Algebra & Number Theory

Volume 2
2008
No. 3

The intersection of a curve with a union of translated codimension-two subgroups in a power of an elliptic curve

Evelina Viada

mathematical sciences publishers

The intersection of a curve with a union of translated codimension-two subgroups in a power of an elliptic curve

Evelina Viada

Let E be an elliptic curve. An irreducible algebraic curve C embedded in E^g is called weak-transverse if it is not contained in any proper algebraic subgroup of E^g, and transverse if it is not contained in any translate of such a subgroup.

Suppose E and C are defined over the algebraic numbers. First we prove that the algebraic points of a transverse curve C that are close to the union of all algebraic subgroups of E^g of codimension 2 translated by points in a subgroup Γ of E^g of finite rank are a set of bounded height. The notion of closeness is defined using a height function. If Γ is trivial, it is sufficient to suppose that C is weak-transverse.

The core of the article is the introduction of a method to determine the finiteness of these sets. From a conjectural lower bound for the normalized height of a transverse curve C, we deduce that the sets above are finite. Such a lower bound exists for $g \leq 3$.

Concerning the codimension of the algebraic subgroups, our results are best possible.

1. Introduction

Let A be a semiabelian variety over $\overline{\mathbb{Q}}$ of dimension g. An irreducible algebraic subvariety V of A defined over $\overline{\mathbb{Q}}$ is *weak-transverse* if V is not contained in any proper algebraic subgroup of A, and *transverse* if it is not contained in any translate of such a subgroup.

Given an integer r with $1 \leq r \leq g$ and a subset F of $A(\overline{\mathbb{Q}})$, we define the set

$$S_r(V, F) = V(\overline{\mathbb{Q}}) \cap \bigcup_{\text{codim } B \geq r} (B + F),$$

where B runs over all semiabelian subvarieties of A of codimension at least r and

$$B + F = \{b + f : b \in B,\ f \in F\}.$$

MSC2000: primary 11G05; secondary 11D45, 11G50, 14K12.

Keywords: heights, diophantine approximation, elliptic curves, counting algebraic points.

Supported by the SNF (Swiss National Science Foundation).

For $r > g$, we define $S_r(V, F)$ to be the empty set. We denote the set $S_r(V, A_{\mathrm{Tor}})$ simply by $S_r(V)$. Note that

$$S_{r+1}(V, F) \subset S_r(V, F).$$

A natural question to ask would be: For which sets F and integers r is the set $S_r(V, F)$ not Zariski-dense in V?

Sets of this kind, for $r = g$, appear in the literature in the context of the Mordell–Lang, Manin–Mumford and Bogomolov conjectures. More recently Bombieri, Masser and Zannier [Bombieri et al. 1999] proved that $S_2(C)$ is finite for a transverse curve C in a torus. They investigated, for the first time, intersections with the union of all algebraic subgroups of a given codimension. This opens a vast number of conjectures for subvarieties of semiabelian varieties.

In this article we consider the elliptic case for curves. Let E be an elliptic curve and C an irreducible algebraic curve in E^g, both defined over $\overline{\mathbb{Q}}$. Let $\|\cdot\|$ be a seminorm on $E^g(\overline{\mathbb{Q}})$ induced by a height function. For $\varepsilon \geq 0$, we set

$$\mathcal{O}_\varepsilon = \{\xi \in E^g(\overline{\mathbb{Q}}) : \|\xi\| \leq \varepsilon\}.$$

Let $\Gamma \subseteq E^g(\overline{\mathbb{Q}})$ be a subgroup of finite rank. Define $\Gamma_\varepsilon = \Gamma + \mathcal{O}_\varepsilon$.

Conjecture 1.1. *Let $C \subset E^g$.*

(i) *If C is weak-transverse, $S_2(C)$ is finite.*

(ii) *If C is transverse, $S_2(C, \Gamma)$ is finite.*

(iii) *If C is weak-transverse, there exists $\varepsilon > 0$ such that $S_2(C, \mathcal{O}_\varepsilon)$ is finite.*

(iv) *If C is transverse, there exists $\varepsilon > 0$ such that $S_2(C, \Gamma_\varepsilon)$ is finite.*

The transversality hypothesis is crucially stronger than weak transversality. One should note carefully which hypothesis is assumed in each of the four statements.

Clearly (iv) implies (ii) by setting $\varepsilon = 0$, and similarly (iii) implies (i).

The union of all algebraic subgroups of codimension g is exactly the torsion of E^g. Then, $C \cap \Gamma_\varepsilon \subset S_g(C, \Gamma_\varepsilon) \subset S_2(C, \Gamma_\varepsilon)$. So, Conjecture 1.1(iii) implies the Bogomolov Theorem [Ullmo 1998; Zhang 1998], and (iv) implies Mordell–Lang plus Bogomolov [Poonen 1999].

Partial results related to (i) and (ii) have been proved. In [Viada 2003] we solved a weak form of (i), namely we assumed the stronger hypothesis that C is transverse. If E has CM (complex multiplication) then $S_2(C)$ is finite. If E has no CM then $S_{(g/2)+2}(C)$ is finite. In [Rémond and Viada 2003] a weak version of (ii) was presented. Again if E has CM the result is optimal. If E has no CM the codimension of the algebraic subgroups depends on Γ. In addition, we show that (i) and (ii) are equivalent. There are no trivial implications between (iii) and (iv), because of the different hypotheses on C.

These known proofs rely on Northcott's theorem: a set is finite if and only if it has bounded height and degree. To prove that the degree is bounded one uses Siegel's Lemma and an essentially optimal generalized Lehmer's Conjecture. Up to a logarithmic factor, the generalized Lehmer conjecture is presently known for a point in a torus [Amoroso and David 1999] and in a CM abelian variety [David and Hindry 2000]. This method has some disadvantages: it is only known to work for transverse curves and for $\varepsilon = 0$, and a quasioptimal generalized Lehmer's Conjecture is not likely to be proved in a near future for a general abelian variety.

In this article we introduce a different method. First, we bound the height also for weak-transverse curves.

Theorem 1.2. *There exists* $\varepsilon > 0$ *such that*:

(i) *If* C *is weak-transverse*, $S_2(C, \mathcal{O}_\varepsilon)$ *has bounded height.*

(ii) *If* C *is transverse*, $S_2(C, \Gamma_\varepsilon)$ *has bounded height.*

The proof of both statements uses a Vojta inequality, as stated in Proposition 2.1 of [Rémond and Viada 2003]. The second assertion is proved in Theorem 1.5 of the same paper. To prove the first assertion (see Section 7), we embed $S_2(C, \mathcal{O}_\varepsilon)$ into two sets associated to a transverse curve. We then manage to apply a Vojta inequality on each of these two sets.

As a second result, we prove:

Theorem 1.3. *For* $r \geq 2$, *the following statements are equivalent*:

(i) *If* C *is weak-transverse*, *there exists* $\varepsilon > 0$ *such that* $S_r(C, \mathcal{O}_\varepsilon)$ *is finite.*

(ii) *If* C *is transverse*, *there exists* $\varepsilon > 0$ *such that* $S_r(C, \Gamma_\varepsilon)$ *is finite.*

That (i) implies (ii) is elementary, but the converse implication is not as easy as the equivalence of (i) and (ii) in Conjecture 1.1. In particular we make use of Theorem 1.2 (see Section 7).

In the third instance, we show how to avoid the use of the Siegel Lemma and the generalized Lehmer Conjecture. Instead, we use Dirichlet's Theorem and a conjectural effective version of the Bogomolov Theorem. Bogomolov's Theorem states that the set of points of small height on a curve of genus at least 2 is finite. We define $\mu(C)$ as the supremum of the reals $\epsilon(C)$ such that $S_g(C, \mathcal{O}_{\epsilon(C)}) = C \cap \mathcal{O}_{\epsilon(C)}$ is finite. The essential minimum of C is $\mu(C)^2$. (Often in the literature the notation $\mathcal{O}_\varepsilon$ corresponds to what we write as $\mathcal{O}_{\varepsilon^2}$; thus in the references given below the bounds are given for the essential minimum and not for its square root $\mu(C)$ as we do here.)

Nonoptimal effective lower bounds for $\mu(C)$ are given by S. David and P. Philippon [2002, Theorem 1.4; 2007, Theorem 1.6]. The lower bound we need is the elliptic analogue of [Amoroso and David 2003, Theorem 1.4], which gives a quasioptimal lower bound for the essential minimum of a variety.

The following conjecture is a weak form of [David and Philippon 2007, Conjecture 1.5(ii)] where the line bundle is fixed.

Conjecture 1.4. *Let $A = E_1 \times \cdots \times E_g$ be a product of elliptic curves defined over a number field k. Let L be the tensor product of the pullbacks of symmetric line bundles on E_i via the natural projections. Let $C \subset A$ be an irreducible transverse curve defined over $\overline{\mathbb{Q}}$. Let η be any positive real. Then there exists a constant $c(g, A, \eta) = c(g, \deg_L A, h_L(A), [k : \mathbb{Q}], \eta)$ such that, for*

$$\epsilon(C, \eta) = c(g, A, \eta)(\deg_L C)^{-1/(2(g-1))-\eta},$$

the set

$$C(\overline{\mathbb{Q}}) \cap \mathcal{O}_{\epsilon(C,\eta)}$$

is finite.

In Section 11, we prove:

Theorem 1.5. *Conjecture 1.4 implies Conjecture 1.1.*

Conjecture 1.4 can be stated for subvarieties of A. Galateau [2007] proved that such a conjecture holds for varieties of codimension 1 or 2 in a product of elliptic curves. Then, for $g \leq 3$, Conjecture 1.1 holds unconditionally.

Theorems 1.2 and 1.5 are optimal with respect to the codimension of the algebraic subgroups; see Remark 9.2.

We have already pointed out that Conjecture 1.1 implies the Bogomolov Conjecture and the Mordell–Lang plus Bogomolov Theorem. Let us emphasize that our Theorem 1.5 does not give a new proof of the Bogomolov Conjecture, as we assume such an effective result. On the other hand, it gives a new proof of the Mordell–Lang plus Bogomolov Theorem, under the assumption of Conjecture 1.4.

The proof of Theorem 1.5 is based on the observation that a union of sets is finite if and only if

(1) the union can be taken over finitely many sets, and

(2) all sets in the union are finite.

Showing (1) is a typical problem of Diophantine approximation. The proof relies on Dirichlet's Theorem on the rational approximation of reals. The fact that we consider small neighborhoods enables us to move the algebraic subgroups "a bit". So we can consider only subgroups of bounded degree, of which there are finitely many; see Proposition A, Section 12.

Step (2) takes place in the context of height theory. Its proof relies on Conjecture 1.4. The bound $\epsilon(C, \eta)$ depends on the invariants of the ambient variety and on the degree of C. A weaker dependence on the degree of C would not be enough for our application. Also the independence of the bound from the field of definition of C proves useful. Playing on Conjecture 1.4, we produce a sharp lower bound for the essential minimum of the image of a curve under certain morphisms (see Proposition B and Section 13).

The effectiveness aspect of our method is noteworthy; the use of a Vojta inequality makes Theorem 1.2, and consequently Theorem 1.5, ineffective. Though, the rest of the method is effective. Indeed, in Section 14, we prove a weaker, but effective analogue of Theorem 1.5.

Theorem 1.6. *Assume Conjecture 1.4. If C is transverse, there exists an effective $\varepsilon > 0$ such that the set $S_2(C, \mathcal{O}_\varepsilon)$ is finite.*

A bound for the number of points of small height on the curve would then imply a bound on the cardinality of $S_2(C, \mathcal{O}_\varepsilon)$ for C transverse and ε small (Theorem 14.3).

The toric version of Theorem 1.6 was independently studied by P. Habegger in his Ph.D. thesis [2007]. He follows the idea of using a Bogomolov-type bound, proved in the toric case in [Amoroso and David 2003, Theorem 1.4]. He proves the finiteness of $S_2(C, \mathcal{O}_\epsilon)$, for $\epsilon > 0$ and C a transverse curve in a torus.

2. Preliminaries

Morphisms and their height. Let $(R, |\cdot|)$ be a hermitian ring, that means R is a domain and $|\cdot|$ an absolute value on R.

We denote by $M_{r,g}(R)$ the module of $r \times g$ matrices with entries in R.

For $F = (f_{ij}) \in M_{r,g}(R)$, we define the height of F as the maximum of the absolute value of its entries

$$H(F) = \max_{ij} |f_{ij}|.$$

Let E be an elliptic curve defined over a number field. The ring of endomorphism $\mathrm{End}\, E$ is isomorphic either to $\mathbb{Z}$ (if E does not have CM) or to an order in an imaginary quadratic field (if E has CM). We consider on $\mathrm{End}\, E$ the standard absolute value of $\mathbb{C}$. This absolute value does not depend on the embedding of $\mathrm{End}\, E$ in $\mathbb{C}$. An intrinsic definition of absolute value on $\mathrm{End}\, E$ can be given using the Rosati involution.

We identify a morphism $\phi : E^g \to E^r$ with a matrix in $M_{r,g}(\mathrm{End}\, E)$. The set of morphisms of height bounded by a constant is finite.

In the following, we aim to be as transparent as possible, polishing statements from technicality. Therefore, we principally present proofs for E without CM Then $\mathrm{End}\, E$ is identified with $\mathbb{Z}$ and a morphism ϕ with an integral matrix. In the final section, we explain how to deal with the technical complication of a ring of endomorphisms of rank 2 and with a product of elliptic curves instead of a power.

Small points. On E, we fix a symmetric very ample line bundle $\mathscr{L}$. On E^g, we consider the bundle L which is the tensor product of the pullbacks of $\mathscr{L}$ via the natural projections on the factors. Degrees are computed with respect to the polarization L.

Usually $E^g(\overline{\mathbb{Q}})$ is endowed with the L-canonical Néron–Tate height h'. Though, to simplify constants, we prefer to define on E^g the height of the maximum

$$h(x_1, \dots, x_g) = \max_i(h(x_i)).$$

where $h(\cdot)$ on $E(\overline{\mathbb{Q}})$ is the $\mathscr{L}$-canonical Néron–Tate height. The height h is the square of a norm $\|\cdot\|$ on $E^g(\overline{\mathbb{Q}}) \otimes \mathbb{R}$. For a point $x \in E^g(\overline{\mathbb{Q}})$, we write $\|x\|$ for $\|x \otimes 1\|$.

Note that $h(x) \leq h'(x) \leq gh(x)$. Hence, the two norms induced by h and h' are equivalent.

For $a \in \operatorname{End} E$, we denote by $[a]$ the multiplication by a. For $y \in E^g(\overline{\mathbb{Q}})$ we have

$$\big\| [a]y \big\| = |a| \cdot \|y\|.$$

The height of a nonempty set $S \subset E^g(\overline{\mathbb{Q}})$ is the supremum of the heights of its elements. The norm of S is the nonnegative square root of its height.

For $\varepsilon \geq 0$, we denote

$$\mathcal{O}_\varepsilon = \mathcal{O}_{\varepsilon, E^g} = \{\xi \in E^g(\overline{\mathbb{Q}}) : \|\xi\| \leq \varepsilon\}.$$

Subgroups. Let M be a R-module. The R-rank of M is the supremum of the cardinality of a set of R-linearly independent elements of M. If M has finite rank s, a maximal free set of M is a set of s linearly independent elements of M. If M is a free R-module of rank s, we call a set of s generators of M, integral generators of M.

Note that a free $\mathbb{Z}$-module of finite rank is a lattice; in the literature, what we call integral generators can be called basis, and what we define as maximal free set is a basis of the vector space given by tensor product with the quotient field of R.

We say that $(M, \|\cdot\|)$ is a hermitian R-module if M is an R-module and $\|\cdot\|$ is a norm on the tensor product of M with the quotient field of R. For an element $p \in M$ we write $\|p\|$ for $\|p \otimes 1\|$.

Let E be an elliptic curve. In the following, we will simply say module for an $\operatorname{End} E$-module.

Note that any subgroup of $E^g(\overline{\mathbb{Q}})$ of finite rank is contained in a submodule of finite rank. Conversely, a submodule of E^g of finite rank is a subgroup of finite rank.

Let Γ be a subgroup of finite rank of $E^g(\overline{\mathbb{Q}})$. We define

$$\Gamma_\varepsilon = \Gamma + \mathcal{O}_\varepsilon.$$

The saturated module Γ_0 of the coordinates group of Γ (in short of Γ) is a submodule of $E(\overline{\mathbb{Q}})$ defined as

$$\Gamma_0 = \{\phi(y) \in E \text{ for } \phi : E^g \to E \text{ and } Ny \in \Gamma \text{ with } N \in \mathbb{Z}^*\}. \tag{2-1}$$

Note that $\Gamma_0^g = \Gamma_0 \times \cdots \times \Gamma_0$ is a submodule of E^g invariant via the image or preimage of isogenies. Furthermore, it contains Γ and it is a module of finite rank. Thus to prove finiteness statements for Γ it is enough to prove them for Γ_0^g.

We denote by s the rank of Γ_0. Let $\gamma_1, \ldots, \gamma_s$ be a maximal free set of Γ_0. We denote the associated point of E^s by

$$\gamma = (\gamma_1, \ldots, \gamma_s).$$

For $p = (p_1, \ldots, p_s) \in E^s$ we define Γ_p as the saturated module of $\langle p_1, \ldots, p_s \rangle$.

3. Some geometry of numbers

We present a property from the geometry of numbers and extend it to points of $E^g(\overline{\mathbb{Q}})$. The idea is that, if in $\mathbb{R}^n$ we consider n linearly independent vectors and move them within a "small" angle, they will still be linearly independent. The norm of a linear combination of such vectors depends on the norm of these vectors, on their angles, and on the norm of the coefficients of the combination. Such estimates are frequent in the geometry of numbers.

Lemma 3.1 (compare [Schlickewei 1997, Theorem 1.1; Viada 2003, Lemma 3]). *Every hermitian free $\mathbb{Z}$-module of rank n admits integral generators $\rho_1, \ldots, \rho_n$ such that*

$$c_0(n) \sum_i |\alpha_i|^2 \|\rho_i\|^2 \leq \left\| \sum_i \alpha_i \rho_i \right\|^2$$

for all integers α_i, where $c_0(n)$ is a constant depending only on n.

