Easy scalar decompositions for efficient scalar multiplication on elliptic curves and genus 2 Jacobians

Benjamin Smith

Easy scalar decompositions for efficient scalar multiplication on elliptic curves and genus 2 Jacobians

Benjamin Smith

Abstract. The first step in elliptic curve scalar multiplication algorithms based on scalar decompositions using efficient endomorphisms—including Gallant–Lambert–Vanstone (GLV) and Galbraith–Lin–Scott (GLS) multiplication, as well as higher-dimensional and higher-genus constructions—is to produce a short basis of a certain integer lattice involving the eigenvalues of the endomorphisms. The shorter the basis vectors, the shorter the decomposed scalar coefficients, and the faster the resulting scalar multiplication. Typically, knowledge of the eigenvalues allows us to write down a long basis, which we then reduce using the Euclidean algorithm, Gauss reduction, LLL, or even a more specialized algorithm.

In this work, we use elementary facts about quadratic rings to immediately write down a short basis of the lattice for the GLV, GLS, GLV+GLS, and $\mathbb{Q}$-curve constructions on elliptic curves, and for genus 2 real multiplication constructions. We do not pretend that this represents a significant optimization in scalar multiplication, since the lattice reduction step is always an offline precomputation—but it does give a better insight into the structure of scalar decompositions. In any case, it is always more convenient to use a ready-made short basis than it is to compute a new one.

1. Introduction

Scalar multiplication on elliptic curves (or Jacobians of genus 2 curves) is a key operation in many modern asymmetric cryptographic primitives. The classic scenario is as follows: let $\mathcal{G} \subset \mathcal{A}(\mathbb{F}_q)$ be a cyclic subgroup of order N, where $\mathcal{A}$ is an elliptic curve or an abelian surface over a finite field $\mathbb{F}_q$. Given an integer m (typically on the order of N) and a point P in $\mathcal{G}$, our goal is to compute

$$[m]P := \underbrace{P + P + \cdots + P}_{m \text{ times}}$$

as quickly as possible.

Since elliptic curve scalar multiplication is analogous to exponentiation in finite fields, many algorithms originally developed with the multiplicative groups of finite fields (or general abelian groups) in mind transfer directly to scalar multiplication: square-and-multiply loops in finite fields become double-and-add loops on elliptic curves, for example. However, the geometry of elliptic curves can offer us new algorithms with no true finite field analogues. A spectacular (and easy) example of this phenomemon is scalar multiplication with endomorphism decompositions, originally proposed by Gallant, Lambert, and Vanstone [**10**]. We present a general version of their idea below that is flexible enough to accommodate higher-dimensional and higher-genus constructions.

The general scalar decomposition technique. Let $\mathcal{A}$, $\mathcal{G}$, and N be as above, and let $\phi_1, \ldots, \phi_r$ be $\mathbb{F}_q$-endomorphisms of $\mathcal{A}$. We lose nothing by supposing $\phi_1 = 1$. In contrast to [**19**], we do *not* suppose that the ϕ_i form a linearly independent set.

Suppose that $\phi_i(\mathcal{G}) \subseteq \mathcal{G}$ for $1 \leq i \leq r$ (this is the typical situation in cryptographic applications, where N is so close to $\#\mathcal{A}(\mathbb{F}_q)$ that there is no room for the image of $\mathcal{G}$ to be anything but $\mathcal{G}$ itself); then each ϕ_i restricts to an endomorphism of $\mathcal{G}$. But $\mathcal{G}$ is a cyclic group, isomorphic to $\mathbb{Z}/N\mathbb{Z}$, and as such each of its endomorphisms is multiplication by some integer (defined modulo N). In particular, each endomorphism ϕ_i acts on $\mathcal{G}$ as multiplication by an integer *eigenvalue* $-N/2 < \lambda_{\phi_i} \leq N/2$, such that

$$\phi_i|_{\mathcal{G}} = [\lambda_{\phi_i}]_{\mathcal{G}} \ .$$

Definition 1. Let D be the $\mathbb{Z}$-module homomorphism

$$\begin{array}{rrcl} D: & \mathbb{Z}\phi_1 \oplus \cdots \oplus \mathbb{Z}\phi_r & \longrightarrow & \mathbb{Z}/N\mathbb{Z} \\ & (a_1, \ldots, a_r) & \longmapsto & a_1\lambda_{\phi_1} + \cdots + a_r\lambda_{\phi_r} \ ; \end{array}$$

an r-dimensional[1] *decomposition* of a scalar m is any element of $D^{-1}(m)$.

Returning to the scalar multiplication problem: we can compute $[m]P$ for any P in $\mathcal{G}$ by using a multiexponentiation algorithm on the points $\phi_1(P), \ldots, \phi_r(P)$ to compute

$$[m]P = [a_1]\phi_1(P) \oplus \cdots \oplus [a_r]\phi_r(P) \qquad \text{for any} \quad (a_1, \ldots, a_r) \in D^{-1}(m) \ .$$

[1] We emphasize that the dimension of r of a decomposition has no relation to the dimension of $\mathcal{A}$, or to the $\mathbb{Z}$-rank of the endomorphism ring. Typical values for r are $r = 1$, corresponding to classical scalar multiplication; $r = 2$, as in in Gallant–Lambert–Vanstone [**10**] and Galbraith–Lin–Scott [**9**] multiplication; and $r = 4$, as proposed by Longa and Sica [**19**] and Guillevic and Ionica [**12**]. A technique with $r = 3$ was proposed by Zhou, Hu, Xu, and Song [**32**], but this is essentially Longa–Sica with $a_4 = 0$. Bos, Costello, Hisil, and Lauter have implemented a genus 2 scalar multiplication with $r = 8$, but this seems to be the upper limit of practicality for these techniques [**3**].

The literature on exponentation and multiexponentiation algorithms is vast, and we will not attempt to summarize it here (but for an introduction to general exponentation and multiexponentation algorithms, we recommend [**8**, §2.8,§11.2] and [**7**, Chapter 9]). For the purposes of this article, it suffices to note that for the scalar decomposition technique to offer an advantage over simply computing $[m]P$ as a conventional exponentiation,

The endomorphisms must be *efficient*: that is, any $\phi_i(P)$ must be computable for the cost of a few group operations, and

The decomposition must be *short*: that is,

$$\|(a_1, \ldots, a_r)\|_\infty = \max_i |a_i|$$

should be significantly smaller than $|m|$, which is typically on the order of N.

