# The norm of Gaussian periods

P. Habegger

Departement Mathematik und Informatik
Fachbereich Mathematik
Universität Basel
CH-4051 Basel

Preprint No. 2016-22
November 2016

www.math.unibas.ch

# THE NORM OF GAUSSIAN PERIODS

P. HABEGGER

Abstract. Gaussian periods are cyclotomic integers with a long history in number theory and connections to problems in combinatorics. We investigate the asymptotic behavior of the absolute norm of a Gaussian period and provide a rate of convergence in a case of Myerson's Conjecture for periods of arbitrary odd length. Our method involves a result of Bombieri, Masser, and Zannier on unlikely intersections in the algebraic torus as well as work of the author on the diophantine approximations to a set definable in an o-minimal structure. In the appendix we make a result of Lawton on Mahler measures quantitative.

## 1. Introduction

Let $f \geq 1$ be an integer and $p$ a prime number. We are interested in the asymptotic behavior of the norm of

$$\zeta^{a_1} + \zeta^{a_2} + \cdots + \zeta^{a_f} \quad \text{where} \quad \zeta = e^{2\pi\sqrt{-1}/p} \tag{1}$$

as $a_1, \ldots, a_f \in \mathbb{Z}$ and $p$ vary.

These cyclotomic integers appear naturally in algebraic number theory. We identify the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ with $\mathbb{F}_p^\times = \mathbb{F}_p \smallsetminus \{0\}$. Say $a_1, \ldots, a_f$ represent the elements of a subgroup $G \subseteq \mathbb{F}_p^\times$ of order $f$. Then the sum (1) is the trace of $\zeta$ relative to the subfield of $\mathbb{Q}(\zeta)$ fixed by the said subgroup and it is called a Gaussian period. It has degree $k = [\mathbb{F}_p^\times : G] = (p-1)/f$ over $\mathbb{Q}$, we refer to Chapter 10.10 of Berndt, Evans, and Williams' book [3] for these and other facts. A Gaussian period can be expressed in terms of $p$ and $f$ for small values of $k$. Indeed, if $k = 1$ then $G = \mathbb{F}_p^\times$ and the Gaussian period is of course $\zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1$. Gauss evaluated the sum if $k = 2$ and the minimal polynomial of a Gaussian period has been computed if $k \leq 4$.

The absolute norm of a Gaussian period appears in combinatorial problems, cf. Myerson's work [18, 19]. Let $A_1, \ldots, A_k \in \mathbb{F}_p^\times$ denote a complete set of representatives of $\mathbb{F}_p^\times/G$. Then the cardinality satisfies

$$\#\{(x_1, \ldots, x_k) \in G^k : A_1x_1 + \cdots + A_kx_k = 0\} - \frac{1}{p}f^k = \frac{p-1}{p}\Delta \tag{2}$$

where

$$\Delta = \prod_{t \in \mathbb{F}_p^\times/G} \left( \sum_{g \in G} \zeta^{tg} \right);$$

note that $\zeta^t$ is well-defined for $t \in \mathbb{F}_p$ as is the sum. If $A_1x_1 + \cdots + A_kx_k$ were to attain all values of $\mathbb{F}_p$ equally often then $\Delta$ would vanish. As Myerson [18] observed,

2010 *Mathematics Subject Classification.* Primary: 11R06, secondary: 05A15, 11J71, 11K60, 37A45.

*Key words and phrases.* Gaussian period, Mahler measure, Diophantine Approximation, Ergodic Theory and Number Theory.

this linear form attains *non-zero* values equally often. It is tempting to interpret (2) as an error term. But note that the trivial estimate $\left|\sum_{g\in G}\zeta^{tg}\right| \leq f$ leads to the upper bound $(1-p^{-1})f^k$ for the modulus of (2). This bound exceeds $p^{-1}f^k$ for all $p \geq 3$. In this paper we will improve on the trivial bound if the length $f$ of the Gaussian period is a fixed prime and $p$ is large.

When well-defined, the logarithmic absolute norm of the Gaussian period is

$$\frac{1}{k}\log|\Delta| = \frac{1}{p-1}\sum_{t=1}^{p-1}\log\left|\sum_{g\in G}\zeta^{tg}\right|. \tag{3}$$

Our Theorem 1 below determines the asymptotic behavior of this value as $p\to\infty$ when $f = \#G$ is a fixed prime. Before stating our first result, we survey what is known for groups $G$ of order $f$.

Certainly (3) vanishes if $G$ is trivial. If $f = 2$, then $G = \{\pm 1\}$ and $p$ is odd. Note that $\zeta + \zeta^{-1} = \zeta^{-1}(\zeta^2+1)$ is a unit in $\mathbb{Q}(\zeta)$. So (3) is again zero. The value of $\Delta$, i.e. its sign, can be computed using the Kronecker symbol.

Already the case $f = 3$ is more involved. It requires the logarithmic Mahler measure

$$\mathrm{m}(P) = \int_0^1\cdots\int_0^1 \log\left|P\left(e^{2\pi\sqrt{-1}x_1},\ldots,e^{2\pi\sqrt{-1}x_n}\right)\right| dx_1\cdots dx_n,$$

of a non-zero Laurent polynomial $P\in\mathbb{C}[X_1^{\pm1},\ldots,X_n^{\pm1}]$; for the fact that this integral converges and other properties we refer to Chapter 3.4 in Schinzel's book [23]. If $p\equiv 1 \pmod 3$, then $\mathbb{F}_p^\times$ contains an element $\theta$ of order 3. Myerson, cf. Lemma 21 [19], proved

$$\frac{1}{p-1}\sum_{t=1}^{p-1}\log\left|\zeta^t+\zeta^{t\theta}+\zeta^{t\theta^2}\right| = \mathrm{m}(1+X_1+X_2)+o(1) \tag{4}$$

as $p\to\infty$. The logarithmic Mahler measure of $1+X_1+X_2$ was evaluated by Smyth [26] and equals $L'(-1,\chi)$ where $\chi$ is the non-trivial character modulo 3 and $L(\cdot,\chi)$ is its associated Dirichlet $L$-function. Duke [8] gave a new proof of (4) which extended to a larger class of vectors in $\mathbb{F}_p^3$ containing the exponent vector $(1,\theta,\theta^2)$. Moreover, he provided a rate of convergence.

Due to a fortunate factorization, the case $f = 4$ is similar to order 2. Indeed, Theorem 6 [19] implies $\Delta = \pm 1$ if $p\equiv 1 \pmod 4$ and also determines the sign. So the limit in question is again zero.

For higher order, the approaches in [19] and [8] break down. But Myerson's Conjecture [18] predicts convergence of (3) as $p\to\infty$ and the limit point. The full conjecture is more general as it also covers subgroups of $\mathbb{F}_q^\times$ where $q$ is a fixed power of $p$.

Myerson's Conjecture has an ergodic flavor. Indeed, using methods from ergodic theory, Lind, Schmidt, and Verbitskiy [15] proved convergence in the following setting. They suitably averaged the value of the logarithm of the modulus of a polynomial evaluated at a finite subgroup of roots of unity. Their polynomials are required to satisfy an intersection theoretical property with respect to the maximal compact subgroup of $(\mathbb{C}\smallsetminus\{0\})^n$. They computed the limit of this average for certain sequences of groups of roots of unity.

In this paper we concentrate on the special case when $G$ has fixed odd order. We prove that (3) converges and compute the limit.

Our method is based on a recent result [12] of the author on diophantine approximation of sets definable in a polynomially bounded o-minimal structure. It counts strong rational approximations to a definable set and is related to the Pila-Wilkie Counting Theorem [21]. Our approach is quantitative in the sense that it can provide a rate of convergence.

The following theorem is the special case of our main result when $\#G$ is an odd prime. We refer to Corollary 21 below for a more general statement. This corollary contains the case $q = p$ of Myerson's Conjecture.

**Theorem 1.** *Suppose $f$ is an odd prime. For a prime $p$ with $p \equiv 1 \pmod f$ let $G_p \subseteq \mathbb{F}_p^\times$ denote the subgroup of order $f$. Then*

$$\frac{1}{p-1}\sum_{t=1}^{p-1}\log\left|\sum_{g\in G_p} e^{2\pi\sqrt{-1}\frac{tg}{p}}\right| = \mathrm{m}(1+X_1+\cdots+X_{f-1}) + O\left(p^{-\frac{1}{5(f-1)^2}}\right) \tag{5}$$

*as $p \to \infty$; in particular, the logarithm is well-defined for all sufficiently large $p$.*

We have the estimate $\mathrm{m}(1+X_1+\cdots+X_{f-1}) \leq \frac{1}{2}\log f$ by Corollary 6 in Chapter 3.4 [23]. This justifies the treatment of (2) as an error term if $f = \#G$ is a prime and $p$ is large.

The value $\mathrm{m}(1+X_1+\cdots+X_{f-1})$ is non-zero if $f \geq 3$. This implies an amusing corollary of Theorem 1 on Gaussian periods that are units.

**Corollary 2.** *Suppose $f$ is an odd prime. There are at most finitely many primes $p$ with $p \equiv 1 \pmod f$ such that*

$$\sum_{g\in G} e^{2\pi\sqrt{-1}\frac{g}{p}}$$

*is an algebraic unit where $G \subseteq \mathbb{F}_p^\times$ denotes the subgroup of order $f$.*

Gaussian periods and their generalizations were investigated by Duke, Garcia, and Lutz [9] from several points of view. In Theorem 6.3 they prove that the Galois orbit of a Gaussian period becomes equidistributed in a suitable sense. Our average (3) involves the logarithm whose singularity at the origin often makes applying equidistribution directly impossible, see for example Autissier's example [1].

Our main technical result is Theorem 20 below. It essentially amounts to a convergence result when averaging over groups of roots of unity of prime order. It is used to deduce the theorem and corollary above.

The main difficult when $f = \#G \geq 5$ is that the integrand

$$1+X_1+\cdots+X_{f-1}$$

in the logarithmic Mahler measure (5) has singularities along a positive dimensional real semi-algebraic set.

Our approach requires new tools and we now give a brief overview of the proof of Theorem 1. As in Duke's work [8] we start with a basic observation; to simplify notation

we set $n = f - 1$. Let $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$, then

$$\prod_{t=1}^{p-1} \left(1 + \zeta^{ta_1} + \cdots + \zeta^{ta_n}\right)$$

is the product of

$$P_a = 1 + X^{a_1} + \cdots + X^{a_n}$$

evaluated at all roots of unity of order $p$. If $a_n > a_{n-1} > \cdots > a_1 > 0$, then $P_a$ is a monic polynomial and the product above is the resultant of $P_a$ and $1 + X + \cdots + X^{p-1}$. If this resultant is non-zero, then by symmetry properties we find that (3) equals

$$-\frac{\log(n+1)}{p-1} + \frac{1}{p-1} \sum_{i=1}^{d} \log|\alpha_i^p - 1|. \tag{6}$$

where $\alpha_1, \dots, \alpha_d$ are the roots of $P_a$. Comparing $\frac{1}{p-1} \log|\alpha_i^p - 1|$ to the local contribution $\log \max\{1, |\alpha_i|\}$ of the logarithmic Mahler measure $\mathrm{m}(P_a)$ is a crucial aspect of the problem at hand; see Section 2 for details on the Mahler measure. Indeed, by a result of Lawton [14] the value $\mathrm{m}(P_a)$ converges towards the logarithmic Mahler measure of a multivariate polynomial as in Theorem 1 if $|a| \to \infty$ for $a$ in sufficiently general position. In a self-contained appendix, we provide a quantitative version of Lawton's Theorem, see Theorem 24.

Baker's theory on linear forms in logarithms yields a lower bound for non-zero values of $|\alpha_i^p - 1|$. But the current estimates are not strong enough to directly establish Theorem 1, see Duke's comment after the proof of this Theorem 3 [8]. However, as we shall see below, strong lower bounds for $|\alpha_i^p - 1|$ are available if $|\alpha_i| \neq 1$. Indeed, $|\alpha_i^p - 1| \geq ||\alpha_i|^p - 1| \geq ||\alpha_i| - 1|$. If $|\alpha_i| \neq 1$ we will use an old result of Mahler on the separation of distinct roots of a polynomials to bound $||\alpha_i| - 1|$ from below. If $\alpha_i$ lies in $\mu_\infty$, the set of all roots of unity in $\mathbb{C}$, then a sufficiently strong lower bound for $|\alpha_i^p - 1|$ follows from simpler considerations.

This estimate gives us sufficient control on each term in the sum (6) subject to the condition that $P_a$ does not have any root in $S^1 \smallsetminus \mu_\infty$, here $S^1$ is the unit circle in $\mathbb{C}$. But it seems unreasonable to expect this hypothesis to hold for all $a$. To address this concern we use symmetry in (3). Indeed, this mean is invariant under translating $a$ by an element of $p\mathbb{Z}^n$ and also by replacing $a$ by $ta$ with $t \in \mathbb{Z}$ coprime to $p$. We exploit this symmetry by using a result of Bombieri, Masser, and Zannier [5] on unlikely intersections. This in combination with Dirichlet's Theorem in diophantine approximation allows us to assume that $P_a$ has no roots on $S^1 \smallsetminus \mu_\infty$ after a suitable transformation as described above. Here the parity assumption on $f$ in Corollary 21 below is used.

At this point we have a sufficient lower bound for each term of the sum (6). However, the method cannot proceed if too many terms are close to this bound. Duke [8] already use the following basic principle. Suppose that for some $\alpha = \alpha_i$ the distance $|\alpha^p - 1|$ is small, i.e. at most a fixed power of $p^{-1}$. Than one can expect that $\alpha$ is close to some $\zeta \in \mu_p$ where $\mu_p$ is the set of roots of unity in $\mathbb{C}$ of order dividing $p$. As $P_a(\alpha) = 0$ we find that

$$|1 + \zeta^{a_1} + \cdots + \zeta^{a_n}| \tag{7}$$

is small. Myerson [20] proved a lower bound for non-vanishing sums of roots of unity if $n = 1, 2$, and 3. His estimates are are polynomial in $p^{-1}$ and are strong enough to imply Duke's result. However, for fixed $n \geq 4$ only exponential bounds such as $(n+1)^{-p}$ are known to hold in general. They are not good enough for our purposes.

If $|\alpha_i^p - 1|$ is small for many $i$, we are able to show that (7) is small for many $p$-th roots of unity $\zeta$. This situation can be analyzed using the following theorem that counts small sums of roots of unity of prime order. Its proof requires recent work of the author [12] on diophantine approximations on definable sets in an o-minimal structure.

