ACTA ARITHMETICA
177.4 (2017)

Divisor divisibility sequences on tori

by

Joseph H. Silverman (Providence, RI)

Contents

1. Introduction. A classical divisibility sequence is a sequence $(W_n)_{n\ge1}$ of (non-zero) integers having the property

$$m \,|\, n \;\Rightarrow\; W_m \,|\, W_n. \tag{1}$$

Well-known examples of such sequences include a^n-b^n, Fibonacci and Lucas sequences, and elliptic divisibility sequences. See [7] for an overview of the history and study of divisibility sequences. These and similar sequences are associated to multiples of points in one-dimensional algebraic groups, specifically in (twisted) multiplicative groups or elliptic curves. They tend to have a number of important properties, such as those described in Table 1.

It is natural to look for analogous sequences associated to higher-dimensional algebraic groups. An obvious approach (see Section 2) yields sequences such as

$$W_n = \gcd(a^n - 1, b^n - 1) \tag{2}$$

2010 *Mathematics Subject Classification*: Primary 11B39; Secondary 14G25, 14L99.
Key words and phrases: divisibility sequence.
Received 13 December 2015; revised 16 November 2016.
Published online 22 February 2017.

DOI: 10.4064/aa8381-11-2016

Table 1. A list of sequence properties

Divisibility	W_n is a divisibility sequence
∞-Growth	$\log\lvert W_n\rvert$ grows like $O(n^d)$ for some $d \ge 1$
p-adic Growth	$\operatorname{ord}_p(W_n)$ grows regularly (and slowly)
Recursion	W_n satisfies a (possibly non-linear) recursion
Zsigmondy	Most W_n have a primitive prime divisor

for integers a and b that are multiplicatively independent in $\mathbb{Q}^*$. Such sequences are quite interesting and lead to deep theorems and conjectures, for example:

THEOREM (Bugeaud, Corvaja, Zannier [3]).

$$\lim_{n\to\infty} \frac{1}{n} \log \gcd(a^n - 1, b^n - 1) = 0.$$

CONJECTURE (Ailon, Rudnick [2]).

$$\#\{n \ge 1 : \gcd(a^n - 1, b^n - 1) = \gcd(a - 1, b - 1)\} = \infty.$$

In particular, the sequence (2), which is associated to the powers of the point (a, b) in the group $\mathbb{G}_{\mathrm{m}}^2(\mathbb{Q})$, fails to have the ∞-Growth Property, and conjecturally fails quite badly.

In this paper we suggest a new way to associate divisibility sequences to higher-dimensional algebraic groups. These sequences have the Divisibility Property and (conjecturally) the ∞-Growth Property. For concreteness, in this article we concentrate on the N-dimensional torus $\mathbb{G}_{\mathrm{m}}^N$. A formulation for more general algebraic groups is discussed briefly in Section 11 and will form the content of a subsequent paper [29]. To define our new sequences, we replace the point $(a, b) \in \mathbb{G}_{\mathrm{m}}^2$ used in (2) with a divisor in $\mathbb{G}_{\mathrm{m}}^N$, or equivalently, with the zero set of a non-zero Laurent polynomial.

DEFINITION (Preliminary). Let $\boldsymbol{\mu}_n \subset \mathbb{C}^*$ denote the group of nth roots of unity. The *Divisor Divisibility sequence*, or *DD-sequence* for short, associated to a non-zero Laurent polynomial $f \in \mathbb{Z}[X_1^{\pm 1}, \dots, X_N^{\pm 1}]$ is the sequence

$$W_n(f) = \prod_{\substack{\zeta_1,\dots,\zeta_N \in \boldsymbol{\mu}_n \\ f(\zeta_1,\dots,\zeta_N)\neq 0}} f(\zeta_1, \dots, \zeta_N). \tag{3}$$

For example, taking $N = 1$ and $f(X) = aX - b$ recovers the classical divisibility sequence $W_n(aX - b) = a^n - b^n$.

One easily checks that $W_n(f) \in \mathbb{Z}$ is a divisibility sequence, so DD-sequences have the Divisibility Property. Further, it is conjectured (and proven if $N = 1$ or if f is "atoral" [16]) that $\log\lvert W_n(f)\rvert \sim n^N \log \mathcal{M}(f)$ as $n \to \infty$, where $\mathcal{M}(f)$ is the Mahler measure of f, so DD-sequences (conjecturally) have the ∞-Growth Property. See Section 6 for details.

Computing numerical examples, one quickly notices that higher-dimensional DD-sequences tend to be highly factorizable. We now explain why, which leads to a generalized definition of the DD-sequences that are the primary objects of study in this article.

An intrinsic and enlightening way to describe the classical Divisibility Property (1) is to view the positive integers $\mathbb{N}$ as a *partially ordered set* (*poset*), ordered by divisibility. Then a sequence $W : \mathbb{N} \to \mathbb{N}$ satisfies (1) if and only if it is a morphism of posets, i.e., a map that preserves the partial ordering.

Next we observe that a 1-dimensional DD-sequence may be viewed as assigning an integer $W_n(f)$ to each finite subgroup $\boldsymbol{\mu}_n$ of $\mathbb{C}^*$. Thus a 1-dimensional DD-sequence may be viewed as a poset morphism

$$\{\text{finite subgroups of } \mathbb{C}^*\} \to \mathbb{N}, \qquad \boldsymbol{\mu}_n \mapsto |W_n(f)|,$$

where we order the subgroups of $\mathbb{C}^*$ by inclusion and the elements of $\mathbb{N}$ by divisibility. This suggests that for higher-dimensional DD-sequences, we should define W to be a function on the set of all finite subgroups of $(\mathbb{C}^*)^N$, rather than restricting attention to subgroups of the form $\boldsymbol{\mu}_n^N$.

Further, there is no reason to restrict our coefficient ring to be $\mathbb{Z}$. Table 2 sets some notation that will remain in effect for the rest of this article.

Table 2. Notation

N	a positive integer
R	an integrally closed integral domain
K	the fraction field of R, with fixed separable closure $\bar{K}$
$R^{(N)}$	the ring of Laurent polynomials $R[X_1^{\pm 1}, \dots, X_N^{\pm 1}]$
$\langle \boldsymbol{\zeta} \rangle$	the cyclic subgroup generated by $\boldsymbol{\zeta} \in \mathbb{G}_{\mathrm{m}}^N(\bar{K})$
$\|\Lambda\|$	the cardinality of a finite subgroup $\Lambda \subset \mathbb{G}_{\mathrm{m}}^N(\bar{K})$

By a slight abuse of terminology, we view $R \setminus \{0\}$ as a poset under divisibility ([1]). We now define the "sequences" that are our primary object of study.

Definition. Let $f \in R^{(N)}$ be a non-zero Laurent polynomial. The *Divisor Divisibility sequence* (*DD-sequence*) associated to f is the map

$$W_f : \{\text{finite subgroups of } \mathbb{G}_{\mathrm{m}}^N(\bar{K})\} \to R, \qquad \Lambda \mapsto \prod_{\substack{\boldsymbol{\zeta} \in \Lambda \\ f(\boldsymbol{\zeta}) \neq 0}} f(\boldsymbol{\zeta}).$$

For notational convenience, we may at various times use $W_f(\Lambda)$, $W_\Lambda(f)$,

([1]) It is really the non-zero ideals that form a poset, since $a \mid b$ and $b \mid a$ only imply that $aR = bR$, not that $a = b$.

or $W(f,\Lambda)$ to denote the DD-sequence map, and when $\Lambda = \boldsymbol{\mu}_n^N$, we may write $W_n(f)$ or $W_f(n)$ for $W_f(\boldsymbol{\mu}_n^N)$.

Our first result provides some justification for this definition.

PROPOSITION 1. *Let $f \in R^{(N)}$ be a non-zero Laurent polynomial.*

(a) *Let $\Lambda \subseteq \mathbb{G}_{\mathrm{m}}^N(\bar{K})$ be a finite subgroup. Then $W_f(\Lambda) \in R$.*

(b) *The map W_f is a poset morphism, i.e.,*

$$\Lambda' \subseteq \Lambda \;\Rightarrow\; W_f(\Lambda') \,|\, W_f(\Lambda).$$

Proof. See Section 3. ∎

How large should we expect $W_f(\Lambda)$ to be as the size of Λ increases? We observe that $W_f(\Lambda)$ is a product of $\|\Lambda\|$ factors, and that the triangle inequality shows that each factor $f(\boldsymbol{\zeta})$ is bounded, independently of Λ. Thus $|W_f(\Lambda)|$ is likely to grow exponentially in $\|\Lambda\|$. If we further take a sequence of subgroups whose points become equidistributed in the torus

$$\mathbb{T}^N := \{\boldsymbol{z} = (z_1,\dots,z_N) \in \mathbb{C}^N : |z_1| = \cdots = |z_N| = 1\},$$

then it is natural to compare the growth rate of $W_f(\Lambda)$ to the *Mahler measure of f*, which we recall is the quantity

$$\mathcal{M}(f) = \exp\biggl(\int_{\mathbb{T}^N} \log|f(z_1,\dots,z_N)|\,\frac{dz_1}{z_1}\cdots\frac{dz_N}{z_N}\biggr);$$

see [15, 22]. For ease of exposition here, we state the growth conjecture only for the groups $\Lambda = \boldsymbol{\mu}_n^N$; see Section 6 for a general formulation.

CONJECTURE 2. *Let $f \in \bar{\mathbb{Q}}^{(N)} \subset \mathbb{C}^{(N)}$ be a non-zero Laurent polynomial with algebraic coefficients. Then*

$$\lim_{n\to\infty} |W_n(f)|^{1/n^N} = \mathcal{M}(f).$$

THEOREM 3. *Let $f \in \bar{\mathbb{Q}}^{(N)} \subset \mathbb{C}^{(N)}$ be a non-zero Laurent polynomial with algebraic coefficients.*

(a) *Conjecture 2 is true if $N = 1$.*

(b) *Conjecture 2 is true if $N \ge 2$ and f is* atoral*, which may be defined by the property that the intersection of the zero locus $\{f = 0\}$ and the torus $\mathbb{T}^N$ satisfies* ([2])

$$\dim\{\boldsymbol{z} \in \mathbb{T}^N : f(\boldsymbol{z}) = 0\} \le N-2, \tag{4}$$

where dim *is the dimension as a real-analytic subvariety of $\mathbb{T}^N$.*

([2]) The general definition is that an algebraic set $X \subseteq \mathbb{C}^N$ is *atoral* if there exists a non-zero regular function f on X that vanishes identically on $X \cap \mathbb{T}^N$. And a polynomial f is atoral if the hypersurface $f = 0$ is atoral. See [1].

The proof of Theorem 3(a), which we sketch in Section 6, uses a strong estimate for linear forms in logarithms. Theorem 3(b), which is due to Lind, Schmidt, and Verbitskiy [16], applies to "almost all" f, since generically for $N \geq 2$, the intersection $\{f = 0\} \cap \mathbb{T}^N$ has real codimension at least 2 in $\mathbb{T}^N$. We also mention that Conjecture 2 is false if f is allowed to have arbitrary complex coefficients, so any proof will necessarily require an arithmetic argument; see Remark 20 for details.

As noted earlier, DD-sequences tend to be highly factorizable. This is true even in the classical 1-dimensional setting, since if n is highly composite, then W_n has many factors coming from W_m for $m \,|\, n$. Classically, one generically factors W_n as $W_n = \prod_{m|n} V_m$, where the factors are defined either using the Möbius μ-function or using primitive nth roots. For ease of exposition, we take the latter approach here, but see Section 4 for both approaches and a proof of their equivalence.

PROPOSITION 4. *For each finite subgroup $\Lambda \subset \mathbb{G}_{\mathrm{m}}^N(\bar{K})$, let*

$$V_f(\Lambda) = \prod_{\boldsymbol{\zeta} \,:\, \langle \boldsymbol{\zeta} \rangle = \Lambda \text{ and } f(\boldsymbol{\zeta}) \neq 0} f(\boldsymbol{\zeta}),$$

so in particular, if Λ is not cyclic, then $V_f(\Lambda) = 1$. Then

$$V_f(\Lambda) \in R \quad \textit{and} \quad W_f(\Lambda) = \prod_{\Lambda' \subseteq \Lambda} V_f(\Lambda'),$$

where the product is over all subgroups Λ' of Λ.

Proposition 4 gives a generic factorization of $W_f(\Lambda)$, but it turns out that $V_f(\Lambda)$ may generically factor further, depending on Λ and the non-zero monomials appearing in f. The main result of Section 4 is Theorem 9, which describes the complete factorization of $W_f(\Lambda)$ when f is generic over $\mathbb{Q}$ for a prescribed pattern of non-zero monomials. For such f, we further show that W_f is a so-called *strong divisibility sequence* in the sense that there is an equality of ideals

$$\gcd(W_f(\Lambda_1), W_f(\Lambda_2)) = W_f(\Lambda_1 \cap \Lambda_2).$$

We next consider $\mathfrak{p}$-divisibility and $\mathfrak{p}$-adic behavior of the terms in a DD-sequence. This prompts several definitions, which are generalizations of the classical 1-dimensional case.

