ENTROPY AND THE CANONICAL HEIGHT

M. EINSIEDLER, G. EVEREST, AND T. WARD

Abstract. The height of an algebraic number in the sense of Diophantine geometry is a measure of arithmetic complexity. There is a well-known relationship between the entropy of automorphisms of solenoids and classical heights. We consider an elliptic analogue of this relationship, which involves two novel features. Firstly, the introduction of a notion of entropy for sequences of transformations. Secondly, the recognition of canonical local heights as integrals over the closure of the torsion subgroup of the curve (an elliptic Jensen formula).

A sequence of transformations is defined for which there is a canonical arithmetically defined quotient whose entropy is the canonical height, and in which the fibre entropy is accounted for by canonical local heights at primes of singular reduction, yielding a dynamical interpretation of singular reduction. This system is related to local systems, whose entropy coincides with the canonical local height up to sign. The proofs use transcendence theory, a strong form of Siegel's theorem, and an elliptic analogue of Jensen's formula.

1991 *Mathematics Subject Classification.* 11G07, 37B40.

The first author acknowledges the support of EPSRC postdoctoral award GR/M49588, the second thanks Jonathan Lubin and Joe Silverman for the AMS Sectional meeting on Arithmetic Dynamics at Providence, RI, 1999.

1. Introduction

Let Q denote a finite rational point of the projective line $\mathbb{P}^1$. If $Q = [q, 1]$ corresponds to the rational number $q = a/b$ where a and b are relatively prime integers, then Q has an associated Diophantine height $h(Q) = \log \max\{|a|, |b|\}$, a measure of the arithmetic complexity of Q. The height can be written using Jensen's formula as an integral,

$$h(Q) = \log \max\{|a|, |b|\} = \int_{\mathbb{T}} \log |bx - a| dm, \tag{1}$$

where $\mathbb{T}$ is the unit circle and m is Haar measure. Moreover, if $\phi_n(x) = x^n - 1$, the polynomial whose roots form the n-torsion subgroup of the unit circle, then (1) may be written (assuming that $a \neq \pm b$)

$$h(Q) = \lim_{n\to\infty} \frac{1}{n} \sum_{\xi:\phi_n(\xi)=0} \log |b\xi - a|. \tag{2}$$

On the other hand, the point Q has a naturally associated automorphism $T_Q : X_Q \to X_Q$, where T_Q is a continuous map on an underlying compact group X_Q known as a *solenoid* (defined later). The topological entropy of this dynamical system, an intrinsic invariant measuring orbit complexity, coincides with the Diophantine height $h(Q)$ of Q. The equation (2) is the Riemann sum approximation to an *integral over the closure of torsion points*. The number of elements of X_Q fixed by T_Q^n is $|b^n \phi_n(a/b)| = |b^n - a^n|$, which is related to the torsion points expression (2) by the identity

$$\sum_{\xi:\phi_n(\xi)=0} \log |b\xi - a| = \log |b^n - a^n|.$$

The main point of reference is the approach taken in [17], where the entropy is calculated by noting that the space X_Q is covered by the adeles and the dynamics lift nicely. The lifted map restricts to the local components, and the local entropies agree with the local projective heights. In this covering space, the periodic point data is destroyed however.

The arithmetic meaning of (1) and (2) has a direct analogue in which (roughly speaking) $\mathbb{T}$ is replaced by a complex elliptic curve, and the projective height is replaced by the global canonical height, which is known to decompose as a sum of canonical local heights. The cyclotomic division polynomials carrying knowledge of torsion in the circle are replaced by the elliptic division polynomials. Several attempts have been made to find the fourth corner of this square of ideas, namely a family of *elliptic dynamical systems*, whose topological entropy is given by the canonical height on the curve, and whose periodic point data is given by expressions involving the elliptic division polynomial (see [5], [11], [12]).

There are two main objectives in this paper. The first is to show how the viewpoint afforded by (1) and (2) in an elliptic setting gives new insights into the canonical height. The arithmetic dynamics of the automorphism T_Q gives concrete expression to the idea that the usual Diophantine height is a natural measure of complexity by identifying it with the topological entropy. The second objective is to show this has an elliptic analogue. To achieve this, the usual concept of a dynamical system is widened to include sequences of transformations which are not necessarily the iterates of a single transformation. Dynamical systems are constructed from rational points on elliptic curves which interpret the known arithmetic properties of heights. In particular, the analogous identification of the canonical height with a topological entropy (a measure of the growth in orbit complexity) is achieved. The results include a dynamical interpretation of the phenomenon of singular reduction. The maps constructed act on the adeles, just as in [17]; they are built from the duplication map on the underlying elliptic curve.

A technical issue that arises is that if the underlying space is compact this places severe restrictions upon the volume growth rates in the entropy calculations; thus the maps on the adeles are natural settings to find the characteristic quadratic-exponential growth rates familiar in elliptic curves.

The main result arrived at may be summarized as follows.

Theorem (see Section 6) *Let E denote an elliptic curve defined over $\mathbb{Q}$, and Q a rational point on E. Then Q generates a sequence of diagonal transformations $\mathbf{U}$ on the adeles with the following properties.*
1. If Q has non-singular reduction modulo p for all primes p then the entropy $h(\mathbf{U}) = \hat{h}(Q)$, the global canonical height of Q.
2. Let S denote the set of primes p for which Q has singular reduction modulo p; write $\mathbb{Q}_S = \prod_{p \in S} \mathbb{Q}_p$, and $\mathbf{U}_S$ for the restriction of $\mathbf{U}$ to $\mathbb{Q}_S$. Then the quotient entropy $h(\mathbf{U}/\mathbf{U}_S) = \hat{h}(Q)$.

Thus the sequences of maps constructed here give a direct connection between the canonical height on elliptic curves (and some of its ramifications, like singular reduction) and growth in orbit complexity of associated sequences of maps. The main results are in Sections 5 and 6, and these two sections may be read independently if standard material on elliptic curves and some material on entropy is assumed.

