A Dynamical Interpretation of the Global Canonical Height on an Elliptic Curve

Graham Everest and Thomas Ward

CONTENTS

1. Introduction
2. Mahler Measures Arise as Entropies
3. The Dynamical System Attached to a Polynomial
4. Arithmetic of Mahler's Measure
5. The Elliptic Mahler Measure
6. Elliptic Entropy
7. Counting Periodic Points
8. Conclusion
References

There is a well-understood connection between polynomials and certain simple algebraic dynamical systems. In this connection, the Mahler measure corresponds to the topological entropy, Kronecker's Theorem relates ergodicity to positivity of entropy, approximants to the Mahler measure are related to growth rates of periodic points, and Lehmer's problem is related to the existence of algebraic models for Bernoulli shifts. There are similar relationships for higher-dimensional algebraic dynamical systems.

We review this connection, and indicate a possible analogous connection between the global canonical height attached to points on elliptic curves and a possible 'elliptic' dynamical system.

1. INTRODUCTION

The simplest examples of dynamical systems are often those of algebraic origin. For such examples, it is unsurprising that almost every dynamical property can ultimately be related to a property of polynomials. In this paper we bring the polynomial into the foreground, and collect well-known results that show how to associate a dynamical system to a polynomial, and how the classical Mahler measure attached to the polynomial corresponds to the entropy of the dynamical system. Underlying everything in some sense is the compact group structure of the circle $\mathbb{S}^1$.

Recently, Everest and others have studied an analogous measure for polynomials where the underlying compact group is an elliptic curve. In an arithmetic situation, this can be seen as a generalisation of the global canonical height attached to a rational point. We conjecture that there is an analogous associated dynamical system whose

1991 Mathematics Subject Classification: 22D40, 11C08

Everest thanks the organisers of the York Number Theory and Dynamical Systems conference in September 1997 for the opportunity to present this work.

Ward gratefully acknowledges support from NSF grant No. DMS-94-01093 at the Ohio State University.

1058-6458/1998 $0.50 per page

entropy, suitably interpreted, corresponds to the elliptic Mahler measure.

Given the speculative nature of this work, we state results in rather restricted settings and prove them for the simplest possible case that displays the desired phenomena.

2. MAHLER MEASURES ARISE AS ENTROPIES

A *topological dynamical system* is a representation $\alpha : \mathbb{N}^d \to \mathrm{C}(X, \rho)$, where $\mathrm{C}(X, \rho)$ is the semigroup of continuous maps of the metric space (X, ρ) to itself. If each map in the image of α is a homeomorphism, then it is an *invertible* dynamical system, and α extends to a $\mathbb{Z}^d$-action

$$\alpha : \mathbb{Z}^d \to \mathrm{Homeo}(X, \rho).$$

The *topological entropy* of α is a measure of orbit complexity first introduced for compact X and $d = 1$ by Adler, Konheim and McAndrew [Adler et al. 1965]. The definition we give follows that given by Bowen [1971] for $d = 1$ and does not require compactness. In the compact case several equivalent definitions are given for $d > 1$ in Appendix A of [Lind et al. 1990].

Let $R(n) = [0, n-1]^d \cap \mathbb{Z}^d$ denote a d-dimensional cube of side n in $\mathbb{Z}^d$. A set $E \subset X$ is said to be *$(R(n), \varepsilon)$-separated under* α if for every pair $x \neq y$ in E there is an $\boldsymbol{n} \in R(n)$ with the property that $\rho(\alpha_{\boldsymbol{n}} x, \alpha_{\boldsymbol{n}} y) > \varepsilon$. For each compact set $K \subset X$, let

$$\begin{aligned} s_K(R(n), \varepsilon) &= \max\{|E| : E \subset K \text{ is} \\ &\qquad\qquad (R(n), \varepsilon)\text{-separated under } \alpha\}, \\ h_K(\alpha, \varepsilon) &= \limsup_{n\to\infty} \frac{1}{n^d} \log s_K(R(n), \varepsilon), \\ h_K(\alpha) &= \lim_{\varepsilon \searrow 0} h_K(\alpha, \varepsilon), \end{aligned}$$

and finally define the topological entropy of α to be

$$h(\alpha) = \sup_K h_K(\alpha). \tag{2–1}$$

Notice that $h_X(\alpha) = h(\alpha)$ if X is compact.

Theorem 2.1. [1] *If X is compact, $d = 1$, and α is invertible, then $h(\alpha) = h(\alpha^{-1})$. More generally, if α is a $\mathbb{Z}^d$-action and M is a $d \times d$ integer matrix with nonzero determinant, then $h(\beta) = |\det(M)| h(\alpha)$, where $\beta_{\boldsymbol{n}} = \alpha_{M\boldsymbol{n}}$.*

[2] *If X is a locally compact metrizable group with Haar measure μ, and α acts by continuous endomorphisms of X, then*

$$h(\alpha) = \lim_{\varepsilon\searrow 0} \limsup_{n\to\infty} -\frac{1}{n^d} \log \mu \Bigg(\bigcap_{\boldsymbol{n} \in R(n)} \alpha_{-\boldsymbol{n}} (B_\varepsilon(0)) \Bigg),$$

where $B_\varepsilon(0)$ is the metric open ball of radius ε around the identity in X.

Proof. The first part of [1] (where $d = 1$) follows from [Adler et al. 1965, Corollary to Theorem 2], and the second part follows by similar arguments (the analogue of [1] for measurable dynamics is in [Conze 1972/73, Section 6]); [2] may be proved using the ideas for the $d = 1$ case in [Bowen 1971, Section 2]. □

Example 2.2. [1] Let $X = \mathbb{T}$ (the additive circle) with the usual metric, and define α by $\alpha_1(x) = 2x$ (mod 1). Here $R(n) = \{0, 1, \dots, n-1\}$, and using Theorem 2.1 we see that

$$\bigcap_{j \in R(n)} \alpha_{-j}(B_\varepsilon(0)) = (-2^{-(n-1)}\varepsilon, +2^{-(n-1)}\varepsilon),$$

so $h(\alpha) = \log 2$.

