Smooth Conjugacy of Difference Equations derived from Elliptic Curves

Paul Glendinning [a] and Sasha Glendinning[b]

[a]Department of Mathematics, University of Manchester, Oxford Road, Manchester M13 9PL, UK; [b]Greenhead College, Greenhead Road, Huddersfield HD1 4ES, UK.

ARTICLE HISTORY
Compiled April 15, 2020

ABSTRACT
We describe the dynamics associated with a construction of tangent lines to elliptic curves which depend on two parameters. With the exception of a half-curve in the parameter plane the natural compactifications of these maps are shown to be *smoothly* (i.e. C^∞) conjugate to each other and to the classic chaotic map $Q(x) = 1 - 2x^2$. This provides a new non-trivial example of a class of maps which are smoothly conjugate to each other.

KEYWORDS
difference equations, elliptic curves, invariant measures, smooth conjugacy

1. Introduction

Elliptic curves arise in Number Theory where they are typically parametrized by two real numbers [14]. A classic construction defines a group operation on these curves, and the repeated process of 'adding' a point to itself is described by a family of difference equations [14], see equation (7) of section 2. We investigate the dynamics induced by these equations and show that there is a strong equivalence of the systems independent of the parameters. Since this paper brings together two different areas of mathematics, equivalence of dynamical systems and operations on elliptic curves, we begin with a brief overview of the relevant definitions and results that are needed to formulate the problem.

Given a map $f : [-1, 1] \to [-1, 1]$ and $x_0 \in [-1, 1]$ the difference equation $x_{n+1} = f(x_n)$ generates an orbit $(x_0, x_1, x_2, \dots)$ and we write $f^n(x) = f(f^{n-1}(x))$ for $n \geq 2$ (the n^{th} iterate of x), so $x_n = f^n(x_0)$. A point is periodic if $x_p = x_0$ for some $p > 0$ (the period of the orbit) and the stability of a periodic orbit is determined by the eigenvalue $E(x) = (f^p)'(x)$ evaluated at any point on the periodic orbit: if $|E(x)| < 1$ then the orbit is stable whilst if $|E(x)| > 1$ it is unstable. The term eigenvalue is used in e.g. [1, 8] whilst in [11] it is referred to as a multiplier. Two maps f and g may generate dynamics which is similar, and mathematically this is expressed via the idea of topological conjugation. The maps $f : I \to I$ and $g : J \to J$ are topologically conjugate if there exists a homeomorphism $h : J \to I$ such that $f = h \circ g \circ h^{-1}$. The conjugating function h can be thought of as a change of coordinates, and if h is a

CONTACT Paul Glendinning. Email: p.a.glendinning@manchester.ac.uk

diffeomorphism then we say that the maps are differentiably conjugate. Differentiable conjugation is a much stronger condition than topological conjugation since it implies (for example) that the eigenvalues of corresponding periodic orbits are equal (the corresponding orbit of a point $x \in J$ under g is the orbit of the point $h(x)$ under f). The conjugacy is smooth if both the conjugating function and its inverse are C^∞.

A canonical example of a chaotic map is the logistic map, $x_{n+1} = 4x_n(1 - x_n)$ on $[0, 1]$ or equivalently, after scaling,

$$x_{n+1} = Q(x_n) = 1 - 2x_n^2, \quad x_n \in [-1, 1]. \tag{1}$$

The quadratic map Q has many nice properties. It has periodic orbits of all periods, periodic orbits are dense in $[-1, 1]$, there is a dense orbit, and it has an invariant probability density

$$\rho_Q(x) = \frac{1}{\pi\sqrt{1 - x^2}}. \tag{2}$$

More detail can be added: for example the modulus of the eigenvalue of every periodic orbit of period n except the fixed point at $x = -1$ is 2^n.

Jiang [7, 8] investigates this issue of differentiable conjugacy for maps like Q (Ulam-von Neumann maps, see Definition 5.1 below; the name is derived from a short and somewhat gnomic abstract [17]), but there seem to be no explicit examples of families of differentiably conjugate maps except those that can be reverse engineered by defining the family via the conjugating functions. Differentiable conjugacies do arise naturally, for example in the study of period-doubling, and this property leads to rigidity results in which topological properties imply metric properties, see [9, 13] for a more detailed discussion and history. Li and Shen [11] show that two topologically conjugate C^r unimodal maps ($r \geq 3$) are C^r conjugate if they have negative Schwarzian derivative, attractors which are neither periodic orbits nor Cantor sets, and the eigenvalues of corresponding periodic orbits are equal. Removing the negative Schwarzian derivative condition has been the focus of much attention both for conjugacies and more general properties of maps [5, 6, 12]. More recently Alves, Pinheiro and Pinto [1] have shown that if attractors of two C^r maps are conjugate and the conjugating function is locally differentiable then it is C^r on the attractor, see section 5. This generalizes earlier results e.g. [8, 10].

In this paper we show that the addition formula on elliptic curves generates maps which are smoothly conjugate to each other and to the quadratic map. Examples are shown in Figure 3, from which it is clear that some of the maps do not have negative Schwarzian derivatives. On the face of it this is a surprise. We know of no natural classes of examples with this property. Indeed, Jiang [7, 8] cites only two examples of differentiably conjugate maps, and both of these are abstract classes which are essentially alternative formulations of the conditions of the theorems.