**Theorem 3.** *Let $n \geq 1$. For all $\epsilon > 0$ there exist constants $c = c(n, \epsilon) \geq 1$ and $\lambda = \lambda(n, \epsilon) \geq 1$ with the following property. If $p$ is a prime and $\zeta_1, \ldots, \zeta_n \in \mu_p$ satisfy $1 + \zeta_1 + \cdots + \zeta_n \neq 0$, then*

$$\#\left\{t \in \mathbb{F}_p : |1 + \zeta_1^t + \cdots + \zeta_n^t| < c^{-1} p^{-\lambda}\right\} \leq c p^{\epsilon}. \tag{8}$$

As this paper was being finished up, Dimitrov [7] announced a extension to more general polynomials of Lind, Schmidt, and Verbitskiy's work for subgroups that are Cartesian powers. His approach used ideas from diophantine approximation and is independent from ours.

We hope to expand the connection between counting points approximating a definable set and questions related to ergodic theory in future work.

## 2. Notation

The supremum norm on $\mathbb{R}^n$ is $|\cdot|$ for any $n \geq 1$. We have already seen the definition of the logarithmic Mahler measure $\mathrm{m}(P)$ if $P \in \mathbb{C}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}] \smallsetminus \{0\}$. The Mahler measure of $P$ is $\mathrm{M}(P) = e^{\mathrm{m}(P)}$.

The absolute logarithmic Weil height, or just height, of an algebraic number $\alpha$ with minimal polynomial $P$ in $\mathbb{Z}[X]$ and leading term $p_0 \geq 1$ is

$$h(\alpha) = \frac{1}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \mathrm{m}(P) = \frac{1}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \log \left( p_0 \prod_{\substack{z \in \mathbb{C} \\ P(z) = 0}} \max\{1, |z|\} \right)$$

where the second equality follows from Jensen's Formula. We write $H(\alpha) = e^{h(\alpha)}$. Moreover, we set $H(\alpha_1, \ldots, \alpha_n) = \max\{H(\alpha_1), \ldots, H(\alpha_n)\}$ if $\alpha_1, \ldots, \alpha_n$ are algebraic.

## 3. Algebraic Numbers Close to the Unit Circle

An algebraic number $\alpha \in \mathbb{C} \smallsetminus \{1\}$ of degree $D = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ can be bounded away from 1 using Liouville's Inequality, Theorem 1.5.21 [4],

$$\log |\alpha - 1| \geq -D \log 2 - D h(\alpha).$$

The modulus $|\alpha| = \sqrt{\alpha \overline{\alpha}}$ is again an algebraic number, here and below $\bar{\cdot}$ denotes complex conjugation. Its height satisfies

$$h(|\alpha|) \leq \frac{1}{2} h(\alpha \overline{\alpha}) \leq h(\alpha)$$

since $h(\overline{\alpha}) = h(\alpha)$. If $\alpha$ is real, then clearly $\mathbb{Q}(|\alpha|) = \mathbb{Q}(\alpha)$. However, for $D \geq 2$ we only have $[\mathbb{Q}(|\alpha|) : \mathbb{Q}] \leq D(D-1)$ and equality is possible. So Liouville's Inequality applied to $|\alpha|$ gives

$$\log ||\alpha| - 1| \geq -D(D-1)\log 2 - D(D-1)h(\alpha)$$

if $|\alpha| \neq 1$. We will use a result of Mahler to improve on the dependency in $D$ in front of $\log 2$.

**Theorem 4** (Mahler)**.** *Let $P \in \mathbb{Z}[X]$ be a polynomial with $D = \deg P \geq 2$. If $z, z' \in \mathbb{C}$ are distinct roots of $P$, then*

$$|z' - z| > \sqrt{3}D^{-(D+2)/2}\mathrm{M}(P)^{-(D-1)}.$$

*Proof.* We may assume that $P$ has no multiple roots over $\mathbb{C}$ after replacing it by its squarefree part. The estimate then follows from Theorem 2 [16] as the absolute value of the new discriminant is at least 1. □

**Lemma 5.** *Let $\alpha \in \mathbb{C}$ be an algebraic number of degree $D = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. If $|\alpha| \neq 1$ then*

$$\log |\alpha^p - 1| \geq \log ||\alpha| - 1| \geq -1 - (D+1)\log(2D) - 2(2D-1)Dh(\alpha)$$

*for all integers $p \geq 1$.*

*Proof.* The first inequality follows from $|\alpha^p - 1| \geq ||\alpha|^p - 1| = ||\alpha| - 1| \cdot ||\alpha|^{p-1} + \cdots + 1| \geq ||\alpha| - 1|$. To prove the second inequality we may assume $|\alpha| \geq 1/2$, in particular $\alpha \neq 0$. Let $P \in \mathbb{Z}[X]$ denote the minimal polynomial of $\alpha$. We will apply Mahler's Theorem to $F = P(X)P(1/X)X^D \in \mathbb{Z}[X]$. Observe that $F(\alpha) = F(\overline{\alpha}^{-1}) = 0$ and $\deg F = 2D$. Therefore, $|\alpha - \overline{\alpha}^{-1}| > \sqrt{3}(2D)^{-(2D+2)/2}\mathrm{M}(F)^{-(2D-1)}$ since $|\alpha| \neq 1$. As $\mathrm{M}(P(1/X)X^D) = \mathrm{M}(P)$ and since the Mahler measure is multiplicative, we find, after multiplying with $|\alpha| = |\overline{\alpha}|$, that

$$\big||\alpha|^2 - 1\big| > \sqrt{3}|\alpha|(2D)^{-(D+1)}\mathrm{M}(P)^{-2(2D-1)}.$$

Observe that $\log \mathrm{M}(P) = Dh(\alpha)$ and $||\alpha| - 1| = ||\alpha|^2 - 1|/(|\alpha| + 1)$. Therefore,

$$||\alpha| - 1| > \sqrt{3}\frac{|\alpha|}{|\alpha|+1}(2D)^{-(D+1)}\mathrm{M}(P)^{-2(2D-1)} \geq \frac{\sqrt{3}}{3}(2D)^{-(D+1)}e^{-2(2D-1)Dh(\alpha)}$$

using $|\alpha| \geq 1/2$. We conclude the proof by taking the logarithm. □

## 4. A First Estimate

Let $n \geq 1$ and $p \geq 2$ be integers. For $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ we define

$$\Delta_p(a) = \prod_{t=1}^{p-1} |1 + \zeta^{ta_1} + \cdots + \zeta^{ta_n}| \quad \text{where} \quad \zeta = e^{2\pi\sqrt{-1}/p}. \tag{9}$$

If $p$ is a prime, then $\Delta_p(a)$ is the $\mathbb{Q}(\zeta)/\mathbb{Q}$ norm of the cyclotomic integer $1+\zeta^{a_1}+\cdots+\zeta^{a_n}$ up-to sign. We attach to $a$ the lacunary Laurent polynomial

$$P_a = 1 + X^{a_1} + \cdots + X^{a_n} \in \mathbb{Z}[X^{\pm 1}]. \tag{10}$$

Say $e = \max\{0, -a_1, \ldots, -a_n\} \geq 0$, then

$$X^e P_a = X^e + X^{e+a_1} + \cdots + X^{e+a_n} \tag{11}$$

is a polynomial with integral coefficients, non-zero constant term, and degree $d = \max\{a_i - a_j : 0 \le i, j \le n\} \le 2|a|$, where $a_0 = 0$. We write $\alpha_1, \dots, \alpha_d \in \mathbb{C}$ for the zeros of $X^e P_a$ with multiplicity, i.e. $X^e P_a = p_0(X - \alpha_1) \cdots (X - \alpha_d)$ where $p_0 \ge 1$ is the leading term of $P_a$. We note that $\alpha_i \ne 0, 1$ for all $i$.

Our goal in this section is to bound

$$\left| \frac{1}{p-1} \log \Delta_p(a) - \mathrm{m}(P_a) \right| \tag{12}$$

from above, here $\mathrm{m}(P_a) = \mathrm{m}(X^e P_a) = \log p_0 + \sum_{i=1}^{d} \log \max\{1, |\alpha_i|\}$ is the logarithmic Mahler measure of $P_a$.

As $\Delta_p(a)$ is essentially a resultant we can rewrite it as a product over the roots $\alpha_i$. This will allow us to express the difference (12) in terms of these roots.

In the next 4 lemmas we obtain several statements on the roots $\alpha_i$ in terms of $a \in \mathbb{Z}^n$.

**Lemma 6.** *We have* $\Delta_p(a) = p_0^p (n+1)^{-1} \prod_{i=1}^{d} |\alpha_i^p - 1|$.

*Proof.* A variant of this calculation can also be found in the proof of Duke's Theorem 3 [8]. We have

$$\Delta_p(a) = \prod_{t=1}^{p-1} |P_a(\zeta^t)| = p_0^{p-1} \prod_{i=1}^{d} \left( \prod_{t=1}^{p-1} |\zeta^t - \alpha_i| \right) = p_0^{p-1} \prod_{i=1}^{d} \left| \frac{1 - \alpha_i^p}{1 - \alpha_i} \right|.$$

The lemma follows since $p_0 \prod_{i=1}^{d} (1 - \alpha_i) = P_a(1) = n + 1$. □

Each $\alpha_i$ is an algebraic number with $D_i = [\mathbb{Q}(\alpha_i) : \mathbb{Q}] \le d$ whose height is bounded by the next lemma.

**Lemma 7.** *Let* $i \in \{1, \dots, d\}$, *then* $D_i h(\alpha_i) \le \mathrm{m}(P_a) \le \log(n+1)$.

*Proof.* Recall that $\alpha_i$ is a root of the polynomial in (11) which, by the Gauss Lemma, is divisible by the minimal polynomial $Q$ in $\mathbb{Z}[X]$ of $\alpha_i$. So $D_i h(\alpha_i) = \mathrm{m}(Q) \le \mathrm{m}(X^e P_a) = \mathrm{m}(P_a)$ as the logarithmic Mahler measure is additive and non-negative on $\mathbb{Z}[X] \smallsetminus \{0\}$. By Corollary 6, Chapter 3.4 [23] the Mahler measure $\mathrm{M}(P_a)$ is at most the euclidean norm of the coefficient vector of $P_a$. This gives $\mathrm{m}(P_a) \le \log(n+1)$. □

We now come to a lower bound for $|\alpha_i^p - 1|$ which is independent of $p$ under the assumption that $\alpha_i$ lies off the unit circle or is a root of unit of order not divisible by $p$.

**Lemma 8.** *Suppose* $a \ne 0$, *let* $i \in \{1, \dots, d\}$, *and let* $p \ge 1$ *be an integer.*

(i) *If* $|\alpha_i| \ne 1$, *then* $\log |\alpha_i^p - 1| \ge -18 \log(n+1)|a| \log(2|a|)$.
(ii) *If* $\alpha_i$ *is a root of unity and* $\alpha_i^p \ne 1$, *then* $\log |\alpha_i^p - 1| \ge -2 \log(2|a|)$.

*Proof.* Observe that $|\alpha_i| \ne 1$ implies $n \ge 2$. According to Lemmas 5 and 7 we have

$$\begin{aligned} \log |\alpha_i^p - 1| &\ge -1 - (D_i + 1) \log(2D_i) - 2(2D_i - 1) \log(n+1) \\ &\ge -(D_i + 1) \log(2D_i) - 4D_i \log(n+1). \end{aligned}$$

Now $D_i \le 2|a|$ by (11). The first part of the lemma follows from

$$(2|a| + 1) \log(4|a|) + 8|a| \log(n+1) \le 18 \log(n+1)|a| \log(2|a|).$$

The second part is more elementary. Let $m \ge 2$ be the multiplicative order of $\alpha_i^p$. If $m \ge 3$, then $|\alpha_i^p - 1| \ge \sin(2\pi/m) \ge 2/m$. The bound $|\alpha_i^p - 1| \ge 2/m$ certainly also holds

for $m = 2$. It is well-known that Euler's totient function $\varphi$ satisfies $\varphi(m) \geq \sqrt{m/2}$. As $\varphi(m) = [\mathbb{Q}(\alpha_i^p) : \mathbb{Q}] \leq D_i$ we find $m \leq 2D_i^2$. Hence $\log|\alpha_i^p - 1| \geq -2\log D_i \geq -2\log(2|a|)$, as $D_i \leq 2|a|$. □

This last lemma allows us to compare $\log|\alpha_i^p - 1|$ with the corresponding contribution $p\log\max\{1, |\alpha_i|\}$ in the logarithmic Mahler measure.

**Lemma 9.** *Suppose $a \neq 0$, let $i \in \{1, \dots, d\}$, and let $p \geq 1$ be an integer.*

(i) *If $|\alpha_i| \neq 1$, then*

$$\big|\log|\alpha_i^p - 1| - p\log\max\{1, |\alpha_i|\}\big| \leq 18\log(n+1)|a|\log(2|a|). \tag{13}$$

(ii) *If $\alpha_i$ is a root of unity and $\alpha_i^p \neq 1$, then*

$$\big|\log|\alpha_i^p - 1|\big| \leq 2\log(2|a|).$$

*Proof.* For the proof of part (i) let us first assume $|\alpha_i| < 1$. Then $|\alpha_i^p - 1| \leq 2$ and Lemma 8(i) yields $|\log|\alpha_i^p - 1|| \leq 18\log(n+1)|a|\log(2|a|)$, as desired.

If $|\alpha_i| > 1$ we use that $\alpha_i^{-1}$ is a root of $P_{-a}$. We obtain the same bound as before for $\big|\log|\alpha_i^{-p} - 1|\big| = \big|\log|\alpha_i^p - 1| - p\log|\alpha_i|\big|$ and this completes the proof of (i).

To prove (ii) we argue as in the case $|\alpha_i| < 1$ above but use Lemma 8(ii). □

Suppose for the moment that all $\alpha_i$ satisfy $|\alpha_i| \neq 1$ and for sake of simplicity also $p_0 = 1$. By Lemma 6 the bound given in part (i) of the last lemma leads to the bound

$$\frac{d|a|\log(2|a|)}{p} \leq \frac{2|a|^2\log(2|a|)}{p} \tag{14}$$

for (12) up-to a factor depending only on $n$. However, this estimate is not strong enough for our aims due to the contribution $|a|^2/p$.

To remedy this we begin by splitting up the roots $\alpha_i$ into two parts depending on a parameter $\lambda \geq 1$. The first part

$$\mathscr{B} = \mathscr{B}(p, a, \lambda) = \big\{i : |\alpha_i| < 1 \text{ and } |\alpha_i^p - 1| < p^{-\lambda}\big\} \cup \big\{i : |\alpha_i| > 1 \text{ and } |\alpha_i^{-p} - 1| < p^{-\lambda}\big\} \tag{15}$$

corresponds to those roots whose $p$-th power is excessively close to 1. The second part is the complement

$$\{1, \dots, d\} \smallsetminus \mathscr{B}.$$

Later we will bound the cardinality of $\mathscr{B}$.