[2] Let $X = \widehat{\mathbb{Z}[\frac{1}{ab}]}$, and define α to be the automorphism of the solenoid X dual to $x \mapsto \frac{a}{b}x$ on $\mathbb{Z}[\frac{1}{ab}]$ for coprime integers a, b. Then Abramov's formula [1959] shows that

$$h(\alpha) = \log \max\{|a|, |b|\}.$$

[3] Let X be a local field (for example, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_p$ or a completion of $\mathbb{F}_p(t)$) with valuation $|\cdot|$, and let $\alpha : X \to X$ be given by $\alpha(x) = \xi x$ for some $\xi \in X \backslash \{0\}$. Then a calculation similar to [1] shows that

$$h(\alpha) = \max\{0, \log \mathrm{mod}(\alpha)\},$$

where $\mathrm{mod}(\alpha)$ is the module of the automorphism α; see [Weil 1974, Chapter 1].

For example, $x \mapsto 2x$ on $\mathbb{C}$ has entropy $\log 4$, $x \mapsto \frac{1}{6}x$ on $\mathbb{Q}_3$ has entropy $\log 3$, $x \mapsto 2x$ on $\mathbb{Q}_2$ has entropy 0, and $x \mapsto tx$ has entropy $\log p$ on the completion $\mathbb{F}_p(t)_{t^{-1}}$.

Now let $F \in \mathbb{Z}[u]$ denote a primitive polynomial in one variable with factorisation over the complex numbers

$$F(u) = b\prod_i (u - \lambda_i).$$

The *Mahler measure of F*, denoted $m(F)$, is defined by

$$m(F) = \log|b| + \sum_i \log\max\{1, |\lambda_i|\}. \qquad (2\text{–}2)$$

The same definition could be given for any polynomial with complex coefficients but our bias is towards arithmetic results so we will stick to the integral case. A discussion of the Mahler measure for polynomials with coefficients in rings of integers in number fields can be found in [Einsiedler 1997].

Example 2.3. [1] If $F(u) = u - 2$ then $m(F) = \log 2$.

[2] Let $F(u) = bu - a$, where a and b are coprime integers. The definition in (2–2) gives

$$m(F) = \log|b| + \log\max\{1, |a/b|\}.$$

If $b > a$ then the second term contributes nothing and $m(F) = \log|b|$, while if $a \geq b$ then the second term contributes $\log|a/b| = \log|a| - \log|b|$. Thus the $\log|b|$ terms cancel and we have $m(F) = \log|a|$. In other words, $m(F)$ simplifies to

$$m(F) = \log\max\{|a|, |b|\}. \qquad (2\text{–}3)$$

Notice that the same expression arose in Example 2.2[2] above.

The reason $m(F)$ carries Mahler's name is the two papers [Mahler 1960; 1962]. Many fascinating properties of the measure (and its generalisations) have been discovered; we will review some of them in Section 4. We next indicate how the Mahler measure $m(F)$ arises as the entropy of a dynamical system attached in a natural way to the polynomial F. Since the construction and the relationship hold in several variables, we first indicate the higher-dimensional analogue of the Mahler measure (2–2). The route to this generalisation begins with a simple application of Jensen's formula which we call Mahler's Lemma; see [Mahler 1960]. Here (and elsewhere) we assume the polynomial is nonzero. To be consistent with the dynamical interpretation, we define $m(0)$ to be infinite.

Lemma 2.4. *For any $F \in \mathbb{C}[u]$,*

$$m(F) = \int_0^1 \log|F(e^{2\pi i\theta})|\, d\theta. \qquad (2\text{–}4)$$

Proof. This is an easy consequence of Jensen's formula,

$$\int_0^1 \log|e^{2\pi i\theta} - \lambda| = \log\max\{1, |\lambda|\}. \qquad \square$$

Definition 2.5. Let $F(\boldsymbol{u}) \in \mathbb{Z}[u_1, \dots, u_d]$ be a primitive polynomial in d commuting variables. The *Mahler measure* of F is defined by

$$m(F) = \int_0^1 \cdots \int_0^1 \log\bigl|F(e^{2\pi i\theta_1}, \dots, e^{2\pi i\theta_d})\bigr|\, d\theta_1 \dots d\theta_d. \qquad (2\text{–}5)$$

Notice that the definition is unambiguous since any variables that do not appear in F integrate out, and accords with (2–2) for $d = 1$ by Mahler's Lemma 2.4. Calculations involving (2–5) are not straightforward unless F has a dominant coefficient.

Example 2.6. [1] Let $F = s$, a constant. Then $m(F) = \log|s|$.

[2] Let $F(u_1, u_2) = 3 - u_1 - u_2$. Then by Jensen's formula,

$$m(3 - u_1 - u_2) = \max\{0,\, m(3 - u_1)\} = \log 3.$$

More general calculations in this direction appear in [Smyth 1981, Section 2].

[3] If the polynomial F has the property that singularities appear in the integral (2–5) — that is, if F

vanishes somewhere on the torus $(\mathbb{S}^1)^d$ — the calculation of $m(F)$ is much harder. For example,

$$m(1+u_1+u_2) = \frac{3\sqrt{3}}{4\pi}L(2,\chi_3),$$
$$m(1+u_1+u_2+u_3) = \frac{7}{2\pi^2}\zeta(3),$$

where $L(2,\chi_3) = \sum_{n=1}^{\infty}\left(\frac{n}{3}\right)\frac{1}{n^2}$, $\left(\frac{\cdot}{n}\right)$ denotes the quadratic character modulo 3, and ζ is the Riemann zeta function; see [Boyd 1981b; Smyth 1981].

Recent work by Boyd and Deninger gives a possible explanation of the appearance of L-functions in the explicit values of higher-dimensional Mahler measures; see [Boyd 1998; Deninger 1997].

In a similar vein, calculating the entropy of a $\mathbb{Z}^d$-action from first principles is more involved for $d > 1$, so we will give just two simple examples.

