Decimation limits of principal algebraic $\mathbb{Z}^d$-actions

Arzhakova, E.; Lind, D.; Schmidt, K.; Verbitskiy, E.

DOI
10.1007/s11856-024-2676-z
Publication date
2025
Document Version
Final published version
Published in
Israel Journal of Mathematics

ISRAEL JOURNAL OF MATHEMATICS **265** (2025), 255–299
DOI: 10.1007/s11856-024-2676-z

DECIMATION LIMITS OF PRINCIPAL ALGEBRAIC $\mathbb{Z}^d$-ACTIONS

BY

Elizaveta Arzhakova

Mathematical Institute, Leiden University
Postbus 9512, 2300 RA Leiden, The Netherlands

AND

Douglas Lind

Department of Mathematics, University of Washington
Seattle, WA 98195, USA
e-mail: lind@math.washington.edu

AND

Klaus Schmidt

Mathematics Institute, University of Vienna
Oskar-Morgenstern-Platz 1, A-1090 Vienna, Austria
e-mail: klaus.schmidt@univie.ac.at

AND

Evgeny Verbitskiy

Mathematical Institute, Leiden University
Postbus 9512, 2300 RA Leiden, The Netherlands
and
Korteweg-de Vries Institute for Mathematics, University of Amsterdam
Postbus 94248, 1090 GE Amsterdam, Netherlands
e-mail: evgeny@math.leidenuniv.nl

Received August 22, 2022 and in revised form November 20, 2022

ABSTRACT

Let f be a Laurent polynomial in d commuting variables with integer coefficients. Associated to f is the principal algebraic $\mathbb{Z}^d$-action α_f on a compact subgroup X_f of $\mathbb{T}^{\mathbb{Z}^d}$ determined by f. Let $N \geqslant 1$ and restrict points in X_f to coordinates in $N\mathbb{Z}^d$. The resulting algebraic $N\mathbb{Z}^d$-action is again principal, and is associated to a polynomial g_N whose support grows with N and whose coefficients grow exponentially with N. We prove that by suitably renormalizing these decimations we can identify a limiting behavior given by a continuous concave function on the Newton polytope of f, and show that this decimation limit is the negative of the Legendre dual of the Ronkin function of f. In certain cases with two variables, the decimation limit coincides with the surface tension of random surfaces related to dimer models, but the statistical physics methods used to prove this are quite different and depend on special properties of the polynomial.

1. Introduction

Let $d \geqslant 1$ and $f \in \mathbb{Z}[x_1^{\pm 1}, \dots, x_d^{\pm 1}]$ be a Laurent polynomial with integer coefficients in d commuting variables. We write

$$f(x_1, \dots, x_d) = f(\mathbf{x}) = \sum_{\mathbf{n} \in \mathbb{Z}^d} \widehat{f}(\mathbf{n}) \mathbf{x}^{\mathbf{n}},$$

where $\mathbf{x}^{\mathbf{n}} = x_1^{n_1} \cdots x_d^{n_d}$ and $\widehat{f}(\mathbf{n}) \in \mathbb{Z}$ for all $\mathbf{n} \in \mathbb{Z}^d$ and is nonzero for only finitely many $\mathbf{n} \in \mathbb{Z}^d$.

Denote the additive torus $\mathbb{R}/\mathbb{Z}$ by $\mathbb{T}$. Use f to define a compact subgroup X_f of $\mathbb{T}^{\mathbb{Z}^d}$ by

$$X_f := \left\{ t \in \mathbb{T}^{\mathbb{Z}^d} : \sum_{\mathbf{n} \in \mathbb{Z}^d} \widehat{f}(\mathbf{n}) t_{\mathbf{m}+\mathbf{n}} = 0 \quad \text{for all } \mathbf{m} \in \mathbb{Z}^d \right\}. \tag{1.1}$$

By its definition this subgroup is invariant under the natural shift-action σ of $\mathbb{Z}^d$ on $\mathbb{T}^{\mathbb{Z}^d}$ defined by $\sigma^{\mathbf{n}}(t)_{\mathbf{m}} = t_{\mathbf{m}-\mathbf{n}}$. Hence the restriction α_f of σ to X_f gives an action of $\mathbb{Z}^d$ by automorphisms of the compact abelian group X_f. We call (X_f, α_f) the **principal algebraic $\mathbb{Z}^d$-action defined by f**.

Such $\mathbb{Z}^d$-actions serve as a rich class of examples and have been studied intensively. An observation of Halmos [19] shows that α_f automatically preserves Haar measure μ_f on X_f. It is known that the topological entropy of α_f coincides with its measure-theoretic entropy with respect to μ_f. For nonzero f this common value was computed in [24] to be the logarithmic Mahler measure of f, defined as

$$\mathsf{m}(f) := \int_0^1 \cdots \int_0^1 \log |f(e^{2\pi i s_1}, \dots, e^{2\pi i s_d})| \, ds_1 \cdots ds_d \tag{1.2}$$

(when $f = 0$ the entropy is infinite).

It will be convenient to identify the Laurent polynomial ring $\mathbb{Z}[x_1^{\pm 1}, \dots, x_d^{\pm 1}]$ with the integral group ring $\mathbb{Z}[\mathbb{Z}^d]$, where the monomial $\mathbf{x}^{\mathbf{n}}$ corresponds to $\mathbf{n} \in \mathbb{Z}^d$. Thus $f \in \mathbb{Z}[x_1^{\pm 1}, \dots, x_d^{\pm 1}]$ is identified with its coefficient function $\widehat{f}\colon \mathbb{Z}^d \to \mathbb{Z}$. When emphasizing the behavior of coefficients we will always use the notation $\widehat{f}$.

Principal algebraic $\mathbb{Z}^d$-actions are special cases of **algebraic $\mathbb{Z}^d$-actions**, which we define as actions of $\mathbb{Z}^d$ by automorphisms of a compact abelian group. Modules over the integral group ring $\mathbb{Z}[\mathbb{Z}^d]$ arise naturally as Pontryagin duals of algebraic $\mathbb{Z}^d$-actions: an algebraic $\mathbb{Z}^d$-action on X induces a $\mathbb{Z}[\mathbb{Z}^d]$-module structure on the discrete dual group $\widehat{X}$, and conversely if M is a $\mathbb{Z}[\mathbb{Z}^d]$-module there is an induced algebraic $\mathbb{Z}^d$-action on its compact dual group $\widehat{M}$ (see [36, Chap. II] for a detailed description). In §6 we give a concrete account of this correspondence for the algebraic actions we study here.

Fix a principal algebraic $\mathbb{Z}^d$-action (X_f, α_f). Let $N \geqslant 1$ and $r_N\colon \mathbb{T}^{\mathbb{Z}^d} \to \mathbb{T}^{N\mathbb{Z}^d}$ be the map restricting the coordinates of a point to only those in the sublattice $N\mathbb{Z}^d$. We call the image $r_N(X_f)$ the **Nth decimation** of X_f, although this is considerably more brutal that the term's original meaning since only every Nth coordinate in each coordinate direction survives. Clearly $r_N(X_f)$ is again a compact abelian group, and it is invariant under the natural shift action of $N\mathbb{Z}^d$ on $\mathbb{T}^{N\mathbb{Z}^d}$.

Using commutative algebra applied to contracted ideals in integral extensions, we show in §6 that $r_N(X_f)$ is a principal algebraic $N\mathbb{Z}^d$-action with some defining polynomial $g_N \in \mathbb{Z}[N\mathbb{Z}^d]$. Typically both the support of g_N grows with N and its coefficient function $\widehat{g}_N$ grows exponentially in N. Our goal in this paper is to prove that with suitable renormalizations the concave hulls of the resulting functions converge uniformly on the Newton polytope of f to a continuous decimation limit D_f. Furthermore, D_f can be computed via Legendre duality using a well-studied object called the Ronkin function of f.

The analytical parts of our analysis apply to Laurent polynomials with complex coefficients. For such an $f \in \mathbb{C}[\mathbb{Z}^d]$ we define its Nth **decimation** $f_{\langle N \rangle}$

by

$$f_{\langle N\rangle}(x_1,\dots,x_d) := \prod_{k_1=0}^{N-1}\cdots\prod_{k_d=0}^{N-1} f(e^{2\pi i k_1/N}x_1,\dots,e^{2\pi i k_d/N}x_d). \tag{1.3}$$

Since $f_{\langle N\rangle}$ is unchanged after multiplying each of its variables by an arbitrary Nth root of unity, it follows that it is a polynomial in the Nth powers of the x_i, i.e., that $f_{\langle N\rangle}\in\mathbb{C}[N\mathbb{Z}^d]$. Decimations of polynomials have appeared in many contexts, including Purbhoo's approximations to shapes of complex amoebas [33], Boyd's proof that the Mahler measure of a polynomial is continuous in its coefficients [5], and dimer models in statistical physics [22].

For most $f\in\mathbb{Z}[\mathbb{Z}^d]$ the generator g_N of the Nth decimation of X_f coincides with $f_{\langle N\rangle}$. But under special circumstances characterized in §6, involving the support of f and the Galois properties of the coefficients of the polynomials occurring in the factorization of f over the algebraic closure of the rationals, it can happen that $f_{\langle N\rangle}$ is a power $g_N^{e_N}$ of g_N. Our results give a way to explicitly compute the exponent e_N and provide a way to determine the renormalized behavior of g_N from that of $f_{\langle N\rangle}$.

To give a simple example when $d=1$, let $f(x)=x^2-2$. Then since f is already in $\mathbb{Z}[2\mathbb{Z}]$ we have that $g_2(x)=f(x)$, while

$$f_{\langle 2\rangle}(x)=f(x)f(-x)=f(x)^2=g_2(x)^2.$$

In Example 8.8 we show that the exponents for this case are $e_N=1$ if N is odd, while $e_N=2$ if N is even.

For $f\in\mathbb{C}[\mathbb{Z}^d]$ let $\operatorname{supp} f=\{\mathbf{n}\in\mathbb{Z}^d:\widehat{f}(\mathbf{n})\neq 0\}$ denote its support. The **Newton polytope** $\mathcal{N}_f$ of f is the convex hull in $\mathbb{R}^d$ of $\operatorname{supp} f$. It is well-known that if f and g are in $\mathbb{C}[\mathbb{Z}^d]$, then $\mathcal{N}_{fg}$ is the Minkowski sum $\mathcal{N}_f+\mathcal{N}_g$. Since $f_{\langle N\rangle}$ is the product of N^d polynomials all of whose Newton polytopes are $\mathcal{N}_f$, it follows that $\mathcal{N}_{f_{\langle N\rangle}}=N^d\mathcal{N}_f$.

The **Ronkin function** $R_f\colon\mathbb{R}^d\to\mathbb{R}$ of $0\neq f\in\mathbb{C}[\mathbb{Z}^d]$ is defined by

$$R_f(u_1,\dots,u_d) := \int_0^1\cdots\int_0^1 \log|f(e^{u_1}e^{2\pi i s_1},\dots,e^{u_d}e^{2\pi i s_d})|\,ds_1\cdots ds_d. \tag{1.4}$$

By [32] this is a convex function on $\mathbb{R}^d$. Letting $\langle\mathbf{r},\mathbf{u}\rangle=r_1u_1+\cdots+r_du_d$ denote the usual inner product on $\mathbb{R}^d$, then R_f has a Legendre dual R_f^* defined by

$$R_f^*(\mathbf{r}) := \sup\{\langle\mathbf{r},\mathbf{u}\rangle-R_f(\mathbf{u}):\mathbf{u}\in\mathbb{R}^d\},$$

which turns out to be a convex function on $\mathcal{N}_f$ (and is ∞ off $\mathcal{N}_f$).

To describe rescaling of polynomials $g \in \mathbb{C}[\mathbb{Z}^d]$ it is convenient to extend the domain of $\widehat{g}$ from $\mathbb{Z}^d$ to $\mathbb{R}^d$ by declaring its value to be 0 off $\operatorname{supp} g$.

Let $\phi\colon \mathbb{R}^d \to \mathbb{C}$. For any $a > 0$ define the **rescaling operator** E_a on ϕ by

$$(\mathsf{E}_a\phi)(\mathbf{r}) = \phi(a\mathbf{r})$$

for all $\mathbf{r} \in \mathbb{R}^d$. When dealing with concave functions it is often convenient to use the extended range $\underline{\mathbb{R}} = \mathbb{R} \cup \{-\infty\}$, with the usual algebraic rules for handling $-\infty$ and with the convention that $\log 0 = -\infty$. Then $\log|\phi|\colon \mathbb{R}^d \to \underline{\mathbb{R}}$, and we define its **concave hull** $\mathsf{CH}(\log|\phi|)$ to be the infimum of all affine functions on $\mathbb{R}^d$ that dominate $\log|\phi|$.

Definition 1.1: Let $f \in \mathbb{C}[\mathbb{Z}^d]$ and $f_{\langle N\rangle}$ be its Nth decimation. Define the Nth **logarithmic rescaling** $\mathsf{L}_N f$ of f by

$$\mathsf{L}_N f := \mathsf{E}_{N^d}\Big(\frac{1}{N^d}\log|\widehat{f}_{\langle N\rangle}|\Big).$$

Clearly $\mathsf{L}_N f(\mathbf{r}) = -\infty$ if $\mathbf{r} \notin \mathcal{N}_f$, and is finite at every extreme point of $\mathcal{N}_f$ and at only finitely many other points in $\mathcal{N}_f$. The Nth **renormalized decimation** $\mathsf{D}_N f$ of f is the concave hull $\mathsf{CH}(\mathsf{L}_N f)$ of $\mathsf{L}_N f$. By our previous remark, $\mathsf{D}_N f$ equals $-\infty$ off $\mathcal{N}_f$ and is finite at every point of $\mathcal{N}_f$.

With these preparations we can now state one of our main results.

Theorem 1.2: *Let $0 \neq f \in \mathbb{C}[\mathbb{Z}^d]$. Then the Nth renormalized decimations $\mathsf{D}_N f$ of f are concave polyhedral functions on the Newton polytope $\mathcal{N}_f$ of f that converge uniformly on $\mathcal{N}_f$ as $N \to \infty$ to a continuous concave limit function D_f called the* ***decimation limit*** *of f. Off $\mathcal{N}_f$ both $\mathsf{D}_N f$ and D_f are equal to $-\infty$. Furthermore $\mathsf{D}_f = -\mathsf{R}_f^*$, where R_f^* is the Legendre dual of the Ronkin function R_f of f.*

The proof of this theorem uses two main ideas: Mahler's fundamental estimate [29] relating the largest coefficient of a polynomial to its Mahler measure and support, and a method used by Boyd [5], applied to decimations along powers of 2, to prove that for polynomials whose support is contained in a fixed finite subset of $\mathbb{Z}^d$ the Mahler measure is a continuous function of their coefficients.

If $f \in \mathbb{Z}[\mathbb{Z}^d]$ the decimation limit of f contains dynamical information about α_f.

Corollary 1.3: *Let $0 \neq f \in \mathbb{C}[\mathbb{Z}^d]$. Then the maximum value of the decimation limit D_f on the Newton polytope $\mathcal{N}_f$ equals the logarithmic Mahler measure $\mathsf{m}(f)$ of f defined in (1.2). In particular, if $f \in \mathbb{Z}[\mathbb{Z}^d]$ then this maximum value equals the entropy of the principal algebraic $\mathbb{Z}^d$-action α_f.*

Duality allows us to compute the decimation limit of a product of two polynomials. Suppose that $\phi, \psi \colon \mathbb{R}^d \to \underline{\mathbb{R}}$ both have finite supremum. Define their **tropical convolution** $\phi \circledast \psi$ by

$$(\phi \circledast \psi)(\mathbf{r}) := \sup\{\phi(\mathbf{s}) + \psi(\mathbf{r} - \mathbf{s}) : \mathbf{s} \in \mathbb{R}^d\}.$$

This is the tropical analogue of standard convolution, but using tropical (or max-plus) arithmetic in $\underline{\mathbb{R}}$.

Corollary 1.4: *Let f and g be nonzero polynomials in $\mathbb{C}[\mathbb{Z}^d]$. Then*

$$\mathsf{D}_{fg} = \mathsf{D}_f \circledast \mathsf{D}_g.$$

Thus decimation limits live in the tropics.

Acknowledgment. The authors are grateful to Hanfeng Li for several suggestions and clarifications.

2. Examples

Here we give some examples to illustrate the phenomena we are investigating. They use either one or two variables, and for these we denote the variables by x and y rather than x_1 and x_2. Let $\Omega_N = \{e^{2\pi i k/N} : 0 \leqslant k < N\}$ denote the group of Nth roots of unity.

Example 2.1: Let $d = 1$ and $f(x) = x^2 - x - 1 = (x - \lambda)(x - \mu)$, where $\lambda = (1+\sqrt{5})/2$ and $\mu = (1-\sqrt{5})/2$. Then

$$\begin{aligned} f_{\langle N \rangle}(x) &= \prod_{\omega \in \Omega_N} f(\omega x) = \prod_{\omega \in \Omega_N} (\omega x - \lambda)(\omega x - \mu) \\ &= (x^N - \lambda^N)(x^N - \mu^N) = x^{2N} - (\lambda^n + \mu^N)x^N + (-1)^N. \end{aligned}$$

Hence

$$(\mathsf{L}_N f)(r) = \begin{cases} 0 & \text{if } r = 0 \text{ or } 2, \\ \frac{1}{N} \log|\lambda^N + \mu^N| & \text{if } r = 1, \\ -\infty & \text{otherwise.} \end{cases}$$

Since $L_N f(1) \to \log \lambda$ as $N \to \infty$, the concave hulls $D_N f$ converge uniformly on $\mathcal{N}_f = [0,2]$ to the decimation limit

$$D_f(r) = \begin{cases} r \log \lambda & \text{if } 0 \leqslant r \leqslant 1, \\ (2-r)\log \lambda & \text{if } 1 \leqslant r \leqslant 2, \\ -\infty & \text{otherwise,} \end{cases}$$

which is shown in Figure 1(a).