Any equation defined by equating a quadratic polynomial in y to a cubic polynomial in x can be written in the form

$$y^2 = x^3 + Ax + B \tag{3}$$

after rescaling and shifting the coordinates. Solutions lie on *elliptic curves* and for given A and B these may take one of three forms as shown in Figure 1. Let Δ denote

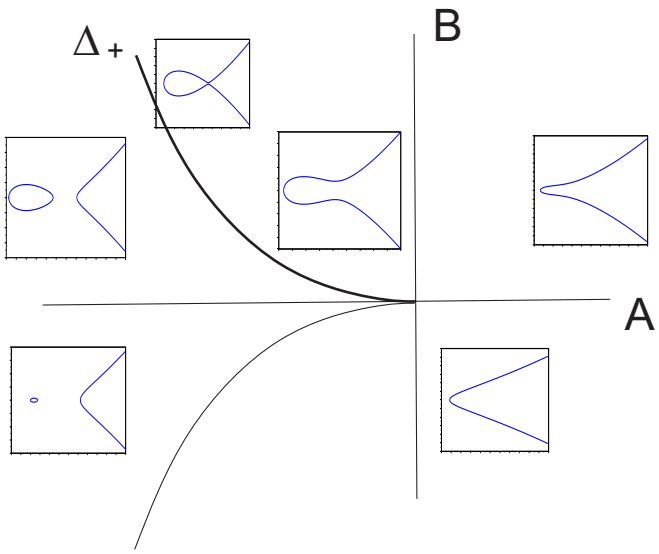

Figure 1. Schematic view of the elliptic curves in the (A, B)-plane. Δ_+ is the part of the curve $\Delta = 0$ in $B \geq 0$, see (8).

the cubic discriminant

$$\Delta = 4A^3 + 27B^2. \tag{4}$$

If $\Delta > 0$ then solutions to (3) lie on a single curve, if $\Delta < 0$ then solutions lie on the union of a closed bounded curve and an unbounded curve, whilst if $\Delta = 0$ then there is a single curve of solutions with a point of self-intersection if $B > 0$ or the union of a curve and a single point if $B < 0$. In the special case of $(A, B) = (0, 0)$ there is a single curve with a cubic cusp singularity. This reflects the number of distinct real zeroes of the right hand side of (3): one if $\Delta \geq 0$, two if $\Delta = 0$ and three if $\Delta < 0$.

Elliptic curves have many beautiful properties, and a principle area of investigation is the existence of rational points on these curves, which are related to problems in number theory centred around Fermat's Last Theorem. A starting point in these studies is the definition of a natural operation which defines a group induced on the points on the curve [14]. This operation ('$\oplus$') is geometric. Any line which intersects the curve does so in three points, with multiplicity and including the point at infinity. If the coordinates of a point P are denoted by $(x(P), y(P))$ and 'minus P' is defined by $\ominus P = (x(P), -y(P))$ then if these three points are P, Q and $\ominus R$, in any order, then

$$P \oplus Q = R. \tag{5}$$

The line between P and $\ominus P$ is vertical, so in this case the third point of intersection is the point at infinity, denoted $\mathcal{O}$ since it acts as an additive zero: $P \oplus (\ominus P) = \mathcal{O}$.

If $P = Q = (x, y)$ then the line is tangential to the elliptic curve and we write $P \oplus P = 2P$. An elementary calculation shows that

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}. \tag{6}$$

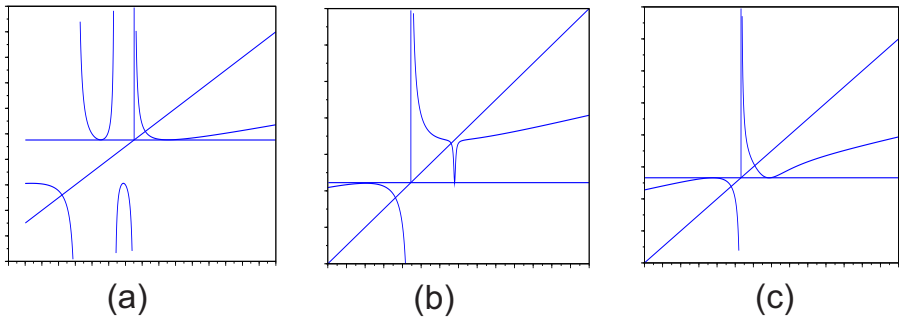

Figure 2. The graph of the right hand side of (6) for (a) $(A, B) = (-3, 1)$, scale $[-8, 10] \times [-6, 12]$; (a) $(A, B) = (-1.88, 1)$, scale $[-6, 8] \times [-6, 8]$; and (c) $(A, B) = (1, 1)$, scale $[-6, 8] \times [-6, 10]$. Note that (b) is just to the right of the curve Δ_+ of Figure 1 as $(27/4)^{\frac{1}{3}} \approx 1.88988$.

It is now natural to think of this as defining a dynamical system by iteration, obtaining $x(2^n P)$ by n iterations of the equation. This may not be as natural from a number theory point of view, particularly as it does not answer questions about rational points, but the iterated construction of drawing a tangent to a point, finding the next point of intersection, reflecting in the x-axis, drawing a tangent at the new point and so on, has many similarities to dual billiard problems [16] in dynamical systems. As we shall see, the dynamics induced by this process appears to have many nice properties. In particular we show that for most values of (A, B) ($(A, B) \notin \Delta_+$, see Figure 1 and (8)) the compactifications of these maps via real Möbius transformations are smoothly conjugate to each other and to the quadratic map Q of (1).