DEFINITION. Let $f \in R^{(N)}$ be a non-zero Laurent polynomial, let $\mathfrak{p}$ be a prime ideal of R, and let $\Lambda \subset \mathbb{G}_{\mathrm{m}}^N(\bar{K})$ be a finite subgroup. Suppose that

$$W_f(\Lambda) \in \mathfrak{p} \quad \text{and} \quad W_f(\Lambda') \notin \mathfrak{p} \quad \text{for all } \Lambda' \subsetneq \Lambda.$$

Then we say that $\mathfrak{p}$ is a *primitive prime divisor* of $W_f(\Lambda)$ and that Λ is a *rank of apparition* for $\mathfrak{p}$. We write

$$\mathcal{RA}_f(\mathfrak{p}) = \{\Lambda : \Lambda \text{ is a rank of apparition for } \mathfrak{p}\}.$$

It is not hard to prove (Proposition 22) that $\mathcal{RA}_f(\mathfrak{p})$ consists entirely of cyclic groups, so we define the *Zsigmondy set* of the DD-sequence W_f to be

$$\mathrm{Zsig}(f) = \{\text{cyclic } \Lambda : W_f(\Lambda) \text{ has no primitive prime divisors}\}.$$

When $N = 1$, it is not hard to show that W_f has a unique rank of apparition for $\mathfrak{p}$, i.e., there is an integer $r_{\mathfrak{p}} \geq 1$ with the property that

$$\mathfrak{p} \mid W_n(f) \;\Leftrightarrow\; r_{\mathfrak{p}} \mid n.$$

But when $N \geq 2$, the set $\mathcal{RA}_f(\mathfrak{p})$ may be infinite. The following analytic result, which is the main theorem of Section 6, shows in particular that $\mathcal{RA}_f(\mathfrak{p})$ cannot be too large. Again, for ease of exposition, we restrict here to $R = \mathbb{Z}$.

THEOREM 5. *Let $f \in \mathbb{Z}^{(N)}$ be a non-zero Laurent polynomial. There is a constant C_f such that for all $\epsilon > 0$,*

$$\sum_{p\,prime} \frac{\log p}{p} \sum_{\Lambda \in \mathcal{RA}_f(p)} \frac{1}{\|\Lambda\|^{\epsilon}} \leq (N+1)\epsilon^{-1} + C_f.$$

One consequence is the fact that the (cyclic) groups in $\mathcal{RA}_f(p)$ are comparatively sparse, since for example the series $\sum_{\Lambda\,\mathrm{cyclic}} \|\Lambda\|^s$ diverges for $\mathrm{Re}(s) < N$, while Theorem 5 says that if we restrict to $\Lambda \in \mathcal{RA}_f(p)$, then the sum converges for $\mathrm{Re}(s) > 0$. Theorem 5 also implies that for any $\theta > 0$, the (upper logarithmic) Dirichlet density of the set

$$\{p : \mathcal{RA}_f(p) \text{ contains a } \Lambda \text{ with } \|\Lambda\| < p^{\theta}\}$$

is at most $(N+1)\theta$. See Section 6 for details.

A much-studied classical problem is that of perfect powers, and more recently, powerful numbers, in divisibility sequences. For example, it is known that the only perfect powers in the Fibonacci sequence are 1, 8, and 144, a longstanding conjecture recently proven by Bugeaud, Mignotte, and Siksek [4]. The analogous question of classifying powerful Fibonacci numbers is still open. (We recall that n is *powerful* if, whenever $p \mid n$, then $p^2 \mid n$.) More generally, combining a result of Shorey and Stewart [25] with Siegel's theorem on integral points on curves gives an (ineffective) proof that there are only finitely many perfect powers in any non-degenerate binary recurrent sequence.

This suggests the general question of describing perfect powers and powerful numbers in higher-dimensional DD-sequences. We do not consider such questions in this paper, but we note that some care must be taken, because if the Laurent polynomial f has symmetries, then the associated DD-sequence is often divisible by large powers. We illustrate this principle in Section 9 by studying the DD-sequence for the family

$$P_T(X,Y) = X + X^{-1} + Y + Y^{-1} + T \in \mathbb{Z}[T]^{(2)},$$

so $W_n(P_T) \in \mathbb{Z}[T]$ is a polynomial of degree n^2. We prove that $W_n(P_T)$ is almost a perfect 8th power; more precisely, it factors in $\mathbb{Z}[T]$ as $W_n(P_T) = A_n(T)B_n(T)^8$ with $\deg B_n(T) = \frac{1}{8}n^2 + O(n)$. We also prove that $W_n(P_{2T+4})$ and $W_n(P_T)$ have a common factor in $\mathbb{Z}[T]$ of degree roughly $2n$.

In summary, there are many natural questions and problems associated to DD-sequences, some of which are direct analogues of the 1-dimensional situation, and some of which appear only in the higher-dimensional setting. And while some of these questions have elementary answers, others appear to lead to deep and interesting conjectures. In this article we give some elementary results, state some conjectures as motivation for the study of DD-sequences, and prove two deeper theorems:

- Generic factorization of DD-sequences, covered in Sections 4 and 5; see especially Theorems 8 and 9 and Proposition 14.
- Distribution of ranks of apparition, covered in Section 7; see especially Theorem 23 and Corollary 25.

Addendum. Recent preprints by Habegger [10] and Dimitrov [5] include proofs of Conjecture 2. The two papers use distinct methods, and the specific estimates that they prove are rather different, but both suffice to prove Conjecture 2. On the other hand, neither method seems to be strong enough to prove the growth conjecture for general algebraic subgroups of $\mathbb{G}_{\mathrm{m}}^N$ as described in Conjecture 16.

2. Some brief remarks on divisibility sequences. Factorization and other properties of sequences $a^n - b^n$ and the Fibonacci and Lucas sequences have been studied for a very long time, so we will not attempt to give a history. The arithmetic of elliptic divisibility sequences (EDS) was first seriously studied by Ward [34] and has since attracted considerable attention. Again, the literature is too vast to survey here.

The first reference of which we are aware for higher degree, but still one-dimensional, DD-sequences, is the 1916 Ph.D. thesis of T. Pierce [19]. He takes a monic polynomial $f(X) \in \mathbb{Z}[X]$, factors it (over $\mathbb{C}$) as $f(X) = \prod(X - \alpha_i)$, and studies elementary arithmetic properties of the associated 1-dimensional DD-sequence $W_n(f) = \prod_{i=1}^{d}(1 - \alpha_i^n)$. In particular, he gives various factorizations of $W_n(f)$ and studies the relationship between divisors of $W_n(f)$ and roots of $f(X) \equiv 0 \pmod{n}$, especially when n is prime or a prime power.

For higher-dimensional divisibility sequences, we have already mentioned the interesting sequences $\gcd(a^n - 1, b^n - 1)$ investigated in [2, 3], and there are analogous sequences on abelian varieties, for example the gcd of two EDS [27], but they do not appear to have the growth property. A general

"non-growth" theorem for sequences of this sort, conditional on Vojta's conjecture, is given in [28].

Marco Streng [32] has studied an interesting generalization of EDS in the case that the elliptic curve E has complex multiplication. He associates to a point $P \in E(K)$ a "sequence" indexed by the elements of the endomorphism ring, $\alpha \in \mathrm{End}(E)$, more or less by taking the (square root of the) denominator of $x(\alpha(P))$. He proves the Divisibility Property and a Zsigmondy theorem regarding primitive prime divisors.

Although somewhat different, we must also mention Stange's theory of elliptic nets [31]. This generalization of classical EDS attaches a "sequence" indexed by $\mathbb{Z}^r$ to a collection of linearly independent points $P_1, \ldots, P_r$ on an elliptic curve. She proves, among many results, that the terms in an elliptic net are generated by a non-linear recursion applied to a finite (but potentially quite large) set of initial values.

3. Basic properties of DD-sequences. We begin with the elementary proof of Proposition 1, where we note the importance in the proof of our assumption that R is an integrally closed integral domain.

Proof of Proposition 1. (a) The finite subgroup Λ of $\mathbb{G}_{\mathrm{m}}^N(\bar{K})$ and the set $\{\boldsymbol{z} \in \mathbb{G}_{\mathrm{m}}^N(\bar{K}) : f(\boldsymbol{z}) = 0\}$ are $\mathrm{Gal}(\bar{K}/K)$ invariant, so $W_f(\Lambda)$ is Galois invariant, and hence $W_f(\Lambda) \in K$. On the other hand, every root of unity is integral over R, so $W_f(\Lambda)$ is integral over R. But by assumption, the ring R is integrally closed, hence $W_f(\Lambda) \in R$.

(b) From (a) we know that $W_f(\Lambda)/W_f(\Lambda')$ is in K. Further, the inclusion $\Lambda' \subseteq \Lambda$ implies that the quotient

$$\frac{W_f(\Lambda)}{W_f(\Lambda')} = \prod_{\boldsymbol{\zeta} \in \Lambda \setminus (\Lambda' \cup \{f=0\})} f(\boldsymbol{\zeta})$$

is integral over R. Again the fact that R is integrally closed tells us that the quotient is in R. ∎

We next consider the factorization of a DD-sequence, analogous to the classical factorization of $X^n - 1$ as a product of cyclotomic polynomials. This latter factorization may be described either using primitive nth roots of unity or via the classical Möbius function. More generally, we note that there is a Möbius function attached to any (locally finite) poset [11, Section 8.6], so in particular there is a Möbius function associated to the set of finite subgroups of $\mathbb{G}_{\mathrm{m}}^N(\bar{K})$, ordered by inclusion. We denote this function by

$$\mu : \{\text{pairs of finite subgroups } \Lambda' \subseteq \Lambda \subset \mathbb{G}_{\mathrm{m}}^N(\bar{K})\} \to \mathbb{Z}. \tag{5}$$

It is characterized by $\mu(\Lambda, \Lambda) = 1$ and the Möbius inversion formula.

THEOREM 6. *Let $f \in R^{(N)}$ be a non-zero Laurent polynomial, and let $\Lambda \subset \mathbb{G}_{\mathrm{m}}^N(\bar{K})$ be a finite group.*

(a) *The following formula gives two equivalent ways to define a quantity $V_f(\Lambda)$:*

$$V_f(\Lambda) := \prod_{\substack{\boldsymbol{\zeta}\in\mathbb{G}_{\mathrm{m}}^N(\bar{K})\\ f(\boldsymbol{\zeta})\neq 0,\,\langle\boldsymbol{\zeta}\rangle=\Lambda}} f(\boldsymbol{\zeta}) = \prod_{\Lambda'\subseteq\Lambda} W_f(\Lambda')^{\mu(\Lambda,\Lambda')}.$$

In particular, if Λ is not cyclic, then $V_f(\Lambda) = 1$.

(b) *$V_f(\Lambda) \in R$.*

(c) *$W_f(\Lambda)$ factors in R as*

$$W_f(\Lambda) = \prod_{\Lambda'\subseteq\Lambda} V_f(\Lambda').$$

(d) *Let $\boldsymbol{\xi} \in \mathbb{G}_{\mathrm{m}}^N(\bar{K})$ have order n. Then*

$$V_f(\langle\boldsymbol{\xi}\rangle) = \prod_{\substack{d\in(\mathbb{Z}/n\mathbb{Z})^*\\ f(\boldsymbol{\xi}^d)\neq 0}} f(\boldsymbol{\xi}^d) \quad \textit{and} \quad W_f(\langle\boldsymbol{\xi}\rangle) = \prod_{\substack{d\in\mathbb{Z}/n\mathbb{Z}\\ f(\boldsymbol{\xi}^d)\neq 0}} f(\boldsymbol{\xi}^d).$$

Proof. (a) We start with the formula for $V_f(\Lambda)$ in terms of the Möbius function and derive the formula in terms of generators for Λ. We compute

$$\begin{aligned}\prod_{\Lambda'\subseteq\Lambda} W_f(\Lambda')^{\mu(\Lambda,\Lambda')} &= \prod_{\Lambda'\subseteq\Lambda}\Big(\prod_{\boldsymbol{\zeta}\in\Lambda'\setminus\{f=0\}} f(\boldsymbol{\zeta})\Big)^{\mu(\Lambda,\Lambda')}\\ &= \prod_{\boldsymbol{\zeta}\in\mathbb{G}_{\mathrm{m}}^N(\bar{K})_{\mathrm{tors}}\setminus\{f=0\}}\Big(\prod_{\Lambda'\,:\,\langle\boldsymbol{\zeta}\rangle\subseteq\Lambda'\subseteq\Lambda} f(\boldsymbol{\zeta})^{\mu(\Lambda,\Lambda')}\Big).\end{aligned}$$

Möbius inversion tells us that for any $\Lambda_1 \subseteq \Lambda_2$, we have

$$\sum_{\Lambda_1\subseteq\Lambda'\subseteq\Lambda_2} \mu(\Lambda_2,\Lambda') = \begin{cases} 1 & \text{if } \Lambda_1 = \Lambda_2,\\ 0 & \text{otherwise.}\end{cases}$$

Hence

$$\prod_{\Lambda'\subseteq\Lambda} W_f(\Lambda')^{\mu(\Lambda,\Lambda')} = \prod_{\substack{\boldsymbol{\zeta}\in\mathbb{G}_{\mathrm{m}}^N(\bar{K})_{\mathrm{tors}}\setminus\{f=0\}\,:\\ \langle\boldsymbol{\zeta}\rangle=\Lambda}} f(\boldsymbol{\zeta}),$$

which is the desired formula.