2. Background on heights and elliptic curves

Let E be an elliptic curve defined over the rationals, given by a generalized Weierstrass equation

$$y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6, \tag{3}$$

where $c_1, \dots, c_6 \in \mathbb{Z}$. For each rational prime p, there is a continuous function $\lambda_p : E(\mathbb{Q}_p)\backslash\{0\} \to \mathbb{R}$ which satisfies the *parallelogram law*

$$\lambda_p(Q + P) + \lambda_p(Q - P) = 2\lambda_p(Q) + 2\lambda_p(P) - \log|x(Q) - x(P)|_p \tag{4}$$

for $Q, P, Q \pm P \neq 0$. If it is required that the expression $\lambda_p(Q) - \frac{1}{2}\log|x(Q)|_p$ be bounded as $Q \longrightarrow 0$ (the identity of E), then there is only one such map, called the *canonical local height*. Note that in [22], local heights are normalized to make them invariant under isomorphisms: this involves adding a constant which depends on the discriminant of E, the local heights in [22] then satisfy a different form of the parallelogram law. For a discussion of local heights in the form used here, see [21]. On $E(\mathbb{Q})$ the canonical (global) height $\hat{h}$ can be written as a sum of canonical local heights – see (9) below – or there is a more direct definition using limits of projective heights. If $0 \neq Q = [x(Q), y(Q)] \in E(\mathbb{Q})$ has $x(Q) = \frac{a}{b}$ where a and b are relatively prime integers, define $h_E(Q)$ to be $\frac{1}{2}\log\max\{|a|, |b|\}$. Then $h_E(Q)$ coincides with $\frac{1}{2}h([x(Q), 1])$ in the usual sense of Diophantine geometry. Taking the logarithmic height of the identity to be zero gives the alternative definition

$$\hat{h}(Q) = \lim_{n\to\infty} 4^{-n}h_E(2^nQ).$$

There are explicit formulæ for each of the canonical local heights (see [20], and [22]; [10] for an alternative approach). For a prime p where Q has non-singular reduction,

$$\lambda_p(Q) = \tfrac{1}{2}\log^+|x(Q)|_p. \tag{5}$$

Notice in particular that if $x(Q)$ is integral at p and Q has non-singular reduction at p then $\lambda_p(Q) = 0$. The singular reduction case is more involved, and to avoid a major digression only the *split multiplicative reduction* case is considered (see [22, p. 362] for details on this). The results all hold more generally but require passage to extension fields. In the split multiplicative case, the points on the curve are isomorphic to the group $\mathbb{Q}_p^*/\ell^{\mathbb{Z}}$ where $\ell \in \mathbb{Q}_p^*$ has $|\ell|_p < 1$. The explicit formulæ for the x and y coordinates of a non-identity point on the Tate curve are given in terms of the parameter $u \in \mathbb{Q}_p^*$ by

$$\begin{aligned} x &= x_u = \sum_{n\in\mathbb{Z}} \frac{\ell^n u}{(1-\ell^n u)^2} - 2\sum_{n\geq 1} \frac{n\ell^n}{(1-\ell^n)^2}, \\ y &= y_u = \sum_{n\in\mathbb{Z}} \frac{\ell^{2n} u^2}{(1-\ell^n u)^3} + \sum_{n\geq 1} \frac{n\ell^n}{(1-\ell^n)^2}. \end{aligned}$$

It is clear that $x_u = x_{u\ell}$ and $x_u = x_{u^{-1}}$. Suppose Q corresponds to the point $u \in \mathbb{Q}_p^*$ and assume, by invariance under multiplication by ℓ, that u lies in the fundamental domain $\{u \mid p^{-k} = |\ell|_p < |u|_p \leq 1\}$. Then (by [10] or [22]),

$$\lambda_p(Q) = \begin{cases} -\log|1-u|_p & \text{if } |u|_p = 1, \\ -\frac{k}{2}\left(\frac{r}{k} - \left(\frac{r}{k}\right)^2\right)\log p & \text{if } |u|_p = p^{-r} < 1. \end{cases}$$

Notice that for $|u|_p = 1$, the canonical local height is non-negative, while if $|u|_p < 1$ the canonical local height is negative. Also, these formulæ extend to all of $E(\Omega_p)$ by [22] (Ω_p is the completion of a fixed algebraic closure of $\mathbb{Q}_p$). In [5], [11] and [12], attempts have been made to define dynamical systems whose topological entropy is given by $\hat{h}(Q)$, the global canonical height of Q. In the spirit of the algebraic case, and to reflect the fact that the global canonical height is a sum of canonical local heights, one looks to realize each canonical local height as the entropy of a corresponding local component. In [5] the elliptic adeles are used. D'Ambros [6] works over function fields and assumes that the point Q has everywhere non-singular reduction. In [5] a similar non-singular reduction assumption is made, together with an assumption that Q lies in a neighbourhood of the identity; there is also an artificiality in the construction. The extra freedom of sequential actions allows a different approach to these problems, and gives a clear dynamically motivated description of the global canonical height and the phenomenon of singular reduction.

3. Background on entropy

Most of the definitions and results below are straightforward modifications of well-known theory, so the results are simply stated. The interest is in the later examples. Let X be a 'space': a standard probability space $(X, \mathcal{B}, \mu)$, a compact metric space (X, ρ), or a locally compact metric space (X, d). A *sequential action* on X is a sequence $\mathbf{T} = (T_n)_{n\geq 1}$ of maps $T_n : X \to X$ with the property that each T_n is a μ-preserving $\mathcal{B}$-measurable map, a continuous map, or a uniformly continuous map respectively. One of the essential features of the elliptic phenomena we are trying to capture is that the volume grows at some natural rate. Let $r:\mathbb{N}\to\mathbb{R}$ be non-decreasing with $r(n)\nearrow\infty$. A finite partition ξ of $(X,\mathcal{B},\mu)$ is a collection $\{A_1,\dots,A_k\}$ of $\mathcal{B}$-measurable sets with $\mu(\bigcup_{i=1}^{k}A_i)=1$ and $\mu(A_i\cap A_j)=0$ for all $i\neq j$. The *entropy* of such a partition is $H(\xi)=-\sum_{i=1}^{k}\mu(A_i)\log\mu(A_i)$ (with the convention that $0\log 0=0$), and the *join* of ξ with another finite partition $\eta=\{B_1,\dots,B_\ell\}$ is the partition $\xi\vee\eta=\{A_i\cap B_j\mid 1\le i\le k, 1\le j\le\ell\}$. If $T:X\to X$ is a measurable map, then $T^{-1}\xi$ denotes the partition $\{T^{-1}A_1,\dots,T^{-1}A_k\}$.