Figure 2 shows the graph of the right hand side of (6) for three choices of (A, B). Note that in (b) the graph develops a 'nose' close to double roots of the denominator of (6). Each of the right hand boxes indicates a non-compact invariant region for the iterated map.

The dynamics of elliptic curves has been discussed in the dynamical systems literature, but almost always respecting the interest in rational points, e.g. [2]. Here we make no claims to relevance in the usual context of the study of elliptic curves. Umeno [18, 19] has used elliptic functions to describe maps with simple invariant density functions (*'exactly solvable chaos'*), and these are related to the multiplication formula (6) for elliptic curves. Our results prove that the maps have absolutely continuous invariant measures (see Corollary 5.7), but do not provide explicit formulas. It seems likely that Umeno's approach coupled with the results of Dobbs [4], which relate the existence of absolutely continuous invariant measures of C^r maps to C^r conjugacies to continuous piecewise linear maps away from the critical orbit, could be used to provide an alternative approach to this problem. We will not pursue this approach below.

2. Definitions and statement of results

Some basic definitions of the smoothness of functions will be important in what follows.

A function $f : M \to N$ is C^k if the first k derivatives exist and are continuous at all $x \in M$. A diffeomorphism $f : M \to N$ is a C^k diffeomorphism if both f and f^{-1} are C^k functions. A function $f : M \to N$ is α-Hölder continuous, $\alpha \in (0, 1)$, if there exists a constant $K > 0$ such that $|f(x) - f(y)| < K|x - y|^\alpha$ for all $x, y \in M$. A diffeomorphism $f : M \to N$ is $C^{1+\alpha}$ if both f and f^{-1} are C^1 functions and their

derivatives are both α-Hölder continuous. A homeomorphism which is C^1 except on a finite set $\mathcal{C}$ is in $C^1_{\mathcal{C}}$.

A unimodal map is a continuous map of an interval M, $f : M \to M$ if there exists $c \in \mathrm{int}(M)$ such that f is monotonically increasing on one side of c and monotonically decreasing on the other side of c. A 2-unimodal map is a unimodal map $f : [-1, 1] \to [-1, 1]$ with $c = 0$, $f(0) = 1$, $f(1) = f(-1) = -1$ and $f(x) > x$ if $x \in (-1, 0)$. Thus the image of the interval $[-1, 1]$ covers itself twice. A standard example of a 2-unimodal map is the quadratic map Q of (1). The transformation $h : [-1, 1] \to [-1, 1]$

$$h(x) = \sin \frac{\pi x}{2},$$

is a $C^1_{\mathcal{C}}$ conjugacy between Q and the tent map $T(x) = 1 - 2|x|$ with $\mathcal{C} = \{-1, 0, 1\}$, the orbit of the critical point.

A rather more boring class of unimodal map is the class of superstable unimodal maps for which f is C^1, $f(0) = 0$, $f(1) = f(-1) = -1$ and $f(x) > x$ if $x \in (-1, 0)$. The dynamics of such maps is very simple: all orbits with $x \in (-1, 1)$ tend to zero.

If f has a periodic orbit of period n with points $p_1, \ldots, p_n$ then the eigenvalue of the orbit is $\prod f'(p_k)$ and if f and g are C^1 topologically conjugate, or $C^1_{\mathcal{C}}$ topologically conjugate and the periodic points are disjoint from $\mathcal{C}$, then the eigenvalues of the corresponding periodic orbits of f and g are equal. Thus the modulus of the eigenvalues of all the periodic points of Q with period n except the fixed point $x = -1$ equal 2^n, but the eigenvalue of -1 for Q is 4.

For clarity we recall that we are considering (6) as defining a dynamical system by iteration:

$$x_{n+1} = F(x_n) = \frac{x_n^4 - 2Ax_n^2 - 8Bx_n + A^2}{4(x_n^3 + Ax_n + B)}. \tag{7}$$

Note that strictly speaking we should refer to $F_{(A,B)}$ to emphasize the dependence on parameters, but we will avoid unnecessary subscripts and simply refer to the maps F. Since the maps F of (7) are defined on semi-infinite intervals $[r, \infty)$, see section 3, it is natural to use a (real) Möbius transformation to provide a topologically conjugate map f on the interval $[-1, 1]$. All our results will be stated for the compactified maps f which are defined precisely in section 4.

Only the upper part of Δ defined in (4) plays a role in the statement of the theorems, so let

$$\Delta_+ = \{(A, B) \mid 27B^2 = -4A^3,\ B \geq 0\}. \tag{8}$$

With this notation our main results can be stated.

Theorem 2.1. *If $(A, B) \notin \Delta_+$ then every compactified map f is smoothly conjugate to every other map f, and to the quadratic map Q.*

Theorem 2.2. *If $(A, B) \in \Delta_+ \backslash \{(0, 0)\}$ then every compactified map f is a superstable unimodal map. If $(A, B) = (0, 0)$ then the uncompactified map is $F(x) = x^3$, $r = 0$ and initial conditions in $0 < x < 1$ tend to zero and those with $x > 1$ tend to infinity.*

Whilst the parameterisation in terms of A and B is natural in the context of elliptic curves, from a dynamical systems point of view the behaviour can be reduced to three

one-parameter families of maps by an orientation preserving scaling of the variable x. If $B = 0$ then (7) becomes

$$x_{n+1} = \frac{(x_n - A)^2}{4x_n(x_n + A)} \tag{9}$$

whilst if $B \neq 0$ then the linear transformation $x \to |B|^{\frac{1}{3}}x$ shows that without loss of generality we may consider the two one-parameter families in terms of $C = A|B|^{-\frac{1}{3}}$ given by

$$x_{n+1} = \frac{(x_n^2 - C)^2 \mp x_n}{4(x_n^3 + Cx_n \pm 1)}, \tag{10}$$

with the upper signs chosen if $B > 0$ and the lower signs if $B < 0$. Whilst this formulation simplifies some calculations (for example the condition $\Delta = 0$ becomes $C^3 = -\frac{27}{4}$), we will retain the standard parameterisation of A and B.