To compute the Ronkin function R_f, recall Jensen's formula that for every $\xi \in \mathbb{C}$ we have that

$$\int_0^1 \log |e^{2\pi i s} - \xi| \, ds = \max\{0, \log|\xi|\} := \log^+ |\xi|. \tag{2.1}$$

Thus

$$\begin{aligned} R_f(u) &= \int_0^1 \log |f(e^u e^{2\pi i s})| \, ds \\ &= \int_0^1 \log |e^u e^{2\pi i s} - \lambda| \, ds + \int_0^1 \log |e^u e^{2\pi i s} - \mu| \, ds \\ &= 2u + \log^+ |e^{-u}\lambda| + \log^+ |e^{-u}\mu|, \end{aligned}$$

whose polygonal graph is depicted in Figure 1(b). It is then easy to verify using the definition of Legendre transform that $D_f = -R_f^*$.

Finally, the decimation limits $D_{x-\lambda}$ and $D_{x-\mu}$ are computed similarly, and shown in Figures 1(c) and 1(d). It is easy to check using the definition of tropical convolution that $D_{x-\lambda} \circledast D_{x-\mu} = D_{(x-\lambda)(x-\mu)} = D_f$, in agreement with Corollary 1.4.

More generally, if $f(x) = \prod_{j=1}^m (x - \lambda_j)$ and $|\lambda_1| > |\lambda_2| > \cdots > |\lambda_m|$, then a computation similar to that in Example 2.1 shows that $(L_N f)(m) = 0$ and that $(L_N f)(k)$ converges to $\log|\lambda_1 \lambda_2 \ldots \lambda_{m-k}|$ for $k = 0, 1, \ldots, m-1$, and this gives uniform convergence of $D_N f$ to D_f on $\mathcal{N}_f = [0, m]$. However, if some roots of f have equal absolute value, then convergence is more delicate, or may even fail, as the next two examples show.

Example 2.2: Let $d = 1$ and

$$f(x) = x^4 - 4x^3 - 2x^2 - 4x + 1,$$

which is irreducible in $\mathbb{Z}[\mathbb{Z}]$. The roots of f are $\lambda = 1 + \sqrt{2} + \sqrt{2\sqrt{2}+2} \approx 4.611$, $\mu = 1 + \sqrt{2} - \sqrt{2\sqrt{2}+2} \approx 0.217$, and $1 - \sqrt{2} \pm i\sqrt{2\sqrt{2}-2} = e^{\pm 2\pi i\theta}$, where θ is

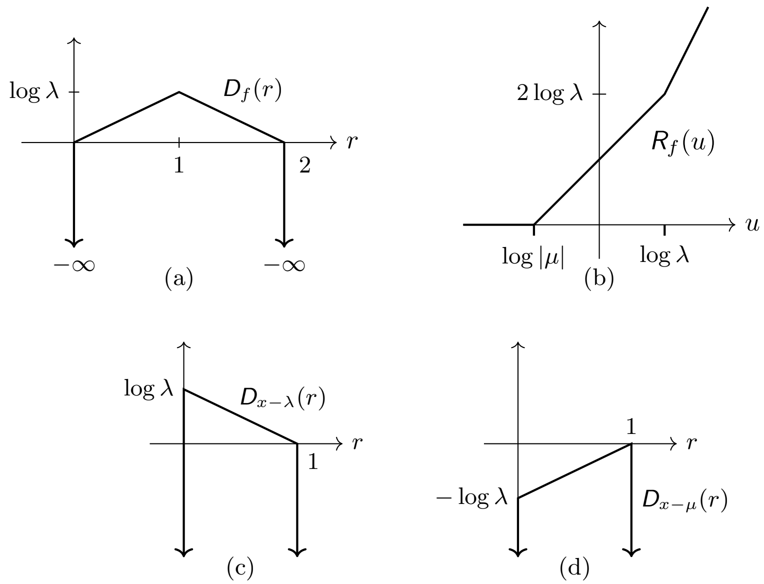


Figure 1. Graphs in Example 2.1.

irrational. Simple estimates show that $(\mathsf{L}_N f)(k)$ converges for $k = 0, 1, 3, 4$ with limits $0, \log\lambda, \log\lambda, 0$, respectively. However, the dominant term controlling the behavior of $(\mathsf{L}_N f)(2)$ is

$$\frac{1}{N}\log|2\lambda^N\cos(2\pi N\theta)|.$$

Since θ is irrational, the factor $\cos(2\pi N\theta)$ occasionally becomes very small, and so convergence is in question.

In fact, $(\mathsf{L}_N f)(2)$ does converge, but the proof requires a deep result of Gelfond [17, Thm. III, p. 28] on the diophantine properties of algebraic numbers on the unit circle (see [2, Thm. 3.1] for a more accessible treatment). According to this result, if ξ is an algebraic number (such as $e^{2\pi i\theta}$ above) such that $|\xi| = 1$ and ξ is not a root of unity, and if $\varepsilon > 0$, then $|\xi^n - 1| > e^{-n\varepsilon}$ for all but finitely many n. From this it is easy to deduce that $|e^{2\pi i N\theta} - i| > e^{-N\varepsilon}$ for almost every N, and hence that $(1/N)\log|\cos(2\pi N\theta)| \to 0$ as $N \to \infty$. This convergence is illustrated in Figure 2(a).

Both $(\mathsf{L}_N f)(1)$ and $(\mathsf{L}_N f)(3)$ converge to $\log\lambda$, and clearly

$$\limsup_{N\to\infty}(\mathsf{L}_N f)(2) \leqslant \log\lambda.$$

Hence any lack of convergence of $(\mathsf{L}_N f)(2)$ would not affect the limiting behavior of the concave hull $\mathsf{D}_N f$, nor uniform convergence of $\mathsf{D}_N f$ to D_f on $[0,4]$. Thus such diophantine issues are covered up by taking concave hulls.

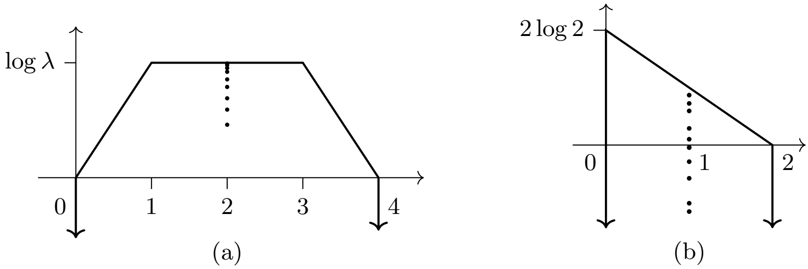


Figure 2. (a) Convergence in Example 2.2, and (b) lack of convergence in Example 2.3.

The next example shows that if we allow the coefficients of f to be arbitrary complex numbers instead of integers, then $(\mathsf{L}_N f)(k)$ can badly fail to converge at some k.

Example 2.3: Let $d=1$ and $f(x)=(x-2e^{2\pi i\theta})(x-2e^{-2\pi i\theta})$, where we will determine θ. Then $(\mathsf{L}_N f)(0)=2\log 2$ and $(\mathsf{L}_N f)(2)=0$ for all $N\geqslant 1$, while

$$(\mathsf{L}_N f)(1)=\frac{1}{N}\log|2^N\cdot 2\cos(2\pi N\theta)|.$$

It is possible to construct an irrational θ and a sequence $N_j\to\infty$ such that $\frac{1}{N_j}\log|\cos(2\pi N_j\theta)|\to-\infty$ as $j\to\infty$. Hence using this value of θ to define f we see that $(\mathsf{L}_N f)(1)$ does not converge, as depicted in Figure 2(b), although the concave hulls $\mathsf{D}_N f$ do converge uniformly to D_f.

Using arguments similar to those above, it is possible to give an elementary direct proof of Theorem 1.2 in the case $d=1$.

Example 2.4: Let $d = 2$ and $f(x,y) = 1 + x + y$. Then $f_{\langle N\rangle}$ is a polynomial in x^N and y^N of degree N^2 in each variable. For example,

$$\begin{aligned} &f_{\langle 5\rangle}(x,y) \\ &\quad= x^{25} + 5x^{20}y^5 + 5x^{20} + 10x^{15}y^{10} - 605x^{15}y^5 + 10x^{15} + 10x^{10}y^{15} \\ &\qquad + 1905x^{10}y^{10} + 1905x^{10}y^5 + 10x^{10} + 5x^5y^{20} - 605x^5y^{15} + 1905x^5y^{10} \\ &\qquad - 605x^5y^5 + 5x^5 + y^{25} + 5y^{20} + 10y^{15} + 10y^{10} + 5y^5 + 1. \end{aligned}$$

The Nth logarithmic rescaling $\mathsf{L}_N f$ of f is finite at points in the unit simplex $\Delta = \mathcal{N}_f$ whose coordinates are integer multiples of $1/N$. Thus its concave hull $\mathsf{D}_N f$ is a polyhedral surface over Δ, and as $N \to \infty$ these surfaces converge uniformly on Δ to the graph of the concave decimation limit D_f. Figure 3(a) shows the polyhedral surface $D_5 f$ corresponding to the calculation of $f_{\langle 5\rangle}$ above, and Figure 3(b) depicts the limiting smooth surface for D_f.

For this example it is possible to derive an explicit formula for D_f. Clearly $\mathsf{D}_f(r,s)$ is symmetric in r and s, so we may assume that $s \leqslant r$. Let

$$\Delta_1 = \{(r,s) \in \Delta : s \leqslant r \text{ and } s \leqslant (1-r)/2\}, \tag{2.2}$$

$$\Delta_2 = \{(r,s) \in \Delta : s \leqslant r \text{ and } s \geqslant (1-r)/2\}. \tag{2.3}$$

For $(r,s) \in \Delta_1 \cup \Delta_2$ with $r + s < 1$ define

$$b(r,s) = \csc[\pi(r+s)]\sin(\pi s).$$

Then it turns out that $0 \leqslant b(r,s) \leqslant 1$ for $(r,s) \in \Delta_1$ while $1 \leqslant b(r,s) < \infty$ for $(r,s) \in \Delta_2$.

Using Legendre duality and calculations of R_f by Lundqvist [25], in Appendix A we show that that if $(r,s) \in \Delta_1$ then

$$\mathsf{D}_f(r,s) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{\pi n^2}\, b(r,s)^n \sin[n\pi(1-r)] - s\log b(r,s), \tag{2.4}$$

while if $(r,s) \in \Delta_2$ then

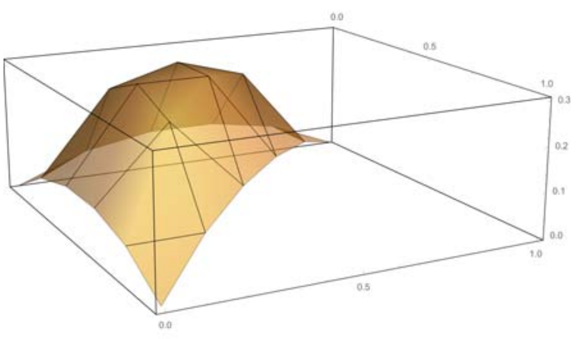
$$\mathsf{D}_f(r,s) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{\pi n^2}\, b(r,s)^{-n} \sin[n\pi(1-r)] + (1-r-s)\log b(r,s). \tag{2.5}$$

We will prove in Corollary 1.3 that the maximum value of D_f equals the entropy of α_f, which is the logarithmic Mahler measure $\mathsf{m}(f)$ of f defined in (1.2). In this example, the maximum value is attained at $(1/3, 1/3)$, which is in both Δ_1 and Δ_2. Either formula therefore applies, and each gives Smyth's calculation [37] that

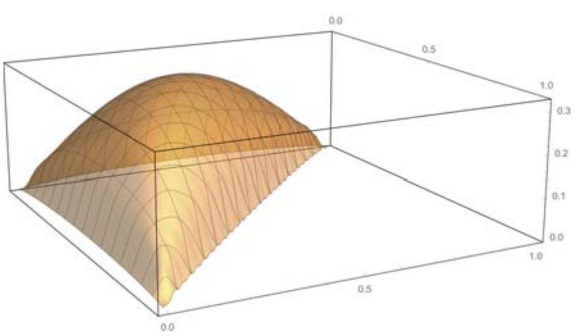
$$(2.6)\quad \mathsf{m}(1+x+y) = \mathsf{D}_f(1/3,1/3) = \frac{3\sqrt{3}}{4\pi}\sum_{n=1}^{\infty}\frac{\chi_3(n)}{n^2} = \frac{3\sqrt{3}}{4\pi}L(2,\chi_3) \approx 0.3230,$$

where χ_3 is the nontrivial character of $\mathbb{Z}/3\mathbb{Z}$ and $L(s,\chi_3)$ is the L-function associated with χ_3.

Unlike the previous example, some decimation limits exhibit non-smooth behavior.



(a)



(b)

Figure 3. (a) Polyhedral approximation $\mathsf{D}_5 f$, and (b) limiting smooth surface D_f for $f(x,y) = 1+x+y$ in Example 2.4.

Example 2.5: Let $d = 2$ and

$$f(x,y) = 5 + x + x^{-1} + y + y^{-1}.$$

The decimation limit D_f is depicted in Figure 4(a). The non-smooth peak at the origin is due to a “hole” in the amoeba of f, as defined in §4 and shown in Figure 4(b).

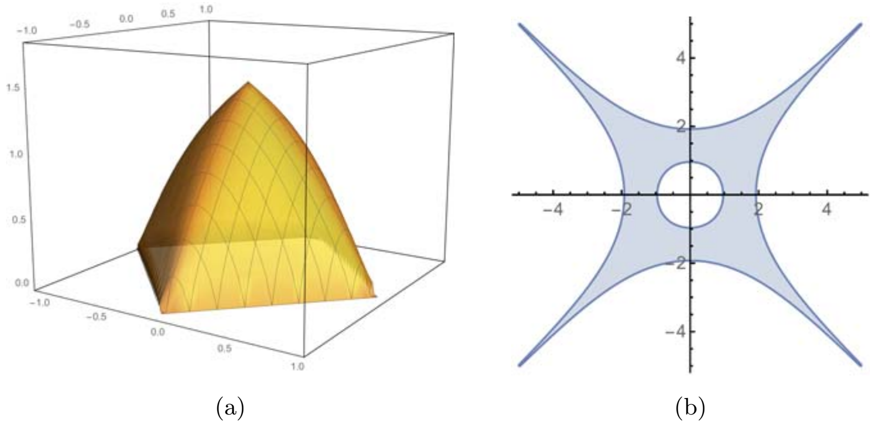


Figure 4. (a) The decimation limit for the polynomial $f(x,y) = 5 + x + x^{-1} + y + y^{-1}$ from Example 2.5, and (b) the “hole” in its amoeba causing the peak.

As in the previous example, the decimation limit describes the surface tension for a physical model, in this case dimer tilings of the square-octagon graph (see [22, Fig. 3]).

Remark 2.6: Dimer models have a long history in statistical physics. A particularly important instance involves $f(x,y) = 1 + x + y$ from Example 2.4, and has been studied in enormous detail by many authors, including Kenyon, Okounkov, and Sheffield [22].

To describe this model, let $\mathcal{H}$ denote the regular hexagonal lattice in $\mathbb{R}^2$. We can assign the vertices of $\mathcal{H}$ alternating colors red and black, much like a checkerboard. A **perfect matching** on $\mathcal{H}$ is an assignment of each red vertex to a unique adjacent black vertex, these forming an edge or **dimer**. A perfect matching is equivalent to a tiling of $\mathbb{R}^2$ by three types of lozenges, one type for each of the three edges incident to each vertex. Using a natural height function, such a lozenge tiling gives a surface, and the study of the statistical properties of such random surfaces has resulted in many remarkable discoveries (see Okounkov's survey [31] or Gorin's detailed account of lozenge tilings [18]).

Kasteleyn discovered that by cleverly assigning signs to the edges of $\mathcal{H}$, he could compute the number of perfect matchings on a finite approximation using periodic boundary conditions by a determinant formula. Furthermore, this determinant can be explicitly evaluated to have the form of a decimation of $f(x,y) = 1 + x + y$. Each of the three terms of f corresponds to one of the three types of lozenges in the random tiling. Then according to [22, §3.2] the logarithmic scaling limit $\mathsf{D}_f(r,s)$ counts the growth rate of perfect matchings for which the frequencies of the three lozenge types are r, s, and $1-r-s$. As such, it is called the **surface tension** for this model.

The two-variable polynomials with integer coefficients arising from such dimer models, such as the preceding two examples, define curves of a very special type called Harnack curves. For these there are probabilistic interpretations of the coefficients of decimations. The additional structure enables one to show that the individual nonzero coefficients of $f_{\langle N\rangle}$ grow at a rate predicted by D_f. Example 2.3 shows this can fail if complex coefficients are allowed. But whether or not this is true for every polynomial in $\mathbb{Z}[\mathbb{Z}^d]$ for all $d \geqslant 1$ appears to be quite an interesting problem (see Question 9.2 for a precise formulation).

3. Convex functions and Legendre duals

We briefly review some basic facts about convex functions and their Legendre duals. Rockafellar's classic book [34] contains a comprehensive account of this theory.

Let $\overline{\mathbb{R}}$ denote $\mathbb{R} \cup \{\infty\}$, with the standard conventions about arithmetic operations and inequalities involving ∞. Let $\phi\colon \mathbb{R}^d \to \overline{\mathbb{R}}$ be a function, and define its **epigraph** by

$$\operatorname{epi}\phi := \{(\mathbf{u},t) : \mathbf{u} \in \mathbb{R}^d, t \in \mathbb{R}, \text{ and } t \geqslant \phi(\mathbf{u})\} \subset \mathbb{R}^d \times \mathbb{R}.$$

Then ϕ is defined to be **convex** provided that $\operatorname{epi}\phi$ is a convex subset of $\mathbb{R}^d \times \mathbb{R}$. A function $\psi\colon \mathbb{R}^d \to \underline{\mathbb{R}}$ is called **concave** if $-\psi\colon \mathbb{R}^d \to \overline{\mathbb{R}}$ is convex.

The **effective domain** of a convex function ϕ is defined by

$$\operatorname{dom}\phi := \{\mathbf{u} \in \mathbb{R}^d : \phi(\mathbf{u}) < \infty\}.$$

By allowing ϕ to take the value ∞, we may assume that it is defined on all of $\mathbb{R}^d$, enabling us to combine convex functions without needing to take into account their effective domains. A convex function is **closed** if its epigraph is a closed subset of $\mathbb{R}^d \times \mathbb{R}$. This property normalizes the behavior of a convex function at the boundary of its effective domain, and holds for all convex (and concave) functions that arise here.