In this article, we suppose that we are given a fixed set of efficient ϕ_i, and concentrate on the problem of computing short scalar decompositions. First, consider the lattice of decompositions of 0:

$$\mathcal{L} := \ker D = \langle (z_1, \ldots, z_r) \in \mathbb{Z}^r \mid z_1\lambda_{\phi_1} + \cdots + z_r\lambda_{\phi_r} \equiv 0 \pmod{N} \rangle \ .$$

The set of decompositions of any m in $\mathbb{Z}/N\mathbb{Z}$ is then the lattice coset

$$D^{-1}(m) = (m, 0, \ldots, 0) + \mathcal{L} \ .$$

To find a short decomposition of m, we can subtract a nearby vector in $\mathcal{L}$ from $(m, 0, \ldots, 0)$. The reference technique for finding such a vector in $\mathcal{L}$ is Babai rounding [**1**], which works as follows: if $\mathbf{b}_1, \ldots, \mathbf{b}_r$ is a basis for $\mathcal{L}$, then we let $(\alpha_1, \ldots, \alpha_r)$ be the (unique) solution in $\mathbb{Q}^r$ to the linear system

$$(m, 0, \ldots, 0) = \sum_{i=1}^{r} \alpha_i \mathbf{b}_i \ ,$$

and set

$$(a_1, \ldots, a_r) := (m, 0, \ldots, 0) - \sum_{i=1}^{r} \lfloor \alpha_i \rceil \mathbf{b}_i \ ;$$

then $(a_1, \ldots, a_r)$ is an r-dimensional decomposition of m. Since

$$(a_1, \ldots, a_r) = \sum_{i=1}^{r} (\alpha_i - \lfloor \alpha_i \rceil) \mathbf{b}_i$$

and $|x - \lfloor x \rceil| \leq 1/2$ for any x in $\mathbb{Q}$, we have

$$\|(a_1, \ldots, a_r)\|_\infty \leq \frac{r}{2} \max_i \|\mathbf{b}_i\|_\infty \ .$$

It is clear, therefore, that finding short decompositions depends on finding a short basis for $\mathcal{L}$. Note that $\mathcal{L}$ depends only on the ϕ_i, and not on the eventual scalars m or points P to be multiplied; as such, the short basis can (and should) be precomputed. Assuming that the eigenvalues have pairwise differences of absolute value at least $N^{1/r}$, there exists a basis with

$\max_i \|\mathbf{b}\|_\infty$ in $O(N^{1/r})$, which will yield scalar decompositions of bitlength around $\frac{1}{r}\log_2 N$.

In most of the scalar decomposition literature, a short basis of $\mathcal{L}$ is produced by starting with a long basis —typically the basis

$$\begin{aligned}
\mathbf{b}_1 &= (N, 0, \ldots, 0) \ , \\
\mathbf{b}_2 &= (-\lambda_{\phi_2}, 1, 0, \ldots, 0) \ , \\
\mathbf{b}_3 &= (-\lambda_{\phi_3}, 0, 1, 0, \ldots, 0) \ , \\
&\ \vdots \\
\mathbf{b}_r &= (-\lambda_{\phi_r}, 0, \ldots, 1)
\end{aligned}$$

—before applying a lattice reduction algorithm to produce a short basis. For $r = 2$, Gallant, Lambert, and Vanstone used the Euclidean algorithm, which is equivalent to the usual Gauss lattice reduction algorithm (though Kaib's algorithm for the infinity norm [**15**] may give marginally better results). In higher dimensions, we would typically use a fast LLL variant (such as `fpLLL` [**5**])—though Longa and Sica [**19**] went so far as to propose a new 4-dimensional lattice basis reduction algorithm for their GLV+GLS construction on elliptic curves.

Our contribution: ready-made short bases. Our contention in this article is that in most cryptographic situations, no lattice basis reduction is required to find a short basis of $\mathcal{L}$: one can simply write down vectors of length at most $O(\#\mathcal{A}(\mathbb{F}_q)^{1/r})$ from scratch. The information that allows us to do so is typically a by-product of the group order computation (or of the CM method). For the abelian varieties most useful in cryptography, these vectors either form a basis for $\mathcal{L}$, or can be easily modified to do so.

Galbraith, Lin, and Scott [**9**] and the author [**26**] have already constructed families of endomorphisms equipped with a convenient ready-made basis; in this work, we generalize these ready-made bases to all of the other known efficient endomorphism constructions for elliptic curves and to real multiplication techniques for genus 2 Jacobians. In this way, we construct explicit short bases for the Galbraith–Lin–Scott (GLS), Gallant–Lambert–Vanstone (GLV), Guillevic–Ionica [**12**], Longa–Sica, and $\mathbb{Q}$-curve reduction techniques, as well as for the Kohel–Smith [**17**] and Takashima [**28**] methods for genus 2 Jacobians.

We do not pretend that this is a significant optimization for scalar decomposition methods: the construction of a short basis is essentially a one-shot precomputation, and existing lattice basis reduction methods are certainly fast enough on the relevant input sizes. However, the construction of these "instant" bases turns out to be an illuminating exercise: short bases can be read off from they are simple endomorphism ring relations that are, in practice, known in advance. The bottom line is that it is always more convenient to not compute something than it is to compute it.

2. Relations between quadratic orders

We recall some elementary facts from the theory of quadratic fields. Further details and proofs can be found in almost any basic algebraic number theory text (we recommend [**27**]).

