. Our improved bound in Theorem 3.3 will come from giving a lower bound on $\text{M} = \max\{|\text{LC}(g)| \cdot d(g), |\text{TC}(g)| \cdot d(g_{\text{rev}})\}$.

Lemma 3.14. *Let $g \in \mathbb{C}[x]$. Let $p_{\min} \in \mathbb{N}$ and $L(n) = n \log n$. Set $p_{\max} = \lceil 2L(p_{\min} + 12\|g\|_0(\deg g - ord_0 g))\rceil$. Then, there exists a prime $p \in (p_{\min}, p_{\max}]$ such that*

$$|g(\omega)| \geq M \cdot \left(\frac{\pi}{\sqrt{2} \cdot \|g\|_0 \cdot p_{\max}^2}\right)^{\|g\|_0 - 1},$$

for any p-th root of unity $\omega \neq 1$.

Proof. If $\|g\|_0 = 1$, then the statement is trivial since $|g(\omega)| = |\text{LC}(g)| = |\text{TC}(g)|$ for every root of unity ω. Hence, we can assume that $\|g\|_0 \geq 2$ and $\deg g \geq 1$.

Let $t = p_{\min} + 12\|g\|_0(\deg g - \text{ord}_0 g)$, and let $\pi(n)$ be the prime counting function. Our assumption implies that $t \geq 24$. By Fact 2.8 we conclude that

$$\begin{aligned}\pi(p_{\max}) &= \pi(\lceil 2t \log t\rceil) \\ &\geq \frac{2t \log t}{\log 2 + \log t + \log\log t} \\ &> \frac{2t \log t}{2 \log t} = t.\end{aligned}$$

Let $B(g)$ be as in Lemma 3.11 and

$$P = \{p_{\min} < p \leq p_{\max} : p \text{ is prime}\}.$$

We bound the size of P by counting the primes in the interval $(p_{\min}, p_{\max}]$:

$$|P| \geq \pi(p_{\max}) - p_{\min} > t - p_{\min} = 12\|g\|_0(\deg g - \text{ord}_0 g) \geq |B(g)|.$$

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

By Lemma 3.6, there exists $p \in P$ such that for any integer $0 < a < p$ and any $\alpha \in B(g)$

$$|a/p - \alpha/2\pi| \geq \frac{1}{2p_{\max}^2}.$$

Thus,

$$\left|2\pi\frac{a}{p} - \alpha\right| \geq \frac{\pi}{p_{\max}^2}.$$

In particular, every nontrivial p-th root of unity is $\frac{\pi}{p_{\max}^2}$-far from $B(g)$. Finally, by applying Corollary 3.12 with $\delta = \frac{\pi}{\|g\|_0 \cdot p_{\max}^2}$, we conclude that for any p-th root of unity $\omega \neq 1$,

$$\begin{aligned}|g(\omega)| &\geq \max\{|\mathrm{LC}(g)| \cdot d(g), |\mathrm{TC}(g)| \cdot d(g_{\mathrm{rev}})\} \cdot \left(\frac{\pi}{\sqrt{2} \cdot \|g\|_0 \cdot p_{\max}^2}\right)^{\|g\|_0 - 1} \\ &= M \cdot \left(\frac{\pi}{\sqrt{2} \cdot \|g\|_0 \cdot p_{\max}^2}\right)^{\|g\|_0 - 1}.\end{aligned}$$

□

We can now prove Theorem 3.3. We repeat its statement for convenience.

Theorem 3.3. *Let $f, g, h \in \mathbb{C}[x]$ such that $f = gh$. Denote $L(n) = n \log n$. Then,*

$$\|h\|_2 \leq \frac{\sqrt{2}\|f\|_1}{M}\left(2\|g\|_0 \cdot L(12\|g\|_0(\deg g - ord_0 g) + 2\deg f)^2\right)^{\|g\|_0 - 1}.$$

Proof. Let $p_{\min} = 2\deg f$ and $p_{\max}$ as in Lemma 3.14. From Lemma 3.14 we conclude that there exists a prime $p \in (p_{\min}, p_{\max}]$ such that

$$|g(\omega)| \geq \mathrm{M} \cdot \left(\frac{\pi}{\sqrt{2} \cdot \|g\|_0 \cdot (\lceil 2L(12\|g\|_0(\deg g - \mathrm{ord}_0 g) + 2\deg f)\rceil)^2}\right)^{\|g\|_0 - 1}$$

for any primitive p-th root of unity $\omega \neq 1$. The theorem then follows from Lemma 3.5. □

As $d(g) \geq 1$ we have $\mathrm{M} \geq \mathrm{LC}(g)$. Hence Theorem 3.3 implies the bound stated in [NS24, Theorem 3.8]. We next prove stronger lower bounds on M.