Definition 3.1. The (measure-theoretic) sequential entropy of $\mathbf{T}$ on $(X,\mathcal{B},\mu)$ is given by

$$h^r_\mu(\mathbf{T})=\sup_{\xi}\limsup_{n\to\infty}\frac{1}{r(n)}H\left(\bigvee_{j=1}^{n}T_j^{-1}\xi\right),$$

where the supremum is taken over all finite partitions.

Example 3.2. 1. Let $r(n)=n$, and let $T_j=T^j$ for all $j\ge 1$ where T is a single measure-preserving transformation. Then $h^r_\mu(\mathbf{T})=h_\mu(T)$, the usual measure-theoretic entropy of T.
2. Let $r(n)=n$ again, and let $T_j=T^{a_j}$ for a fixed increasing sequence $A=(a_1,a_2,\dots)$. Then $h^r_\mu(\mathbf{T})=h_A(T)$ the 'A-entropy' or sequence-entropy introduced by Kushnirenko [16] as an invariant of measure-preserving transformations not reducible to entropy or spectral invariants unless T has positive entropy (see [15]).

Following Bowen, we next define a topological entropy and a volume-growth entropy for the topological context. Let X be a compact metric space (X,ρ), write $N(U)$ for the least cardinality of a finite subcover of an open cover U, and use $\vee$ to denote the common refinement of two open covers.

Definition 3.3. The (topological) entropy of $\mathbf{T}$ on (X,ρ) is

$$h^r_{top}(\mathbf{T})=\sup_{U}\limsup_{n\to\infty}\frac{1}{r(n)}\log N\left(\bigvee_{j=1}^{n}T_j^{-1}U\right),$$

where the supremum is taken over all open covers U of X.

Example 3.4. 1. Let $r(n)=n$, and let $T_j=T^j$ for all $j\ge 1$ where T is a single continuous map on (X,ρ). Then $h^r_{top}(\mathbf{T})=h_{top}(T)$, the topological entropy of T introduced in [1].
2. Let $r(n)=n$, and let $T_j=T^{a_j}$ for a fixed increasing sequence $A=(a_1,a_2,\dots)$. Then $h^r_{top}(\mathbf{T})=h^A_{top}(T)$ is the topological sequence entropy (see [8]).

3. The directional entropy introduced by Milnor coincides with the entropy in this sense, with $r(n) = n$, for the sequence of transformations seen in a strip along the chosen direction (see [18]).

Definition 3.3 is less than easy to work with, and the calculation of topological entropy is facilitated by Bowen's introduction of spanning and separated sets, homogeneous measures, and volume growth. Let now X be a locally compact metric space (X, d), and assume that each T_j is uniformly continuous.

Definition 3.5. Let $K \subset X$ be compact. A set $E \subset K$ is (n, ϵ)-*separated* under $\mathbf{T}$ if for any distinct points x, y in E, there is a j, $1 \leq j \leq n$, for which $d(T_j x, T_j y) > \epsilon$. A set $F \subset X$ (n, ϵ)-*spans* K if, for every $x \in K$ there is a $y \in F$ for which $d(T_j x, T_j y) \leq \epsilon$ for $1 \leq j \leq n$. Let $r_n(\epsilon, K)$ (resp. $s_n(\epsilon, K)$) denote the largest (smallest) cardinality of a separating (spanning) set for K under $\mathbf{T}$. Then define

$$\begin{aligned} h^r_{Bowen}(\mathbf{T}) &= \sup_K \lim_{\epsilon \searrow 0} \limsup_{n \to \infty} \frac{1}{r(n)} \log r_n(\epsilon, K) \\ &= \sup_K \lim_{\epsilon \searrow 0} \limsup_{n \to \infty} \frac{1}{r(n)} \log s_n(\epsilon, K), \end{aligned}$$

where the supremum is taken over all compact sets $K \subset X$, and the coincidence of the two limits is shown as in [3, Lemma 1].

As in the usual case, it may be shown that $h^r_{Bowen}(\mathbf{T}) = h^r_{top}(\mathbf{T})$ (see [4], [23, Sect. 7.2]) when (X, d) is compact, and that $h^r_{Bowen}(\mathbf{T})$ depends only on the uniform equivalence class of the metric d (see [3, Prop. 3]).

Definition 3.6. Assume that each T_j is a uniformly continuous map on the locally compact metric space (X, d); write

$$D_n(x, \epsilon, \mathbf{T}) = \bigcap_{k=1}^{n} T_k^{-1} B_\epsilon(T_k x)$$

with B_ϵ a metric open ball of radius ϵ. Just as in [3, Def. 6], call a Borel measure μ on X *homogeneous* for $\mathbf{T}$ if μ is finite on compact sets, positive on some compact set, and, for every $\epsilon > 0$ there exist a $\delta > 0$ and a $C > 0$ such that $\mu\big(D_n(y, \delta, \mathbf{T})\big) \leq C\mu\big(D_n(x, \epsilon, \mathbf{T})\big)$ for all $n \geq 1$ and $x, y \in X$. For such a measure, the volume-growth entropy is defined to be

$$\lim_{\epsilon \searrow 0} \limsup_{n \to \infty} -\frac{1}{r(n)} \log \mu\big(D_n(x, \epsilon, \mathbf{T})\big),$$

which is independent of x by homogeneity, and (see [3], *mutatis mutandis*) it coincides with $h^r_{Bowen}(\mathbf{T})$.

