Riv. Mat. Univ. Parma, Vol. **13** (2022), 175-182

David Masser and Umberto Zannier

Estimating isogenies on tangent spaces

To Roberto, in friendly collegiality

Abstract. If two elliptic curves are isogenous, then there is an integer matrix connecting their representatives in the upper half plane. When these are normalized to lie in the standard fundamental domain, we give a best possible upper bound for the matrix entries in terms of the degree of the isogeny.

Keywords. Isogeny bounds, elliptic curves, abelian varieties.

Mathematics Subject Classification: 14K02, 11G05, 11G10.

1 - Introduction

Let E, E' be complex elliptic curves with j-invariants $j(\tau), j(\tau')$ respectively, for the standard modular function j with τ, τ' in the upper half plane. When E, E' are isogenous, it is well-known that there is a relation

$$\tau' = \frac{a\tau + b}{c\tau + d} \tag{1}$$

with integers a, b, c, d such that $m = ad - bc$ is the degree of the isogeny. Over the last years one has required upper bounds for these integers in terms of m and possibly other quantities (and even analogous bounds relating to general abelian varieties). As τ, τ' are well-defined only up to the action of $\mathrm{SL}_2(\mathbf{Z})$, it is natural to take them to lie in the standard fundamental domain (see below) for this action.

The paper [**5**] of Wüstholz and the first author was mainly concerned with certain upper bounds for m itself in terms of arithmetic information about E, E'. Such upper bounds are sometimes referred to in the literature as "isogeny

Received: April 24, 2021; accepted in revised form: May 24, 2021.

estimates". To find bounds for a, b, c, d may be regarded as similar problems about the rational representations on the tangent spaces (in case m is already known).

In fact already in Lemma 4.1 of [**5**] (p. 10), it was shown that an upper bound $Cm^{1/2}$ is possible; in the statement it is assumed that E, E' are defined over the field $\overline{\mathbf{Q}}$ of algebraic numbers, and then C depends also on certain heights $h(E), h(E')$ (which we need not define here) as well as the degrees of the fields of definition of E, E'. However on inspection one sees that the proof actually gives

$$\max\{|a|, |b|, |c|, |d|\} \leq C_0 \sqrt{yy'} m^{1/2} \tag{2}$$

without specifying the fields of definition, where y, y' are the imaginary parts of τ, τ' and now C_0 is absolute.

In Lemma 10.3 of David [**1**] (p. 133) in his study of linear forms in elliptic logarithms, the above bound $Cm^{1/2}$ was made completely explicit (and then used by Pellarin to improve the main result of [**5**] above). Again the proof leads to (2), now with $C_0 = 8/3$.

Then in Lemma 5.2 of the work [**4**] (p. 19) of Habegger and Pila going beyond the André-Oort Conjecture it was shown that there are integers a, b, c, d as above with bound $C_1 m^{10}$ in (2); still C_1 is absolute (and easily computable) but there is no longer any dependence on y, y'. When E has no complex multiplication this implies the same bound for any such integers.

And the rather general Theorem 1.1 of Orr [**8**] (p. 455) in an investigation on the Zilber-Pink Conjecture for Shimura varieties - see also the remarks following equation (1) p. 456 - implies an improvement to $C_2 m$ for C_2 absolute (possibly not quite so easily computable in general). The example

$$\tau = i, \ a = m, \ b = c = 0, \ d = 1$$

shows that the exponent of m cannot be reduced and that no bound $< m$, even for m large, is valid. Thus in particular the exponent $1/2$ in (2) is slightly misleading, even though it may appear somewhat natural due to the obvious lower bound

$$\max\{|a|, |b|, |c|, |d|\} \geq 2^{-1/2} m^{1/2}.$$

Nevertheless it is not difficult to show that given any $N \geq 1$ and any exponent with $1/2 < \theta < 1$ the number of quadruples (a, b, c, d) in $\mathbf{Z}^4$ with

$$|ad - bc|^\theta \leq \max\{|a|, |b|, |c|, |d|\} \leq N$$

is at most $220 N^{2+\frac{1}{\theta}}$. As $2 + \frac{1}{\theta} < 4$, we may say that "most of" these quadruples have

$$\max\{|a|, |b|, |c|, |d|\} < m^\theta.$$

Also we may remark that for any $Y \geq 1$ the hyperbolic area of the τ in the fundamental domain with $y \geq Y$ is the fraction $3/(\pi Y)$ of the total area. Thus by (2) we may also say that for "most of" the τ, τ' we have (in some standard measure-theoretical sense)

$$\max\{|a|, |b|, |c|, |d|\} = O(m^{1/2}).$$

More recently in [**6**] during the construction of many abelian varieties over $\overline{\mathbf{Q}}$ not isogenous to jacobians we obtained independently the bound $2m^{3/2}$ (Lemma 2.1 p. 643). And Orr has mentioned the bound $(2/\sqrt{3})m$ in a private communication.