3.4. Improved lower bound on M

In this section we prove Lemma 3.4 which lower bounds $\mathrm{M} = \max\{|\mathrm{LC}(g)| \cdot d(g), |\mathrm{TC}(g)| \cdot d(g_{\mathrm{rev}})\}$. For this we first lower bound the product $d(g) \cdot d(g_{\mathrm{rev}})$.

To fix notation, denote

$$g(x) = \sum_{i=1}^{s} c_i x^{n_i} \tag{15}$$

and recall $d(g)$ as given in Definition 3.1. For the rest of the section we recall the notation from subsection 2.1: $g_0 = g/x^{\mathrm{ord}_0 g}$ and $g_{\mathrm{rev}} = x^{\deg g} \cdot g(1/x)$.

Claim 3.15. Let $g \in \mathbb{C}[x]$. Then $d(g) = d(g_0) = \deg g_0 \cdot d((g_0)')$.

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

Proof. The claim follows by an easy calculation. Using (15) we have

$$d(g_0) = \prod_{i=1}^{s-1}((n_s - n_1) - (n_i - n_1)) = \prod_{i=1}^{s-1}(n_s - n_i) = d(g).$$

Next, observe that

$$(g_0)' = (\sum_{i=1}^{s} c_i x^{n_i - n_1})' = \sum_{i=2}^{s}(n_i - n_1)c_i x^{n_i - n_1 - 1}.$$

Hence,

$$\begin{aligned}\deg g_0 \cdot d((g_0)') &= (n_s - n_1) \cdot \prod_{i=2}^{s-1}((n_s - n_1 - 1) - (n_i - n_1 - 1)) \\ &= \prod_{i=1}^{s-1}(n_s - n_i) = d(g).\end{aligned}$$

□

Claim 3.16. Let g as in (15). Then, $d(g_{\text{rev}}) = \prod_{i=2}^{s}(n_i - n_1)$.

Proof. The case $s = 1$ is clear. For $1 \le i \le s$ let $m_{s-i+1} = n_s - n_i$. Clearly, $0 = m_1 < m_2 < \ldots < m_s = n_s - n_1$. Then, $g_{\text{rev}} = \sum_{i=1}^{s} c_i x^{n_s - n_i} = \sum_{i=1}^{s} c_{s-i+1} x^{m_i}$ and we get that

$$d(g_{\text{rev}}) = \prod_{i=1}^{s-1}(m_s - m_i) = \prod_{i=1}^{s-1}((n_s - n_1) - (n_s - n_{s-i+1})) = \prod_{i=2}^{s}(n_i - n_1).$$

□

The next propositions contain the main technical calculations used to estimate M.

Proposition 3.17. *Let g as in (15). Denote $N \triangleq n_s - n_1$ and $k \triangleq \lfloor \frac{s-2}{2} \rfloor$. If $s \ge 2$ then,*

$$\max\{d(g), d(g_{rev})\} \ge \sqrt{2\pi k} N \left(\frac{k(N-k)}{e}\right)^{\frac{s-2}{2}}.$$

Proof. Using Claim 3.16,

$$\begin{aligned}\max\{d(g), d(g_{\text{rev}})\} &\ge \sqrt{d(g)d(g_{\text{rev}})} \\ &= \left(\prod_{i=1}^{s-1}(n_s - n_i) \cdot \prod_{i=2}^{s}(n_i - n_1)\right)^{1/2} \\ &= \left((n_s - n_1)^2 \cdot \prod_{i=2}^{s-1}((n_s - n_i)(n_i - n_1))\right)^{1/2}. \qquad (16)\end{aligned}$$

For $1 \le i \le s-2$ let $z_i = n_{i+1} - n_1$. Clearly, $1 \le z_1 < \cdots < z_{s-2} < N$. We rewrite (16) as

$$\max\{d(g), d(g_{\text{rev}})\} \ge N \cdot \left(\prod_{i=1}^{s-2}(z_i(N - z_i))\right)^{1/2}. \qquad (17)$$