(b) We know from Proposition 1(a) that $W_f(\Lambda) \in R$, so the formula for $V_f(\Lambda)$ as a product of (positive and negative) powers of $W_f(\Lambda')$ shows that $V_f(\Lambda) \in K$. On the other hand, the formula for $V_f(\Lambda)$ as a product of values of $f(\boldsymbol{\zeta})$ for N-tuples of roots of unity $\boldsymbol{\zeta} \in \mathbb{G}_{\mathrm{m}}^N(\bar{K})_{\mathrm{tors}}$ shows that $V_f(\Lambda)$ is integral over R. Hence $V_f(\Lambda) \in R$ by our assumption that R is integrally closed.

(c) This is just Möbius inversion, but we do the calculation. We have

$$\prod_{\Lambda'\subseteq\Lambda} V_f(\Lambda') = \prod_{\Lambda'\subseteq\Lambda}\prod_{\Lambda''\subseteq\Lambda'} W_f(\Lambda'')^{\mu(\Lambda',\Lambda'')} = \prod_{\Lambda''\subseteq\Lambda}\prod_{\Lambda''\subseteq\Lambda'\subseteq\Lambda} W_f(\Lambda'')^{\mu(\Lambda',\Lambda'')}$$
$$= W_f(\Lambda) \quad \text{from Möbius inversion.}$$

(d) The first formula is immediate from (a) applied to the cyclic group $\Lambda = \langle\boldsymbol{\zeta}\rangle$, and then the second formula follows from the first and the factorization of $W_f(\Lambda)$ given in (c). ∎

4. Generic factorization of DD-sequences. Theorem 6(c) gives a generic factorization of $W_f(\Lambda)$ in R that is analogous to the factorization of X^n-1 as a product of cyclotomic polynomials, but it turns out that $W_f(\Lambda)$ may admit a further generic factorization, depending on the interaction of Λ with the non-zero monomials appearing in f. In this section we describe this factorization and prove that if $K\cap\bar{\mathbb{Q}} = \mathbb{Q}$ and the non-zero coefficients of f are algebraically independent over $\mathbb{Q}$, then $W_f(\Lambda)$ does not factor further. This last result is a DD-sequence analogue of the irreducibility of the cyclotomic polynomials over $\mathbb{Q}$. And in the next section (Proposition 14) we use these results to show that a generic DD-sequence satisfies a strong divisibility property given by an equality of ideals ([3])

$$\gcd_R(W_f(\Lambda_1), W_f(\Lambda_2)) = W_f(\Lambda_1\cap\Lambda_2)R.$$

We begin with some useful notation. In order to write elements of $R^{(N)}$ succinctly, for N-tuples

$$\boldsymbol{m} = (m_1,\dots,m_N)\in\mathbb{Z}^N \quad\text{and}\quad \boldsymbol{X} = (X_1,\dots,X_N),$$

we let

$$\boldsymbol{X}^{\boldsymbol{m}} = X_1^{m_1}\cdots X_N^{m_N}.$$

Then every $f\in R^{(N)}$ can be written as

$$f(\boldsymbol{X}) = \sum_{\boldsymbol{m}\in\mathbb{Z}^N} a_{\boldsymbol{m}}(f)\boldsymbol{X}^{\boldsymbol{m}}$$

with $a_{\boldsymbol{m}}(f)\in R$ and all but finitely many $a_{\boldsymbol{m}}(f)$ equal to 0. We note that the unit group of $R^{(N)}$ is exactly the set of monomials with unit coefficients, i.e., $\{u\boldsymbol{X}^{\boldsymbol{m}} : \boldsymbol{m}\in\mathbb{Z}^N,\ u\in R^*\}$. As usual, we say that an element $f\in R^{(N)}$ is *irreducible* if it is not a unit and has no factorizations $f = gh$ except with g or h a unit.

Example 7. We give an example illustrating the fact that $W_f(\Lambda)$ may admit a further generic factorization beyond its factorization as a product

([3]) This generalizes the classical *strong divisibility property* $\gcd(W_m, W_n) = W_{\gcd(m,n)}$ satisfied, for example, by the Fibonacci and Lucas sequences.

of $V_f(\Lambda')$ values as in Theorem 6(c). Let $f(X) = aX^2 - b$ with a and b independent indeterminates. Then

$$V_f(\boldsymbol{\mu}_n) = \prod_{\zeta\,:\,\langle\zeta\rangle=\boldsymbol{\mu}_n} (a\zeta^2 - b) = \begin{cases} \Phi_n(a,b) & \text{if } n \text{ is odd,} \\ \Phi_{n/2}(a,b)^2 & \text{if } n \text{ is even,} \end{cases}$$

where $\Phi_n(U,V) \in \mathbb{Z}[U,V]$ is the homogenized nth cyclotomic polynomial. Thus if n is even, then $V_f(\boldsymbol{\mu}_n)$ is generically a square. This is due to the fact that $f(X)$ is a polynomial in X^2.

Our next result generalizes Example 7 to all DD-sequences, but first we need some additional notation.

DEFINITION. Let $f \in R^{(N)}$. The *set of monomials* of f is

$$M(f) = \{\boldsymbol{m} \in \mathbb{Z}^N : a_{\boldsymbol{m}}(f) \neq \mathbf{0}\}.$$

For any finite subset $M \subset \mathbb{Z}^N$ and any $\boldsymbol{\xi} \in \mathbb{G}_{\mathrm{m}}^N(\bar{K})_{\mathrm{tors}}$, we let

$$\boldsymbol{\xi}^M = \{\boldsymbol{\xi}^{\boldsymbol{m}} : \boldsymbol{m} \in M\}, \qquad K(\boldsymbol{\xi}^M) = (\text{the field generated by } \boldsymbol{\xi}^M).$$

We note that $K(\boldsymbol{\xi}^M)$ is a Galois extension of K, since even in the case that K has positive characteristic, adjoining roots of unity gives a separable extension. Further, $\mathrm{Gal}(K(\boldsymbol{\xi}^M)/K)$ is abelian.

THEOREM 8. *For $f \in R^{(N)}$ and $\boldsymbol{\xi} \in \mathbb{G}_{\mathrm{m}}^N(\bar{K})_{\mathrm{tors}}$, define*

$$C_f(\boldsymbol{\xi}) = \prod_{\tau \in \mathrm{Gal}(K(\boldsymbol{\xi}^{M(f)})/K)} \tau(f(\boldsymbol{\xi})).$$

(a) $C_f(\boldsymbol{\xi}) \in R$.

(b) *Let $\Lambda \subset \mathbb{G}_{\mathrm{m}}^N(\bar{K})_{\mathrm{tors}}$ be a cyclic group, and let $\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_r$ be generators for Λ that are representatives for the distinct orbits for* $\mathrm{Gal}(\bar{K}/K)$ *acting on the set of all generators of Λ. Then $V_f(\Lambda)$ factors in R as*

$$V_f(\Lambda) = \prod_{i=1}^{r} C_f(\boldsymbol{\xi}_i)^{[K(\boldsymbol{\xi}_i):K(\boldsymbol{\xi}_i^{M(f)})]}.$$

(c) *Let $\Lambda \subset \mathbb{G}_{\mathrm{m}}^N(\bar{K})$ be a finite group. Then $W_f(\Lambda)$ factors in R as*

$$W_f(\Lambda) = \prod_{\substack{\text{cyclic sub-} \\ \text{groups } \Lambda' \subset \Lambda}} \prod_{\substack{\text{generators } \boldsymbol{\xi} \text{ for } \Lambda' \text{ lying} \\ \text{in distinct } \mathrm{Gal}(\bar{K}/K)\text{-orbits}}} C_f(\boldsymbol{\xi})^{[K(\boldsymbol{\xi}):K(\boldsymbol{\xi}^{M(f)})]}.$$

Proof. (a) The quantity $f(\boldsymbol{\xi})$ is in $K(\boldsymbol{\xi}^{M(f)})$, so the product of all of the $K(\boldsymbol{\xi}^{M(f)})/K$-conjugates of $f(\boldsymbol{\xi})$ is in K, and hence $C_f(\boldsymbol{\xi}) \in K$. On the other hand, each $\tau(f(\boldsymbol{\xi}))$ is integral over R, so $C_f(\boldsymbol{\xi})$ is integral over R. Hence $C_f(\boldsymbol{\xi}) \in R$ from our assumption that R is integrally closed.

(b) The coordinates of any element $\boldsymbol{\xi} \in \mathbb{G}_{\mathrm{m}}^N(\bar{K})_{\mathrm{tors}}$ are roots of unity, so for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$, we have $\sigma(\boldsymbol{\xi}) = \boldsymbol{\xi}^k$ for some $k = k(\sigma)$. It follows

that $\mathrm{Gal}(\bar{K}/K)$ acts on Λ, and similarly it acts on the set of generators of Λ. This justifies our choice of representatives for the orbits. Further, the action factors through an abelian group, since roots of unity generate abelian extensions. We now compute (for notational convenience we assume that all products omit any factors that vanish)

$$\begin{aligned}
V_f(\Lambda) &= \prod_{\text{generators } \boldsymbol{\xi} \text{ for } \Lambda} f(\boldsymbol{\xi}) && \text{from Theorem 6(a)}\\
&= \prod_{i=1}^{r} \prod_{\lambda\in\mathrm{Gal}(K(\boldsymbol{\xi}_i)/K)} f(\lambda(\boldsymbol{\xi}_i)) && \text{since } \boldsymbol{\xi}_1,\dots,\boldsymbol{\xi}_r \text{ are orbit reps}\\
&= \prod_{i=1}^{r} \Bigl(\prod_{\substack{\sigma\in\mathrm{Gal}(K(\boldsymbol{\xi}_i)/K(\boldsymbol{\xi}_i^{M(f)}))\\ \tau\in\mathrm{Gal}(K(\boldsymbol{\xi}_i^{M(f)})/K)}} \sigma\tau(f(\boldsymbol{\xi}_i)) \Bigr)\\
&= \prod_{i=1}^{r} \Bigl(\prod_{\tau\in\mathrm{Gal}(K(\boldsymbol{\xi}_i^{M(f)})/K)} \tau(f(\boldsymbol{\xi}_i)) \Bigr)^{[K(\boldsymbol{\xi}):K(\boldsymbol{\xi}^{M(f)})]}\\
& && \text{since } \mathrm{Gal}(K(\boldsymbol{\xi}_i)/K(\boldsymbol{\xi}_i^{M(f)})) \text{ fixes } f(\boldsymbol{\xi}_i)\\
&= \prod_{i=1}^{r} C_f(\boldsymbol{\xi}_i)^{[K(\boldsymbol{\xi}):K(\boldsymbol{\xi}^{M(f)})]} && \text{by definition of } C_f.
\end{aligned}$$

(c) This follows from (b) and the decomposition of $W_f(\Lambda)$ as a product of $V_f(\Lambda')$ values in Theorem 6(c). ∎

Theorem 8(c) gives a factorization of $W_f(\Lambda)$ in R that is a product of powers of $C_f(\boldsymbol{\xi})$ values. For particular choices of R, f, and Λ, it is quite possible for these $C_f(\boldsymbol{\xi})$ to factor further. The main result of this section says that if the coefficients of f are generic for the given pattern $M(f)$ of non-zero coefficients, then the $C_f(\boldsymbol{\xi})$ appearing in Theorem 8(c) are irreducible in R. In particular, combining Theorem 9 with Corollary 11 gives a generalization to DD-sequences of the classical result that the complete factorization of $X^n - 1$ in $\mathbb{Q}[X]$ is as a product of cyclotomic polynomials.

THEOREM 9. *Let $\mathbb{F}$ be a field, let $M \subset \mathbb{Z}^N$ be a finite set with $\mathbf{0} \in M$, let R be the polynomial ring*

$$R = \mathbb{F}[a_{\boldsymbol{m}}]_{\boldsymbol{m}\in M},$$

where the $a_{\boldsymbol{m}}$ are independent indeterminates, and let $f_M \in R^{(N)}$ be the Laurent polynomial

$$f_M(\boldsymbol{X}) = \sum_{\boldsymbol{m}\in M} a_{\boldsymbol{m}} \boldsymbol{X}^{\boldsymbol{m}} \in R^{(N)}.$$

Thus f_M is the generic Laurent polynomial over $\mathbb{F}$ whose non-zero monomials are in the positions specified by M.

(a) *For all $\boldsymbol{\xi} \in \mathbb{G}_{\mathrm{m}}^N(\bar{K})_{\mathrm{tors}}$, the element*

$$C_{f_M}(\boldsymbol{\xi}) := \prod_{\tau \in \mathrm{Gal}(\mathbb{F}(\boldsymbol{\xi}^M)/\mathbb{F})} \tau(f_M(\boldsymbol{\xi})) \in R \tag{6}$$

described in Theorem 8 is irreducible in R.