Example 2.7. [1] Let $X = \{0,1,\dots,s-1\}^{\mathbb{Z}^d}$, viewed as a compact abelian group with Haar measure μ. Define the shift $\mathbb{Z}^d$-action α on X by

$$(\alpha_{\boldsymbol{n}}(\boldsymbol{x}))_{\boldsymbol{m}} = x_{\boldsymbol{n}+\boldsymbol{m}}$$

for all $\boldsymbol{n},\boldsymbol{m} \in \mathbb{Z}^d$ and $\boldsymbol{x} = (x_{\boldsymbol{n}}) \in X$. A metric ball of radius ε around the identity in X is a set of the form

$$B_\varepsilon(0) = \{\boldsymbol{x} \in X : x_{\boldsymbol{n}} = 0 \ \forall\ \boldsymbol{n} \text{ with } \|\boldsymbol{n}\| \le R_\varepsilon\}$$

for some R_ε. Applying Theorem 2.1[2], we find that

$$\bigcap_{\boldsymbol{n}\in R(n)} \alpha_{\boldsymbol{n}}\left(B_\varepsilon(0)\right) = \{\boldsymbol{x} \in X : x_{\boldsymbol{n}} = 0 \text{ for all } \boldsymbol{n} \text{ with } \boldsymbol{n} = \boldsymbol{a}+\boldsymbol{b},\ \|\boldsymbol{a}\| \le R_\varepsilon,\ \boldsymbol{b} \in R(n)\}.$$

It follows that

$$\mu\biggl(\bigcap_{\boldsymbol{n}\in R(n)} \alpha_{\boldsymbol{n}}\left(B_\varepsilon(0)\right)\biggr) = s^{-n^d - |\{\boldsymbol{a}\,:\,\|\boldsymbol{a}\|\le R_\varepsilon\}|},$$

and so $h(\alpha) = \log|s|$.

[2] Let $X = \mathbb{T}^{\mathbb{Z}}$, again viewed as a compact abelian group with Haar measure μ. Define a $\mathbb{Z}^2$-action α on X by

$$\alpha_{(a,b)}(\boldsymbol{x})_k = 2^b x_{k+a} \bmod 1$$

for all $a,b,k \in \mathbb{Z}$ and $\boldsymbol{x} = (x_n) \in X$. A metric on X compatible with its natural topology is given by

$$\rho(\boldsymbol{x},\boldsymbol{y}) = \sum_{a\in\mathbb{Z}} 2^{-|a|}|x_a - y_a|.$$

It follows that

$$\mu\biggl(\bigcap_{(a,b)\in R(n)} \alpha_{(a,b)}\left(B_\varepsilon(0)\right)\biggr) \approx (2^{-n}\varepsilon)^n,$$

so $h(\alpha) = \log 2$. Examples of this kind have been studied in the measurable dynamics framework by Conze [1972/73, Section 2, Example 3], who calculated their measurable entropy.

3. THE DYNAMICAL SYSTEM ATTACHED TO A POLYNOMIAL

We now describe how an element of $\mathbb{Z}[u_1,\dots,u_d]$ determines a $\mathbb{Z}^d$-dynamical system (in the sense of Section 2). This follows exactly the work of Schmidt and others in algebraic dynamical systems: see [Kitchens and Schmidt 1989; Lind et al. 1990; Einsiedler and Ward 1997; Lawton 1973; Schmidt 1995].

First recall that $\mathbb{T}^{\mathbb{Z}^d}$ is the dual (character) group of $\mathbb{Z}[u_1,\dots,u_d]$ with the pairing

$$\langle\,\cdot\,,\cdot\,\rangle : \mathbb{Z}[u_1,\dots,u_d] \times \mathbb{T}^{\mathbb{Z}^d} \to \mathbb{S}^1$$

defined by

$$\Bigl\langle \sum c_{\boldsymbol{n}}\boldsymbol{u}^{\boldsymbol{n}}, \boldsymbol{x}\Bigr\rangle = \exp\Bigl(2\pi i \sum c_{\boldsymbol{n}} x_{\boldsymbol{n}}\Bigr),$$

where $\boldsymbol{u}^{\boldsymbol{n}} = u_1^{n_1}\dots u_d^{n_d}$.

Definition 3.1. Let $F \in \mathbb{Z}[u_1,\dots,u_d]$ be a primitive polynomial. The $\mathbb{Z}^d$-action α^F associated to F is the shift action

$$\alpha^F_{\boldsymbol{n}}(\boldsymbol{x})_{\boldsymbol{m}} = x_{\boldsymbol{n}+\boldsymbol{m}}$$

on the closed, shift-invariant subgroup

$$\begin{aligned} X &= X_F \\ &= \{\boldsymbol{x} \in \mathbb{T}^{\mathbb{Z}^d} : \langle \boldsymbol{u}^{\boldsymbol{n}} F(\boldsymbol{u}), \boldsymbol{x}\rangle = 1 \text{ for all } \boldsymbol{n} \in \mathbb{Z}^d\}.\end{aligned}$$

The basic connection between the Mahler measure and dynamical systems is the following theorem.

Theorem 3.2. *The topological entropy of the dynamical system associated to a polynomial F is the polynomial's Mahler measure*: $h(\alpha^F) = m(F)$.

Proof. See [Lind et al. 1990, Theorem 3.1]. □

Example 3.3. [1] Taking $F(u) = u - 2$ gives the group $X_F = \widehat{\mathbb{Z}[\frac{1}{2}]}$, and the map α^F is the natural invertible extension of Example 2.2[1].

[2] Taking $F(u) = bu - a$ gives the group $X_F = \widehat{\mathbb{Z}[\frac{1}{ab}]}$, with α^F the automorphism dual to $x \mapsto \frac{a}{b}x$ on $\mathbb{Z}[\frac{1}{ab}]$. The Mahler measure is given by (2–2) and the entropy by Abramov's formula in Example 2.2[2].

[3] If $F = s$, a constant, then the group X_F is $\{0, 1, \ldots, s-1\}^{\mathbb{Z}^d}$, and α^F is the full d-dimensional shift with entropy $\log |s|$.