**Proposition 10.** *Let $\lambda \geq 1$, let $a \in \mathbb{Z}^n \smallsetminus \{0\}$, and let $p \geq 1$ be an integer satisfying $|a| \leq p$. Suppose that the only roots of $P_a$ that lie on the unit circle are roots of unity of order not dividing $p$. Then $\Delta_p(a) \neq 0$ and*

$$\frac{1}{p-1}\log\Delta_p(a) = \mathrm{m}(P_a) + O\left(\frac{|a|\log(2p)}{p}(\lambda + \#\mathscr{B})\right) \tag{16}$$

*where the implied constant depends only on $n$.*

*Proof.* We recall Lemma 6, it implies $\Delta_p(a) \neq 0$ under the given circumstances. Let $\alpha_1, \dots, \alpha_d$ be the roots of $P_a$ with multiplicities, as above.

Say first $i \in \{1, \dots, d\} \smallsetminus \mathscr{B}$. If $|\alpha_i| < 1$, then $|\alpha_i^p - 1| \geq p^{-\lambda}$. Thus $\big|\log|\alpha_i^p - 1|\big| \leq \lambda\log(2p)$ since $\lambda\log(2p) \geq \log 2$. For $|\alpha_i| > 1$ we proceed similarly and obtain $\big|\log|\alpha_i^p -$

$1| - p\log|\alpha_i|\big| \le \lambda\log(2p)$. If $|\alpha_i| = 1$, then by hypothesis $\alpha_i$ is a root of unity whose order does not divide $p$, so Lemma 9(ii) implies $|\log|\alpha_i^p - 1|| \le 2\log(2|a|) \le 2\log(2p)$.

We recall $d \le 2|a|$ and sum over $\{1,\dots,d\} \smallsetminus \mathscr{B}$ to find

$$\sum_{\substack{i=1\\ i\notin\mathscr{B}}}^{d}\big|\log|\alpha_i^p - 1| - p\log\max\{1,|\alpha_i|\}\big| \le (d - \#\mathscr{B})\max\{\lambda\log(2p), 2\log(2p)\} \le 4|a|\log(2p)\lambda. \tag{17}$$

If $i \in \mathscr{B}$ then $|\alpha_i| \ne 1$. We apply Lemma 9(i) and use $|a| \le p$. The bound (13) holds for $\#\mathscr{B}$ roots and therefore

$$\sum_{i\in\mathscr{B}}\big|\log|\alpha_i^p - 1| - p\log\max\{1,|\alpha_i|\}\big| \le 18\log(n+1)|a|\log(2p)\#\mathscr{B}.$$

We combine this bound with (17) to obtain

$$\sum_{i=1}^{d}\big|\log|\alpha_i^p - 1| - p\log\max\{1,|\alpha_i|\}\big| \le 18\log(n+1)|a|\log(2p)(\lambda + \#\mathscr{B}). \tag{18}$$

The logarithmic Mahler measure of $P_a$ is $\log p_0 + \sum_{i=1}^{d}\log\max\{1,|\alpha_i|\}$ where $p_0 \ge 1$ is the leading term of $P_a$. We use Lemma 6 and apply the triangle inequality to find that $|\frac{1}{p-1}\log\Delta_p(a) - \mathrm{m}(P_a)|$ is at most

$$\frac{1}{p-1}\left|\log\left(\frac{p_0^p}{n+1}\right) - (p-1)\log p_0\right| + \frac{1}{p-1}\sum_{i=1}^{d}|\log|\alpha_i^p - 1| - (p-1)\log\max\{1,|\alpha_i|\}|$$
$$\le \frac{\log(n+1)}{p-1} + 18\log(n+1)\frac{|a|\log(2p)}{p-1}(\lambda + \#\mathscr{B}) + \frac{1}{p-1}\mathrm{m}(P_a)$$

where we used (18). From Lemma 7 we deduce $\mathrm{m}(P_a) \le \log(n+1)$. So (16) holds true. □

If we ignore for the moment all logarithmic contributions, then we have traded in $d$ in (14) for $\lambda + \#\mathscr{B}$ in (16).

Before continuing we make two elementary, but important, observations on symmetry properties of $\Delta_p(a)$ when $p$ is a prime.

**Lemma 11.** *Let $p$ be a prime and let $a \in \mathbb{Z}^n$ be arbitrary.*

(i) *If $a' \in \mathbb{Z}^n$ with $a \equiv a' \pmod p$, then $\Delta_p(a) = \Delta_p(a')$.*
(ii) *If $t \in \mathbb{Z}$ with $p \nmid t$, then $\Delta_p(a) = \Delta_p(ta)$.*

*Proof.* Part (i) follows using the definition (9) and $\zeta^p = 1$. For part (ii) observe that $\zeta \mapsto \zeta^t$ permutes the factors in (9) since $p \nmid t$. □

Using this lemma we will transform $a' = ta - b$ with $p \nmid t$ and $b \in p\mathbb{Z}^n$ such that $|a'|$ is small compared to $p$. This will be done using Dirichlet's Theorem from diophantine approximation. A theorem of Bombieri-Masser-Zannier leads to a criterion that rules out that $P_{a'}$ has roots on the unit circle of infinite order. This opens the door to applying the previous proposition.

In a final step we will need a strong upper bound for $\mathscr{B}$ for a sufficiently large but fixed $\lambda$. This is where counting rational points close to a definable sets comes into play.

## 5. Lacunary Polynomials with Roots off the Unit Circle

Say $n \geq 2$. In this section we investigate a condition on $a \in \mathbb{Z}^n$ such that $P_a$, as defined in (10), does not vanish at any point of $S^1 \smallsetminus \mu_\infty$. It will prove useful to restrict $a$ to a subgroup $\Omega \subseteq \mathbb{Z}^n$ and we will introduce a condition on $\Omega$ that ensures that $P_a$ does not have any roots in $S^1 \smallsetminus \mu_\infty$ for $a \in \Omega$ in general position.

Our condition is based on a theorem of Bombieri, Masser, and Zannier [5] on unlikely intersections in the algebraic torus.

We also make use of (very rudimentary) tropical geometry. Say $K$ is the field of Puiseux series over $\mathbb{C}$; it is algebraically closed and equipped with a surjective valuation $\operatorname{ord} : K \to \mathbb{Q} \cup \{\infty\}$. Let $\mathcal{X}$ be an irreducible subvariety defined over $K$ of the algebraic torus $\mathbb{G}_{\mathrm{m}}^n$. The tropical variety $\operatorname{Trop}(\mathcal{X})$ of $\mathcal{X}$ is the closure in $\mathbb{R}^n$ of

$$\{(\operatorname{ord}(x_1), \dots, \operatorname{ord}(x_n)) : (x_1, \dots, x_n) \in \mathcal{X}(K)\}.$$

We need the following two basic facts.

First, if $\mathcal{Y} \subseteq \mathcal{X}$ is an irreducible subvariety defined over $K$, then $\operatorname{Trop}(\mathcal{Y}) \subseteq \operatorname{Trop}(\mathcal{X})$; this follows directly from the definition.

Second, if $r = \dim \mathcal{X} \geq 1$ and after permuting coordinates, the projection of $\operatorname{Trop}(\mathcal{X})$ to the first $r$ coordinates of $\mathbb{R}^n$ contains $\mathbb{Q}^r$. We prove this using basic algebraic geometry. After permuting coordinates the projection $\pi : \mathcal{X}(K) \to \mathbb{G}_{\mathrm{m}}^r(K)$ onto the first $r$ coordinates contains a Zariski open and dense subset of $\mathbb{G}_{\mathrm{m}}^r$. There exists a polynomial $P \in K[X_1^{\pm 1}, \dots, X_r^{\pm 1}] \smallsetminus \{0\}$ such that any point of $\mathbb{G}_{\mathrm{m}}^r(K)$ outside of the zero locus of $P$ lies in the image of $\pi$. Let $(a_1, \dots, a_n) \in \mathbb{Q}^r$ be arbitrary. For sufficiently general $(c_1, \dots, c_r) \in \mathbb{G}_{\mathrm{m}}^r(\mathbb{C})$ the polynomial $P$ does not vanish at $(c_1 T^{a_1}, \dots, c_r T^{a_r}) \in \mathbb{G}_{\mathrm{m}}^r(K)$. This point has a pre-image under $\pi$ in $\mathcal{X}(K)$ and the valuation of its first $r$ coordinates are $a_1, \dots, a_r$. This yields our claim.

Einsiedler, Kapranov and Lind's [10] Theorem 2.2.5 on the structure of $\operatorname{Trop}(\mathcal{X})$ can be used instead of this second property in the proof of Lemma 12 below.

We write $\langle \cdot, \cdot \rangle$ for the standard scalar product on $\mathbb{R}^n$. If $\Omega$ is a subgroup of $\mathbb{Z}^n$, then we set

$$\Omega^\perp = \{a \in \mathbb{Z}^n : \langle a, \omega \rangle = 0 \text{ for all } \omega \in \Omega\}.$$

We write $e_1, \dots, e_n$ for the standard basis elements of $\mathbb{R}^n$ augmented by $e_0 = 0$.

**Lemma 12.** *Let $\Omega \subseteq \mathbb{Z}^n$ be a subgroup of rank $m \geq 2$ for which the following property holds. If $(\alpha, \beta) \in \mathbb{Z}^2 \smallsetminus \{0\}$ and if $i, j, k, l \in \{0, \dots, n\}$ are pairwise distinct with $v = \alpha(e_i - e_j) + \beta(e_k - e_l)$, then $\Omega \not\subseteq (v\mathbb{Z})^\perp$. Then there exist finitely many subgroups $\Omega_1, \dots, \Omega_N \subseteq \Omega$ of rank at most $m - 1$ such that if $a \in \Omega \smallsetminus \bigcup_{i=1}^N \Omega_i$ then $P_a$ does not vanish at any point of $S^1 \smallsetminus \mu_\infty$.*

*Proof.* We consider an irreducible component $\mathcal{X} \subseteq \mathbb{G}_{\mathrm{m}}^n$ of the zero set of

$$1 + X_1 + \cdots + X_n \quad \text{and} \quad 1 + X_1^{-1} + \cdots + X_n^{-1}. \tag{19}$$

Then $\dim \mathcal{X} = n - 2$ as these two polynomials are coprime in $\mathbb{C}[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$.

Say $a = (a_1, \dots, a_n) \in \Omega$ such that $P_a$ has a root $z \in S^1 \smallsetminus \mu_\infty$. Then $1 + z^{a_1} + \cdots + z^{a_n} = 0$ by definition and after applying complex conjugation we find

$$1 + z^{-a_1} + \cdots + z^{-a_n} = 0.$$

So $z^a = (z^{a_1}, \dots, z^{a_n}) \in \mathcal{X}(\mathbb{C})$ for one of the irreducible components above.

But $z^a$ also lies in an algebraic subgroup of $\mathbb{G}_{\mathrm{m}}^n$ of dimension 1. According to Bombieri, Masser, and Zannier's Theorem 1.7 [5] there are two cases. Either $z^a$ lies in a finite set that depends only on $\mathcal{X}$, and hence only on $n$, or $z^a \in \mathcal{H}(\mathbb{C})$ where $\mathcal{H} \subseteq \mathbb{G}_{\mathrm{m}}^n$ is an irreducible component of an algebraic subgroup with

$$\dim_{z^a} \mathcal{X} \cap \mathcal{H} \geq \max\{1, \dim \mathcal{X} + \dim \mathcal{H} - n + 1\} = \max\{1, \dim \mathcal{H} - 1\}.$$

Moreover, in the second case $\mathcal{H}$ comes from a finite set that depends only on $n$, cf. the first paragraph of the proof of Theorem 1.7 [5] on page 26.

In the first case we claim that $a$ must lie in one of finitely many subgroups of $\Omega$ of rank $1 \leq m-1$. Indeed, we may assume $a \neq 0$. If $z' \in S^1 \smallsetminus \mu_\infty$ is a root of some $P_{a'}$ with $a' \in \Omega$ and $z^a = z'^{a'}$, then $a$ and $a'$ are linearly dependent as $z'$ is not a root of unity. Our claim follows as there are only finitely many possible $z^a$ in this case. We add these rank 1 subgroups to our collection of $\Omega_i$.

In the second case there is an irreducible component $\mathcal{Y} \subseteq \mathcal{X} \cap \mathcal{H}$ of positive dimension at least $\dim \mathcal{H} - 1$ that contains $z^a$. In this case $n \geq 3$. We recall that algebraic subgroups of $\mathbb{G}_m^n$ are in bijection with subgroups of $\mathbb{Z}^n$, see Theorem 3.2.19 [4] for details. Let $\Lambda \subseteq \mathbb{Z}^n$ be a subgroup from a finite set depending only on $n$ with rank $r = n - \dim \mathcal{H}$ such that $\mathcal{H}$ is contained in the algebraic subgroup defined by all

$$X_1^{b_1} \cdots X_n^{b_n} - 1 \quad \text{where} \quad (b_1, \ldots, b_n) \in \Lambda. \tag{20}$$

Hence $z^{\langle a,b\rangle} = 1$ for all $b \in \Lambda$. As $z$ is not a root of unity we find $a \in \Lambda^\perp$.

We would like to add $\Omega \cap \Lambda^\perp$ to our list of $\Omega_i$. However, we must ensure that its rank is at most $m-1$. Once this is done, our proof is complete.

Suppose the rank does not drop, then $[\Omega : \Omega \cap \Lambda^\perp]\Omega \subseteq \Lambda^\perp$ and hence $\Omega \subseteq \Lambda^\perp$ because $\Lambda^\perp$ is primitive. We now derive a contradiction from this situation by analyzing $\Lambda$.