Proof. A hermitian free $\mathbb{Z}$-module $(\Gamma, \|\cdot\|)$ of rank n is a lattice in the metric space $\Gamma_{\mathbb{R}}$ given by tensor product with $\mathbb{R}$. The proof now follows that of [Viada 2003, Lemma 3] (page 57, from line 19 onwards), with n instead of r and ρ_i instead of g_i. □

This lemma allows us to explicit the comparison constant for two norms on a finite-dimensional vector space over the quotient field of R.

Proposition 3.2. *Let $(M, \|\cdot\|)$ be a hermitian R-module, where R is a finitely generated free $\mathbb{Z}$-module. Let $p_1, \ldots, p_s$ be R-linearly independent elements of M. Then there exists an effective positive constant $c_1(p, \tau)$ such that*

$$c_1(p, \tau) \sum_i |b_i|_R^2 \|p_i\|^2 \leq \left\| \sum_i b_i p_i \right\|^2$$

for all $b_1, \dots, b_s \in R$, *where* $p = (p_1, \dots, p_s)$ *and* $\tau = (1, \tau_2, \dots, \tau_t)$ *are integral generators of* R.

Proof. The submodule of M defined by $\Gamma_{\mathbb{Z}} = \langle p_1, \dots, p_s, \dots, \tau_t p_1, \dots, \tau_t p_s \rangle_{\mathbb{Z}}$ has rank st over $\mathbb{Z}$. Clearly, for $1 \le i \le t$ and $1 \le j \le s$ the elements $\tau_i p_j$ are integral generators of $\Gamma_{\mathbb{Z}}$. Consider the normed space $(M \otimes_{\mathbb{Z}} \mathbb{R}, \|\cdot\|)$, in which $\Gamma_{\mathbb{Z}}$ is embedded, and endow $\Gamma_{\mathbb{Z}}$ with the induced metric.

Apply Lemma 3.1 to $(\Gamma_{\mathbb{Z}}, \|\cdot\|)$ with $n = st$. Then, there exist integral generators $\rho_1, \dots, \rho_{st}$ of $\Gamma_{\mathbb{Z}}$ satisfying

$$\Big\|\sum_i \alpha_i \rho_i\Big\|^2 \ge c_0(st) \sum_i |\alpha_i|^2 \|\rho_i\|^2 \ge c_0(st) \sum_i |\alpha_i|^2 \min_k \|\rho_k\|^2, \tag{3-1}$$

for all $\alpha_1, \dots, \alpha_{st} \in \mathbb{Z}$.

We decompose the elements $b_1, \dots, b_s \in R$ as

$$b_i = \sum_{j=1}^{t} \alpha_{ij} \tau_j$$

with $\alpha_{ij} \in \mathbb{Z}$. We set

$$\alpha = (\alpha_{11}, \dots, \alpha_{1t}, \dots, \alpha_{s1}, \dots, \alpha_{st}) \in \mathbb{Z}^{st}.$$

Next we write

$$p^\tau = (\tau_1 p_1, \dots, \tau_t p_1, \tau_1 p_2, \dots, \tau_t p_2, \dots, \tau_1 p_s, \dots, \tau_t p_s)^{\mathrm{T}} \in \Gamma_{\mathbb{Z}}^{st},$$
$$\rho = (\rho_1, \dots, \rho_{st})^{\mathrm{T}} \in \Gamma_{\mathbb{Z}}^{st},$$

where the superscript T indicates the transpose, as usual. Let $P \in \mathrm{SL}_{st}(\mathbb{Z})$ be the base change matrix such that

$$p^\tau = P\rho.$$

Then

$$\sum_i b_i p_i = \sum_{ij} \alpha_{ij} \tau_j p_i = \alpha \cdot p^\tau = \alpha \cdot (P\rho) = (\alpha P) \cdot \rho.$$

Passing to the norms and using relation (3-1) with the coefficients $(\alpha_1, \dots, \alpha_{st}) = \alpha P$, we deduce

$$\Big\|\sum_i b_i p_i\Big\|^2 = \|(\alpha P) \cdot \rho\|^2 \ge c_0(st) |\alpha P|_2^2 \min_k \|\rho_k\|^2,$$

where $|\cdot|_2$ is the standard Euclidean norm. On the other hand, the triangle inequality gives

$$|b_i|_R^2 \leq \max_k |\tau_k|_R^2 \Big(\sum_{j=1}^t |\alpha_{ij}| \Big)^2 \leq t \max_k |\tau_k|_R^2 \sum_{j=1}^t |\alpha_{ij}|^2.$$

We deduce

$$\frac{\| \sum_i b_i p_i \|^2}{\sum_i |b_i|_R^2 \| p_i \|^2} \geq \frac{c_0(st)}{t \max_j |\tau_j|_R^2} \frac{\min_i \|\rho_i\|^2}{\max_i \|p_i\|^2} \frac{|\alpha P|_2^2}{|\alpha|_2^2}.$$

We shall still estimate $|\alpha P|_2^2 / |\alpha|_2^2$ independently of α. For a linear operator A and a row vector β, there holds the classical norm relation $|\beta A|_2 \leq H(A)|\beta|_2$. For $A = P^{-1}$ and $\beta = \alpha P$, we deduce

$$\frac{|\alpha P|_2^2}{|\alpha|_2^2} \geq \frac{1}{H(P^{-1})^2}.$$

Then

$$\frac{\| \sum_i b_i p_i \|^2}{\sum_i |b_i|_R^2 \| p_i \|^2} \geq \frac{c_0(st)}{t \max_j |\tau_j|_R^2} \frac{\min_i \|\rho_i\|^2}{\max_i \|p_i\|^2} \frac{1}{H(P^{-1})^2}$$

or equivalently

$$\Big\| \sum b_i p_i \Big\|^2 \geq c_1(p, \tau) \sum_i |b_i|_R^2 \| p_i \|^2,$$

where

$$c_1(p, \tau) = \frac{c_0(st)}{t \max_j |\tau_j|_R^2} \frac{\min_i \|\rho_i\|^2}{\max_i \|p_i\|^2} \frac{1}{H(P^{-1})^2}. \qquad \square$$

The following unsurprising proposition has some surprising implications; it allows us to prove Theorems 1.2 and 1.3.

Proposition 3.3. *Let $p_1, \dots, p_s$ be linearly independent points of $E(\overline{\mathbb{Q}})$ and $p = (p_1, \dots, p_s)$. Let τ be a set of integral generators of* End E. *Then, there exist positive reals $c_2(p, \tau)$ and $\varepsilon_0(p, \tau)$ such that*

$$c_2(p, \tau) \sum_i |b_i|^2 \|p_i\|^2 \leq \Big\| \sum_i b_i (p_i - \xi_i) - b\zeta \Big\|^2$$

for all $b_1, \dots, b_s, b \in$ End E with $|b| \leq \max_i |b_i|$ and for all $\xi_1, \dots, \xi_s, \zeta \in E(\overline{\mathbb{Q}})$ with $\|\xi_i\|, \|\zeta\| \leq \varepsilon_0(p, \tau)$.

In particular $p_1 - \xi_1, \dots, p_s - \xi_s$ are linearly independent points of E.

Proof. Recall that the norm on End E is compatible with the height norm on $E(\overline{\mathbb{Q}})$, that is, $\|b_i p_i\| = |b_i|_{\mathrm{End}\, E} \|p_i\|$. Thus (End E, $|\cdot|$) is a hermitian free $\mathbb{Z}$-module of rank 1 if E has no CM or 2 is E has CM. Furthermore, $(E, \|\cdot\|)$ is a hermitian End E-module.

Apply Proposition 3.2 with $R = \operatorname{End} E$, $M = E$ and $\tau = (1)$ if $\operatorname{End} E \cong \mathbb{Z}$ or $\tau = (1, \tau_2)$ if $\operatorname{End} E \cong \mathbb{Z} + \tau_2\mathbb{Z}$. For $b_1, \dots, b_s \in \operatorname{End} E$, we obtain

$$\Bigl\|\sum b_i p_i\Bigr\|^2 \geq c_1(p,\tau) \sum_i |b_i|^2 \|p_i\|^2. \tag{3-2}$$

Let $\|\xi_i\|, \|\zeta\| \leq \varepsilon$. Since $|b| \leq \max |b_i|$ the triangle inequality implies

$$\begin{aligned}\Bigl\|\sum_i b_i(p_i - \xi_i) - b\zeta\Bigr\| &\geq \Bigl\|\sum_i b_i p_i\Bigr\| - \varepsilon \sum_i |b_i| - \varepsilon|b| \\ &\geq \Bigl\|\sum_i b_i p_i\Bigr\| - 2\varepsilon \sum_i |b_i|.\end{aligned}$$

Squaring and keeping in mind that $\bigl(\sum_{i=1}^s |b_i|\bigr)^2 \leq s \sum_{i=1}^s |b_i|^2$, we deduce

$$\begin{aligned}\Bigl\|\sum_i b_i(p_i - \xi_i) - b\zeta\Bigr\|^2 &\geq \Bigl\|\sum_i b_i p_i\Bigr\|^2 - 4\varepsilon\Bigl\|\sum_i b_i p_i\Bigr\|\sum_i |b_i| + 4\varepsilon^2\Bigl(\sum_i |b_i|\Bigr)^2 \\ &\geq \Bigl\|\sum_i b_i p_i\Bigr\|^2 - 4s\varepsilon\Bigl(\sum_i |b_i|^2\Bigr)\max_i \|p_i\|.\end{aligned}$$

Choose

$$\varepsilon \leq \varepsilon_0(p,\tau) = \frac{c_1(p,\tau)}{8s}\,\frac{\min_i \|p_i\|^2}{\max_i \|p_i\|}. \tag{3-3}$$

Using relation (3-2), we deduce

$$\begin{aligned}\Bigl\|\sum_i b_i(p_i - \xi_i) - b\zeta\Bigr\|^2 &\geq c_1(p,\tau)\sum_i |b_i|^2\|p_i\|^2 - \tfrac{1}{2}c_1(p,\tau)\Bigl(\sum_i |b_i|^2\Bigr)\min_i \|p_i\|^2 \\ &\geq \tfrac{1}{2}c_1(p,\tau)\sum_i |b_i|^2\|p_i\|^2.\end{aligned}$$

Set, for example,

$$c_2(p,\tau) = \tfrac{1}{2}c_1(p,\tau), \tag{3-4}$$

where $c_1(p,\tau)$ is defined at the end of the previous proof (page 257).

The preceding relation, with $b = 0$, implies in particular that only the trivial linear combination of $p_1 - \xi_1, \dots, p_s - \xi_s$ is zero. □

We next state a lemma that will enable us to choose a nice maximal free set of Γ_0, the saturated module of a submodule Γ of $E(\overline{\mathbb{Q}})$ of finite rank, as defined in relation (2-1). There is nothing deep here, as we are working with finite-dimensional vector spaces.

Lemma 3.4 (Quasiorthonormality). *Let Γ_0 be the saturated module of Γ. Let s be the rank of Γ_0. Then for any real $K > 0$, there exists a maximal free set $\gamma_1, \dots, \gamma_s$ of Γ_0, with $\|\gamma_i\| \geq K$, such that for all $b_1, \dots, b_s \in \operatorname{End} E$*

$$\left\| \sum_i b_i \gamma_i \right\|^2 \geq \frac{1}{9} \sum_i |b_i|^2 \|\gamma_i\|^2.$$

Proof. Recall that End E is an order in an imaginary quadratic field k. Furthermore, the height norm $\|\cdot\|$ makes Γ_0 a hermitian End E-module. Let Γ^{free} be a submodule of Γ_0 isomorphic to its free part. Then Γ^{free} is a k vector space of dimension s. Its tensor product with $\mathbb{C}$ over k is a normed $\mathbb{C}$ vector space of dimension s, and Γ^{free} is isomorphic to $\Gamma^{\text{free}} \otimes 1$. Using for instance the Gram–Schmidt orthonormalization algorithm in $\Gamma^{\text{free}} \otimes_k \mathbb{C}$, we can choose an orthonormal basis

$$v_i = g_i \otimes \rho_i.$$

So

$$\left\| \sum_i b_i v_i \right\|^2 = \sum_i |b_i|^2.$$

Decompose $\rho_i = r_{i1} + \tau r_{i2}$ for $1, \tau$ integral generators of End E and $r_{ij} \in \mathbb{R}$. Choose $\delta = (2(1 + |\tau|) \max_i \|g_i\|)^{-1}$ and rationals q_{ij} such that $q_{ij} = r_{ij} + d_{ij}$ with $|d_{ij}| \leq \delta$ (use the density of the rationals).

Define

$$\gamma_i' = g_i \otimes (q_{i1} + \tau q_{i2}) = (q_{i1} + \tau q_{i2}) g_1 \otimes 1 \in \Gamma^{\text{free}} \otimes 1,$$

and

$$\delta_i = g_i \otimes (d_{i1} + \tau d_{i2}).$$

Then $v_i = \gamma_i' + \delta_i$, with $\|\delta_i\| \leq \|g_i\|(1 + |\tau|)\delta \leq \frac{1}{2}$. The triangle inequality gives

$$2 \left\| \sum_i b_i \gamma_i' \right\|^2 \geq \left\| \sum_i b_i v_i \right\|^2 - 2 \left\| \sum_i b_i \delta_i \right\|^2.$$

The orthonormality of v_i and $\|\delta_i\| \leq \frac{1}{2}$ implies that

$$2 \left\| \sum_i b_i \gamma_i' \right\|^2 \geq \sum_i |b_i|^2 - 2 \sum_i |b_i|^2 \frac{1}{4} = \frac{1}{2} \sum_i |b_i|^2.$$

Finally $\|\gamma_i'\| \leq \|v_i\| + \|\delta_i\| \leq \frac{3}{2}$, so

$$\left\| \sum_i b_i \gamma_i' \right\|^2 \geq \frac{1}{9} \sum_i |b_i|^2 \|\gamma_i'\|^2.$$

It is evident that for any integer n_0 the same relation holds:

$$\left\| \sum_i b_i n_0 \gamma_i' \right\|^2 \geq \frac{1}{9} \sum_i |b_i|^2 \| n_0 \gamma_i' \|^2.$$

Let n_0 be an integer such that $n_0 \geq 2K$. Note that

$$\|\gamma_i'\| \geq \|v_i\| - \|\delta_i\| \geq \tfrac{1}{2},$$

so

$$\|n_0 \gamma_i'\| \geq K.$$

Thus the maximal free set $\gamma_i = n_0 \gamma_i'$ satisfies the desired conditions. □

We cannot directly choose an orthonormal basis in Γ^{free}, because the norm has values in $\mathbb{R}$ and not in $\mathbb{Q}$. What one can prove is that for any small positive real δ, there exists a maximal free set $\gamma_1, \ldots, \gamma_s$ such that

$$\left\| \sum_i b_i \gamma_i \right\|^2 \geq \frac{(1-\delta)^2}{(1+\delta)^2} \sum_i |b_i|^2 \| \gamma_i \|^2.$$

4. Gauss-reduced morphisms

The aim of this section is to show that we can consider our union over Gauss-reduced algebraic subgroups, instead of over all algebraic subgroups.

Let B be an algebraic subgroup of E^g of codimension r. Then $B \subset \ker \phi_B$ for a surjective morphism $\phi_B : E^g \to E^r$. Conversely, we denote by B_ϕ the kernel of a surjection $\phi : E^g \to E^r$. Then B_ϕ is an algebraic subgroup of E^g of codimension r.

The matrices in $M_{r \times g}(\operatorname{End} E)$ of the form

$$\phi = (aI_r | L) = \begin{pmatrix} a & \ldots & 0 & a_{1,r+1} & \ldots & a_{1,g} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \ldots & a & a_{r,r+1} & \ldots & a_{r,g} \end{pmatrix},$$

with $H(\phi) = |a|$ and entries having no common factors (up to units), will play a key role in this work. For $r = g$, such a morphism becomes the identity, and L shall be forgotten. These matrices have three main advantages:

- The restriction of ϕ to the set $E^r \times \{0\}^{g-r}$ is just the multiplication by a.
- The image of $\mathcal{O}_\varepsilon \subset E^g$ under ϕ is contained in the image of $\mathcal{O}_{g\varepsilon} \cap (E^r \times \{0\}^{g-r})$. Similarly, the image of Γ_0^g under ϕ is contained in the image of $\Gamma_0^r \times \{0\}^{g-r}$.
- The matrix ϕ has small height compared to other matrices with same zero component of the kernel.

Definition 4.1 (Gauss-reduced morphisms). We say that a surjective morphism $\phi : E^g \to E^r$ is Gauss-reduced of rank r if the following conditions are satisfied:

(i) There exists $a \in (\mathrm{End}\, E)^*$ such that aI_r is a submatrix of ϕ, with I_r the r-identity matrix.

(ii) $H(\phi) = |a|$.

(iii) If there exists $f \in \mathrm{End}\, E$ and $\phi' : E^g \to E^r$ such that $\phi = f\phi'$ then f is an isomorphism.

We say that an algebraic subgroup is Gauss-reduced if it is the kernel of a Gauss-reduced morphism.

Remark 4.2. If $\mathrm{End}\, E \cong \mathbb{Z}$, condition (iii) simply says that the greatest common divisor of the entries of ϕ is 1 and $f = \pm 1$. Also when $\mathrm{End}\, E \cong \mathbb{Z}$, we make condition (ii) more restrictive, requiring that $H(\phi) = a$, instead of $H(\phi) = |a|$; this assumption simplifies the notation. Obviously $B_\phi = B_{-\phi}$, so all lemmas below hold with this "up to units" definition of Gauss-reduced.

A morphism ϕ' given by a reordering of the rows of a morphism ϕ, has the same kernel as ϕ. Saying that aI_r is a submatrix of ϕ fixes one permutation of the rows of ϕ.

A reordering of the columns, on the other hand, corresponds to a permutation of the coordinates. Statements will be proved for Gauss-reduced morphisms of the form $\phi = (aI|L)$. For any other reordering of the columns the proofs are analogous. Since there are finitely many permutations of g columns, the finiteness statements will follow.

The following lemma is a simple useful trick to keep in mind.