(b) *The formula in Theorem 8(c) is a complete factorization of $W_{f_M}(\Lambda)$ into irreducible elements of R.*

REMARK 10. In the setting of Theorem 9, if we drop the condition that $\mathbf{0} \in M$, then it is possible for $C_{f_M}(\boldsymbol{\xi})$ to be reducible. For example, take $\mathbb{F} = \mathbb{Q}$, let $\boldsymbol{m}, \boldsymbol{n} \in \mathbb{Z}^N$ be exponents with $\boldsymbol{\xi}^{\boldsymbol{m}} \neq \pm 1$ and $\boldsymbol{\xi}^{\boldsymbol{n}} = 1$, and let $M = \{\boldsymbol{m}, \boldsymbol{m}+\boldsymbol{n}\}$. Then $\boldsymbol{\xi}^M = \{\boldsymbol{\xi}^{\boldsymbol{m}}\}$ consists of a single element, and

$$\begin{aligned} C_{f_M}(\boldsymbol{\xi}) &= \prod_{\tau \in \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\xi}^M)/\mathbb{Q})} \tau(f_M(\boldsymbol{\xi})) = \prod_{\tau \in \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\xi}^{\boldsymbol{m}})/\mathbb{Q})} \tau(f_M(\boldsymbol{\xi})) \\ &= \prod_{\tau \in \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\xi}^{\boldsymbol{m}})/\mathbb{Q})} \tau(f_M(1)\boldsymbol{\xi}^{\boldsymbol{m}}) \quad \text{since } M = \{\boldsymbol{m}, \boldsymbol{m}+\boldsymbol{n}\} \\ &= f_M(1)^{[\mathbb{Q}(\boldsymbol{\xi}^{\boldsymbol{m}}):\mathbb{Q}]}\, \mathrm{N}_{\mathbb{Q}(\boldsymbol{\xi}^{\boldsymbol{m}})/\mathbb{Q}}\, \boldsymbol{\xi}^{\boldsymbol{m}} = \pm f_M(1)^{[\mathbb{Q}(\boldsymbol{\xi}^{\boldsymbol{m}}):\mathbb{Q}]}. \end{aligned}$$

Since $\boldsymbol{\xi}^{\boldsymbol{m}} \neq \pm 1$ by assumption, we have $\boldsymbol{\xi}^{\boldsymbol{m}} \notin \mathbb{Q}$, so $C_{f_M}(\boldsymbol{\xi})$ is reducible. For an explicit example, we take $N = 1$, $M = \{1, 5\}$, $f(X) = a_1 X + a_5 X^5$, and $\boldsymbol{\xi} = i = \sqrt{-1}$. Then $\boldsymbol{\xi}^M = \{i, i^5\} = \{i\}$ and

$$C_{f_M}(\boldsymbol{\xi}) = \prod_{\tau \in \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})} \tau(a_1 i + a_5 i^5) = (a_1 i + a_5 i)(-a_1 i - a_5 i) = (a_1 + a_5)^2.$$

Proof of Theorem 9. Each factor $\tau(f_M(\boldsymbol{\xi}))$ in the product (6) that defines $C_{f_M}(\boldsymbol{\xi})$ is a non-trivial homogeneous linear form in the indeterminates $a_{\boldsymbol{m}}$, and such linear forms are irreducible in the polynomial ring $R \otimes_{\mathbb{F}} \mathbb{F}(\boldsymbol{\xi}^M)$, which is a UFD. Hence any non-constant factor of $C_{f_M}(\boldsymbol{\xi})$ in R has the form

$$\beta \prod_{\tau \in H} \tau(f_M(\boldsymbol{\xi})) \in R \tag{7}$$

for some $\beta \in \mathbb{F}(\boldsymbol{\xi}^M)^*$ and some non-empty subset

$$H \subseteq \mathrm{Gal}(K(\boldsymbol{\xi}^M)/K) = \mathrm{Gal}(\mathbb{F}(\boldsymbol{\xi}^M)/\mathbb{F}).$$

We now use the assumption that $\mathbf{0} \in M$, which implies that $f_M(\boldsymbol{\xi})$ has an $a_{\mathbf{0}}$ term. The elements of H act trivially on $a_{\mathbf{0}}$, so (7) has a monomial of the form $\beta a_{\mathbf{0}}^{\#H}$. But (7) is in R, i.e., its coefficients are in $\mathbb{F}$, so $\beta \in \mathbb{F}^*$.

Next we apply an arbitrary element $\sigma \in \mathrm{Gal}(\mathbb{F}(\boldsymbol{\xi}^M)/\mathbb{F})$ to the product (7). By assumption, this leaves the product invariant, so again by unique factorization in $R \otimes_{\mathbb{F}} \mathbb{F}(\boldsymbol{\xi}^M)$ and the fact that the homogeneous linear forms

$f_M(\xi)$ are irreducible, we deduce that for all $\sigma \in \mathrm{Gal}(\mathbb{F}(\boldsymbol{\xi}^M)/\mathbb{F})$ and all $\tau \in H$ there is a $\lambda_{\sigma,\tau} \in H$ and a scalar $\gamma_{\sigma,\tau} \in \mathbb{F}(\boldsymbol{\xi}^M)^*$ such that

$$\sigma(\tau(f_M(\boldsymbol{\xi}))) = \gamma_{\sigma,\tau} \cdot \lambda_{\sigma,\tau}(f_M(\boldsymbol{\xi})). \tag{8}$$

Again using the assumption that $\mathbf{0} \in M$, we look at the $a_{\mathbf{0}}$ monomial on both sides of (8). This monomial is unaffected by the action of Galois, which allows us to conclude that $\gamma_{\sigma,\tau} = 1$. Expanding (8) gives

$$\sum_{\boldsymbol{m}\in M} \sigma\tau(\boldsymbol{\xi}^{\boldsymbol{m}})a_{\boldsymbol{m}} = \sum_{\boldsymbol{m}\in M} \lambda_{\sigma,\tau}(\boldsymbol{\xi}^{\boldsymbol{m}})a_{\boldsymbol{m}}.$$

Keeping in mind that the $a_{\boldsymbol{m}}$ are indeterminates, we find that

$$\sigma\tau(\boldsymbol{\xi}^{\boldsymbol{m}}) = \lambda_{\sigma,\tau}(\boldsymbol{\xi}^{\boldsymbol{m}}) \quad \text{for all } \boldsymbol{m} \in M,$$

and then, since $\sigma, \tau, \lambda_{\sigma,\tau} \in \mathrm{Gal}(\mathbb{F}(\boldsymbol{\xi}^M)/\mathbb{F})$, we conclude that

$$\sigma\tau = \lambda_{\sigma,\tau}.$$

The key here is the fact that τ and $\lambda_{\sigma,\tau}$ are in H, while σ is an arbitrary element of $\mathrm{Gal}(\mathbb{F}(\boldsymbol{\xi}^M)/\mathbb{F})$. Hence for any $g \in \mathrm{Gal}(\mathbb{F}(\boldsymbol{\xi}^M)/\mathbb{F})$ and any $h \in H$, we can take $\sigma = gh^{-1}$ and $\tau = h$ to conclude that

$$g = gh^{-1}h = \lambda_{gh^{-1},h} \in H.$$

This proves that $H = \mathrm{Gal}(\mathbb{F}(\boldsymbol{\xi}^M)/\mathbb{F})$, and thus that the product (7) is equal to $C_{f_M}(\boldsymbol{\xi}^\vee)$ up to multiplication by an element of $\mathbb{F}^*$. This proves (a), and (b) is immediate from (a) and Theorem 8(c). ∎

Corollary 11. *Assume that* $\mathrm{char}(K) = 0$ *and that* $K \cap \bar{\mathbb{Q}} = \mathbb{Q}$. *Let* $f \in R^{(N)}$, *and let* $\boldsymbol{\xi} \in \mathbb{G}_{\mathrm{m}}^N(\bar{K})_{\mathrm{tors}}$. *Then:*

(a) $V_f(\langle\boldsymbol{\xi}\rangle) = C_f(\boldsymbol{\xi})^{[\mathbb{Q}(\boldsymbol{\xi}):\mathbb{Q}(\boldsymbol{\xi}^{M(f)})]}$.

(b) $W_f(\langle\boldsymbol{\xi}\rangle) = \displaystyle\prod_{\substack{\text{cyclic sub-}\\ \text{groups } \langle\boldsymbol{\zeta}\rangle\subset\langle\boldsymbol{\xi}\rangle}} C_f(\boldsymbol{\zeta})^{[K(\boldsymbol{\zeta}):K(\boldsymbol{\zeta}^{M(f)})]}$.

Further, if f *is generic for its pattern of non-zero coefficients as in Theorem* 9, *then* (a) *and* (b) *give the complete factorizations of* V_f *and* W_f *in* R.

The proof of Corollary 11 uses Theorem 8 and the following transitivity result, which is more-or-less equivalent to the irreducibility of the cyclotomic polynomials over $\mathbb{Q}$.

Lemma 12. *Assume* $\mathrm{char}(K)=0$ *and* $K\cap\bar{\mathbb{Q}}=\mathbb{Q}$. *Let* $\boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2 \in \mathbb{G}_{\mathrm{m}}^N(\bar{K})_{\mathrm{tors}}$. *Then the following are equivalent*:

(a) *The points* $\boldsymbol{\zeta}_1$ *and* $\boldsymbol{\zeta}_2$ *generate the same cyclic subgroup of* $\mathbb{G}_{\mathrm{m}}^N(\bar{K})$.

(b) *There is a* $\sigma \in \mathrm{Gal}(\bar{K}/K)$ *such that* $\boldsymbol{\zeta}_2 = \sigma(\boldsymbol{\zeta}_1)$.

Proof. Let $\Lambda \subset \mathbb{G}_{\mathrm{m}}^N(\bar{K})$ be a finite subgroup, let $d = \#\Lambda$, let $\zeta_d \in \bar{K}$ be a primitive dth root of unity, and let $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Then $\sigma(\zeta_d) = \zeta_d^k$ for some $k = k(\sigma)$. Since every coordinate of every element $\boldsymbol{\xi} \in \Lambda$ is a power of ζ_d, we have $\sigma(\boldsymbol{\xi}) = \boldsymbol{\xi}^k$. Since Λ is a subgroup, it follows that $\sigma(\Lambda) \subseteq \Lambda$, and since σ is invertible, we see that $\sigma(\Lambda) = \Lambda$. Applying this to $\Lambda = \langle \boldsymbol{\zeta}_1 \rangle$, we find that

$$\boldsymbol{\zeta}_2 = \sigma(\boldsymbol{\zeta}_1) \;\Rightarrow\; \langle \boldsymbol{\zeta}_2 \rangle = \langle \sigma(\boldsymbol{\zeta}_1) \rangle = \sigma(\langle \boldsymbol{\zeta}_1 \rangle) = \langle \boldsymbol{\zeta}_1 \rangle.$$

This completes the proof that (b) implies (a).

For the reverse implication, we assume that $\langle \boldsymbol{\zeta}_2 \rangle = \langle \boldsymbol{\zeta}_1 \rangle$. Write

$$\boldsymbol{\zeta}_1 = (\zeta_1, \ldots, \zeta_N) \quad \text{with } \zeta_i \text{ a primitive } r_i\text{th root of unity.}$$

Then

$$r := \#\langle \boldsymbol{\zeta}_1 \rangle = \mathrm{LCM}(r_1, \ldots, r_N).$$

By assumption, there are exponents k and ℓ such that $\boldsymbol{\zeta}_2 = \boldsymbol{\zeta}_1^k$ and $\boldsymbol{\zeta}_1 = \boldsymbol{\zeta}_2^\ell$. Then $\boldsymbol{\zeta}_1^{k\ell} = 1$, so

$$k\ell \equiv 1 \pmod{r_i} \quad \text{for all } 1 \le i \le N,$$

and hence

$$k\ell \equiv 1 \pmod{r}.$$

In particular, we have $\gcd(k, r) = 1$, so there exists an element

$$\sigma \in \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_r)/\mathbb{Q}) \subset \mathrm{Gal}(K(\boldsymbol{\mu}_r)/K)$$

with the property that

$$\sigma(\eta) = \eta^k \quad \text{for every } \eta \in \boldsymbol{\mu}_r.$$

(This is where we use the assumption that $K \cap \bar{\mathbb{Q}} = \mathbb{Q}$ and the standard fact that $\mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_r)/\mathbb{Q}) \cong (\mathbb{Z}/r\mathbb{Z})^*$.) The coordinates of $\boldsymbol{\zeta}_1$ are in $\boldsymbol{\mu}_r$, so we find that

$$\sigma(\boldsymbol{\zeta}_1) = \boldsymbol{\zeta}_1^k = \boldsymbol{\zeta}_2.$$

This completes the proof that (a) implies (b). ∎

Proof of Corollary 11. Lemma 12 tells us that $\mathrm{Gal}(\bar{K}/K)$ acts transitively on the generators of the cyclic subgroup $\langle \boldsymbol{\xi} \rangle$, so the formulas in (a) and (b) are immediate consequences of Theorem 8(b) and (c). Then the final statement follows from Theorem 9 which tells us that, under our genericity assumption, each $C_f(\boldsymbol{\xi})$ is irreducible in R. ∎

5. Strong divisibility of generic DD-sequences. Classical one-dimensional divisibility sequences over $\mathbb{Z}$, such as $a^n - b^n$, Fibonacci and Lucas sequences, and elliptic divisibility sequences, have the strong divisibility property

$$\gcd(W_m, W_n) = \pm W_{\gcd(m,n)},$$

and it is an exercise to show that such strong divisibility sequences are automatically divisibility sequences.