3. The non-compact map F

Let

$$H(x) = x^3 + Ax + B, \tag{11}$$

so H is the denominator of the rational map F of (7). Almost all the proofs for this paper stem from a remarkable factorization lemma relating the derivative of F to F and H. We are sure that this must have been noted elsewhere, but have been unable to find any explicit reference.

Lemma 3.1. *Suppose that F is defined by (7) and H by (11) then*

$$H(F(x)) = \frac{1}{4}H(x)[F'(x)]^2 \quad \text{if } H(x) \neq 0. \tag{12}$$

Proof. The proof is a brute force calculation which we have verified using Mathematica. A straightforward calculation shows that

$$F'(x) = \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - (A^3 + 8B^2)}{4(x^3 + Ax + B)^2}$$

and so

$$F'(x) = \frac{G(x)}{4[H(x)]^2}, \tag{13}$$

where

$$G(x) = x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - (A^3 + 8B^2), \tag{14}$$

and $F'(x) = 0$ iff $G(x) = 0$.

Thus (12) can be rewritten as

$$H(F(x)) = \frac{1}{4}H(x)[F'(x)]^2 = \frac{[G(x)]^2}{64[H(x)]^3} \quad \text{if } H(x) \neq 0. \tag{15}$$

Now

$$F(x) = \frac{J(x)}{4H(x)}, \quad \text{where} \quad J(x) = x^4 - 2Ax^2 - 8Bx + A^2,$$

so if

$$[J(x)]^3 + 16AJ(x)[H(x)]^2 + 64B[H(x)]^3 \equiv [G(x)]^2 \tag{16}$$

then (12) follows immediately from (16) by dividing through by $64[H(x)]^3$.

Equation (16) is an identity relating between two polynomials of degree twelve, and each side when multiplied out gives

$$\begin{aligned}
&x^{12} + 10Ax^{10} + 40Bx^9 + 15A^2x^8 + 192ABx^7 \\
&-(52A^3 - 384B^2)x^6 - 240A^2Bx^5 \\
&+(15A^4 - 240AB^2)x^4 - 320B^3x^3 + (10A^5 + 96A^2B^2)x^2 \\
&+(8A^4B + 64AB^3)x + A^6 + 16A^3B^2 + 64B^4.
\end{aligned}$$

□

The first step towards understanding the dynamics of (7) is to determine the domain of definition for recurrent dynamics. The following lemma simply confirms the remark in the caption of Fugure 2.

Lemma 3.2. *Let r denote the largest real solution of $H(x) = 0$ if $(A, B) \notin \Delta_+$, and the smallest (most negative) real solution if $(A, B) \in \Delta_+ \backslash \{(0, 0)\}$. Let $I = [r, \infty)$. Then F maps I onto itself and F has a unique minimum, $c \in (r, \infty)$, with*

$$F(c) = \begin{cases} r & \text{if } (A, B) \notin \Delta_+ \\ c & \text{if } (A, B) \in \Delta_+ \backslash \{(0, 0)\}. \end{cases}$$

Proof. If $\Delta < 0$ then the denominator of F has one zero and if $\Delta > 0$ then there are three zeroes. Graphs of F are shown in Figure 2 showing how F develops a 'nose' as Δ approaches zero from below to transition between the two cases. Clearly

$$\lim_{x \downarrow r} F(x) \to \infty,$$

and for sufficiently large x, $F(x) < x$ since $F(x) = \frac{1}{4}x + O(1)$.

Thus F has a minimum $c \in (r, \infty)$, and $F(c) = r$ by (12). (To show that it cannot equal a different zero of H takes some additional manipulation, but also follows immediately from the group property of the geometric addition operation: if $F(c) < r$ then the image of some parts of the curve would be in a region in which the graph of the curve has no image, and hence the geometric addition formula would not be defined). The turning point c must be the only minimum in (r, ∞) since if there were

two minima they would have to be a maximum between them, i.e. a point c_1 such that $G(c_1) = 0$ and $F(c_1) > r$, which contradicts (12). □

Lemma 3.2 has a nice interpretation in terms of the geometry. The continuous components of the graphs of F which tend to minus infinity at the points of discontinuity are not relevant to the geometry; the elliptic curve has no points with those values of x. In the case $\Delta > 0$ when the elliptic curve has two connected components the image of the closed curve lies on the unbounded connected curve (including the point at infinity) and the unbounded connected component is invariant. The point $(r, 0)$ is the intersection of the unbounded component with the x-axis, at which point the tangent is vertical and so the image of this point is the point at infinity, $\mathcal{O}$.

Let

$$\mathbb{R}_r = [r, \infty) \cup \mathcal{O}.$$

By Lemma 3.2, if $(A, B) \notin \Delta_+$ then $F((c, \infty)) = (r, \infty)$, $F((r, c)) = (r, \infty)$ and F is continuous and monotonic on each of the intervals (r, c) and (c, ∞). This means that F restricted to $\mathbb{R}_r$ is essentially a unimodal map whose turning point is mapped to the unstable fixed point $\mathcal{O}$. This structure is exploited in the next section to define families of maps on the compact interval $[-1, 1]$ which are obtained by real Möbius transformations from the maps F.