Simple estimates show that if the underlying space is of finite measure (or compact), then the measure-theoretic (resp. topological) entropy h^r can only be positive if $r(n)$ grows linearly or sub-linearly. Example 7.1 shows that other rates are possible: the point is that in those examples the underlying space is not compact. This restriction in rate is characteristic of $\mathbb{Z}$-actions (and their sequential analogues). It is possible that an approach via $\mathbb{Z}^2$-actions, which share a natural quadratic-exponential behaviour with canonical heights on elliptic curves, may be possible on compact spaces.

4. Solenoids

Suppose first that $Q = [q, 1] \in \mathbb{P}^1(\bar{\mathbb{Q}})$ is a finite point on the algebraic projective line. Then the map $x \mapsto qx$ on $\mathbb{Z}[q]$ or $\mathbb{Z}[q^{\pm 1}]$ determines a dual map $T_Q : X_Q \to X_Q$ on the compact abelian dual group. Identify X_Q with the dual of a subgroup of $\mathbb{Q}^d$ for some d; then T_Q becomes the map dual to a rational $d \times d$ matrix A. The topological entropy of T_Q is given by Yuzvinskii's formula, $h_{top}(T_Q) = \log|s| + \sum_i \log^+|\lambda_i|$, where s is the g.c.d. of the denominators of the coefficients of the characteristic polynomial of A, and $\{\lambda_i\}$ are the eigenvalues of A counted with multiplicity (see [14] for the original derivation of this result). A more suggestive 'local-to-global' formulation of this result is given in [17]: $h_{top}(T_Q) = \sum_{p\le\infty}\sum_i \log^+|\lambda_{i,p}|_p$, where the inner sum is taken over the eigenvalues of A in the algebraic closure of $\mathbb{Q}_p$, and $|\cdot|_p$ denotes the usual extension of the p-adic valuation.

Example 4.1. In each case the solenoid X_Q is described, and periodic points – points whose orbit under the map T_Q is finite – are also discussed.

1. If $q \in \mathbb{Z}\backslash\{-1, 0, 1\}$, then $\mathbb{Z}[q] = \mathbb{Z}$, so the dual group X_Q is the circle $\mathbb{T}$. The map T_Q is $x \mapsto qx$ mod 1, and it is easy to see that $h_{top}(T) = \log|q|$. Writing $f_n(T_Q) = \{x \mid T_Q^n(x) = x\}$ for the set of points of period n under T_Q gives $|f_n(T_Q)| = |q^n - 1| = |\phi_n(q)|$, where $\phi_n(x) = x^n - 1$ is the nth division polynomial on the circle. Notice that $(1/n)\log|f_n(T_Q)| \to h_{top}(T_Q)$.

2. If q is an algebraic integer (non unit-root) of degree d whose minimal polynomial has constant coefficient ±1, then X_Q is the d-torus $\mathbb{T}^d$, and A can be chosen to be the companion matrix to the minimal polynomial of q. A similar argument shows that $h_{top}(T_Q) = \sum_i \log^+|\lambda_i|$, and $|f_n(T)| = \prod_i |\lambda_i^n - 1|$. It is still the case that $(1/n)\log|f_n(T_Q)| \to h_{top}(T_Q)$, but this is non-trivial because of the possibility of eigenvalues with unit modulus (see [12] for a detailed discussion).

3. If $q = a/b$ is a rational in lowest terms, and X_Q is dual to the group $\mathbb{Z}[q^{\pm 1}] = \mathbb{Z}[\frac{1}{ab}]$, then $h_{top}(T_Q) = \sum_{p \le \infty} \log^+ |\frac{a}{b}|_p = \log \max\{|a|, |b|\}$ is the usual projective height of the point $[q, 1]$. Here $f_n(T_Q) = |a^n - b^n| = |b^n \phi_n(a/b)|$, and again $(1/n) \log |f_n(T_Q)| \to h_{top}(T_Q)$.

Notice that the topological entropy in each case is given by an integral over the circle by Jensen's formula. Yuzvinskii's formula is proved in [17] using an adelic covering space: Example 4.1.3 is a natural quotient of the map $x \mapsto qx$ on the $\mathbb{Q}$-adeles $\mathbb{Q}_{\mathbb{A}}$, and the entropy may be calculated in the adelic covering space using the following results. Firstly, the topological entropy of the action of $A \in M_d(\mathbb{Q})$ on $\mathbb{Q}_p^d$ is given by $h_{Bowen}(A) = \sum_i \log^+ |\lambda_{i,p}|_p$, where the sum is taken over the eigenvalues of A in the algebraic closure of $\mathbb{Q}_p$. Secondly, the covering map has the same topological entropy as the quotient map: $h^r_{Bowen}(\mathbb{Q}_p \overset{\times q}{\to} \mathbb{Q}_p) = h^r_{top}(X_Q \overset{\times q}{\to} X_Q)$.

We therefore pursue an elliptic analogue of Yuzvinskii's formula by considering actions on the adele ring.

5. Duplication on elliptic curves

To fix notation, let E be given in generalized Weierstrass form as in (3). From the shape of this equation, the denominator of the x-coordinate of any rational point is a square. Write $x(2^n Q) = \theta_n = a_n/b_n^2$, $b_n > 0$ as a rational in lowest terms.