[4] If $F = 1 + u_1 + u_2$, the group X_F is

$$X_F = \{\boldsymbol{x} \in \mathbb{T}^{\mathbb{Z}^2} : x_{(a,b)} + x_{(a+1,b)} + x_{(a,b+1)} \equiv 0 \pmod 1 \\ \text{for all } (a, b) \in \mathbb{Z}^2\},$$

and the shift α^F has entropy given by Example 2.6[3].

A modern proof of Abramov's formula is given in [Lind and Ward 1988] using adelic methods. Briefly, the compact group $X_F = \widehat{\mathbb{Z}[\frac{1}{ab}]}$ arises as a quotient of the topological ring $\widetilde{X}_F = \mathbb{R} \times \prod_{p|ab} \mathbb{Q}_p$ by a discrete subgroup isomorphic to $\mathbb{Z}[\frac{1}{ab}]$. The automorphism α^F lifts to an automorphism $\tilde{\alpha}^F$ of $\widetilde{X}_F$ which is simply the direct product of the automorphisms $x \mapsto \frac{a}{b}x$ on each of the (finitely many) local fields $\mathbb{R}$ and $\mathbb{Q}_p$ for $p|ab$.

The dynamics of the local covering maps are very simple to describe: on $\mathbb{R}$, $\times\frac{a}{b}$ is a dilation scaling distances by $|\frac{a}{b}|$ if $|\frac{a}{b}| \geq 1$, and is a contraction (zero entropy) if $|\frac{a}{b}| < 1$. On each finite place p dividing a, $\times\frac{a}{b}$ is a contraction (zero entropy). Finally, on each of the finite places $\mathbb{Q}_p$ with p dividing b, $\times\frac{a}{b}$ is a dilation scaling distances by $|b|_p^{-1}$.

General considerations show that

$$h(\alpha^F) = h(\tilde{\alpha}^F),$$

and the right hand side is then simply a finite sum of expressions of the form described in Example 2.2[3]. Abramov's formula then naturally takes the form

$$h(\alpha^F) = \sum_{p \in \{p|ab\} \cup \{\infty\}} \log^+ |\tfrac{a}{b}|_p = \textstyle\sum_{p \leq \infty} \log^+ |\frac{a}{b}|_p,$$

where the last equality holds since the finite places with $p \not| ab$ contribute nothing to the sum.

More generally, the dynamical system associated to a polynomial $F(u)$ is an automorphism of a solenoid of the form described in [Kitchens and Schmidt 1989; Lawton 1973]. The adelic covering space method of [Lind and Ward 1988] shows that the resulting entropy is given by Yuzvinskii's formula,

$$h(\alpha^F) = m(F) = \sum_{p \leq \infty} \sum_{\{\lambda_{i,p}\}} |\lambda_{i,p}|_p, \tag{3–1}$$

where $\{\lambda_{i,p}\}$ are the roots of $F(u) = 0$ in a finite extension of $\mathbb{Q}_p$. Comparing (2–2) with (3–1) and using the product formula shows that the sum over the finite (nonarchimedean) places contributes the $\log |b|$ term to (2–2). It is interesting to compare this observation with the proof of Lemma 4.6.

4. ARITHMETIC OF MAHLER'S MEASURE

We start by recording a simple lemma, a restatement of Kronecker's Theorem which says that an algebraic integer whose conjugates are all equal to 1 in modulus must be a root of unity. First recall the definition of a *cyclotomic polynomial.* This is the term used to describe a primitive polynomial in $\mathbb{Z}[u]$, all of whose roots are algebraic roots of unity. The term cyclotomic means literally 'circle dividing' and refers to the way the roots of unity divide up the unit circle in the complex plane. A cyclotomic polynomial must divide $u^N - 1$ for some N. It follows that it must be monic and therefore roots of unity are algebraic integers.

Lemma 4.1. *Suppose that $F \in \mathbb{Z}[u]$ is a primitive polynomial. Then $m(F) = 0$ if and only if F is a* *monomial times a product of cyclotomic polynomials in monomials.*

Proof. Clearly a polynomial of this form has zero measure because it is monic and all its roots have absolute value 1. Conversely, a polynomial with zero measure must be monic. Thus its roots must be zero or algebraic integers all having absolute value 1 and Kronecker's Theorem says they must in fact be algebraic roots of unity. □

In view of the fact that $m(F)$ is an entropy, this lemma may be interpreted as a statement about the entropy of certain measure preserving transformations: α^F has positive entropy whenever F is not a product of cyclotomics.

Mahler's measure was really discovered by D. H. Lehmer, one of the great mathematical experimentalists, nearly thirty years before the work of Mahler [Lehmer 1933]. Lehmer was able to manufacture some 'large' primes from monic polynomials $F(u) \in \mathbb{Z}[u]$ provided the growth rate of a sequence attached to F was not too great. In our language, the sequence is the number of periodic points and the growth rate is Mahler's measure (see Section 7 for more details). Realising Lemma 4.1 above, he asked whether it might be possible that the nonzero measures are uniformly bounded below by a positive constant and mentioned that he could not find a smaller nonzero measure than that of the polynomial

$$u^{10} + u^9 - u^7 - u^6 - u^5 - u^4 - u^3 + u + 1. \quad (4\text{–}1)$$

That is still the position today! Proving that there is a smallest positive measure has become known as Lehmer's problem. Extensive calculations have been made and no smaller positive measure has been found. However, one must set beside this the fact that, even if one is convinced that $(0, \pm 1)$-coefficient polynomials will yield the smallest measures, there are still a lot of them to check for fixed (large) degree. A very elegant positive answer in a special case was provided by Smyth [1971].

A natural question is whether the analogue of Lehmer's problem holds for polynomials in several variables. The next theorem is stated in the special case where $d = 2$ for brevity. Let $F \in \mathbb{Z}[u_1, u_2]$ denote a polynomial. For general polynomials F (in which the integrand in (2–5) has singularities) it is not clear what the limiting behaviour of the measures $m(F(u, u^N))$ of one-variable polynomials has to do with the two-variable $m(F)$. Nonetheless, Boyd and Lawton have shown the following.