The main purpose of the present note is to obtain the sharpest possible upper bound. Thus we shall prove (no longer mentioning isogenies or even elliptic curves) the following.

T h e o r e m. *If τ, τ' are in the fundamental domain, then any integers a,b,c,d with* (1) *satisfy*

$$\max\{|a|, |b|, |c|, |d|\} \leq ad - bc.$$

The proof is given in section 2. We shall also briefly discuss the situation for abelian varieties in section 3. It will be seen that in general there is no upper bound which depends only on the varieties and the degree of the connecting isogeny; but if we measure the isogeny through Rosati forms the situation improves.

We thank Gabriel Dill for his comments on a first version of this note.

2 - Proof of Theorem

We recall that the standard fundamental domain, or more precisely its closure $\mathcal{F}$, is the set of τ with real part x and imaginary part y satisfying

$$x^2 + y^2 \geq 1, \quad -\frac{1}{2} \leq x \leq \frac{1}{2}. \tag{3}$$

We note $y \geq \sqrt{3}/2$ and so

$$\frac{y^2}{x^2 + y^2} \geq \frac{y^2}{\frac{1}{4} + y^2} \geq \frac{3}{4}. \tag{4}$$

We also need the following

L e m m a. *For $\tau = x + iy$ in $\mathcal{F}$ and all real u, v we have*

$$(ux + v)^2 + u^2 y^2 \geq \frac{y^2}{x^2 + y^2} \max\{u^2, v^2\} \geq \frac{3}{4} \max\{u^2, v^2\}.$$

P r o o f. If $v = 0$ it is easy, because $(x^2 + y^2)^2 = |\tau|^4 \geq |\tau|^2 \geq y^2$ and then we use (4).

Now by homogeneity we may assume $v = 1$, so we have to bound $E = (ux + 1)^2 + u^2y^2$.

If $|u| \geq 1$ then

$$E \geq u^2y^2 \geq \frac{y^2}{x^2 + y^2}u^2 = \frac{y^2}{x^2 + y^2}\max\{u^2, 1\}.$$

If $|u| \leq 1$ then

$$E = (x^2 + y^2)\left(u + \frac{x}{x^2 + y^2}\right)^2 + \frac{y^2}{x^2 + y^2} \geq \frac{y^2}{x^2 + y^2} = \frac{y^2}{x^2 + y^2}\max\{u^2, 1\}.$$

Again by (4) this completes the proof. □

Now let τ, τ' be in the fundamental domain with

$$\tau' = \frac{a\tau + b}{c\tau + d}, \quad ad - bc = m,$$

and write

$$\tau' = x' + iy', \quad \tau = x + iy.$$

We have the well-known

$$y' = \frac{my}{L} \tag{5}$$

for $L = |c\tau + d|^2$. Also for $M = |a\tau + b|^2$ we can verify the identities

$$M = Lx'^2 + \frac{m^2y^2}{L} = L|\tau'|^2.$$

We now begin the estimation of $\max\{|a|, |b|, |c|, |d|\}$, organizing the argument in three stages depending on the size of c.

Suppose first $c = 0$ (this stage will be relatively easy). Then $m = ad$ so at once $|a|, |d| \leq m$. Also

$$M = Lx'^2 + \frac{m^2y^2}{L} = d^2x'^2 + \frac{m^2y^2}{d^2} = d^2x'^2 + a^2y^2 \leq \frac{d^2}{4} + a^2y^2$$

thanks to $|x'| \leq 1/2$. On the other hand $M = (ax + b)^2 + a^2y^2$ so

$$(ax + b)^2 \leq \frac{d^2}{4} \leq \frac{m^2}{4}$$

and then

$$|b| \le \frac{m}{2} + \frac{|a|}{2} \le m$$

giving the bound

$$\max\{|a|, |b|, |c|, |d|\} \le m.$$

Next suppose $|c| = 1$ (this stage contains the key step). We may assume $y \le y'$ because interchanging involves the adjoint matrix with the same $|c|$. We may even suppose $c = 1$. Now (5) leads to

$$m \ge L = (x + d)^2 + y^2$$

and so the Lemma with $u = 1, v = d$ gives

$$|d| \le \max\{1, |d|\} \le \frac{2}{\sqrt{3}}\sqrt{m} < m + 1.$$

If $|d| \ge 1$ then $|x + d| \ge 1/2 \ge |x|$ and this $|x + d| \ge |x|$ holds also for $d = 0$. So $L \ge x^2 + y^2$.