Since all monomials (20) vanish on $\mathcal{H}$ we find that $\mathrm{Trop}(\mathcal{H})$ lies in $\Lambda^\perp\mathbb{R}$, the vector subspace of $\mathbb{R}^n$ generated by $\Lambda^\perp$. We also need to study $\mathrm{Trop}(\mathcal{X})$. Say $(x_1, \ldots, x_n) \in \mathcal{X}(\mathbb{C})$. Since it is a zero of the first polynomial in (19) and by the ultrametric triangle inequality the minimum among $0, \mathrm{ord}(x_1), \ldots, \mathrm{ord}(x_n)$ is attained twice. The same argument applied to the second polynomial in (19) shows that the maximum is attained twice. Hence $\mathrm{Trop}(\mathcal{X})$ is contained in the finite union of the codimension 2 vector subspaces of $\mathbb{R}^n$ defined by relations

$$\mathrm{ord}(x_i) = \mathrm{ord}(x_j), \quad \mathrm{ord}(x_k) = \mathrm{ord}(x_l) \quad \text{with} \quad \#\{i,j,k,l\} = 4$$

and

$$\mathrm{ord}(x_i) = \mathrm{ord}(x_j), \quad \mathrm{ord}(x_k) = 0 \quad \text{with} \quad \#\{i,j,k\} = 3.$$

By the discussion before this lemma, $\mathrm{Trop}(\mathcal{Y}) \subseteq \mathrm{Trop}(\mathcal{X}) \cap \mathrm{Trop}(\mathcal{H}) \subseteq \mathrm{Trop}(\mathcal{X}) \cap \Lambda^\perp\mathbb{R}$. Moreover, the projection of $\mathrm{Trop}(\mathcal{Y})$ to some choice of $\dim \mathcal{Y}$ distinct coordinates of $\mathbb{R}^n$ contains $\mathbb{Q}^{\dim \mathcal{Y}}$. So $\Lambda^\perp\mathbb{R}$ intersected with one of the codimension 2 subspaces mentioned above must have dimension at least $\dim \mathcal{Y} \geq \dim \mathcal{H} - 1 = n - r - 1$. Therefore, there exists $(\alpha, \beta) \in \mathbb{Z}^2 \smallsetminus \{0\}$ and pairwise distinct $i,j,k,l \in \{0, \ldots, n\}$ with $v = \alpha(e_i - e_j) + \beta(e_k - e_l) \in \Lambda$. Recall that $\Omega \subseteq \Lambda^\perp$. So $\Omega$ lies in the orthogonal complement of $v$, which contradicts the hypothesis of the lemma. □

Suppose $n \geq 2$, let $\Omega \subseteq \mathbb{Z}^n$ be a subgroup of rank at least 2 and let $a \in \mathbb{Z}^n$. For a prime $p$ we define

$$\rho_p(a;\Omega) = \inf\{|\omega| : \omega \in \Omega \smallsetminus \{0\} \text{ and } \langle \omega, a\rangle \equiv 0 \pmod p\} \tag{21}$$

this is a well-defined real number as the set is non-empty.

**Proposition 13.** *Let $\Omega \subseteq \mathbb{Z}^n$ be a subgroup of rank $m \geq 2$ that satisfies the following hypothesis. If $(\alpha, \beta) \in \mathbb{Z}^2 \smallsetminus \{0\}$ and if $i, j, k, l \in \{0, \dots, n\}$ are pairwise distinct with $v = \alpha(e_i - e_j) + \beta(e_k - e_l)$, then $\Omega \not\subseteq (v\mathbb{Z})^\perp$. Then there exists a constant $c = c(\Omega) \geq 1$ with the following property. Say $a \in \Omega$ and let $p$ be a prime with $\rho_p(a;\Omega) \geq c$. Then there exist $t \in \mathbb{Z}$ with $p \nmid t$ and $\omega \in \Omega$ such that $a' = ta - p\omega \neq 0$,*

(i) *we have $|a'| \leq cp^{1-1/m}$, and*
(ii) *the Laurent polynomial $P_{a'} \in \mathbb{Z}[X^{\pm 1}]$ does not vanish at any point of $S^1 \smallsetminus \mu_\infty$.*

*Proof.* The proposition follows from combining Lemma 12 with Dirichlet's Theorem from diophantine approximation. Indeed, we let $\Omega_1, \dots, \Omega_N$ be the subgroups of $\Omega$ from this lemma. If $N = 0$ we set $\Omega_1 = \{0\}$. We will see how to choose $c$ below.

We fix a basis $(\omega_1, \dots, \omega_m)$ of the abelian group $\Omega$. Then $a = \nu_1\omega_1 + \cdots + \nu_m\omega_m$, where $\nu_1, \dots, \nu_m \in \mathbb{R}$ are unique.

If $p \geq 3$, then Dirichlet's Theorem, cf. Theorem 1B [24], applied to $\nu_1/p, \dots, \nu_m/p$, and $p - 1 > 1$ yields $t, \nu_1', \dots, \nu_m' \in \mathbb{Z}$ such that $1 \leq t \leq p-1$ and $|t\nu_i/p - \nu_i'| \leq (p-1)^{-1/m}$. The same conclusion holds for $p = 2$. We set $\omega = \sum_{i=1}^m \nu_i'\omega_i \in \Omega$. Then $|a'/p| \leq (|\omega_1| + \cdots + |\omega_m|)(p-1)^{-1/m} \leq cp^{-1/m}$ where $a' = ta - p\omega$ for $c$ large enough. This yields part (i).

As each $\Omega_i$ has rank at most $m - 1$ we have $\Omega \cap (\Omega_i)^\perp \neq 0$ for all $i$. For each $i$ we fix a non-zero $\omega^* \in \Omega \cap (\Omega_i)^\perp$ of minimal norm. If $\langle \omega^*, ta - p\omega\rangle = 0$, then $\langle \omega^*, a\rangle \equiv 0 \pmod p$, since $p \nmid t$. So $|\omega^*| \geq \rho_p(a;\Omega) \geq c$ by hypothesis. We can avoid this outcome by fixing $c$ large in terms of the $\Omega \cap (\Omega_i)^\perp$. Thus $\langle \omega^*, a'\rangle \neq 0$. This implies $a' \notin \Omega_i$ for all $1 \leq i \leq N$ and in particular $a' \neq 0$. Part (ii) follows from the conclusion of Lemma 12. □

## 6. Rational Points Close to a Definable Set

In this section we prove Theorem 3. To do this we temporarily adopt the language of o-minimal structures. Our main reference is van den Dries' book [27] and his paper with Miller [28]. We work exclusively with the o-minimal structure $\mathbb{R}_{\text{an}}$ of restricted analytic functions. It contains the graph of any function $[0,1]^n \to \mathbb{R}$ that is the restriction of an analytic function $\mathbb{R}^n \to \mathbb{R}$.

The main technical tool in this section is a result of the author [12] which we cite in a special case below. We retain much of the notation used in the said reference. Roughly speaking, the result gives an upper bound for the number of rational points of bounded height that are close to a subset of $\mathbb{R}^n$ that is definable in $\mathbb{R}_{\text{an}}$. Note that $\mathbb{R}_{\text{an}}$ is a polynomially bounded o-minimal structure as required by this reference.

For any subset $Z \subseteq \mathbb{R}^n$ we write $Z^{\text{alg}}$ for the union of all connected, semi-algebraic sets that are contained completely in $Z$. For $\epsilon > 0$ we define $\mathcal{N}(Z, \epsilon)$ to be the set of $y \in \mathbb{R}^n$ for which $|x - y| < \epsilon$ for some $x \in Z$. We recall that the height $H(\cdot)$ was defined in Section 2.

**Theorem 14** (Theorem 2 [12]). *Let $Z \subseteq \mathbb{R}^n$ be a closed set that is definable in $\mathbb{R}_{\mathrm{an}}$ and let $\epsilon > 0$. There exist $c = c(Z, \epsilon) \geq 1$ and $\theta = \theta(Z, \epsilon) \in (0, 1]$ such that if $\lambda \geq \theta^{-1}$ then*

$$\#\left\{q \in \mathbb{Q}^n \smallsetminus \mathcal{N}(Z^{\mathrm{alg}}, T^{-\theta\lambda}) : H(q) \leq T \text{ and there is } x \in Z \text{ with } |x - q| < T^{-\lambda}\right\} \leq cT^{\epsilon}$$

*for all $T \geq 1$.*

*Proof of Theorem 3.* For $n = 1$ the theorem follows with $\lambda = 1$ and taking $c$ sufficiently large. Our proof is by induction on $n$ and we suppose $n \geq 2$. We will choose $c \geq 1$ and $\lambda \geq 1$ in terms of $n$ and $\epsilon$ during the argument.

Let

$$Z = \left\{(x_1, \ldots, x_n) \in [0, 1]^n : 1 + e^{2\pi\sqrt{-1}x_1} + \cdots + e^{2\pi\sqrt{-1}x_n} = 0\right\}$$

which is compact and definable in $\mathbb{R}_{\mathrm{an}}$.

Let us write $\zeta_j = e^{2\pi\sqrt{-1}q_j}$ for $j \in \{1, \ldots, n\}$ with $q_j \in \frac{1}{p}\mathbb{Z} \cap [0, 1)$. Say $t$ is as in the set (8). For convenience, we identify it with its representative in $\{0, \ldots, p-1\}$. Then

$$\left|1 + \zeta_1^t + \cdots + \zeta_n^t\right| < c^{-1}p^{-\lambda}, \tag{22}$$

$(\zeta_1, \ldots, \zeta_n)$ has precise order $p$, and $t \neq 0$. We claim that $\tilde{q}_t = (tq_1 - \lfloor tq_1 \rfloor, \ldots, tq_n - \lfloor tq_n \rfloor) \in \frac{1}{p}\mathbb{Z}^n \cap [0, 1)^n$ lies close to $Z$. Indeed, a suitable version of Łojasiewicz's Inequality, see 4.14.(2) [28], implies that the distance of this point to $Z$ is at most

$$c_1 \left|1 + e^{2\pi\sqrt{-1}tq_1} + \cdots + e^{2\pi\sqrt{-1}tq_n}\right|^{\delta} \leq c_1 c^{-\delta} p^{-\lambda\delta} \leq c_1 c^{-\delta}.$$

where $c_1 > 0$ and $\delta > 0$ depend only on $Z$. We may assume $c_1 c^{-\delta} < 1$, so

$$|\tilde{q}_t - x| < p^{-\lambda\delta} \quad \text{for some } x \in Z. \tag{23}$$

The vectors $\tilde{q}_0, \ldots, \tilde{q}_{p-1}$ are pairwise distinct. So it is enough to bound the number of $\tilde{q}_t$ with (23).

If $\lambda$ is sufficiently large, then $\lambda\delta \geq \theta^{-1}$ where $\theta$ is provided by Theorem 14 applied to $Z$ and $\epsilon$. So there are at most $cp^{\epsilon}$ many $\tilde{q}_t$ that are not in the $p^{-\theta\lambda\delta}$-tube around $Z^{\mathrm{alg}}$.

To prove (8) we need only consider those $t$ with $|\tilde{q}_t - x'| < p^{-\theta\lambda\delta}$ for some $x' = (x_1', \ldots, x_n') \in Z^{\mathrm{alg}}$. The algebraic locus $Z^{\mathrm{alg}}$ is well understood; see Ax's work [2] and how it is applied for example in the proof of Theorem 7 [12]. There exists $\emptyset \neq J \subsetneq \{1, \ldots, n\}$ such that $1 + \sum_{j \in J} e^{2\pi\sqrt{-1}x_j'} = 0$. We subtract this from the partial sum over the coordinates of $t(q_1, \ldots, q_n)$ and get

$$1 + \sum_{j \in J} \zeta_j^t = \sum_{j \in J} (e^{2\pi\sqrt{-1}tq_j} - e^{2\pi\sqrt{-1}x_j'}).$$

Thus

$$\left|1 + \sum_{j \in J} \zeta_j^t\right| \leq \sum_{j \in J} \left|e^{2\pi\sqrt{-1}(tq_j - \lfloor tq_j \rfloor)} - e^{2\pi\sqrt{-1}x_j'}\right| \leq 2\pi(n-1)|\tilde{q}_t - x'|.$$

Hence there is a constant $c_2 > 0$ depending only on $n$ with

$$\left|1 + \sum_{j \in J} \zeta_j^t\right| < c_2 p^{-\theta\lambda\delta}.$$

Recall $\#J \leq n-1$. Now suppose $c' > 0$ and $\lambda' > 0$ are the constants from this theorem applied by induction to the terms in $J$. We are free to assume that $\lambda$ satisfies $2^{\theta\lambda\delta/2} \geq c_2 c'$ and $\theta\lambda\delta \geq 2\lambda'$. Then $c_2 p^{-\theta\lambda\delta} \leq c_2 2^{-\theta\lambda\delta/2} p^{-\theta\lambda\delta/2} \leq c'^{-1} p^{-\lambda'}$ as $p \geq 2$. So

$$\left|1 + \sum_{j\in J} \zeta_j^t\right| < c'^{-1} p^{-\lambda'}.$$

If $1 + \sum_{j\in J} \zeta_j \neq 0$, then (8) follows from induction.

On the other hand, if this sum vanishes, then its Galois conjugates $1 + \sum_{j\in J} \zeta_j^t$ vanish for all $t \in \mathbb{F}_p^\times$. By hypothesis, the normalized complementary sum

$$1 + \sum_{j\in I\smallsetminus\{j_0\}} \zeta_j \zeta_{j_0}^{-1}$$

is non-zero; here $I = \{1,\dots,n\} \smallsetminus J$ and $j_0 \in I$. We may apply induction since $|I| - 1 \leq n-2$. Using (22) we find

$$\left|1 + \sum_{j\in I\smallsetminus\{j_0\}} (\zeta_j\zeta_{j_0}^{-1})^t\right| = \left|1 + \zeta_1^t + \cdots + \zeta_n^t\right| < c^{-1} p^{-\lambda}.$$

and there are at most $cp^\epsilon$ possibilities for $t$. □

## 7. Counting Small Sums of Roots of Unity

Let $P_a$ be a lacunary Laurent polynomial as in (10) with $a \in \mathbb{Z}^n$ where $n \geq 1$. The goal of this section is to bound the number of roots $\alpha$ of $P_a$ coming from $\mathscr{B} = \mathscr{B}(p, a, \lambda)$ defined in (15). If $\alpha^p$ is close to 1, then $\alpha$ is close to a root of unity $\zeta$ with $\zeta^p = 1$. So $|P_a(\zeta)|$ will be small. Thus $1 + \zeta^{a_1} + \cdots + \zeta^{a_n}$ is small in modulus where $a = (a_1,\dots,a_n)$. This is where the counting result proved in Section 6 comes into play.

We make the first part of this approach precise in the next lemma.

**Lemma 15.** *Suppose $\alpha = re^{2\pi\sqrt{-1}\vartheta}$ with $r \in (0,1]$ and $\vartheta \in [0,1)$. If $p \geq 2$ is an integer with $|\alpha^p - 1| \leq 1/2$, then there exists $t \in \{0,\dots,p\}$ such that*

$$\left|\vartheta - \frac{t}{p}\right| \leq \frac{1}{4\sqrt{2}} |\alpha^p - 1|. \tag{24}$$

*If in addition $a \in \mathbb{Z}^n$ and $P_a(\alpha) = 0$, then*

$$\left|P_a\left(e^{2\pi\sqrt{-1}t/p}\right)\right| \leq 5n|a||\alpha^p - 1|. \tag{25}$$

*Proof.* Observe that $|z-1| \geq |z|^{1/2}|z/|z| - 1|$ for all $z \in \mathbb{C} \smallsetminus \{0\}$, see Lemma 11.6.1 [22]. We substitute $z = \alpha^p$ to find $|\alpha^p - 1| \geq r^{p/2}|e^{2\pi\sqrt{-1}\vartheta p} - 1|$. Now $1 - r^p \leq |r^p - 1| \leq |\alpha^p - 1|$, so $r^p \geq 1 - |\alpha^p - 1| \geq 1/2$ by hypothesis. We find

$$\left|e^{2\pi\sqrt{-1}\vartheta p} - 1\right| \leq \sqrt{2}|\alpha^p - 1|. \tag{26}$$

Let $t$ be an integer with $|\vartheta p - t| \leq 1/2$. Then $t \in \{0,\dots,p\}$ as $\vartheta \in [0,1)$. So

$$\left|e^{2\pi\sqrt{-1}\vartheta p} - 1\right| = \left|e^{2\pi\sqrt{-1}(\vartheta p - t)} - 1\right| \geq 4|\vartheta p - t| \tag{27}$$

by elementary geometry. Combining (26) with (27) and dividing by $p \geq 2$ yields (24).