Let K be a quadratic field, real or imaginary, with maximal order $\mathcal{O}_K$ and discriminant Δ_K. If ξ is an element of $\mathcal{O}_K$ then we write t_ξ for its trace, n_ξ for its norm. If ξ is not in $\mathbb{Z}$, then it generates an order $\mathbb{Z}[\xi]$ in $\mathcal{O}_K$; we write $\Delta(\xi) = t_\xi^2 - 4n_\xi$ for the discriminant of $\mathbb{Z}[\xi]$, and $P_\xi(T) = T^2 - t_\xi T + n_\xi$ for the minimal polynomial of ξ. The discriminants of $\mathcal{O}_K$ and $\mathbb{Z}[\xi]$ are related by $\Delta(\xi) = c_\xi^2 \Delta_K$ for some positive integer c_ξ, the conductor of $\mathbb{Z}[\xi]$ in $\mathcal{O}_K$.

The set of orders in K form a lattice (in the combinatorial sense), indexed by the conductor: $\mathbb{Z}[\xi] \subset \mathbb{Z}[\xi']$ if and only if $c_{\xi'} \mid c_\xi$. If $\mathbb{Z}[\xi] \subset \mathbb{Z}[\xi']$ are orders in K, then necessarily

$$\xi = c\xi' + b \tag{1}$$

for some integers b and c. It follows that

$$b = \frac{1}{2}\left(t_\xi - c t_{\xi'}\right) \qquad \text{and} \qquad c^2 = \frac{\Delta(\xi)}{\Delta(\xi')} \ . \tag{2}$$

Note that c is, up to sign, the relative conductor of $\mathbb{Z}[\xi]$ in $\mathbb{Z}[\xi']$. Multiplying Eq. (1) through by $t_{\xi'} - \xi'$, which is also $n_{\xi'}/\xi'$, we obtain a second relation

$$\xi\xi' - t_{\xi'}\xi - b\xi' + (cn_{\xi'} + bt_{\xi'}) = 0 \ . \tag{3}$$

The following lemma turns the relations between endomorphisms of Eqs. (1) and (3) into relations between eigenvalues, which we will use later to produce short lattice vectors.

Lemma 1. *Let ξ and ξ' be endomorphisms of an abelian variety $\mathcal{A}/\mathbb{F}_q$ such that $\mathbb{Z}[\xi]$ and $\mathbb{Z}[\xi']$ are quadratic rings and $\mathbb{Z}[\xi] \subseteq \mathbb{Z}[\xi']$, so $\xi = c\xi' + b$ for some integers b and c. Let $\mathcal{G} \subset \mathcal{A}$ be a cyclic subgroup of order N such that $\xi(\mathcal{G}) \subseteq \mathcal{G}$ and $\xi'(\mathcal{G}) \subseteq \mathcal{G}$, and let λ and λ' be the eigenvalues in $\mathbb{Z}/N\mathbb{Z}$ of ξ and ξ' on $\mathcal{G}$, respectively. Then*

$$\lambda - c\lambda' - b \equiv 0 \pmod{N} \quad \textit{and}$$
$$\lambda\lambda' - t_{\xi'}\lambda - b\lambda' + cn_{\xi'} + bt_{\xi'} \equiv 0 \pmod{N} \ .$$

Proof. This follows immediately by mapping the relations in Eqs. (1) and (3) through the homomorphism $\mathbb{Z}[\xi'] \to \mathrm{End}(\mathcal{G}) \cong \mathbb{Z}/N\mathbb{Z}$ sending ξ' to $\lambda' \pmod{N}$ (and ξ to $\lambda \pmod{N}$). □

3. General two-dimensional decompositions for elliptic curves

Let $\mathcal{E}/\mathbb{F}_q$ be an ordinary elliptic curve. If π is the q-power Frobenius endomorphism on $\mathcal{E}$ then

$$P_\pi(T) = T^2 - t_\pi T + q \ ,$$

where

$$|t_\pi| \leq 2\sqrt{q} \qquad \text{and} \qquad \Delta_\pi := t_\pi^2 - 4q < 0 \ .$$

THEOREM 2. *Let ϕ be a non-integer endomorphism of $\mathcal{E}$ such that $\mathbb{Z}[\pi] \subset \mathbb{Z}[\phi]$, so $\pi = c\phi + b$ for some integers c and b. Suppose that we are in the situation of §1 with $\mathcal{A} = \mathcal{E}$ and $(\phi_1, \phi_2) = (1, \phi)$. The vectors*

$$\mathbf{b}_1 = (b-1, c) \qquad \textit{and} \qquad \mathbf{b}_2 = (c\deg(\phi) + (b-1)t_\phi, 1-b)$$

generate a sublattice of $\mathcal{L}$ of determinant $\#\mathcal{E}(\mathbb{F}_q)$. If $\mathcal{G} = \mathcal{E}(\mathbb{F}_q)$, then $\mathcal{L} = \langle \mathbf{b}_1, \mathbf{b}_2 \rangle$.

PROOF. The Frobenius endomorphism π fixes the points in $\mathcal{E}(\mathbb{F}_q)$, so $\pi(\mathcal{G}) = \mathcal{G}$ and the eigenvalue of π on $\mathcal{G}$ is $\lambda_\pi = 1$. Applying Lemma 1 with $(\xi, \xi') = (\pi, \phi)$ and $(\lambda, \lambda') = (1, \lambda_\phi)$, we obtain relations

$$\begin{aligned} (b-1) \cdot 1 + c \cdot \lambda &\equiv 0 \pmod{N} \qquad \text{and} \\ ((b-1)t_\phi + cn_\phi) \cdot 1 + (1-b) \cdot \lambda &\equiv 0 \pmod{N} \ . \end{aligned}$$

The first implies that $\mathbf{b}_1$ is in $\mathcal{L}$, the second that $\mathbf{b}_2$ is in $\mathcal{L}$. Equations (2) imply that

$$\det(\langle \mathbf{b}_1, \mathbf{b}_2 \rangle) = (b-1)^2 + c(c\deg(\phi) + (b-1)t_\phi) = q - t_\pi + 1 \ ,$$

which is $\#\mathcal{E}(\mathbb{F}q)$. □

Theorem 2 constructs two basis vectors, but it makes no claim about their length. We can give some almost-trivial bounds on the size of b and c, using $4q - t_\pi^2 = -c^2\Delta(\phi)$, $b = \frac{1}{2}(t_\pi - ct_\phi)$, and the triangle inequality:

$$|c| = 2\sqrt{q}\sqrt{((t_\pi/2\sqrt{q})^2 - 1)/\Delta(\phi)} \qquad \text{and} \qquad |b| \leq \frac{1}{2}|t_\pi| + \frac{1}{2}|t_\phi||c| \ . \tag{4}$$