EXAMPLE 13. It is easy to construct examples showing that higher-dimensional DD-sequences need not be strong divisibility sequences. For example, the DD-sequence associated to $f(X,Y) = X - Y - 4$ satisfies

$$\begin{aligned} W_4(f) &= 2^{16} \cdot 3 \cdot 5^3 \cdot 13^2, \\ W_6(f) &= 2^{18} \cdot 3^6 \cdot 5^2 \cdot 7^5 \cdot 13^2 \cdot 19^2 \cdot 31^2, \\ \gcd(W_4(f), W_6(f)) &= 2^{16} \cdot 3 \cdot 5^2 \cdot 13^2, \\ W_{\gcd(4,6)}(f) = W_2(f) &= 2^6 \cdot 3. \end{aligned}$$

Our main result in this section says that *generic* DD-sequences do have the strong divisibility property.

PROPOSITION 14. *Let $\mathbb{F}$, M, R, and f_M be as in the statement of Theorem 9, so in particular R is a UFD. Assume further that $\#M \ge 2$, i.e., f_M is not a monomial. Let Λ_1 and Λ_2 be finite subgroups of $\mathbb{G}_{\mathrm{m}}^N(\bar{K})$. Then there is an equality of ideals* ([4])

$$\gcd_R(W_{f_M}(\Lambda_1), W_{f_M}(\Lambda_2)) = W_{f_M}(\Lambda_1 \cap \Lambda_2)R.$$

The proof uses the following key result.

LEMMA 15. *Continuing the notation from Proposition 14, let Λ_1 and Λ_2 be finite subgroups of $\mathbb{G}_{\mathrm{m}}^N(\bar{K})$. Then*

$$\Lambda_1 \ne \Lambda_2 \;\Rightarrow\; \gcd_R(V_{f_M}(\Lambda_1), V_{f_M}(\Lambda_2)) = 1,$$

where this is an equality of ideals in R, which is a UFD.

Proof. If Λ_1, respectively Λ_2, is not cyclic, then Theorem 6(a) says that $V_{f_M}(\Lambda_1)$, respectively $V_{f_M}(\Lambda_2)$, is 1, so the conclusion is automatically true.

We are thus reduced to the case that $\Lambda_1 = \langle \boldsymbol{\xi}_1 \rangle$ and $\Lambda_2 = \langle \boldsymbol{\xi}_2 \rangle$. Writing n_1 and n_2 for the orders of $\boldsymbol{\xi}_1$ and $\boldsymbol{\xi}_2$, respectively, from Theorem 6(a) we get

$$V_{f_M}(\Lambda_1) = \prod_{i \in (\mathbb{Z}/n_1\mathbb{Z})^*} f_M(\boldsymbol{\xi}_1^i) \quad \text{and} \quad V_{f_M}(\Lambda_2) = \prod_{j \in (\mathbb{Z}/n_2\mathbb{Z})^*} f_M(\boldsymbol{\xi}_2^j).$$

We prove the contrapositive of the desired statement, so we suppose that the gcd is larger than 1 and aim to prove that $\Lambda_1 = \Lambda_2$. Our assumption is that $V_{f_M}(\Lambda_1)$ and $V_{f_M}(\Lambda_2)$ have a common non-trivial factor in R, so they also have a common non-trivial factor in the UFD $R \otimes_{\mathbb{F}} \overline{\mathbb{F}}$. But the quantities $f_M(\boldsymbol{\xi}_1^i)$ and $f_M(\boldsymbol{\xi}_2^j)$ are irreducible in $R \otimes_{\mathbb{F}} \overline{\mathbb{F}}$, since they are linear forms in

([4]) The quantity $\gcd_R(a,b)$ denotes the largest ideal dividing both a and b. This is well-defined for any UFD, but we note that it is not, in general, equal to the ideal generated by a and b, the latter being a property of PIDs.

the variables $a_{\boldsymbol{m}}$. It follows that there exists an i and a j such that

$$f_M(\boldsymbol{\xi}_1^i) = u f_M(\boldsymbol{\xi}_2^j) \quad \text{for some unit } u \in (R \otimes_{\mathbb{F}} \overline{\mathbb{F}})^* = \overline{\mathbb{F}}^*.$$

Keeping in mind that the non-zero coefficients $a_{\boldsymbol{m}}$ of f_M are independent indeterminates and that $a_{\boldsymbol{0}} \neq 0$, we first find that $u = 1$ by comparing the coefficients of $a_{\boldsymbol{0}}$, and then we find that $\boldsymbol{\xi}_1^i = \boldsymbol{\xi}_2^j$ by comparing the coefficients of $a_{\boldsymbol{m}}$ for any non-zero $\boldsymbol{m} \in M(f)$.

We know that $\gcd(i, n_1) = 1$, so we can find a k with $ik \equiv 1 \pmod{n_1}$. Then $\boldsymbol{\xi}_1 = \boldsymbol{\xi}_1^{ik} = \boldsymbol{\xi}_2^{jk} \in \langle \boldsymbol{\xi}_2 \rangle$, and similarly using $\gcd(j, n_2) = 1$, we find that $\boldsymbol{\xi}_2 \in \langle \boldsymbol{\xi}_1 \rangle$. Hence $\langle \boldsymbol{\xi}_1 \rangle = \langle \boldsymbol{\xi}_2 \rangle$, i.e, $\Lambda_1 = \Lambda_2$. ∎

Proof of Proposition 14. We compute

$$\begin{aligned}
\gcd(W_{f_M}(\Lambda_1), W_{f_M}(\Lambda_2)) &= \gcd\Big(\prod_{\Lambda \subseteq \Lambda_1} V_{f_M}(\Lambda), \prod_{\Lambda' \subseteq \Lambda_2} V_{f_M}(\Lambda') \Big) \\
&= \prod_{\Lambda \subseteq \Lambda_1 \text{ and } \Lambda \subseteq \Lambda_2} V_{f_M}(\Lambda) \quad \text{from Lemma 15} \\
&= \prod_{\Lambda \subseteq \Lambda_1 \cap \Lambda_2} V_{f_M}(\Lambda) = W_{f_M}(\Lambda_1 \cap \Lambda_2). \ ∎
\end{aligned}$$

6. ∞-Growth properties of DD-sequences. In this section we consider the growth rate of a DD-sequence $W_f(\Lambda)$ as a function of $\|\Lambda\|$. As noted earlier, intuitively we expect $\log |W_f(\Lambda)|$ to grow like a multiple of $\|\Lambda\|$, but there are subtle Diophantine issues at play due to the possibility of an element $\boldsymbol{\zeta} \in \Lambda$ lying very close to a root of f, thereby contributing a very small factor $f(\boldsymbol{\zeta})$ to $W_f(\Lambda)$. Before stating our main growth conjecture, we need a number of definitions.

Definition. Let $G \subseteq \mathbb{G}_{\mathrm{m}}^N$ be an algebraic subgroup. We let

$$\mathbb{T}(G) := G(\mathbb{C}) \cap \mathbb{T}^N = \{\boldsymbol{z} \in G(\mathbb{C}) : |z_1| = \cdots = |z_N| = 1\},$$

and we let μ_G denote normalized Haar measure on the real torus $\mathbb{T}(G)$. Let $f \in \mathbb{C}^{(N)}$ be a non-zero Laurent polynomial. Then the *G-Mahler measure* of f is

$$\mathcal{M}_G(f) := \exp\Big(\int_{\mathbb{T}(G)} \log |f(\boldsymbol{z})| \, d\mu_G(\boldsymbol{z}) \Big).$$

For example, if $G = \mathbb{G}_{\mathrm{m}}^N$, then $\mathcal{M}_G(f)$ is the classical Mahler measure. For each finite subgroup $\Lambda \subset \mathbb{G}_{\mathrm{m}}^N(\mathbb{C})$, we define a measure

$$\mu_\Lambda := \frac{1}{\|\Lambda\|} \sum_{\boldsymbol{\zeta} \in \Lambda} \delta_{\boldsymbol{\zeta}},$$

where $\delta_{\boldsymbol{\zeta}}$ denotes a point mass at $\boldsymbol{\zeta}$. We then say that a collection $\mathcal{L}$ of

finite subgroups of $\mathbb{G}_{\mathrm{m}}^N(\mathbb{C})$ *converges to* G if there is a weak convergence of measures

$$\lim_{\substack{\Lambda\in\mathcal{L}\\ \|\Lambda\|\to\infty}} \mu_\Lambda = \mu_G.$$

Conjecture 16 (Growth conjecture). *Let $G \subseteq \mathbb{G}_{\mathrm{m}}^N$ be an algebraic subgroup, let $\mathcal{L}$ be a collection of finite subgroups of $\mathbb{G}_{\mathrm{m}}^N(\mathbb{C})$ that converges to G, and let $f \in \bar{\mathbb{Q}}^{(N)}$ be a Laurent polynomial with algebraic coefficients that is not identically zero on G. Then*

$$\lim_{\substack{\Lambda\in\mathcal{L}\\ \|\Lambda\|\to\infty}} \frac{1}{\|\Lambda\|} \log|W_f(\Lambda)| = \log \mathcal{M}_G(f).$$

Theorem 17. *With the above notation, Conjecture* 16 *is true in the following situations:*

(a) $N = 1$.
(b) *N is arbitrary and f does not vanish on $\mathbb{T}(G)$.*
(c) *$N \ge 2$ and $\mathcal{L} = \{\mu_n^N : n \ge 1\}$ and f is atoral, which we recall means that $\{\boldsymbol{z} \in \mathbb{T}^N : f(\boldsymbol{z}) = 0\}$ has real codimension at least 2 in $\mathbb{T}^N$.*

Proof. (a) For the convenience of the reader and to illustrate the use of the key estimate, which is due to Gel'fond, we briefly sketch the proof; cf. [16, Section 7]. Factoring $f(X) = bX^k \prod(X - \beta_i)$ and using the fact that $\mathcal{M}(X - \beta) = \log\max\{|\beta|, 1\}$, we find that

$$\frac{1}{n}\log|W_n(f)| - \log\mathcal{M}(f) = \sum_{j=1}^{d} \frac{1}{n} \log\frac{|\beta_j^n - 1|}{\max\{|\beta_j^n|, 1\}}.$$

The terms with $|\beta_j| \ne 1$ clearly go to 0 as $n \to \infty$, and it is not hard to see that the same is true for the terms with $|\beta_j| = 1$ provided β_j^n never gets too close to 1. The key to the proof is thus the following result, which says that nth roots of unity cannot come too close to the algebraic number β.

Theorem 18 (Gel'fond [9]). *Let $\beta \in \bar{\mathbb{Q}}^*$ that is not a root of unity. Then for every $\epsilon > 0$ there is a constant $C(\beta, \epsilon) > 0$ such that*

$$|\beta^n - 1| \ge C(\beta, \epsilon) 2^{-\epsilon n} \quad \text{for all } n \ge 1.$$

(We mention that linear forms in logarithm estimates such as those in [8, 17] can be used to prove even stronger results of the form $|\beta^n - 1| \gg n^{-C(\beta)}$.)

(b) This is elementary, and indeed is true even if f has arbitrary complex coefficients. Our non-vanishing assumption implies that the function $\log|f(\boldsymbol{z})|$ is continuous on the compact set $\mathbb{T}(G)$, so the assumed weak convergence of measures $\mu_\Lambda \to \mu_G$ implies that

$$\lim_{\|\Lambda\|\to\infty} \int_{\mathbb{T}(G)} \log|f(\boldsymbol{z})|\, d\mu_\Lambda(\boldsymbol{z}) = \int_{\mathbb{T}(G)} \log|f(\boldsymbol{z})|\, d\mu_G(\boldsymbol{z}).$$

But the definition of μ_Λ as a sum of point masses says that the left-hand integral is exactly the sum

$$\int_{\mathbb{T}(G)} \log|f(\boldsymbol{z})|\, d\mu_\Lambda(\boldsymbol{z}) = \frac{1}{\|\Lambda\|} \sum_{\boldsymbol{\zeta}\in\Lambda} \log|f(\boldsymbol{\zeta})| = \frac{1}{\|\Lambda\|} \log|W_f(\Lambda)|,$$

which gives the desired result.

(c) This is due to Lind, Schmidt, and Verbitskiy [16, Theorem 1.3]. It is likely that their proof can be adapted to more general G and $\mathcal{L}$, subject to the atoral constraint that $\{\boldsymbol{z} \in \mathbb{T}(G) : f(\boldsymbol{z}) = 0\}$ has real codimension at least 2 in $\mathbb{T}(G)$. ∎

Remark 19. We mention that if the limit in Conjecture 16 is changed to a lim sup, then K. Schmidt [23, Theorem 21.1] has shown that

$$\limsup_{n\to\infty} \frac{1}{n^N} \log|W_n(f)| = \log \mathcal{M}(f),$$

even if f is allowed arbitrary complex coefficients.