Theorem 4.2.

$$\lim_{N\to\infty} m(F(u, u^N)) = m(F(u_1, u_2)).$$

Proof. See [Boyd 1981b; Lawton 1983]. □

A similar result holds for suitably defined one-variable polynomials built using polynomials in several variables. It follows that gaps in the range of the one-variable measure will be inherited by the many-variable measures. Boyd [1981b] wrote a fascinating paper exploring this in a far-reaching way.

It is easy to construct polynomials in several variables with vanishing measure. Any monomial times a product of cyclotomic polynomials in monomials will obviously have zero measure, by Jensen's Formula. Conversely, there is the following generalization of Lemma 4.1. It is technically easier to state this if we work with Laurent polynomials, that is, polynomials in $u_1^{\pm 1}, \dots, u_d^{\pm 1}$. We say a polynomial is generalised cyclotomic if it is a product of cyclotomic polynomials in monomials.

Theorem 4.3. *If $F \in \mathbb{Z}[u_1^{\pm 1}, \dots, u_d^{\pm 1}]$ is a primitive polynomial then $m(F) = 0$ if and only if F is a monomial times a generalised cyclotomic polynomial.*

Proof. This can be found in [Boyd 1981a; Lawton 1977; Smyth 1981]. □

Our final result is really much simpler but is conceptually important. We have seen that for a polynomial in one variable, Mahler's measure arises as the entropy of an automorphism of an adelic space. It was clear during the calculation of the measure that contributions to the measure really were coming from local entropies. It will help us, when searching for elliptic analogues, to make this precise.

Notice first of all that we can realise the integral formula in (2–4) as a limit in the following way.

Lemma 4.4. *Let λ denote any algebraic number. For each $N \in \mathbb{N}$, let ζ run through the N-th roots of unity. Then*

$$m(u-\lambda) = \lim_{N\to\infty} \frac{1}{N} \sum_{\zeta^N=1} \log|\zeta-\lambda|. \tag{4–2}$$

Proof. Note that we take it as assumed that any undefined terms in (4–2) (such as when $\zeta = \lambda$) are omitted. The limit looks straightforward except for problems which might arise if $|\lambda| = 1$. In that case we can put a ball of radius ε around λ. To get the limit shown, we need to guarantee that ε can be chosen to vary with N in a harmless way. Baker's Theorem does guarantee this because it gives the following inequality,

$$|\zeta-\lambda| > AN^{-B}, \tag{4–3}$$

for all ζ with $\zeta^N = 1$, provided the left hand side of (4–3) is nonzero, where A and B are positive constants depending only upon λ. Thus the contribution to the integral arising from the ε-ball is $O(\log N/N)$ which vanishes in the limit. □

Expressions of the form (4–2), summing over vectors of unit roots, converge to the Mahler measure in the higher-dimensional case if the integrand has no singularities, but in general the higher-dimensional analogue of (4–2) is not known to hold.

Now suppose that, for each prime p, we adjoin to $\mathbb{Q}_p$ the roots of F and the N-th roots of unity. The p-adic value extends to this field and we will keep the same notation to denote this extension. Then define, for each λ_i with $F(\lambda_i) = 0$,

$$m_{\mathbb{T}_p}(x-\lambda_i) = \lim_{N\to\infty} \frac{1}{N} \sum_{\zeta^N=1} \log|\zeta-\lambda_i|_p.$$

The next lemma may be thought of as a p-adic version of Jensen's formula.

Lemma 4.5. *We have*

$$m_{\mathbb{T}_p}(x-\lambda_i) = \log\max\{1, |\lambda_i|_p\}. \tag{4–4}$$

Proof. The proof goes over word for word as above, using the p-adic version of Baker's Theorem. □

Notice how this all makes sense even if $p|\infty$. We can define a 'local-to-global' measure by taking

$$\sum_i \sum_p m_{\mathbb{T}_p}(x-\lambda_i). \tag{4–5}$$

Lemma 4.6. *The measure in* (4–5) *is equal to* $m(F)$.

Proof. What is happening here is that the total contribution from the finite (or nonarchimedean) primes is $-\sum_p \log|b|_p$. By the product formula, this is precisely $\log|b|$. This accounts for the first term on the right of (2–2). The remaining terms appear as the total contribution from the archimedean primes. □

This simple lemma allows us to interpret each of the local components of $m(F)$ as local entropies as in the discussion after Example 3.3. The space $\widetilde{X}_F$ is replaced by a product of completions of the field generated by the $\{\lambda_i\}$. For more details, see [Lind and Ward 1988]. Later on, in the elliptic case, we will be groping in the dark to try to realise elliptic analogues of these statements. It will be useful to be able to look at this particular aspect of the toral case.

The last remark in this section concerns the connection between Lehmer's problem and the measurable structure of the dynamical system α^F.

Theorem 4.7. *Let $F \in \mathbb{Z}[u_1, \dots, u_d]$ be an irreducible polynomial. Then the $\mathbb{Z}^d$-action α^F on X_F is measurably isomorphic to a d-dimensional Bernoulli shift with entropy $h(\alpha^F)$ if and only if $h(\alpha^F) > 0$.*

Proof. This is proved in [Rudolph and Schmidt 1995]. □

What this means is that there are certain abstract measure-theoretic model dynamical systems (the Bernoulli shifts), and these occur with all possible entropies. Lehmer's problem therefore becomes a question about dynamical systems: is there an algebraic system isomorphic to any Bernoulli shift, or must the Bernoulli shift have constrained entropy? For a fuller discussion of this question, see [Lind et al. 1990] and references there.