To prove the second claim we set $\xi = e^{2\pi\sqrt{-1}t/p}$ and estimate

$$|\alpha - \xi| = |re^{2\pi\sqrt{-1}\vartheta} - \xi| \le |r-1| + |e^{2\pi\sqrt{-1}\vartheta} - \xi| = |r-1| + |e^{2\pi\sqrt{-1}(\vartheta - t/p)} - 1|$$

$$\le |\alpha^p - 1| + 2\pi|\vartheta - t/p| \le (1 + \pi/\sqrt{8})|\alpha^p - 1|; \tag{28}$$

where we used $|r-1| \le |r^p - 1| \le |\alpha^p - 1|$.

We fix $e \in \mathbb{Z}$ such that $X^e P_a(X)$ is a polynomial with non-zero constant term. Then

$$|P_a(\xi)| = |\xi^e P_a(\xi) - \alpha^e P_a(\alpha)| \le \sum_{k=0}^{n} |\xi^{a_k+e} - \alpha^{a_k+e}|$$

here $a = (a_1, \dots, a_n)$ and $a_0 = 0$. Some $a_k + e$ vanishes and we use $|\xi| = 1$ and $|\alpha| \le 1$ to find

$$|P_a(\xi)| \le n \max_{0 \le k \le n} \{a_k + e\} |\xi - \alpha| \le 2n|a||\xi - \alpha|.$$

We recall (28) to obtain (25). □

Next we show that many elements in $\mathscr{B}$ will lead to many different roots of unity as given by the lemma above. The reason for this is that roots of lacunary polynomials are nearly angularly equidistributed by a result of Hayman, known already to Biernacki.

**Lemma 16.** *Let $a \in \mathbb{Z}^n$ and suppose $p \ge 2$ is an integer with $|a| \le p$. If $\lambda \ge 1$, then*

$$\#\mathscr{B} \le 12n \#\{\zeta \in \mu_p : |P_a(\zeta)| < 5n|a|p^{-\lambda}\}.$$

*Proof.* We may assume $a \neq 0$. Let us partition $\mathscr{B} = \mathscr{B}(p, a, \lambda)$ into $\mathscr{B}_{<1} = \{i \in \mathscr{B} : |\alpha_i| < 1\}$ and $\mathscr{B}_{>1} = \{i \in \mathscr{B} : |\alpha_i| > 1\}$.

We construct a map

$$\psi_{<1} : \mathscr{B}_{<1} \to \{0, \dots, p\}$$

in the following manner. If $i \in \mathscr{B}_{<1}$, then $\alpha_i = |\alpha_i| e^{2\pi\sqrt{-1}\vartheta}$ for $\vartheta \in [0,1)$, which depends on $i$, and we have $|\alpha_i^p - 1| < p^{-\lambda} \le 1/2$. Lemma 15 yields $t \in \{0, \dots, p\}$ with $|\vartheta - t/p| \le |\alpha_i^p - 1|/\sqrt{32} < p^{-\lambda}/\sqrt{32}$. We set $\psi(i) = t$.

We define $\psi_{>1} : \mathscr{B}_{>1} \to \{0, \dots, p\}$ in the same spirit. For if $i \in \mathscr{B}_{>1}$, then $|\alpha_i| > 1$ and there is $\vartheta \in [0,1)$ such that $\alpha_i = |\alpha_i| e^{-2\pi\sqrt{-1}\vartheta}$. We apply the said lemma to $\alpha_i^{-1}$ and $P_{-a}$ to obtain $\psi(i) \in \{0, \dots, p\}$ with $|\vartheta - \psi(i)/p| < p^{-\lambda}/\sqrt{32}$.

For $i \in \mathscr{B}_{<1}$ we get

$$\left|P_a(\xi^{\psi(i)})\right| < 5n|a|p^{-\lambda}$$

with $\xi = e^{2\pi\sqrt{-1}/p}$. If $i \in \mathscr{B}_{>1}$, the same bound holds for $|P_{-a}(\xi^{\psi(i)})| = |P_a(\xi^{-\psi(i)})|$.

Now $\#\mathscr{B} \le 2\#\mathscr{B}_{<1}$ or $\#\mathscr{B} \le 2\#\mathscr{B}_{>1}$. We assume the former, the latter case is dealt with similarly.

Let us fix $e \in \mathbb{Z}$ such that $Q = X^e P(X)$ is a polynomial with non-zero constant term. Then $\deg Q \le 2|a|$ and $Q$ has at most $n+1$ terms. Elements of $\mathscr{B}_{<1}$ that are in a fiber of $\psi$ come from roots of $Q$ that are in an open sector of the complex plane with angle $4\pi p^{-\lambda}/\sqrt{32} = \pi p^{-\lambda}/\sqrt{2}$. By Proposition 11.2.4 [22], such an open sector contains at most

$$\frac{\deg(Q)}{2\sqrt{2}p^{\lambda}} + n + 1 \le \frac{2|a|}{2\sqrt{2}p^{\lambda}} + n + 1 \le \frac{|a|}{\sqrt{2}p} + n + 1 \le \frac{1}{\sqrt{2}} + n + 1 \le 3n$$

roots of $Q$, counting multiplicities; here we used $\lambda \geq 1$ and $|a| \leq p$. Therefore,

$$\#\mathscr{B}_{<1} \leq 3n\#\left\{0 \leq t \leq p : |P_a(\xi^t)| < 5n|a|p^{-\lambda}\right\}$$

We must compensate for the fact that we may be counting $1 = \xi^0 = \xi^p$ twice, so

$$\#\mathscr{B}_{<1} \leq 6n\#\left\{0 \leq t \leq p-1 : |P_a(\xi^t)| < 5n|a|p^{-\lambda}\right\}.$$

The lemma now follows from $\#\mathscr{B} \leq 2\#\mathscr{B}_{<1}$. □

**Proposition 17.** *For all $\epsilon > 0$ there exist constants $c = c(n,\epsilon) \geq 1$ and $\lambda = \lambda(n,\epsilon) \geq 1$ with the following property. Let $a \in \mathbb{Z}^n$ and let $p$ be a prime with $|a| \leq p$ such that $P_a$ does not vanish at any point of $\mu_p$. Then*

$$\#\mathscr{B}(p,a,\lambda) \leq cp^{\epsilon}.$$

*Proof.* Say $c'$ and $\lambda'$ are from Theorem 3. We apply Lemma 16 to a fixed $\lambda \geq \lambda' + 1 \geq 2$ that satisfies $2^{\lambda-\lambda'-1} \geq 5nc'$ and hence $p^{\lambda} \geq 5nc'p^{\lambda'+1}$.

Say $\xi = e^{2\pi\sqrt{-1}/p}$ and $a = (a_1,\dots,a_n)$. Now any $\zeta \in \mu_p$ with $|P_a(\zeta)| < 5n|a|p^{-\lambda}$ equals $\xi^t$ for some $t \in \mathbb{F}_p$ and

$$\left|1 + \xi^{a_1 t} + \cdots + \xi^{a_n t}\right| < 5n|a|p^{-\lambda} \leq {c'}^{-1}\frac{|a|}{p}p^{-\lambda'} \leq {c'}^{-1}p^{-\lambda'},$$

as $|a| \leq p$. Recall that $1 + \xi^{a_1} + \cdots + \xi^{a_n} = P_a(\xi) \neq 0$ for $a$ as in the hypothesis. So by Theorem 3 the number of possible $t$ is at most $cp^{\epsilon}$ for $c$ sufficiently large in terms of $n$ and $\epsilon$. □

## 8. Main Technical Result

Suppose $n \geq 2$, let $\Omega \subseteq \mathbb{Z}^n$ be a subgroup of rank at least 2, and let $a \in \mathbb{Z}^n$. We set

$$\rho(a;\Omega) = \inf\{|\omega| : \omega \in \Omega \smallsetminus \{0\} \text{ and } \langle \omega, a\rangle = 0\} \tag{29}$$

and recall (21).

**Proposition 18.** *Let $\Omega \subseteq \mathbb{Z}^n$ be a subgroup of rank $m \geq 2$ that satisfies the hypothesis in Proposition 13. There exists a constant $c = C(\Omega) \geq 1$ with the following property. Say $a \in \Omega$ and let $p$ be a prime with $\rho_p(a;\Omega) \geq c$. There exists $a' \in \Omega \smallsetminus \{0\}$ with $a' = at - p\omega$, where $t \in \mathbb{Z}$ is coprime to $p$ and $\omega \in \Omega$, such that $|a'| \leq cp^{1-1/m}, \Delta_p(a') = \Delta_p(a) \neq 0$,*

$$\rho(a';\Omega) \geq \rho_p(a;\Omega), \quad \text{and} \quad \frac{1}{p-1}\log\Delta_p(a') = \mathrm{m}(P_{a'}) + O\left(p^{-\frac{1}{2m}}\right); \tag{30}$$

*here the constant implicit in $O(\cdot)$ depends only on $\Omega$.*

*Proof.* Let $\omega_1 \in \Omega \smallsetminus \{0\}$, then $\langle p\omega_1, a\rangle \equiv 0 \pmod p$, hence $\rho_p(a;\Omega) \leq p|\omega_1|$. By increasing $c$ we may assume that $p$ is larger than a prescribed constant. Say $c_1 \geq 1$ is the constant from Proposition 13; we may suppose $c \geq \max\{3, c_1\}$. There is $t \in \mathbb{Z}$ not divisible by $p$ and $\omega \in \Omega$ such that $a' = ta - p\omega$ satisfies $0 < |a'| \leq c_1 p^{1-1/m}$ and the only roots of $P_{a'}$ on the unit circle are roots of unity. We may assume $|a'| < (p-1)/2$ by increasing $c$.

Suppose $\langle \omega_0, a'\rangle = 0$ with $\omega_0 \in \Omega \smallsetminus \{0\}$. Then $\langle \omega_0, a\rangle \equiv 0 \pmod p$ as $t$ and $p$ are coprime. So $|\omega_0| \geq \rho_p(a';\Omega)$ by hypothesis. This implies the inequality in (30).

Let $e \in \mathbb{Z}$ such that $X^e P_{a'}$ is a polynomial with non-zero constant part, then $\deg(X^e P_{a'}) \leq 2|a'| < p-1$. Since $X^e P_{a'}$ has integral coefficients we find $P_{a'}(\zeta) \neq 0$ if $\zeta$ has order $p$. Clearly, we also have $P_{a'}(1) = n+1 \neq 0$. So $P_{a'}$ does not vanish at any point of $\mu_p$.

We apply Proposition 17 to $\epsilon = 1/(2m), a'$, and $p$ to conclude $\#\mathscr{B}(p, a', \lambda) \leq c_2 p^{1/(2m)}$ for constants $c_2, \lambda \geq 1$ that depend only on $m$ and $n$.

We use this bound in the estimate from Proposition 10 applied to $a'$, to get $\Delta_p(a') \neq 0$ and

$$\left| \frac{1}{p-1} \log \Delta_p(a') - \mathrm{m}(P_{a'}) \right| \leq c_3 \frac{|a'| \log p}{p} \left( \lambda + c_2 p^{\frac{1}{2m}} \right) \leq c_4 p^{-\frac{1}{2m}}$$

where $c_3$ and $c_4$ depend only on $m, n$, and $\epsilon$.

Now recall that $a' = ta - p\omega$, so $\Delta_p(a') = \Delta_p(ta) = \Delta_p(a) \neq 0$, by Lemma 11, parts (i) and (ii), respectively. This completes the proof. □

Let $A \in \mathrm{Mat}_{mn}(\mathbb{Z})$ be a matrix with entries $a_{ij}$. We define

$$P_A = 1 + \sum_{j=1}^{n} X_1^{a_{1j}} X_2^{a_{2j}} \cdots X_m^{a_{mj}} \in \mathbb{Z}[X_1^{\pm 1}, \ldots, X_m^{\pm 1}]. \tag{31}$$

If we consider $a \in \mathbb{Z}^n$ as a $1 \times n$ matrix and identify $X_1$ with $X$, then the definitions (10) and (31) coincide.

Now suppose that $\Omega \subseteq \mathbb{Z}^n$ is a subgroup of rank $m \geq 1$ and assume that the rows of $A$ are a basis of $\Omega$. Then the value $\mathrm{m}(P_A)$ is independent of the choice of basis. Indeed, if the rows of $B \in \mathrm{Mat}_{mn}(\mathbb{Z})$ constitute another basis of $\Omega$, then $A = UB$ with $U \in \mathrm{GL}_m(\mathbb{Z})$. The Mahler measure is known to be invariant under a change of coordinates by $U$, i.e. $\mathrm{m}(P_A) = \mathrm{m}(P_{UB}) = \mathrm{m}(P_B)$, cf. Corollary 8 in Chapter 3.4 [23]. So $\mathrm{m}(P_A)$ depends only on $\Omega$ and we write

$$\mathrm{m}(\Omega) = \mathrm{m}(P_A) \tag{32}$$

for any $A$ as before.

**Theorem 19.** *Let $\Omega \subseteq \mathbb{Z}^n$ be a subgroup of rank $m \geq 2$ that satisfies the hypothesis in Proposition 13 and say $\epsilon > 0$. Suppose $a \in \Omega$ and $p$ is a prime such that $\rho_p(a; \Omega)$ is sufficiently large in terms of $\Omega$. Then $\Delta_p(a) \neq 0$ and*

$$\frac{1}{p-1} \log \Delta_p(a) = \mathrm{m}(\Omega) + O\left( \rho_p(a; \Omega)^{-\frac{1}{4n} + \epsilon} \right) \tag{33}$$

*as $\rho_p(a; \Omega) \to \infty$ where the implicit constant depends only on $\Omega$ and $\epsilon$.*

*Proof.* If $\rho_p(a; \Omega)$ is sufficiently large, then by Proposition 18 we have $\Delta_p(a) \neq 0$ and $a' \in \Omega$ with the stated properties.

Let us fix a basis $\omega_1, \ldots, \omega_m$ of $\Omega$ and write $A \in \mathrm{Mat}_{mn}(\mathbb{Z})$ for the matrix with rows $\omega_1, \ldots, \omega_m$. We fix a tuple of independent elements $(\omega_1^*, \ldots, \omega_m^*)$ in $\Omega$ and an integer $d \geq 1$ with $\langle \omega_j^*, \omega_l \rangle = 0$ if $j \neq l$ and $\langle \omega_j^*, \omega_j \rangle = d$ for all $1 \leq j, l \leq m$.