We next lower bound the RHS of (17). Denote $\phi(x) = x(N-x)$. Clearly $\phi(x) = \phi(N-x)$. Furthermore $\phi(x+1) - \phi(x) = N - 1 - 2x$ making ϕ monotone increasing for $1 \le x \le N/2$ and decreasing for $x > N/2$. We thus have that

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

$$\phi(1) = \phi(N-1) < \phi(2) = \phi(N-2) < \cdots < \phi(\lfloor N/2 \rfloor) = \phi(\lceil N/2 \rceil).$$

Denote $\delta = \mathbb{1}_{s \text{ is odd}}$. Substituting into (17), and recalling $k = \lfloor \frac{s-2}{2} \rfloor$, we get

$$\begin{aligned}
\max\{d(g), d(g_{\text{rev}})\} &\geq N \cdot \left(\prod_{i=1}^{s-2} \phi(z_i) \right)^{1/2} \\
&= N \cdot ((k+1)(N-k-1))^{\delta/2} \prod_{i=1}^{k} (i(N-i)) \\
&\geq N \cdot ((k+1)(N-k-1))^{\delta/2} \cdot k! \cdot (N-k)^k.
\end{aligned}$$

By Robbin's estimate of the factorial function [Rob55]

$$\sqrt{2\pi k}(k/e)^k \leq \sqrt{2\pi k} k^k e^{-k} e^{\frac{1}{12k+1}} \leq k!,$$

and the fact that in our setting $(k+1)(N-k-1) \geq k(N-k)$, we conclude that

$$\begin{aligned}
\max\{d(g), d(g_{\text{rev}})\} &\geq N \cdot ((k+1)(N-k-1))^{\delta/2} \cdot \sqrt{2\pi k} \cdot \left(\frac{k(N-k)}{e} \right)^k \\
&\geq N \cdot \sqrt{2\pi k} \left(\frac{k(N-k)}{e} \right)^{k+\delta/2} \\
&= N \cdot \sqrt{2\pi k} \left(\frac{k(N-k)}{e} \right)^{\frac{s-2}{2}}.
\end{aligned}$$

□

Proposition 3.18. *Let g as in (15). Denote (as before) $N \triangleq n_s - n_1$ and $k \triangleq \lfloor \frac{s-2}{2} \rfloor$. If $s \geq 6$ then,*

$$\max\{d(g), d(g_{rev})\} \geq N \cdot \sqrt{2\pi k} \left(\frac{s(N-1)-3}{4e} \right)^{\frac{s-2}{2}}.$$

Proof. Since $s \geq 6$, it holds that $k = \lfloor \frac{s-2}{2} \rfloor \geq 2$. By Proposition 3.17, it is enough to show that $k(N-k) \geq \frac{s(N-1)-3}{4}$. Since $N = n_s - n_1 \geq s-1$ and by the monotonicity of $k(N-k)$ for $k \leq N/2$ it holds that,

$$\begin{aligned}
k(N-k) &= \left\lfloor \frac{s-2}{2} \right\rfloor \left(N - \left\lfloor \frac{s-2}{2} \right\rfloor \right) \\
&\geq \frac{s-3}{2} \left(N - \frac{s-3}{2} \right) \\
&= \frac{1}{4}(N(2s-6) - (s-3)(s-3)) \\
&= \frac{1}{4}\left(Ns + N(s-6) - (s-3)^2 \right) \\
&\geq^{(*)} \frac{1}{4}\left(Ns + (s-1)(s-6) - (s-3)^2 \right) \\
&= \frac{s(N-1)-3}{4},
\end{aligned}$$

where $^{(*)}$ holds as $s \geq 6$ and hence $N(s-6) \geq (s-1)(s-6)$. □

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

Proposition 3.19. *Let g as in (15). If $s \geq 2$ then*

$$\max\{d(g), d(g_{rev})\} \geq \sqrt{e}\left(\frac{s}{4e}\right)^{\frac{s-1}{2}} (n_s - n_1)^{\frac{s}{2}}.$$