5. THE ELLIPTIC MAHLER MEASURE

Suppose now that E denotes a complex elliptic curve (for full definitions in this and the remaining sections, see [Silverman 1986]). Then the complex points of E are parametrised by transcendental functions, just as the points of the circle are parametrised by the exponential function. Precisely, there is a lattice L in $\mathbb{C}$ with associated Weierstrass $\wp$-function $\wp_L(z)$ defined by

$$\wp_L(z) = \frac{1}{z^2} + \sum_{0\neq \ell\in L}\left(\frac{1}{(z-\ell)^2} - \frac{1}{\ell^2}\right) \tag{5–1}$$

for $z \notin L$. It can be shown that the series in (5–1) is absolutely convergent for $z \notin L$, that it is a meromorphic function with double poles only at points in L, that $\wp_L(z)$ and its derivative $\wp'_L(z)$ are periodic with respect to L and, finally, that the algebraic differential equation

$$\tfrac{1}{4}\wp'_L(z)^2 = \wp_l(z)^3 + A\wp_L(z) + B \tag{5–2}$$

is satisfied for all $z \notin L$. In (5–2), A and B denote complex numbers. Thus the pairs $(\wp_L(z), \frac{1}{2}\wp'_L(z))$ for $z \in \mathbb{C}/L$ parametrise the complex points on the cubic curve with equation

$$y^2 = x^3 + Ax + B. \tag{5–3}$$

It can be shown that this curve is nonsingular and, moreover, given any nonsingular curve of the type in (5–3), we can find a lattice L so that the curve is parametrised as above.

In view of this, it might seem appropriate to define an elliptic Mahler measure by

$$m_E(F) = \int_{z\in\mathbb{C}/L} \log|F(\wp_L(z))|\,dz. \tag{5–4}$$

In (5–4), dz denotes the area measure on the fundamental parallelogram for $\mathbb{C}/L$, that is, the usual Lebesgue measure normalised to give area 1 to the parallelogram. It is true that some kind of elliptic theory could be developed in that way, but it would certainly lack the sophistication we require. For example, we wish at least that the coefficients A and B be rational. Even then, this global approach turns out not to have the right kind of functoriality properties. For example, we need to impose extra conditions upon F to ensure it satisfies Kronecker's Theorem. A full discussion is presented in [Everest 1999].

In order to obtain a properly functorial elliptic Mahler measure, we need to give a local-to-global approach. This will exactly mirror the approach to Mahler's measure we gave in Section 4. Our aim is to recognise the local factors of the elliptic Mahler measure as local entropies. We are successful for almost all of the factors, and for those factors where we are frustrated, we can begin to see why there are difficulties.

For each p, define the local curve E_p comprising all points with coordinates in $\mathbb{Q}_p$ (this makes sense if $A, B \in \mathbb{Q}$). This curve forms a compact group with Haar measure denoted μ_p. Define

$$m_{E_p}(F) = \int_{E_p} \log|F|_p\,d\mu_p. \tag{5–5}$$

Now we can add up the local measures to obtain a global measure

$$m_E(F) = \sum_p m_{E_p}(F). \tag{5–6}$$

For each root λ_i of F, we have a point on the (complex) curve $P_i = (\lambda_i, *\,)$.

Theorem 5.1. *For a primitive polynomial $F \in \mathbb{Z}[u]$, $m_E(F) = 0$ if and only if all the P_i are torsion points on E.*

This is the analogue of Kronecker's Theorem (see Lemma 4.1), and is proved in [Everest 1999]. It is useful to have an even more down to earth version of the definitions. For each i, we could adjoin λ_i

to $\mathbb{Q}_p$ then define

$$m_{E_p}(u-\lambda_i) = \int_{E_p} \log|u-\lambda_i|_p \, d\mu_p.$$

In [Everest 1999], it was shown that

$$m_E(F) = \sum_i \sum_p m_{E_p}(u-\lambda_i).$$

Note the exact comparison with the toral counterpart in (4–5). Our development of the elliptic Mahler measure is a generalisation of the canonical height attached to rational points on elliptic curves. The heart of the matter is to be found in [Everest and Fhlathúin 1996], where an integral representation for the local canonical heights was exploited. For a linear polynomial $F(u) = bu - a$, with a and b coprime integers, we have the relation $m_E(F) = 2\hat{h}(P)$, where $P = (a/b, *)$ and $\hat{h}$ denotes the global canonical height: see [Everest 1999]. Thus any dynamical interpretation of the elliptic Mahler measure will necessarily entail an interpretation of the global canonical height.

6. ELLIPTIC ENTROPY

We conjecture that the elliptic Mahler measure defined in Section 5 arises in a natural way as an entropy. Having restricted ourselves to this arithmetic version we are looking for arithmetic dynamical systems. Our feeling that we really do have an adelic space to act upon comes from the following lemma, which is an elliptic analogue of Jensen's Formula. Suppose λ is a rational number, with $P = (\lambda, *)$ denoting the corresponding point on the elliptic curve. Let p denote any prime of $\mathbb{Q}$ (possibly infinity). In [Everest 1999] an intimate relation between the local elliptic Mahler measure $m_{E_p}(u-\lambda)$ and the local canonical height of the point P at p was found. In special cases, this exactly mirrors the toral case.

Lemma 6.1. *Suppose p is a prime of good reduction for E. Then*

$$m_{E_p}(u-\lambda) = \log\max\{1, |\lambda|_p\}. \qquad (6\text{–}1)$$

Proof. This is formula (2.11) in [Everest 1999]. □

To an extent then, we can justify our conjecture about the existence of elliptic entropy. At the good nonarchimedean primes, we could let the point P act by multiplication of its x-coordinate on $\mathbb{Q}_p$. But this is all we did in the toral case and it cannot represent the whole story.

Things are more interesting at the archimedean primes and at the primes of (split multiplicative) bad reduction. If we take the simple action as before we actually get the 'wrong' answer. Coincidentally, it happens that the 'analysis' of elliptic curves is essentially the same at these two types of primes. So let K denote a local field which is the completion of $\mathbb{Q}$ at infinity or at a prime of bad split multiplicative reduction corresponding to the absolute value $|\cdot| = |\cdot|_p$ (note that, by extending the field of definition, we can always assume the reduction is of this type).

Theorem 6.2. [1] *There is an element q of K with $|q| < 1$ such that*

$$E(K) \simeq K^*/q^{\mathbb{Z}}.$$

[2] *Let $t \in K^*/q^{\mathbb{Z}}$ correspond to $P = (\lambda, *)$ under the isomorphism in* [1]. *Let $B_2(x) = x^2 - x + 1/6$ denote the second Bernoulli polynomial. Then*

$$m_{E_p}(u-\lambda) = \\ -\log\left| q^{(1/2)B_2\left(\frac{\log|t|}{\log|q|}\right)} (1-t) \prod_{n=1}^{\infty} (1-q^n t)(1-q^n t^{-1}) \right|. \qquad (6\text{–}2)$$

Proof. It follows from [Everest and Fhlathúin 1996] that the left hand side of (6–2) is the local canonical height of the point P. The formula (6–2) can be found in [Silverman 1994, pp. 468 and 473]. □

We are therefore predicting that there is an action of the point P upon a certain 'adelic' space with these properties:

(i) At the primes of good reduction, the space is isomorphic to $\mathbb{Q}_p$.