Theorem 5.1. *Let $r(n) = 4^n$, $X = \mathbb{R}$, and $T_j(x) = b_j x$ for $j > 1$ with the sequence (b_n) defined by $x(2^n Q) = a_n/b_n^2$. Then $h^r_{Bowen}(\mathbf{T}) = \hat{h}(Q)$ for non-torsion Q.*

Proof. By a strong form of Siegel's theorem (see [20, p. 250]),

$$\lim_{n\to\infty} \frac{\log |a_n|}{2 \log |b_n|} = 1. \tag{6}$$

Also,

$$\lim_{n\to\infty} \frac{1}{r(n)} \log \frac{1}{2} \max\{|a_n|, |b_n^2|\} = \hat{h}(Q) \tag{7}$$

by [20, Chap. VIII, Sect. 9]. Thus $|b_n| \to \infty$ and $\lim_{n\to\infty} \frac{1}{r(n)} \log b_n = \hat{h}(Q)$ by (6) and (7). It follows that

$$\log \mu \left(\bigcap_{j=1}^{n} T_j^{-1} B_\epsilon \right) = -\log \max_{1\le j \le n} \{|b_j|\} + \log 2\epsilon.$$

For any real sequence (d_n) with $\frac{d(n)}{r(n)} \longrightarrow \omega \geq 0$,

$$\frac{\max_{1\leq j\leq n}\{d(j)\}}{r(n)} \longrightarrow \omega \geq 0. \tag{8}$$

It follows that $\frac{1}{r(n)} \log \max_{1\leq j\leq n}\{|b_j|\} \to \hat{h}(Q)$ as required. □

More subtle arithmetic volume growth is visible on the ring of adeles (see [25, Chap. IV] for details on the adele ring). Write elements of the adele ring $\mathbb{Q}_{\mathbb{A}}$ as $\mathbf{x} = (x_\infty, x_2, x_3, \dots)$, then define (for $\alpha \in \mathbb{Q}$) $\alpha\mathbf{x} = (\alpha x_\infty, \alpha x_2, \alpha x_3, \dots)$. Let μ_p be the Haar measure on $\mathbb{Q}_p$ ($p \leq \infty$) normalized to have $\mu_p(\mathbb{Z}_p) = 1$ ($p < \infty$) and $\mu_\infty([0,1)) = 1$, and write $\mu = \prod_{p\leq\infty} \mu_p$. It is enough to consider the neighbourhood $B = (-1,1) \times \prod_{p<\infty} \mathbb{Z}_p$ in Theorem 5.2, Section 6 and Example 7.1 since any ϵ-ball around the identity contains the image of B under an automorphism of $\mathbb{Q}_{\mathbb{A}}$.

Theorem 5.2. *Let $r(n) = 4^n$, $X = \mathbb{Q}_{\mathbb{A}}$, and $T_n(\mathbf{x}) = \theta_n \mathbf{x}$ where $\theta_n = a_n/b_n^2 = x(2^n Q)$. Then $h^r_{Bowen}(\mathbf{T}) = 2\hat{h}(Q)$ for non-torsion Q.*

Proof. At the infinite place, a bound on $\max_{1\leq n\leq N}\{|\theta_n|\}$ is provided by elliptic transcendence theory (see [7]). The minimum distance of nQ from the identity on $\mathbb{C}/L$ is bounded below by n^{-A} for some $A = A(E,Q) > 0$. The size of the x-coordinate is approximately the inverse square of this quantity. Since we are running through the powers of 2 only, this gives an upper bound for $\max_{1\leq n\leq N}\{|\theta_n|\}$ of the shape C^N. Thus, if

$$\bigcap_{j=1}^{N} T_j^{-1} B = B_{N,\infty} \times \prod_{p<\infty} B_{N,p},$$

the measure of $B_{N,\infty}$ is $O(C^N)$. For the finite places, the sequence (b_n) – and hence (b_n^2) – has a very strong divisibility property: $b_i | b_{i+1}$ for all $i \geq 1$ (by the duplication formula). Thus

$$\begin{aligned}
\mu\left(B_{N,p}\right) &= \mu\left(\bigcap_{n=1}^{N} \left(a_n/b_n^2\right)^{-1} \mathbb{Z}_p\right) \\
&= \min_{1\leq n\leq N} \left\{\left|a_n/b_n^2\right|_p^{-1}\right\} \\
&= |b_N|_p^2.
\end{aligned}$$

It follows that

$$\begin{aligned}\log\mu\left(\bigcap_{j=1}^{N}T_j^{-1}B\right) &= 2\log\prod_{p<\infty}|b_N|_p+O(\log C^N)\\ &= -2\log|b_N|+O(N).\end{aligned}$$

So $h^r_{Bowen}(\mathbf{T})=2\hat{h}(Q)$ as in the proof of Theorem 5.1. □

6. A dynamical interpretation of singular reduction

The systems described in Example 4.1 have local entropies which sum to the global topological entropy. Example 7.1 shows that the entropy of simple examples of sequences of transformations on the adeles may not add up in an analogous way. In pursuit of the connection between heights and entropy on elliptic curves, a more substantial problem appears, preventing Theorems 5.1 and 5.2 from decomposing into local contributions. On the height side, it is still the case that the canonical global height is a sum of local canonical heights,

$$\hat{h}(Q)=\sum_{p\le\infty}\lambda_p(Q), \tag{9}$$

(see [20, App. C, Sect. 18]). When p is a prime of singular reduction for the curve, or $p=\infty$, it is possible for the canonical local height $\lambda_p(Q)$ to be strictly negative. This means that it certainly cannot represent the topological entropy of anything, even in the sense of Definition 3.1. In [5], an approach to interpreting the global height as the entropy of a dynamical system is presented. Roughly speaking, since (9) decomposes into an expression for the global canonical height as the difference of two non-negative quantities, it was suggested there that a global system on the adeles might have a canonical factor, whose quotient has the canonical height as entropy, and whose fibres carry the other component of the entropy.