Remark 20. On the other hand, it is easy to see that Conjecture 2 is false if f is allowed to have complex coefficients, and indeed, it is false in this case even for atoral f. To construct a counterexample for $N = 1$, let $\alpha \in \mathbb{R}$ be a real number that is extremely well approximable by rational numbers. Set $a = \exp(2\pi i\alpha)$. Then

$$\begin{aligned} W_n(X-a) &\le \min_{0\le k<n} |a - e^{2\pi ik/n}| \cdot 2^{n-1} && \text{since } |a-\zeta| \le 2 \\ &\le 2^n \pi \min_{0\le k<n} \left|\alpha - \frac{k}{n}\right| && \text{by the Mean Value Theorem.} \end{aligned}$$

For an appropriate choice of α, we can find a sequence of $k_i/n_i \in \mathbb{Q}$ satisfying, say, $|\alpha - k_i/n_i| < 2^{-n_i^2}$, and then

$$\lim_{i\to\infty} n_i^{-1} \log|W_{n_i}(X-a)| = -\infty.$$

For a counterexample with $N = 2$, we can take $f(X,Y) = (X-a)+(Y-1)$, where now α has rational approximations satisfying $|\alpha - k_i/n_i| < 2^{-n_i^3}$. Further, we observe that a linear polynomial such as f is always atoral (provided $a \ne 1$), since the intersection of the two circles $\{x - a : x \in \mathbb{T}^1\}$ and $\{1 - y : y \in \mathbb{T}^1\}$ is a finite set of points. Hence even Theorem 17(c) is false if f is allowed to have arbitrary complex coefficients.

Remark 21. Lind has given $f(X,Y) = X+Y+X^{-1}+Y^{-1}-3$ as a specific example of a polynomial that is not atoral and for which Conjecture 16 is currently not known. Here $\{f = 0\} \cap \mathbb{T}^2$ is an oval containing exactly four points whose coordinates are roots of unity.

7. Rank of apparition for DD-sequences. Let $f \in R^{(N)}$ be a non-zero Laurent polynomial, let $\mathfrak{p}$ be a prime ideal of R, and let $\Lambda \subset \mathbb{G}_{\mathrm{m}}^N(\bar{K})$ be a finite subgroup. We recall from the introduction that Λ is said to be a *rank of apparition* for $\mathfrak{p}$ if

$$W_f(\Lambda) \in \mathfrak{p} \quad \text{and} \quad W_f(\Lambda') \notin \mathfrak{p} \quad \text{for all } \Lambda' \subsetneq \Lambda.$$

The intuition is that the divisibility of $W_f(\Lambda)$ by $\mathfrak{p}$ is not forced by the fact that W_f is a divisibility sequence. The set of ranks of apparition for $\mathfrak{p}$ is denoted $\mathcal{RA}_f(\mathfrak{p})$.

We start with an elementary, but useful, result.

PROPOSITION 22. *Let $f \in R^{(N)}$ be a non-zero Laurent polynomial, and let $\mathfrak{p}$ be a prime ideal of R.*

(a) *Let $\Lambda \in \mathcal{RA}_f(\mathfrak{p})$. Then $V_f(\Lambda) \in \mathfrak{p}$.*
(b) *Every $\Lambda \in \mathcal{RA}_f(\mathfrak{p})$ is cyclic.*

Proof. (a) Theorem 6(c) gives the factorization

$$W_f(\Lambda) = \prod_{\Lambda' \subseteq \Lambda} V_f(\Lambda'). \tag{9}$$

By definition, our assumption that $\Lambda \in \mathcal{RA}_f(\mathfrak{p})$ implies that $W_f(\Lambda) \in \mathfrak{p}$, so (9) tells us that $V_f(\Lambda') \in \mathfrak{p}$ for some $\Lambda' \subseteq \Lambda$. It follows that $W_f(\Lambda') \in \mathfrak{p}$, since the analogous factorization of $W_f(\Lambda')$ contains $V_f(\Lambda')$ as a factor. By definition of $\mathcal{RA}_f(\mathfrak{p})$, we must have $\Lambda' = \Lambda$, and hence $V_f(\Lambda) \in \mathfrak{p}$.

(b) Theorem 6(a) says that $V_f(\Lambda) = 1$ if Λ is not cyclic, while (a) tells us that $V_f(\Lambda) \in \mathfrak{p}$, so $V_f(\Lambda)$ cannot equal 1. Hence Λ is cyclic. ∎

Our main result is an analytic estimate which shows that the set of ranks of apparition is not too large. It is a generalization of a theorem of Romanoff [20], as quantified in [18]. Our proof is an adaptation of the proof in [18]. For ease of exposition, we take $R = \mathbb{Z}$, but everything easily generalizes to rings of integers in number fields.

THEOREM 23. *Let $f \in \mathbb{Z}^{(N)}$ be a non-zero Laurent polynomial. There is a constant C_f such that for all $\epsilon > 0$,*

$$\sum_{p \text{ prime}} \frac{\log p}{p} \sum_{\Lambda \in \mathcal{RA}_f(p)} \frac{1}{|\Lambda|^{\epsilon}} \le (N+1)\epsilon^{-1} + C_f.$$

The proof requires an estimate for the number of groups of $\mathbb{G}_{\mathrm{m}}^N(\mathbb{C})$ of given size. The following result is undoubtedly well-known, but for lack of a suitable reference, we sketch the proof.

LEMMA 24. *For $N \ge 1$ and $n \ge 1$, let*

$$\nu_N(n) = \#\{\Lambda \subset \mathbb{G}_{\mathrm{m}}^N(\mathbb{C}) : \|\Lambda\| = n\}.$$

Then for all $k \geq -(N-1)$ we have

$$\sum_{n \leq X} n^k \nu_N(n) \sim \frac{X^{N+k}}{N+k} \quad \text{as } X \to \infty.$$

Proof sketch. Finite subgroups of $\mathbb{G}_{\mathrm{m}}^N(\mathbb{C})$ of order n are dual to sublattices of $\mathbb{Z}^N$ of index n. The number of the latter is the degree of the Hecke operator $T(n)$. Formal expansions for the generating function $\sum T(p^k)X^k$ and the Dirichlet series $\sum T(n)n^{-s}$ are given in [24, Theorem 3.21]. Replacing each $T(n)$ in these formulas by its degree, which is $\nu_N(n)$, gives (after some manipulation) the beautiful formula

$$\sum_{n=1}^{\infty} \nu_N(n) n^{-s} = \prod_{j=0}^{N-1} \zeta(s-j),$$

where $\zeta(s)$ is the Riemann ζ-function. Now a standard Tauberian theorem such as in [14, Chapter VI, Section 3] gives $\sum_{n \leq X} \nu_N(n) n^{-(N-1)} \sim X$, from which it is an exercise to derive the more general estimate stated in the lemma. ∎

Proof of Theorem 23. We set the following useful notation:

$$A_f(x) = \prod_{\substack{\Lambda \subseteq \mathbb{G}_{\mathrm{m}}^N(\mathbb{C}) \\ \|\Lambda\| \leq x}} W_f(\Lambda), \quad d_f(\Lambda) = \sum_{\substack{p \text{ prime} \\ \Lambda \in \mathcal{RA}_f(p)}} \frac{\log p}{p}, \quad D_f(x) = \sum_{\substack{\Lambda \subseteq \mathbb{G}_{\mathrm{m}}^N(\mathbb{C}) \\ \|\Lambda\| \leq x}} d_f(\Lambda).$$

We note that if $\Lambda \in \mathcal{RA}_f(p)$ for a lattice with $\|\Lambda\| \leq x$, then $p \,|\, A_f(x)$, since p divides the factor $W_f(\Lambda)$ appearing in $A_f(x)$. We use this observation to estimate

$$\begin{aligned}
D_f(x) &= \sum_{\substack{\Lambda \subseteq \mathbb{G}_{\mathrm{m}}^N(\mathbb{C}) \\ \|\Lambda\| \leq x}} d_f(\Lambda) && \text{by definition of } D_f(x) \\
&= \sum_{\substack{\Lambda \subseteq \mathbb{G}_{\mathrm{m}}^N(\mathbb{C}) \\ \|\Lambda\| \leq x}} \sum_{\substack{p \text{ prime} \\ \Lambda \in \mathcal{RA}_f(p)}} \frac{\log p}{p} && \text{by definition of } d_f(\Lambda) \\
&= \sum_{\substack{p \text{ prime} \\ \exists \Lambda \in \mathcal{RA}_f(p) \\ \text{with } \|\Lambda\| \leq x}} \frac{\log p}{p} \\
&\leq \sum_{p \mid A(x)} \frac{\log p}{p} && \text{from the above observation} \\
&\leq \log\log |A(x)| + O(1).
\end{aligned}$$

The last inequality is a standard estimate; see for example [18, Section 2].

We define a constant C'_f, depending only on f, by

$$C'_f = \sup_{\substack{(z_1,\dots,z_N)\in\mathbb{C}^N\\ |z_1|=\cdots=|z_N|=1}} \log|f(z_1,\dots,z_N)|.$$

We use C'_f to estimate the size of $A_f(x)$ as follows:

$$\begin{aligned}
\log|A_f(x)| &= \sum_{\substack{\Lambda\subseteq\mathbb{G}_{\mathrm{m}}^N(\mathbb{C})\\ \|\Lambda\|\le x}} \log|W_f(\Lambda)| && \text{by definition of } A_f(x)\\
&= \sum_{\substack{\Lambda\subseteq\mathbb{G}_{\mathrm{m}}^N(\mathbb{C})\\ \|\Lambda\|\le x}} \sum_{\boldsymbol{\zeta}\in\Lambda} \log|f(\boldsymbol{\zeta})| && \text{by definition of } W_f(\Lambda)\\
&\le \sum_{\substack{\Lambda\subseteq\mathbb{G}_{\mathrm{m}}^N(\mathbb{C})\\ \|\Lambda\|\le x}} C'_f\|\Lambda\| && \text{by definition of } C'_f\\
&= C'_f \sum_{n\le x} n\nu_N(n) && \text{by definition of } \nu_N(n)\\
&= C'_f \frac{x^{N+1}}{N+1}(1+o(1)) && \text{from Lemma 24 with } k=1\\
&\le C''_f x^{N+1} && \text{for a new constant.} \qquad (10)
\end{aligned}$$

We next use a telescoping sum argument (or in fancier terms, Abel summation) to compute

$$\begin{aligned}
\sum_{p\,\text{prime}} \frac{\log p}{p} \sum_{\Lambda\in\mathcal{RA}_f(p)} \frac{1}{\|\Lambda\|^\epsilon} &= \sum_{\Lambda\subseteq\mathbb{G}_{\mathrm{m}}^N(\mathbb{C})} \frac{1}{\|\Lambda\|^\epsilon} \sum_{\substack{p\,\text{prime}\\ \Lambda\in\mathcal{RA}_f(p)}} \frac{\log p}{p}\\
&= \sum_{\Lambda\subseteq\mathbb{G}_{\mathrm{m}}^N(\mathbb{C})} \frac{1}{\|\Lambda\|^\epsilon} d_f(\Lambda) \quad \text{definition of } d_f(\Lambda)\\
&= \sum_{k=1}^{\infty} \frac{1}{k^\epsilon} \sum_{\substack{\Lambda\subseteq\mathbb{G}_{\mathrm{m}}^N(\mathbb{C})\\ \|\Lambda\|=k}} d_f(\Lambda) = \sum_{k=1}^{\infty} \frac{1}{k^\epsilon}\Big(\sum_{\substack{\Lambda\subseteq\mathbb{G}_{\mathrm{m}}^N(\mathbb{C})\\ \|\Lambda\|\le k}} d_f(\Lambda) - \sum_{\substack{\Lambda\subseteq\mathbb{G}_{\mathrm{m}}^N(\mathbb{C})\\ \|\Lambda\|\le k-1}} d_f(\Lambda)\Big)\\
&= \sum_{k=1}^{\infty} \frac{1}{k^\epsilon}(D_f(k)-D_f(k-1)) \quad \text{definition of } D_f(x)\\
&= \Big(\sum_{k=1}^{\infty} \frac{1}{k^\epsilon} D_f(k)\Big) - \Big(\sum_{k=1}^{\infty} \frac{1}{(k+1)^\epsilon} D_f(k)\Big)\\
&\le \sum_{k=1}^{\infty} \Big(\frac{1}{k^\epsilon} - \frac{1}{(k+1)^\epsilon}\Big)(\log\log|A_f(k)| + O(1))
\end{aligned}$$

$$\begin{aligned}
&\le \sum_{k=1}^{\infty}\left(\frac{1}{k^{\epsilon}}-\frac{1}{(k+1)^{\epsilon}}\right)((N+1)\log(k)+O(1)) \quad \text{from (10)}\\
&\le \sum_{k=1}^{\infty}\left(\frac{\epsilon}{k^{1+\epsilon}}+O\left(\frac{1}{k^{2+\epsilon}}\right)\right)((N+1)\log(k)+O(1))\\
&\le (N+1)\epsilon\sum_{k=1}^{\infty}\frac{\log k}{k^{1+\epsilon}}+O\left(\sum_{k=1}^{\infty}\frac{\epsilon}{k^{1+\epsilon}}\right)+O\left(\sum_{k=1}^{\infty}\frac{\log k}{k^{2+\epsilon}}\right)\\
&= (N+1)\epsilon^{-1}+O(1),
\end{aligned}$$

where the $O(1)$ depends on f, but is independent of ϵ. This completes the proof of Theorem 23. ∎

An immediate corollary of Theorem 23 is an upper bound for the Dirichlet density of the set of primes p such that $\mathcal{RA}_f(p)$ contains a "small" group. We recall that the *upper logarithmic Dirichlet density* of a set $\mathcal{P}$ of primes is the quantity

$$\overline{\delta}(\mathcal{P}) = \limsup_{s\to 1^+}\,(s-1)\sum_{p\in\mathcal{P}}\frac{\log p}{p^s}.$$