Now

$$M = Lx'^2 + \frac{m^2 y^2}{L} \le \frac{L}{4} + \frac{y^2}{x^2 + y^2} m^2 \le \frac{m}{4} + \frac{y^2}{x^2 + y^2} m^2.$$

This is

$$\frac{y^2}{x^2 + y^2} m^2 \left(1 + \frac{x^2 + y^2}{y^2} \frac{1}{4m}\right) \le \frac{y^2}{x^2 + y^2} m^2 \left(1 + \frac{1}{3m}\right) < \frac{y^2}{x^2 + y^2} m^2 \left(1 + \frac{1}{6m}\right)^2$$

where we used (4). Now the Lemma gives $M \ge (y^2/(x^2 + y^2)) \max\{a^2, b^2\}$ so

$$\max\{|a|, |b|\} < m \left(1 + \frac{1}{6m}\right) = m + \frac{1}{6}$$

and the result.

Finally suppose $|c| \ge 2$ (which happens "most" of the time). Then $L \ge c^2 y^2$ so

$$M = Lx'^2 + \frac{m^2 y^2}{L} \le \frac{L}{4} + \frac{1}{c^2} m^2 \le \frac{M}{4} + \frac{1}{c^2} m^2$$

where we used $1 \le |\tau'|^2 = M/L$. So $L \le M \le 4m^2/3c^2$ and now the Lemma gives the somewhat sharper

$$\max\{|a|, |b|, |c|, |d|\} \le \frac{4}{3|c|} m \le \frac{2}{3} m < m$$

(so also "most" of the time).

3 - Abelian varieties

One cannot expect similar bounds for isogenies between abelian varieties A, A' of dimension $g > 1$. Suppose they are principally polarized, so that the analogues $\mathcal{T}, \mathcal{T}'$ of τ, τ' are in the Siegel upper half space. If we take the period matrices as $(\mathcal{I}, \mathcal{T}), (\mathcal{I}, \mathcal{T}')$ for the identity matrix $\mathcal{I}$, then (1) becomes

$$\mathcal{T}' = (\mathcal{A}\mathcal{T} + \mathcal{B})(\mathcal{C}\mathcal{T} + \mathcal{D})^{-1}$$

with $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ integer square matrices of size g, with the degree of an isogeny (from A to A')

$$m = \det \begin{pmatrix} \mathcal{A} & -\mathcal{B} \\ -\mathcal{C} & \mathcal{D} \end{pmatrix}.$$

Fundamental domains are much more complicated now (see for example Gottschling [**3**] who for $g = 2$ gives 28 inequalities in place of (3) and shows that all are needed), but any reasonable one certainly includes $i\mathcal{I}$. One could also use the Siegel sets, which are liable to be larger.

In fact there is no bound of any form

$$\max\{\|\mathcal{A}\|, \|\mathcal{B}\|, \|\mathcal{C}\|, \|\mathcal{D}\|\} \leq C(A, A', m) \tag{6}$$

involving any matrix norms. For example, with $g = 2$ one can take $A = A' = E^2$ for the elliptic curve E isomorphic to $\mathbf{C}/(\mathbf{Z} + \mathbf{Z}i)$. With the map defined by taking (U, V) in E^2 to $(pU + qV, rU + sV)$ in E^2 for integers p, q, r, s one finds for $\mathcal{T} = \mathcal{T}' = i\mathcal{I}$

$$\mathcal{A} = \mathcal{D} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}, \quad \mathcal{B} = \mathcal{C} = 0 \tag{7}$$

so $m = (ps - qr)^2$ and an isogeny if and only if $ps - qr \neq 0$. So (6) would be bounding the entries of a general integer matrix in terms of its determinant.

The underlying reason here is that the endomorphism ring of E^2 contains the matrix ring $M_2(\mathbf{Z})$, which has units of infinite order (such units are impossible in the endomorphism ring of E). Thus as soon as A contains the square of an abelian variety B, the impossibility of (6) remains. And the same is true even when something isogenous to A contains a B^2.

Thus we may assume that A is (or is even isogenous to) a product $A_1 \times \cdots \times A_k$ for mutually non-isogenous abelian varieties $A_1, \ldots, A_k$. Since an isogeny from A now splits into isogenies from each of the factors, we may consider each factor separately.

For $g = 2$ and $k = 2$ we have two non-isogenous elliptic curves, and it is not hard to see that our Theorem gives a bound $C(A, A')m$ in (6), with a suitable interpretation of fundamental domain.

For $g = 2$ and $k = 1$ we have simple A. The standard classification shows that then the endomorphism algebra of A (and so also A'), if not $\mathbf{Q}$, is a real quadratic field, or a totally imaginary quadratic extension of a real quadratic field, or a totally indefinite quaternion algebra over $\mathbf{Q}$. But these latter all contain a real quadratic field and so units η of infinite order, so different $1, \eta, \eta^2, \ldots$. The corresponding isogenies from A to A all have degree $m = 1$; but a bound (6) would imply at most finitely possibilities for $1, \eta, \eta^2, \ldots$, since the rational representation on endomorphisms is faithful.