Lemma 4.3. *Let $\phi : E^g \to E^r$ be Gauss-reduced of rank r.*

(i) *For $\xi = (\xi_1, \dots, \xi_g) \in \mathcal{O}_\varepsilon$, there exists a point $\xi' = (\xi'', \{0\}^{g-r}) \in \mathcal{O}_{g\varepsilon}$ such that*
$$\phi(\xi) = \phi(\xi') = [a]\xi''.$$

(ii) *For $y = (y_1, \dots, y_g) \in \Gamma_0^g$, there exists a point $y' = (y'', \{0\}^{g-r}) \in \Gamma_0^r \times \{0\}^{g-r}$ such that*
$$\phi(y) = \phi(y') = [a]y''.$$

Proof. Up to a reordering of the columns, the morphism ϕ has the form

$$\phi = \begin{pmatrix} a & \dots & 0 & a_{1,r+1} & \dots & a_{1,g} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & a & a_{r,r+1} & \dots & a_{r,g} \end{pmatrix},$$

with $H(\phi) = |a|$.

(i) Consider a point $\xi'' \in E^r$ such that $[a]\xi'' = \phi(\xi)$. Since

$$\|\xi''\| = \frac{\|\phi(\xi)\|}{|a|} = \max_i \frac{\left\|\sum_j a_{ij}\xi_j\right\|}{|a|}$$

and $|a| = \max_{ij} |a_{ij}|$, we obtain

$$\|\xi''\| \leq g\varepsilon.$$

Define $\xi' = (\xi'', \{0\}^{g-r})$. Clearly

$$\phi(\xi') = [a]\xi'' = \phi(\xi).$$

(ii) Note that $\phi(y) \in \Gamma_0^r$. Since Γ_0 is a division group, the point y'' such that

$$[a]y'' = \phi(y),$$

belongs to Γ_0^r. Define $y' = (y'', \{0\}^{g-r})$. Then $\phi(y') = [a]y'' = \phi(y)$. □

In the next result we show that the zero components of B_ϕ, for ϕ ranging over all Gauss-reduced morphisms of rank r, are all possible abelian subvarieties of E^g of codimension r. This is proved using the classical Gauss algorithm, where the pivots have maximal absolute values.

Lemma 4.4. *Let $\psi : E^g \to E^r$ be a morphism of rank r. Then*:

(i) *For every $N \in \operatorname{End} E^*$,*

$$B_{N\psi} \subset B_\psi + (E^r_{\mathrm{Tor}} \times \{0\}^{g-r}).$$

(ii) *There exists a Gauss-reduced morphism $\phi : E^g \to E^r$ of rank r such that*

$$B_\psi \subset B_\phi + (E^r_{\mathrm{Tor}} \times \{0\}^{g-r}).$$

Proof. (i) Let $b \in B_{N\psi}$. Then $N\psi(b) = 0$, so $\psi(b) = t$ with t a N-torsion point in E^r. Let ψ_1 be an invertible r-submatrix of ψ. Up to a reordering of the columns, we can suppose $\psi = (\psi_1|\psi_2)$. Let t' be a torsion point in E^r such that $\psi_1(t') = t$. Then $\psi(b - (t', 0)) = 0$. Thus $b \in B_\psi + (E^r_{\mathrm{Tor}} \times \{0\}^{g-r})$.

(ii) The Gauss algorithm gives an invertible integral r-matrix Δ such that, up to the order of the columns, $\Delta\psi$ is of the form

$$\Delta\psi = \begin{pmatrix} a & \dots & 0 & a_{1,r+1} & \dots & a_{1,g} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & a & a_{r,r+1} & \dots & a_{r,g} \end{pmatrix},$$

with $H(\Delta\psi) = |a|$ (potentially there are common factors of the entries).

Let $b \in B_\psi$. Then $\psi(b) = 0$, so $\Delta\psi(x) = 0$. It follows that

$$B_\psi \subset B_{\Delta\psi}.$$

Take $N \in \operatorname{End} E^*$ such that $N|\Delta\psi$ and such that if $f|(\Delta\psi/N)$ then f is a unit (if $\operatorname{End} E \cong \mathbb{Z}$, then N is simply the greatest common divisor of the entries of $\Delta\psi$). Define

$$\phi = \Delta\psi/N.$$

Clearly ϕ is Gauss-reduced and $B_\psi \subset B_{\Delta\psi} = B_{N\phi}$. By part (i) of this lemma applied to $N\phi$, we conclude

$$B_\psi \subset B_\phi + (E^r_{\mathrm{Tor}} \times \{0\}^{g-r}). \qquad \square$$

Note that, in the previous lemma, a reordering of the columns of ψ or ϕ induces the same reordering of the coordinates of $E^r_{\mathrm{Tor}} \times \{0\}^{g-r}$.

Taking intersections with the algebraic points of our curve, part (ii) of the previous lemma translates immediately as

Lemma 4.5. *Let $C \subset E^g$ be an algebraic curve* (*transverse or not*). *For any real $\varepsilon \geq 0$*

$$S_r(C, (\Gamma_0^g)_\varepsilon) = \bigcup_{\substack{\phi \text{ Gauss-reduced} \\ \mathrm{rk}(\phi)=r}} C(\overline{\mathbb{Q}}) \cap (B_\phi + (\Gamma_0^g)_\varepsilon).$$

Proof. By definition

$$S_r(C, (\Gamma_0^g)_\varepsilon) \supseteq \bigcup_{\substack{\phi \text{ Gauss-reduced} \\ \mathrm{rk}(\phi)=r}} C(\overline{\mathbb{Q}}) \cap (B_\psi + (\Gamma_0^g)_\varepsilon).$$

On the other hand, by Lemma 4.4(ii), we see that

$$C(\overline{\mathbb{Q}}) \cap (B_\psi + (\Gamma_0^g)_\varepsilon) \subset C(\overline{\mathbb{Q}}) \cap (B_\phi + (E^r_{\mathrm{Tor}} \times \{0\}^{g-r}) + (\Gamma_0^g)_\varepsilon),$$

with ϕ Gauss-reduced of rank r. Moreover $(E^r_{\mathrm{Tor}} \times \{0\}^{g-r}) \subset \mathcal{O}_\varepsilon \subset (\Gamma_0^g)_\varepsilon$. $\square$

5. Relation between transverse and weak-transverse curves

We discuss here how we can associate to a couple (C, Γ), where C is a transverse curve and Γ a subgroup of finite rank, a weak-transverse curve C' and vice versa. There are properties which are easier for C and others for C'. Using this association, we will try to gain advantages from both situations.

From transverse to weak-transverse. Let C be transverse in E^g. If Γ has rank 0, we set $C' = C$. If $\mathrm{rk}\,\Gamma \geq 1$, consider the saturated module Γ_0 of rank s associated to Γ, as defined in relation (2-1). Let $\gamma_1, \dots, \gamma_s$ be a maximal free set of Γ_0. We denote the associated point of E^s by

$$\gamma = (\gamma_1, \dots, \gamma_s).$$

We define

$$C' = C \times \gamma.$$

Since C is transverse and the γ_i are End E-linearly independent, the curve C' is weak-transverse. For suppose to the contrary that C' were contained in an algebraic subgroup B_ϕ of codimension 1, with $\phi = (a_1, \dots, a_{g+s})$. Take a point $y_1 \in E$ such that $a_1 y_1 = \sum_{i=g+1}^{g+s} a_i \gamma_{i-g}$ and define $y = (y_1, 0, \dots, 0) \in E^g$. Then $C \subset B_{\phi_1} + y$ with $\phi_1 = (a_1, \dots, a_g)$, contradicting that C is transverse.

From weak-transverse to transverse. Let C' be weak-transverse in E^n. If C' is transverse, we set $C = C'$ and $\Gamma = 0$. Suppose that C' is not transverse. Let H_0 be the abelian subvariety of smallest dimension g such that $C' \subset H_0 + p$ for $p \in H_0^\perp(\overline{\mathbb{Q}})$ and let $H_0^\perp$ be the orthogonal complement of H_0 with respect to the canonical polarization. Then E^n is isogenous to $H_0 \times H_0^\perp$. Furthermore H_0 is isogenous to E^g and $H_0^\perp$ is isogenous to E^s, where $s = n - g$. Let j_0, j_1 and j_2 be such isogenies. We fix the isogeny

$$j = (j_1 \times j_2) \circ j_0 : E^n \to H_0 \times H_0^\perp \to E^g \times E^s,$$

which sends H_0 to $E^g \times 0$ and $H_0^\perp$ to $0 \times E^s$. Then

$$j(C') \subset (E^g \times 0) + j(p),$$

with $j(p) = (0, \dots, 0, p_1, \dots, p_s)$.

We consider the natural projection on the first g coordinates

$$\pi : E^g \times E^s \to E^g, \quad j(C') \mapsto \pi(j(C')).$$

We define

$$C = \pi(j(C')) \text{ and } \Gamma = \langle p_1, \dots, p_s \rangle^g.$$

Since H_0 has minimal dimension, the curve C is transverse in E^g.

Note that

$$j(C') = C \times (p_1, \dots, p_s).$$

In addition $j(C')$ is weak-transverse, because C' is. Therefore, $\langle p_1, \dots, p_s \rangle$ has rank s; indeed if $\sum_{i=1}^s a_i p_i = 0$, then $j(C') \subset B_\phi$ for $\phi = (\{0\}^g, a_1, \dots, a_s)$.

Weak-transverse up to an isogeny. Statements on boundedness of heights or finiteness of sets are invariant under an isogeny of the ambient variety. Namely, given an isogeny j of E^g, Theorems 1.2 and 1.5 hold for a curve if and only if they hold for its image via j. Thus, the previous discussion shows that without loss of generality, we can assume that a weak-transverse curve C' in E^n is of the form

$$C' = C \times p,$$

where

(i) C is transverse in E^g,

(ii) $p=(p_1,\dots,p_s)\in E^s$ is such that the module $\langle p_1,\dots,p_s\rangle$ has rank s, and

(iii) $n=g+s$.

This simplifies the setting for weak-transverse curves.

Implying Mordell–Lang plus Bogomolov for curves. Note that

$$S_g(C,\mathcal{O}_\varepsilon)=C\cap\mathcal{O}_\varepsilon \quad \text{and} \quad S_g(C(\Gamma_0^g)_\varepsilon)=C\cap(\Gamma_0^g)_\varepsilon.$$

Moreover $S_2(C,\cdot)\supset S_g(C,\cdot)$. This immediately shows that Conjecture 1.1 implies the Bogomolov Theorem for weak-transverse curves and the Mordell–Lang and Bogomolov Theorems for transverse curves. We want to show that Conjecture 1.1 implies these theorems for all curves of genus ≥ 2.

In E^g a curve of genus 2 is a translate of an elliptic curve isogenous to E. If C is not transverse, then $C\subsetneq H_0+p$ with H_0 an algebraic subgroup of minimal dimension satisfying such inclusion. Let $\pi:E^g\to E^g/H_0^\perp$ be the natural projection and let $\psi:E^g/H_0^\perp\to E^k$ be an isogeny. Then $\|\psi\pi(x)\|\ll\|x\|$. In E^k, consider the transverse curve $C'=\psi\pi(C-p)$ and $\Gamma'=\psi\pi\langle\Gamma,\Gamma_p\rangle$. Note that $\psi\pi(\mathrm{Tor}_{E^g})\subset\mathrm{Tor}_{E^k}$. Then

$$S_g(C,(\Gamma_0^g)_\varepsilon)\subset\pi_{|C}^{-1}S_k(C',(\Gamma'^g_0)_{\varepsilon'}).$$

The map $\pi_{|C}^{-1}$ has finite fiber. Applying Conjecture 1.1 to $C'\subset E^k$ we deduce that $S_g(C,(\Gamma_0^g)_\varepsilon)$ is finite.

Note that such a proof works only for $S_g(C,\cdot)$, because the projection $\psi\pi(B)\subset E^k$ of an algebraic subgroup B of E^g of codimension r may not have codimension r in E^k. It could even be all of E^k.

6. Quasispecial morphisms

Just as Gauss-reduced morphisms play a key role for transverse curves, quasispecial morphisms play a key role for weak-transverse curves. In particular, for small ε, quasispecial morphisms are enough to cover the whole of $S_r(C\times p,\mathcal{O}_\varepsilon)$; this is Lemma 6.2 below.

To motivate quasispecialness, suppose that $C\times p$ is weak-transverse in E^{g+s} with C transverse in E^g. A point of $C\times p$ is of the form (x,p). The last s-coordinates are constant and just the x varies. This two parts must be treated differently. Saying that a morphism $\tilde\phi=(\phi|\phi')$ is quasispecial ensures that the rank of ϕ is maximal (note that ϕ acts on x). In particular, this allows us to apply the Gauss algorithm on the first g columns of $\tilde\phi$.

Definition 6.1 (Quasispecial morphism). A surjective morphism $\tilde\phi:E^{g+s}\to E^r$ is quasispecial if there exist $N\in\mathrm{End}\,E^*$, morphisms $\phi:E^g\to E^r$ and $\phi':E^s\to E^r$ such that

(i) $\tilde{\phi} = (N\phi|\phi')$,

(ii) $\phi = (aI_r|L)$ is Gauss-reduced of rank r, and

(iii) if there exists $f \in \operatorname{End} E$ and $\tilde{\phi}' : E^{g+s} \to E^r$ such that $\tilde{\phi} = f\tilde{\phi}'$, then f is an isomorphism.

We do not require that $\tilde{\phi}$ be Gauss-reduced; the fact is that $H(\phi')$ might not be controlled by $NH(\phi)$. This extra condition will define special morphisms (see Definition 10.1).

Lemma 6.2. *Let $C \times p$ be weak-transverse in E^{g+s} with C transverse in E^g. Then, there exists $\varepsilon > 0$ such that*

$$S_r(C \times p, \mathcal{O}_\varepsilon) \subset \bigcup_{\substack{\tilde{\phi} \text{ quasispecial} \\ \operatorname{rk} \tilde{\phi} = r}} (C(\overline{\mathbb{Q}}) \times p) \cap (B_{\tilde{\phi}} + \mathcal{O}_\varepsilon).$$

We can choose $\varepsilon \leq \varepsilon_0(p, \tau)$, where $\varepsilon_0(p, \tau)$ is as in Proposition 3.3.

Proof. Take $(x, p) \in S_r(C \times p, \mathcal{O}_\varepsilon)$. Then $(x, p) \in (C(\overline{\mathbb{Q}}) \times p) \cap (B_{\tilde{\psi}} + \mathcal{O}_\varepsilon)$ for a morphism $\tilde{\psi} = (\psi|\psi') : E^{g+s} \to E^r$ of rank r. In other words, there exists a point $(\xi, \xi') \in \mathcal{O}_\varepsilon$ such that

$$\tilde{\psi}((x, p) + (\xi, \xi')) = 0.$$

First, we show that ψ has rank r. Suppose, on the contrary, that the rank of ψ were less than r. Then a linear combination of the rows of ψ is trivial, namely

$$(\lambda_1, \ldots, \lambda_r)\psi = 0.$$

Since $\psi(x+\xi) + \psi'(p+\xi') = 0$, the same linear combination of the r coordinates of $\psi'(p+\xi')$ is trivial, namely

$$(\lambda_1, \ldots, \lambda_r)\psi'(p+\xi') = 0.$$

Apply Proposition 3.3 with $(b_1, \ldots, b_s) = (\lambda_1, \ldots, \lambda_r)\psi'$, $(\xi_1, \ldots, \xi_s) = -\xi'$, $\zeta = 0$ and $b = 0$. This implies that, if $\varepsilon \leq \varepsilon_0(p, \tau)$, then the points $p_1 + \xi_1', \ldots, p_s + \xi_s'$ are linearly independent. It follows that

$$(\lambda_1, \ldots, \lambda_r)\psi' = 0.$$

Hence, the rank of $\tilde{\psi}$ would be less than r, contradicting the fact that the rank of $\tilde{\psi}$ is r.

Since the rank of ψ is r, we can apply the Gauss algorithm using pivots in ψ of maximal absolute values in ψ (clearly we cannot require that they have maximal absolute values in $\tilde{\psi}$). Let Δ be an invertible matrix, given by the Gauss algorithm, such that $\Delta\tilde{\psi} = (\phi_1|\phi_2)$ with fI_r a submatrix of ϕ_1.

We next get rid of possible common factors. Take $N_1, n_1 \in \operatorname{End} E^*$ such that $N_1|\phi_1$ and $n_1|\Delta\tilde{\psi}$. Further suppose that, if $f|(\phi_1/N_1)$ or $f|(\Delta\tilde{\psi}/n_1)$ then f is a unit of End E (if End $E \cong \mathbb{Z}$, then N_1 is the greatest common divisor of the entries of ϕ_1 and n_1 the greatest common divisor of the entries of $\Delta\tilde{\psi}$). Then

$$\Delta\tilde{\psi} = n_1(N\phi|\phi')$$

with $N = N_1/n_1$, $\phi = \phi_1/N_1$ and $\phi' = \phi_2/n_1$. We define

$$\tilde{\phi} = (N\phi|\phi').$$

Clearly $\tilde{\phi}$ is quasispecial. In addition

$$B_{\tilde{\psi}} \subset B_{\Delta\tilde{\psi}} = B_{n_1\tilde{\phi}}.$$

By Lemma 4.4(i), with $\psi = \tilde{\phi}$ and $N = n_1$, we deduce that

$$B_{\tilde{\psi}} \subset B_{\tilde{\phi}} + E^r_{\mathrm{Tor}} \times \{0\}^{g+s-r}.$$

Since $(x, p) \in B_{\tilde{\psi}} + \mathcal{O}_\varepsilon$, we obtain $(x, p) \in B_{\tilde{\phi}} + \mathcal{O}_\varepsilon$ with $\tilde{\phi}$ quasispecial. □

7. Estimates for the height: the proof of Theorem 1.2

As mentioned, Theorem 1.2(ii) is part of Theorem 1.5 in [Rémond and Viada 2003]. In this section, we adapt the proof given there to part (i) of Theorem 1.2.

In view of Section 5, we can assume, without loss of generality, that a weak-transverse curve C' in E^n has the form

$$C' = C \times p,$$

where C and p satisfy conditions (i)–(iii) on page 265.

Definition 7.1. Let p be a point in E^s and ε a nonnegative real. We define G_p^ε as the set of points $\theta \in E^2$ for which there exist a matrix $A \in M_{2,s}(\operatorname{End} E)$, an element $a \in \operatorname{End} E$ with $0 < |a| \le H(A)$, points $\xi \in E^s$ and $\zeta \in E^2$ of norm at most ε such that

$$[a]\theta = A(p + \xi) + [a]\zeta.$$

We identify G_p^ε with the subset $G_p^\varepsilon \times \{0\}^{g-2}$ of E^g.