It remains to check that $\mathrm{m}(P_{a'})$ converges to $\mathrm{m}(P_A) = \mathrm{m}(\Omega)$. Observe

$$P_{a'} = P_A(X^{\nu_1}, X^{\nu_2}, \ldots, X^{\nu_m})$$

where $\nu = (\nu_1, \ldots, \nu_m) \in \mathbb{Z}^m$ is determined by $a' = \nu_1 \omega_1 + \cdots + \nu_m \omega_m$.

Our quantitative version of Lawton's Theorem, Theorem 24 in the self-contained appendix, relies on $\rho(\nu;\mathbb{Z}^m)$. Say $(\lambda_1,\dots,\lambda_m)\in\mathbb{Z}^m\smallsetminus\{0\}$ has norm $\rho(\nu;\mathbb{Z}^n)$ with $\sum_{j=1}^m\lambda_j\nu_j=0$. Then $\langle\sum_{j=1}^m\lambda_j\omega_j^*,a'\rangle=0$ and hence

$$\rho_p(a;\Omega)\le\rho(a';\Omega)\le\left|\sum_{j=1}^m\lambda_j\omega_j^*\right|\le\rho(\nu;\mathbb{Z}^m)(|\omega_1^*|+\cdots+|\omega_m^*|)$$

where we used (30). The theorem follows as $P_A$ has at most $n+1$ and at least $m+1\ge 2$ non-zero terms. □

## 9. Applications to Gaussian Periods

Using our method we prove the following theorem from which we will deduce two applications. Suppose $n\ge 2$. Recall that $\mathrm{m}(\Omega)$ was defined in (32).

A place of a number field is an absolute value on the said number field whose restriction to $\mathbb{Q}$ coincides with the standard complex absolute value or the $p$-adic absolute value for a prime $p$ taking the value $p^{-1}$ at $p$.

**Theorem 20.** *Let $K$ be a number field, let $\alpha_1,\dots,\alpha_n\in K$, and define the subgroup*

$$\Omega=\{(b_1,\dots,b_n)\in\mathbb{Z}^n:b_1\alpha_1+\cdots+b_n\alpha_n=0\}^\perp$$

*of rank $m$. Let $\epsilon>0$. We suppose $m\ge 2$ and that the following hypothesis holds. The $0=\alpha_0,\alpha_1,\dots,\alpha_n$ are pairwise distinct and $(\alpha_i-\alpha_j)/(\alpha_k-\alpha_l)\notin\mathbb{Q}$ for all pairwise distinct $i,j,k,l\in\{0,\dots,n\}$. Let $p$ be a prime, $v_0$ a place of $K$ that extends the $p$-adic absolute value, and $e(v_0)$ the ramification index of $K/\mathbb{Q}$ at $v_0$. Suppose $(a_1,\dots,a_n)\in\mathbb{Z}^n$ with $|a_i-\alpha_i|_{v_0}<1$ for all $i\in\{1,\dots,n\}$, then*

(34)

$$\frac{1}{p-1}\sum_{t=1}^{p-1}\log\left|1+\zeta^{ta_1}+\cdots+\zeta^{ta_n}\right|=\mathrm{m}(\Omega)+O\left(p^{-\frac{1}{4n[K:\mathbb{Q}]e(v_0)}+\epsilon}\right)\quad\text{where}\quad\zeta=e^{2\pi\sqrt{-1}/p}$$

*as $p\to\infty$ and the implicit constant depends only on $\alpha_1,\dots,\alpha_n$, and $\epsilon$; in particular, the logarithm is well-defined for all large $p$.*

*Proof.* Observe that $\Lambda=\{(b_1,\dots,b_n)\in\mathbb{Z}^n:b_1\alpha_1+\cdots+b_n\alpha_n=0\}$ is a primitive subgroup of $\mathbb{Z}^n$ of rank $r=n-m$. If $r\ge 1$ and if $M\in\mathrm{Mat}_{rn}(\mathbb{Z})$ is a matrix whose rows are a basis of $\Lambda$, then

$$0\to p\Omega\xrightarrow{\text{inclusion}}p\mathbb{Z}^n\xrightarrow{\text{multiplication by }M}p\mathbb{Z}^r\to 0$$

is a short exact sequence. By the Snake Lemma we find that the image of $\Omega$ in $\mathbb{F}_p^n$ equals the kernel of multiplication by $M$ taken as an endomorphism $\mathbb{F}_p^n\to\mathbb{F}_p^r$.

Say $a=(a_1,\dots,a_n)\in\mathbb{Z}^n$ is as in the hypothesis. Then the left-hand side of (34) equals $\frac{1}{p-1}\log\Delta_p(a)$. This mean is invariant under translating $a$ by a vector in $p\mathbb{Z}^n$, cf. Lemma 11(i). For all $(b_1,\dots,b_n)\in\Lambda$ we find

$$|a_1b_1+\cdots+a_nb_n|_{v_0}=|(a_1-\alpha_1)b_1+\cdots+(a_n-\alpha_n)b_n|_{v_0}\le\max_{1\le i\le n}|a_i-\alpha_i|_{v_0}<1.$$

By the previous paragraph we may assume, after adding an element of $p\mathbb{Z}^n$ to $a$, i.e. without loss of generality, that $a\in\Omega$. The current theorem will follow from Theorem 19.

As $\Lambda^{\perp\perp} = \Lambda$, we find that the hypothesis on $\Omega$ implies the hypothesis on $\Omega$ in Proposition 13.

To estimate $\rho_p(a;\Omega)$ say $\omega = (\omega_1, \dots, \omega_n) \in \Omega \smallsetminus \{0\}$ with $\langle \omega, a\rangle \equiv 0 \pmod p$ and $|\omega| = \rho_p(a;\Omega)$. We define $\Delta = \omega_1\alpha_1 + \cdots + \omega_n\alpha_n \in K$. Observe that $\Delta \neq 0$ since $\Lambda \cap \Lambda^\perp = \{0\}$. We estimate

$$|\Delta|_{v_0} = |\omega_1(\alpha_1 - a_1) + \cdots + \omega_n(\alpha_n - a_n) + \omega_1 a_1 + \cdots + \omega_n a_n|_{v_0} \leq p^{-1/e(v_0)}.$$

If $v$ is an archimedean place of $K$, then the triangle inequality yields $|\Delta|_v \leq n|\omega| \max\{|\alpha_1|_v, \dots, |\alpha_n|_v\}$ For any non-archimedean place $v$ of $K$ we get a stronger bound due to the ultrametric triangle inequality, i.e. $|\Delta|_v \leq \max\{|\alpha_1|_v, \dots, |\alpha_n|_v\}$.

We take the product of $|\Delta|_v \neq 0$ over all places with the appropriate multiplicities and use the local bounds above in combination with the product formula to obtain

$$1 \leq \left(n|\omega| e^{h(\alpha_1)+\cdots+h(\alpha_n)}\right)^{[K:\mathbb{Q}]} p^{-1/e(v_0)}.$$

So (34) follows from (33) as $|\omega| = \rho_p(a;\Omega)$. □

The following corollary generalizes Theorem 1 to subgroups of $\mathbb{F}_p^\times$ of odd order.

**Corollary 21.** *Let $f \geq 3$ be an odd integer and $\epsilon > 0$. Say $\xi$ is a root of unity of order $f$ and define*

$$\Omega = \left\{(b_1, \dots, b_{f-1}) \in \mathbb{Z}^{f-1} : b_1(\xi - 1) + b_2(\xi^2 - 1) + \cdots + b_{f-1}(\xi^{f-1} - 1) = 0\right\}^\perp.$$

*For any prime $p$ with $p \equiv 1 \pmod f$ let $G_p \subseteq \mathbb{F}_p^\times$ be the subgroup of order $f$. Then*

$$\frac{1}{p-1}\sum_{t=1}^{p-1} \log\left|\sum_{g\in G_p} \zeta^{tg}\right| = \mathrm{m}(\Omega) + O\left(p^{-\frac{1}{4(f-1)\varphi(f)}+\epsilon}\right) \quad \text{where} \quad \zeta = e^{2\pi\sqrt{-1}/p}$$

*as $p \to \infty$ where the implicit constant depends only on $f$ and $\epsilon$; in particular, the logarithm is well-defined for all large $p$.*

We will prove this corollary further down. Here we treat the hypothesis on $\Omega$ in Theorem 20 for roots of unity.

**Lemma 22.** *Let $\zeta_1, \zeta_2, \zeta_3, \zeta_4$ be pairwise distinct roots of unity. If $(\zeta_1 - \zeta_2)/(\zeta_3 - \zeta_4) \in \mathbb{Q}$, then there exist distinct $i, j \in \{1, 2, 3, 4\}$ with $\zeta_i = -\zeta_j$.*

*Proof.* Set $\eta = \zeta_3\zeta_4^{-1}, \xi = \zeta_1\zeta_2^{-1}$, and $\zeta = \zeta_2\zeta_4^{-1}$ and define

$$x = \frac{\zeta_1 - \zeta_2}{\zeta_3 - \zeta_4} = \zeta\frac{\xi - 1}{\eta - 1}.$$

We assume $x \in \mathbb{Q}$ and, after possibly swapping $\zeta_1$ and $\zeta_2$, also $x > 0$.

Note that the number field $K = \mathbb{Q}(\zeta_1, \zeta_2, \zeta_3, \zeta_4)$ has only complex embeddings as it contains at least 4 roots of unity. So the $K/\mathbb{Q}$-norm $\mathrm{N}_{K/\mathbb{Q}}(\cdot)$ is never negative. We have

$$x^{[K:\mathbb{Q}]} = \mathrm{N}_{K/\mathbb{Q}}(x) = \frac{\mathrm{N}_{K/\mathbb{Q}}(\xi - 1)}{\mathrm{N}_{K/\mathbb{Q}}(\eta - 1)}. \tag{35}$$

We now divide into four cases, depending on whether the orders of $\eta$ and $\xi$ are prime powers or not.

First suppose that neither $\eta$ nor $\xi$ has order a prime power. Then $\eta-1$ and $\xi-1$ are units and hence $x=1$ by (35). We obtain the vanishing sum of roots of unity

$$\eta-\zeta\xi+\zeta-1=0. \tag{36}$$

If a non-trivial subsum vanishes, then

$$\eta-\zeta\xi=\zeta-1=0 \quad \text{or} \quad \eta+\zeta=-\zeta\xi-1=0 \quad \text{or} \quad \eta-1=-\zeta\xi+\zeta=0.$$

The first and third cases are impossible as $\zeta\neq 1$ and $\eta\neq 1$. Thus $\zeta\xi=-1$ and this implies $\zeta_1=-\zeta_4$, as desired.

If no non-trivial subsum vanishes, then Mann's Theorem 1 [17] implies $\eta^6=\xi^6=\zeta^6=1$. In the current case, $\eta$ and $\xi$ must have precise order 6. If $\eta=\xi$, then (36) implies $\eta=1$ or $\zeta=1$ which contracts the hypothesis. Hence $\eta\neq\xi$ and thus $\eta\xi=1$. When combined with (36) we have

$$\zeta\xi=\frac{\eta-1}{\xi-1}\xi=\frac{\eta\xi-\xi}{\xi-1}=\frac{1-\xi}{\xi-1}=-1, \tag{37}$$

and again $\zeta_1=-\zeta_4$.

Now suppose that $\xi$ has order $p^e$ with $p$ a prime and $e\geq 1$ and that the order of $\eta$ is not a prime power. Then $\eta-1$ remains a unit but now $\mathrm{N}_{K/\mathbb{Q}}(\xi-1)=p^{[K:\mathbb{Q}(\xi)]}$, so $x^{\varphi(p^e)}=p$. As $x$ is rational, we must have $\varphi(p^e)=1$, so $p^e=2$ and thus $\zeta_1\zeta_2^{-1}=\xi=-1$, which completes this case.

Similarly, if $\eta$ has prime power order and $\xi$ does not, then we apply the argument from the last paragraph to $x^{-1}=\zeta^{-1}(\eta-1)/(\xi-1)$ and conclude $\zeta_3\zeta_4^{-1}=\eta=-1$, as desired.

Finally, suppose $\eta$ has order $q^{e'}$ and $\xi$ has order $p^e$, here $p$ and $q$ are primes and $e,e'\geq 1$. Now (35) implies $x=p^{1/\varphi(p^e)}q^{-1/\varphi(q^{e'})}\in\mathbb{Q}$. If $p\neq q$, then $p^e=q^{e'}=2$ and so $\eta=\xi=-1$, as desired. So say $p=q$, hence $x=p^{1/\varphi(p^e)-1/\varphi(p^{e'})}\in\mathbb{Q}$ and it follows that

$$\frac{1}{(p-1)p^{e-1}}-\frac{1}{(p-1)p^{e'-1}}\in\mathbb{Z}$$

and this entails $e=e'$. We find $x=1$ and are thus back in the situation of the first case except that $\eta$ and $\xi$ now have prime power order. We proceed similarly. If a non-trivial subsum in (36) vanishes, then again $\zeta_1=-\zeta_4$. Otherwise Mann's Theorem yields $\eta^6=\xi^6=1$. This time $\eta$ and $\xi$ have equal order which is 2 or 3. If the common order is 2 then we are done. Else wise it is 3 and again we must have $\eta\neq\xi$ which again implies $\eta\xi=1$. We conclude $\zeta_1=-\zeta_4$ as in (37). □

*Proof of Corollary 21.* Let $\xi$ be a root of unity of order $f$. We set

$$\alpha_1=\xi-1, \quad \alpha_2=\xi^2-1, \quad \dots \quad \alpha_{f-1}=\xi^{f-1}-1.$$

Our aim is to apply Theorem 20 to $K=\mathbb{Q}(\xi)$ and $n=f-1\geq 2$. Say $\Omega$ is as in the said theorem.

Observe that

$$\alpha_1\mathbb{Z}+\cdots+\alpha_n\mathbb{Z}=(\xi-1)(\mathbb{Z}+(\xi+1)\mathbb{Z}+\cdots+(\xi^{f-2}+\cdots+\xi+1)\mathbb{Z})=(\xi-1)\mathbb{Z}[\xi]$$

as $\xi^{f-1}=-(\xi^{f-2}+\cdots+\xi+1)$. This group has rank $m=\varphi(f)$ and therefore $\Omega$ also has rank $m\geq 2$.

We shall show that the hypothesis on $\Omega$ in Theorem 20 is satisfied. Indeed, if $i, j, k, l \in \{0, \dots, n\}$ are pairwise distinct, then

$$\frac{\xi^i - \xi^j}{\xi^k - \xi^l} \in \mathbb{Q}$$

implies that $\xi$ has even order by Lemma 22. This contradicts our hypothesis on $f$.