4. Compactification and eigenvalues

The map F of (7) is defined on a non-compact domain, and so to avoid issues of convergence at infinity we will work with a compactified version. It is natural to choose a Möbius transformation that takes the three points (r, c, ∞) to $(1, 0, -1)$ respectively, i.e. $h : \mathbb{R}_r \to [-1, 1]$ with

$$h(x) = \frac{-x + c}{x + (c - 2r)} \tag{17}$$

with inverse $h^{-1} : [-1, 1] \to \mathbb{R}_r$ defined by

$$h^{-1}(x) = \frac{c - (c - 2r)x}{1 + x}. \tag{18}$$

Note that since $c > r$,

$$h'(x) = -\frac{2(c - r)}{(x + c - 2r)^2} < 0, \quad \text{if } x \in \mathbb{R}_r \quad \text{and} \quad (h^{-1})'(x) = -\frac{2(c - r)}{(1 + x)^2} < 0, \quad \text{if } x \in [-1, 1].$$

The conjugate function $f : [-1, 1] \to [-1, 1]$ is

$$f(x) = h \circ F \circ h^{-1}(x). \tag{19}$$

Lemma 4.1. *(Elementary properties of f) Let $f : [-1, 1] \to [-1, 1]$ be defined by (19) and suppose that $(A, B) \neq (0, 0)$.*

(i) $f(0) = 1$; $f(1) = f(-1) = -1$;

(ii) f *is* C^∞ *on* $[-1,1]$ *and* $f'(-1)=4$.
(iii) $f'(x)>0$ *if* $x\in[-1,0)$ *and* $f'(x)<0$ *if* $x\in(0,1]$*; and*
(iv) $f'(0)=0$ *and* $f''(0)<0$.

Proof. (i) $F(r)=\mathcal{O}$, $F(c)=r$ and $F(\mathcal{O})=\mathcal{O}$ imply that $f(0)=1$ and $f(1)=f(-1)=-1$.

(ii) If $x\in(-1,1)$ then f is a composition of rational functions with non-vanishing denominators and so it is C^∞. In a neighbourhood of $x=-1$ set $x=-1+v$. Then a routine calculation shows that if $v\neq 0$, f is the ratio of two quartics in v and the denominator is non-zero in a neighbourhood of $v=0$. Thus this ratio is C^∞ at $v=0$ and f is C^∞ at $x=-1$. In fact, if $L(v)=1-(\frac{c-2r}{2(c-r)})v$ then

$$h^{-1}(x)=\frac{2(c-r)L(v)}{v},$$

from which

$$F\circ h^{-1}(x)=\left(\frac{c-r}{2v}\right)\frac{L^4-2Av^2L^2-8Bv^3L+Av^4}{L^3+Av^2L+Bv^3}$$

and so

$$f(-1+v)=-\frac{L^4-2Av^2L^2-8Bv^3L+Av^4-\frac{2c}{c-r}(L^3+Av^2L+Bv^3)}{L^4-2Av^2L^2-8Bv^3L+Av^4+\frac{2(c-2r)}{c-r}(L^3+Av^2L+Bv^3)}.$$

This is the ratio of two quartics in v and the denominator equals one at $v=0$ so it is C^∞ in a neighbourhood of $v=0$, i.e. $x=-1$. Moreover, simplifying a little more,

$$f'(-1)=\frac{d}{dv}\left(\frac{-(c-r)+2cv+O(v^2)}{c-r+2(c-2r)v+O(v^2)}\right)\Big|_{v=0}=4.$$

A similar argument holds in a neighbourhood of $x=1$.

(iii) Since the derivatives of both h and h^{-1} are negative, the sign of the derivative of f at x is the sign of the derivative of F evaluated at $h^{-1}(x)$ establishing (iii) by remarks of the previous section.

(iv) Differentiating (12)

$$H'(F(x))F'(x)=\frac{1}{4}\Big(H'(x)[F'(x)]^2+2H(x)F'(x)F''(x)\Big)$$

and evaluating at $x=c$ being careful about the limits:

$$F''(c)=2\frac{H'(r)}{H(c)}.$$

But if $(A,B)\notin\Delta_+$ then $r<c$, $H(c)>0$ and $H'(r)>0$ so $F''(c)>0$. For finite x and $h^{-1}(x)$ the chain rule gives

$$f''(c)=h'(F(c))F''(c)[(h^{-1})'(c)]^2$$

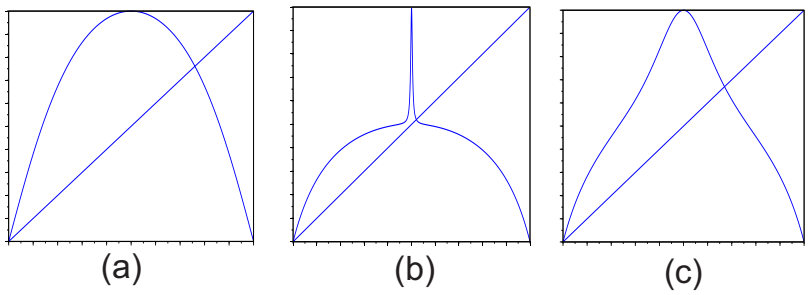

Figure 3. Compactified maps $f : [-1, 1] \to [-1, 1]$: (a) $(A, B) = (-2, 1)$; (a) $(A, B) = (-1.88, 1)$, and (c) $(A, B) = (1, 1)$.

and since both h and h^{-1} are decreasing the sign of $f''(c)$ is negative. □

Examples of the return maps obtained from the compactification onto $[-1, 1]$ are given in Figure 3. Note that the maps are clearly not always 'nice' in the sense of convex, negative Schwarzian derivative or any other simple criterion. The sharp peak in Figure 3b is explained by the limiting behaviour on Δ_+ described in section 6.