Recall that Γ_p is the saturated module of the coordinates of p.

Now we embed $S_2(C \times p, \mathcal{O}_\varepsilon)$ in two sets related to the transverse curve C. We then use the Vojta inequality on these new sets.

Lemma 7.2. *The natural projection on the first g coordinates,*

$$E^g \times E^s \to E^g, \quad (x, y) \mapsto x,$$

defines an injection

$$S_2(C \times p, \mathcal{O}_{\varepsilon/2gs}) \hookrightarrow S_2(C, (\Gamma_p^g)_\varepsilon) \cup \bigcup_{\substack{\phi: E^g \to E^2 \\ \text{Gauss-reduced}}} C(\overline{\mathbb{Q}}) \cap B_\phi + G_p^\varepsilon.$$

Proof. Let $(x, p) \in S_2(C \times p, \mathcal{O}_{\varepsilon/2gs})$. By Lemma 6.2, $(x, p) \in B_{\tilde{\phi}} + \mathcal{O}_{\varepsilon/2gs}$, with $\tilde{\phi} = (N\phi|\phi') : E^{g+s} \to E^2$ quasispecial of rank 2. Hence

$$\tilde{\phi}((x, p) + (\xi, \xi')) = 0,$$

for $(\xi, \xi') \in \mathcal{O}_{\varepsilon/2gs}$. We can write the equality as

$$N\phi(x) + N\phi(\xi) + \phi'(p + \xi') = 0.$$

By the definition of quasispecialness ϕ is Gauss-reduced, so

$$\phi = (aI_2|L).$$

By Lemma 4.3(i) applied to ϕ and ξ, we can assume that

$$\xi = (\xi_1, \xi_2, 0, \dots 0) \in \mathcal{O}_{\varepsilon/2s}.$$

Suppose first that $NH(\phi) \geq H(\tilde{\phi})$. Let ζ be a point in $E^2 \times \{0\}^{g-2}$ such that

$$N[a]\zeta = (\phi'(\xi'), 0 \dots, 0).$$

Then

$$\|\zeta\| = \frac{\|\phi'(\xi')\|}{NH(\phi)} \leq \frac{\varepsilon}{2}.$$

Let y be a point in $E^2 \times \{0\}^{g-2}$ such that

$$N[a]y = (\phi'(p), 0, \dots, 0).$$

Since Γ_p is saturated, $y \in \Gamma_p^2 \times \{0\}^{g-2}$. Then

$$N\phi(x + \xi + \zeta + y) = 0$$

with $y + \xi + \zeta \in \Gamma_p^g + \mathcal{O}_\varepsilon$. So

$$x \in S_2(C, (\Gamma_p^g)_\varepsilon).$$

Now suppose that $NH(\phi) < H(\tilde{\phi})$ or, equivalently, $NH(\phi) < H(\phi')$. Let θ' be a point in E^2 such that

$$N[a]\theta' = \phi'(p + \xi') + N[a]\begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix},$$

and $\theta = (\theta', \{0\}^{g-r})$. Then $\theta \in G_p^\varepsilon$. Moreover

$$\begin{aligned} N\phi(x+\theta) &= N\phi(x) + N\phi(\theta) \\ &= N\phi(x) + N[a]\theta' = N\phi(x) + \phi'(p+\xi') + N[a]\begin{pmatrix}\xi_1\\ \xi_2\end{pmatrix} \\ &= N\phi(x) + N\phi(\xi) + \phi'(p+\xi') \\ &= \tilde{\phi}((x,p) + (\xi,\xi')) = 0. \end{aligned}$$

Thus $x \in B_{N\phi} + G_p^\varepsilon$, and by Lemma 4.4(i),

$$x \in B_\phi + (E^2_{\mathrm{Tor}} \times \{0\}^{g-2}) + G_p^\varepsilon.$$

Note that $G_p^\varepsilon + (E^2_{\mathrm{Tor}} \times \{0\}^{g-2}) \subset G_p^\varepsilon$. Hence,

$$x \in C(\overline{\mathbb{Q}}) \cap B_\phi + G_p^\varepsilon. \qquad \square$$

Lemma 7.3 (Counterpart to [Rémond and Viada 2003, Lemma 3.2]). *For $\phi : E^g \to E^2$ Gauss-reduced of rank 2, we have the set inclusion*

$$(B_\phi + G_p^\varepsilon) \subset \left\{ P + \theta : P \in B_\phi,\ \theta \in G_p^\varepsilon \text{ and } \max(\|\theta\|, \|P\|) \le 2g\|P+\theta\| \right\}.$$

Proof. Take $x \in (B_\phi + G_p^\varepsilon)$ with $\phi = (aI_r|L)$ Gauss-reduced of rank 2. Then $x = P+\theta$ with $P \in B_\phi$ and $\theta \in G_p^\varepsilon$ and $\phi(x-\theta) = 0$. By definition $G_p^\varepsilon \subset E^2 \times \{0\}^{g-2}$, so $\phi(\theta) = [a]\theta$. Then

$$\|\theta\| = \frac{\|\phi(\theta)\|}{H(\phi)} = \frac{\|\phi(x)\|}{H(\phi)} \le g\|x\|.$$

So

$$\|P\| = \|x-\theta\| \le (g+1)\|x\| = (g+1)\|P+\theta\|. \qquad \square$$

Lemma 3.3(1) of [Rémond and Viada 2003] is a statement on the morphism; therefore it holds with no need for any remarks.

Lemma 7.4 (Counterpart to [Rémond and Viada 2003, Lemma 3.3(2)]). *There exists an effective $\varepsilon_2 > 0$ such that, for all $\varepsilon \le \varepsilon_2$, any sequence of elements in G_p^ε admits a subsequence in which every two elements θ, θ' satisfy*

$$\left\| \frac{\theta}{\|\theta\|} - \frac{\theta'}{\|\theta'\|} \right\| \le \frac{1}{16gc_1},$$

where c_1 depends on C and is as defined in [Rémond and Viada 2003, Proposition 2.1].

Proof. We decompose two elements θ and θ' in a given sequence of elements of G_p^ε as

$$[a]\theta = A(p+\xi) + [a]\zeta, \quad [a']\theta' = A'(p+\xi') + a'\zeta',$$

with $A, A' \in M_{2,s}(\mathrm{End}\, E)$ and $0 < |a| \leq H(A)$, $0 < |a'| \leq H(A')$. Define y and y' such that

$$[a]y = A(p) \quad \text{and} \quad [a']y' = A'(p).$$

Since the sphere of radius 1 is compact in $(\langle p_1, \dots, p_s\rangle \times \langle p_1, \dots, p_s\rangle) \otimes \mathbb{R}$, we can extract a subsequence such that, for any two elements y and y',

$$\left\| \frac{y}{\|y\|} - \frac{y'}{\|y'\|} \right\| \leq \frac{1}{48gc_1}.$$

Note that

$$\left\| \frac{\theta}{\|\theta\|} - \frac{y}{\|\theta\|} \right\| = \left\| \frac{A(\xi) + [a]\zeta}{A(p+\xi) + [a]\zeta} \right\|$$

and

$$\left\| \frac{y}{\|\theta\|} - \frac{y}{\|y\|} \right\| = \left| \frac{\|A(p)\| - \|A(p+\xi) + [a]\zeta\|}{\|A(p+\xi) + [a]\zeta\|} \right| \leq \left\| \frac{A(\xi) + [a]\zeta}{A(p+\xi) + [a]\zeta} \right\|,$$

and the same relations for primed variables. We deduce that

$$\begin{aligned} \left\| \frac{\theta}{\|\theta\|} - \frac{\theta'}{\|\theta'\|} \right\| &\leq \left\| \frac{y}{\|y\|} - \frac{y'}{\|y'\|} \right\| + \left\| \frac{y}{\|\theta\|} - \frac{y}{\|y\|} \right\| + \left\| \frac{y'}{\|\theta'\|} - \frac{y'}{\|y'\|} \right\| \\ &\qquad + \left\| \frac{\theta}{\|\theta\|} - \frac{y}{\|\theta\|} \right\| + \left\| \frac{\theta'}{\|\theta'\|} - \frac{y'}{\|\theta'\|} \right\| \\ &\leq \left\| \frac{y}{\|y\|} - \frac{y'}{\|y'\|} \right\| + 2\left\| \frac{A(\xi) + [a]\zeta}{A(p+\xi) + [a]\zeta} \right\| + 2\left\| \frac{A'(\xi') + [a']\zeta'}{A'(p+\xi') + [a']\zeta'} \right\|. \end{aligned}$$

Choose

$$\varepsilon \leq \varepsilon_2 = \min(\varepsilon_0(p, \tau), \varepsilon_0'(p, \tau)), \tag{7-1}$$

where $\varepsilon_0(p, \tau)$ is defined in (3-3), $c_2(p, \tau)$ is defined in (3-4) and

$$\varepsilon_0'(p, \tau) = \frac{c_2(p, \tau)^{1/2} \min\|p_i\|}{96(s+1)c_1}.$$

Note that $\|A(p+\xi) + [a]\zeta\| = \|A_k(p+\xi) + a\zeta_k\|$ for $k = 1$ or 2 and $A = \binom{A_1}{A_2}$. Proposition 3.3 applied with $b_1, \dots, b_s = A_k$, $\xi = -\xi$, $\zeta = -\zeta_k$ and $b = a$, implies

$$\|A(p+\xi) + [a]\zeta\| \geq H(A) c_2(p, \tau)^{1/2} \min\|p_i\|$$

(same relation with $'$).

It follows that

$$\left\| \frac{\theta}{\|\theta\|} - \frac{\theta'}{\|\theta'\|} \right\| \le \frac{1}{48gc_1} + \varepsilon \frac{2H(A)(s+1)}{H(A)c_2(p,\tau)^{1/2}\min\|p_i\|} + \varepsilon \frac{2H(A')(s+1)}{H(A')c_2(p,\tau)^{1/2}\min\|p_i\|} \le \frac{1}{48gc_1} + \frac{1}{48gc_1} + \frac{1}{48gc_1},$$

where in the last inequality we use $\varepsilon \le \varepsilon_0'(p,\tau)$. □

We are ready to conclude.

Proof of Theorem 1.2(i). In view of Lemma 7.2, we shall prove that there exists $\varepsilon > 0$ such that $S_2(C, (\Gamma_p^g)_\varepsilon)$ and $\bigcup_{\substack{\phi : E^g \to E^2 \\ \text{Gauss-reduced}}} C(\overline{\mathbb{Q}}) \cap B_\phi + G_p^\varepsilon$ have bounded height.

By Theorem 1.2(ii), there exists $\varepsilon_1 > 0$ such that for $\varepsilon \le \varepsilon_1$, the first set has bounded height.

It remains to show that there exists $\varepsilon_2 > 0$ such that, for $\varepsilon \le \varepsilon_2$, the second set has bounded height. The proof follows, step by step, the proof of [Rémond and Viada 2003, Theorem 1.5]. In view of Lemma 7.3 and 7.4, all conditions for the proof of that theorem are satisfied. The proof is then exactly equal to the one in [Rémond and Viada 2003, p. 1927–1928]. □

Remark 7.5. In Theorem 1.5 of [Rémond and Viada 2003] we showed that for $\varepsilon_1 = 1/(2^g c_1)$, the set $S_2(C, \Gamma_{\varepsilon_1})$ has bounded height. The constant c_1 depends on the invariants of the curve C. This constant is defined in Proposition 2.1 of the same reference and it is effective. On the other hand, the height of $S_2(C, \Gamma_{\varepsilon_1})$ is bounded by a constant which is not known to be effective, unless Γ has rank 0.

For $C \times p$, we have shown that for

$$\varepsilon_2' = \frac{\min(1, c_2(p,\tau)) \min\|p_i\|^2}{2^8 g(s+1)^2 \max\|p_i\| c_1}$$

the set $S_2(C \times p, \mathbb{O}_{\varepsilon_2'})$ has bounded height; see relation (7-1) and Lemma 7.2. As in the previous case, the height of $S_2(C \times p, \mathbb{O}_{\varepsilon_2'})$ is bounded by a constant which, in general, is not known to be effective.

8. Summary of notation

We stop to recapitulate and fix the notations for the rest of the article.

For simplicity, we assume that $\operatorname{End} E \cong \mathbb{Z}$. In this case the saturated module of a group coincides with its division group. According to Remark 4.2, we use $H(\phi) = a$ in the definition of a Gauss-reduced morphism and $N \in \mathbb{N}^*$ in the definition of quasispecialness.

- Let E be an elliptic curve without CM over $\overline{\mathbb{Q}}$.
- Let C be a transverse curve in E^g over $\overline{\mathbb{Q}}$.
- Let
$$\phi = \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_r \end{pmatrix} = \begin{pmatrix} a & \dots & 0 & L_1 \\ \vdots & & \vdots & \vdots \\ 0 & \dots & a & L_r \end{pmatrix}$$
be a Gauss-reduced morphism of rank $1 \le r \le g$, with $L_i \in \mathbb{Z}^{g-r}$ and $H(\phi) = a$.
- Let Γ be a subgroup of finite rank of $E^g(\overline{\mathbb{Q}})$.
- Let Γ_0 be the division group of Γ and s its rank (the definition is given in relation (2-1)).
- Choose $\varepsilon_1 > 0$ so that $S_2(C, (\Gamma_0^g)_{\varepsilon_1})$ has bounded height; the definition is consistent in view of Theorem 1.2 (ii).
- Let K_1 be the norm of $S_2(C, (\Gamma_0^g)_{\varepsilon_1})$.
- Let $\gamma = (\gamma_1, \dots, \gamma_s)$ be a point of $E^s(\overline{\mathbb{Q}})$ such that $\gamma_1, \dots, \gamma_s$ is a maximal free set of Γ_0 satisfying the conditions of Lemma 3.4 with $K = 3gK_1$. Namely, for all integers b_i
$$\frac{1}{9} \sum_i |b_i|^2 \|\gamma_i\|^2 \le \Big\| \sum_i b_i \gamma_i \Big\|^2 \tag{8-1}$$
and
$$\min_i \|\gamma_i\| \ge 3gK_1. \tag{8-2}$$
- Let $C \times \gamma$ be the associated weak-transverse curve in E^{g+s}.
- Let $\tilde{\phi} = (N\phi | \phi') : E^{g+s} \to E^r$ be a quasispecial morphism with $N \in \mathbb{N}^*$.
- Choose $\varepsilon_2 > 0$ so that $S_2(C \times \gamma, \mathcal{O}_{\varepsilon_2})$ has bounded height; this definition is consistent in view of Theorem 1.2(i).
- Let K_2 be the norm of $S_2(C \times \gamma, \mathcal{O}_{\varepsilon_2})$.
- Let $p = (p_1, \dots, p_s) \in E^s$ be a point such that the rank of $\langle p_1, \dots, p_s \rangle$ is s.
- Let Γ_p be the division group of $\langle p_1, \dots, p_s \rangle$ (in short the division group of p).
- Let c_p and ε_p be the constants $(c_2(p, \tau))^{1/2}$ and $\varepsilon_0(p, \tau)$ defined in Proposition 3.3 for the point p and $\tau = 1$ (please note the square root in c_p).
- Let $C \times p$ be the associated weak-transverse curve in E^{g+s}.
- Choose $\varepsilon_3 > 0$ so that $S_2(C \times p, \mathcal{O}_{\varepsilon_3})$ has bounded height; the definition is consistent in view of Theorem 1.2 (i).
- Let K_3 be the norm of $S_2(C \times p, \mathcal{O}_{\varepsilon_3})$.

9. Equivalence of the strong statements: the proof of Theorem 1.3

The following theorem implies Theorem 1.3 immediately; in addition it gives explicit inclusions. Once more, we emphasize that we need to assume that $S_r(C \times p, \mathcal{O}_\varepsilon)$ has bounded height in order to embed it in a set of the type $S_r(C, \Gamma_{\varepsilon'})$. Therefore we assume $r \geq 2$ and $\varepsilon \leq \varepsilon_3$ in part (ii).

Theorem 9.1. *Let* $\varepsilon \geq 0$*.*

(i) *The map* $x \to (x, \gamma)$ *defines an injection*

$$S_r(C, \Gamma_\varepsilon) \hookrightarrow S_r(C \times \gamma, \mathcal{O}_\varepsilon).$$

(Recall that γ is a maximal free set of Γ_0.)

(ii) *For* $2 \leq r$ *and* $\varepsilon \leq \min(\varepsilon_p, \varepsilon_3)$, *the map* $(x, p) \to x$ *defines an injection*

$$S_r(C \times p, \mathcal{O}_\varepsilon) \hookrightarrow S_r(C, (\Gamma_p^g)_{\varepsilon K_4}),$$

where $K_4 = (g+s)\max\left(1, \dfrac{g(K_3+\varepsilon)}{c_p \min_i \|p_i\|}\right)$. (Recall that Γ_p is the division group of p.)

Proof. (i) Let $x \in S_r(C, \Gamma_\varepsilon)$. There exists a surjective $\phi : E^g \to E^r$ and points $y \in \Gamma$ and $\xi \in \mathcal{O}_\varepsilon$ such that

$$\phi(x + y + \xi) = 0.$$

Since $\gamma = (\gamma_1, \dots, \gamma_s)$ is a maximal free set of Γ_0, there exists a positive integer N and a matrix $G \in M_{r,s}(\mathbb{Z})$ such that

$$[N]y = G\gamma.$$

We define

$$\tilde{\phi} = (N\phi | \phi G).$$

Then $\tilde{\phi}((x, \gamma) + (\xi, 0)) = N\phi(x + \xi) + \phi G(\gamma) = N\phi(x + \xi + y) = 0$, so

$$(x, \gamma) \in S_r(C \times \gamma, \mathcal{O}_\varepsilon).$$

(ii) Take $(x, p) \in S_r(C \times p, \mathcal{O}_\varepsilon)$. Thanks to Lemma 6.2, the assumption $\varepsilon \leq \varepsilon_p$ implies

$$(x, p) \in (B_{\tilde{\phi}} + \mathcal{O}_\varepsilon)$$

with $\tilde{\phi} = (N\phi | \phi')$ quasispecial. Hence

$$\tilde{\phi}((x, p) + (\xi, \xi')) = 0$$

for $(\xi, \xi') \in \mathcal{O}_\varepsilon$. Equivalently,

$$N\phi(x + \xi) = -\phi'(p + \xi'). \tag{9-1}$$

By the definition of quasispecialness, ϕ is Gauss-reduced of rank r. Let

$$\phi = \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_r \end{pmatrix} = \begin{pmatrix} a & \dots & 0 & L_1 \\ \vdots & & \vdots & \vdots \\ 0 & \dots & a & L_r \end{pmatrix},$$

with $L_i \in \mathbb{Z}^{g-r}$ and $H(\phi) = a$.