Suppose that $\phi\colon \mathbb{R} \to \overline{\mathbb{R}}$ is convex. Its **Legendre dual** (or, more accurately, its **Legendre–Fenchel dual**) ϕ^* is defined for all $\mathbf{r} \in \mathbb{R}^d$ by

$$\phi^*(\mathbf{r}) := \sup\{\langle \mathbf{r}, \mathbf{u}\rangle - \phi(\mathbf{u}) : \mathbf{u} \in \mathbb{R}^d\}. \tag{3.1}$$

The Legendre dual ϕ^* is also a convex function, and provides an alternative description of $\operatorname{epi}\phi$ in terms of its support hyperplanes. Furthermore, Legendre duality states that $\phi^{**} = \phi$ for closed convex functions.

The Legendre dual of a concave function $\psi\colon \mathbb{R}^d \to \underline{\mathbb{R}}$ is similarly defined as

$$\psi^*(\mathbf{r}) = \inf\{\langle \mathbf{r}, \mathbf{u}\rangle - \psi(\mathbf{u}) : \mathbf{u} \in \mathbb{R}^d\}. \tag{3.2}$$

Then $\phi = -\psi$ is convex, and a simple manipulation shows that their Legendre duals are related by $\psi^*(\mathbf{r}) = -\phi^*(-\mathbf{r})$.

4. Amoebas and Ronkin functions

Let $0 \neq f \in \mathbb{C}[\mathbb{Z}^d]$. Put $\mathbb{C}^* = \mathbb{C} \smallsetminus \{0\}$ and define

$$\mathsf{V}(f) := \{\mathbf{z} \in (\mathbb{C}^*)^d : f(\mathbf{z}) = 0\}.$$

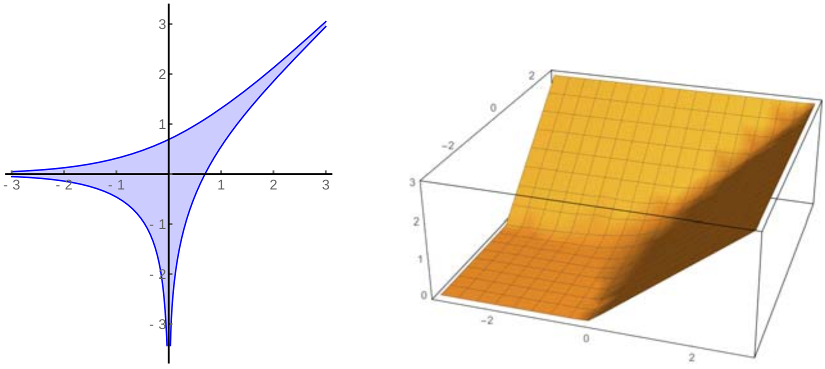
Let $\operatorname{Log}\colon (\mathbb{C}^*)^d \to \mathbb{R}^d$ be the map $\operatorname{Log}(z_1, \dots, z_d) = (\log|z_1|, \dots, \log|z_d|)$.

In 1993 Gel′fand, Kapranov, and Zelevinsky [16] introduced the notion of the **amoeba** $\mathcal{A}_f$ of f, defined as

$$\mathcal{A}_f := \operatorname{Log}(\mathsf{V}(f)) \subset \mathbb{R}^d.$$

The amoeba of $1+x+y$ is depicted in Figure 5(a). The complement $\mathcal{A}_f^c = \mathbb{R}^d \smallsetminus \mathcal{A}_f$ of $\mathcal{A}_f$ consists of a finite number of connected components, all convex. The unbounded components are created by "tentacles" of $\mathcal{A}_f$. Unfortunately, biological amoebas look nothing like their mathematical namesakes.

Closely related to $\mathcal{A}_f$ is the Ronkin function R_f of f, introduced by Ronkin [35] in 2001, and defined earlier in (1.4). The Ronkin function of $1 + x + y$ is shown in Figure 5(b).



(a) (b)

Figure 5. (a) The amoeba of $1 + x + y$, and (b) its Ronkin function .

The Ronkin function of a polynomial f is known to be a convex function on $\mathbb{R}^d$ and affine on each connected component of $\mathcal{A}_f^c$ (see [32] for all properties of R_f and $\mathcal{A}_f$ used here). Moreover, on each connected component of $\mathcal{A}_f^c$ the (constant) gradient of R_f is contained in $\mathcal{N}_f \cap \mathbb{Z}^d$, and the convex hull of these values equals $\mathcal{N}_f$. From this we conclude that the Legendre dual R_f^* of R_f has effective domain $\mathcal{N}_f$.

5. Decimation limits of polynomials

In this section we prove Theorem 1.2, one of our main results, and Corollaries 1.3 and 1.4. If $0 \neq f \in \mathbb{C}[\mathbb{Z}^d]$ we will show that the Nth renormalized decimation $D_N f = CH(L_N f)$ converges uniformly on $\mathcal{N}_f$ to a continuous concave limit function D_f, and that $D_f = -R_f^*$.

The first ingredient in our proof is the basic estimate of Mahler relating the largest coefficient of a polynomial to its Mahler measure and its support. Let us begin with some terminology. For $0 \neq g \in \mathbb{C}[\mathbb{Z}^d]$ define its **height** $H(g)$ by $H(g) = \max\{ |\widehat{g}(\mathbf{k})| : \mathbf{k} \in \mathbb{Z}^d\}$. The **Mahler measure** of g is $M(g) = \exp(m(g))$, where $m(g)$ is the logarithmic Mahler measure defined in (1.2).

Proposition 5.1 (Mahler [29]): *Suppose that* $0 \neq g \in \mathbb{C}[\mathbb{Z}^d]$ *and that*

$$\operatorname{supp} g \subset [0, C-1]^d \cap \mathbb{Z}^d.$$

Then

$$2^{-dC}\mathsf{H}(g) \leqslant \mathsf{M}(g) \leqslant C^d \mathsf{H}(g). \tag{5.1}$$

Proof. Let $\mathbf{k} = (k_1, \ldots, k_d) \in \operatorname{supp} g$. Then by [29, Eqn. (3)],

$$|\widehat{g}(\mathbf{k})| \leqslant \binom{C-1}{k_1}\binom{C-1}{k_2}\cdots\binom{C-1}{k_d}\mathsf{M}(g).$$

Since each binomial coefficient is bounded above by 2^C, the first inequality in (5.1) follows.

To prove the second inequality, observe that for all real numbers $s_1, \ldots, s_d$ we have that

$$|g(e^{2\pi i s_1}, \ldots, e^{2\pi i s_d})| \leqslant \sum_{\mathbf{k}\in\mathbb{Z}^d} |\widehat{g}(\mathbf{k})| \leqslant |[0, C-1]^d \cap \mathbb{Z}^d| \cdot \mathsf{H}(g) = C^d \mathsf{H}(g). \tag{5.2}$$

Hence

$$\begin{aligned}\mathsf{M}(g) &= \exp\left[\int_0^1 \cdots \int_0^1 \log|g(e^{2\pi i s_1}, \ldots, e^{2\pi i s_d})|\, ds_1 \cdots ds_d\right] \\ &\leqslant C^d \mathsf{H}(g). \qquad \blacksquare\end{aligned}$$

Consider $(\mathbb{C}^*)^d$ as a group under coordinate-wise multiplication. Define the action of $\mathbf{z} \in (\mathbb{C}^*)^d$ on $f \in \mathbb{C}[\mathbb{Z}^d]$ by $(\mathbf{z}\cdot f)(x_1, \ldots, x_d) = f(z_1x_1, \ldots, z_dx_d)$. This action is commutative since

$$\mathbf{z}\cdot(\mathbf{z}'\cdot f) = (\mathbf{z}\mathbf{z}')\cdot f = \mathbf{z}'\cdot(\mathbf{z}\cdot f),$$

and also $\mathbf{z}\cdot(fg) = (\mathbf{z}\cdot f)(\mathbf{z}\cdot g)$ for all $f, g \in \mathbb{C}[\mathbb{Z}^d]$. Hence the map $f \mapsto \mathbf{z}\cdot f$ is a ring isomorphism of $\mathbb{C}[\mathbb{Z}^d]$. Furthermore, $(\mathbf{z}\cdot f)\widehat{\ }(\mathbf{k}) = \mathbf{z}^{\mathbf{k}}\widehat{f}(\mathbf{k})$ for all $\mathbf{k} \in \mathbb{Z}^d$, and so $\mathcal{N}_{\mathbf{z}\cdot f} = \mathcal{N}_f$ for all $\mathbf{z} \in (\mathbb{C}^*)^d$.

Recall that Ω_N denotes the group of Nth roots of unity. For $\boldsymbol{\omega} \in \Omega_N^d \subset (\mathbb{C}^*)^d$ we call $\boldsymbol{\omega}\cdot f$ the **rotate of f by $\boldsymbol{\omega}$**. Then $f_{\langle N\rangle} = \prod_{\boldsymbol{\omega}\in\Omega_N^d} \boldsymbol{\omega}\cdot f$ is the product of all rotates of f by elements in Ω_N^d.

If $g, h \in \mathbb{C}[\mathbb{Z}^d]$ then it is well known that $\mathcal{N}_{gh} = \mathcal{N}_g + \mathcal{N}_h$ (the Minkowski sum), and trivially $\mathsf{R}_{gh} = \mathsf{R}_g + \mathsf{R}_h$. By our previous remarks,

$$\mathcal{N}_{f_{\langle N\rangle}} = \sum_{\boldsymbol{\omega}\in\Omega_N^d} \mathcal{N}_{\boldsymbol{\omega}\cdot f} = \sum_{\boldsymbol{\omega}\in\Omega_N^d} \mathcal{N}_f = N^d \mathcal{N}_f.$$

Also, $\mathsf{R}_{\boldsymbol{\omega}\cdot f} = \mathsf{R}_f$, and hence $\mathsf{R}_{f_{\langle N\rangle}} = N^d \mathsf{R}_f$.

For $\mathbf{u} \in \mathbb{R}^d$ put $e^{\mathbf{u}} = (e^{u_1}, \dots, e^{u_d})$. Then $(e^{\mathbf{u}} \cdot f)\widehat{\ }(\mathbf{k}) = e^{\mathbf{u}\cdot\mathbf{k}} \widehat{f}(\mathbf{k})$. Commutativity of the action of $(\mathbb{C}^*)^d$ on f then shows that $(e^{\mathbf{u}} \cdot f)_{\langle N\rangle} = e^{\mathbf{u}} \cdot (f_{\langle N\rangle})$. Also

$$R_f(\mathbf{u}) = \log M(e^{\mathbf{u}} \cdot f) = \frac{1}{N^d} \log M((e^{\mathbf{u}} \cdot f)_{\langle N\rangle}) = \frac{1}{N^d} \log M(e^{\mathbf{u}} \cdot f_{\langle N\rangle}).$$

Observe that

$$\log H(e^{\mathbf{u}} \cdot f_{\langle N\rangle}) = \max\{\langle \mathbf{u}, \mathbf{k}\rangle + \log|\widehat{f}_{\langle N\rangle}(\mathbf{k})| : \mathbf{k} \in \mathbb{Z}^d\},$$

indicating a connection with Legendre duals.

Proof of Theorem 1.2. Let $0 \neq f \in \mathbb{C}[\mathbb{Z}^d]$. Fix $\mathbf{m} \in \mathbb{Z}^d$ and let $g(\mathbf{x}) = \mathbf{x}^{\mathbf{m}} f(\mathbf{x})$. It is straightforward to verify that

$$(D_N g)(\mathbf{r}) = (D_N f)(\mathbf{r} - \mathbf{m})$$

for all $\mathbf{r} \in \mathbb{R}^d$. Therefore by adjusting f by suitable monomial, we may assume that $\operatorname{supp} f \subset [0, B-1]^d \cap \mathbb{Z}^d$ for some $B \geqslant 1$. Then

$$\operatorname{supp}(e^{\mathbf{u}} \cdot f_{\langle N\rangle}) \subset [0, N^d(B-1)]^d \cap \mathbb{Z}^d \subset [0, N^d B - 1]^d \cap \mathbb{Z}^d$$

for every $\mathbf{u} \in \mathbb{R}^d$. By Proposition 5.1,

$$\begin{aligned} R_f(\mathbf{u}) &= \frac{1}{N^d} \log M(e^{\mathbf{u}} \cdot f_{\langle N\rangle}) \leqslant \frac{1}{N^d}\{\log[(N^d B)^d] + \log H(e^{\mathbf{u}} \cdot f_{\langle N\rangle})\} \\ &= \frac{\log[(N^d B)^d]}{N^d} + \frac{1}{N^d} \max_{\mathbf{k}\in\mathbb{Z}^d}\{\langle \mathbf{u}, \mathbf{k}\rangle + \log|\widehat{f}_{\langle N\rangle}(\mathbf{k})|\}, \end{aligned}$$

where the error term $b_N := N^{-d} \log[(N^d B)^d] \to 0$ as $N \to \infty$, uniformly for $\mathbf{u} \in \mathbb{R}^d$.

An opposite inequality is based on the following fundamental observation, used both by Boyd [5] and Purbhoo [33] for different purposes. As we noticed before, $f_{\langle N\rangle}$ is a polynomial in the Nth powers of the variables. Therefore $E_N \widehat{f}_{\langle N\rangle}$ is again a polynomial to which we can apply Prop. 5.1, but with improved constants since the support has now shrunk by a factor of N. This improvement is crucial.

Specifically,

$$\operatorname{supp}(e^{\mathbf{u}} \cdot f_{\langle N\rangle}) \subset [0, N^d(B-1)]^d \cap (N\mathbb{Z}^d),$$

so that

$$\operatorname{supp}(E_N(e^{\mathbf{u}} \cdot f_{\langle N\rangle})) \subset [0, N^{d-1}(B-1)] \cap \mathbb{Z}^d.$$

Applying Prop. 5.1,

$$(5.3) \qquad \begin{aligned} \mathsf{H}(e^{\mathbf{u}} \cdot f_{\langle N \rangle}) &= \mathsf{H}(\mathsf{E}_N(e^{\mathbf{u}} \cdot f_{\langle N \rangle})) \leqslant 2^{dN^{d-1}B} \mathsf{M}(\mathsf{E}_N(e^{\mathbf{u}} \cdot f_{\langle N \rangle})) \\ &= 2^{dN^{d-1}B} \mathsf{M}(e^{\mathbf{u}} \cdot f)^{N^d}. \end{aligned}$$

Hence

$$\frac{1}{N^d} \log \mathsf{H}(e^{\mathbf{u}} \cdot f_{\langle N \rangle}) \leqslant \frac{dN^{d-1}B \log 2}{N^d} + \log \mathsf{M}(e^{\mathbf{u}} \cdot f) = a_N + \mathsf{R}_f(\mathbf{u}),$$

where again the error term $a_N := (dB \log 2)/N \to 0$ uniformly for $\mathbf{u} \in \mathbb{R}^d$. We can summarize these estimates as

$$(5.4) \qquad \Big| \mathsf{R}_f(\mathbf{u}) - \frac{1}{N^d} \max_{\mathbf{k} \in \mathbb{Z}^d} \{ \langle \mathbf{u}, \mathbf{k} \rangle + \log |\widehat{f}_{\langle N \rangle}(\mathbf{k})| \} \Big| \leqslant \max\{a_N, b_N\} \to 0$$

as $N \to \infty$ uniformly in $\mathbf{u} \in \mathbb{R}^d$.

Next we relate the first max occurring in (5.4) with the Nth normalized decimation $\mathsf{D}_N f$. We have that

$$\begin{aligned} &\frac{1}{N^d} \max_{\mathbf{k} \in \mathbb{Z}^d} \{ \langle \mathbf{u}, \mathbf{k} \rangle + \log |\widehat{f}_{\langle N \rangle}(\mathbf{k})| \} \\ &\qquad = \max_{\mathbf{k} \in \mathbb{Z}^d} \Big\{ \Big\langle \mathbf{u}, \Big(\frac{\mathbf{k}}{N^d} \Big) \Big\rangle + \frac{1}{N^d} \log |\widehat{f}_{\langle N \rangle}(\mathbf{k})| \Big\} \\ &\qquad = \max_{\mathbf{k} \in \mathbb{Z}^d} \Big\{ \Big\langle \mathbf{u}, \Big(\frac{\mathbf{k}}{N^d} \Big) \Big\rangle + \frac{1}{N^d} \mathsf{E}_{N^d} \log \Big| \widehat{f}_{\langle N \rangle} \Big(\frac{1}{N^d} \mathbf{k} \Big) \Big| \Big\} \\ &\qquad = \max_{\mathbf{k} \in \mathbb{Z}^d} \Big\{ \Big\langle \mathbf{u}, \Big(\frac{\mathbf{k}}{N^d} \Big) \Big\rangle + (\mathsf{D}_N f) \Big(\frac{\mathbf{k}}{N^d} \Big) \Big\} \\ &\qquad = \max_{\mathbf{r} \in \mathbb{R}^d} \{ \langle \mathbf{u}, \mathbf{r} \rangle + \mathsf{D}_N f(\mathbf{r}) \} = -(\mathsf{D}_N f)^*(-\mathbf{u}). \end{aligned}$$

Hence by (5.4), $-(\mathsf{D}_N f)^*(-\mathbf{u})$ converges to $\mathsf{R}_f(\mathbf{u})$ uniformly for $\mathbf{u} \in \mathbb{R}^d$, or, equivalently,

$$(5.5) \qquad (\mathsf{D}_N f)^*(\mathbf{u}) \to -\mathsf{R}_f(-\mathbf{u}) \quad \text{uniformly for } \mathbf{u} \in \mathbb{R}^d.$$

If ϕ and ψ are concave functions on $\mathbb{R}^d$ such that $|\phi(\mathbf{u}) - \psi(\mathbf{u})| \leqslant \varepsilon$ for all $\mathbf{u} \in \mathbb{R}^d$, it is easy to check from the definitions that ϕ^* and ψ^* have the same effective domain, and that $|\phi^*(\mathbf{r}) - \psi^*(\mathbf{r})| \leqslant \varepsilon$ for all $\mathbf{r} \in \operatorname{dom} \phi^* = \operatorname{dom} \psi^*$. Applying this to (5.5) and using duality we finally obtain that

$$(\mathsf{D}_N f)^{**} = \mathsf{D}_N f \to -\mathsf{R}_f^*$$

uniformly on $\mathcal{N}_f$, completing the proof. ∎

Proof of Corollary 1.3. By Theorem 1.2, Legendre duality, and (3.2),

$$-\mathsf{m}(f) = -\mathsf{R}_f(0,0) = \mathsf{D}_f^*(0,0) = \inf_{(r,s)\in\mathcal{N}_f} -\mathsf{D}_f(r,s) = -\sup_{(r,s)\in\mathcal{N}_f} \mathsf{D}_f(r,s).$$