But proving general bounds that apply for arbitrary endomorphisms is probably the wrong approach when all of the endomorphisms used in practical scalar decompositions are special (and deliberately non-general) constructions. Consider the Ciet–Sica–Quisquater bounds of [**6**, Theorem 1] for the case $r = 2$ of §1: for every integer m, there exists a decomposition (a_1, a_2) of m such that $\|(a_1, a_2)\|_\infty \leq C\sqrt{N}$, with $C = (1 + |t_\phi| + n_\phi)^{1/2}$. In terms of bitlength,

$$\log_2 \|(a, b)\|_\infty \leq \tfrac{1}{2}\log_2 N + \tfrac{1}{2}\log_2(1 + |t_\phi| + n_\phi) \ . \tag{5}$$

In this theorem, t_ϕ and n_ϕ (and C) are implicitly treated as constants—that is, independent of N and q. While this is appropriate for GLV curves, t_ϕ and n_ϕ are not "constant" when ϕ is inseparable (notably, n_ϕ is divisible by p). In this case, the bound above is spectacularly loose: Remark 3 below gives a detailed example of this in the context of GLS endomorphisms.

4. Shrinking the basis (or expanding the sublattice) to fit $\mathcal{G}$

Let h be the cofactor such that $\#\mathcal{E}(\mathbb{F}_q) = hN$. By the Pohlig–Hellman–Silver reduction [**23**], the cryptographic strength of $\mathcal{E}$ depends entirely on the size of the prime N, so we should choose $\mathcal{E}$ with N as large as possible. While $h = 1$ is ideal, allowing $h = 2$ or 4 permits faster curve arithmetic via transformations to Montgomery [**22**] or twisted Edwards [**14**] models, for example. (In the pairing-based context h may be somewhat larger.)

The lattice $\mathcal{L}$ has determinant N, but the vectors $\mathbf{b}_1, \mathbf{b}_2$ constructed by Theorem 2 are a basis for a (sub)lattice of determinant hN. If $h \neq 1$, then while our sublattice will still give short decompositions, it is suboptimal. If $h = 4$, for example, then our basis may be one bit too long—which generally means one double too many when the resulting decompositions are used in a multiexponentiation algorithm.

If for some reason $\mathcal{G} \neq \mathcal{E}(\mathbb{F}_q)$, then we want to be able to derive a basis of the full lattice $\mathcal{L}$ from $\mathbf{b}_1, \mathbf{b}_2$. First, note that

$$\left\langle \tfrac{1}{g}\mathbf{b}_1 \ , \tfrac{1}{g}\mathbf{b}_2 \right\rangle \subseteq \mathcal{L} \qquad \text{where} \qquad g = \gcd(c, b-1) \ ,$$

because the relations $(b-1) + c\lambda \equiv 0 \pmod{N}$ and $c\deg(\phi) + (b-1)t_\phi + (b-1)\lambda \equiv 0 \pmod{N}$ still hold when we divide through by g. This new sublattice has index $\#\mathcal{E}(\mathbb{F}_q)/(g^2N)$ in $\mathcal{L}$. Note that if $g \neq 1$, then $\mathcal{E}[g] \subset \mathcal{E}(\mathbb{F}_q)$, because $\pi - 1 = g((c/g)\phi + (b-1)/g)$, so $\pi - 1$ factors through $[g]$.

More generally, suppose ℓ is a prime dividing h: then there exists a sublattice $\mathcal{L}'$ such that

$$\langle \mathbf{b}_1, \mathbf{b}_2 \rangle \subset \mathcal{L}' \subseteq \mathcal{L} \qquad \text{with} \qquad [\mathcal{L}' : \langle \mathbf{b}_1, \mathbf{b}_2 \rangle] = \ell \ .$$

Looking at the components of $\mathbf{b}_1$ and $\mathbf{b}_2$, we see that if ℓ divides c, then it must also divide $b-1$ (otherwise $\mathcal{L}'$ cannot exist),[2] and we can replace each $\mathbf{b}_i$ with $\frac{1}{\ell}\mathbf{b}_i$ as above to produce a sublattice of index h/ℓ^2 in $\mathcal{L}$.

Suppose now that ℓ does not divide c. If ℓ divides $b-1$ and $\deg\phi$, then $\frac{1}{\ell}\mathbf{b}_2$ is in $\mathcal{L}$, so we can take $\mathcal{L}' = \langle \mathbf{b}_1, \frac{1}{\ell}\mathbf{b}_2 \rangle$. Otherwise, $\frac{1}{\ell}(\mathbf{b}_1 + i\mathbf{b}_j)$ is in $\mathcal{L}$ for precisely one $0 < i < \ell$: that is, $i = -c(b-1)^{-1} \bmod \ell$. We can therefore take $\mathcal{L}' = \langle \mathbf{b}_1, \frac{1}{\ell}(\mathbf{b}_1 + i\mathbf{b}_2) \rangle$.

Iterating this process factor by factor of h, we can gradually shrink the vectors produced by Theorem 2 to derive a true basis of $\mathcal{L}$. But as we remarked above, in conventional discrete-log based cryptography the most important cases are $h = 1, 2$, and 4, and then there is almost nothing to be done. To handle the cases where $\mathcal{E}(\mathbb{F}_q) \cong \mathcal{G} \oplus \mathbb{Z}/2\mathbb{Z}$ or $\mathcal{G} \oplus (\mathbb{Z}/2\mathbb{Z})^2$, for example, the following simple procedure produces a basis for $\mathcal{L}$:

- If c is even, then $\mathcal{L} = \langle \frac{1}{2}\mathbf{b}_1, \frac{1}{2}\mathbf{b}_2 \rangle$.