Corollary 25. *Let $f \in \mathbb{Z}^{(N)}$ be a non-zero Laurent polynomial. For $\theta > 0$, define*

$$\mathcal{P}_f(\theta) = \{p : \textit{there exists a } \Lambda \in \mathcal{RA}_f(p) \textit{ with } \|\Lambda\| \le p^{\theta}\}.$$

Then

$$\overline{\delta}(\mathcal{P}_f(\theta)) \le (N+1)\theta.$$

Proof. We set $s = 1+\epsilon$ and compute

$$\begin{aligned}
\sum_{p\in\mathcal{P}_f(\theta)}\frac{\log p}{p^s} &= \sum_{p\in\mathcal{P}_f(\theta)}\frac{\log p}{p}\cdot\frac{1}{p^{\epsilon}}\\
&\le \sum_{p\in\mathcal{P}_f(\theta)}\frac{\log p}{p}\cdot\min_{\Lambda\in\mathcal{RA}_f(p)}\frac{1}{\|\Lambda\|^{\epsilon/\theta}} && \text{by definition of } \mathcal{P}_f(\theta)\\
&\le \sum_{p\in\mathcal{P}_f(\theta)}\frac{\log p}{p}\cdot\sum_{\Lambda\in\mathcal{RA}_f(p)}\frac{1}{\|\Lambda\|^{\epsilon/\theta}} && \text{by adding more } \Lambda\text{'s}\\
&\le \sum_{p}\frac{\log p}{p}\cdot\sum_{\Lambda\in\mathcal{RA}_f(p)}\frac{1}{\|\Lambda\|^{\epsilon/\theta}} && \text{by adding more primes}\\
&\le \frac{(N+1)\theta}{\epsilon}+O(1) && \text{from Theorem 23.}
\end{aligned}$$

Multiplying by $s-1=\epsilon$ and letting $s\to 1^+$ (so $\epsilon\to 0^+$) gives the desired result. ∎

8. Zsigmondy sets of DD-sequences. We recall that the *Zsigmondy set* of the DD-sequence W_f is

$$\mathrm{Zsig}(f) := \{\text{cyclic } \Lambda : W_f(\Lambda) \text{ has no primitive prime divisors}\},$$

where $\mathfrak{p}$ is a primitive prime divisor for Λ if $\Lambda \in \mathcal{RA}_f(\mathfrak{p})$. Classical results say that the Zsigmondy set is finite for 1-dimensional sequences such as $a^n - b^n$, Fibonacci and Lucas sequences, and elliptic divisibility sequences provided that the sequence has an appropriate growth property. We conjecture a similar statement for higher-dimensional DD-sequences, but the growth condition is more subtle. Roughly speaking, we want to exclude those Λ for which the size of $W_f(\Lambda)$ is not exponential in $\|\Lambda\|$.

We recall from Section 6 that there is a Mahler measure $\mathcal{M}_G(f)$ associated to every algebraic subgroup $G \subseteq \mathbb{G}_{\mathrm{m}}^N$. Further, we say that a collection $\mathcal{L}$ of finite subgroups of $\mathbb{G}_{\mathrm{m}}^N(\mathbb{C})$ converges to G if there is a weak convergence of measures $\mu_\Lambda \to \mu_G$ as Λ is chosen in $\mathcal{L}$ with $\|\Lambda\| \to \infty$. (Here μ_G is normalized Haar measure on $G(\mathbb{C}) \cap \mathbb{T}^N$ and μ_Λ is normalized uniform discrete measure on Λ.)

Conjecture 26. *Let $f \in \bar{\mathbb{Q}}^{(N)}$ be a non-zero Laurent polynomial, let $G \subset \mathbb{G}_{\mathrm{m}}^N$ be an algebraic subgroup, and let $\mathcal{L}$ be a collection of finite cyclic subgroups of $\mathbb{G}_{\mathrm{m}}^N(\mathbb{C})$ that converges to G. Then*

$$\mathcal{M}_G(f) > 1 \;\Rightarrow\; \mathrm{Zsig}(f) \cap \mathcal{L} \text{ is finite.}$$

As in the classical cases, we expect that a proof of Conjecture 26 will require some version of the growth conjecture (Conjecture 16), a reasonable description of the sets of ranks of apparition $\mathcal{RA}_f(\mathfrak{p})$, and an estimate showing slow $\mathfrak{p}$-adic growth of $W_f(\Lambda)$ for Λ containing a fixed element of $\mathcal{RA}_f(\mathfrak{p})$.

9. DD-sequences for highly symmetric polynomials. If a Laurent polynomial has symmetries given by inversions and/or permutations of its coordinates, then its associated DD-sequence tends to be powerful, i.e., have many factors that are powers. In this section we illustrate this principle for a prototypical highly symmetric family of polynomials.

Proposition 27. *Let*

$$P_T(X,Y) = X + X^{-1} + Y + Y^{-1} + T \in \mathbb{Z}[T]^{(2)}.$$

Then the associated DD-sequence of polynomials $W_n(P_T) \in \mathbb{Z}[T]$ factors in $\mathbb{Z}[T]$ as $W_n(P_T) = A_n(T)B_n(T)^8$ with

$$\deg B_n(T) = \begin{cases} \frac{1}{8}(n-1)(n-3) & \text{if } n \text{ is odd,} \\ \frac{1}{8}(n-2)(n-4) & \text{if } n \text{ is even.} \end{cases}$$

Thus $W_n(P_T)$, which has degree n^2, is almost an 8th power ([5]).

([5]) One can say even more. If n is odd, respectively even, then $A_n(T)/W_1(P_T)$, respectively $A_n(T)/W_2(P_T)$, is a perfect 4th power in $\mathbb{Z}[T]$.

REMARK 28. The equation $P_T(X,Y)=0$, which defines a family of elliptic curves over $\mathbb{Q}(T)$, has been much studied ([6]). For $t\in\mathbb{Z}$, the Mahler measure $\mathcal{M}(P_t)$ is conjecturally related to the value of $L'(E_t,0)$, and a number of deep relations between various $\mathcal{M}(P_t)$ values have been proven, for example $\mathcal{M}(P_8)=\mathcal{M}(P_2)^4$ and $\mathcal{M}(P_5)=\mathcal{M}(P_1)^6$ (see [12, 13]). It is thus natural to ask whether $W_n(P_8)$ and $W_n(P_2)^4$, or $W_n(P_5)$ and $W_n(P_1)^6$, are similarly related. This was the original, albeit as yet unsuccessful, motivation for studying the DD-sequences associated to the family $P_T(X,Y)$. However, we can prove that $W_n(P_{2T+4})$ and $W_n(P_T)$ have a common factor in $\mathbb{Z}[T]$ of degree roughly $2n$, so in particular $W_n(P_8)$ and $W_n(P_2)$ tend to have a fairly large common factor.

PROPOSITION 29. *The DD-sequence of polynomials $W_n(P_T)\in\mathbb{Z}[T]$ associated to the Laurent polynomial $P_T(X,Y)$ satisfies*

$$\deg\gcd_{\mathbb{Z}[T]}(W_n(P_{2T+4}),W_n(P_T))\ge\begin{cases}2n-1 & \text{if } n \text{ is odd,}\\ 2n-2 & \text{if } n \text{ is even.}\end{cases}$$

Proof of Proposition 27. The maps

$$(X,Y)\mapsto(Y,X)\quad\text{and}\quad(X,Y)\mapsto(Y^{-1},X)$$

generate a group of automorphisms of the ring $R^{(2)}=R[X^{\pm1},Y^{\pm1}]$ that is isomorphic to the dihedral group D_4. Further, the polynomial $P_T(X,Y)\in\mathbb{Z}[T]^{(2)}$ is fixed by D_4. These maps also induce automorphisms of $\boldsymbol{\mu}_n^2$. For each $\boldsymbol{\zeta}\in\boldsymbol{\mu}_n^2$, we write $D_4\cdot\boldsymbol{\zeta}$ for the orbit. We are particularly interested in those $\boldsymbol{\zeta}$ whose orbit is maximal, and we write this set of $\boldsymbol{\zeta}$ as a disjoint union of orbits, say

$$\{\boldsymbol{\zeta}\in\boldsymbol{\mu}_n^2:\#(D_4\cdot\boldsymbol{\zeta})=8\}=(D_4\cdot\boldsymbol{\zeta}_1)\cup(D_4\cdot\boldsymbol{\zeta}_2)\cup\cdots\cup(D_4\cdot\boldsymbol{\zeta}_{k(n)}),\tag{11}$$

where later we will give the value of $k(n)$. We compute

$$\begin{aligned}\prod_{\substack{\boldsymbol{\zeta}\in\boldsymbol{\mu}_n^2\\ \#(D_4\cdot\boldsymbol{\zeta})=8}}P_T(\boldsymbol{\zeta})&=\prod_{\sigma\in D_4}\Big(\prod_{i=1}^{k(n)}P_T(\sigma(\boldsymbol{\zeta}_i))\Big)\quad\text{from (11)}\\ &=\Big(\prod_{i=1}^{k(n)}P_T(\boldsymbol{\zeta}_i)\Big)^8\qquad\text{since } P_T(X,Y)\text{ is } D_4\text{-invariant.}\end{aligned}$$

On the other hand, the action of D_4 on $\boldsymbol{\mu}_n^2$ commutes with the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, so the set of $\boldsymbol{\zeta}$ satisfying $\#(D_4\cdot\boldsymbol{\zeta})=8$ is Galois invariant, and hence (since $P_T(X,Y)$ is D_4-invariant), we see that the product $\prod_{i=1}^{k(n)}P_T(\boldsymbol{\zeta}_i)$ is $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-invariant. It is thus in $\mathbb{Q}[T]$, and its coefficients

([6]) The transformation $x=-1/XY$, $y=(Y-X)(1+XY)/2X^2Y^2$ maps it to the Weierstrass equation $y^2=x^3+(T^2/4-2)x^2+x$.

are clearly integral over $\mathbb{Z}$, so it is in $\mathbb{Z}[T]$. This proves that $W_n(T)$ is divisible by $B(T)^8$ for a polynomial $B(T) \in \mathbb{Z}[T]$ of degree $k(n)$. It remains to compute $k(n)$.

Checking the effect of the eight elements of D_4 on $\boldsymbol{\mu}_n^2$, we find that $\boldsymbol{\zeta} \in \boldsymbol{\mu}_n^2$ has a non-trivial stabilizer if and only if

$$\boldsymbol{\zeta} \in \bigcup_{\zeta \in \boldsymbol{\mu}_n} \{(\pm 1, \zeta), (\zeta, \pm 1), (\zeta, \zeta), (\zeta, \zeta^{-1})\}.$$

When n is odd, this set is the disjoint union of $(1,1)$ and the sets

$$\{(1,\zeta), (\zeta,1), (\zeta,\zeta), (\zeta,\zeta^{-1})\}$$

with $\zeta \in \boldsymbol{\mu}_n \setminus 1$, so there are $1 + 4(n-1) = 4n-3$ points in the set. This gives $k(n) = n^2 - 4n + 3$. When n is even, a similar computation, which we leave to the reader, leads to the formula $k(n) = n^2 - 6n + 8$. ∎

Proof of Proposition 29. The key fact is the following identity in the Laurent ring $\mathbb{Z}[Z^{\pm 1}]$:

$$P_{2T+4}(Z,Z) = 2(Z + Z^{-1}) + 2T + 4 = 2(Z + Z^{-1} + T + 2) = 2P_T(1,Z).$$

Further, by exploiting the symmetry of P_T, we obtain

$$P_{2T+4}(Z,Z) = P_{2T+4}(Z^{-1},Z) = 2P_T(1,Z) = 2P_T(Z,1).$$

Suppose first that n is odd. Then $W_n(P_{2T+4})$ has a factor of the form

$$\begin{aligned} P_{2T+4}(1,1) \prod_{1 \neq \zeta \in \boldsymbol{\mu}_n} P_{2T+4}(\zeta,\zeta) P_{2T+4}(\zeta^{-1},\zeta) & \\ &= 2P_T(1,1) \prod_{1 \neq \zeta \in \boldsymbol{\mu}_n} 2P_T(1,\zeta) 2P_T(\zeta,1) \\ &= 2^{2n-1} P_T(1,1) \prod_{1 \neq \zeta \in \boldsymbol{\mu}_n} P_T(1,\zeta) P_T(\zeta,1). \end{aligned}$$

Without the 2^{2n-1}, this last quantity is also a factor of $W_n(P_T)$. Hence $W_n(P_{2T+4})$ and $W_n(P_T)$ have a common factor in $\mathbb{Z}[T]$ of degree $2n-1$.