If the endomorphism algebra of A is $\mathbf{Q}$, then there is essentially only one polarization on A and A', so all isogenies are automatically polarized. Now the work of [**8**] gives a bound $C_0 m$ in (6) with C_0 absolute if A, A' are already principally polarized.

The situation for $g > 2$ is less clear. For example with $g = 3$ a simple abelian variety can have endomorphism algebra which is an imaginary quadratic field. That rules out units of infinite order; but is (6) still impossible? Or for $g = 4$ we could have a totally definite quaternion algebra over $\mathbf{Q}$, again ruling out units of infinite order.

For general g and endomorphism algebra $\mathbf{Q}$, the work of [**8**] applies as above.

And when the automorphism group of A is finite, Proposition 3.3(ii) (p. 11) of Dill [**2**] implies (6) with a polynomial dependence on m (see Orr [**7**] as well).

But for general g and general endomorphism algebra we know very little. Here it may be worth noting that we could measure an endomorphism of a principally polarized abelian variety not simply by its degree but rather a "length" ℓ coming from the square root of the positive definite quadratic form attached to the Rosati involution. Then in Lemma 4.1 (p. 653) of [**6**] we proved the following analogue of (2), at least for $A = A'$. Namely

$$\max\{\|\mathcal{A}\|, \|\mathcal{B}\|, \|\mathcal{C}\|, \|\mathcal{D}\|\} \leq C(g) y \ell \tag{8}$$

where y is the largest of the diagonal entries of $\mathcal{T}$ (again with a suitable fundamental domain).

Concretely ℓ is the square root of the trace of

$$\begin{pmatrix} \mathcal{A} & -\mathcal{B} \\ -\mathcal{C} & \mathcal{D} \end{pmatrix} \begin{pmatrix} 0 & -\mathcal{I} \\ \mathcal{I} & 0 \end{pmatrix} \begin{pmatrix} \mathcal{A} & -\mathcal{B} \\ -\mathcal{C} & \mathcal{D} \end{pmatrix}^t \begin{pmatrix} 0 & -\mathcal{I} \\ \mathcal{I} & 0 \end{pmatrix}^{-1}$$

for the transpose, and the degree m is the square root of the determinant. For example with $g = 2$ we have

$$\frac{1}{\sqrt{2}} \ell = \sqrt{a_{11}d_{11} - b_{11}c_{11} + a_{12}d_{12} - b_{12}c_{12} + a_{21}d_{21} - b_{21}c_{21} + a_{22}d_{22} - b_{22}c_{22}}.$$

Thus for (7) we have

$$\frac{1}{\sqrt{2}}\ell = \sqrt{p^2+q^2+r^2+s^2}$$

(whose square is now clearly positive definite) so that in this case (8) holds with upper bound simply $2^{-1/2}\ell$.

We do not know if in general (8) holds with $C(g)\ell$ or even $C(g)\ell^{\kappa(g)}$.

References

[**1**] S. David, *Minorations de formes linéaires de logarithmes elliptiques,* Mém. Soc. Math. France (N.S.) **62** (1995), 143 pp.

[**2**] G. A. Dill, *Unlikely intersections between isogeny orbits and curves,* J. Eur. Math. Soc. (JEMS) **23** (2021), 2405–2438.

[**3**] E. Gottschling, *Explizite Bestimmung der Randflächen des Fundamentalbereiches der Modulgruppe zweiten Grades,* Math. Ann. **138** (1959), 103–124.

[**4**] P. Habegger and J. Pila, *Some unlikely intersections beyond André-Oort,* Compos. Math. **148** (2012), 1–27.

[**5**] D. W. Masser and G. Wüstholz, *Estimating isogenies on elliptic curves,* Invent. Math. **100** (1990), 1–24.

[**6**] D. Masser and U. Zannier, *Abelian varieties isogenous to no Jacobian,* Ann. of Math. **191** (2020), 635–674.

[**7**] M. Orr, *Families of abelian varieties with many isogenous fibres,* J. Reine Angew. Math. **705** (2015), 211–231.

[**8**] M. Orr, *Height bounds and the Siegel property,* Algebra Number Theory **12** (2018), 455–478.

David Masser
Departement Mathematik und Informatik
Universität Basel
Spiegelgasse 1
4051 Basel, Switzerland
e-mail: David.Masser@unibas.ch

Umberto Zannier
Scuola Normale Superiore
Piazza dei Cavalieri 7
56126 Pisa, Italy
e-mail: u.zannier@sns.it