[2] It is possible to take a much more highbrow view of all this: Theorem 1 of [**18**] implies that if $\mathcal{E}[\ell] \subseteq \mathcal{E}(\mathbb{F}_q)$ then ℓ must divide the conductor of $\mathbb{Z}[\pi]$ in the endomorphism ring of $\mathcal{E}$ (see also [**16**, p. 40]). In this case ℓ divides both $\pi - 1$ and $c\phi$, so it must also divide $b-1$. Removing the factor of ℓ^2 from the index of our sublattice therefore corresponds to removing the contribution of the full ℓ-torsion to our endomorphism relations.

- If c and b are odd and $\deg \phi$ is even, then $\mathcal{L} = \left\langle \mathbf{b}_1, \frac{1}{2}\mathbf{b}_2 \right\rangle$.
- Otherwise, $\mathcal{L} = \left\langle \mathbf{b}_1, \frac{1}{2}(\mathbf{b}_1 + \mathbf{b}_2) \right\rangle$.

5. Decompositions for GLV endomorphisms

Let $\widetilde{\mathcal{E}}$ be an elliptic curve over $\overline{\mathbb{Q}}$ with complex multiplication by $\mathbb{Z}[\sqrt{\Delta}]$; that is, with an explicit endomorphism $\widetilde{\phi}$ such that $\mathbb{Z}[\widetilde{\phi}] \cong \mathbb{Z}[\sqrt{\Delta}]$. Let $\mathcal{E}/\mathbb{F}_q$ be the (good) reduction modulo p of $\mathcal{E}$, (and suppose that $\mathcal{E}$ is not supersingular); by definition, $\mathcal{E}$ comes equipped with an explicit separable endomorphism ϕ such that $\mathbb{Z}[\phi] \cong \mathbb{Z}[\sqrt{\Delta}]$. If Δ and $\widetilde{\mathcal{E}}$ were was chosen in such a way that ϕ has very low degree, then ϕ can be efficiently computable, and hence useful for scalar decompositions.

Suppose, therefore, that ϕ has very low degree for efficiency reasons. Then $n_\phi = \deg(\phi)$ must be very small; and since $\Delta(\phi)$ must be negative, t_ϕ^2 (and hence $|\Delta(\phi)|$) must also be very small. In particular, $|t_\phi| < 2\sqrt{\deg(\phi)}$ and $|\Delta(\phi)| < 4\deg(\phi)$.

In practice, $\mathbb{Z}[\phi]$ is either the maximal order in $\mathbb{Q}(\pi)$, or (exceptionally) an order of index two in the maximal order. It is therefore reasonable to

$$\text{assume } \mathbb{Z}[\pi] \text{ is contained in } \mathbb{Z}[\phi],$$

so

$$\pi = c\phi + b \qquad \text{with} \qquad b = \tfrac{1}{2}\left(t_\pi - ct_\phi\right) \qquad \text{and} \qquad c^2\Delta(\phi) = t_\pi^2 - 4q \ .$$

This allows us to write down a basis for (a sublattice of) the GLV lattice using Theorem 2.

It is important to note that in practice, b and c are already known from the determination of the curve order, precisely because $\pi = c\phi + b$. Indeed, if we want to compute the order of an elliptic curve known to have complex multiplication by a CM order (such as $\mathbb{Z}[\phi]$, in this case), then we would typically use the algorithm described in [**25**, §4], which computes the trace t_π of Frobenius *by computing b and c.* This approach uses Cornacchia's algorithm to compute a generator of a principal ideal in $\mathbb{Z}[\phi]$ of norm q, before taking its trace to compute $\#\mathcal{E}(\mathbb{F}_q)$; but this generator is none other than $\pi = c\phi + b$.

Alternatively, $\mathcal{E}$ could be constructed using the CM method starting from the small discriminant $\Delta(\phi)$. In this case, b and c are explicitly constructed so that $c\phi + b$ will have norm q.

In any case, if we had somehow mislaid the values of b and c, then we could recover them by factoring the ideal (q) in $\mathbb{Z}[\phi]$ using (for example) Cornacchia's algorithm, which amounts to repeating the point counting algorithm described above. The element $c\phi + b$ will be (up to sign) one of the two resulting generators of the factors of (q). Alternatively, we could use $c \equiv (2 - t_\pi)/(2\lambda_\phi - t_\phi) \pmod{N}$; though inverting $2\lambda_\phi - t_\phi$ modulo N is roughly equivalent to the use of the Euclidean algorithm in the original GLV method.

One important feature of the GLV setting is that t_ϕ, n_ϕ, and $\Delta(\phi)$ are independent of q and t_π, so the bitlength of the basis produced by Theorem 2 exceeds $\frac{1}{2}\log_2 q$ by no more than an explicit constant. The following examples consider the new basis for the GLV curves with endomorphisms of degree at most 3 (treated in detail elsewhere by Gallant, Lambert, and Vanstone [**10**] and Longa and Sica [**19**]).

Example 1 (j-invariant 1728: cf. [**10**, Ex. 3] and [**19**, Ex. 1]). If $q \equiv 3 \pmod 4$, then for every $a \neq 0$ in $\mathbb{F}_q$ the curve $\mathcal{E}_{1728} : y^2 = x^3 + ax$ has an $\mathbb{F}_q$-endomorphism $\phi : (x, y) \mapsto (-x, -iy)$ (where $i^2 = -1$), with $P_\phi(T) = T^2+1$; so $\mathbb{Z}[\phi] \cong \mathbb{Z}[\sqrt{-1}]$. Theorem 2 constructs the basis

$$\mathbf{b}_1 = \left(\tfrac{1}{2}t_\pi - 1, c\right) \qquad \text{and} \qquad \mathbf{b}_2 = \left(c, 1 - \tfrac{1}{2}t_\pi\right) \ ,$$

where $c^2 = q - (t_\pi/2)^2$. This basis is not only short (clearly $\|\mathbf{b}_1\|_\infty = \|\mathbf{b}_2\|_\infty \leq \frac{1}{2}\log_2 q$) and reduced, it is also orthogonal.