If $P=[x(P),y(P)]$ denotes a generic point on the curve E, described by a generalized Weierstrass equation as before, then $x(nP)$ is a rational function of x and y. In particular, the denominator of that rational function is a polynomial which vanishes on the n-torsion of E. This polynomial can be used to generate a sequence of transformations with more arithmetical subtlety. Let ψ_n denote the nth division polynomial of E for $n\geq 1$ (see [12, App. C], [20]). Thus, ψ_n is an integral polynomial of degree n^2-1 and leading coefficient n^2 whose roots are exactly the x-coordinates of all the non-identity points of order dividing n on E. It is well-known that $\psi_n(x)$ is always the square of a polynomial in both x and y and, for odd n, it is the square of a polynomial in x

alone (see [20, p. 105]). Writing $q = a/b = x_Q$ as a rational in lowest terms with $b > 0$ for the x-coordinate of a fixed rational point Q, recall that b must be a perfect square and define

$$q_n = |b^{n^2-1}\psi_n(a/b)| \in \mathbb{Z}.$$

The remarks above show that q_n is a square for all $n \geq 1$. Additionally, the sequence (q_n) is a divisibility sequence in the usual sense: $m|n$ implies $q_m|q_n$. These elliptic divisibility sequences were studied in an abstract setting by Morgan Ward in a sequence of papers - see [24] for the details. Shipsey's thesis [19] contains more recent applications of these sequences.

Define a sequence of non-negative integers by $u_n^2 = q_{2^n}$. If Q is not a torsion point then the terms of the sequence (u_n) are always non-zero. The divisibility of the sequence (q_n) implies that

$$u_1|u_2|u_3|\dots.$$

Define a sequence of transformations on $\mathbb{Q}_{\mathbb{A}}$ by

$$U_j(\mathbf{x}) = u_j^{-1}\mathbf{x} \tag{10}$$

for $j \geq 1$. To motivate this definition, notice that in Theorems 5.1 and 5.2 the denominator of θ_n is responsible for the volume growth, and hence the entropy. These denominators may be thought of as evaluations of the division polynomial (though in practice a large amount of cancellation takes place). Let S denote the set of primes for which the point Q has singular reduction, and define the S-adeles to be $\mathbb{Q}_S = \prod_{p\in S}\mathbb{Q}_p$. Write $\mathbf{U}_S$ for restriction of $\mathbf{U}$ to $\mathbb{Q}_S$. The canonical local height of Q is non-positive for each prime in S, while for any prime p dividing b, Q has non-singular reduction and the canonical local height there is $-\frac{1}{2}\log|b|_p$.

Theorem 6.1. *For the sequence of transformations* (10) *and* $r(n) = 4^n$*,*
1. $h^r_{Bowen}(\mathbf{U}) = \lambda_\infty(Q) + \frac{1}{2}\log|b|$*,*
2. $h^r_{Bowen}(\mathbf{U}_S) = -\sum_{p\in S}\lambda_p(Q) \geq 0$*, and*
3. $h^r_{Bowen}(\bar{\mathbf{U}}) = \hat{h}(Q) = \lambda_\infty(Q) + \frac{1}{2}\log|b| + \sum_{p\in S}\lambda_p(Q)$ *where* $\bar{\mathbf{U}}$ *is the quotient sequence of transformations induced by* $\mathbf{U}$ *on* $\mathbb{Q}_{\mathbb{A}}/\mathbb{Q}_S$*.*

Notice that the first formula is an analogue of Yuzvinskii's formula. Theorem 6.1 will be proved later.

Corollary 6.2. *If* Q *has everywhere non-singular reduction then*

$$h^r_{Bowen}(\mathbf{U}) = \hat{h}(Q).$$

If Q has singular reduction at $p \in S$ then, with $\bar{\mathbf{U}}$ as before,

$$h^r_{Bowen}(\bar{\mathbf{U}}) = \hat{h}(Q).$$

Define $\epsilon_p(Q)$ to be 1 if $\lambda_p(Q) \geq 0$ and -1 if $\lambda_p(Q) < 0$. This map has the following properties.
1. If Q is integral, then $\epsilon_\infty(Q) = 1$ (see comments after (11)).
2. The set of primes p for which $\epsilon_p(Q) = -1$ is finite.
3. There is a finite-index subgroup in $E(\mathbb{Q})$ on which $\epsilon_p(Q) = 1$ for all $p \in S$ (and therefore for all finite p) – see [12, Sect. 6.2] or [5, Sect. 5].
4. For all Q in a neighbourhood of the identity, $\epsilon_p(Q) = 1$.

Theorem 6.3. *For the sequence of transformations on $\mathbb{Q}_p$ defined by $T_j(x) = q_j^{\epsilon_p(Q)}x$ for $j \geq 1$, where $Q \in E(\mathbb{Q})$ is a non-torsion point, $q = x(Q)$, $q_j^2 = |\psi_j(q)|$, $q_j > 0$, and $r(n) = n^2$, $h^r_{Bowen}(\mathbf{T}) = \epsilon_p(Q)\lambda_p(Q)$.*

Proof. There are three cases to consider. If $p = \infty$, we claim firstly that

$$\lim_{N\to\infty} N^{-2} \log |\psi_N(q)| = 2\lambda_\infty(Q). \tag{11}$$

Notice that this explains the first of the properties of ϵ_∞ above: if Q is integral, then the left-hand side of (11) is non-negative for all N. Formula (11) was proved in [12, Theorem 6.18]; the proof is sketched here because it is similar to the singular reduction case. Take $G = E(\mathbb{C})$ and consider the elliptic Jensen formula

$$\int_G \log |x(P) - x(Q)| d\mu_G(P) = 2\lambda_\infty(Q) \tag{12}$$

where μ_G is the normalized Haar measure on G (see [9]). The points of N-torsion are dense and uniformly distributed in $E(\mathbb{C})$ as $N \to \infty$, so the limit sum over the torsion points will tend to the integral when the integrand is continuous. The only potential problem arises from torsion points close to Q: by [7], for $x = x(P)$ with $NP = 0$, $|x - x(Q)| > N^{-C}$ for some $C > 0$ which depends on E and Q only. This inequality is enough to imply that the Riemann sum given by the N-torsion points for $\log |x(P) - x(Q)|$ converges, which gives (11). Now $q_n^2 = |\psi_n(q)|$, so

$$\log \mu \left(\bigcap_{j=1}^{N} T_j^{-1} B_\epsilon \right) = -\log e_N + \log \epsilon,$$