Finally, observe that $p \equiv 1 \pmod f$ means that $p$ splits completely in $K$. For such $p$ there is $(a_1, \dots, a_n)$ as above (34) where $v_0$ is any place of $K$ extending the $p$-adic absolute value. Here $e(v_0) = 1$. Now $1, 1 + a_1, \dots, 1 + a_n$ is a complete set of representatives of the subgroup of $\mathbb{F}_p^\times$ of order $f = n + 1$. The corollary follows as

$$\left|1 + \zeta^{ta_1} + \cdots + \zeta^{ta_n}\right| = \left|\zeta^t + \zeta^{t(1+a_1)} + \cdots + \zeta^{t(1+a_n)}\right|$$

for all $1 \le t \le p - 1$. □

*Proof of Theorem 1.* We set $\Omega$ as in the proof of Corollary 21. Its rank is $\varphi(f) = f - 1$ as $f$ is a prime by hypothesis. Since $\Omega$ is a primitive subgroup of $\mathbb{Z}^{f-1}$ we conclude $\Omega = \mathbb{Z}^{f-1}$. In the definition (32) of $\mathrm{m}(\Omega)$ we may take $A$ to equal the $(f-1) \times (f-1)$ unit matrix. The resulting logarithmic Mahler measure is that of $1 + X_1 + \cdots + X_{f-1}$. □

*Proof of Corollary 2.* Observe that $\sum_{g \in G} e^{2\pi\sqrt{-1}g/p}$ is an algebraic integer. In view of Theorem 1 it suffices to verify $\mathrm{m}(1 + X_1 + \cdots + X_{f-1}) \neq 0$. The higher dimensional version of Kronecker's Theorem classifies integral polynomials whose logarithmic Mahler measure vanishes, see work of Boyd [6], Lawton [13], and Smyth [25]. As our $1 + X_1 + \cdots + X_{f-1}$ is irreducible and $f \ge 3$ we easily deduce from this classification that its logarithmic Mahler measure is non-zero. □

## Appendix On Lawton's Theorem

In this appendix we provide a rate of convergence for the following theorem of Lawton. The arguments here do not rely on the rest of the paper. Say $n \ge 1$ is an integer. Recall that the definition of $\rho$ is given in (29).

**Theorem 23** (Lawton, Theorem 2 [14])**.** *Suppose $P \in \mathbb{C}[X_1^{\pm 1}, \dots, X_n^{\pm 1}] \smallsetminus \{0\}$. If $a \in \mathbb{Z}^n$, then $\mathrm{m}(P(X^{a_1}, \dots, X^{a_n})) = \mathrm{m}(P) + o(1)$ as $\rho(a; \mathbb{Z}^n) \to \infty$.*

We closely following Lawton's approach but keep track of estimates to obtain the following refinement.

**Theorem 24.** *Suppose $P \in \mathbb{C}[X_1^{\pm 1}, \dots, X_n^{\pm 1}] \smallsetminus \{0\}$ has $k \ge 2$ non-zero terms and let $\epsilon > 0$. For $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$ we have*

$$\mathrm{m}(P(X^{a_1}, \dots, X^{a_n})) = \mathrm{m}(P) + O\left(\rho(a; \mathbb{Z}^n)^{-\frac{1}{4(k-1)} + \epsilon}\right)$$

*as $\rho(a; \mathbb{Z}^n) \to \infty$ where the implied constant depends on $n, P$, and $\epsilon$.*

An important tool is an estimate on the measure of the subset of the unit circle, where a polynomial takes small values. We use $\mathrm{vol}(\cdot)$ to denote the Lebesgue measure on $\mathbb{R}^n$. For $P \in \mathbb{C}[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ and $y > 0$ we define

$$S(P, y) = \{x \in [0, 1)^n : |P(e(x))| < y\}$$

where $e(x) = (e^{2\pi\sqrt{-1}x_1}, \dots, e^{2\pi\sqrt{-1}x_n})$ for $x = (x_1, \dots, x_n) \in \mathbb{R}^n$.

**Lemma 25** (Lawton, Theorem 1 [14])**.** *For $k \geq 1$ there exists a constant $C_k > 0$ with the following property. If $P \in \mathbb{C}[X]$ is a monic polynomial with $k$ non-zero terms and $y > 0$, then* $\mathrm{vol}(S(P, y)) \leq C_k y^{1/\max\{1,k-1\}}$

The reference covers the important case $k \geq 2$. If $k = 1$, then $|P(e(x))| = 1$ for all $x \in \mathbb{R}^n$ and the claim is clear with $C_1 = 1$.

**Lemma 26.** *Assume $P \in \mathbb{C}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}] \smallsetminus \{0\}$ has $k \geq 1$ non-zero terms.*

(i) *If for all $y \in (0, 1]$ then $\mathrm{vol}(S(P, y)) = O\left(y^{1/(2\max\{1,k-1\})}\right)$ where the constant in $O(\cdot)$ depends only on $P$.*
(ii) *If $q > 0$ then $\int_{[0,1)^n} \left|\log |P(e(x))|\right|^q dx$ is well-defined and finite.*

*Proof.* Our proof of (i) is by induction on $n$. We may assume that $P$ is a polynomial.

If $n = 1$, then the lemma follows from Lawton's Theorem after normalizing $P$.

Say $n \geq 2$. There is nothing to prove if $k = 1$, so suppose $k \geq 2$. We may also assume that $P$ is a polynomial, hence $P = P_0 X_n^d + \cdots + P_d$ where $P_0, \ldots, P_d \in \mathbb{C}[X_1, \ldots, X_{n-1}]$ and $P_0 \neq 0$. We abbreviate $\Sigma = S(P_0, y^{1/2}) \subseteq [0, 1)^{n-1}$. If $x' \in \mathbb{R}^{n-1}$ and $P_0(e(x')) \neq 0$, then $P(e(x'), X)/P_0(e(x'))$ is a monic polynomial in $X$. Fubini's Theorem implies

$$\begin{aligned}
\mathrm{vol}(S(P, y)) &= \int_{\Sigma} \mathrm{vol}(S(P(e(x'), X), y))dx' + \int_{[0,1)^{n-1} \smallsetminus \Sigma} \mathrm{vol}(S(P(e(x'), X), y))dx' \\
&\leq \mathrm{vol}(\Sigma) + \int_{[0,1)^{n-1} \smallsetminus \Sigma} \mathrm{vol}(S(P(e(x'), X)/P_0(e(x'))), y/|P_0(e(x'))|)dx' \\
&\leq \mathrm{vol}(\Sigma) + \int_{[0,1)^{n-1} \smallsetminus \Sigma} \mathrm{vol}(S(P(e(x'), X)/P_0(e(x'))), y^{1/2})dx' \\
&\leq \mathrm{vol}(\Sigma) + C_k y^{1/(2k-2)}
\end{aligned}$$

since $\mathrm{vol}(S(P(e(x'), X), y)) \leq 1$ and by Lemma 25.

By this lemma applied by induction to $P_0 \in \mathbb{C}[X_1, \ldots, X_{n-1}] \smallsetminus \{0\}$ we conclude $\mathrm{vol}(\Sigma) \leq c(P_0) y^{1/(2k-2)}$. This yields part (i).

The statement in (ii) is possible known, we give a proof based on (i). For an integer $m \geq 0$ and $x \in \mathbb{R}^n$ we define $p_m(x) = \min\{m, |\log |P(e(x))||^q\} \geq 0$ which is interpreted as $m$ if $P(e(x)) = 0$. Then $p_m$ is a non-decreasing sequence of continuous functions on $[0, 1)^n$. We set $I_m = \int_{[0,1)^n} p_m(x)dx$. By the Monotone Convergence Theorem it suffices to prove that the non-decreasing sequence $(I_m)_{m \geq 1}$ converges. For all sufficiently large $m$ we have $|P(e(x))| \leq e^{m^{1/q}}$ if $x \in [0, 1)^n$. Observe that $p_m$ equals $m$ on $S(P, e^{-m^{1/q}})$ and that it coincides with $p_{m+1}$ outside this set. Thus for all large $m$ we have

$$I_{m+1} - I_m = \int_{S(P, e^{-m^{1/q}})} (p_{m+1}(x) - p_m(x))dx \leq \mathrm{vol}(S(P, e^{-m^{1/q}})) = O\left(e^{-m^{1/q}/(2k)}\right)$$

as $p_{m+1}(x) \leq m + 1$ and where we used (i), the implied constant is independent of $m$. Since $\sum_{m \geq 1} e^{-m^{1/q}/(2k)} < \infty$ we can use a telescoping sum to show that $\sup_{m \geq 0} I_m < \infty$, as desired. □

Let $\mathbb{N}_0$ denote the non-negative integers. Say $b \in \mathbb{N}_0$ and let $g$ lie in $C^b(\mathbb{R}^n)$, the set of real valued functions on $\mathbb{R}^n$ whose derivatives exist up-to and including order $b$ and are

continuous. For a multiindex $i = (i_1, \dots, i_n) \in \mathbb{N}_0^n$ we set $\ell(i) = i_1 + \cdots + i_n$. If $\ell(i) \le b$, then we define $\partial^i g = (\partial/\partial x_1)^{i_1} \cdots (\partial/\partial x_n)^{i_n} g$ and

$$|g|_{C^b} = \max_{\substack{i \in \mathbb{N}_0^n \\ \ell(i) \le b}} \sup_{x \in \mathbb{R}^n} |\partial^i g(x)|$$

which is possibly $\infty$.

We now introduce a function that equals $\log|P(e(\cdot))|$ away from the singular locus but is continuous on $\mathbb{R}^n$ and attains 0 when $P(e(\cdot))$ does.

Say $\phi \in C^b(\mathbb{R})$ is non-decreasing with $\phi(0) = 0, \phi(1) = 1$, $\phi(x) = 0$ if $x < 0$, and $\phi(x) = 1$ if $x > 1$. We ask in addition that $\partial^i\phi(0) = \partial^i(1) = 0$ for all $i \in \{1, \dots, b\}$. For example, we could take the anti-derivative of $x^b(1-x)^b$ that attains 0 at $x = 0$, scale it to attain 1 at $x = 1$, and extend by 0 for $x < 0$ and by 1 for $x > 1$.

Say $y \in (0, 1/2]$. We define $\phi_y$ as $x \mapsto ((2/y)^2 x - 1)/3$, which rescales $[(y/2)^2, y^2]$ to $[0, 1]$, composed with $\phi$. Then

$$|\partial^i(\phi_y)(t)| \le \left(\frac{4}{3y^2}\right)^i \left|\partial^i\phi(t)\right|$$

for all $i \in \{0, \dots, b\}$ and all $t \in \mathbb{R}$. Hence

$$|\phi_y|_{C^b} = O_{b,\phi}(y^{-2b}), \tag{38}$$

here and below the implied constant depends on the quantities appearing in the subscript. Finally, we define $\psi_y$ as

$$\psi_y(t) = \begin{cases} \frac{1}{2}\phi_y(t)\log t & : t > 0, \\ 0 & : t \le 0. \end{cases}$$

Then $\psi_y \in C^b(\mathbb{R})$ and all its derivatives up-to and including order $b$ vanish outside of $((y/2)^2, y^2)$. Thus

$$|\psi_y|_{C^b} = O_{b,\phi}(y^{-2b}|\log y|) \tag{39}$$

by the Leibniz product rule applied using (38) and since $y \in (0, 1/2]$.

Say $P \in \mathbb{C}[X_1, \dots, X_n]$ and write $g(x) = |P(e(x))|^2$, this is a smooth function $\mathbb{R}^n \to \mathbb{R}$ and

$$|g|_{C^b} = O_{b,P,n}(1). \tag{40}$$

We define $f_y = \psi_y \circ g$. If $P(e(x)) \neq 0$ with $x \in \mathbb{R}^n$, then

$$f_y(x) = \psi_y(|P(e(x))|^2) = \phi_y(|P(e(x))|^2)\log|P(e(x))|$$

and for any $x \in \mathbb{R}^n$ we have

$$f_y(x) = \begin{cases} 0 & : \text{ if } |P(e(x))| \le y/2, \\ \log|P(e(x))| & : \text{ if } |P(e(x))| \ge y. \end{cases}$$

Moreover, the composition $f_y : \mathbb{R}^n \to [0, 1]$ lies in $C^b(\mathbb{R}^n)$. We can bound its norm using the following lemma.

**Lemma 27.** *Let $b \ge 0, \psi \in C^b(\mathbb{R})$, and $g \in C^b(\mathbb{R}^n)$ satisfy $|\psi|_{C^b} < \infty$ and $|g|_{C^b} < \infty$. Then $|\psi \circ g|_{C^b} \le 2^{b(b-1)/2}|\psi|_{C^b}\max\{1, |g|_{C^b}\}^b$.*

*Proof.* The lemma is evident for $b = 0$. So say $b \geq 1$ and let $i \in \mathbb{N}_0^n \smallsetminus \{0\}$ with $\ell = \ell(i) \leq b$. Let $j \in \mathbb{N}_0^n$ be a standard basis vector with $i - j \in \mathbb{N}_0^n$. Using the chain rule and the Leibniz product rule we find

$$|\partial^i(\psi \circ g)|_{C^0} = |\partial^{i-j}(\partial^j(\psi \circ g))|_{C^0} = |\partial^{i-j}((\psi' \circ g)\partial^j g)|_{C^0} \leq 2^{\ell-1}|\psi' \circ g|_{C^{\ell-1}}|g|_{C^\ell}.$$

Thus $|\partial^i(\psi \circ g)|_{C^0} \leq 2^{b-1}|\psi' \circ g|_{C^{b-1}}|g|_{C^b} \leq 2^{b(b-1)/2}|\psi|_{C^b}\max\{1, |g|_{C^b}\}^b$, where we applied this lemma by induction to bound $|\psi' \circ g|_{C^{b-1}}$ from above. This upper bound for $|\partial^i(\psi \circ g)|_{C^0}$ continues to hold for $i = 0$ and it is therefore an upper bound for $|\psi \circ g|_{C^b}$. □

This lemma, together with (39) and (40), implies

$$|f_y|_{C^b} = O_{b,P,n,\phi}(y^{-2b}|\log y|). \tag{41}$$

From now on we suppose $b \geq n + 1$. In the next three lemmas and if not stated otherwise, $P \in \mathbb{C}[X_1, \ldots, X_n] \smallsetminus \{0\}$ is a polynomial with $k \geq 2$ non-zero terms.