Example 2 (j-invariant 0: cf.[**10**, Ex. 4] and [**19**, Ex. 2]). If $q \equiv 2 \pmod 3$, then for any $a \neq 0$ in $\mathbb{F}_q$, the curve $\mathcal{E}_{1728} : y^2 = x^3 + a$ has an $\mathbb{F}_q$-endomorphism $\phi : (x, y) \mapsto (\zeta_3 x, y)$ (where ζ_3 is a primitive third root of unity), with $P_\phi(T) = T^2 + T + 1$: that is, $\mathcal{E}_0$ has explicit CM by $\mathbb{Z}[(1 + \sqrt{-3})/2]$. Looking at the basis produced by Theorem 2, we find

$$\mathbf{b}_1 = \left(\tfrac{1}{2}(t_\pi - c) - 1, c\right) \quad \text{and} \quad \mathbf{b}_2 = \left(\tfrac{1}{2}(t_\pi + c) - 1, 1 - \tfrac{1}{2}(t_\pi - c)\right) \ ,$$

where $c^2 = \frac{1}{3}\left(4q - t_\pi^2\right)$. We note that in this case, two applications of the triangle inequality yields $\log_2 \|\mathbf{b}_i\|_\infty < \frac{1}{2}\log_2 q + 1$.

Example 3 (j-invariant -3375: cf. [**10**, Ex. 5] and [**19**, Ex. 3]). Suppose -7 is a square in $\mathbb{F}_q$. The curve $\mathcal{E}_{-3375} : y^2 = x^3 - \frac{3}{4}x^2 - 2x - 1$ over $\mathbb{F}_q$ has a degree-2 endomorphism ϕ with $P_\phi(T) = T^2 - T + 2$ (and $\ker\phi = \langle(2, 0)\rangle$); that is, $\mathcal{E}_{-3375}$ has explicit CM by $\mathbb{Z}[(-1 + \sqrt{-7})/2]$. Theorem 2 yields vectors

$$\mathbf{b}_1 = (b - 1, c) \qquad \text{and} \qquad \mathbf{b}_2 = (2c - (b - 1), (1 - b)) \ ;$$

as before, $\log_2 \|\mathbf{b}_i\|_\infty < \frac{1}{2}\log_2 q + 1$.

Example 4 (j-invariant 8000: cf. [**10**, Ex. 6] and [**19**, Ex. 4]). Suppose -2 is a square in $\mathbb{F}_q$. The curve $\mathcal{E}_{8000} : y^2 = 4x^3 - 30x - 28$ over $\mathbb{F}_q$ has a degree-2 endomorphism ϕ with $P_\phi(T) = T^2 + 2$ (and $\ker\phi = \langle(-2, 0)\rangle$): that is, $\mathcal{E}_{8000}$ has explicit CM by $\mathbb{Z}[\sqrt{-2}]$. Theorem 2 yields vectors

$$\mathbf{b}_1 = (b - 1, c) \qquad \text{and} \qquad \mathbf{b}_2 = (2c, 1 - b)$$

with $\log_2 \|\mathbf{b}_i\| \leq \frac{1}{2}\log_2 q + 1$.

Example 5 (j-invariant 32768: cf. [**19**, Ex. 5]). Suppose -11 is a square in $\mathbb{F}_q$. The curve $\mathcal{E}_{32768} : y^2 = x^3 - \frac{13824}{539}x + \frac{27648}{539}$ over $\mathbb{F}_q$ has a degree 3 endomorphism ϕ with $P_\phi(T) = T^2 - T + 3$: that is, $\mathcal{E}_{32768}$ has explicit CM by $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-11})]$. The kernel of ϕ is cut out by $(x - \frac{24}{7}(1 - 1/\sqrt{-11}))$. Theorem 2 constructs a pair of vectors

$$\mathbf{b}_1 = (b-1, c) \qquad \text{and} \qquad \mathbf{b}_2 = (3c - (b-1), 1-b)$$

with $\log_2 \|\mathbf{b}_i\|_\infty < \frac{1}{2}\log_2 q + 2$.

Example 6 (j-invariant 54000: cf. [**19**, Example 6]). Suppose -3 is a square in $\mathbb{F}_q$. The curve $\mathcal{E}_{54000} : y^2 = x^3 - \frac{3375}{121}x + \frac{6750}{121}$ over $\mathbb{F}_q$ has an $\mathbb{F}_q$-endomorphism ϕ of degree 3 with minimal polynomial $P_\phi(T) = T^2 + 3$ (and kernel cut out by $(x - 45/11)$): that is, $\mathcal{E}_{54000}$ has explicit CM by $\mathbb{Z}[\sqrt{-3}]$. Theorem 2 yields vectors

$$\mathbf{b}_1 = (b-1, c) \qquad \text{and} \qquad \mathbf{b}_2 = (3c, 1-b)$$

with $\log_2 \|\mathbf{b}_i\|_\infty < \frac{1}{2}\log_2 q + 1$.

6. Decompositions for the GLS endomorphism

Let $\mathcal{E}_0$ be an ordinary elliptic curve over $\mathbb{F}_p$, and let $\mathcal{E} := \mathcal{E}_0 \times \mathbb{F}_{p^2}$ be the base extension of $\mathcal{E}_0$ to $\mathbb{F}_{p^2}$. The Frobenius endomorphism π_0 of $\mathcal{E}_0$ has characteristic polynomial $P_\pi(T) = T^2 - t_0 T + p$ with $|t_0| < 2\sqrt{p}$, while the (p^2-power) Frobenius endomorphism π of $\mathcal{E}$ satisfies $\pi = \pi_0^2$, so $P_\pi(T) = T^2 - (t_0^2 - 2p)T + p^2$. In particular,

$$\#\mathcal{E}(\mathbb{F}_{p^2}) = P_\pi(1) = (p+1)^2 - t_0^2 = \#\mathcal{E}_0(\mathbb{F}_p) \cdot (p + 1 + t_0),$$

so $\#\mathcal{E}(\mathbb{F}_{p^2})$ cannot have prime divisors larger than $O(p)$.