where $e_N = \max_{1\leq j\leq N}\{q_j^{\epsilon_\infty(Q)}\}$, so using (11) gives

$$\lim_{N\to\infty} N^{-2} \log e_N = \epsilon_\infty(Q)\lambda_\infty(Q).$$

Assume that p is a prime of singular reduction. If $|x(Q)|_p > 1$ then Q has non-singular reduction at p and the result follows from the final case below. Assume therefore that $|x|_p \leq 1$, and use the parametrisation of the curve described in Section 2. The explicit formulæ of that section show that the canonical local height is non-positive. The points of order dividing N on the Tate curve are precisely those of the form $\zeta^i \ell^{j/N}$, $1 \leq i, j \leq N$, where $\zeta \in \Omega_p$ denotes a fixed, primitive Nth root of unity in Ω_p. We claim that

$$\lim_{N\to\infty} N^{-2} \log |\psi_N(q)|_p = 2\lambda_p(Q); \tag{13}$$

this gives another proof that the canonical local height is non-positive at a point which is p-integral, where p is a prime of singular reduction. Let G denote the closure of the torsion points: G is not compact, so the p-adic elliptic Jensen formula cannot be used. Instead we use a variant of the Shnirelman integral: for $f : E(\Omega_p) \to \mathbb{R}$ define the elliptic Shnirelman integral to be

$$\int_G f(Q) \mathrm{d}Q = \lim_{N\to\infty} N^{-2} \sum_{N\tau=0;\tau\neq 0} f(\tau)$$

whenever the limit exists.

We claim firstly that for any $P \in E(\mathbb{Q}_p)$, the Shnirelman integral

$$\int_G \lambda_p(P+Q)\mathrm{d}Q = S(E) \text{ exists and is independent of } P. \tag{14}$$

First assume that P is the identity. Using the explicit formula for the canonical local height gives

$$-N^{-2}\sum_{i=1}^{N-1} \log|1-\zeta^i|_p - N^{-2}\sum_{i=0}^{N-1}\sum_{j=1}^{N-1} \frac{k}{2}\left(\frac{j}{N} - \left(\frac{j}{N}\right)^2\right)\log p. \tag{15}$$

Since $\prod_{i=1}^{N-1}(1-\zeta^i) = N$ in Ω_p, the first sum is $\frac{-\log|N|_p}{N^2}$, which vanishes in the limit; the second sum converges to $-\frac{k}{12}\log p$.

For the general case, let P correspond to the point v on the multiplicative Tate curve. If for some large N no j has $|\ell^{j/N}v|_p = 1$ then the analogous sum to (15) is close to $-\frac{k}{12}\log p$ by the same argument. Assume therefore that there is a j with this property. Then the first sum in (15) is replaced by

$$-N^{-2}\sum_{i=1}^{N-1} \log|1-\ell^{j/N}v\zeta^i|_p - N^{-2}\log|1-(\ell^r v)^N|_p, \tag{16}$$

where $r = j/N$ only depends on v. By p-adic elliptic transcendence theory (see [7]), there is a lower bound for $\log|1-(\ell^r v)^N|_p$ of the form

$-(\log N)^A$, where A depends on E and $v = v(P)$ only. It follows that the first sum vanishes in the limit as before. The second sum in (15) is simply rearranged under rotation by v, so converges to $-\frac{k}{12}\log p$ as before. This proves (14).

The claimed limit (13) now follows by taking the elliptic Shnirelman integral of both sides of the parallelogram law (4) and noting that equation (14) shows that three terms cancel to leave the required limit, so

$$\int_G \log|x(P) - x(Q)|dP = 2\lambda_p(Q)$$

which implies (13). Consider

$$\log\mu\left(\bigcap_{j=1}^N T_j^{-1}B_\epsilon\right) = -\log f_N + \log\epsilon,$$

where $f_N = \max_{1\le j\le N}\{|q_j|_p^{\epsilon_p(Q)}\}$. Dividing by N^2 and taking the limit gives the result as in the case $p = \infty$.

Finally, assume that Q has non-singular reduction at p: In this case, $\lambda_p(Q) \ge 0$ so $\epsilon_p(Q) = 1$. If $|x(Q)|_p = |q|_p > 1$, then

$$\log\mu\left(\bigcap_{j=1}^N T_j^{-1}B_\epsilon\right) = -\log f_N + \log\epsilon,$$

where $f_N = \max_{1\le j\le N}\{|q_j|_p\}$.

If $(p, n) = 1$ then $|\psi_n(q)|_p = |q|_p^{n^2-1}$. If $(p, n) \ne 1$ then $(p, n-1) = 1$. It follows that

$$|q|_p^{(N-1)^2-1} \le f_N^2 \le |q|_p^{N^2-1}.$$

Therefore

$$-\lim_{N\to\infty} N^{-2}\log\mu\left(\bigcap_{j=1}^N T_j^{-1}B_\epsilon\right) = \frac{1}{2}\log|q|_p = \lambda_p(Q)$$

by the explicit formula (5). If $|q|_p \le 1$ then q is a p-adic integer and thus $\lambda_p(Q) = 0$. In this case $\bigcap_{j=1}^N T_j^{-1}B_\epsilon = B_\epsilon$, so there is no contribution to the entropy. □

Proof. (of Theorem 6.1) For $p = \infty$ there can be no entropy contribution for the sequence $U_j(\mathbf{x}) = u_j^{-1}\mathbf{x}$, since u_n is an integer sequence. For p finite, recall that $u_1|u_2|u_3|\ldots$. It follows that

$$\bigcap_{j=1}^N U_j^{-1}\left(\prod_{p<\infty}\mathbb{Z}_p\right) = u_N\left(\prod_{p<\infty}\mathbb{Z}_p\right),$$

which has measure u_N^{-1}. The first result follows, since $\log u_N = \frac{1}{2}(4^N - 1)\log|b| + \frac{1}{2}\log|\psi_{2^N}(q)|$, by (11). The second follows at once by using $\mathbb{Q}_S$ and (13). For the third part of the theorem, the calculation is the same except that we are adrift by $\sum_{p\in S,(p,b)=1}\log|u_N|_p$. It follows from the proof of Theorem 6.3 that the entropy is adjusted by the contribution of the canonical local heights where Q has singular reduction. □

7. Examples on sequence entropy

To see Definition 3.6 in an arithmetic setting, let X be the locally compact ring $\mathbb{Q}_{\mathbb{A}}$. The following examples illustrate some of the ways in which local and global volume growths can interact. Recall that B is the open ball $(-1,1)\times\prod_{p<\infty}\mathbb{Z}_p$.