Since Γ_p is the division group of p, the point y' defined by

$$N[a]y' = \phi'(p)$$

belongs to Γ_p^r.

Let ζ' be a point of E^r such that

$$N[a]\zeta' = \tilde{\phi}(\xi, \xi').$$

We define

$$y = (y', 0, \dots, 0) \in \Gamma_p^r \times \{0\}^{g-r}, \quad \zeta = (\zeta', 0, \dots, 0) \in E^r \times \{0\}^{g-r}.$$

We have

$$N\phi(y) = N[a]y' = \phi'(p) N\phi(\zeta) = N[a]\zeta' = \tilde{\phi}(\xi, \xi').$$

It follows that

$$N\phi(x + y + \zeta) \;=\; N\phi(x) + \phi'(p) + \tilde{\phi}(\xi, \xi') = \;\tilde{\phi}((x, p) + (\xi, \xi')) \;=\; 0.$$

Thus

$$x \in C(\overline{\mathbb{Q}}) \cap (B_{N\phi} + \Gamma_p^g + \mathcal{O}_{\|\zeta\|}).$$

In order to finish the proof, we shall prove

$$\|\zeta\| \leq \varepsilon K_4.$$

By the definition of ζ we see that

$$\|\zeta\| = \|\zeta'\| = \frac{\|\tilde{\phi}(\xi, \xi')\|}{Na} \leq (g+s)\frac{\max(H(\phi'), Na)}{Na}\|(\xi, \xi')\|$$
$$\leq (g+s)\frac{\max(H(\phi'), Na)}{Na}\varepsilon.$$

We claim that

$$\frac{\max(H(\phi'), Na)}{Na} \leq \frac{K_4}{g+s}.$$

Let $\phi' = (b_{ij})$. We shall prove that $H(\phi') = \max_{ij} |b_{ij}| \le \dfrac{K_4}{g+s} Na$. Let $|b_{kl}| = H(\phi')$. Consider the k-th row of the system (9-1)

$$N\phi_k(x) + N\phi_k(\xi) = -\sum_j b_{kj}(p_j + \xi'_j).$$

The triangle inequality gives

$$\frac{\|\phi_k(x)\|}{a} + \frac{\|\phi_k(\xi)\|}{a} \ge \frac{\|\sum_j b_{kj}(p_j + \xi'_j)\|}{Na}. \tag{9-2}$$

Since $\varepsilon \le \varepsilon_3$ and $r \ge 2$, we have $(x, p) \in S_2(C \times p, \mathbb{O}_{\varepsilon_3})$, which has norm K_3. Hence

$$\|x\| \le \|(x, p)\| \le K_3.$$

Since $a = H(\phi)$, we see that

$$\frac{\|\phi_k(x)\|}{a} \le (g - r + 1)K_3 \quad \text{and} \quad \frac{\|\phi_k(\xi)\|}{a} \le (g - r + 1)\varepsilon.$$

Substituting in (9-2),

$$(g - r + 1)(K_3 + \varepsilon) \ge \frac{\left\|\sum_j b_{kj}(p_j + \xi'_j)\right\|}{Na}.$$

Recall that $\varepsilon \le \varepsilon_p$. Hence, Proposition 3.3 with $(b_1, \dots, b_s) = (b_{k1}, \dots, b_{ks})$, $(\xi_1, \dots, \xi_s) = -\xi'$ and $\zeta = 0$, implies that

$$(g - r + 1)(K_3 + \varepsilon) \ge \frac{1}{Na}\left({c_p}^2 \sum_j |b_{kj}|^2 \|p_j\|^2\right)^{1/2} \ge \frac{c_p H(\phi')}{Na} \min_i \|p_i\|.$$

Whence

$$H(\phi') \le \frac{K_4}{g+s} Na. \qquad \square$$

The inclusion in Theorem 9.1(ii) has been proved only for a set $S_r(C \times p, \mathbb{O}_\varepsilon)$ known to have bounded height. If the norm K_3 of $S_r(C \times p, \mathbb{O}_\varepsilon)$ goes to infinity, the set $(\Gamma_p^g)_{\varepsilon K_4}$ tends to be the whole of E^g.

Remark 9.2. We would like to show that our Theorems 1.2 and 1.5 are optimal. Take $\Gamma = \langle (y_1, 0, \dots, 0) \rangle$, where y_1 is a nontorsion point in $E(\overline{\mathbb{Q}})$. Since C is transverse, the projection π_1 of $C(\overline{\mathbb{Q}})$ on the first factor $E(\overline{\mathbb{Q}})$ is surjective. Let $x_n \in C(\overline{\mathbb{Q}})$ such that $\pi_1(x_n) = ny_1$. So $x_n - n(y_1, 0, \dots, 0)$ has first coordinate zero, and belongs to the algebraic subgroup $0 \times E^{g-1}$. Then, for all $n \in \mathbb{N}$ we have

$$x_n \in B_{\phi=(1,0,\dots,0)} + \Gamma.$$

This shows that $x_n \in S_1(C, \Gamma)$, so $S_1(C, \Gamma)$ does not have bounded height. By Theorem 9.1(i), neither does $S_1(C \times y_1)$.

10. Special morphisms and an important inclusion

We can actually show a stronger inclusion than the one in Theorem 9.1(i). The set $S_r(C,\Gamma_\varepsilon)$ can be included in a subset of $S_r(C\times\gamma,\mathcal{O}_\varepsilon)$, namely the subset defined by special morphisms.

Definition 10.1 (Special morphisms). A surjective morphism $\tilde{\phi}:E^{g+s}\to E^r$ is special if $\tilde{\phi}=(N\phi|\phi')$ is quasispecial and satisfies the further condition

$$H(\tilde{\phi})=NH(\phi).$$

Equivalently, $\tilde{\phi}$ is special if and only if

(i) $\tilde{\phi}$ is Gauss-reduced, and

(ii) $H(\tilde{\phi})I_r$ is a submatrix of the matrix consisting of the first g columns of $\tilde{\phi}$.

Proof of the equivalence of the two definitions. That the first definition implies the second is clear. For the converse, take the decomposition $\tilde{\phi}=(A|\phi')$, with $A\in M_{r\times g}(\mathbb{Z})$ and $\phi'\in M_{r\times s}(\mathbb{Z})$. Let N be the greatest common divisor of the entries of A. Define $\phi=A/N$ and $a=H(\tilde{\phi})/N$. Then $\phi=(aI_r|L')$ is Gauss-reduced and $\tilde{\phi}=(N\phi|\phi')$. □

A nice remark is that the obstruction to showing unconditionally that $S_r(C\times p,\mathcal{O}_\varepsilon)$ is included in $S_r(C,(\Gamma_p^g)_{\varepsilon'})$ is exactly due to the nonspecial morphisms. Sets of the form

$$(C(\overline{\mathbb{Q}})\times p)\cap(B_{\tilde{\phi}}+\mathcal{O}_\varepsilon)$$

not having bounded height can be included in $S_r(C,(\Gamma_p^g)_{\varepsilon'})$ if $\tilde{\phi}$ is special; indeed in general

$$\varepsilon'=\mathrm{c}(g,s)\frac{H(\tilde{\phi})}{H(A)}\varepsilon$$

for any $\tilde{\phi}=(A|\phi')$.

Proposition 10.2. *Let $2\le r$ and $\varepsilon\le\min(\varepsilon_1,K_1/g)$. The map $x\to(x,\gamma)$ defines an injection*

$$\bigcup_{\substack{\phi\text{ Gauss-reduced}\\ \mathrm{rk}\,\phi=r}} C(\overline{\mathbb{Q}})\cap\big(B_\phi+(\Gamma_0^g)_\varepsilon\big)\hookrightarrow\bigcup_{\substack{\tilde{\phi}=(N\phi|\phi')\text{ special}\\ \mathrm{rk}\,\tilde{\phi}=r}}(C(\overline{\mathbb{Q}})\times\gamma)\cap(B_{\tilde{\phi}}+\mathcal{O}_\varepsilon).$$

Proof. Let $x\in C(\overline{\mathbb{Q}})\cap(B_\phi+\Gamma_0^g+\mathcal{O}_\varepsilon)$, with ϕ Gauss-reduced of rank r. Equivalently, there exist $y\in\Gamma_0^g$ and $\xi\in\mathcal{O}_\varepsilon\subset E^g$ such that

$$\phi(x+y+\xi)=0.$$

Since $\gamma_1, \ldots, \gamma_s$ is a maximal free set of Γ_0, there exists an integer N and a matrix $G \in M_{r,s}(\mathbb{Z})$ such that

$$[N]y = G(\gamma).$$

Let n be the greatest common divisor of the entries of $(N\phi|\phi G)$. We define

$$\tilde{\phi} = \frac{1}{n}(N\phi|\phi G).$$

Clearly

$$(N\phi|\phi G)\,((x, \gamma) + (\xi, 0)) = N\phi(x) + \phi G(\gamma) + N\phi(\xi) = N\phi(x + y + \xi) = 0.$$

Thus

$$n\tilde{\phi}\big((x, \gamma) + (\xi, 0)\big) = 0. \tag{10-1}$$

Equivalently,

$$(x, \gamma) \in (C(\overline{\mathbb{Q}}) \times \gamma) \cap (B_{n\tilde{\phi}} + \mathcal{O}_\varepsilon).$$

By Lemma 4.4(i) with $\psi = \tilde{\phi}$ and $N = n$, it follows

$$(x, \gamma) \in (C(\overline{\mathbb{Q}}) \times \gamma) \cap (B_{\tilde{\phi}} + \mathcal{O}_\varepsilon).$$

We next show that $\tilde{\phi}$ is special. By assumption, the morphism ϕ is Gauss-reduced. By the definition of $\tilde{\phi}$, the greatest common divisor of its entries is 1. In order to conclude that $\tilde{\phi}$ is special, we still have to show that

$$H(\tilde{\phi}) = Na$$

or equivalently

$$H(\phi') \leq Na.$$

The proof is similar to the last part of the proof of Theorem 9.1(ii).

Let $\phi' = (b_{ij}) = \phi G$. Let $|b_{kl}| = \max_{ij} |b_{ij}| = H(\phi')$. Let ϕ_k be the k-th row of ϕ. Consider the k-th row of the system (10-1):

$$nN(\phi_k(x) + \phi_k(\xi)) = -n \sum_j b_{kj}\gamma_j.$$

Then

$$\frac{\|\phi_k(x)\|}{a} + \frac{\|\phi_k(\xi)\|}{a} \geq \frac{1}{Na} \left\| \sum_j b_{kj}\gamma_j \right\|.$$

Clearly $x \in S_r(C, (\Gamma_0^g)_\varepsilon)$. Since $\varepsilon \leq \varepsilon_1$, we have $x \in S_2(C, (\Gamma_0^g)_{\varepsilon_1})$, which has norm bounded by K_1. So

$$\|x\| \leq K_1.$$

Since $H(\phi_k) \leq H(\phi) = a$,

$$\frac{\|\phi_k(x)\|}{a} \leq (g - r + 1)K_1.$$

Furthermore,

$$\frac{\|\phi_k(\xi)\|}{a} \leq (g-r+1)\varepsilon.$$

Then

$$(g-1)(K_1+\varepsilon) \geq \frac{1}{Na}\left\|\sum_j b_{kj}\gamma_j\right\|.$$

From relations (8-1) with $(b_1, \dots, b_s) = (b_{k1}, \dots, b_{ks})$ and (8-2), we deduce

$$(g-1)(K_1+\varepsilon) \geq \frac{1}{Na}\left(\frac{1}{9}\sum_j |b_{kj}|^2\|\gamma_j\|^2\right)^{1/2} \geq \frac{H(\phi')}{3Na}\min_j \|\gamma_j\| \geq \frac{H(\phi')}{3Na}3gK_1.$$

We assumed that $\varepsilon \leq K_1/g$, so $H(\phi') \leq Na$. □

This inclusion is important; the Bogomolov-type bounds are given for intersections with $\mathbb{O}_\varepsilon$ and not with Γ_ε. Actually there exist bounds for ε such that $C \cap \Gamma_\varepsilon$ is finite. They are deduced using the Bogomolov-type bounds and their dependence on the degree of the curve is not sharp enough for our purpose. To overcome this obstacle and solve the problem with Γ_ε, we use Proposition 10.2 and the Bogomolov-type bounds for $C \times \gamma$ intersected with $B_{\tilde{\phi}} + \mathbb{O}_\varepsilon$, where $\tilde{\phi}$ is special of rank 2.

11. Proof of Theorem 1.5: Structure

Sections 12 and 13 below will develop the core of the proof of Theorem 1.5. In Proposition A we show that the union can be taken over finitely many sets, while in Proposition B we show that each set in the union is finite.

We prefer to present first the proof of Theorem 1.5 assuming Propositions A and B, and then to prove them. We hope that, knowing a priori the aim of sections 12 and 13, the reader gets the right inspiration to handle the proofs.

Proof of Theorem 1.5. Assuming Conjecture 1.4, we prove Conjecture 1.1(iv). In view of Theorem 1.3, part (iii) is also proved. Parts (i) and (ii) are then obtained by setting $\varepsilon = 0$.

Choose

$$n = 2(g+s)-3,$$

$$\delta_1 = \frac{\min(\varepsilon_4, \varepsilon_2)}{(g+s)^2}, \quad \text{where } \varepsilon_4 \text{ is as in Proposition B},$$

$$\delta = \delta_1 M'^{-1-1/(2n)}, \quad \text{where } M' = \max\left(2, \lceil K_2/\delta_1 \rceil^2\right)^n.$$

Recall that $\Gamma_\delta \subset (\Gamma_0^g)_\delta$. Apply Lemma 4.5, replacing ε by δ. Then

$$S_2(C,\Gamma_\delta) \subset \bigcup_{\substack{\phi \text{ Gauss-reduced} \\ \operatorname{rk}\phi=2}} C(\overline{\mathbb{Q}}) \cap (B_\phi + (\Gamma_0^g)_\delta).$$

Observing that $\delta < \delta_1 < \min(\varepsilon_1, K_1/g)$ and applying Proposition 10.2 (again with $\varepsilon = \delta$) we obtain an injection

$$\bigcup_{\substack{\phi \text{ Gauss-reduced} \\ \operatorname{rk}\phi=2}} C(\overline{\mathbb{Q}}) \cap (B_\phi + (\Gamma_0^g)_\delta) \hookrightarrow \bigcup_{\substack{\tilde{\phi}=(N\phi|\phi') \text{ special} \\ \operatorname{rk}\tilde{\phi}=2}} (C(\overline{\mathbb{Q}}) \times \gamma) \cap (B_{\tilde{\phi}} + \mathcal{O}_\delta).$$

Note that $\delta = \delta_1 M'^{-(1+1/(2n))}$ and $\delta_1 \le \varepsilon_2$. Then, Proposition A(ii) in Section 12 below, with $\varepsilon = \delta_1$, $r = 2$ (and n already defined as $2(g+s)-4+1$), shows that

$$\bigcup_{\substack{\tilde{\phi} \text{ special} \\ \operatorname{rk}\tilde{\phi}=2}} (C(\overline{\mathbb{Q}}) \times \gamma) \cap (B_{\tilde{\phi}} + \mathcal{O}_\delta)$$

is a subset of

$$\bigcup_{\substack{\tilde{\phi} \text{ special} \\ H(\tilde{\phi}) \le M' \\ \operatorname{rk}\tilde{\phi}=2}} (C(\overline{\mathbb{Q}}) \times \gamma) \cap \left(B_{\tilde{\phi}} + \mathcal{O}_{(g+s)\delta_1/H(\tilde{\phi})^{1+1/(2n)}}\right). \tag{11-1}$$

Observe that in (11-1), $\tilde{\phi}$ ranges over finitely many morphisms, because $H(\tilde{\phi})$ is bounded by M'.

We have chosen $\delta_1 \le \varepsilon_4/(g+s)^2$. Proposition B(ii) in Section 13 below with $\varepsilon = (g+s)\delta_1$, implies that for all $\tilde{\phi} = (N\phi|\phi')$ special of rank 2, the set

$$(C(\overline{\mathbb{Q}}) \times \gamma) \cap \left(B_{\tilde{\phi}} + \mathcal{O}_{(g+s)\delta_1/H(\phi)^{1+1/(2n)}}\right)$$

is finite. Note that $H(\phi) \le H(\tilde{\phi})$, thus also the sets

$$(C(\overline{\mathbb{Q}}) \times \gamma) \cap \left(B_{\tilde{\phi}} + \mathcal{O}_{(g+s)\delta_1/H(\tilde{\phi})^{1+1/(2n)}}\right)$$

appearing in (11-1) are finite.

It follows that, the set $S_2(C,\Gamma_\delta)$ is contained in the union of finitely many finite sets. So it is finite. □

Despite our proof relying on Dirichlet's Theorem and a Bogomolov-type bound, a direct use of these two theorems is not sufficient to prove Theorem 1.5. Using Dirichlet's Theorem in a more natural way, one can prove that, for $r \ge 2$,

$$S_r(C,\Gamma_\varepsilon) \subset \bigcup_{\substack{H(\phi) \le M(\varepsilon) \\ \operatorname{rk}\phi=r}} C(\overline{\mathbb{Q}}) \cap \left(B_\phi + \Gamma_\varepsilon\right).$$

On the other hand, a direct use of the Bogomolov type bound shows that

$$C(\overline{\mathbb{Q}}) \cap \left(B_\phi + \mathcal{O}_{\varepsilon/H(\phi)^2}\right)$$

is finite, for ϕ of rank at least 2. Even if we forget Γ, the discrepancy between ε and $\varepsilon/H(\phi)^2$ does not look encouraging, and it took us a long struggle to overcome the problem. In Propositions A and B, we succeed in overcoming the mismatch; in both statements we obtain neighborhoods of radius $\varepsilon/H(\phi)^{1+1/(2n)}$.