We remark that differentiability of D_f at the maximum value is not assumed for Legendre duality to apply here, and Example 2.5 provides a case when differentiability fails. ∎

Proof of Corollary 1.4. Let f and g be nonzero polynomials in $\mathbb{C}[\mathbb{Z}^d]$. Clearly

$$\mathsf{R}_{fg} = \mathsf{R}_f + \mathsf{R}_g.$$

By [34, Thm. 16.4], the Legendre dual of the sum $\phi+\psi$ of two convex functions is their infimal convolution defined for $\mathbf{r}\in\mathbb{R}^d$ by

$$\inf\{\phi(\mathbf{s}) + \psi(\mathbf{r}-\mathbf{s}) : \mathbf{s}\in\mathbb{R}^d\}.$$

Applying this with $\phi = -\mathsf{R}_f$ and $\psi = -\mathsf{R}_g$, using Thm. 1.2, and taking negatives we obtain that $\mathsf{D}_{fg} = \mathsf{D}_f \circledast \mathsf{D}_g$. ∎

Remark 5.2: Our estimate (5.4) can be expressed in the language of tropicalization of polynomials (see [26, §3.1] for background and motivation). Let

$$0 \neq g(\mathbf{x}) = \sum_{\mathbf{k}\in\mathbb{Z}^d} \widehat{g}(\mathbf{k})\mathbf{x}^{\mathbf{k}} \in \mathbb{C}[\mathbb{Z}^d].$$

Define the **tropicalization** of g to be the function $\operatorname{trop} g\colon \mathbb{R}^d\to\mathbb{R}$ given by

$$(\operatorname{trop} g)(\mathbf{u}) = \max_{\mathbf{k}\in\mathbb{Z}^d}\{\langle\mathbf{u},\mathbf{k}\rangle + \log|\widehat{g}(\mathbf{k})|\},$$

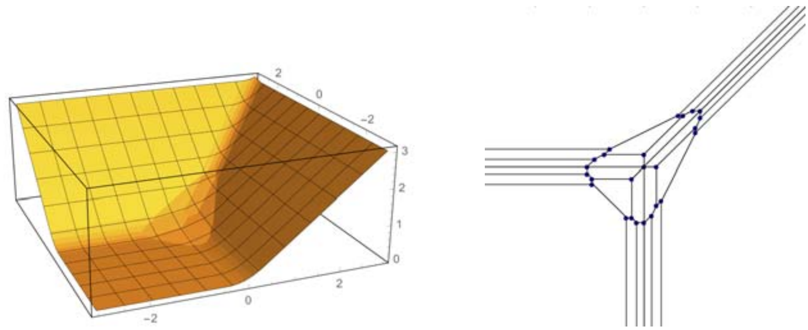
which is a polyhedral convex function. Then by (5.4) we see that

$$\frac{1}{N^d}\operatorname{trop} f_{\langle N\rangle} \to \mathsf{R}_f \quad \text{uniformly on } \mathbb{R}^d, \tag{5.6}$$

so that the normalized tropicalization of $f_{\langle N\rangle}$ converges uniformly to the Ronkin function of f. Figure 6(a) depicts this polyhedral approximation for

$$f(x,y) = 1 + x + y$$

and $N = 5$ (compare with Figure 5(b)). The tropical variety of this polyhedral approximation is the projection to the plane of the vertices and edges of its graph, and is shown in Figure 6(b). These tropical varieties converge in the Hausdorff metric to the amoeba of f as $N\to\infty$ (compare with Figure 5(a)).



(a) (b)

Figure 6. (a) Tropical approximation to the Ronkin function of $1 + x + y$, and (b) its corresponding tropical variety .

Remark 5.3: In [33] Purbhoo used decimations for a different purpose, namely to find a computational way to detect whether or not a point is in the amoeba of a given polynomial. Call a polynomial **lopsided** if it has one coefficient whose absolute value strictly exceeds the sum of the absolute values of all the other coefficients. Let $f \in \mathbb{Z}[\mathbb{Z}^d]$ and $\mathbf{u} \in \mathbb{R}^d$. Clearly if $e^{\mathbf{u}} \cdot f$ is lopsided then $\mathbf{u} \notin \mathcal{A}_f$. Purbhoo used decimations to amplify size differences among the coefficients. More precisely, he proves that given $\varepsilon > 0$ there is an N_0, depending only on ε and the support of f, such that if $N > N_0$ and the distance from $\mathbf{u}$ to $\mathcal{A}_f$ is greater than ε then $e^{\mathbf{u}} \cdot f_{\langle N \rangle}$ is lopsided. Since f and $f_{\langle N \rangle}$ have the same amoeba, this gives an effective algorithm for approximating the complement of $\mathcal{A}_f$.

One direct consequence of [33] is that the normalized tropicalizations in (5.6) converge to the Ronkin function off the amoeba of f, while our result is that this convergence is uniform on all of $\mathbb{R}^d$. Roughly speaking, Purbhoo is concerned with the coefficients of $e^{\mathbf{u}} \cdot f$ for points $\mathbf{u}$ off the amoeba, while our focus is on $\mathbf{u}$ within the amoeba.

Remark 5.4: Let F be a lower-dimensional face of the Newton polytope $\mathcal{N}_f$ of f, and put $f|_F = \sum_{\mathbf{n} \in F} \widehat{f}(\mathbf{n}) \mathbf{x}^{\mathbf{n}}$. Clearly the restriction of D_f to F is just the decimation limit of $f|_F$, or in symbols $\mathsf{D}_f|_F = \mathsf{D}_{f|_F}$. By Corollary 1.3, this generalizes [24, Rem. 5.5], which gave a dynamical proof of the inequality due to Smyth [38, Thm. 2] that $\mathsf{m}(f) \geqslant \mathsf{m}(f_F)$ for every face F of $\mathcal{N}_f$.

6. Decimations of principal actions and contracted ideals

We return to decimations of principal algebraic $\mathbb{Z}^d$-actions, and in this section show that they are again principal. The proof uses machinery from commutative algebra, including contractions of ideals.

Suppose that X is a compact, shift-invariant subgroup of $\mathbb{T}^{\mathbb{Z}^d}$. Using Pontryagin duality we can obtain an alternative description of X as follows (for a comprehensive account see [36, Chap. II]).

As a discrete abelian group the Pontryagin dual of $\mathbb{T}^{\mathbb{Z}^d}$ is the direct sum of $\mathbb{Z}^d$ copies of $\mathbb{Z}$, which we suggestively write as $\bigoplus_{\mathbf{k}\in\mathbb{Z}^d}\mathbb{Z}\mathbf{x}^{\mathbf{k}}=\mathbb{Z}[\mathbb{Z}^d]$. The (additive) dual pairing between $\mathbb{T}^{\mathbb{Z}^d}$ and $\mathbb{Z}[\mathbb{Z}^d]$ is given by

$$\langle t,g\rangle=\sum_{\mathbf{k}\in\mathbb{Z}^d} t_{\mathbf{k}}\,\widehat{g}(\mathbf{k})\in\mathbb{T}.$$

Multiplication by the inverses of each of the variables x_j on $\mathbb{Z}[\mathbb{Z}^d]$ gives a $\mathbb{Z}^d$-action that is dual to the natural shift action σ on $\mathbb{T}^{\mathbb{Z}^d}$ defined earlier.

Since X is shift-invariant, $\{g\in\mathbb{Z}[\mathbb{Z}^d]:\langle t,g\rangle=0 \text{ for all } t\in X\}$ is an ideal $\mathfrak{a}$ in $\mathbb{Z}[\mathbb{Z}^d]$, and the dual group of X equals $\mathbb{Z}[\mathbb{Z}^d]/\mathfrak{a}$. Conversely, if $\mathfrak{a}$ is an arbitrary ideal in $\mathbb{Z}[\mathbb{Z}^d]$, then the compact dual group $X_{\mathfrak{a}}$ of $\mathbb{Z}[\mathbb{Z}^d]/\mathfrak{a}$ is a shift-invariant subgroup of $\mathbb{T}^{\mathbb{Z}^d}$. Thus there is a one-to-one correspondence between shift-invariant compact subgroups of $\mathbb{T}^{\mathbb{Z}^d}$ and ideals in $\mathbb{Z}[\mathbb{Z}^d]$. When $\mathfrak{a}$ is the principal ideal $\langle f\rangle$ generated by f, then $X_{\mathfrak{a}}=X_f$ as defined above, explaining the terminology “principal actions”.

Fix $N\geqslant 1$ and recall the restriction map $r_N\colon\mathbb{T}^{\mathbb{Z}^d}\to\mathbb{T}^{N\mathbb{Z}^d}$ from §1. Let $f\in\mathbb{Z}[\mathbb{Z}^d]$. Then the Nth decimation $r_N(X_f)$ is a compact subgroup of $\mathbb{T}^{N\mathbb{Z}^d}$ that is invariant under the shift-action of $N\mathbb{Z}^d$. By our previous discussion, the dual group of $r_N(X_f)$ has the form $\mathbb{Z}[N\mathbb{Z}^d]/\mathfrak{a}_N$, where $\mathfrak{a}_N$ is an ideal in $\mathbb{Z}[N\mathbb{Z}^d]$. The following result identifies this ideal.

Lemma 6.1: *Let $f\in\mathbb{Z}[\mathbb{Z}^d]$ and $N\geqslant 1$. Then the dual group of $r_N(X_f)$ is $\mathbb{Z}[N\mathbb{Z}^d]/\mathfrak{a}_N$, where $\mathfrak{a}_N=\langle f\rangle\cap\mathbb{Z}[N\mathbb{Z}^d]$.*

Proof. Let

$$\mathfrak{b}_N=\{g\in\mathbb{Z}[N\mathbb{Z}^d]:\langle t,g\rangle=0 \text{ for all } t\in r_N(X_f)\}.$$

If $g\in\mathfrak{a}_N$, then for every $t\in X_f$ we have that $0=\langle t,g\rangle=\langle r_N(t),g\rangle$, so that $g\in\mathfrak{b}_N$. Conversely, if $g\in\mathfrak{b}_N$ and $t\in X_f$, then g annihilates the restriction of t to every coset of $N\mathbb{Z}^d$, and hence annihilates t, so that $g\in\mathfrak{a}_N$. ∎

The ideal $\langle f\rangle \cap \mathbb{Z}[N\mathbb{Z}^d]$ defining $r_N(X_f)$ is called the **contraction** of $\langle f\rangle$ to $\mathbb{Z}[N\mathbb{Z}^d]$. The main result of this section is that this contraction is always principal.

Proposition 6.2: *Let $f \in \mathbb{Z}[\mathbb{Z}^d]$ and $N \geqslant 1$. Then the contracted ideal $\langle f\rangle \cap \mathbb{Z}[N\mathbb{Z}^d]$ is a principal ideal in $\mathbb{Z}[N\mathbb{Z}^d]$.*

We begin by briefly sketching the necessary terminology and machinery from commutative algebra, all of which is contained in [1] or can be easily deduced from material there.

For brevity let

$$R = \mathbb{Z}[N\mathbb{Z}^d] \quad \text{and} \quad S = \mathbb{Z}[\mathbb{Z}^d].$$

Both R and S are unique factorization domains, and therefore both are integrally closed [1, Prop. 5.12]. Furthermore, S is integral over R since each variable x_j in S satisfies the monic polynomial $y^N - x_j^N \in R[y]$.

A prime ideal $\mathfrak{p}$ in an integral domain has **height one** if there are no prime ideals strictly between 0 and $\mathfrak{p}$. In a unique factorization domain the prime ideals of height one are exactly the principal ideals generated by irreducible elements. A proper ideal $\mathfrak{q}$ in an integral domain is **primary** if whenever $ab \in \mathfrak{q}$ then either $a \in \mathfrak{q}$ or $b^n \in \mathfrak{q}$ for some $n \geqslant 1$. In this case its radical

$$\{a : a^n \in \mathfrak{q} \text{ for some } n \geqslant 1\}$$

is a prime ideal, say $\mathfrak{p}$, and then $\mathfrak{q}$ is called **$\mathfrak{p}$-primary**. Examples show that in general a power of a prime ideal need not be primary, that a primary ideal need not be the power of a prime ideal, and that even if an ideal has prime radical it need not be primary. The notion of primary ideal, although the correct one for decomposition theory, is quite subtle. However, in our situation things are much simpler.

Lemma 6.3: *Let P be a unique factorization domain, and let $r \in P$ be irreducible. Then the principal ideal $\mathfrak{p} = \langle r\rangle$ is prime, and the $\mathfrak{p}$-primary ideals are exactly the powers $\mathfrak{p}^n$ of $\mathfrak{p}$ for $n \geqslant 1$.*

Proof. It is clear that $\mathfrak{p}$ is prime. To prove that $\mathfrak{p}^n = \langle r^n\rangle$ is $\mathfrak{p}$-primary, suppose that $ab \in \mathfrak{p}^n$, but $a \notin \mathfrak{p}^n$. Then $r \mid b$, so $b^n \in \mathfrak{p}^n$, showing that $\mathfrak{p}^n$ is primary. Clearly the radical of $\mathfrak{p}^n$ is $\mathfrak{p}$, and so $\mathfrak{p}^n$ is $\mathfrak{p}$-primary.

Conversely, suppose that $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal. Since the radical of $\mathfrak{q}$ is $\mathfrak{p}$, it follows that $r^n \in \mathfrak{q}$ for some $n \geqslant 1$. Choose n to be the minimal such power, so that $\mathfrak{p}^n \subset \mathfrak{q}$. Suppose that $\mathfrak{p}^n \neq \mathfrak{q}$, and let $a \in \mathfrak{q} \smallsetminus \mathfrak{p}^n$. Write $a = cr^m$, where $r \nmid c$. Clearly $m \leqslant n-1$, and so $r^m \notin \mathfrak{q}$ by minimality of n. Since $\mathfrak{q}$ is primary, there is a $k \geqslant 1$ such that $c^k \in \mathfrak{q} \subset \mathfrak{p}$. But this contradicts $r \nmid c$. Hence $\mathfrak{p}^n = \mathfrak{q}$. ∎

If $\mathfrak{a}$ is an ideal in S, we denote its **contraction** $\mathfrak{a} \cap R$ to R by $\mathfrak{a}^{\mathsf{c}}$. If $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal in S, then $\mathfrak{p}^{\mathsf{c}}$ is prime and $\mathfrak{q}^{\mathsf{c}}$ is $\mathfrak{p}^{\mathsf{c}}$-primary in R.

One of the important results in commutative algebra, essential to developing a dimension theory using chains of prime ideals, is the so-called "Going Down" theorem [1, Thm. 5.16]. Its hypotheses are satisfied in our situation, and it says the following. Suppose that $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ is a chain of prime ideals in R, and that there is a prime ideal $\mathfrak{q}_2$ in S with $\mathfrak{q}_2^{\mathsf{c}} = \mathfrak{p}_2$. Then there is a chain $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \mathfrak{q}_2$ of prime ideals in S such that $\mathfrak{q}_j^{\mathsf{c}} = \mathfrak{p}_j$ for $j = 0, 1, 2$. From this it follows that prime ideals in S of height one contract to prime ideals in R of height one. In other words, if $h \in S$ is irreducible, then $\langle h \rangle_S \cap R$ is a principal ideal $\langle g \rangle_R$ in R generated by an irreducible polynomial g in R.

Proof of Proposition 6.2. First suppose that $f \in S$ is irreducible. As we just showed, there is an irreducible $g \in R$ such that $\langle f \rangle_S \cap R = \langle g \rangle_R$. Furthermore, if $n \geqslant 1$ then $\langle f^n \rangle_S$ is $\langle f \rangle_S$-primary, and so $\langle f^n \rangle_S \cap R$ is $\langle g \rangle_R$-primary, hence equals $\langle g^k \rangle_R$ for some $k \geqslant 1$.

The result is obvious if $f = 0$, so suppose that $0 \neq f \in S$, and let

$$f = f_1^{n_1} \cdots f_r^{n_r}$$

be its factorization in S into powers of distinct irreducibles f_j. Then there are irreducible polynomials $g_j \in R$ and $k_j \geqslant 1$ such that

$$\langle f_j^{n_j} \rangle_S \cap R = \langle g_j^{k_j} \rangle_R.$$

Hence

$$\begin{aligned}
\langle f \rangle_S \cap R &= \langle f_1^{n_1} \cdots f_r^{n_r} \rangle_S \cap R = (\langle f_1^{n_1} \rangle_S \cap \cdots \langle f_r^{n_r} \rangle_S) \cap R \\
&= (\langle f_1^{n_1} \rangle_S \cap R) \cap \cdots \cap (\langle f_r^{n_r} \rangle_S \cap R) \\
&= \langle g_1^{k_1} \rangle_R \cap \cdots \cap \langle g_r^{k_r} \rangle_R = \langle \mathrm{LCM}(g_1^{k_1}, \ldots, g_r^{k_r}) \rangle_R,
\end{aligned}$$

proving that $\langle f \rangle_S \cap R$ is principal. ∎

Remarks 6.4: (1) It is possible for distinct principal prime ideals in S to contract to the same prime ideal in R. As a simple example, let $d = 1$, $N = 2$, $f_1(x) = x^2 - x - 1$, and $f_2(x) = x^2 + x - 1$. Then each is irreducible in S, but both $\langle f_1\rangle_S$ and $\langle f_2\rangle_S$ contract in $R = \mathbb{Z}[2\mathbb{Z}]$ to $\langle x^4 - 3x^2 + 1\rangle_R$, where $x^4 - 3x^2 + 1$ is irreducible in $\mathbb{Z}[2\mathbb{Z}]$ (but of course not in $\mathbb{Z}[\mathbb{Z}]$). In the proof this is accounted for by using the least common multiple LCM in the last line of the displayed equation above.