We now turn to the eigenvalues of the map at periodic orbits.

Lemma 4.2. *If $(A, B) \notin \Delta_+$ then in (r, ∞) F has one and only one fixed point x^* and $|F'(x^*)| = 2$.*

Proof. Evaluating (12) at x^* using $F(x^*) = x^*$ gives

$$1 = \frac{1}{4}[F'(x^*)]^2,$$

so $|F'(x^*)| = 2$. Clearly F has a fixed point in (r, c). Suppose that it has a fixed point y^* in $x > c$. Since $F(c) < c$ and the slope of the map at y^* is 2, $F(x) > x$ for $x > y^*$ (as if there were another fixed point at larger values of x it would have to intersect the diagonal with slope less than or equal to one). But $F(x) < x$ at large x since $F(x) \sim \frac{1}{4}x + O(1)$ as $x \to \infty$, a contradiction. □

The same technique generalizes to every periodic orbit except $x = -1$ ($\mathcal{O}$ on the infinite domain).

Lemma 4.3. *Let $(x_1, \ldots x_n)$ be points on a periodic orbit of $F : [r, \infty) \to [r, \infty)$ with $x_k \in (r, \infty)$, $F(x_k) = x_{k+1}$, $k = 1, \ldots, n-1$ and $f^n(x_n) = 1$. Then*

$$\prod_1^n |F'(x_k)| = 2^n.$$

Proof. Note that $H(x) > 0$ for $x \in (r, \infty)$. Evaluating (12) at x_k gives

$$H(x_1) = \frac{[G(x_n)]^2}{64[H(x_n)]^3}, \quad H(x_{k+1}) = \frac{[G(x_k)]^2}{64[H(x_k)]^3}, \quad k = 1, \ldots, n-1.$$

Thus

$$\frac{H(x_1)}{H(x_n)} = \frac{1}{4}[F'(x_n)]^2, \quad \frac{H(x_{k+1})}{H(x_k)} = \frac{1}{4}[F'(x_k)]^2, \quad k = 1, \ldots, n-1,$$

and multiplying all n right hand sides together and similarly for the left hand sides

$$1 = \frac{1}{2^{2n}} \prod_1^n [F'(x_k)]^2,$$

from which the result follows by taking the square root. Since h is continuously differentiable on (r, ∞), the derivatives of f^n and F^n at corresponding periodic points of period n in the open sets (r, ∞) and $(-1, 1)$ are equal. □

This result shows that all periodic points are expanding and provides evidence supporting the claim that the topological conjugacy is differentiable.

5. Differentiable conjugacy and invariant measures

In this section we use results from Jiang and van Strien to establish that the dynamics on each elliptic curve is differentiably conjugate to each other and to the classic quadratic map $Q(x) = 1 - 2x^2$.

Let $J_{n,k}$ denote the set of maximal intervals on which f^n is monotonic, i.e. the maximal intervals such that $f^n|J_{n,k}$ is a homeomorphism. Also, for given $\gamma \geq 1$, define the power function

$$r_f(x) = \frac{f'(x)}{|x|^{\gamma-1}}.$$

Jiang [8] works with Ulam-von Neumann maps which can be defined as follows using Lemma 5 of [8].

Definition 5.1. A $C^{1+\alpha}$ 2-unimodal map $f : [-1, 1] \to [-1, 1]$ for some $0 < \alpha \leq 1$ is a *Ulam-von Neumann* map if

(U1) there exists $\gamma \geq 1$ and real number $A < 0$ such that

$$\lim_{x \uparrow 0} r_f(x) = \lim_{x \downarrow 0} r_f(x) = A, \tag{20}$$

(γ is called the power law of f);

(U2) the power function $r_f(x)$ is β-Hölder continuous when restricted to $[-1, 0)$ and to $(0, 1]$; and

(U3) there exists $\mu < 1$ and real $C > 0$ such that $|J_{n,k}| \leq C\mu^n$ for all (n, k).

In fact, Jiang works in a slightly more general setting in which the two limits in (20) can take different values, but this will be unnecessary for the application below.

Theorem 5.2. *[8] Two Ulam-von Neumann maps are $C^{1+\epsilon}$-topologically conjugate to each other for some $0 < \epsilon \leq 1$ provided the eigenvalues at corresponding periodic orbits are equal.*

To prove Theorem 2.1 we start with differentiable conjugacy.

Theorem 5.3. *If $(A,B) \notin \Delta_+$ then every map f is $C^{1+\frac{1}{2}}$ conjugate to every other map f, and to the quadratic map Q.*

Here we need only establish that the conditions for Jiang's Theorem hold. The only difficult part is checking (U3) of Definition 5.1. To do this we need a further definition and a result from van Strien [15].