(ii) At archimedean primes and primes of bad reduction the point acts upon a local space in such a way that the entropy is given by the formula in (6–2).

7. COUNTING PERIODIC POINTS

In this section, we will consider the relationship between entropy and the periodic points of an action. In the toral case this is well understood. We will go on to discuss a potential elliptic analogue. Our claim is basically this: although we do not yet know what the action should be in the elliptic case, we do predict the periodic behaviour. See [Chothi et al. 1997] for a discussion of periodic point behaviour in a class of arithmetic dynamical systems.

For simplicity, we begin by letting a denote a positive integer with $F(u) = u - a$ the corresponding linear polynomial. Now α^F acts on $X_F = \widehat{\mathbb{Z}[\frac{1}{a}]}$ via the map dual to $x \mapsto ax$. The number of points of period $n \in \mathbb{N}$ is given by $F_n = a^n - 1 = x^n - 1|_{x=a}$. Let $\varphi_n(x) = x^n - 1$ and consider the expression

$$\frac{1}{n}\log|\varphi_n(a)|. \tag{7–1}$$

Let $F \in \mathbb{Z}[u]$ be monic, with A_F the companion matrix associated to F. We assume below that F has no zeros which are unit roots (this is equivalent to assuming that α^F is ergodic). If F has degree r then α^F acts on $X_F \sim \mathbb{T}^r$ in the natural linear way. Now F_n, the number of points of period n is given by $|\det(A_F^n - I_r)|$. If the roots of $F = 0$ (the eigenvalues of A_F) are listed with multiplicity as $\lambda_1, \dots, \lambda_r$ then we can express this number as

$$F_n = |(\lambda_1^n - 1)\dots(\lambda_r^n - 1)| = \prod_{i=1}^{r} |\varphi_n(\lambda_i)|. \tag{7–2}$$

It was this sequence F_n that Lehmer studied in [1933]. These numbers (all in $\mathbb{N}$) are generalizations of the Mersenne numbers arising from $F(u) = u - 2$. The growth rate is measured by the quantity $\frac{1}{n}\log F_n$. Taking $\frac{1}{n}\log F_n$ in the limit we get the following result (see [Lind 1982] for more details about this kind of dynamical system).

Lemma 7.1. *The limit of* $\frac{1}{n}\log F_n$ *exists as* $n \to \infty$ *and equals* $m(F)$.

Proof. This is obvious if $|\lambda_i| \neq 1$, the only cases Lehmer could handle. The potential difficulties lie with the case where $|\lambda_i| = 1$ for one or more i. However, just as in Lemma 4.4, Baker's Theorem comes to the rescue. It guarantees that

$$|\lambda_i^n - 1| > Cn^{-D}$$

for some $C, D > 0$. Therefore, in the limit, terms arising from $|\lambda_i| = 1$ contribute nothing. □

Now consider the elliptic case. Suppose that the curve E is given by a generalised Weierstrass equation (see [Silverman 1986]) with integer coefficients. Then for every $1 \le n \in \mathbb{N}$, there is a polynomial $\psi_n(x) \in \mathbb{Z}[x]$ with degree $n^2 - 1$ and leading coefficient n^2 whose roots are the x-coordinates of the (nonidentity) points of order dividing n on E. In the $d = 1$ case, let $E_n = |\psi_n(a)|$ and consider

$$\frac{1}{n^2}\log E_n. \tag{7–3}$$

Theorem 7.2. *Suppose that* $P = (a, *) \in E$ *has everywhere good reduction. Then the limit*

$$\lim_{n\to\infty} \frac{1}{n^2}\log E_n$$

exists and equals $m_E(u - a)$.

Proof. For an integral point with the good reduction condition, we know that the total contribution to m_E comes from the archimedean prime. Write the expression in (7–3) as

$$\frac{1}{n^2}\left(\log n^2 + \sum_{n\rho=O} \log|x(\rho) - a|\right), \tag{7–4}$$

where here the sum is over the points ρ which are not the identity O but have $n\rho = O$. Clearly the term $(\log n^2)/n^2$ contributes nothing in the limit. The limit over the n-th torsion points in (7–4) tends to the integral over the parallelogram. This is obvious (as in the toral case) except for the problem of points near to P. Write $\alpha \in \mathbb{C}/L$ with $\wp_L(\alpha) = a$. The elliptic analogue of Baker's Theorem says that $|\rho - \alpha| \gg n^{-D}$, when ρ is an n-th torsion point and a corresponds to an algebraic point on E. Therefore, just as before, the contribution to the Riemann sum is negligible for points close to a and thus the limit of (7–4) is equal to the integral giving the elliptic Mahler measure. □

A similar argument holds for monic $F \in \mathbb{Z}[u]$ with degree greater than 1.

In short, for $a \in \mathbb{N}$, we are claiming that an action can be found which has approximately $E_n = |\psi_n(a)|$ points of period n and with the property that

$$\lim_{n\to\infty} \frac{1}{n^2} \log E_n = m_E(u-a). \tag{7–5}$$

8. CONCLUSION

The connection between the arithmetic properties of the classical Mahler measure and algebraic dynamical systems is well-known. Recent work shows that an elliptic analogue of the classical Mahler measure has properties analogous to the Mahler measure, and there are indications that there is a corresponding 'elliptic' dynamical system whose entropy is related to the elliptic Mahler measure.

Table 1 summarizes our deliberations. For simplicity, assume that the polynomial is irreducible.