(2) A polynomial is **primitive** if the greatest common divisor of its coefficients is 1. If $0 \neq f \in S$ is a nonconstant primitive polynomial with factorization

$$f = f_1^{n_1} \cdots f_r^{n_r}$$

into powers of distinct irreducible polynomials, then by Gauss's Lemma each f_j is primitive as well. Furthermore, $\langle f_j\rangle_S \cap R = \langle g_j\rangle_R$, where each g_j is nonconstant and primitive. It then follows from the proof that $\langle f\rangle_S \cap R$ is generated by a primitive element of R.

(3) There is a completely different proof of Prop. 6.2 using entropy that is valid for all polynomials in S except for those of a very special and easily determined form. Recall that the entropy of α_f is the logarithmic Mahler measure $\mathsf{m}(f)$ defined in (1.2). A **generalized cyclotomic polynomial** in S is one of the form $\mathbf{x}^{\mathbf{n}}c(\mathbf{x}^{\mathbf{k}})$, where c is a cyclotomic polynomial in one variable and $\mathbf{k} \neq \mathbf{0}$. Smyth [38] proved that $\mathsf{m}(f) = 0$ if and only if f is, up to sign, a product generalized cyclotomic polynomial. Assume that $f \in S$ is not such a polynomial, so that the entropy of α_f is strictly positive. A simple argument using cosets of $N\mathbb{Z}^d$ shows that $r_N(X_f)$ also has positive entropy. Now $r_N(X_f) = X_{\mathfrak{a}_N}$ by Lemma 6.1, where $\mathfrak{a}_N = \langle f\rangle_S \cap R$. But an ideal $\mathfrak{a}$ in R for which the shift action of $N\mathbb{Z}^d$ on $X_{\mathfrak{a}}$ has positive entropy must be principal [24, Thm. 4.2].

7. Absolutely irreducible factorizations and Gauss's Lemma

Suppose that $f \in \mathbb{Z}[\mathbb{Z}^d]$ is nonconstant and irreducible. Its factorization into absolutely irreducible polynomials in an extension field of $\mathbb{Q}$ will play a decisive role. A generalization of Gauss's Lemma to number fields enables us to deal with the algebraic properties of the coefficients of the factors.

Two polynomials in $\mathbb{C}[\mathbb{Z}^d]$ are **distinct** if one is not a nonzero scalar multiple of the other. An element $\phi \in \mathbb{C}[\mathbb{Z}^d]$ is **adjusted** if $\mathbf{0}$ is an extreme point of its Newton polytope $\mathcal{N}_\phi$, and is **monic** if it is both adjusted and $\widehat{\phi}(\mathbf{0}) = 1$.

A polynomial in $\mathbb{C}[\mathbb{Z}^d]$ is **absolutely irreducible** if it is irreducible in the unique factorization domain $\mathbb{C}[\mathbb{Z}^d]$. Hence every non-unit $f \in \mathbb{C}[\mathbb{Z}^d]$ has some factorization $f = \phi_1 \cdots \phi_r$ into absolutely irreducible factors ϕ_j. The method of Galois descent [10] shows that, after multiplying the factors by suitable constants, there is a finite normal extension $\mathbb{K}$ of $\mathbb{Q}$ such that each $\phi_j \in \mathbb{K}[\mathbb{Z}^d]$, and also that the coefficients of the ϕ_j generate $\mathbb{K}$, so that $\mathbb{K}$ is the splitting field of f. Furthermore an elementary argument shows that if f is adjusted, then we can multiply the ϕ_j by units in $\mathbb{K}[\mathbb{Z}^d]$ so that each ϕ_j is monic, $\mathcal{N}_{\phi_j} \subset \mathcal{N}_f$, and $f = \widehat{f}(\mathbf{0})\phi_1 \cdots \phi_r$.

Remarks 7.1: (1) When $d = 1$ this factorization is into the linear factors guaranteed by the fundamental theorem of algebra.

(2) A simple sufficient condition for ϕ to be absolutely irreducible is that $\mathcal{N}_\phi$ is not the nontrivial Minkowski sum of two integer polytopes (see [15] for applications of this idea).

(3) There are reasonably good factoring algorithms which, on input f, produce a monic irreducible polynomial in $\mathbb{Z}[x]$ with root θ and an absolutely irreducible $\phi \in \mathbb{Q}(\theta)[\mathbb{Z}^d]$ such that $f = \sigma_1(\phi)\sigma_2(\phi) \cdots \sigma_r(\phi)$, where the σ_j are all the distinct field embeddings of $\mathbb{Q}(\theta)$ into $\mathbb{C}$ (see [12] for an overview of these methods).

The following shows that, unlike factoring, divisibility is not affected when passing to an extension field.

Lemma 7.2: *Suppose that $\mathbb{L}$ is an extension of the field $\mathbb{K}$ and that $f, g \in \mathbb{K}[\mathbb{Z}^d]$. Then f divides g in $\mathbb{K}[\mathbb{Z}^d]$ if and only if f divides g in $\mathbb{L}[\mathbb{Z}^d]$.*

Proof. For the nontrivial direction, suppose there is an $h \in \mathbb{L}[\mathbb{Z}^d]$ such that $fh = g$. Equating coefficients of like monomials gives a system of $\mathbb{K}$-linear equations in the coefficients of h. Since this system has a solution over $\mathbb{L}$, Gaussian elimination shows that this (unique) solution is actually over $\mathbb{K}$, and so $h \in \mathbb{K}[\mathbb{Z}^d]$. ∎

Proposition 7.3: *Let $f \in \mathbb{Z}[\mathbb{Z}^d]$ be nonconstant, adjusted, and irreducible in $\mathbb{Z}[\mathbb{Z}^d]$. Then there is a finite normal extension field $\mathbb{K}$ of $\mathbb{Q}$ and monic absolutely irreducible polynomials $\phi_1, \dots, \phi_r \in \mathbb{K}[\mathbb{Z}^d]$ such that $f = \widehat{f}(\mathbf{0})\phi_1 \cdots \phi_r$ and $\mathcal{N}_{\phi_f} \subset \mathcal{N}_f$ for $1 \leqslant j \leqslant r$. Furthermore, the Galois group* $\mathrm{Gal}(\mathbb{K} : \mathbb{Q})$ *acts transitively on the set of factors ϕ_j, and these factors are pairwise distinct.*

Proof. Our earlier discussion shows there is a factorization $f = \widehat{f}(\mathbf{0})\phi_1 \cdots \phi_r$ over the splitting field $\mathbb{K}$ of f, where each ϕ_j is monic and $\mathcal{N}_{\phi_j} \subset \mathcal{N}_f$ for $1 \leqslant j \leqslant r$. Suppose that $\sigma \in \mathrm{Gal}(\mathbb{K} : \mathbb{Q})$. Since $\sigma(f) = f$, it follows that σ must permute the absolutely irreducible factors up to multiplication by units. But if $\sigma(\phi_j) = c\mathbf{x}^{\mathbf{n}}\phi_k$, then $\mathbf{n} = \mathbf{0}$ since the factors are adjusted and $c = 1$ since they are monic. Hence σ permutes the factors themselves. If there were a proper subset of factors that is invariant under $\mathrm{Gal}(\mathbb{K} : \mathbb{Q})$, then their product ψ would be in $\mathbb{Q}[\mathbb{Z}^d]$ since its coefficients are invariant under $\mathrm{Gal}(\mathbb{K} : \mathbb{Q})$. But then ψ would be a proper divisor of f in $\mathbb{Q}[\mathbb{Z}^d]$ by Lemma 7.2, contradicting irreducibility of f by Gauss's Lemma. A similar argument shows that each factor appears with multiplicity one. ∎

We now give a brief sketch of the extension of Gauss's Lemma to number fields and the consequences we use. Let $\mathbb{K}$ be a finite extension of $\mathbb{Q}$, and $\mathcal{O}_{\mathbb{K}}$ be the ring of algebraic integers in $\mathbb{K}$. A **fractional ideal** $\mathfrak{a}$ in $\mathbb{K}$ is a nonzero $\mathcal{O}_{\mathbb{K}}$-submodule such that there is an integer b for which $b\mathfrak{a} \subset \mathcal{O}_{\mathbb{K}}$. Fractional ideals can be added and multiplied, with $\mathcal{O}_{\mathbb{K}}$ being the multiplicative identity. A fractional ideal contained in $\mathcal{O}_{\mathbb{K}}$ is an ideal in the usual ring-theoretic sense. The pivotal result is that the set of fractional ideals form a group, the set of principal fractional ideals (those of the form $\mathcal{O}_{\mathbb{K}}\beta$ for some $\beta \in \mathbb{K}$) form a subgroup, and the quotient of these groups is a finite abelian group called the class group which measures how far $\mathcal{O}_{\mathbb{K}}$ is from being a principal ideal domain.

Let $\phi \in \mathbb{K}[\mathbb{Z}^d]$. Define the **content** $\mathfrak{c}_{\mathbb{K}}(\phi)$ to be the factional ideal in $\mathbb{K}$ generated by the coefficients of ϕ. Say that ϕ is **primitive** if $\mathfrak{c}_{\mathbb{K}}(\phi) = \mathcal{O}_{\mathbb{K}}$. It is easy to check that although content depends on the ambient field $\mathbb{K}$, primitivity does not: if $\phi \in \mathbb{K}[\mathbb{Z}^d]$ and $\phi \in \mathbb{L}[\mathbb{Z}^d]$, then $\mathfrak{c}_{\mathbb{K}}(\phi) = \mathcal{O}_{\mathbb{K}}$ if and only if $\mathfrak{c}_{\mathbb{L}}(\phi) = \mathcal{O}_{\mathbb{L}}$. For a proof of the following version of Gauss's Lemma, see [8, Chap. 6, Lemma 2.1], or the more leisurely account in [27, Thm. 8.2].

Theorem 7.4 (Gauss's Lemma for number fields): *Let $\mathbb{K}$ be a number field and $\phi, \psi \in \mathbb{K}[\mathbb{Z}^d]$. Then*

$$\mathfrak{c}_{\mathbb{K}}(\phi\psi) = \mathfrak{c}_{\mathbb{K}}(\phi)\mathfrak{c}_{\mathbb{K}}(\psi).$$

In particular, if $\phi, \psi \in \mathcal{O}_{\mathbb{K}}[\mathbb{Z}^d]$ then $\phi\psi$ is primitive if and only if both ϕ and ψ are primitive. If $\phi, \psi \in \mathcal{O}_{\mathbb{K}}[\mathbb{Z}^d]$ are primitive, and if $\phi = \beta\psi$ for some $\beta \in \mathbb{K}$, then β is a unit in $\mathcal{O}_{\mathbb{K}}$.

Remark 7.5: Suppose that $f \in \mathbb{Z}[\mathbb{Z}^d]$ is primitive and that $N \geqslant 1$. Let $\zeta_N = e^{2\pi i/N}$, which is a unit in $\mathbb{Q}(\zeta_N)$. Hence each rotate $\boldsymbol{\omega} \cdot f$, where $\boldsymbol{\omega} \in \Omega_N^d$, is primitive in $\mathbb{Q}(\zeta_N)[\mathbb{Z}^d]$. The preceding theorem then shows that the product $f_{\langle N \rangle}$ of these rotates is also primitive in $\mathbb{Q}(\zeta_N)[\mathbb{Z}^d]$, and hence in $\mathbb{Z}[\mathbb{Z}^d]$ (since primitivity is independent of ambient field), a fact we already observed in Remark 6.4(2).

8. Decimated polynomials and decimated actions

Let $f \in \mathbb{Z}[\mathbb{Z}^d]$ be irreducible. Here we explain the relationship between the Nth decimation $f_{\langle N \rangle}$ of f and the generator g_N of the contracted ideal $\langle f \rangle \cap \mathbb{Z}[N\mathbb{Z}^d]$ that defines the Nth decimation $r_N(X_f)$ of (X_f, α_f). Roughly speaking, g_N is a constant times the product of all distinct rotates by elements of Ω_N^d of the absolutely irreducible factors ϕ_j of f as described in Proposition 7.3. Each rotate appears with the same multiplicity e_N that can be computed from the ϕ_j. Thus $f_{\langle N \rangle} = c\, g_N^{e_N}$, and an application of Gauss's Lemma shows that we may take $c = 1$. Furthermore, there is an integer $Q(f)$, that can also be computed from the ϕ_j, such that $f_{\langle N \rangle} = g_N$ for all N relatively prime to $Q(f)$. Examples will illustrate the two sources of the multiplicity e_N.

In what follows we let $\zeta_N = e^{2\pi i/N}$, which is a generator of Ω_N.

LEMMA 8.1: *If $f \in \mathbb{Z}[\mathbb{Z}^d]$ then $f_{\langle N \rangle} \in \mathbb{Z}[N\mathbb{Z}^d]$.*

Proof. Since $f_{\langle N \rangle} = \prod_{\boldsymbol{\omega} \in \Omega_N^d} \boldsymbol{\omega} \cdot f$, it follows that $f_{\langle N \rangle} = \boldsymbol{\omega} \cdot f_{\langle N \rangle}$ for every $\boldsymbol{\omega} \in \Omega_N^d$. Suppose that $\widehat{f}_{\langle N \rangle}(\mathbf{k}) \neq 0$. Then since

$$\widehat{f}_{\langle N \rangle}(\mathbf{k}) = (\boldsymbol{\omega} \cdot f_{\langle N \rangle})\widehat{\ }(\mathbf{k}) = \boldsymbol{\omega}^{\mathbf{k}}\, \widehat{f}_{\langle N \rangle}(\mathbf{k}),$$

we see that

$$\boldsymbol{\omega}^{\mathbf{k}} = 1$$

for every $\boldsymbol{\omega} \in \Omega_N^d$, and hence $\mathbf{k} \in N\mathbb{Z}^d$. Thus $f_{\langle N \rangle} \in \mathbb{Q}(\zeta_N)[N\mathbb{Z}^d]$.

The Galois group $G := \mathrm{Gal}(\mathbb{Q}(\zeta_N) : \mathbb{Q})$ acts on Ω_N^d coordinate-wise. If $\sigma \in G$, then $\sigma(\boldsymbol{\omega} \cdot f) = \sigma(\boldsymbol{\omega}) \cdot f$ since f has integer coefficients. Thus σ permutes the rotates of f, and so $\sigma(f_{\langle N \rangle}) = f_{\langle N \rangle}$ for every $\sigma \in G$. It follows that the coefficients of $f_{\langle N \rangle}$ are both rational and algebraic integers, and so $f_{\langle N \rangle} \in \mathbb{Z}[N\mathbb{Z}^d]$. ∎

LEMMA 8.2: *Let $f \in \mathbb{Z}[\mathbb{Z}^d]$ and g_N be a generator of the contracted ideal $\langle f\rangle \cap \mathbb{Z}[N\mathbb{Z}^d]$. Then g_N divides $f_{\langle N\rangle}$ in $\mathbb{Z}[N\mathbb{Z}^d]$.*

Proof. Since f is one of the factors in forming $f_{\langle N\rangle}$, it follows that f divides $f_{\langle N\rangle}$ in $\mathbb{Q}(\zeta_N)[\mathbb{Z}^d]$. Hence f divides $f_{\langle N\rangle}$ in $\mathbb{Q}[\mathbb{Z}^d]$ by Lemma 7.2. The coefficients of $f_{\langle N\rangle}/f$ are both rational and algebraic integers, and so $f_{\langle N\rangle}/f \in \mathbb{Z}[\mathbb{Z}^d]$. Hence $f_{\langle N\rangle} \in \langle f\rangle \cap \mathbb{Z}[N\mathbb{Z}^d]$, and it is thus divisible by the generator g_N. ∎

Remark 8.3: Since the generator of a principal ideal is unique only up to units, it will be convenient to have a convention to pick a generator. In what follows we will assume that f is adjusted and that $\widehat{f}(\mathbf{0}) > 0$. Then clearly $f_{\langle N\rangle}$ has the same properties. By the previous lemma, we can also assume that g_N is adjusted, that $\mathcal{N}_{g_N} \subset \mathcal{N}_{f_{\langle N\rangle}}$, and that $\widehat{g}_N(\mathbf{0}) > 0$.

Before continuing, we remark that if f is a constant integer n, then

$$f_{\langle N\rangle} = n^{N^d}$$

while $g_N = n$. Let us call a polynomial $f \in \mathbb{Z}[\mathbb{Z}^d]$ **nonconstant** if $|\operatorname{supp} f| > 1$, and it is these we now turn to.

Let $f \in \mathbb{Z}[\mathbb{Z}^d]$ be adjusted. Define its **support group** Γ_f to be the subgroup of $\mathbb{Z}^d$ generated by $\operatorname{supp} f$. It is easy to check that the support group is independent of which extreme point of $\mathcal{N}_f$ is used to adjust f. We say that f is **full** if $\Gamma_f = \mathbb{Z}^d$.

The following shows that in some cases, including $f(x,y) = 1+x+y$ from Example 2.4, $f_{\langle N\rangle} = g_N$ for all $N \geqslant 1$.

PROPOSITION 8.4: *Let $f \in \mathbb{Z}[\mathbb{Z}^d]$ be adjusted, irreducible, and full. Further assume that f is absolutely irreducible in $\mathbb{C}[\mathbb{Z}^d]$. Then $f_{\langle N\rangle} = g_N$ for every $N \geqslant 1$.*

Proof. Since the map $f \mapsto \boldsymbol{\omega}\cdot f$ is a ring isomorphism of $\mathbb{C}[\mathbb{Z}^d]$, each $\boldsymbol{\omega}\cdot f$ is absolutely irreducible. Suppose that $\boldsymbol{\omega}\cdot f = \boldsymbol{\omega}'\cdot f$. Since

$$\boldsymbol{\omega}^{\mathbf{k}}\widehat{f}(\mathbf{k}) = (\boldsymbol{\omega}')^{\mathbf{k}}\widehat{f}(\mathbf{k}),$$

it follows that $\boldsymbol{\omega}^{\mathbf{k}} = (\boldsymbol{\omega}')^{\mathbf{k}}$ for all $\mathbf{k} \in \operatorname{supp} f$, hence for all $\mathbf{k} \in \Gamma_f = \mathbb{Z}^d$, and so $\boldsymbol{\omega} = \boldsymbol{\omega}'$. Thus the rotates of $\boldsymbol{\omega}\cdot f$ for $\boldsymbol{\omega} \in \Omega_N^d$ are pairwise distinct absolutely irreducible polynomials in $\mathbb{C}[\mathbb{Z}^d]$ whose product is $f_{\langle N\rangle}$.