Proof. We first note that for $s = 2$, trivially $d(g) = d(g_{\text{rev}}) = (n_s - n_1)$ and for $s = 3$

$$\begin{aligned}\max\{d(g), d(g_{\text{rev}})\} &= (n_s - n_1)\max\{n_s - n_2, n_2 - n_1\} \\ &\geq \frac{1}{2}(n_s - n_1)^2 > \frac{3}{4\sqrt{e}}(n_s - n_1)^{\frac{3}{2}},\end{aligned}$$

and the claim holds in both cases. For the cases of $s = 4$ and $s = 5$, we use Proposition 3.17 with $k = 1$ to deduce that,

$$\max\{d(g), d(g_{\text{rev}})\} \geq N \cdot \sqrt{2\pi}\left(\frac{N-1}{e}\right)^{\frac{s-2}{2}}$$

For $s = 4$ we have $N = n_s - n_1 \geq 3$, which implies $N - 1 \geq \frac{2}{3}N$ and so,

$$\max\{d(g), d(g_{\text{rev}})\} \geq N \cdot \sqrt{2\pi}\left(\frac{2N}{3e}\right) \geq \frac{N^2}{e}.$$

Similarly, for $s = 5$ we have $N = n_s - n_1 \geq 4$, which implies $N - 1 \geq \frac{3}{4}N$ and so,

$$\max\{d(g), d(g_{\text{rev}})\} \geq \sqrt{2\pi}\, N\left(\frac{3N}{4e}\right)^{\frac{3}{2}} \geq \sqrt{e}\left(\frac{5}{4e}\right)^2 N^{\frac{5}{2}}.$$

From now on we shall assume $s \geq 6$. Now observe that,

$$s(N-1) - 3 = sN - (s+3) = sN \cdot \left(1 - \frac{s+3}{sN}\right) \geq sN \cdot \left(1 - \frac{s+3}{s(s-1)}\right).$$

Applying Claim 2.4 with $t = \frac{s+3}{s(s-1)}$ yields

$$s(N-1) - 3 \geq sN \cdot \left(1 - \frac{s+3}{s(s-1)}\right) \geq sN \cdot e^{-\frac{s+3}{s(s-1)-(s+3)}} = sN \cdot e^{-\frac{s+3}{(s-3)(s+1)}}$$

Substituting in Proposition 3.18 we get,

$$\max\{d(g), d(g_{\text{rev}})\} \geq N \cdot \sqrt{2\pi k}\left(\frac{sN}{4e}\right)^{\frac{s-2}{2}} \cdot e^{-\frac{(s+3)(s-2)}{2(s-3)(s+1)}}$$

We observe that for $s \geq 6$,

$$e^{-\frac{(s+3)(s-2)}{2(s-3)(s+1)}} = e^{-\frac{1}{2}\left(1+\frac{1}{s-3}\right)\left(1+\frac{2}{s+1}\right)} \geq e^{-\frac{1}{2}\left(1+\frac{1}{3}\right)\left(1+\frac{2}{7}\right)} \geq \frac{1}{\sqrt{6}}$$

and that $\pi(s-3) \geq \frac{3}{2}s$. We can therefore deduce that,

$$\begin{aligned}\max\{d(g), d(g_{\text{rev}})\} &\geq N \cdot \sqrt{\frac{\pi k}{3}}\left(\frac{sN}{4e}\right)^{\frac{s-2}{2}} \\ &\geq N \cdot \sqrt{\frac{\pi(s-3)}{6}}\left(\frac{sN}{4e}\right)^{\frac{s-2}{2}}\end{aligned}$$

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

$$\geq N \cdot \sqrt{\frac{s}{4}}\left(\frac{sN}{4e}\right)^{\frac{s-2}{2}}$$
$$= \sqrt{e}\left(\frac{s}{4e}\right)^{\frac{s-1}{2}} N^{\frac{s}{2}} = \sqrt{e}\left(\frac{s}{4e}\right)^{\frac{s-1}{2}} (n_s - n_1)^{\frac{s}{2}},$$

as claimed. □

We are now ready to prove Lemma 3.4. We recall its statement.

Lemma 3.4. *Let $g \in \mathbb{C}[x]$. Let $M = \max\{|LC(g)| \cdot d(g), |TC(g)| \cdot d(g_{rev})\}$. Then,*

$$M \geq \max\left\{ \begin{array}{c} \min\{|LC(g)|, |TC(g)|\} \cdot \sqrt{e}\left(\frac{\|g\|_0}{4e}\right)^{\frac{\|g\|_0-1}{2}} (\deg g - ord_0 g)^{\frac{\|g\|_0}{2}} \\ \max\{|LC(g)|, |TC(g)|\} \cdot (\deg g - ord_0 g) \end{array} \right\}.$$