Mahler's measure	Elliptic Mahler measure
vanishing ⟷ torsion (Lemma 4.1)	vanishing ⟷ torsion (Theorem 5.1)
local–global principle (Lemma 4.6)	local–global principle (formula after Theorem 5.1)
growth rate of periodic points exists (Lemma 7.1)	growth rate of periodic points exists (Theorem 7.2)
local measure has a dynamical interpretation	in good reduction case (see comment after Lemma 6.1)
arises as an entropy (Theorem 3.2)	?
Lehmer's problem has a dynamical interpretation	?
ergodicity implies positive entropy	?
many variable measure	many variable measure
Kronecker in several variables (Theorem 4.3)	partial results (see [Everest 1999])
Lehmer's problem ⟷ algebraic models	see [Everest 1999] for discussion in elliptic case

TABLE 1. Correspondence of results for the Mahler measure and the elliptic Mahler measure (for irreducible polynomials).

REFERENCES

[Abramov 1959] L. M. Abramov, "The entropy of an automorphism of a solenoidal group", *Teor. Veroyatnost. i Primenen.* **4** (1959), 249–254. In Russian; translated in *Theor. Probability Appl.* **4** (1959), 231–236.

[Adler et al. 1965] R. L. Adler, A. G. Konheim, and M. H. McAndrew, "Topological entropy", *Trans. Amer. Math. Soc.* **114** (1965), 309–319.

[Bowen 1971] R. Bowen, "Entropy for group endomorphisms and homogeneous spaces", *Trans. Amer. Math. Soc.* **153** (1971), 401–414. Erratum in **181** (1973), 509–510.

[Boyd 1981a] D. W. Boyd, "Kronecker's theorem and Lehmer's problem for polynomials in several variables", *J. Number Theory* **13**:1 (1981), 116–121.

[Boyd 1981b] D. W. Boyd, "Speculations concerning the range of Mahler's measure", *Canad. Math. Bull.* **24**:4 (1981), 453–469.

[Boyd 1998] D. W. Boyd, "Mahler's measure and special values of L-functions", *Experiment. Math.* **7**:1 (1998), 37–82.

[Chothi et al. 1997] V. Chothi, G. Everest, and T. Ward, "S-integer dynamical systems: periodic points", *J. Reine Angew. Math.* **489** (1997), 99–132.

[Conze 1972/73] J. P. Conze, "Entropie d'un groupe abélien de transformations", *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **25** (1972/73), 11–30.

[Deninger 1997] C. Deninger, "Deligne periods of mixed motives, K-theory and the entropy of certain $\mathbb{Z}^n$-actions", *J. Amer. Math. Soc.* **10**:2 (1997), 259–281.

[Einsiedler 1997] M. Einsiedler, "A generalisation of Mahler measure and its application in algebraic dynamical systems", preprint, 1997.

[Einsiedler and Ward 1997] M. Einsiedler and T. Ward, "Fitting ideals for finitely presented algebraic dynamical systems", preprint, 1997.

[Everest 1999] G. R. Everest, "The elliptic analogue of Jensen's Formula", *J. London Math. Soc.* (1999). To appear.

[Everest and Fhlathúin 1996] G. R. Everest and B. N. Fhlathúin, "The elliptic Mahler measure", *Math. Proc. Cambridge Philos. Soc.* **120**:1 (1996), 13–25.

[Kitchens and Schmidt 1989] B. Kitchens and K. Schmidt, "Automorphisms of compact groups", *Ergodic Theory Dynamical Systems* **9**:4 (1989), 691–735.

[Lawton 1973] W. Lawton, "The structure of compact connected groups which admit an expansive automorphism", pp. 182–196 in *Recent advances in topological dynamics* (New Haven, Conn., 1972), edited by A. Beck, Lecture Notes in Math. **318**, Springer, Berlin, 1973.

[Lawton 1977] W. Lawton, "A generalization of a theorem of Kronecker", *J. Sci. Fac. Chiangmai Univ.* **4** (1977), 15–23.

[Lawton 1983] W. M. Lawton, "A problem of Boyd concerning geometric means of polynomials", *J. Number Theory* **16**:3 (1983), 356–362.

[Lehmer 1933] D. H. Lehmer, "Factorization of certain cyclotomic functions", *Ann. of Math.* (2) **34** (1933), 461–479.

[Lind 1982] D. A. Lind, "Dynamical properties of quasihyperbolic toral automorphisms", *Ergodic Theory Dynamical Systems* **2**:1 (1982), 49–68.

[Lind and Ward 1988] D. A. Lind and T. Ward, "Automorphisms of solenoids and p-adic entropy", *Ergodic Theory Dynamical Systems* **8**:3 (1988), 411–419.

[Lind et al. 1990] D. Lind, K. Schmidt, and T. Ward, "Mahler measure and entropy for commuting automorphisms of compact groups", *Invent. Math.* **101**:3 (1990), 593–629.

[Mahler 1960] K. Mahler, "An application of Jensen's formula to polynomials", *Mathematika* **7** (1960), 98–100.

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

[Rudolph and Schmidt 1995] D. J. Rudolph and K. Schmidt, "Almost block independence and Bernoullicity of $\mathbb{Z}^d$-actions by automorphisms of compact abelian groups", *Invent. Math.* **120**:3 (1995), 455–488.

[Schmidt 1995] K. Schmidt, *Dynamical systems of algebraic origin*, Progr. Math. **128**, Birkhäuser, Basel, 1995.

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math., Springer, New York, 1986.

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, New York, 1994.

[Smyth 1971] C. J. Smyth, "On the product of the conjugates outside the unit circle of an algebraic integer", *Bull. London Math. Soc.* **3** (1971), 169–175.

[Smyth 1981] C. J. Smyth, "A Kronecker-type theorem for complex polynomials in several variables", *Canad. Math. Bull.* **24**:4 (1981), 447–452. Addenda and errata in **25**:4 (1982), 504.

[Weil 1974] A. Weil, *Basic number theory*, 3rd ed., Grundlehren Math. Wiss. **144**, Springer, New York, 1974.

Graham Everest and Thomas Ward, School of Mathematics, University of East Anglia, Norwich NR4 7TJ, United Kingdom (g.everest@uea.ac.uk, t.ward@uea.ac.uk)

Received December 22, 1997; accepted February 11, 1998