We obtain a similar result if n is even, but now we need to keep track of duplicated factors when $\zeta = \pm 1$. Thus $W_n(P_{2T+4})$ has a factor of the form

$$\begin{aligned} P_{2T+4}(1,1) P_{2T+4}(-1,-1) \prod_{\pm 1 \neq \zeta \in \boldsymbol{\mu}_n} P_{2T+4}(\zeta,\zeta) P_{2T+4}(\zeta^{-1},\zeta) & \\ = 2^{2n-2} P_T(1,1) P_T(1,-1) \prod_{\pm 1 \neq \zeta \in \boldsymbol{\mu}_n} P_T(1,\zeta) P_T(\zeta,1), & \end{aligned}$$

and everything except the 2^{2n-2} is a factor of $W_n(P_T)$. Thus $W_n(P_{2T+4})$ and $W_n(P_T)$ have a common factor in $\mathbb{Z}[T]$ of degree $2n-2$. ∎

10. Further questions. In this section we suggest directions for further research on higher dimensional DD-sequences. For ease of exposition, we fix a non-zero Laurent polynomial $f \in \mathbb{Z}^{(N)}$ and consider the DD-sequence $\mathcal{W}_f$ associated to f.

QUESTION 30 (Zsigmondy). Is the intersection of the Zsigmondy set of f with a set of cyclic subgroups converging to a group G for which $\mathcal{M}_G(f) > 1$ finite? See Conjecture 26 in Section 8 for details.

QUESTION 31 (Powers and powerful numbers).

(a) For a fixed $k \geq 2$, when can $\mathcal{W}_f$ contain infinitely many kth powers?
(b) When can $\mathcal{W}_f$ contain infinitely many perfect powers?
(c) When can $\mathcal{W}_f$ contain infinitely many powerful numbers?

(The referee has pointed out that (a) is related to results of Dvornicich and Zannier [6], and that since Siegel's theorem can be used for $N = 1$, it is possible that Vojta's conjecture might give some light in higher dimension.)

QUESTION 32 (Growth and Mahler measure). Is it true that

$$\lim_{n\to\infty} \frac{1}{n^N} \log |W_f(n)| = \log \mathcal{M}(f)?$$

See Conjecture 16 in Section 6 for details and a more general version.

QUESTION 33 (Order $\boldsymbol{\ell}$ ranks of apparition). Let

$$\mathcal{RA}_f(p, \ell) := \{\Lambda \in \mathcal{RA}_f(p) : \|\Lambda\| = \ell\}$$

denote the ranks of apparition for p of order ℓ. Assume that $N \geq 2$ and $M(f) \geq 2$.

(a) Is it true that for all but finitely many primes p, the set

$$\{\ell : \mathcal{RA}_f(p, \ell) \neq \emptyset\} \text{ is infinite?}$$

(b) Fix a prime p. Does there exist an $\epsilon > 0$ such that the set

$$\{\ell : \#\mathcal{RA}_f(p, \ell) \geq (1 - \epsilon)\#\nu_N(\ell)\} \text{ has density 0?}$$

(c) Fix a prime p. Might it even be true that for all $\epsilon > 0$, the set

$$\{\ell : \#\mathcal{RA}_f(p, \ell) \geq \epsilon\#\nu_N(\ell)\} \text{ has density 0?}$$

QUESTION 34 (Ranks of apparition for varying $\boldsymbol{f}$). Fix a prime ℓ and a finite set $M \subset \mathbb{Z}^N$ of indices with $\mathbf{0} \in M$. Is there a finite set of primes $\mathcal{P}_{\ell,M}$ such for all $f \in \mathbb{Z}^{(N)}$ with shape $M(f) = M$, we have

$$\{p : \#\mathcal{RA}_f(p, \ell) \geq \#M\} \subseteq \mathcal{P}_{\ell,M} \cup \{p : M(\tilde{f} \bmod p) \neq M(f)\}?$$

NB. The essential content of this question is that $\mathcal{P}_{\ell,M}$ depends only on the set M, and not on the specific polynomial f.

Remark 35. We are able to answer Question 34 affirmatively for $M = \{(1,0),(0,1),(0,0)\}$, i.e., for polynomials of the form $f(X,Y) = AX + BY + C$. We omit the rather lengthy case-by-case proof.

Question 36 (Recursion). Classical divisibility sequences satisfy recursion formulas, which may be linear (e.g., Fibonacci) or non-linear (e.g., EDS). For 1-dimensional DD-sequences, it is not hard to prove that $W_f(n)$ satisfies a linear recursion of order at most $2^{\deg f}$. If the DD-sequence $\mathcal{W}_f$ has *true dimension* ([7]) $N \ge 2$, is it possible for $\mathcal{W}_f$ to satisfy a finite order linear recurrence or an EDS-like non-linear recurrence? This could apply to either the partial sequence $W_f(n)$, or to the full sequences $W_f(\Lambda)$, where for the latter one would first need to formulate a suitable definition of finite order linear recurrence. We note that if the growth estimate in Question 32 is valid, then for $N \ge 2$ we cannot have $W_f(n) = L(n)$ for a linear recurrence L, since $\log|L(n)| \asymp n$. However, we might ask if it is possible to have (say) $W_f(n) = L(n^N)$. More generally, how closely can one approximate the sequence $W_f(n)$ using a subsequence of a linear recursion of the form $L(n^N)$?

Question 37 (Signs and characters). The divisibility property of a DD-sequence is a property of the ideals generated by the various $W_f(\Lambda)$, but the sign of $W_f(\Lambda)$ is also of interest. More generally, one can look at character values.

(a) What can one say about the distribution of the sequence of signs $\{\operatorname{sign} W_f(n)\}$? Ditto for $\{\operatorname{sign} W_f(\Lambda)\}$? (See [30] for the analogous question for EDS.)
(b) Fix a modulus q. What can one say about the distribution of the mod q reduction $\{W_f(n) \bmod q)\}$? Ditto for $\{W_f(\Lambda) \bmod q)\}$?
(c) More generally, let $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ be a Dirichlet character. What can one say about the distribution of $\{\chi(W_f(n))\}$? Ditto for $\{\chi(W_f(\Lambda))\}$?

11. DD-sequences for other groups. We briefly indicate how the notion of DD-sequence naturally generalizes to arbitrary commutative algebraic groups. More precisely, let $\mathcal{G}/R$ be a group scheme over R, let $\mathcal{O}$ denote the image of the zero section, and let D be an effective R-divisor on $\mathcal{G}$. Then a preliminary definition of the associated DD-sequence W_D is

$$W_D(n) = (n_*D) \cdot \mathcal{O},$$

([7]) Roughly, this means that no change of variables expresses f as a monomial times a Laurent polynomial in fewer variables. The referee has suggested that the true dimension is linked to the stabilizer of the divisor of f in $\mathbb{G}_{\mathrm{m}}^N$, and in particular, if this stabilizer is finite, then the true dimension is maximal.

where $n : \mathcal{G} \to \mathcal{G}$ is the nth power map, the intersection is arithmetic intersection on $\mathcal{G}$, and the resulting intersection $W_D(n)$ is naturally identified with an ideal of R via the map π_* coming from $\pi : \mathcal{G} \to \mathrm{Spec}(R)$. More generally, analogously to what we have done for $\mathcal{G} = \mathbb{G}_n^N$, we can define

$$W_D : \{R\text{-isogenies } \phi : \mathcal{G} \to \mathcal{G}'\} \to (\text{ideals of } R)$$

by setting

$$W_D(\phi) = (\phi_* D) \cdot \mathcal{O}'. \tag{12}$$

(Here $\mathcal{G}'$ may be any R-group scheme that admits a finite R-homomorphism from $\mathcal{G}$, and $\mathcal{O}'$ is the image of the identity section of $\mathcal{G}'$.)

For example, if $\mathcal{G}$ is an elliptic curve E over R and $D = (P)$, then $W_D(n)$ is the classical elliptic divisibility sequence associated to (E, P), and if E has complex multiplication, then the more general sequence $W_D(\phi)$ is a reformulation of the CM EDS studied by Streng [32].

We conjecture that generalized DD-sequences exhibit the fast growth property if their associated Mahler measures are greater than 1. We remark that if instead of the divisor D we used a point P, then the sequences $W_P(n) = (n_* P) \cdot \mathcal{O}$ are also quite interesting (an example being $\gcd(a^n - 1, b^n - 1)$), but they do not appear to satisfy the growth property. Similarly, it is not unnatural to consider sequences of the form $W_{P,D}(n) = (n_* P) \cdot D$. These sequences probably do have the growth property, but unless D is of a very special form, they will not be divisibility sequences. These two observations may help to justify our use of (12) to define higher-dimensional DD-sequences.

Acknowledgements. This research was partially supported by Simons Collaboration Grant #241309. The author would like to thank Dan Bump, Vesselin Dimitrov, Sol Friedberg, Jeff Hoffstein, Matilde Lalín, Douglas Lind, Chris Smyth, Cam Stewart, Andreas Thom, and Felipe Voloch for their helpful advice (some of which appeared in the answers to the MathOverflow questions [21, 26, 33]). The author would also like to thank Katherine Stange for her extensive comments and corrections to an initial draft of this paper, and the referee for many helpful suggestions and corrections.

References

[1] J. Agler, J. E. McCarthy and M. Stankus, *Toral algebraic sets and function theory on polydisks*, J. Geom. Anal. 16 (2006), 551–562.

[2] N. Ailon and Z. Rudnick, *Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$*, Acta Arith. 113 (2004), 31–38.

[3] Y. Bugeaud, P. Corvaja and U. Zannier, *An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$*, Math. Z. 243 (2003), 79–84.

[4] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers*, Ann. of Math. (2) 163 (2006), 969–1018.

[5] V. Dimitrov, *Convergence to the Mahler measure and the distribution of periodic points for algebraic Noetherian $\mathbb{Z}^d$-actions*, arXiv:1611.04664 (2016).

[6] R. Dvornicich and U. Zannier, *Cyclotomic Diophantine problems* (*Hilbert irreducibility and invariant sets for polynomial maps*), Duke Math. J. 139 (2007), 527–554.

[7] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, Math. Surveys Monogr. 104, Amer. Math. Soc., Providence, RI, 2003.

[8] N. I. Fel'dman, *An improvement of the estimate of a linear form in the logarithms of algebraic numbers*, Mat. Sb. (N.S.) 77 (119) (1968), 423–436 (in Russian).

[9] A. O. Gel'fond, *Transcendental and Algebraic Numbers*, Dover Publ., New York, 1960.

[10] P. Habegger, *Diophantine approximations on definable sets*, arXiv:1608.04547v1 (2016).

[11] N. Jacobson, *Basic Algebra. I*, Freeman, San Francisco, CA, 1974.

[12] M. N. Lalín, *On a conjecture by Boyd*, Int. J. Number Theory 6 (2010), 705–711.

[13] M. N. Lalín and M. D. Rogers, *Functional equations for Mahler measures of genus-one curves*, Algebra Number Theory 1 (2007), 87–117.

[14] S. Lang, *Algebraic Number Theory*, 2nd ed., Grad. Texts in Math. 110, Springer, New York, 1994.

[15] W. M. Lawton, *A problem of Boyd concerning geometric means of polynomials*, J. Number Theory 16 (1983), 356–362.

[16] 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), 1060–1081.

[17] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Ross. Akad. Nauk Ser. Mat. 64 (2000), no. 6, 125–180 (in Russian).

[18] M. R. Murty, M. Rosen and J. H. Silverman, *Variations on a theme of Romanoff*, Int. J. Math. 7 (1996), 373–391.

[19] T. A. Pierce, *The numerical factors of the arithmetic forms $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$*, Ann. of Math. (2) 18 (1916), 53–64.

[20] N. P. Romanoff, *Über einige Sätze der additiven Zahlentheorie*, Math. Ann. 109 (1934), 668–678.

[21] W. Sawin, *The resultant of an arbitrary polynomial and a cyclotomic polynomial*, MathOverflow, http://mathoverflow.net/q/98176.

[22] A. Schinzel, *Polynomials with Special Regard to Reducibility* (with an appendix by U. Zannier), Encyclopedia Math. Appl. 77, Cambridge Univ. Press, Cambridge, 2000.

[23] K. Schmidt, *Dynamical Systems of Algebraic Origin*, Progr. Math. 128, Birkhäuser, Basel, 1995.

[24] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan 11, Kanô Memorial Lectures 1, Princeton Univ. Press, Princeton, NJ, 1994.

[25] T. N. Shorey and C. L. Stewart, *Pure powers in recurrence sequences and some related Diophantine equations*, J. Number Theory 27 (1987), 324–352.

[26] J. H. Silverman, *Small values of a polynomial evaluated at roots of unity*, http://mathoverflow.net/q/178979.

[27] J. H. Silverman, *Common divisors of elliptic divisibility sequences over function fields*, Manuscripta Math. 114 (2004), 431–446.
[28] J. H. Silverman, *Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups*, Monatsh. Math. 145 (2005), 333–350.
[29] J. H. Silverman, *Divisor divisibility sequences on algebraic groups*, in preparation.
[30] J. H. Silverman and N. Stephens, *The sign of an elliptic divisibility sequence*, J. Ramanujan Math. Soc. 21 (2006), 1–17.
[31] K. Stange, *Elliptic nets and elliptic curves*, Algebra Number Theory 5 (2011), 197–229.
[32] M. Streng, *Divisibility sequences for elliptic curves with complex multiplication*, Algebra Number Theory 2 (2008), 183–208.
[33] T. Tao, *How small can a sum of a few roots of unity be?*, http://mathoverflow.net/q/46068.
[34] M. Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. 70 (1948), 31–74.

Joseph H. Silverman
Mathematics Department
Box 1917
Brown University
Providence, RI 02912, U.S.A.
E-mail: jhs@math.brown.edu