Warning: One might think that, since we consider only morphisms ϕ such that $H(\phi) \le M$, it might be enough to choose $\varepsilon' = \varepsilon/M^2$. However, $M = M(\varepsilon)$ is an unbounded function of ε as ε tends to 0.

12. Proof of Theorem 1.5: The box principle and the reduction to a finite union

In Lemma 12.2, we approximate a Gauss-reduced morphism by a Gauss-reduced morphism of bounded height. Such an approximation allows us to restrict our attention to unions over finitely many algebraic subgroups, instead of over all algebraic subgroups; this is Proposition A, already mentioned. We start by recalling Dirichlet's Theorem on the rational approximation of reals.

Theorem 12.1 (Dirichlet, 1842; see [Schmidt 1980, p. 24, Theorem 1]). *Suppose that $\alpha_1, \dots, \alpha_n$ are real numbers and that $Q \ge 2$ is an integer. There exist integers $f, f_1, \dots, f_n$ such that*

$$1 \le f < Q^n \qquad \text{and} \qquad |\alpha_i f - f_i| \le \frac{1}{Q} \quad \textit{for } 1 \le i \le n. \tag{12-1}$$

Lemma 12.2. *Let $Q \ge 2$ be an integer. Let $\phi = (aI_r|L) \in M_{r\times g}(\mathbb{Z})$ be Gauss-reduced. There exists a Gauss-reduced $\psi = (fI_r|L') \in M_{r\times g}(\mathbb{Z})$ such that*

(i) $H(\psi) = f \le Q^{rg-r^2+1}$ *and*

(ii) $\left|\dfrac{\psi}{f} - \dfrac{\phi}{a}\right| \le Q^{-1/2} f^{-1-\frac{1}{2(rg-r^2+1)}}$.

Here the norm $|\cdot|$ of a matrix is the maximum of the absolute values of its entries.

Proof. If $a \le Q^{rg-r^2+1}$ no approximation is needed, since ϕ itself satisfies the conclusion. So we can assume that

$$\phi = \begin{pmatrix} a & \dots & 0 & L_1 \\ \vdots & & \vdots & \vdots \\ 0 & \dots & a & L_r \end{pmatrix}$$

is a Gauss-reduced morphism such that $H(\phi) = a > Q^{rg-r^2+1}$. Consider the element

$$\alpha = \left(1, \frac{L_1}{a}, \dots, \frac{L_r}{a}\right) = (\alpha_1, \alpha_2, \dots, \alpha_{rg-r^2+1}) \in \mathbb{R}^{rg-r^2+1}.$$

Set $n = rg - r^2 + 1$. Apply Dirichlet's Theorem to α to select integers $f, f_1, \dots, f_n$ satisfying (12-1); they can be assumed to have greatest common divisor 1. Define

$$w = \frac{1}{f}(f_1, \dots, f_n) = \frac{1}{f}(f_1, L'_1, \dots, L'_r),$$

with $L'_i \in \mathbb{Z}^{g-r}$. We claim that

$$f_1 = f, \qquad |f_i| \le f.$$

Indeed, (12-1) for $i = 1$ yields

$$\left|\frac{f_1}{f} - 1\right| \le \frac{1}{Qf},$$

so $|f - f_1| < 1$. Since f and f_1 are integers, we must have $f = f_1$. Similarly, by (12-1) for $i = 2, \dots, n$, we have $|f_i/f - \alpha_i| \le 1/(Qf)$. This implies that $|f_i| \le f + 1/Q$. We deduce that $|f_i| \le f$.

It follows that

$$\psi = \begin{pmatrix} f & \dots & 0 & L'_1 \\ \vdots & & \vdots & \\ 0 & \dots & f & L'_r \end{pmatrix}$$

is a Gauss-reduced morphism of rank r with $H(\psi) = f$.

Relation (12-1) immediately gives

$$f \le Q^n$$

and

$$\left|\frac{\psi}{f} - \frac{\phi}{a}\right| \le \frac{1}{Qf} \le \frac{1}{Q^{1/2} f^{1+1/(2n)}},$$

where in the last inequality we have used the inequality $Q^{1/2} \ge f^{1/(2n)}$. □

At last we can prove our first main proposition; the union can be taken over finitely many algebraic subgroups. If ϕ has large height and B_ϕ is close to x, with x in a set of bounded height, then there exists ψ with height bounded by a constant such that B_ψ is also close to x. One shall be careful that, in the following inclusions, on the left-hand side we consider a neighborhood of B_ϕ of fixed radius, while on the right-hand side the neighborhood becomes smaller as the height of ψ grows. This is a crucial gain with respect to the simpler approximation (obtained by a direct use of Dirichlet's Theorem) where the neighborhoods have constant radius on both sides.

Proposition A. *Assume $r \geq 2$.*

(i) *If $0 < \varepsilon \leq \varepsilon_1$, then*

$$\bigcup_{\substack{\phi \text{ Gauss-reduced} \\ \operatorname{rk}\phi = r}} C(\overline{\mathbb{Q}}) \cap \left(B_\phi + \left(\Gamma_0^g\right)_{\varepsilon/M^{1+1/(2n)}}\right) \subset \bigcup_{\substack{\psi \text{ Gauss-reduced} \\ \operatorname{rk}\psi = r \\ H(\psi)\leq M}} C(\overline{\mathbb{Q}}) \cap \left(B_\psi + (\Gamma_0^g)_{g\varepsilon/H(\psi)^{1+1/(2n)}}\right),$$

where $n = rg - r^2 + 1$ and $M = \max\left(2, \lceil K_1/\varepsilon \rceil^2\right)^n$.

(ii) *If $0 < \varepsilon \leq \varepsilon_2$, then*

$$\bigcup_{\substack{\tilde{\phi} \text{ special} \\ \operatorname{rk}\tilde{\phi} = r}} (C(\overline{\mathbb{Q}}) \times \gamma) \cap \left(B_{\tilde{\phi}} + \mathbb{O}_{\varepsilon/M'^{1+1/(2n)}}\right) \subset \bigcup_{\substack{\tilde{\psi} \text{ special} \\ \operatorname{rk}\tilde{\psi} = r \\ H(\tilde{\psi})\leq M'}} (C(\overline{\mathbb{Q}}) \times \gamma) \cap \left(B_{\tilde{\psi}} + \mathbb{O}_{(g+s)\varepsilon/H(\tilde{\psi})^{1+1/(2n)}}\right),$$

where $n = r(g+s) - r^2 + 1$ and $M' = \max\left(2, \lceil K_2/\varepsilon \rceil^2\right)^n$.

Proof. (i) Let $\phi = (aI_r|L)$ be Gauss-reduced of rank r.

First consider the case $H(\phi) \leq M$. Then $\varepsilon/M^{1+1/(2n)} \leq \varepsilon/H(\phi)^{1+1/(2n)}$. Obviously

$$C(\overline{\mathbb{Q}}) \cap (B_\phi + \Gamma_0^g + \mathbb{O}_{\varepsilon/M^{1+1/(2n)}}) \subset C(\overline{\mathbb{Q}}) \cap (B_\phi + \Gamma_0^g + \mathbb{O}_{\varepsilon/H(\phi)^{1+1/(2n)}})$$

is contained in the right-hand side.

Secondly consider the case $H(\phi) > M$. We shall show that there exists ψ Gauss-reduced with $H(\psi) \leq M$ such that

$$C(\overline{\mathbb{Q}}) \cap \left(B_\phi + \Gamma_0^g + \mathbb{O}_{\varepsilon/M^{1+1/(2n)}}\right) \subset C(\overline{\mathbb{Q}}) \cap \left(B_\psi + \Gamma_0^g + \mathbb{O}_{g\varepsilon/H(\psi)^{1+1/(2n)}}\right).$$

We fix $Q = \max\left(2, \lceil K_1/\varepsilon \rceil^2\right)$. Recall that $n = rg - r^2 + 1$. By Lemma 12.2, there exists a Gauss-reduced morphism

$$\psi = \begin{pmatrix} f & \dots & 0 & L'_1 \\ \vdots & & \vdots & \\ 0 & \dots & f & L'_r \end{pmatrix}$$

such that

$$H(\psi) = f \leq M$$

and

$$\left| \frac{\psi}{f} - \frac{\phi}{a} \right| \leq \frac{1}{Q^{1/2} f^{1+1/(2n)}}. \tag{12-2}$$

Let $x \in C(\overline{\mathbb{Q}}) \cap (B_\phi + \Gamma_0^g + \mathbb{O}_{\varepsilon/M^{1+1/(2n)}})$. Then there exist $y \in \Gamma_0^g$ and $\xi \in \mathbb{O}_{\varepsilon/M^{1+1/(2n)}}$ such that

$$\phi(x - y - \xi) = 0.$$

We want to show that there exist $y' \in \Gamma_0^g$ and $\xi' \in \mathbb{O}_{g\varepsilon/f^{1+1/(2n)}}$ such that

$$\psi(x - y' - \xi') = 0.$$

Let y'' be a point such that

$$[a]y'' = \phi(y).$$

Since Γ_0 is a division group, $y'' \in \Gamma_0^r$. We define

$$y' = (y'', 0) \in \Gamma_0^r \times \{0\}^{g-r},$$

whence

$$\psi(y') = [f]y''.$$

Let ξ'' be a point such that

$$[f]\xi'' = \psi(x - y'),$$

and define $\xi' = (\xi'', 0)$. Then

$$\psi(\xi') = [f]\xi'' = \psi(x - y') \quad \text{and} \quad \psi(x - y' - \xi') = 0.$$

It follows that

$$x \in C(\overline{\mathbb{Q}}) \cap (B_\psi + \Gamma_0^g + \mathbb{O}_{\|\xi'\|}).$$

In order to finish the proof, we are going to prove that

$$\|\xi'\| \le \frac{g\varepsilon}{f^{1+1/(2n)}}.$$

By definition

$$\|\xi'\| = \|\xi''\| = \frac{\|\psi(x - y')\|}{f}.$$

Consider the equivalence

$$\begin{aligned} a\psi(x - y') &= a\psi(x) - a\psi(y') = a\psi(x) - a[f]y'' \\ &= a\psi(x) - f\phi(y) = a\psi(x) - f\phi(x) + f\phi(\xi). \end{aligned}$$

Then

$$\|\xi'\| = \frac{1}{af}\left\| f\phi(\xi) - f\phi(x) + a\psi(x) \right\| \le \frac{1}{a}\|\phi(\xi)\| + \frac{1}{af}\left\| a\psi(x) - f\phi(x) \right\|.$$

We estimate separately each norm on the right.

On the one hand,

$$\frac{1}{a}\|\phi(\xi)\| \le (g-r+1)\|\xi\| \le \frac{(g-1)\varepsilon}{M^{1+1/(2n)}} \le \frac{(g-1)\varepsilon}{f^{1+1/(2n)}},$$

because $\|\xi\| \le \varepsilon/M^{1+1/(2n)}$ and $f \le M$.

On the other hand, since the rank of ϕ is at least 2 and $\varepsilon \le \varepsilon_1$, we have $x \in S_2(C, (\Gamma_0^g)_{\varepsilon_1})$, which has norm K_1. Thus

$$\|x\| \le K_1.$$

Using relation (12-2) and that $Q \ge \lceil K_1/\varepsilon\rceil^2$, it follows that

$$\begin{aligned}\frac{1}{af}\|a\psi(x) - f\phi(x)\| &\le \left|\frac{\psi}{f} - \frac{\phi}{a}\right| \|x\| \le \frac{1}{Q^{1/2} f^{1+1/(2n)}}\|x\| \\ &\le \frac{\varepsilon\|x\|}{K_1 f^{1+1/(2n)}} \le \frac{\varepsilon}{f^{1+1/(2n)}}.\end{aligned}$$

We obtain

$$\|\xi'\| \le \frac{(g-1)\varepsilon}{f^{1+1/(2n)}} + \frac{\varepsilon}{f^{1+1/(2n)}} \le \frac{g\varepsilon}{f^{1+1/(2n)}},$$

concluding the proof of part (i) of the proposition.

(ii) We fix $Q = \max(2, \lceil K_2/\varepsilon\rceil^2)$. Let $\tilde\phi = (N\phi|\phi') : E^{g+s} \to E^r$ be special. From conditions (i) and (ii) of Definition 10.1 we know that

$$\tilde\phi = (bI_r|*)$$

is Gauss-reduced and $H(\tilde\phi) = b$.

As in part (i) of the proof, if $H(\tilde\phi) \le M'$ then $\varepsilon/{M'}^{1+1/(2n)} \le \varepsilon/H(\tilde\phi)^{1+1/(2n)}$ and the set

$$(C(\overline{\mathbb{Q}}) \times \gamma) \cap (B_{\tilde\phi} + \mathbb{O}_{\varepsilon/{M'}^{1+1/(2n)}})$$

is contained in the right-hand side.

Now, suppose that $H(\tilde\phi) > M'$. Recall that $n = r(g+s) - r^2 + 1$. By Lemma 12.2 (applied with $\phi = \tilde\phi$ and $\psi = \tilde\psi$) there exists a Gauss-reduced $\tilde\psi = (fI_r|*)$ such that $H(\tilde\psi) = f \le M'$ and

$$\left|\frac{\tilde\phi}{b} - \frac{\tilde\psi}{f}\right| \le \frac{1}{Q^{1/2} f^{1+1/(2n)}}. \tag{12-3}$$

Then $\tilde\psi$ is special, since it satisfies (i) and (ii) in Definition 10.1.

The proof is now similar to that of part (i). We want to show that, if $\tilde\phi((x,\gamma)+\xi)$ vanishes for $\xi \in \mathbb{O}_{\varepsilon/{M'}^{1+1/2n}}$, then $\tilde\psi((x,\gamma)+\xi')$ vanishes for $\xi' \in \mathbb{O}_{(g+s)\varepsilon/H(\tilde\psi)^{1+1/2n}}$.

Let ξ'' be a point in E^r such that

$$[f]\xi'' = -\tilde\psi(x,\gamma).$$

We define $\xi' = (\xi'', \{0\}^{g-r+s})$. Then

$$\tilde{\psi}((x,\gamma)+(\xi',0)) = 0.$$

It follows that

$$(x,\gamma) \in (C(\overline{\mathbb{Q}}) \times \gamma) \cap (B_{\tilde{\psi}} + \mathcal{O}_{\|\xi'\|}),$$

where $\tilde{\psi}$ is special and $H(\tilde{\psi}) \leq M'$.

It remains to prove that

$$\|\xi'\| \leq \frac{(g+s)\varepsilon}{H(\tilde{\psi})^{1+1/(2n)}}.$$

Obviously

$$b\tilde{\psi}(x,\gamma) = f\big(\tilde{\phi}(x,\gamma) - \tilde{\phi}(x,\gamma)\big) + b\tilde{\psi}(x,\gamma).$$

According to the definition of ξ',

$$\begin{aligned}\|\xi'\| = \|\xi''\| = \frac{\|\tilde{\psi}(x,\gamma)\|}{f} &= \frac{1}{bf}\big\| f\big(\tilde{\phi}(x,\gamma) - \tilde{\phi}(x,\gamma)\big) + b\tilde{\psi}(x,\gamma)\big\| \\ &\leq \frac{1}{b}\big\|\tilde{\phi}(x,\gamma)\big\| + \frac{1}{bf}\big\| b\tilde{\psi}(x,\gamma) - f\tilde{\phi}(x,\gamma)\big\|.\end{aligned}$$

We estimate the two norms on the right.

On the one hand,

$$\frac{\|\tilde{\phi}(x,\gamma)\|}{b} = \frac{\|\tilde{\phi}(\xi)\|}{b} \leq (g-r+1+s)\|\xi\| \leq \frac{(g-r+1+s)\varepsilon}{M'^{1+1/(2n)}} \leq \frac{(g-r+1+s)\varepsilon}{f^{1+1/(2n)}},$$

where in the last inequality we have used that $f \leq M'$.

On the other hand, by the definition of ε_2, we know that the norm of the set $S_2(C \times \gamma, \mathcal{O}_{\varepsilon_2})$ is bounded by K_2. Since $\varepsilon \leq \varepsilon_2$, we have $(x,\gamma) \in S_2(C \times \gamma, \mathcal{O}_{\varepsilon_2})$. Therefore

$$\|(x,\gamma)\| \leq K_2.$$

Using relation (12-3) and the inequality $Q \geq \lceil K_2/\varepsilon \rceil^2$, we estimate

$$\begin{aligned}\frac{1}{bf}\big\| b\tilde{\psi}(x,\gamma) - f\tilde{\phi}(x,\gamma)\big\| \leq \left|\frac{\tilde{\phi}}{b} - \frac{\tilde{\psi}}{f}\right| \|(x,\gamma)\| &\leq \frac{\|(x,\gamma)\|}{Q^{1/2} f^{1+1/(2n)}} \\ &\leq \frac{\varepsilon\|(x,\gamma)\|}{(K_2) f^{1+1/(2n)}} \leq \frac{\varepsilon}{f^{1+1/(2n)}}.\end{aligned}$$

Since $r \geq 2$, we conclude that

$$\|\xi'\| \leq \frac{(g-1+s)\varepsilon}{f^{1+1/(2n)}} + \frac{\varepsilon}{f^{1+1/(2n)}} = \frac{(g+s)\varepsilon}{H(\tilde{\psi})^{1+1/(2n)}}. \qquad \square$$

13. Proof of Theorem 1.5: The essential minimum and the finiteness of each intersection

Up until now we have used, several times, the boundedness of the height of our sets. In this section we often use the fact that we are working with a curve.