By Lemma 8.2, g_N divides $f_{\langle N\rangle}$ in $\mathbb{C}[\mathbb{Z}^d]$. Hence some rotate $\boldsymbol{\omega}\cdot f$ divides g_N. Since $g_N \in \mathbb{Z}[N\mathbb{Z}^d]$, it is invariant under all rotations in Ω_N^d. Hence g_N is divisible by all rotates $\boldsymbol{\omega}\cdot f$, and so g_N and $f_{\langle N\rangle}$ have the same absolute factorizations in $\mathbb{C}[\mathbb{Z}^d]$, and hence $f_{\langle N\rangle} = c\,g_N$ for some constant $c \in \mathbb{C}$. Recalling our conventions in Remark 8.3, comparing constant terms shows that $c = \widehat{f}(\mathbf{0})^{N^d}/\widehat{g}_N(\mathbf{0}) \in \mathbb{Q}$. But $f_{\langle N\rangle}$ and g_N are both primitive in $\mathbb{Z}[N\mathbb{Z}^d]$, and so $c = \pm 1$, and our convention on positivity of constant terms then gives $c = 1$. ∎

The following example shows that when the polynomial is not full there can be multiplicity $e_N > 1$.

Example 8.5: Let $d = 2$ and $f(x,y) = 1 + x + y^2$. Since $\mathcal{N}_f$ is not a nontrivial Minkowski sum of integer polytopes, we see that f is absolutely irreducible. Suppose that N is odd. Since $-1 \notin \Omega_N$, all rotates $\boldsymbol{\omega}\cdot f$ for $\boldsymbol{\omega} \in \Omega_N^2$ are distinct, and the same arguments as in the previous proposition show that $f_{\langle N\rangle} = g_N$.

However, if N is even, then $-1 \in \Omega_N$ and the rotate of f by (ω_1, ω_2) equals that by $(\omega_1, -\omega_2)$. As we will see in Proposition 8.7, the product of the distinct rotates of f equals g_N, and so $f_{\langle N\rangle} = g_N^2$ when N is even.

Next we characterize when rotates can coincide.

LEMMA 8.6: *Let $\phi \in \mathbb{C}[\mathbb{Z}^d]$ be adjusted, and Γ_ϕ be its support group. Then the dual of the stabilizer group $S_N(\phi) := \{\boldsymbol{\omega} \in \Omega_N^d : \boldsymbol{\omega}\cdot\phi = \phi\}$ is $\mathbb{Z}^d/(\Gamma_\phi + N\mathbb{Z}^d)$. Two rotates of ϕ differ by a multiplicative unit in $\mathbb{C}[\mathbb{Z}^d]$ if and only if they are equal. If Γ_ϕ has finite index K in $\mathbb{Z}^d$, then $S_N(\phi)$ is trivial for every N relatively prime to K.*

Proof. Suppose that $\boldsymbol{\omega} \in S_N(\phi)$. Since $\widehat{\phi}(\mathbf{k}) = (\boldsymbol{\omega}\cdot\phi)\widehat{\ }(\mathbf{k}) = \boldsymbol{\omega}^{\mathbf{k}}\widehat{\phi}(\mathbf{k})$, it follows that $\boldsymbol{\omega}^{\mathbf{k}} = 1$ for every $\mathbf{k} \in \operatorname{supp}\phi$. Hence $\boldsymbol{\omega}$ annihilates Γ_ϕ as well as $N\mathbb{Z}^d$, thus their sum. Conversely, every $\boldsymbol{\omega}$ annihilating $\Gamma_\phi + N\mathbb{Z}^d$ must be in $S_N(\phi)$. Hence the annihilator of $S_N(\phi)$ equals $\Gamma_\phi + N\mathbb{Z}^d$, and so its dual group is $\mathbb{Z}^d/(\Gamma_\phi + N\mathbb{Z}^d)$.

The multiplicative units in $\mathbb{C}[\mathbb{Z}^d]$ have the form $c\,\mathbf{x}^{\mathbf{n}}$ for some $c \in \mathbb{C}$, so the second statement is obvious since ϕ is adjusted.

Suppose that Γ_ϕ has finite index K in $\mathbb{Z}^d$. If N is relatively prime to K, then multiplication by N on $\mathbb{Z}^d/\Gamma_\phi$ is injective, hence surjective. Thus modulo Γ_ϕ every element in $\mathbb{Z}^d$ is a multiple of N, and hence $\Gamma_\phi + N\mathbb{Z}^d = \mathbb{Z}^d$. ∎

PROPOSITION 8.7: *Let $f \in \mathbb{Z}[\mathbb{Z}^d]$ be adjusted and irreducible, and further assume that f is absolutely irreducible in $\mathbb{C}[\mathbb{Z}^d]$. Then*

$$f_{\langle N\rangle} = g_N^{e_N}, \quad \textit{where } e_N = |S_N(f)| = |\mathbb{Z}^d/(\Gamma_f + N\mathbb{Z}^d)|.$$

Proof. Recall our conventions in Remark 8.3. Since g_N divides $f_{\langle N\rangle}$, it must be divisible by at least one (absolutely irreducible) rotate of f. Invariance of g_N by every rotate in Ω_N^d shows that g_N is therefore divisible by the product h of all the distinct rotates of f. The arguments in Lemmas 8.1 and 8.2 apply to show that $h \in \langle f\rangle \cap \mathbb{Z}[N\mathbb{Z}^d]$. Thus g_N divides h in $\mathbb{C}[\mathbb{Z}^d]$ as well, and so $g_N = c\,h$ for some $c \in \mathbb{C}$. Evaluating constant terms shows that $c \in \mathbb{Q}$. Since g_N is irreducible in $\mathbb{Z}[N\mathbb{Z}^d]$, it is primitive. Each rotate of f is primitive in $\mathbb{Q}(\zeta_N)[\mathbb{Z}^d]$, and so h is primitive by Theorem 7.4. Hence $c = \pm 1$, and then $c = 1$ follows from our sign conventions. By Lemma 8.6, each rotate of f is repeated exactly e_N times, and so $f_{\langle N\rangle} = g_N^{e_N}$. ∎

When f is absolutely irreducible, the only source of multiplicity $e_N > 1$ is its support group. However, if f has several absolutely irreducible factors, a new source of multiplicity can occur, namely that one factor could rotate to another factor. This possibility is illustrated in the following three examples.

Example 8.8: Let $d = 1$ and

$$f(x) = 1 - 2x^2 = (1 + \sqrt{2}x)(1 - \sqrt{2}x) = \phi_1(x)\phi_2(x).$$

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$ be given by $\sigma(\sqrt{2}) = -\sqrt{2}$. Then

$$\sigma(\phi_1) = \phi_2 = (-1)\cdot\phi_1.$$

Now $f_{\langle N\rangle}$ is the product of $\zeta_N^j \cdot \phi_k$ for $0 \leqslant j < N$ and $k = 1, 2$. If N is odd, then $-1 \notin \Omega_N$ and so all $2N$ factors are distinct. Our earlier arguments then show that $f_{\langle N\rangle} = g_N$. However, if N is even, then $-1 \in \Omega_N$, and the set of rotates of ϕ_1 coincide with the set of those of ϕ_2, and so $f_{\langle N\rangle} = g_N^2$ for even N. Here f is an irreducible polynomial with a pair of roots whose ratio is a nontrivial root of unity.

The commingling of absolutely irreducible factors under rotations can happen in more subtle ways.

Example 8.9: Let $d = 1$ and $f(x) = 1 - 2x + 4x^2 - 3x^3 + x^4$, which is full and irreducible in $\mathbb{Z}[\mathbb{Z}]$. Let $\lambda = (1 + \sqrt{5})/2$, $\mu = (1 - \sqrt{5})/2$, and $\zeta = \zeta_5$. The absolutely irreducible factorization of f is

$$f(x) = (1 - \zeta\lambda x)((1 - \zeta^4\lambda x)(1 - \zeta^2\mu x)(1 - \zeta^3\mu x) = \phi_1(x)\phi_2(x)\phi_3(x)\phi_4(x).$$

Note that $\zeta^3 \cdot \phi_1 = \phi_2$ and that $\zeta \cdot \phi_3 = \phi_4$. If N is relatively prime to 5, then $\zeta \notin \Omega_N$, and so all $4N$ rotates are distinct and $f_{\langle N \rangle} = g_N$ as before. However, if $5 \mid N$ then $\zeta \in \Omega_N$ and each rotate is repeated twice, and so $f_{\langle N \rangle} = g_N^2$ in this case.

What is driving this example is the inclusion $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta)$, and so the Galois automorphism $\sqrt{5} \mapsto -\sqrt{5}$ of $\mathbb{Q}(\sqrt{5})$ is the restriction of the automorphism $\zeta \mapsto \zeta^2$ of $\mathbb{Q}(\zeta)$.

Remark 8.10: Irreducible polynomials in $\mathbb{Z}[x]$ having distinct roots whose ratio is a root of unity, such as those in the previous two examples, are called **degenerate**. Such polynomials have an extensive literature (see for instance [14, §1.1.9]), and appear in the celebrated Skolem–Mahler–Lech Theorem that the set of indices at which a recurring sequence of integers vanishes is, modulo a finite set, the union of arithmetic progressions [4].

There is a simple way to detect whether $f(x) \in \mathbb{Z}[x]$ is degenerate. Introduce a new variable t, and compute the resultant $g(x) \in \mathbb{Z}[x]$ of the polynomials $f(tx)$ and $f(t)$ with respect to t, which can be done efficiently using rational arithmetic. The roots of $g(x)$ are the ratios of all pairs of roots of f. Thus $f(x)$ is degenerate if and only if $g(x)$ contains a nontrivial cyclotomic factor. Applying this to $f(x)$ from the previous example gives

$$g(x) = (x-1)^5(x^4-4x^3+6x^2+x+1)(x^4+x^3+6x^2-4x+1)(x^4+x^3+x^2+x+1).$$

The last factor reveals that $f(x)$ has two roots whose ratio is a nontrivial 5th root of unity.

Example 8.11: Let $d = 2$ and

$$f(x, y) = 1 - x - y - xy + x^2 + y^2,$$

which is full and irreducible in $\mathbb{Z}[\mathbb{Z}^2]$. Let $\zeta = \zeta_3$. The absolutely irreducible factorization of f is

$$f(x, y) = (1 + \zeta x + \zeta^2 y)(1 + \zeta^2 x + \zeta y) = \phi_1(x, y)\phi_2(x, y).$$

Here ϕ_1 is mapped to ϕ_2 by the element σ in $\mathrm{Gal}(\mathbb{Q}(\zeta):\mathbb{Q})$ mapping ζ to ζ^2, and also $\sigma(\phi_1)=\phi_2=(\zeta,\zeta^2)\cdot\phi_1$. By the now familiar arguments, if N is relatively prime to 3 then $\zeta\notin\Omega_N$, and so all rotates are distinct and hence $f_{\langle N\rangle}=g_N$. However, if 3 divides N, then distinct rotates are repeated twice, and so $f_{\langle N\rangle}=g_N^2$. For instance

$$f_{\langle 3\rangle}=(1+3x^3+3y^3+3x^6-21x^3y^3+3y^3+x^9+3x^3y^6+3x^6y^3+y^9)^2=g_3^2.$$

With these examples in mind, we come to the main result of this section.

Theorem 8.12: *Let $f\in\mathbb{Z}[\mathbb{Z}^d]$ be irreducible, which we may assume is adjusted with positive constant term. For every $N\geqslant 1$ there is an irreducible $g_N\in\mathbb{Z}[N\mathbb{Z}^d]$ and $e_N\geqslant 1$ such that*

$$\langle f\rangle_{\mathbb{Z}[\mathbb{Z}^d]}\cap\mathbb{Z}[N\mathbb{Z}^d]=\langle g_N\rangle_{\mathbb{Z}[N\mathbb{Z}^d]}\quad\text{and}\quad f_{\langle N\rangle}=g_N^{e_N}.$$

The multiplicity e_N can be computed from the absolutely irreducible factorization of f in $\mathbb{C}[\mathbb{Z}^d]$. If the support of f generates a finite-index subgroup of $\mathbb{Z}^d$, then there is an integer $Q(f)$, which can also be computed from the absolutely irreducible factors of f, such that $e_N=1$ for every N that is relatively prime to $Q(f)$. Finally,

$$\langle f^k\rangle_{\mathbb{Z}[\mathbb{Z}^d]}\cap\mathbb{Z}[N\mathbb{Z}^d]=\langle g_N^k\rangle_{\mathbb{Z}[N\mathbb{Z}^d]}$$

for every $k\geqslant 1$.

Proof. Recall our conventions in Remark 8.3. Let $\mathbb{K}$ be the splitting field of f, and $f=\widehat{f}(\mathbf{0})\phi_1\cdots\phi_r$ be the factorization of f using monic absolutely irreducible $\phi_j\in\mathbb{K}[\mathbb{Z}^d]$ from Proposition 7.3. Let $\Phi=\{\phi_1,\dots,\phi_r\}$. Since the ϕ_j are monic, $\mathrm{Gal}(\mathbb{K}:\mathbb{Q})$ permutes the elements of Φ, and this action is transitive by irreducibility of f.

Now fix $N\geqslant 1$. Then $\mathbb{K}(\zeta_N)$ is a normal extension of $\mathbb{Q}$. Let $G=\mathrm{Gal}(\mathbb{K}(\zeta_N):\mathbb{Q})$. Consider the set $\Omega_N^d\times\Phi$. The group Ω_N^d acts on this set via

$$\boldsymbol{\omega}'\cdot(\boldsymbol{\omega},\phi_j)=(\boldsymbol{\omega}'\boldsymbol{\omega},\phi_j).$$

The group G also acts on this set via $\sigma\cdot(\boldsymbol{\omega},\phi_j)=(\sigma(\boldsymbol{\omega}),\sigma(\phi_j))$. More precisely, $\sigma\in G$ acts on the first coordinate using its restriction to $\mathbb{Q}(\zeta_N)$ and on the second coordinate using its restriction to $\mathbb{K}$. These actions combine to give an action of the semidirect product $G\ltimes\Omega_N^d$ defined using the action of G on Ω_N^d, so that $\sigma\boldsymbol{\omega}=\sigma(\boldsymbol{\omega})\sigma$.

Define an equivalence relation $\sim$ on $\Omega_N^d \times \Phi$ by $(\boldsymbol{\omega}, \phi_j) \sim (\boldsymbol{\omega}', \phi_k)$ if and only if $\boldsymbol{\omega} \cdot \phi_j = \boldsymbol{\omega}' \cdot \phi_k$. It is routine to verify that $G \ltimes \Omega_N^d$ preserves equivalence classes. Since $\mathrm{Gal}(\mathbb{K} : \mathbb{Q})$ acts transitively on Φ, it follows that $G \ltimes \Omega_N^d$ acts transitively on $\Omega_N^d \times \Phi$. Hence all equivalence classes have the same cardinality, say $e_N \geqslant 1$. Pick one representative $(\boldsymbol{\omega}, \phi_j)$ from each equivalence class, and let $\widetilde{g}_N$ be the product of the corresponding polynomials $\boldsymbol{\omega} \cdot \phi_j$.

Observe that by its construction $\widetilde{g}_N$ is invariant under $G \ltimes \Omega_N^d$. Invariance under Ω_N^d implies that $\widetilde{g}_N \in \mathbb{K}(\zeta_N)[N\mathbb{Z}^d]$, and invariance under G further implies that $\widetilde{g}_N \in \mathbb{Q}[N\mathbb{Z}^d]$. Then transitivity of $G \ltimes \Omega_N^d$ on $\Omega_N^d \times \Phi$ shows that $\widetilde{g}_N$ is irreducible in $\mathbb{Q}[N\mathbb{Z}^d]$.

We have that $f_{\langle N \rangle} = \widehat{f}(\mathbf{0})^{N^d} \widetilde{g}_N^{e_N}$. Let q be the least positive integer such that $q\widetilde{g}_N \in \mathbb{Z}[N\mathbb{Z}^d]$, so that $g_N := q\widetilde{g}_N$ is primitive. Then

$$f_{\langle N \rangle} = (\widehat{f}(\mathbf{0})^{N^d} / q^{e_N}) g_N^{e_N}.$$

But both $f_{\langle N \rangle}$ and $g_N^{e_N}$ are primitive with positive constant terms, and hence $f_{\langle N \rangle} = g_N^{e_N}$.

We now turn to computing e_N. Each of the absolutely irreducible factors ϕ_j has the same support since they are all Galois conjugates. Let Γ_ϕ denote the common support group of each. By Lemma 8.6, each contributes multiplicity $|\mathbb{Z}^d/(\Gamma_\phi + N\mathbb{Z}^d)|$. Further multiplicity arises if one factor can be rotated by an element of Ω_N^d to another. This property divides Φ into equivalence classes, with all classes having the same cardinality s. It then follows that

$$e_N = |\mathbb{Z}^d/(\Gamma_\phi + N\mathbb{Z}^d)| s.$$

Next, we determine sufficient conditions on N so that $e_N = 1$. Assume that Γ_f has finite index in $\mathbb{Z}^d$. Clearly $\Gamma_f \subset \Gamma_\phi$, and so Γ_ϕ also has finite index. By Lemma 8.6, if N is relatively prime to the index $[\mathbb{Z}^d : \Gamma_\phi]$ of Γ_ϕ, then $|\mathbb{Z}^d/(\Gamma_\phi + N\mathbb{Z}^d)| = 1$.

To analyze when one ϕ_j can rotate to another, we need to consider the group $\Omega_{\mathbb{K}}$ of roots of unity in the splitting field $\mathbb{K}$ of f. This is a finite cyclic group, and so equals Ω_n for some $n \geqslant 1$. Now $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where φ denotes the Euler function. Since $\mathbb{Q}(\zeta_n) \subset \mathbb{K}$, it follows that $\varphi(n) \leqslant [\mathbb{K} : \mathbb{Q}]$. A simple argument shows that $\varphi(n) \geqslant \sqrt{n}/2$ for all $n \geqslant 1$, and so $n \leqslant 4[\mathbb{K} : \mathbb{Q}]^2$. Hence if N is relatively prime to $(4[\mathbb{K} : \mathbb{Q}]^2)!$, then $\Omega_N \cap \Omega_{\mathbb{K}} = \{1\}$. For such an N suppose that $\boldsymbol{\omega} \cdot \phi_i = \phi_j$ for some $\boldsymbol{\omega} \in \Omega_N^d$. For each $\mathbf{k} \in \operatorname{supp} \phi_i = \operatorname{supp} \phi_j$

we have that $\boldsymbol{\omega}^{\mathbf{k}}\widehat{\phi}_i(\mathbf{k}) = \widehat{\phi}_j(\mathbf{k})$, and so

$$\boldsymbol{\omega}^{\mathbf{k}} = \widehat{\phi}_j(\mathbf{k})/\widehat{\phi}_i(\mathbf{k}) \in \Omega_N \cap \Omega_{\mathbb{K}} = \{1\}.$$

But this implies that $\phi_i = \phi_j$.