Proof. Recall $\mathrm{M} = \max\{|\mathrm{LC}(g)| \cdot d(g), |\mathrm{TC}(g)| \cdot d(g_{\mathrm{rev}})\}$. Clearly $d(g), d(g_{\mathrm{rev}}) \geq (\deg g - \mathrm{ord}_0 g)$ and therefore

$$\mathrm{M} \geq \max\{|\mathrm{LC}(g)|, |\mathrm{TC}(g)|\} \cdot (\deg g - \mathrm{ord}_0 g).$$

In addition, since $\max\{|\mathrm{LC}(g)| \cdot d(g), |\mathrm{TC}(g)| \cdot d(g_{\mathrm{rev}})\} \geq \min\{|\mathrm{LC}(g)|, |\mathrm{TC}(g)|\} \cdot \max\{d(g), d(g_{\mathrm{rev}})\}$, Proposition 3.19 implies that

$$\mathrm{M} \geq \min\{|\mathrm{LC}(g)|, |\mathrm{TC}(g)|\} \cdot \sqrt{e}\left(\frac{\|g\|_0}{4e}\right)^{\frac{\|g\|_0-1}{2}} \cdot (\deg g - \mathrm{ord}_0 g)^{\frac{\|g\|_0}{2}}.$$ □

4. Polynomial division algorithm

In this section, we analyze the polynomial division algorithm (see [CLO13, Chapter 1.5] or [vzGG13, Chapter 2.4]), also called long division or Euclidean division algorithm. We consider a version in which we are given upper bounds on the sparsity and height of the quotient polynomial. Namely, if the sparsity of the quotient polynomial is bounded by s, and its coefficients are bounded (in absolute value) by c, then we execute s steps of the division algorithm and return True if and only if at termination the remainder is zero. If at any step $\|q\|_\infty > c$, we return False.

Algorithm 1 Bounded Polynomial Division over $\mathbb{Z}$

Input: $g, f \in \mathbb{Z}[x]$, a bound $s \in \mathbb{N}$ on $\|f/g\|_0$, and a bound $c \in \mathbb{N}$ on $\|f/g\|_\infty$.
Output: True and a factor f/g if $g \mid f$ and $\|f/g\|_0 \leq s$, $\|f/g\|_\infty \leq c$; False otherwise.

1. Set $q = 0$, $r = f$, $i = 1$, and $t = 0$.
2. While $\deg r \geq \deg g$, $|\mathrm{LC}(r)| \leq c$, and $i \leq s$:
   (a) If $\mathrm{LC}(g) \nmid \mathrm{LC}(r)$, return False.
   (b) Set $\alpha = \frac{\mathrm{LC}(r)}{\mathrm{LC}(g)}$. If $|\alpha| > c$ then return False.
   (c) Set $t = \alpha \cdot x^{\deg r - \deg g}$.
   (d) Set $q = q + t$.
   (e) Set $r = r - t \cdot g$.
   (f) Set $i = i + 1$.
3. If $r = 0$ return True and the quotient polynomial q; Otherwise, return False.

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

The correctness of Algorithm 1 is due to the fact that in every step of the loop, we reveal a single term of the quotient. By definition of c and s, the coefficient of the term cannot exceed c, and the number of terms cannot be larger than s, unless $g \nmid f$.

Proposition 4.1. *The bit complexity of Algorithm 1 is*

$$\widetilde{O}((\|f\|_0 + s \cdot \|g\|_0) \cdot (\log \|g\|_\infty + \log \|f\|_\infty + \log c + \log \deg f))$$

Proof. We first prove upper bounds on $\|r\|_0$ and $\|r\|_\infty$ at each step of the algorithm. As at the beginning $r = f$. At each iteration of the While loop the number of terms of r increases (additively) by at most $\|g\|_0 - 1$ (as we subtract $t \cdot g$ from r, and we know that the leading terms cancel). Similarly, $\|r\|_\infty$ increases (additively) in each step by at $\|g\|_\infty \cdot c$. As at the beginning $r = f$ we get that in every step of the algorithm it holds that

$$\begin{aligned} \|r\|_0 &\le \|f\|_0 + s(\|g\|_0 - 1), \\ \|r\|_\infty &\le \|f\|_\infty + s \cdot c \cdot \|g\|_\infty. \end{aligned}$$