In the following, we set

$$n = 2(g+s) - 3.$$

We would like to use Conjecture 1.4 to provide $\varepsilon > 0$ such that, for all ϕ Gauss-reduced of rank $r = 2$, the set

$$(C(\overline{\mathbb{Q}}) \times \gamma) \cap \left(B_\phi + \mathcal{O}_{\varepsilon/H(\phi)^{1+1/(2n)}}\right) \tag{13-1}$$

is finite. This set is simply

$$\phi^{-1}_{|C\times\gamma}\left(\phi(C\times\gamma) \cap \phi(\mathcal{O}_{\varepsilon/H(\phi)^{1+1/(2n)}})\right).$$

Further

$$\phi(\mathcal{O}_{\varepsilon/H(\phi)^{1+1/(2n)}}) \subset \mathcal{O}_{g\varepsilon/H(\phi)^{1/(2n)}},$$

because if $\zeta \in \mathcal{O}_{\varepsilon/H(\phi)^{1+1/(2n)}}$ then $\|\phi(\zeta)\| \le gH(\phi)\|\zeta\| \le g\varepsilon H(\phi)^{-1/(2n)}$. Thus, the set (13-1) is contained in the preimage of

$$\phi(C\times\gamma) \cap \mathcal{O}_{g\varepsilon/H(\phi)^{1/(2n)}}.$$

If we can ensure that there exists $\varepsilon > 0$ such that, for all morphisms ϕ Gauss-reduced of rank $r = 2$,

$$g\varepsilon H(\phi)^{-1/(2n)} < \mu(\phi(C\times\gamma)), \tag{13-2}$$

then the set (13-1) is finite.

The direct use of a Bogomolov-type bound, even an optimal one, is not successful in the following sense: For a curve $X \subset E^g$ and any $\eta > 0$, Conjecture 1.4 provides an invariant $\epsilon(X,\eta)$ such that $\epsilon(X,\eta) < \mu(X)$. To ensure (13-2), we could naively require that

$$g\varepsilon H(\phi)^{-1/(2n)} \le \epsilon(\phi(C\times\gamma),\eta)$$

for all ϕ Gauss-reduced of rank $r = 2$. But this can be fulfilled only for $\varepsilon = 0$.

We need to throw new light on the problem in order to prove (13-2); via some isogenies, we construct a helping curve D and then we relate its essential minimum to $C\times\gamma$. We then apply Conjecture 1.4 to D. In this way we manage to provide a good lower bound for the essential minimum of $C\times\gamma$. We take advantage of the fact that $\mu([b]C) = b\mu(C)$, while $\epsilon([b]C,\eta) = \epsilon(C,\eta)/b^{1/(g-1)+2\eta}$ for any positive integers b.

Let

$$\phi = \begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix} = \begin{pmatrix} a & 0 & L_1 \\ 0 & a & L_2 \end{pmatrix}$$

be a Gauss-reduced morphism of rank 2 with $H(\phi) = a$. We introduce the notation $\bar{x} = (x_3, \ldots, x_g)$, and recall that $n = 2(g+s) - 3$.

We define

$$a_0 = \lfloor a^{1/(2n)} \rfloor.$$

We associated to the morphism ϕ an isogeny

$$\Phi : E^g \to E^g, \quad (x_1, \ldots, x_g) \mapsto (a_0 \phi(x), x_3, \ldots, x_g).$$

We then relate it to the isogenies

$$\begin{aligned} A : &E^g \to E^g, \quad (x_1, \ldots, x_g) \mapsto (x_1, x_2, a x_3, \ldots, a x_g), \\ A_0 : &E^g \to E^g, \quad (x_1, \ldots, x_g) \mapsto (x_1, x_2, a_0 x_3, \ldots, a_0 x_g), \\ L : &E^g \to E^g, \quad (x_1, \ldots, x_g) \mapsto (x_1 + L_1(\bar{x}), x_2 + L_2(\bar{x}), x_3, \ldots, x_g). \end{aligned}$$

Definition 13.1 (Helping curve). We define the curve D to be an irreducible component of $A_0^{-1} L A^{-1}(C)$, where $(\,\cdot\,)^{-1}$ simply means the inverse image.

The obvious relation

$$[a_0 a] D = \Phi(C)$$

is going to play a key role in the following.

We need to estimate degrees, since the Bogomolov-type bound depends on the degree of the curve.

Lemma 13.2. (i) *The degree of the curve $\phi(C)$ in E^2 is bounded by* $6ga^2 \deg C$.

(ii) *The degree of the curve D in E^g is bounded by* $12g^2 a_0^{2(g-2)} a^{2(g-1)} \deg C$.

Proof. (i) Consider

$$\deg \phi(C) = \sum_{i=1}^{2} \phi(C) \cdot H_i,$$

where H_i is the coordinate divisor given by $3x_i = 0$. The intersection number $\phi(C) \cdot H_i$ is bounded by the degree of the morphism $\phi_{i|C} : C \to E$. Recall that $\phi = \binom{\phi_1}{\phi_2}$. By Bézout's Theorem, $\deg \phi_{i|C}$ is at most $3ga^2 \deg C$; see [Viada 2003, p. 61]. Therefore

$$\deg \phi(C) \leq 6ga^2 \deg C.$$

(ii) Let X be a generic transverse curve in E^g. By [Hindry 1988, Lemma 6(i)], we deduce that

$$\deg A^{-1}(X) \leq 2a^{2(g-2)} \deg X, \quad \deg A_0^{-1}(X) \leq 2a_0^{2(g-2)} \deg X.$$

To estimate the degree of $L(X)$, we proceed as in part (i). We write

$$\deg L(X) = \sum_{i=1}^{g} L(X) \cdot H_i,$$

where H_i is given by $3x_i = 0$. The intersection number $L(X) \cdot H_i$ is bounded by the degree of the morphism $L'_{i|X} : X \to E$, where L'_i is the ith. row of L. By Bézout's Theorem, $\deg L'_{i|X}$ is at most $3ga^2 \deg X$. Therefore

$$\deg L(X) \leq 3g^2 a^2 \deg X.$$

We conclude that

$$\begin{aligned}\deg D &\leq \deg A_0^{-1} L A^{-1}(C) \leq 2a_0^{2(g-2)} \deg L A^{-1}(C) \\ &\leq 6g^2 a_0^{2(g-2)} a^2 \deg A^{-1}(C) \leq 12 g^2 a_0^{2(g-2)} a^2 a^{2(g-2)} \deg C.\end{aligned}$$ □

The next proposition is a lower bound for the essential minimum of the image of a curve under Gauss-reduced morphisms. It reveals the dependence on the height of the morphism. While the first bound is an immediate application of Conjecture 1.4, the second estimate is subtle. Our lower bound for $\mu(\Phi(C + y))$ grows with $H(\phi)$. On the contrary, the Bogomolov-type lower bound $\epsilon(\Phi(C + y))$ goes to zero as $(a_0 H(\phi))^{-1/(g-1)-\eta}$ — a nice gain.

Potentially, this suggests an interesting question; to investigate the behavior of the essential minimum under a general morphism.

Proposition 13.3. *Assume Conjecture 1.4 and take $y \in E^g(\overline{\mathbb{Q}})$ and $\eta > 0$. Then*:

(i)
$$\mu(\phi(C + y)) > \epsilon_1(C, \eta) a^{-(1+2\eta)},$$

where $\epsilon_1(C, \eta)$ is an effective constant depending on C and η. (Recall that $a = H(\phi)$.)

(ii)
$$\mu(\Phi(C + y)) > \epsilon_2(C, \eta) a_0^{1/(g-1)-8(g+s)(g-1)\eta},$$

where $\epsilon_2(C, \eta)$ is an effective constant depending on C, g and η. (Recall that $a_0 = \lfloor a^{1/(2n)} \rfloor$.)

Proof. Recall the Bogomolov-type bound given in Conjecture 1.4: for a transverse irreducible curve X in E^g over $\overline{\mathbb{Q}}$ and any $\eta > 0$,

$$\epsilon(X, \eta) = \frac{c(g, E, \eta)}{\deg X^{1/(2\,\mathrm{codim}\, X)+\eta}} < \mu(X).$$

(i) Observe that $\phi(C) \subset E^2$ has codimension 1.

Let $q'=\phi(y)$. So $\phi(C+y)=\phi(C)+q'$. Since C is irreducible, transverse and defined over $\overline{\mathbb{Q}}$, so is $\phi(C)+q'$. Conjecture 1.4 gives

$$\mu(\phi(C+y))=\mu(\phi(C)+q')>\epsilon(\phi(C)+q',\eta)=\frac{c(2,E,\eta)}{(\deg(\phi(C)+q'))^{1/2+\eta}}.$$

Degrees are preserved by translations; hence Lemma 13.2(i) implies that

$$\deg(\phi(C)+q')=\deg\phi(C)\leq 9ga^2\deg C.$$

If follows that

$$\epsilon(\phi(C)+q',\eta)\geq\frac{c(2,E,\eta)}{(9ga^2\deg C)^{1/2+\eta}}.$$

Define

$$\epsilon_1(C,\eta)=\frac{c(2,E,\eta)}{(9g\deg C)^{1/2+\eta}}.$$

Then

$$\mu(\phi(C+y))\geq\frac{\epsilon_1(C,\eta)}{a^{1+2\eta}}.$$

(ii) Let $q\in E^g$ be a point such that $[a_0a]q=\Phi(y)$. Then

$$\Phi(C+y)=[a_0a]\big(A_0^{-1}LA^{-1}(C)+q\big)=[a_0a](D+q).$$

Therefore

$$\mu\left(\Phi(C+y)\right)=(a_0a)\mu(D+q). \tag{13-3}$$

We now estimate $\mu(D+q)$ using Conjecture 1.4. The curve $D+q$ is irreducible by the definition of D. Since C is transverse and defined over $\overline{\mathbb{Q}}$, so is $D+q$. Thus

$$\mu(D+q)>\epsilon(D+q,\eta)=\frac{c(g,E,\eta)}{\deg(D+q)^{1/(2(g-1))+\eta}}.$$

Translations by a point preserve degrees, so Lemma 13.2(ii) gives

$$\deg(D+q)=\deg D\leq 12g^2a_0^{2(g-2)}a^{2(g-1)}\deg C.$$

Then

$$\epsilon(D+q,\eta)\geq\frac{c(g,E,\eta)}{(12g^2\deg C)^{1/(2(g-1))+\eta}}\big(a_0^{2(g-2)}a^{2(g-1)}\big)^{-\frac{1}{2(g-1)}-\eta}.$$

Define

$$\epsilon_2(C,\eta)=\frac{c(g,E,\eta)}{(12g^2\deg C)^{1/(2(g-1))+\eta}}.$$

So

$$\mu(D+q)\geq\epsilon_2(C,\eta)a_0^{-1+\frac{1}{g-1}-2(g-2)\eta}a^{-1-2(g-1)\eta}.$$

Substitute into (13-3), to obtain

$$\mu(\Phi(C+y)) > \epsilon_2(C,\eta) a_0^{\frac{1}{g-1}-2(g-2)\eta} a^{-2(g-1)\eta}.$$

Recall that a_0 is the integral part of $a^{1/(2n)}$, where $n=2(g+s)-3$. So $2a_0 \geq a^{1/(2n)}$ and

$$a^{2(g-1)\eta} \leq (2a_0)^{4n(g-1)\eta}.$$

Further, $2(g-2)+4n(g-1) \leq 8(g+s)(g-1)$, so

$$\mu(\Phi(C+y)) > \epsilon_2(C,\eta) a_0^{1/(g-1)-8(g+s)(g-1)\eta}. \qquad \square$$

We now come to our second main proposition: each set in the union is finite. The proof of (i) case (1) below is delicate. In general $\mu(\pi(C)) \leq \mu(C)$, for π a projection on some factors. We shall rather find a kind of reverse inequality. On a set of bounded height this will be possible.

Proposition B. *Assume Conjecture 1.4. There exists $\varepsilon_4 > 0$ with the following properties*:

(i) *For $\varepsilon \leq \varepsilon_4$, for all $y \in \Gamma_0^2 \times \{0\}^{g-2}$ and for all Gauss-reduced morphisms ϕ of rank 2, the set*

$$\left(C(\overline{\mathbb{Q}})+y\right) \cap \left(B_\phi + \mathcal{O}_{\varepsilon/H(\phi)^{1+1/(2n)}}\right)$$

is finite.

(ii) *For $\varepsilon \leq \varepsilon_4/(g+s)$ and for all special morphisms $\tilde{\phi} = (N\phi|\phi')$ of rank 2, the set*

$$(C(\overline{\mathbb{Q}}) \times \gamma) \cap \left(B_{\tilde{\phi}} + \mathcal{O}_{\varepsilon/H(\phi)^{1+1/(2n)}}\right)$$

is finite.

(Recall that $n = 2(g+s)-3$.)

Proof. (i) Choose

$$\eta \leq \eta_0 = \frac{1}{2^4(g+s)(g-1)^2}.$$

Define

$$m = \max\left(2, \left(\frac{K_1}{\epsilon_2(C,\eta)}\right)^{\frac{g-1}{1-8(g+s)(g-1)^2\eta}}\right),$$

and choose

$$\varepsilon \leq \min\left(\varepsilon_1, \frac{K_1}{g}, \frac{\epsilon_1(C,\eta)}{gm^{4n}}\right),$$

where $\epsilon_1(C,\eta)$ and $\epsilon_2(C,\eta)$ are as in Proposition 13.3.

Recall that $H(\phi)=a$. We distinguish two cases:

(1) $a_0 = \lfloor a^{1/(2n)} \rfloor \geq m$,

(2) $a_0 = \lfloor a^{1/(2n)} \rfloor \le m$.

Case (1): $a_0 \ge m$. Let $x + y \in (C(\overline{\mathbb{Q}}) + y) \cap (B_\phi + \mathcal{O}_{\varepsilon/a^{1+1/(2n)}})$, where

$$y = (y_1, y_2, 0, \dots, 0) \in \Gamma_0^2 \times \{0\}^{g-2}.$$

Then

$$\phi(x + y) = \phi(\xi)$$

for $\|\xi\| \le \varepsilon/a^{1+1/(2n)}$.

We have chosen $\varepsilon \le \varepsilon_1$, so $x \in S_2(C, (\Gamma_0^g)_{\varepsilon_1})$ which is a set of norm K_1. Then

$$\|x\| \le K_1.$$

Recall that $\Phi(z_1, \dots, z_g) = (a_0\phi(z), z_3, \dots, z_g)$. So

$$\Phi(x + y) = (a_0\phi(x + y), x_3, \dots, x_g) = (a_0\phi(\xi), x_3, \dots, x_g).$$

Therefore

$$\|\Phi(x + y)\| = \|(a_0\phi(\xi), x_3, \dots, x_g)\| \le \max\left(a_0\|\phi(\xi)\|, \|x\|\right).$$

Since $\|\xi\| \le \varepsilon a^{-(1+1/(2n))}$, $a_0 \le a^{1/(2n)}$ and $\varepsilon \le K_1/g$, we have

$$a_0\|\phi(\xi)\| \le a_0(g - r + 1)\frac{\varepsilon}{a^{1/(2n)}} \le K_1.$$

Also $\|x\| \le K_1$. Thus

$$\|\Phi(x + y)\| \le K_1.$$

In view of the hypothesis $a_0 \ge m$, we have

$$K_1 \le \epsilon_2(C, \eta) a_0^{\frac{1}{g-1} - 8(g+s)(g-1)\eta}.$$

In Proposition 13.3(ii) we have proved that

$$\epsilon_2(C, \eta) a_0^{\frac{1}{g-1} - 8(g+s)(g-1)\eta} < \mu(\Phi(C + y)).$$

So

$$\|\Phi(x + y)\| \le K_1 < \mu(\Phi(C + y)).$$

We deduce that $\Phi(x + y)$ belongs to the finite set

$$\Phi(C + y) \cap \mathcal{O}_{K_1}.$$

The morphism $C + y \to \Phi(C + y)$ has finite fiber. We can conclude that since $\varepsilon \le \min(\varepsilon_1, K_1/g)$, for every ϕ Gauss-reduced of rank 2 with $a_0 = \lfloor a^{1/(2n)} \rfloor \ge m$, the set

$$(C(\overline{\mathbb{Q}}) + y) \cap \left(B_\phi + \mathcal{O}_{\varepsilon/H(\phi)^{1+1/(2n)}}\right)$$

is finite.

Case (2): $a_0 \leq m$. Let $x+y \in (C(\overline{\mathbb{Q}})+y) \cap (B_\phi + \mathcal{O}_{\varepsilon/a^{1+1/(2n)}})$, where $y \in \Gamma_0^2 \times \{0\}^{g-2}$. Then

$$\phi(x+y) = \phi(\xi)$$

for $\|\xi\| \leq \varepsilon/a^{1+1/(2n)}$. However we have chosen $\varepsilon \leq \epsilon_1(C,\eta)/gm^{4n}$. Hence

$$\|\phi(x+y)\| = \|\phi(\xi)\| \leq \frac{g\varepsilon}{a^{1/(2n)}} \leq \frac{\epsilon_1(C,\eta)}{m^{4n}a^{1/(2n)}}.$$

We are working under the hypothesis $a_0 = \lfloor a^{1/(2n)} \rfloor \leq m$ and $m \geq 2$, so $a < (2a_0)^{2n} \leq m^{4n}$. Furthermore, $\eta \leq \eta_0 < \frac{1}{4n}$ implies that $a^{2\eta} < a^{1/(2n)}$. Thus

$$a^{1+2\eta} < m^{4n} a^{1/(2n)}.$$

And consequently

$$\|\phi(x+y)\| \leq \frac{\epsilon_1(C,\eta)}{m^{4n}a^{1/(2n)}} < \frac{\epsilon_1(C,\eta)}{a^{1+2\eta}}.$$

In Proposition 13.3(i) we proved that

$$\frac{\epsilon_1(C,\eta)}{a^{1+2\eta}} < \mu(\phi(C+y)).$$

We deduce that $\phi(x+y)$ belongs to the finite set

$$\phi(C+y) \cap \mathcal{O}_{\epsilon_1(C,\eta)m^{-4n}a^{-1/(2n)}}.$$

The morphism $C+y \to \phi(C+y)$ has finite fiber. Since $\varepsilon \leq \epsilon_1(C,\eta)/(gm^{4n})$, we conclude that for all ϕ Gauss-reduced of rank 2 with $a_0 = \lfloor a^{1/(2n)} \rfloor \leq m$, the set

$$(C(\overline{\mathbb{Q}})+y) \cap \left(B_\phi + \mathcal{O}_{\varepsilon/H(\phi)^{1+1/(2n)}}\right)$$

is finite.