Putting these together, we let $Q(f) = [\mathbb{Z}^d : \Gamma_\phi](4[\mathbb{K} : \mathbb{Q}]^2)!$, and conclude that if N is relatively prime to $Q(f)$ then $e_N = 1$. ∎

9. Remarks and Questions

Here we make some further remarks and ask several questions related to decimations.

9.1. More general lattices. Let us call a finite-index subgroup of $\mathbb{Z}^d$ a **lattice**. We have used the sequence $\{N\mathbb{Z}^d\}$ of lattices to define decimation, but these definitions easily extend to all lattices. Let $\Lambda \in \mathbb{Z}^d$ be a lattice, and let Ω_Λ denote the dual group of $\mathbb{Z}^d/\Lambda$, which has cardinality $[\mathbb{Z}^d : \Lambda]$, the index of Λ in $\mathbb{Z}^d$. Define $f_{\langle\Lambda\rangle} = \prod_{\boldsymbol{\omega}\in\Omega_\Lambda} \boldsymbol{\omega} \cdot f$, and

$$L_\Lambda f = E_{[\mathbb{Z}^d :\, \Lambda]}\Big(\frac{1}{[\mathbb{Z}^d : \Lambda]} \log|\widehat{f}_{\langle\Lambda\rangle}|\Big). \tag{9.1}$$

For a sequence $\{\Lambda_N\}$ of lattices, let us say $\Lambda_N \to \infty$ if for every $r > 0$ we have that $\{\mathbf{n} \in \Lambda_N : \|\mathbf{n}\| < r\} = \{\mathbf{0}\}$ for all large enough N.

If we replace the "square" lattices $N\mathbb{Z}^d$ with "rectangular" lattices of the form

$$\Lambda_N = a_N^{(1)}\mathbb{Z} \oplus \cdots \oplus a_N^{(d)}\mathbb{Z},$$

then a straightforward modification of our proof shows that $CH(L_{\Lambda_N} f) \to D_f$ uniformly on $\mathcal{N}_f$ provided that $a_N^{(k)} \to \infty$ as $N \to \infty$ for each $1 \leqslant k \leqslant d$.

However, the analogous question for general lattices is much more subtle, since the rescaling argument that is basic to our proof has no obvious extension. Nevertheless, in recent unpublished work Hanfeng Li has been able to establish the uniform convergence of $CH(L_{\Lambda_N} f)$ to D_f for every sequence $\{\Lambda_N\}$ of lattices with $\Lambda_N \to \infty$.

We can also investigate decimations by lattices with different limiting behavior. Let $\mathcal{C}(\mathbb{Z}^d)$ denote the set of subgroups of $\mathbb{Z}^d$. We can give a topology to $\mathcal{C}(\mathbb{Z}^d)$ by declaring two subgroups to be close if they agree on a large ball around $\mathbf{0}$. For example, in this topology $\Lambda_N \to \{\mathbf{0}\}$ means that $\Lambda_N \to \infty$ as above. This is a special case of the Chabauty topology on the set $\mathcal{C}(G)$ of closed subgroups of a locally compact group G. This topology is named after Claude Chabauty, who in 1950 introduced it [9] to generalize Mahler's compactness criterion [28] for lattices in $\mathbb{R}^d$ to lattices in locally compact groups. The Chabauty space $\mathcal{C}(G)$ has been investigated by many authors, for instance by Cornulier [11] when G is abelian. Even for familiar groups their Chabauty space can be intricate to analyze. For example, Hubbard and Pourezza [20] used a tricky argument to prove that $\mathcal{C}(\mathbb{R}^2)$ is homeomorphic to the four-dimensional sphere.

Question 9.1: Let Δ be a subgroup of $\mathbb{Z}^d$ of infinite index. Suppose that $\{\Lambda_N\}$ is a sequence of lattices such that $\Lambda_N \to \Delta$ as $N \to \infty$. Do the functions $\mathsf{CH}(\mathsf{L}_{\Lambda_N} f)$ always converge on $\mathcal{N}_f$, and if so what is the limit function in terms of f and Δ?

9.2. Exponential size of decimation coefficients. In Example 2.3 we saw that if $f \in \mathbb{C}[\mathbb{Z}]$ is allowed to have complex coefficients, then some of the coefficients of $f_{\langle N\rangle}$ may have exponential size drastically different from that predicted by D_f. However, if $f \in \mathbb{Z}[\mathbb{Z}]$ is restricted to have integer coefficients, then this behavior cannot happen, as indicated by Example 2.2. More precisely, using the diophantine results of Gelfond mentioned there, one can show that if $f \in \mathbb{Z}[\mathbb{Z}]$ has $\operatorname{supp} f = \{0, 1, \dots, r\}$ and $\varepsilon > 0$, then for all sufficiently large N we have that $|\widehat{f}_{\langle N\rangle}(kN)|$ is between $e^{N(\mathsf{D}_f(k)\pm\varepsilon)}$ for each $0 \leqslant k \leqslant r$ for which $\widehat{f}_{\langle N\rangle}(kN) \neq 0$.

This raises the intriguing question of whether this extends to $f \in \mathbb{Z}[\mathbb{Z}^d]$ for $d \geqslant 2$, i.e., do all nonzero coefficients of $f_{\langle N\rangle}$ have the approximate exponential size predicted by D_f. The following gives a precise quantitative formulation.

Question 9.2: Let $f \in \mathbb{Z}[\mathbb{Z}^d]$. Fix $\mathbf{r}_0 \in \mathcal{N}_f$, and let $\varepsilon > 0$. Are there $\delta > 0$ and $N_0 \geqslant 1$ such that if $N \geqslant N_0$ and $\mathbf{r} \in N^{-d}\mathbb{Z}^d \cap \mathcal{N}_f$ with $\|\mathbf{r} - \mathbf{r}_0\| < \delta$, and if $\mathsf{L}_N f(\mathbf{r}) \neq -\infty$, then $|\mathsf{L}_N f(\mathbf{r}) - \mathsf{D}_f(\mathbf{r})| < \varepsilon$? Can δ and N_0 be chosen uniformly for $\mathbf{r}_0 \in \mathcal{N}_f$?

Some evidence for a positive answer comes from polynomials in two variables related to dimer models, as discussed in Remark 2.6. Using the additional machinery afforded by the physical interpretation of the related partition function and the resulting subadditivity, the exponential size of the coefficients can be shown to obey the estimates in the question. In particular, this applies to $f(x, y) = 1 + x + y$, although we do not know of any direct argument for this.

9.3. Continuity of $\exp[\mathsf{D}_f]$ in the coefficients of f. Start by fixing a cube $B_n = \{-n, \dots, n\}^d \subset \mathbb{Z}^d$. We can identify a polynomial $f \in \mathbb{C}[\mathbb{Z}^d]$ whose support is in B_n with its coefficient function $\widehat{f} \in \mathbb{C}^{B_n}$. Boyd [5] showed that the function $\mathbb{C}^{B_n} \to [0, \infty)$ given by $\widehat{f} \mapsto \mathsf{M}(f) = \exp[\mathsf{m}(f)]$ is continuous in the coefficients of f.

Recalling that $\mathsf{m}(f)$ is the maximum value of D_f, this suggests looking at $\exp[\mathsf{D}_f]$, which is a nonnegative upper semicontinuous function on B_n (the discontinuities occur at the boundary of $\mathcal{N}_f \subset B_n$). A function $\phi \colon B_n \to \mathbb{R}$ is upper semicontinuous if and only if its subgraph $\{(\mathbf{u}, t) \in B_n \times \mathbb{R} : t \leqslant \phi(\mathbf{u})\}$ is closed in $B_n \times \mathbb{R}$. The space $\mathrm{USC}(B_n)$ of all upper semicontinuous functions on B_n carries a natural topology by declaring two elements to be close if their subgraphs are close in the Hausdorff metric on closed subsets of $B_n \times \mathbb{R}$ (see [3] for details).

Question 9.3: Is the map $\widehat{f} \to \exp[\mathsf{D}_f]$ from $\mathbb{C}^{B_n}$ to $\mathrm{USC}(B_n)$ continuous?

9.4. Nonprincipal actions. Decimation makes sense for every algebraic $\mathbb{Z}^d$-action (indeed for every algebraic action of a countable residually finite group). Suppose that $\mathfrak{a}$ is an ideal in $\mathbb{Z}[\mathbb{Z}^d]$, and let $X_{\mathfrak{a}}$ be the dual group of $\mathbb{Z}[\mathbb{Z}^d]/\mathfrak{a}$ as described in §6 with its associated algebraic $\mathbb{Z}^d$-action $\alpha_{\mathfrak{a}}$. The commutative algebra there shows that the Nth decimation $r_N(X_{\mathfrak{a}})$ is defined by the contracted ideal $\mathfrak{a} \cap \mathbb{Z}[N\mathbb{Z}^d]$. However, there is no obvious replacement for g_N to measure growth when $\mathfrak{a}$ is not principal,

Question 9.4: If $\mathfrak{a}$ is a nonprincipal ideal in $\mathbb{Z}[\mathbb{Z}^d]$, are there objects related to the contractions $\mathfrak{a} \cap \mathbb{Z}[N\mathbb{Z}^d]$ which can be normalized to converge to a limiting object?

If $\mathfrak{a}$ is not principal, then the $\mathbb{Z}^d$-shift action $\alpha_{\mathfrak{a}}$ on $X_{\mathfrak{a}}$ has zero entropy. However, by restricting the shift to iterates close to lower dimensional subspaces of $\mathbb{R}^d$ the action can have positive entropy [6, §6]. This suggests that Question 9.1 may be relevant here.

Examining concrete examples may shed some light on this question. These include the case of commuting toral automorphisms (see [21, §6] for many such examples), the $\mathbb{Z}^2$-action defined by multiplication by 2 and by 3 on $\mathbb{T}$ (corresponding to $\mathfrak{a} = \langle x - 2, y - 3 \rangle$), and the so-called space helmet example [13, Example 5.8] (corresponding to $\mathfrak{a} = \langle 1 + x + y, z - 2 \rangle$).

An important example of a different character is due to Ledrappier [23], which corresponds to the nonprincipal ideal $\langle 1+x+y, 2\rangle \subset \mathbb{Z}[\mathbb{Z}^2]$. This example has zero entropy as a $\mathbb{Z}^2$-action, but strictly positive entropy along every 1-dimensional subspace of $\mathbb{R}^2$ (see [6, Example 6.4] for the explicit description). Another curious feature of this example is decimation self-similarity. Because $(1+x+y)^{2^n} = 1+x^{2^n}+y^{2^n}$ when taken mod 2, the 2^nth decimation of the example, when rescaled by 2^n, is just the original action.

9.5. Computing entropy using decimations. In his elegant proof that Mahler measure is continuous in the coefficients of polynomials $f \in \mathbb{C}[\mathbb{Z}^d]$, Boyd [5] side-stepped delicate issues about logarithmic singularities of $\log|f|$ by instead computing decimations of f along powers of 2 using the Graeffe root-squaring algorithm. This enabled him to compute $\mathsf{M}(f)$ to any prescribed accuracy using only a finite number of arithmetic operations on the coefficients of f.

This suggests a new approach to computing the entropy of algebraic actions using decimations and contracted ideals.

To describe this approach, let $\mathfrak{a}$ be an ideal in $\mathbb{Z}[\mathbb{Z}^d]$, and $\alpha_{\mathfrak{a}}$ be its associated algebraic $\mathbb{Z}^d$-action. Define the **length** of $g \in \mathbb{Z}[\mathbb{Z}^d]$ to be

$$L(g) := \sum_{\mathbf{k}\in\mathbb{Z}^d} |\widehat{g}(\mathbf{k})|.$$

For a subset $\mathfrak{b}$ of $\mathbb{Z}[\mathbb{Z}^d]$ put $L(\mathfrak{b}) := \min\{L(g) \colon 0 \neq g \in \mathfrak{b}\}$. By convention we define $L(\{0\}) := \infty$. We define the **asymptotic length** $\lambda(\mathfrak{a})$ of the ideal $\mathfrak{a}$ by

$$\lambda(\mathfrak{a}) := \limsup_{N\to\infty} \frac{1}{N^d} \log L(\mathfrak{a} \cap \mathbb{Z}[N\mathbb{Z}^d]).$$

The following shows that for some principal ideals the asymptotic length equals the entropy of the associated action.

Proposition 9.5: *Suppose that $f \in \mathbb{Z}[\mathbb{Z}^d]$ is absolutely irreducible, adjusted, and has support that generates $\mathbb{Z}^d$. Then $\lambda(\langle f\rangle) = \mathsf{h}(\alpha_f)$.*

Proof. First note that by Theorem 8.12, $\langle f\rangle \cap \mathbb{Z}[N\mathbb{Z}^d] = \langle f_{\langle N\rangle}\rangle_{\mathbb{Z}[N\mathbb{Z}^d]}$. Choose B_0 so that $\operatorname{supp} f \subset \{-B_0, \dots, B_0\}^d$, and put $B = 2B_0+1$. By (5.3) applied to the case $\mathbf{u} = \mathbf{0}$, we see that

$$\mathsf{H}(f_{\langle N\rangle}) \leqslant 2^{dN^{d-1}B} \mathsf{M}(f)^{N^d},$$

and hence

$$L(f_{\langle N\rangle}) \leqslant (N^d B)^d 2^{dN^{d-1}B} \mathsf{M}(f)^{N^d}.$$

Thus

$$\begin{aligned}\frac{1}{N^d}\log L(\langle f\rangle \cap \mathbb{Z}[N\mathbb{Z}^d]) &\leqslant \frac{1}{N^d}\log L(f_{\langle N\rangle}) \\ &\leqslant \frac{d\log(N^d B) + dN^{d-1}B\log 2}{N^d} + \mathsf{m}(f),\end{aligned}$$

and so letting $N\to\infty$ we conclude that $\lambda(\langle f\rangle) \leqslant \mathsf{m}(f) = \mathsf{h}(\alpha_f)$.

To prove the reverse inequality, let $gf_{\langle N\rangle}$ be an arbitrary nonzero element in $\langle f\rangle \cap \mathbb{Z}[N\mathbb{Z}^d]$. Then $\mathsf{M}(g) \geqslant 1$. Furthermore, $\mathsf{M}(gf_{\langle N\rangle}) \leqslant L(gf_{\langle N\rangle})$ by (5.2). Hence

$$\mathsf{M}(f)^{N^d} = \mathsf{M}(f_{\langle N\rangle}) \leqslant \mathsf{M}(g)\mathsf{M}(f_{\langle N\rangle}) = \mathsf{M}(gf_{\langle N\rangle}) \leqslant L(gf_{\langle N\rangle}).$$

Thus

$$\mathsf{h}(\alpha_f) = \mathsf{m}(f) = \frac{1}{N^d}\log \mathsf{M}(f_{\langle N\rangle}) \leqslant \log L(gf_{\langle N\rangle}),$$

and so

$$\lambda(\langle f\rangle) \geqslant \liminf_{N\to\infty}\frac{1}{N^d}\log L(\langle f\rangle\cap\mathbb{Z}[N\mathbb{Z}^d]) \geqslant \mathsf{h}(\alpha_f). \qquad \blacksquare$$

Under the assumptions on f in the above result there is actually convergence to $\mathsf{h}(\alpha_f)$. However, convergence can fail if the exponents e_N in Theorem 8.12 are at least 2 infinitely often. To give a simple example, let $d=1$ and $f(x)=x^2-2$. If N is odd then $g_N(x) = x^{2N}-2^N$, while if N is even then $g_N(x)=x^N-2^{N/2}$. Thus $(1/N)\log L(\langle f\rangle\cap\mathbb{Z}[N\mathbb{Z}^d])$ converges to $\frac{1}{2}\log 2$ along even N and to $\log 2$ along odd N.

More seriously, Proposition 9.5 can fail when the support of f does not generate a finite-index subgroup of $\mathbb{Z}^d$. Take for instance $f=2$, so that $\lambda(\langle f\rangle)=0$ but $\mathsf{h}(\alpha_f)=\log 2$.

Question 9.6: What are necessary and sufficient conditions on $f\in\mathbb{Z}[\mathbb{Z}^d]$ so that $\lambda(\langle f\rangle) = \mathsf{h}(\alpha_f)$?

According to [24, Lem. 4.3], to compute the entropy of general algebraic $\mathbb{Z}^d$-actions it suffices to compute those defined by prime ideals. The case of principal prime ideals is part of Question 9.6. By [24, Thm. 4.2], if $\mathfrak{p}$ is a nonprincipal prime ideal in $\mathbb{Z}[\mathbb{Z}^d]$ then $\mathsf{h}(\alpha_{\mathfrak{p}})=0$.

Question 9.7: If $\mathfrak{p}$ is a nonprincipal prime ideal in $\mathbb{Z}[\mathbb{Z}^d]$, does $\lambda(\mathfrak{p})=0$?

This approach to entropy suggests a formulation for algebraic actions of (not necessarily commutative) residually finite groups. Let Γ be a countable discrete group. For each element f in the integral group ring $\mathbb{Z}[\Gamma]$ there is an associated principal algebraic Γ-action α_f dual to the standard left-action of Γ on $\mathbb{Z}[\Gamma]/\mathbb{Z}[\Gamma]f$. Assume now that Γ is residually finite, and let $\mathcal{H}$ denote the collection of all finite-index subgroups of Γ. We say that $H \to \infty$ in $\mathcal{H}$ if for every finite subset $K \subset \Gamma$ we have eventually $H \cap K \subset \{1_\Gamma\}$. The quotient maps $\Gamma \to \Gamma/H$ for $H \in \mathcal{H}$ provide sofic approximations to Γ for computing sofic entropy $h(\alpha_f)$ of α_f. There is an obvious extension of length L to this situation.