Example 7.1. 1. Let $p_1, p_2, p_3, \dots$ be the rational primes in their usual order, let $T_j(\mathbf{x}) = p_1 \dots p_j\mathbf{x}$, and let $r(n) = n\log n$. Then it is clear that

$$\mu\left(\bigcap_{j=1}^{n} T_j^{-1}B\right) = \frac{1}{p_1\dots p_n}, \tag{17}$$

so $h^r_{Bowen}(\mathbf{T}) = 1$ (this follows from the estimate $n\log n \ll p_n \ll n\log n$ in [2, Theorem 4.7]).
2. Let $r(n) = n\log n$ and $T_j(\mathbf{x}) = (1/p_1\dots p_j)\mathbf{x}$. Then (17) holds again, so $h^r_{Bowen}(\mathbf{T}) = 1$ as before. However, in this example each 'local' entropy contribution

$$\limsup_{n\to\infty} -\frac{1}{r(n)}\log\mu_p\left(\bigcap_{j=1}^{n} T_j^{-1}A_p\right),$$

where $A_p = \mathbb{Z}_p$ for $p<\infty$ and $A_\infty = (-1,1)$, is zero. This should be contrasted with the usual setting, where the local entropies sum to the global entropy (see [17]).
3. Let $T_j(\mathbf{x}) = \prod_{p\le j} p\mathbf{x}$, where the product is over all primes less than or equal to j and $r(n) = n$. As before,

$$\mu\left(\bigcap_{j=1}^{n} T_j^{-1}B\right) = \frac{1}{\prod_{p\le n} p},$$

so $h^r_{Bowen}(\mathbf{T})$ is positive and no larger than $2\log 2$ (see [13, Theorem 414]).
4. Let $T_j(\mathbf{x}) = j\mathbf{x}$, and $r(n) = \log n$. Then it is easy to see that $h^r_{Bowen}(\mathbf{T}) = 1$.

5. Let $T_j(\mathbf{x}) = j!\mathbf{x}$ and $r(n) = n \log n$; then in a similar way one sees that $h^r_{Bowen}(\mathbf{T}) = 1$ by Stirling's formula.

References

[1] R. L. Adler, A. G. Konheim, and M. H. McAndrew. Topological entropy. *Trans. Amer. Math. Soc.*, 114:309–319, 1965.

[2] Tom M. Apostol. *Introduction to Analytic Number Theory.* Springer-Verlag, New York, 1976. Undergraduate Texts in Mathematics.

[3] Rufus Bowen. Entropy for group endomorphisms and homogeneous spaces. *Trans. Amer. Math. Soc.*, 153:401–414, 1971.

[4] Rufus Bowen. Periodic points and measures for Axiom A diffeomorphisms. *Trans. Amer. Math. Soc.*, 154:377–397, 1971.

[5] P. D'Ambros, G. Everest, R. Miles, and T. Ward. Dynamical systems arising from elliptic curves. *Colloq. Math.*, 84/85(part 1):95–107, 2000. Dedicated to the memory of Anzelm Iwanik.

[6] P. D'Ambros. Elliptic dynamics over function fields. PhD. thesis, Univ. East Anglia, 2001.

[7] Sinnou David. Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France (N.S.)*, (62):iv+143, 1995.

[8] F. M. Dekking. Some examples of sequence entropy as an isomorphism invariant. *Trans. Amer. Math. Soc.*, 259(1):167–183, 1980.

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

[10] Graham Everest. Explicit local heights. *New York J. Math.*, 5:115–120 (electronic), 1999.

[11] Graham Everest and Thomas Ward. A dynamical interpretation of the global canonical height on an elliptic curve. *Experiment. Math.*, 7(4):305–316, 1998.

[12] Graham Everest and Thomas Ward. *Heights of Polynomials and Entropy in Algebraic Dynamics.* Springer-Verlag London Ltd., London, 1999.

[13] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[14] S. A. Juzvinskiĭ. Calculation of the entropy of a group-endomorphism. *Sibirsk. Mat. Ž.*, 8:230–239, 1967.

[15] E. Krug and D. Newton. On sequence entropy of automorphisms of a Lebesgue space. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 24:211–214, 1972.

[16] A. G. Kušnirenko. Metric invariants of entropy type. *Uspehi Mat. Nauk*, 22(5 (137)):57–65, 1967.

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

[18] John Milnor. On the entropy geometry of cellular automata. *Complex Systems*, 2(3):357–385, 1988.

[19] Rachel Shipsey. Elliptic divisbility sequences and the elliptic curve discrete logarithm problem. PhD thesis, Univ. of London, 2000.

[20] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1986.

[21] Joseph H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, 51(183):339–358, 1988.

[22] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1994.

[23] Peter Walters. *An Introduction to Ergodic Theory*. Springer-Verlag, New York, 1982.

[24] Morgan Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.

[25] André Weil. *Basic Number Theory*. Springer-Verlag, New York, third edition, 1974. Die Grundlehren der Mathematischen Wissenschaften, Band 144.

(M.E.) Mathematical Institute, University of Vienna, Strudlhofgasse 4, A-1090 Wien, Austria.
E-mail address: manfred@mat.univie.ac.at

(G.E. & T.W.) School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK.
E-mail address: g.everest@uea.ac.uk