For the curve C, define

$$\epsilon(C) = \min(\epsilon_1(C,\eta_0), \epsilon_2(C,\eta_0)).$$

Note that

$$\left(\frac{\epsilon(C)}{gK_1}\right)^{8(g+s)g} \leq \frac{\epsilon_1(C,\eta)}{gm^{4n}}.$$

Thus, we could for instance choose

$$\varepsilon_4 = \min\left(\varepsilon_1, \frac{K_1}{g}, \left(\frac{\epsilon(C)}{gK_1}\right)^{8(g+s)g}\right).$$

Proof of (ii). We want to show that, for every $\tilde{\phi} = (N\phi|\phi')$ special of rank 2, there exists ϕ Gauss-reduced of rank 2 and $y \in \Gamma_0^2 \times \{0\}^{g-2}$ such that the map

$(x, \gamma) \to x + y$ defines an injection

$$(C(\overline{\mathbb{Q}}) \times \gamma) \cap \left(B_{\tilde{\phi}} + \mathcal{O}_{\varepsilon/H(\phi)^{1+1/(2n)}}\right) \hookrightarrow (C(\overline{\mathbb{Q}}) + y) \cap \left(B_{\phi} + \mathcal{O}_{(g+s)\varepsilon/H(\phi)^{1+1/(2n)}}\right). \tag{13-4}$$

We then apply part (i) of this proposition; if $(g+s)\varepsilon \le \varepsilon_4$, then

$$(C(\overline{\mathbb{Q}}) + y) \cap \left(B_{\phi} + \mathcal{O}_{(g+s)\varepsilon/H(\phi)^{1+1/(2n)}}\right)$$

is finite. So if $\varepsilon \le \varepsilon_4/(g+s)$, the set

$$(C(\overline{\mathbb{Q}}) \times \gamma) \cap \left(B_{\tilde{\phi}} + \mathcal{O}_{\varepsilon/H(\phi)^{1+1/(2n)}}\right)$$

is finite too.

Let us prove the inclusion (13-4). Let $\tilde{\phi} = (N\phi|\phi')$ be special of rank 2. By definition of special $\phi = (aI_r|L)$ is Gauss-reduced of rank 2. Let

$$(x, \gamma) \in (C(\overline{\mathbb{Q}}) \times \gamma) \cap \left(B_{\tilde{\phi}} + \mathcal{O}_{\varepsilon/H(\phi)^{1+1/(2n)}}\right).$$

Then, there exists $\xi \in \mathcal{O}_{\varepsilon/H(\phi)^{1+1/(2n)}}$ such that

$$\tilde{\phi}((x, \gamma) + \xi) = 0.$$

Equivalently,

$$N\phi(x) + \phi'(\gamma) + \tilde{\phi}(\xi) = 0.$$

Let $y' \in E^2$ be a point such that

$$N[a]y' = \phi'(\gamma).$$

Since Γ_0 is a division group,

$$y = (y', 0, \dots, 0) \in \Gamma_0^2 \times \{0\}^{g-2}$$

and

$$N\phi(y) = N[a]y' = \phi'(\gamma).$$

Therefore

$$N\phi(x+y) + \tilde{\phi}(\xi) = 0.$$

Let $\xi'' \in E^2$ be a point such that

$$N[a]\xi'' = \tilde{\phi}(\xi).$$

We define $\xi' = (\xi'', \{0\}^{g-2})$. Then

$$N\phi(\xi') = N[a]\xi'' = \tilde{\phi}(\xi),$$

and

$$N\phi(x + y + \xi') = 0.$$

Since $\tilde{\phi}$ is special $H(\tilde{\phi}) = Na$. Furthermore $\|\xi\| \le \varepsilon/a^{1+1/(2n)}$. We deduce

$$\|\xi'\| = \|\xi''\| = \frac{\|\tilde{\phi}(\xi)\|}{Na} \le \frac{(g+s)\varepsilon}{a^{1+1/(2n)}}.$$

In conclusion

$$N\phi(x+y+\xi') = 0$$

with $\|\xi'\| \le (g+s)\varepsilon/a^{1+1/(2n)}$ and $y \in \Gamma_0^2 \times \{0\}^{g-2}$. Equivalently,

$$(x+y) \in (C(\overline{\mathbb{Q}})+y) \cap \left(B_{N\phi} + \mathbb{O}_{(g+s)\varepsilon/H(\phi)^{1+1/(2n)}}\right).$$

By Lemma 4.4(i), with $\psi = \phi$, we deduce that

$$(x+y) \in (C(\overline{\mathbb{Q}})+y) \cap \left(B_{\phi} + \mathbb{O}_{(g+s)\varepsilon/H(\phi)^{1+1/(2n)}}\right),$$

with $y \in \Gamma_0^2 \times \{0\}^{g-2}$ and ϕ Gauss-reduced of rank 2.

This proves relation (13-4) and concludes the proof. □

14. The effectiveness aspect

An effective weak height bound. We give an effective bound for the height of $S_1(C, \mathbb{O}_\varepsilon)$ for C transverse.

Theorem 14.1. *Let C be transverse. For every real $\varepsilon \ge 0$, the norm of the set $S_1(C, \mathbb{O}_\varepsilon)$ is bounded by $K_0 \max(1, \varepsilon)$, where K_0 is an effective constant depending on the degree and the height of C.*

Proof. If $x \in S_1(C, \mathbb{O}_\varepsilon)$, there exist $\phi : E^g \to E$ and $\xi \in \mathbb{O}_\varepsilon$ such that $\phi(x-\xi) = 0$. Now the proof follows that of [Viada 2003, Theorem 1, p. 55], where we replace $\hat{h}$ by h, y by ϕ, p by x and $\hat{h}(y(p)) = 0$ by $h(\phi(x)) = c_0(\deg\phi)h(\xi)$ with $h(\xi) \le \varepsilon^2$. □

The strong hypotheses and an effective weak theorem.

Proof of Theorem 1.6. The proof is similar to the proof of Theorem 1.5 given in Section 11.

Theorem 14.1 implies that for $r \ge 1$ the norm of the set $S_r(C, \mathbb{O}_1)$ is bounded by an effective constant K_0. Define

$$\eta_0 = \frac{1}{2^4 g^2},$$

$$\epsilon(C) = \min\big(\epsilon_1(C,\eta_0), \epsilon_2(C,\eta_0)\big), \quad \text{where } \epsilon_1, \epsilon_2 \text{ are as in Proposition 13.3},$$

$$\delta_1 = \frac{1}{g}\min\left(1, \frac{K_0}{g}, \left(\frac{\epsilon(C)}{gK_0}\right)^{8g^2}\right),$$

$$\delta = \delta_1 M^{-1-\frac{1}{2(2g-3)}}, \qquad \text{where } M = \max\left(2, \left\lceil \frac{K_0}{\delta_1}\right\rceil^2\right)^{2g-3}.$$

In Section 12, Proposition A(i) with $\Gamma = 0$, $\varepsilon_1 = 1$ and $K_1 = K_0$, we have shown that

$$\bigcup_{\substack{\phi \text{ Gauss-reduced} \\ \mathrm{rk}(\phi)=2}} C(\overline{\mathbb{Q}}) \cap \left(B_\phi + \mathbb{O}_\delta\right) \subset \bigcup_{\substack{\phi \text{ Gauss-reduced} \\ \mathrm{rk}(\phi)=2 \;\; H(\phi)\le M}} C(\overline{\mathbb{Q}}) \cap \left(B_\phi + \mathbb{O}_{g\delta_1/H(\phi)^{1+1/(2(2g-3))}}\right).$$

In Section 13, Proposition B(i) with $y = 0$, $s = 0$ and $n = 2g-3$, $K_1 = K_0$, we have shown that for all ϕ Gauss-reduced of rank 2, the set

$$C(\overline{\mathbb{Q}}) \cap \left(B_\phi + \mathbb{O}_{g\delta_1/H(\phi)^{1+1/(2(2g-3))}}\right)$$

is finite. It follows that

$$\bigcup_{\substack{\phi \text{ Gauss-reduced} \\ \mathrm{rk}(\phi)=2}} C(\overline{\mathbb{Q}}) \cap (B_\phi + \mathbb{O}_\delta)$$

is finite. By Lemma 4.5(i) we deduce that $S_2(C, \mathbb{O}_\delta)$ is finite. This shows that Theorem 1.6 holds for

$$\varepsilon \le \frac{1}{g^{4g}} \min(1, K_0^{-1})^{4g} \min\left(1, K_0, \left(\frac{\epsilon(C)}{gK_0}\right)^{8g^2}\right)^{4g}. \qquad \square$$

An effective bound for the cardinality of the sets. We have just shown that for C transverse, ε can be made effective. The purpose of this section is to indicate an effective bound for the cardinality of $S_2(C, \mathbb{O}_\varepsilon)$, under the following conjecture:

Conjecture 14.2 (S. David; personal communication). *Let C be a transverse curve in A. There exist constants c' and c'', each depending on g, $\deg_L A$, $h_L(A)$, $[k:\mathbb{Q}]$, such that, for*

$$\epsilon(C) = \frac{c'}{(\deg_L V)^{1/(2 \text{ codim } V)}} \quad \textit{and} \quad \Theta(C) = c''(\deg_L C)^g,$$

the cardinality of $C(\overline{\mathbb{Q}}) \cap \mathbb{O}_{\epsilon(C)}$ is bounded by $\Theta(C)$.

This is the abelian analogue to [Amoroso and David 2003, Conjecture 1.2].

Theorem 14.3. *Let C be transverse. Assume that Conjecture 14.2 holds. Then, there exists an effective $\varepsilon > 0$ such that the cardinality of $S_2(C, \mathbb{O}_\epsilon)$ is bounded by an effective constant.*

Proof. Let δ and δ_1 be as defined in the previous proof.

By Proposition A(i) in Section 12 we deduce that

$$S_2(C, \mathbb{O}_\delta) \subset \bigcup_{\substack{\phi \text{ Gauss-reduced} \\ H(\phi)\le M}} C(\overline{\mathbb{Q}}) \cap \left(B_\phi + \mathbb{O}_{g\delta_1/H(\phi)^{1+1/(2(2g-3))}}\right).$$

Note that, for any curve D and positive integers n, the cardinality of $[n]D \cap \mathbb{O}_{n\epsilon(D)}$ is still $\Theta(D)$. Going through the proofs of Proposition B(i) in Section 13, we see that

$$\#S_2(C, \mathbb{O}_\delta) \leq \sum_{H(\phi)\leq M} \#\big(\phi_{|C}^{-1}(\phi(C) \cap \mathbb{O}_{\epsilon(\phi(C))})\big),$$

where $\phi_{|C} : C \to \phi(C)$ is the restriction of ϕ to C. Recall from [Viada 2003, p. 61] that the fiber of $\phi_{|C}$ has cardinality at most $3gH(\phi)^2 \leq 3gM^2$. We set

$$\mathbf{\Delta}_{\max} = \max_{H(\phi)\leq M} \#(\phi(C) \cap \mathbb{O}_{\epsilon(\phi(C))}).$$

We deduce

$$\#S_2(C, \mathbb{O}_\delta) \leq 3gM^3 \mathbf{\Delta}_{\max}.$$

By Lemma 13.2(i), $\deg \phi(C) \leq (3gH(\phi))^2 \deg C$. Conjecture 14.2 implies that

$$\mathbf{\Delta}_{\max} \leq (3gH(\phi))^{2g} \Theta(C),$$

with $\Theta(C)$ explicitly given. We conclude that

$$\#S_2(C, \mathbb{O}_\delta) \leq (3g)^{2g+1} M^{2g+3} \Theta(C). \tag{14-1}$$

By Theorem 14.1 the constant K_0 is effective. So M is also effective. Thus the bound (14-1) is effective, for C transverse. □

Similar computations imply a bound for the cardinality of $S_2(C, \Gamma_\delta)$.

For $\delta \leq \varepsilon_4 (g+s)^{-2} M'^{-1-1/(4g+4s-6)}$ we obtain

$$\#S_2(C, \Gamma_\delta) \leq c_1(g) M'^{c_2(g,s)} \Theta(C).$$

Here $c_1(g)$ (and $c_2(g, s)$) are effective constants depending only on g (and s). The number M' depends explicitly on C, g and K_2, while ε_4 depends explicitly on C, g, s and K_1. In view of Theorem 9.1, the above bound also implies a bound for the cardinality of $S_2(C \times \gamma, \mathbb{O}_{\delta/(g+s)K_4})$.

However, Theorem 1.2 does not give effective K_1 or K_2. Consequently neither M' nor ε_4 are effective. An effective estimate for K_1 or K_2 would imply an effective Mordell Conjecture. This gives an indication of the difficulty to extend effective height proofs from transverse curves to weak-transverse curves.

15. Final remarks

The CM case. The proofs in 2–7 hold whether or not E has CM. Since Conjecture 1.4 is stated for any E, Proposition B holds unchanged for E with CM.

We can extend Proposition A to Gauss-reduced $\phi \in M_{r,g}(\mathbb{Z} + \tau\mathbb{Z})$ as follows. Decompose $\phi = \phi_1 + \tau\phi_2$ for $\phi_i \in M_{r,g}(\mathbb{Z})$, then let the morphism $\psi = (\phi_1|\phi_2)$ act on $(x, \tau x) + (y, \tau y) + (\xi, \tau\xi)$ for $x \in S_r(C, (\Gamma_0^g)_\varepsilon)$, $y \in \Gamma_0^g$ and $\xi \in \mathbb{O}_\varepsilon$. Apply Proposition A to ψ. Constants will depend on τ.

From powers to products. In a power there are more algebraic subgroups than in a product where not all the factors are isogenous. If we consider a product of non-CM elliptic curves, then the matrix of a morphism ϕ is simply an integral matrix where the entries corresponding to nonisogenous factors are zeros. So nothing changes with respect to our proofs.

If the curve is in a product of elliptic curves in general, we extend the definition of Gauss-reduced, introducing constants $c_1(\tau)$ and $c_2(\tau)$, such that the element a on the diagonal has norm satisfying $c_1(\tau)H(\phi) \leq |a| \leq c_2(\tau)H(\phi)$.

We leave the details to the reader.

Acknowledgments

My deepest thanks go to the referee for his precious comments, which encouraged me to drastically improve a first manuscript.

I kindly thank Francesco Amoroso and Özlem Imamoglu for inspiring me to pursue research in mathematics.

I thank the Centro de Giorgi and in particular Umberto Zannier for inviting me to the Diophantine Geometry Semester in 2005. I gave there a talk where the core material of this paper was presented.

I thank the SNF for the financial support which allows me to work serenely near my family.

It is to my husband Robert that I am most thankful; without him I would have given up long ago and I would not know how nice it is to be happy.

References

[Amoroso and David 1999] F. Amoroso and S. David, "Le problème de Lehmer en dimension supérieure", *J. Reine Angew. Math.* **513** (1999), 145–179. MR 2001a:11116 Zbl 1011.11045

[Amoroso and David 2003] F. Amoroso and S. David, "Minoration de la hauteur normalisée dans un tore", *J. Inst. Math. Jussieu* **2**:3 (2003), 335–381. MR 2004m:11101 Zbl 1041.11048

[Bombieri et al. 1999] E. Bombieri, D. Masser, and U. Zannier, "Intersecting a curve with algebraic subgroups of multiplicative groups", *Internat. Math. Res. Notices* 20 (1999), 1119–1140. MR 2001c:11081 Zbl 0938.11031

[David and Hindry 2000] S. David and M. Hindry, "Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type C. M", *J. Reine Angew. Math.* **529** (2000), 1–74. MR 2001j:11054 Zbl 0993.11034

[David and Philippon 2002] S. David and P. Philippon, "Minorations des hauteurs normalisées des sous-variétés de variétés abeliennes, II", *Comment. Math. Helv.* **77**:4 (2002), 639–700. MR 2004a:11055 Zbl 1030.11026

[David and Philippon 2007] S. David and P. Philippon, "Minorations des hauteurs normalisées des sous-variétés des puissances des courbes elliptiques", *Int. Math. Res. Pap.* 3 (2007), ID rpm006. MR 2355454 Zbl 05238017

[Galateau 2007] A. Galateau, *Problème de Bogomolov sur les variétées abéliennes*, Ph.D. thesis, Université de Paris VI, 2007, Available at http://tel.archives-ouvertes.fr/tel-00203583.

[Habegger 2007] P. Habegger, *Heights and multiplicative relations on algebraic varieties*, Ph.D. thesis, Universität Basel, 2007, Available at http://pages.unibas.ch/diss/2007/DissB_7940.htm.

[Hindry 1988] M. Hindry, "Autour d'une conjecture de Serge Lang", *Invent. Math.* **94**:3 (1988), 575–603. MR 89k:11046 Zbl 0638.14026

[Poonen 1999] B. Poonen, "Mordell–Lang plus Bogomolov", *Invent. Math.* **137**:2 (1999), 413–425. MR 2001c:11070 Zbl 0995.11040

[Rémond and Viada 2003] G. Rémond and E. Viada, "Problème de Mordell–Lang modulo certaines sous-variétés abéliennes", *Int. Math. Res. Not.* 35 (2003), 1915–1931. MR 2004h:11054 Zbl 1072.11038

[Schlickewei 1997] H. P. Schlickewei, "Lower bounds for heights on finitely generated groups", *Monatsh. Math.* **123**:2 (1997), 171–178. MR 98d:11077 Zbl 0973.11067

[Schmidt 1980] W. M. Schmidt, *Diophantine approximation*, Lecture Notes in Mathematics **785**, Springer, Berlin, 1980. MR 81j:10038 Zbl 0421.10019

[Ullmo 1998] E. Ullmo, "Positivité et discrétion des points algébriques des courbes", *Ann. of Math.* (2) **147**:1 (1998), 167–179. MR 99e:14031 Zbl 0934.14013

[Viada 2003] E. Viada, "The intersection of a curve with algebraic subgroups in a product of elliptic curves", *Ann. Sc. Norm. Super. Pisa Cl. Sci.* (5) **2**:1 (2003), 47–75. MR 2004c:11099 Zbl 05019603

[Zhang 1998] S.-W. Zhang, "Equidistribution of small points on abelian varieties", *Ann. of Math.* (2) **147**:1 (1998), 159–165. MR 99e:14032 Zbl 0991.11034

Communicated by Bjorn Poonen
Received 2007-04-12 Revised 2008-04-02 Accepted 2008-04-04

viada@math.ethz.ch *Université de Fribourg Suisse, Pérolles, Département de Mathématiques, 23 Chemin du Musée, CH-1700 Fribourg, Suisse*