We confine our attention to those f which genuinely involve all of Γ. To do this, let $f \in \mathbb{Z}[\Gamma]$ have support $A = \operatorname{supp} f$. Say that f has **finite index** if $A^{-1}A := \{b^{-1}a : a, b \in A\}$ generates a finite-index subgroup of Γ. This property is invariant under left translation by elements of Γ.

Question 9.8: With the previous notations, does

$$\limsup_{H\to\infty} \frac{1}{|\Gamma/H|} \log L(\mathbb{Z}[\Gamma]f \cap \mathbb{Z}[H]) = h(\alpha_f)$$

for every finite-index $f \in \mathbb{Z}[\Gamma]$?

Appendix A. Computing the decimation limit of $1 + x + y$

There are few explicit calculations of the logarithmic Mahler measure, or more generally of the Ronkin function, of polynomials in $\mathbb{Z}[\mathbb{Z}^d]$ when $d \geqslant 2$. Depending on the relative sizes of the coefficients, evaluation of the integrals involved typically requires the torus to be subdivided into a large number of subregions with complicated boundaries, and so simple formulas in terms of familiar functions are rare.

Here we treat the case $f(x, y) = 1 + x + y$ from Example 2.4, where these calculations can be carried out, resulting in the formulas (2.4) and (2.5) for D_f.

Smyth [37] first computed the logarithmic Mahler measure $m(f) = R_f(0, 0)$ to have the value in (2.6). Twenty years later Maillot [30, §7.3], aided by Cassigne, computed the entire Ronkin function $R_f(u, v)$, providing in his long memoir a concrete example of the canonical height of a hypersurface. Their result involves the Bloch–Wigner dilogarithm function, which is an alternative formulation of the series representation in our formulas. Lundqvist [25] gave the formulas for the partial derivatives of R_f we use here. He also investigated the polynomial $1+x+y+z$, and showed that the second order partial derivatives of its Ronkin function can be expressed in terms of standard elliptic functions.

Let $\Delta = \mathcal{N}_f$ be the unit simplex, and denote its interior by Δ°. Let $\mathcal{A}_f$ be the amoeba of f, as shown in Figure 5, and $\mathcal{A}_f^\circ$ be its interior. To evaluate $R_f^*(r,s)$ for $(r,s) \in \Delta^\circ$, we need to know the value of $(u,v) \in \mathcal{A}_f^\circ$ at which the partial derivatives of $R_f(u,v)$ with respect to u and v equal r and s, respectively. Fortunately, there is a simple relationship that was established by Lundqvist [25], whose treatment we follow.

Lemma A.1: *Let $(u,v) \in \mathcal{A}_f^\circ$, so that 1, e^u, and e^v form the sides of a non-degenerate triangle. Let πr and πs be the angles in this triangle shown in Figure 7(a). Then*

$$\frac{\partial R_f}{\partial u}(u,v) = r \quad \text{and} \quad \frac{\partial R_f}{\partial v}(u,v) = s. \tag{A.1}$$

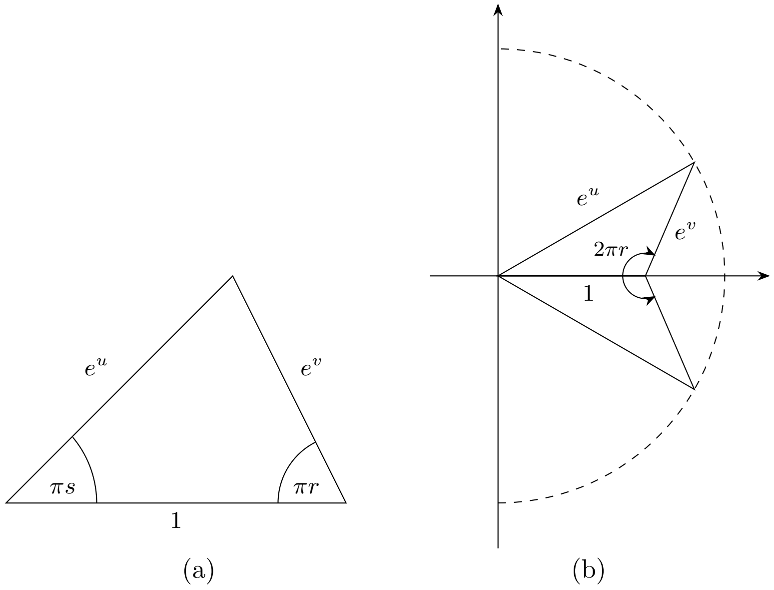


Figure 7. Determining partial derivatives from angles and sides.

Proof. We will compute the partial derivatives by differentiating the integrand in

$$\begin{aligned} R_f(u,v) &= \int_0^1 \int_0^1 \log|1 + e^u e^{2\pi i\theta} + e^v e^{2\pi i\phi}|\, d\theta\, d\phi \\ &= \mathrm{Re}\Big[\int_0^1 \int_0^1 \log(1 + e^u e^{2\pi i\theta} + e^v e^{2\pi i\phi})\, d\theta\, d\phi\Big]. \end{aligned}$$

In the last line log represents a local inverse to exp, which is well-defined up to the addition of an integral multiple of $2\pi i$. After taking partial derivatives, we will get a result that is independent of this multiple.

By symmetry, it suffices to compute $\partial R_f/\partial u$. Differentiating the integrand gives

$$\frac{\partial R_f}{\partial u}(u,v) = \mathrm{Re}\Big[\int_0^1 \int_0^1 \frac{e^u e^{2\pi i\theta}}{1 + e^u e^{2\pi i\theta} + e^v e^{2\pi i\phi}}\, d\theta\, d\phi\Big].$$

Rewriting the integrals as contour integrals, we see that

$$\begin{aligned} &\int_0^1 \int_0^1 \frac{e^u e^{2\pi i\theta}}{1 + e^u e^{2\pi i\theta} + e^v e^{2\pi i\phi}}\, d\theta\, d\phi \\ &\qquad = \frac{1}{(2\pi i)^2}\int_{|z|=e^u}\int_{|w|=e^v} \frac{1}{1+z+w}\, dz \frac{dw}{w} \\ &\qquad = \frac{1}{2\pi i}\int_{|w|=e^v}\Big[\frac{1}{2\pi i}\int_{|z|=e^u} \frac{dz}{z-(-1-w)}\Big]\frac{dw}{w}. \end{aligned}$$

The inner integral is the winding number of the circle of radius e^u around $-1-w = -1-e^v e^{2\pi i\phi}$, and so has value 1 if $|1+e^v e^{2\pi i\phi}| < e^u$ and 0 if $|1+e^v e^{2\pi i\phi}| > e^u$ (these are mistakenly reversed in [25]). A glance at Figure 7(b) shows that the value is 1 for an interval of ϕ of length $2\pi r$, and 0 otherwise. Since $(1/2\pi i)(dw/w)$ is normalized Lebesgue measure $d\phi$, we obtain that $(\partial R_f/\partial u)(u,v) = r$. ∎

To compute the decimation limit D_f, we need to express u and v in terms of r and s. Let $a = e^u$ and $b = e^v$ be the sides of the triangle in Figure 7(a). By the law of sines,

$$\frac{a}{\sin\pi r} = \frac{b}{\sin\pi s} = \frac{1}{\sin\pi(1-r-s)} = \frac{1}{\sin\pi(r+s)},$$

and hence

$$a = a(r,s) = e^{u(r,s)} = \frac{\sin \pi r}{\sin \pi(r+s)}, \tag{A.2}$$

$$b = b(r,s) = e^{v(r,s)} = \frac{\sin \pi s}{\sin \pi(r+s)}. \tag{A.3}$$

For $(u,v) \in \mathcal{A}_f^\circ$ it follows from the definition (3.1) that

$$-\mathsf{R}_f^*(u,v) = \inf_{(r,s)\in\Delta^\circ} \mathsf{R}_f(u,v) - ru - sv,$$

and by calculus the infimum is attained at the (u,v) given by (A.1). Thus for $(r,s) \in \Delta^\circ$ we have that

$$\mathsf{D}_f(r,s) = -\mathsf{R}_f^*(u(r,s),v(r,s)) = \mathsf{R}_f(u(r,s),v(r.s)) - r\,u(r,s) - s\,v(r,s), \tag{A.4}$$

where $u(r,s)$ and $v(r,s)$ are determined by (A.2) and (A.3).

Remark A.2: Observe that the functions $u(r,s)$ and $v(r,s)$ in (A.2) and (A.3) are real analytic on Δ°. Also, $\mathsf{R}_f(u,v)$ is real analytic on $\mathcal{A}_f^\circ$. Together these show that $\mathsf{D}_f(r,s)$ is real analytic on Δ°.

It remains to compute $\mathsf{R}_f(u,v)$. By symmetry it suffices to assume that $u \geqslant v$. Using Jensen's formula (2.1), we see that

$$\begin{aligned}\mathsf{R}_f(u,v) &= \int_0^1\int_0^1 \log|1 + e^u e^{2\pi i\theta} + e^v e^{2\pi i\phi}|\,d\theta\,d\phi \\ &= u + \int_0^1\int_0^1 \log|e^{-u} + e^{v-u}e^{2\pi i\phi} + e^{2\pi i\theta}|\,d\theta\,d\phi \\ &= u + \int_0^1 \log^+|e^{-u} + e^{v-u}e^{2\pi i\phi}|\,d\phi.\end{aligned}$$

Note that $|e^{-u} + e^{v-u}e^{2\pi i\phi}| \geqslant 1$ if and only if $|1 + e^v e^{2\pi i\phi}| \geqslant e^u$, and another glance at Figure 7(b) shows this occurs exactly when $-\pi(1-r) \leqslant 2\pi\phi \leqslant \pi(1-r)$. Hence

$$\begin{aligned}\mathsf{R}_f(u,v) &= u + \int_{-\frac12(1-r)}^{\frac12(1-r)} \log|e^{-u} + e^{v-u}e^{2\pi i\phi}|\,d\phi \\ &= u - (1-r)u + \int_{-\frac12(1-r)}^{\frac12(1-r)} \log|1 + e^v e^{2\pi i\phi}|\,d\phi \\ &= r\,u + \int_{-\frac12(1-r)}^{\frac12(1-r)} \log|1 + e^v e^{2\pi i\phi}|\,d\phi.\end{aligned}$$

First suppose that $e^v < 1$, which corresponds to $(r,s) \in \Delta_1^\circ$, where Δ_1 is defined in (2.2). The series expansion of $\log(1+z)$ for $1+z$ in the domain of integration converges uniformly, and the imaginary part vanishes by symmetry. Hence

$$\begin{aligned} \mathsf{R}_f(u,v) &= r\,u + \int_{-\frac{1}{2}(1-r)}^{\frac{1}{2}(1-r)} \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} e^{nv} e^{2\pi i n\phi}\, d\phi \\ &= r\,u + \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} e^{nv} \frac{1}{\pi n} \sin[\pi n(1-r)]. \end{aligned}$$

Recalling that $e^{v(r,s)} = b(r,s) = (\sin \pi s)/\sin[\pi(r+s)]$, we conclude that

$$\begin{aligned} \mathsf{D}_f(r,s) &= \mathsf{R}_f(u(r,s),v(r,s)) - r\,u(r,s) - s\,v(r,s) \\ &= \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{\pi n^2} b(r,s)^n \sin[\pi n(1-r)] - s\,\log[b(r,s)]. \end{aligned} \tag{A.5}$$

Now suppose that $e^v > 1$, which corresponds to $(r,s) \in \Delta_2^\circ$, where Δ_2 is defined by (2.3). Then $\log|1+e^v e^{2\pi i\phi}| = v + \log|1+e^{-v}e^{-2\pi i\phi}|$. Calculating as before,

$$\begin{aligned} \mathsf{R}_f(u,v) &= r\,u + (1-r)v + \int_{-\frac{1}{2}(1-r)}^{\frac{1}{2}(1-r)} \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} e^{-nv} e^{-2\pi i n\phi}\, d\phi \\ &= r\,u + (1-r)v + \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{\pi n^2} b(r,s)^{-n} \sin[\pi n(1-r)]. \end{aligned}$$

Thus for $(r,s) \in \Delta_2^\circ$ we find that

$$\mathsf{D}_f(r,s) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{\pi n^2} b(r,s)^{-n} \sin[\pi n(1-r)] + (1-r-s)\log[b(r,s)]. \tag{A.6}$$

Finally, note that on the overlap $\Delta_1 \cap \Delta_2$ inside Δ°, we have that $b(r,s) = 1$ and so the series in (2.2) and (2.3) converge and agree, hence give the value of $\mathsf{D}_f(r,s)$ by continuity of the Legendre transform.

References

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, MA.–London–Don Mills, ON, 1969.

[2] A. Baker, *Transcendental Number Theory*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 2022.

[3] G. Beer, *A natural topology for upper semicontinuous functions and a Baire category dual for convergence in measure*, Pacific Journal of Mathematics **96** (1981), 251–263.

[4] J. Berstel and M. Mignotte, *Deux propriétés décidables des suites récurrentes linéaires*, Bulletin de la Société Mathématique de France **104** (1976), 175–184.

[5] D. W. Boyd, *Uniform approximation to Mahler's measure in several variables*, Canadian Mathematical Bulletin **41** (1998), 125–128.

[6] M. Boyle and D. Lind, Expansive subdynamics, Transactions of the American Mathematical Society **349** (1997), 55–102.

[7] J. I. Burgos Gil, P. Philippon and M. Sombra, *Arithmetic geometry of toric varieties. Metrics, measures and heights*, Astérisque **360** (2014).

[8] J. W. S. Cassels, *Local Fields*, London Mathematical Society Student Texts, Vol. 3, Cambridge University Press, Cambridge, 1986.

[9] C. Chabauty, *Limite d'ensembles et géométrie des nombres*, Bulletin de la Société Mathématique de France **78** (1950), 143–151.

[10] K. Conrad, *Galois descent*, `https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisdescent.pdf`

[11] Y. Cornulier, *On the Chabauty space of locally compact abelian groups*, Algebraic & Geometric Topology **11** (2011), 2007–2035.

[12] D. Duval, *Absolute factorization of polynomials: a geometric approach*, SIAM Journal on Computing **20** (1991), 1–21.

[13] M. Einsiedler, D. Lind, R. Miles and T. Ward, *Expansive subdynamics for algebraic $\mathbb{Z}^d$-actions*, Ergodic Theory and Dynamical Systems **21** (2001), 1695–1729.

[14] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs, Vol. 104, American Mathematical Society, Providence, RI, 2003.

[15] S. Gao, *Absolute irreducibility of polynomials via Newton polytopes*, Journal of Algebra **237** (2001), 501–520.

[16] I. M. Gel′fand, M. M. Kapranov and A. V. Zelevinsky, *Discriminants, Resultants, and Multidimensional Determinants*, Modern Birkhäuser Classics, Birkhäuser. Boston, MA, 1994.

[17] A. O. Gelfond, *Transcendental and Algebraic Numbers*, Dover, New York, 1960.

[18] V. Gorin, *Lectures on Random Lozenge Tilings*, Cambridge Studies in Advanced Mathematics, Vol. 193, Cambridge University Press, Cambridge, 2021

[19] P. R. Halmos, *On automorphisms of compact groups*, American Mathematical Society. Bulletin, **49** (1943), 619–624.

[20] J. Hubbard and I. Pourezza, *The space of closed subgroups of $\mathbf{R}^2$*, Topology **18** (1979), 143–146.

[21] A. Katok, S. Katok and K. Schmidt, *Rigidity of measurable structure for $\mathbb{Z}^d$-actions by automorphisms of a torus*, Commentarii Mathematici Helvetici **77** (2002), 718–745.

[22] R. Kenyon, A. Okounkov and S. Sheffield, *Dimers and amoebae*, Annals of Mathematics **163** (2006), 1019–1056.

[23] F. Ledrappier, *Un champ markovien peut être d'entropie nulle et mélangeant*, Comptes Rendus de l'Académie des Sciences, Paris, Série A **287** (1978), A561–A563.

[24] D. Lind, K. Schmidt and T. Ward, *Mahler measure and entropy for commuting automorphisms of compact groups*, Inventiones Mathematicae **101** (1990), 593–629.

[25] J. Lundqvist, *An explicit calculation of the Ronkin function*, Annales de la Faculté des Sciences de Toulouse. Mathématiques. Série 6 **24** (2015), 227–250.

[26] D. Maclagan and B. Sturmfels, *Introduction to Tropical Geometry*, Graduate Studies in Mathematics, Vol. 161, American Mathematical Society, Providence, RI, 2015.

[27] A. Magidin and D. McKinnon, *Gauss's lemma for number fields*, American Mathematical Monthly **112** (2005), 385–416.

[28] K. Mahler, *On lattice points in n-dimensional star bodies. I. Existence theorems*, Proceedings of the Royal Society of London Series A **187** (1946), 151–187.

[29] K. Mahler, *On some inequalities for polynomials in several variables*, Journal of the London Mathematical Society **37** (1962), 341–344.

[30] V. Maillot, *Géométrie d'Arakelov des variétés toriques et fibrés en droites intégrables*, Mémoires de la Société Mathématique de France **80** (2000).

[31] A. Okounkov, *Limit shapes, real and imagined*, American Mathematical Society. Bulletin **53** (2016), 187–216.

[32] M. Passare and H. Rullgård, *Amoebas, Monge-Ampère measures, and triangulations of the Newton polytope*, Duke Mathematical Journal **121** (2004), 481–507.

[33] K. Purbhoo, *A Nullstellensatz for amoebas*, Duke Mathematical Journal **141** (2008), 407–445.

[34] R. T. Rockafellar, *Convex Analysis*, Princeton Mathematical Series, Vol. 28, Princeton University Press, Princeton, NJ, 1970.

[35] L. I. Ronkin, *On zeros of almost periodic functions generated by functions holomorphic in a multicircular domain*, in *Complex Analysis in Modern Mathematics*, FAZIS, Moscow, 2001, pp. 239–251.

[36] K. Schmidt, *Dynamical Systems of Algebraic Origin*, Progress in Mathematics, Vol. 128, Birkhäuser, Basel, 1995.

[37] C. J. Smyth, *On measures of polynomials in several variables*, Bulletin of the Australian Mathematical Society **23** (1981), 49–63.

[38] C. J. Smyth, *A Kronecker-type theorem for complex polynomials in several variables*, Canadian Mathematical Bulletin **24** (1981), 447–452.