This implies that at every step the representation size of r is at most

$$\begin{aligned} \operatorname{size}(r) &= \|r\|_0 \cdot (\log_2 \|r\|_\infty + \log_2 \deg r) \\ &\le (\|f\|_0 + s \cdot (\|g\|_0 - 1)) \cdot (\log_2 \|f\|_\infty + \log_2 s + \log_2 c + \log_2 \|g\|_\infty + \log_2 \deg f). \end{aligned}$$

The algorithm performs in-place addition and subtraction to the polynomials q, r. Each iteration of the While loop requires $\|g\|_0$ multiplications (for computing $t \cdot g$), $\|g\|_0$ additions (for subtracting $t \cdot g$ from r) and a single division, of integers (for computing t), whose absolute values are at most

$$B \le \|r\|_\infty + c \cdot \|g\|_\infty \le \|f\|_\infty + (s+1) \cdot c \cdot \|g\|_\infty.$$

Each of these integers requires at most $b = \lceil \log_2 B \rceil$ bits to represent, and so these arithmetic operations can be performed in time

$$O(b \log b) = \widetilde{O}(b) = \widetilde{O}(\log \|f\|_\infty + \log s + \log c)$$

(see [HvdH21]). In addition, we perform operations on the exponent that require $O(\log \deg f)$ time and we have to store both q and r in memory. Storing q requires storing s terms, each term has degree at most $\deg f$ and coefficient which is at most c in absolute value. Thus, the cost of storing q is at most $\operatorname{size}(q) \le s(\log_2 \deg f + \log_2 c)$.

Combining all these estimates we get that the running time is at most

$$\widetilde{O}((\|f\|_0 + s \cdot \|g\|_0) \cdot (\log \|g\|_\infty + \log \|f\|_\infty + \log c + \log \deg f)).$$ □

The proof of Theorem 1.9 easily follows.

Proof of Theorem 1.9. Set $s = \deg f \ge \|f/g\|_0$ and let $c = \log_2 \|f\|_\infty + O(\|g\|_0 \cdot \log \deg f) \ge \|f/g\|_\infty$ be the upper bound given in (7) on the absolute value of coefficients of f/g. Note that $\deg f$ is a very rough upper bound on $\|f/g\|_0$, but as the division is exact the algorithm will terminate after $\|f/g\|_0$ iterations. Thus, we may assume in the upper bound calculations that $s = \|f/g\|_0$. Substituting these values to Proposition 4.1 (and observing that $\|f\|_0 \le \|g\|_0 \|f/g\|_0$), gives the desired result. □

Acknowledgments. The authors would like to thank Bruno Grenet for his helpful comments and for suggesting Corollary 1.11. We would also like to thank the anonymous referees for their comments that helped improve the presentation of our results.

Competing interest. The authors have no competing interest to declare.

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press

Financial support. This research was co-funded by the European Union (ERC, EACTP, 101142020), the Israel Science Foundation (grant number 514/20) and the Len Blavatnik and the Blavatnik Family Foundation. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

References

[ABW13] Sheldon Axler, Paul Bourdon, and Ramey Wade, *Harmonic Function Theory*, volume 137 (Springer Science & Business Media, 2013).

[Ahl21] Lars Ahlfors, *Complex Analysis: An Introduction to the Theory of Analytic Functions of One Complex Variable*, Third Edition. AMS Chelsea Publishing Series (American Mathematical Society, 2021).

[BG06] Enrico Bombieri and Walter Gubler, *Heights in Diophantine Geometry*. New Mathematical Monographs (Cambridge University Press, 2006).

[CLO13] David Cox, John Little, and Donal O'Shea, *Ideals, Varieties, and Algorithms: an Introduction to Computational Algebraic Geometry and Commutative Algebra* (Springer Science & Business Media, 2013).

[DC09] James Harold Davenport and Jacques Carette, The sparsity challenges. In *2009 11th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, pages 3–7, 2009.

[DST93] James Harold Davenport, Yvon Siret, and Évelyne Tournier, *Computer Algebra Systems and Algorithms for Algebraic Computation* (Academic Press Professional, Inc., 1993).

[Gel60] Alexander O. Gel'fond, *Transcendental and Algebraic Numbers* (Dover Publications, Inc., New York, Russian edition, 1960).

[GGPdC21] Pascal Giorgi, Bruno Grenet, and Armelle Perret du Cray, On exact division and divisibility testing for sparse polynomials. In *Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation*, ISSAC '21, pages 163–170, New York, NY, USA, 2021. Association for Computing Machinery.