Definition 5.4. A critical point c of a unimodal map is *non-flat* if there exists $n \geq 1$ and a neighbourhood $\mathcal{N}$ of c such that

(NF1) f is $C^{\max(3,2n)}$ on $\mathcal{N}$;
(NF2) $f^{(2n)}(c) \neq 0$; and
(NF3) $f^{(k)}(c) = 0$ if $k = 1, \ldots 2n-1$.

Theorem 5.5. *[15] If $f : [-1,1] \to [-1,1]$ is a C^2 unimodal map with non-flat critical point and all periodic orbits are expanding then f has no homtervals and there exists $\lambda > 1$ and a constant C such that for any maximal interval I_n such that $f^n|I_n$ is a diffeomorphism*

$$|f^n(I_n)| \geq K\lambda^n |I_n|. \tag{21}$$

of Theorem 5.3. The eigenvalue of f at the fixed point $x = -1$ is 4 (Lemma 4.1(ii)) and for all other periodic points of period p the eigenvalue is $\pm 2^p$ (Lemma 4.3 together with the fact that the compactification is a C^∞ diffeomorphism away from the end-points of the intervals) with the sign determined by the parity of the number of points in $x > 0$, which is the same for corresponding orbits. The same is true for the quadratic map Q (see the second paragraph of section 2). Hence the eigenvalue condition of Jiang's Theorem (Theorem 5.2 holds.

Differentiating (12)

$$H'(F(x))F'(x) = \frac{1}{4}\Big(H'(x)[F'(x)]^2 + 2H(x)F'(x)F''(x)\Big)$$

and evaluating at $x = c$ being careful about the limits:

$$F''(c) = 2\frac{H'(r)}{H(c)}.$$

But if $(A,B) \notin \Delta_+$ then $r < c$ and $H'(r) \neq 0$ so $F''(c) \neq 0$. Since F is C^∞ on a neighbourhood of c (again, provided $(A,B) \notin \Delta_+$), F and hence f are non-flat critical points and so van Strien's theorem (Theorem 5.5) holds.

Since $f^n(I_n) \subseteq [-1,1]$, $|f^n(I_n)| \leq 2$ and hence (21) implies that

$$|I_n| \leq 2K^{-1}\lambda^{-n}.$$

But the intervals I_n are precisely the intervals $J_{n,k}$ of Jiang and so (U3) holds with $C = 2K^{-1}$ and $\mu = \lambda^{-1}$.

The smoothness conditions are clearly satisfied (U1) and (U2) are clearly satisfied with power law $\gamma = 2$ since $f''(c) \neq 0$ and $\alpha = 1$ since f is C^∞. The exponent $\epsilon = \frac{1}{2}$ follows from the end of the proof of Lemma 8 in [8] which shows that $\epsilon = \alpha/\gamma$.

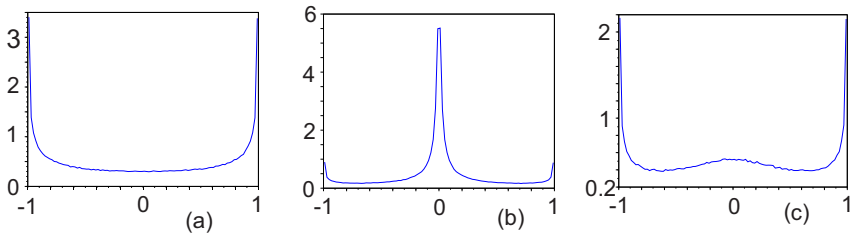

Figure 4. Histograms (100 bins) of 500000 iterations of an initial condition for the compactified maps shown in Figure 3 at the same parameter values: (a) $(A, B) = (-2, 1)$; (a) $(A, B) = (-1.88, 1)$, and (c) $(A, B) = (1, 1)$. Normalization is chosen so that the integral of the density is one. Note that in case (b) numerical instability meant that the map used for iteration was $0.999999999f$, and that the profile shown is accurate for 250000 iterations of the map f using Scilab 6.0.2.

The equivalent results for the quadratic map are well known [9]. □

To complete the proof of Theorem 2.1 we use a result from [1]. To avoid the introduction of more notation we will state their result in a very restricted form of their Corollary 2.6 appropriate for our proof.

Theorem 5.6. *[1] Let $f : I \to I$ and $g : I \to I$ be C^r Ulam-von Neumann maps. Suppose that the eigenvalues of every periodic point of f and of g has modulus greater than one and the power laws of f and g are equal. If the conjugating function h between f and g is C^1 at some periodic point $p \in I$, then h is a C^r diffeomorphism on the whole of I.*

We emphasize that this statement does not begin to do justice to the actual statement in [1], but the restriction is good enough for our purposes.

of Theorem 2.1. By Theorem 5.3 the any two maps of the theorem are differentiably conjugate and hence the conjugating function is C^1 on the whole interval. The maps f of the theorem are C^∞ so by Theorem 5.6 the conjugating function is also C^∞ (it is C^r for all $r \geq 1$). □

Corollary 5.7. *Let $\rho_Q(x)$ denote the invariant density function (2) of the quadratic map. For all $(A, B) \notin \Delta_+$ there exists a smooth diffeomorphism $q : [-1, 1] \to [-1, 1]$ such that $f = q \circ Q \circ q^{-1}$ and the density of the invariant measure of f is ρ_f where*

$$\rho_f(x) = \frac{1}{q'(q^{-1}(x))} \rho_Q(q^{-1}(x)). \tag{22}$$

Proof. By Theorem 2.1, f and Q are smoothly conjugate. Let q denote the conjugating function, then (22) follows by equating probabilities at corresponding intervals in $[-1, 1]$. □

Figure 4 shows numerically computed probability distributions of iterates of f for different values of A and B (the same values as used in the description of maps earlier). The peaks near the turning point for values of parameters close to Δ_+ are to some extent explained by Theorem 2.2.