Now let $\mathcal{E}'$ be the quadratic twist of $\mathcal{E}$, with $\tau : \mathcal{E} \to \mathcal{E}'$ the twisting isomorphism. The Frobenius π' on $\mathcal{E}'$ satisfies $\pi' = \tau\pi\tau^{-1}$, so

$$P_{\pi'}(T) = T^2 - (2p - t_0^2)T + p^2 \qquad \text{and} \qquad \Delta_{\pi'} = t_0^2(t_0^2 - 4p) \ .$$

Note that $\#\mathcal{E}'(\mathbb{F}_q) = P_{\pi'}(1) = (p-1)^2 + t_0^2$; unlike $\#\mathcal{E}(\mathbb{F}_q)$, this can take prime (and near-prime) values, so $\mathcal{E}'$ may be useful for discrete-logarithm-based cryptosystems.

The GLS endomorphism on $\mathcal{E}'$ is $\psi := \tau\pi_0\tau^{-1}$. It is defined over $\mathbb{F}_{p^2}$; its minimal polynomial is

$$P_\psi(T) = P_{\pi_0}(T) = T^2 - t_0 T + p \ , \qquad \text{and} \qquad \Delta_\psi = t_0^2 - 4p \ .$$

If $\mathcal{G}$ is a cyclic subgroup of $\mathcal{E}'(\mathbb{F}_{p^2})$ of order N such that $\psi(\mathcal{G}) \subseteq \mathcal{G}$, then the eigenvalue λ_ψ of ψ on $\mathcal{G}$ is a square root of -1 modulo N.

We have $\psi^2 = \tau\pi_0^2\tau^{-1} = \tau\pi\tau^{-1} = -\pi'$, so $\mathbb{Z}[\psi]$ contains $\mathbb{Z}[\pi']$. We can therefore apply Theorem 2 to the inclusion $\mathbb{Z}[\pi'] \subseteq \mathbb{Z}[\psi]$ in order to compute a short basis for (a sublattice of) $\mathcal{L} = \langle (N, 0), (-\lambda_\psi, 1) \rangle$.

Looking at the discriminants, we see that $\mathbb{Z}[\pi']$ has conductor $|t_0|$ in $\mathbb{Z}[\psi]$. Indeed,

$$\pi' = -t_0\psi + p \ ;$$

so Theorem 2 yields a basis

$$\mathbf{b}_1 = (p-1, -t_0) \qquad \text{and} \qquad \mathbf{b}_2 = (-t_0, 1-p) \ .$$

This is precisely (up to sign) the basis of [**9**, Lemma 3]; it is not only short (the largest coefficient is $p-1$, so $\log_2 \|\mathbf{b}_i\|_\infty < \log_2 p$), it is also orthogonal. If $\mathcal{E}'(\mathbb{F}_{p^2})$ does not have prime order, then we can easily shrink the basis to fit $\mathcal{G}$ by following the procedure described in §4.

Remark 3. From a purely formal point of view, we could have treated this identically to the GLV case, with ψ in place of ϕ, but there are a number of important differences. First of all, the ring $\mathbb{Z}[\psi]$ has a much larger discriminant than any GLV order: in general $\mathbb{Z}[\psi]$ is far from being the maximal order of the endomorphism algebra. Second, the parameters t_ψ, n_ψ, and $\Delta(\psi)$ vary with p and t, so we cannot treat the excess bitlength in the Ciet–Sica–Quisquater bounds (Ineq. (5)) as a constant. Indeed, if we simply plug the values

$$\begin{aligned} q &= p^2 \ , & t_\pi &= 2p - t_0^2 \ , & \Delta(\pi) &= t_0^2(t_0^2 - 4p) \ , \\ n_\psi &= p \ , & t_\psi &= t_0 \ , & \Delta(\psi) &= t_0^2 - 4p \end{aligned}$$

into Inequalities (4) or (5), or even the “optimal” bound of [**6**, Theorem 4], then we obtain a rather pessimistic bitlength bound of around $\frac{3}{4}\log_2 q$, which exceeds the true length of the basis by $\frac{1}{4}\log_2 q$ bits.

7. Decompositions for reductions of $\mathbb{Q}$-curves

GLS curves may be seen as a special case of a more general construction involving reductions of quadratic $\mathbb{Q}$-curves. We give a very brief description of this construction here (see [**26**] for more details, and families of examples). In [**26**, Proposition 2], a basis is constructed in a seemingly ad-hoc way that yields half-length scalar decompositions; we will see below that this basis also results from Theorem 2.

Let K be a quadratic field, σ the nontrivial automorphism of K fixing $\mathbb{Q}$. Let $\widetilde{\mathcal{E}} : y^2 = x^3 + ax + b$ and ${}^\sigma\widetilde{\mathcal{E}} : y^2 = x^3 + \sigma(a)x + \sigma(b)$ be a pair of Galois-conjugate curves over K such that there exists an isogeny $\widetilde{\phi} : \mathcal{E} \to {}^{(p)}\mathcal{E}$ of small degree d defined over $K(\sqrt{-d})$. If p is an inert prime in K that is a prime of good reduction for $\widetilde{\mathcal{E}}$ (and not dividing d), then we can reduce $\widetilde{\phi} : \widetilde{\mathcal{E}} \to {}^\sigma\widetilde{\mathcal{E}}$ modulo p to obtain a d-isogeny $\phi : \mathcal{E} \to {}^{(p)}\mathcal{E}$ of curves over $\mathbb{F}_{p^2}$. Here ${}^{(p)}\mathcal{E}$, the reduction of ${}^\sigma\mathcal{E}$ modulo p, is the curve formed from $\mathcal{E}$ by applying p-th powering to its coefficients; so there also exists a p-th power Frobenius isogeny $\pi_0 : {}^{(p)}\mathcal{E} \to \mathcal{E}$. Composing ϕ with π_0, we obtain an inseparable endomorphism $\psi := \pi_0\phi$ of $\mathcal{E}$, of degree dp. If d is very small, then ψ can be efficiently computable, since p-th powering in $\mathbb{F}_{p^2}$ is essentially free. (The GLS construction is equivalent to the special case where ϕ is an isomorphism—that is, $d = 1$.)