**Lemma 28.** *Suppose $a \in \mathbb{Z}^n$ and $y \in (0, 1/2]$, then*

$$\int_0^1 f_y(at)dt = \int_{[0,1)^n} f_y(x)dx + O_{b,P,\phi,n}\left(\frac{|\log y|}{y^{2b}}\frac{1}{\rho(a;\mathbb{Z}^n)^{b-n}}\right).$$

*Proof.* All implied constants in this proof depend only on $b, P, \phi$, and $n$. The Fourier coefficients $\widehat{f_y}(m)$ of $f_y \in C^b(\mathbb{R})$, here $m \in \mathbb{Z}^n$, decay quickly. Indeed, by Theorem 3.2.9(b) [11][1] with $s = b$ and $|\widehat{\partial^a f_y}(m)| \leq |\partial^a f_y|_{C^0} \leq |\partial^a f_y|_{C^b}$ where $\ell(i) = b$. We conclude

$$|\widehat{f_y}(m)| = O\left(\frac{|f_y|_{C^b}}{|m|^b}\right) \quad \text{and so} \quad |\widehat{f_y}(m)| = O\left(\frac{|\log y|}{y^{2b}|m|^b}\right)$$

for all $m \in \mathbb{Z}^n \smallsetminus \{0\}$ by (41). Say $H \geq 1$, then $\sum_{|m|\geq H}|\widehat{f_y}(m)| = O\left(\frac{|\log y|}{y^{2b}}\sum_{|m|\geq H}\frac{1}{|m|^b}\right)$, and hence

$$\sum_{|m|\geq H}|\widehat{f_y}(m)| = O\left(\frac{|\log y|}{y^{2b}}\frac{1}{H^{b-n}}\right) \tag{42}$$

as $b - n \geq 1$

Since the Fourier coefficients of the continuous function $f_y$ are absolutely summable, its Fourier series converges uniformly to $f_y$. Hence

$$\int_0^1 f_y(at)dt = \sum_{m\in\mathbb{Z}^n}\int_0^1 \widehat{f_y}(m)e^{2\pi\sqrt{-1}\langle a,m\rangle t}dt = \widehat{f_y}(0) + \sum_{\substack{m\in\mathbb{Z}^n\smallsetminus\{0\}\\ \langle a,m\rangle=0}}\widehat{f_y}(m).$$

Now $\widehat{f_y}(0)$ equals $\int_{[0,1)^n} f_y(x)dx$, so the estimate in the assertion follows from (42) and

$$\left|\sum_{\substack{m\in\mathbb{Z}^n\smallsetminus\{0\}\\ \langle a,m\rangle=0}}\widehat{f_y}(m)\right| \leq \sum_{|m|\geq\rho(a;\mathbb{Z}^n)}|\widehat{f_y}(m)| = O\left(\frac{|\log y|}{y^{2b}}\frac{1}{\rho(a;\mathbb{Z}^n)^{b-n}}\right). \qquad \square$$

[1] $|\cdot|$ in the reference is the $\ell^2$-norm

**Lemma 29.** *Suppose each non-zero term of $P$ has modulus at least 1. If $a \in \mathbb{Z}^n$ such that $\rho(a;\mathbb{Z}^n)$ is sufficiently large in terms of $P$. Then $|P(e(as))|$ is non-zero for all $s \in [0,1]$ outside a finite set of points. Moreover, if $y \in (0,1/2]$ then*

$$\int_0^1 \log|P(e(as))|ds = \int_0^1 f_y(as)ds + O\left(y^{1/(k-1)}|\log y|\right)$$

*where the implicit constant depends only on $P$ and $n$.*

*Proof.* Say $a = (a_1,\dots,a_n)$ and suppose that $\rho(a;\mathbb{Z}^n)$ is strictly larger than $|m-m'|$ for all distinct $m, m'$ in the support of $P$. Then $P(X^{a_1},\dots,X^{a_n})$ has the same coefficients as $P$. It is in particular non-zero and the first claim holds true. For the second claim we can apply Lawton's Lemma 4 [14]. □

**Lemma 30.** *Let $\epsilon > 0$. If $y \in (0,1/2]$ then*

$$\left|\int_{[0,1)^n} (f_y(x) - \log|P(e(x))|)dx\right| = O\left(y^{\frac{1}{2(k-1)}-\epsilon}\right)$$

*where the implied constant depends only on $n, P$, and $\epsilon$.*

*Proof.* Let $p > 1$ and fix $q > 1$ such that $1/p + 1/q = 1$. By definition we get the equality in

$$\begin{aligned}\left|\int_{[0,1)^n} (f_y(x) - \log|P(e(x))|)dx\right| &= \left|\int_{[0,1)^n} (\phi_y(|P(e(x))|^2) - 1)\log|P(e(x))|dx\right| \\ &\le \int_{[0,1)^n} |\phi_y(|P(e(x))|^2) - 1|\,|\log|P(e(x))||\,dx \\ &\le \left(\int_{[0,1)^n} |\phi_y(|P(e(x))|^2) - 1|^p dx\right)^{1/p} \left(\int_{[0,1)^n} |\log|P(e(x))||^q\,dx\right)^{1/q}\end{aligned}$$

we used the Hölder inequality in the last step; the final integral is finite by Lemma 26(ii). As $\phi_y(|P(e(x))|^2) = 1$ if $|P(e(x))| \ge y$ we have

$$\int_{[0,1)^n} |\phi_y(|P(e(x))|^2) - 1|^p dx = \int_{S(P,y)} |\phi_y(|P(e(x))|^2) - 1|^p dx \le \mathrm{vol}(S(P,y)).$$

Recall $k \ge 2$. The current Lemma follows from Lemma 26(i) because we may suppose $1/(2p(k-1)) \ge 1/(2k-2) - \epsilon$. □

*Proof of Proposition 24.* Without loss of generality, we may suppose that all non-zero coefficients of $P$ have modulus at least 1 and that $P$ is a polynomial. We fix $b \ge n+1$ sufficiently large and a sufficiently small $\epsilon' > 0$ with

$$-\frac{\gamma}{2(k-1)} + \epsilon'\gamma \le -\frac{1}{4(k-1)} + \epsilon \quad \text{where} \quad \gamma = \frac{b-n}{2b + 1/(2k-2)}. \tag{43}$$

We fix a step function $\phi \in C^b(\mathbb{R})$ as above, abbreviate $H = \rho(a;\mathbb{Z}^n) \ge 1$, and set $y = H^{-\gamma}$.

For $H$ large enough we find $y \le 1/2$ and that $|\mathrm{m}(P(X^{a_1},\dots,X^{a_n})) - \mathrm{m}(P)|$ equals

$$\begin{aligned}&\left|\int_0^1 \log|P(e(as))|ds - \int_{[0,1)^n} \log|P(e(x))|dx\right| \\ &\quad\le \left|\int_0^1 f_y(as)ds - \int_{[0,1)^n} f_y(x)dx\right| + \left|\int_0^1 (\log|P(e(as))| - f_y(as))ds\right| \\ &\qquad + \left|\int_{[0,1)^n} (f_y(x) - \log|P(e(x))|)dx\right|.\end{aligned}$$

Then by Lemmas 28, 29, and 30, the final one applied to a sufficiently small $\epsilon'$, this sum is in

$$O\left(\frac{|\log y|}{y^{2b}}\frac{1}{H^{b-n}} + y^{\frac{1}{2(k-1)}-\epsilon'}\right)$$

where the implied constant here and below depends only on $b, P, \phi$, and $\epsilon$. So the sum is in

$$O\left(\gamma(\log H)H^{2b\gamma+n-b} + H^{-\frac{\gamma}{2(k-1)}+\epsilon'\gamma}\right)$$

The proposition follows for small enough $\epsilon'$ as $2b\gamma + n - b = -\gamma/(2k-2)$, cf. (43). □

## References


1. P. Autissier, *Sur une question d'équirépartition de nombres algébriques*, C. R. Math. Acad. Sci. Paris **342** (2006), no. 9, 639–641.
2. J. Ax, *On Schanuel's conjectures*, Ann. of Math. (2) **93** (1971), 252–268.
3. B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, Inc., New York, 1998.
4. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.
5. E. Bombieri, D. W. Masser, and U. Zannier, *Anomalous Subvarieties - Structure Theorems and Applications*, Int. Math. Res. Not. IMRN (2007), no. 19, 1–33.
6. D. W. Boyd, *Kronecker's theorem and Lehmer's problem for polynomials in several variables*, J. Number Theory **13** (1981), no. 1, 116–121.
7. V. Dimitrov, *Convergence to the Mahler measure and the distribution of periodic points for algebraic Noetherian $\mathbb{Z}^d$-actions*, `arXiv:1611.04664`.
8. W. Duke, *A combinatorial problem related to Mahler's measure*, Bull. Lond. Math. Soc. **39** (2007), no. 5, 741–748.
9. W. Duke, S. R. Garcia, and B. Lutz, *The graphic nature of Gaussian periods*, Proc. Amer. Math. Soc. **143** (2015), no. 5, 1849–1863.
10. M. Einsiedler, M. Kapranov, and D. Lind, *Non-Archimedean amoebas and tropical varieties*, J. Reine Angew. Math. **601** (2006), 139–157.
11. L. Grafakos, *Classical Fourier analysis*, third ed., Graduate Texts in Mathematics, vol. 249, Springer, New York, 2014.
12. P. Habegger, *Diophantine Approximations on Definable Sets*, `arXiv:1608.04547`.
13. W. M. Lawton, *A generalization of a theorem of kronecker*, J. Sci. Fat. Chiangmai Unit. (Thailand) **4** (1977), 15–23.
14. ———, *A problem of Boyd concerning geometric means of polynomials*, J. Number Theory **16** (1983), no. 3, 356–362.
15. D. Lind, K. Schmidt, and E. Verbitskiy, *Homoclinic points, atoral polynomials, and periodic points of algebraic $\mathbb{Z}^d$-actions*, Ergodic Theory Dynam. Systems **33** (2013), no. 4, 1060–1081.
16. K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. **11** (1964), 257–262.
17. H. B. Mann, *On linear relations between roots of unity*, Mathematika **12** (1965), 107–117.

18. G. Myerson, *A combinatorial problem in finite fields. I*, Pacific J. Math. **82** (1979), no. 1, 179–187.
19. ———, *A combinatorial problem in finite fields. II*, Quart. J. Math. Oxford Ser. (2) **31** (1980), no. 122, 219–231.
20. ———, *Unsolved Problems: How Small Can a Sum of Roots of Unity Be?*, Amer. Math. Monthly **93** (1986), no. 6, 457–459.
21. J. Pila and A. J. Wilkie, *The rational points of a definable set*, Duke Math. J. **133** (2006), no. 3, 591–616.
22. Q. I. Rahman and G. Schmeisser, *Analytic theory of polynomials*, London Mathematical Society Monographs. New Series, vol. 26, The Clarendon Press, Oxford University Press, Oxford, 2002.
23. A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications, vol. 77, Cambridge University Press, Cambridge, 2000, With an appendix by Umberto Zannier.
24. W.M. Schmidt, *Diophantine approximations and Diophantine equations*, Lecture Notes in Mathematics, vol. 1467, Springer-Verlag, Berlin, 1991.
25. C. J. Smyth, *A Kronecker-type theorem for complex polynomials in several variables*, Canad. Math. Bull. **24** (1981), no. 4, 447–452.
26. ———, *On measures of polynomials in several variables*, Bull. Austral. Math. Soc. **23** (1981), no. 1, 49–63.
27. L. van den Dries, *Tame topology and o-minimal structures*, London Mathematical Society Lecture Note Series, vol. 248, Cambridge University Press, Cambridge, 1998.
28. L. van den Dries and C. Miller, *Geometric categories and o-minimal structures*, Duke Math. J. **84** (1996), no. 2, 497–540.

Department of Mathematics and Computer Science, University of Basel, Spiegelgasse 1, 4051 Basel, Switzerland

*E-mail address*: philipp.habegger@unibas.ch

## LATEST PREPRINTS

| No. | Author: *Title* |
|---|---|
| 2015-41 | **H. Harbrecht, W. L. Wendland, N. Zorii**<br>*Minimal energy problems for strongly singular Riesz kernels* |
| 2015-42 | **H. Harbrecht, M. Utzinger**<br>*On adaptive wavelet boundary element methods* |
| 2016-01 | **S. Iula, G. Mancini**<br>*Extremal functions for singular Moser-Trudinger embeddings* |
| 2016-02 | **J. K. Canci, L. Paladino**<br>*On preperiodic points of rational functions defined over* $\mathbb{F}_p(t)$ |
| 2016-03 | **H. Harbrecht, R. Schneider**<br>*A note on multilevel based error estimation* |
| 2016-04 | **C. Urech**<br>*On homomorphisms between Cremona groups* |
| 2016-05 | **A. P. Choudhury, H. Heck**<br>*Stability of the inverse boundary value problem for the biharmonic operator: Logarithmic estimates* |
| 2016-06 | **M. Dambrine, I. Greff, H. Harbrecht, B. Puig**<br>*Numerical solution of the homogeneous Neumann boundary value problem on domains with a thin layer of random thickness* |
| 2016-07 | **G. Alberti, G. Crippa, A. L. Mazzucato**<br>*Exponential self-similar mixing by incompressible flows* |
| 2016-08 | **M. Bainbridge, P. Habegger, M. Möller**<br>*Teichmüller curves in genus three and just likely intersections in* $G^n_m \times G^n_a$ |
| 2016-09 | **Gabriel A. Dill**<br>*Effective approximation and Diophantine applications* |
| 2016-10 | **J. Blanc, S. Zimmermann**<br>*Topological simplicity of the Cremona groups* |
| 2016-11 | **I. Hedén, S. Zimmermann**<br>*The decomposition group of a line in the plane* |
| 2016-12 | **J. Ballani, D. Kressner, M. Peters**<br>*Multilevel tensor approximation of PDEs with random data* |

---

Preprints are available under *https://math.unibas.ch/research/publications*

## LATEST PREPRINTS

**No.** **Author:** *Title*

2016-13 **M. J. Grote, M. Kray, U. Nahum**
*Adaptive eigenspace method for inverse scattering problems in the frequency domain*

2016-14 **H. Harbrecht, M. Peters, M. Schmidlin**
*Uncertainty quantification for PDEs with anisotropic random diffusion*

2016-15 **F. Da Lio, L. Martinazzi**
*The nonlocal Liouville-type equation in $R$ and conformal immersions of the disk with boundary singularities*

2016-16 **A. Hyder**
*Conformally Euclidean metrics on $R^n$ with arbitrary total $Q$-curvature*

2016-17 **G. Mancini, L. Martinazzi**
*The Moser-Trudinger inequality and its extremals on a disk via energy estimates*

2016-18 **R. N. Gantner, M. D. Peters**
*Higher order quasi-Monte Carlo for Bayesian shape inversion*

2016-19 **C. Urech**
*Remarks on the degree growth of birational transformations*

2016-20 **S. Dahlke, H. Harbrecht, M. Utzinger, M. Weimar**
*Adaptive wavelet BEM for boundary integral equations: Theory and numerical experiments*

2016-21 **A. Hyder, S. Iula, L. Martinazzi**
*Large blow-up sets for the prescribed Q-curvature equation in the Euclidean space*

2016-22 **P. Habegger**
*The norm of Gaussian periods*

---

Preprints are available under *https://math.unibas.ch/research/publications*