6. Proof of Theorem 2.2

On Δ_+, A and B are related as $\Delta = 0$ and we may calculate directly that

$$r = -2\sqrt{\frac{-A}{3}}, \quad c = \sqrt{\frac{-A}{3}},$$

and c is a fixed point of the map. Indeed, c is the double zero of $H(x) = 0$ and this gives the impression that F is singular at c, but there is again a cancellation in the calculation and F may be calculated explicitly:

$$F(x) = \frac{-A + \sqrt{\frac{-A}{3}}(x - \sqrt{\frac{-A}{3}}) + \frac{1}{4}(x - \sqrt{\frac{-A}{3}})^2}{3\sqrt{\frac{-A}{3}} + (x - \sqrt{\frac{-A}{3}})}$$

with

$$F'(\sqrt{\frac{-A}{3}}) = \frac{\sqrt{\frac{-A}{3}}(3\sqrt{\frac{-A}{3}}) + A}{(3\sqrt{\frac{-A}{3}})^2} = 0.$$

Thus c is both the fixed point and the turning point of the map: it is superstable.

7. Conclusion

We have shown that the maps in a natural family of dynamical systems derived from a simple geometric construction on elliptic curves are smoothly conjugate to each other. This is a restricted form of rigidity for which we have no intuitive explanation. The proof relies on a factorization result (Lemma 3.1) which should have interesting generalizations and which may lead to a better understanding of the conditions for smooth conjugacy. It would be natural to consider other classes of curves (e.g. some of those used in cryptography, [3]) to determine whether this smooth conjugacy is special to elliptic curves or a more general phenomenon.

Acknowledgements

The idea for this paper was provided by Sir Martin Taylor's eulogy at the memorial service for Sir Peter Swinnerton-Dyer at Trinity College, Cambridge in June 2019. We are grateful to Tom Kempton (University of Manchester) and Sebastian van Strien (Imperial College, London) for helpful remarks.

Disclosure Statement

We know of no conflict of interest arising from this research.

References

[1] J.F. Alves, V. Pinheiro, and A.A. Pinto, *Explosion of smoothness for conjugacies between multimodal maps*, J. Lond. Math. Soc. 89 (2014), pp. 255-274.

[2] P. D'Ambros, G. Everest, R. Miles, and T. Ward, *Dynamical systems arising from elliptic curves*, Colloquium mathematicum 84/85 (2000), pp. 95-107.

[3] J. W. Bos, C. Costello, P. Longa, and M. Naehrig, *Selecting elliptic curves for cryptography: an efficiency and security analysis*, J. Crypt. Eng. 6 (2016), pp. 259–286.

[4] N. Dobbs, *Visible measures of maximal entropy in dimension one*, Bull. Lond. Math. Soc. 39 (2007), pp. 366-376.

[5] J. Graczyk, D. Sands, and G. Swiatek, *Metric Attractors for Smooth Unimodal Maps*, Ann. Math. 159 (2004), pp. 725-740.

[6] J. Graczyk, D. Sands, and G. Swiatek, *Decay of Geometry for Unimodal maps: Negative Schwarzian Derivative Case*, Ann. Math. 161 (2005), pp. 613-677.

[7] Y. Jiang, *Generalised Ulam-von Neumann Transformations*, Ph.D. Thesis, CUNY, 1990.

[8] Y. Jiang, *On Ulam-von Neumann Transformations*, Comm. Math. Phys. 172 (1995), pp. 449-459.

[9] Y. Jiang, *On rigidity of one-dimensional maps*, Contemp. Math. AMS 211 (1997), pp. 319-431.

[10] Y. Jiang, *Differentiable rigidity and smooth conjugacy*, Ann. Acad. Sci. Fenn. Math. 30 (2005), pp. 361-383.

[11] S. Li and W. Shen, *Smooth conjugacy between S-unimodal maps*, Nonlinearity 19 (2006), pp. 1629-1634.

[12] O.S. Kozlovski, *Getting Rid of the Negative Schwarzian Derivative Condition*, Ann. Math. 152 (2000), pp. 743-762.

[13] W. de Melo, *Rigidity and Renormalization in One Dimensional Dynamical Systems*, Documenta Math. Extra Volume ICM II, (1998), pp. 765-778.

[14] J.H. Silverman, *The Arithmetic of Elliptic Curves (2nd Edition)*, Graduate Texts in Mathematics 109, Springer, Dordrecht Heidelberg London New York, 2009.

[15] S. van Strien, *Hyperbolicity and Invariant Measures for General C^2 Interval Maps Satisfying the Misiurewicz Condition*, Comm. Math. Phys. 128 (1990), pp. 437-495.

[16] S. Tabachnikov and F. Dogru, *Dual Billiards*, Math. Intell. 27 (2005), pp. 18-25.

[17] S. Ulam and J. von Neumann, *On Combination of Stochastic and Deterministic Processes*, Bull. AMS 53 (1947), p. 1120.

[18] K. Umeno, *Method of constructing exactly solvable chaos*, Phys. Rev. E 55 (1997), pp. 5280–5284.

[19] K. Umeno, *Exactly solvable chaos and addition theorems of elliptic functions*, RIMS Kokyuroku 1098 (1999), pp. 104-117.