[GGPdCR22] Pascal Giorgi, Bruno Grenet, Armelle Perret du Cray, and Daniel S. Roche, Sparse polynomial interpolation and division in soft-linear time. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*, pages 459–468, 2022.

[GR11] Mark Giesbrecht and Daniel S. Roche, 'Detecting lacunary perfect powers and computing their roots', *J. Symb. Comput.* **46**(11) (2011), 1242–1259.

[Har92] Joe Harris, *Algebraic Geometry*, volume 133 of *Graduate Texts in Mathematics* (Springer-Verlag, New York, 1992). A first course.

[HvdH21] David Harvey and Joris van der Hoeven, 'Integer multiplication in time $O(n \log n)$', *Ann. of Math. (2)*, **193**(2) (2021), 563–617.

[Joh74] Stephen C. Johnson, 'Sparse polynomial arithmetic', *SIGSAM Bull.* **8**(3) (1974), 63–71.

[Kho91] Askold G. Khovanskiĭ, *Fewnomials,* volume 88 of *Translations of Mathematical Monographs* (American Mathematical Society, Providence, RI, 1991). Translated from the Russian by Smilka Zdravkovska.

[LLL82] Arjen K. Lenstra, Hendrik W. Lenstra, and László Lovász, 'Factoring polynomials with rational coefficients', *Mathematische Annalen*, **261** (1982), 515–534.

[Mah62] Kurt Mahler, 'On some inequalities for polynomials in several variables', *J. London Math. Soc.* **37**(1) (1962), 341–344.

[Mig74] Maurice Mignotte, 'An inequality about factors of polynomials', *Math. Comput.* **28** (1974), 1153–1157.

[Mig88] Maurice Mignotte, 'An inequality about irreducible factors of integer polynomials', *J. Number Theory* **30**(2) (1988), 156–166.

[Mig12] Maurice Mignotte, *Mathematics for Computer Algebra* (Springer Science & Business Media, 2012).

[MP13] Michael Monagan and Roman Pearce, 'Poly: A new polynomial data structure for Maple 17', *ACM Commun. Comput. Algebra* **46**(3/4) (2013), 164–167.

[NS24] Ido Nahshon and Amir Shpilka, New bounds on quotient polynomials with applications to exact division and divisibility testing of sparse polynomials. In Jonathan D. Hauenstein, Wen-shin Lee, and Shaoshi Chen, editors, *Proceedings of the 2024 International Symposium on Symbolic and Algebraic Computation, ISSAC 2024, Raleigh, NC, USA, July 16-19, 2024*, pages 91–99. ACM, 2024.

[Pla77] David A. Plaisted, 'Sparse complex polynomials and polynomial reducibility', *J. Comput. Syst. Sci.* **14**(2) (1977), 210–221.

[Pla84] David A. Plaisted, 'New NP-hard and NP-complete polynomial and integer divisibility problems', *Theor. Comput. Sci.* **31**(1) (1984), 125–138.

[Ram19] Srinivasa Ramanujan, 'A proof of Bertrand's postulate', *J. Indian Math. Soc.* **11** (1919), 181–182.

[Rob55] Herbert Robbins, 'A remark on Stirling's formula', *Amer. Math. Monthly* **62** (1955), 26–29.

[Roc18] Daniel S. Roche. What can (and can't) we do with sparse polynomials? In *Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation*, ISSAC '18, page 25–30, New York, NY, USA, 2018. Association for Computing Machinery.

[RS62] John Barkley Rosser and Lowell Schoenfeld, 'Approximate formulas for some functions of prime numbers', *Illinois J. Math.* **6**(1) (1962), 64–94.

[S+08] William Stein et al. Sage reference manual. *Release*, **21**:2008, 2008.

[Sch03] Hans Schönemann, 'Singular in a framework for polynomial computations', in *Algebra, Geometry and Software Systems* (Springer, 2003), 163–176.

[Tit02] Edward C. Titchmarsh, *The Theory of Functions* (Oxford University Press, 2002).

[vzGG13] Joachim von zur Gathen and Jürgen Gerhard, *Modern Computer Algebra* (Cambridge University Press, 2013).

[Wol99] Stephen Wolfram. *The MATHEMATICA® book, version 4* (Cambridge University Press, 1999).

https://doi.org/10.1017/fms.2026.10202 Published online by Cambridge University Press