Let $\epsilon_p := -\left(\frac{-d}{p}\right)$; that is, $\epsilon_p = 1$ if $-d$ is a nonsquare modulo p, and -1 if it is a square. Then according to [**26**, Proposition 1], the minimal polynomial of ψ is

$$P_\psi(T) = T^2 - \epsilon_p r d T + dp \ ,$$

and

$$dr^2 = 2p + \epsilon_p t_\pi \ .$$

(This determines r up to sign; exchanging r with $-r$ corresponds to exchanging ϕ with $-\phi$.) Squaring the endomorphism, we obtain $\psi^2 = \pi_0\phi\pi_0\phi = \epsilon_p\pi_0\phi\phi^\dagger\pi_0 = \epsilon_p[d]\pi$, where π is the usual p^2-power Frobenius on $\mathcal{E}$. In particular, $\mathbb{Z}[\pi]$ is contained in $\mathbb{Z}[\psi]$; we find that

$$\pi = r\psi - \epsilon_p p \ .$$

If $\mathcal{G} \subseteq \mathcal{E}(\mathbb{F}_q)$ is a cyclic subgroup of order N such that $\psi(\mathcal{G}) = \mathcal{G}$, then the eigenvalue of ψ on $\mathcal{G}$ is a square root of $\epsilon_p d$ modulo N.

Applying Theorem 2 to the orders $\mathbb{Z}[\pi] \subseteq \mathbb{Z}[\psi]$, we obtain the basis

$$\mathbf{b}_1 = (-(1+\epsilon_p p), r) \qquad \text{and} \qquad \mathbf{b}_2 = (-\epsilon_p r d, 1+\epsilon_p p) \ .$$

Up to sign, this is the basis appearing in the proof of [**26**, Proposition 2], where it is used to produce scalar decompositions having bitlength at most $\lceil \log_2 p \rceil$. While this basis generates a sublattice of determinant $\#\mathcal{E}(\mathbb{F}_{p^2})$, if $N \neq \#\mathcal{E}(\mathbb{F}_{p^2})$ then the basis may be easily shrunk to fit $\mathcal{G}$ following the procedure outlined in §4.

8. Four-dimensional decompositions for GLV+GLS

Recently, Longa and Sica [**19**] followed by Guillevic and Ionica [**12**] have proposed using a pair of efficiently computable endomorphisms ϕ and ψ to construct four-dimensional scalar decompositions on elliptic curves, corresponding to the situation of §1 with $(\phi_1, \phi_2, \phi_3, \phi_4) = (1, \phi, \psi, \phi\psi)$. (The Longa–Sica technique supersedes the earlier 3-dimensional construction of Zhou, Hu, Xu, and Song [**32**] with $(\phi_1, \phi_2, \phi_3) = (1, \phi, \psi)$, which we will not cover here.) Longa and Sica propose an elaborate iterated Cornacchia algorithm to derive their lattice basis. In this section, we show that no lattice algorithms are necessary: we can generate four short lattice vectors using Lemma 1.

Recall the Longa–Sica construction: Let $\mathcal{E}_0/\mathbb{F}_p$ be a GLV curve, with an efficiently computable endomorphism ϕ_0, and Frobenius π_0. Applying the GLS construction (exactly as in §6) to $\mathcal{E}_0$, we obtain a twisted elliptic curve $\mathcal{E}'$ over $\mathbb{F}_{p^2}$ with an efficiently computable endomorphism ψ corresponding to the twist of π_0: if $\tau : \mathcal{E}_0 \otimes \mathbb{F}_{p^2} \to \mathcal{E}'$ is the twisting isomorphism, then $\psi = \tau\pi_0\tau^{-1}$. The endomorphisms ψ and π' satisfy

$$P_\psi(T) = P_{\pi_0}(T) = T^2 - t_{\pi_0}T + p \quad \text{and} \quad P_{\pi'}(T) = T^2 - (2p - t_{\pi_0}^2)T + p^2,$$

respectively. Clearly, $\mathbb{Z}[\psi]$ contains $\mathbb{Z}[\pi']$: the discriminants of the orders $\mathbb{Z}[\pi']$ and $\mathbb{Z}[\psi]$ are

$$\Delta(\psi) = t_{\pi_0}^2 - 4p \qquad \text{and} \qquad \Delta(\pi') = t_{\pi_0}^2(t_{\pi_0}^2 - 4p) = t_{\pi_0}^2\Delta(\psi) \ ,$$

so the relative conductor of $\mathbb{Z}[\pi']$ in $\mathbb{Z}[\psi]$ is $|t_{\pi_0}| < 2\sqrt{p}$. As in vanilla GLS, we can write

$$\pi' = -t_{\pi_0}\psi + p \ .$$

The GLV endomorphism ϕ_0 on $\mathcal{E}_0$ induces a second efficient endomorphism $\phi := \tau\phi_0\tau^{-1}$ on $\mathcal{E}'$. We have $P_\phi = P_{\phi_0}$, so $\mathbb{Z}[\phi] \cong \mathbb{Z}[\phi_0]$. Since ϕ_0 is a GLV endomorphism, $\mathbb{Z}[\phi]$ is either the maximal order of the endomorphism algebra of $\mathcal{E}'$, or very close to it—so it makes sense to assume that $\mathbb{Z}[\phi]$ contains $\mathbb{Z}[\psi]$ (cf. Remark 5 below), so that we can write ψ as

$$\psi = c\phi + b \ ,$$

where

$$b = \frac{1}{2}(t_{\pi_0} - ct_\phi) \qquad \text{and} \qquad c^2 = \frac{\Delta_\psi}{\Delta_\phi} = \frac{t_{\pi_0}^2 - 4p}{t_\phi^2 - 4n_\phi} \ . \tag{6}$$

Observe that b and c are both in $O(\sqrt{p})$. As with conventional GLV curves, c and b are both already known as byproducts of the curve construction (via the CM method) or its order computation: if $\pi_0 = c_0\phi_0 + b_0$, then

$$c = \frac{c_0}{t_0} \quad \text{and} \quad b = \frac{1}{t_0}(b_0 - p) \ .$$

Theorem 4. *With ϕ and ψ defined as above, suppose we are in the situation of §1 with $(\phi_1, \phi_2, \phi_3, \phi_4) = (1, \phi, \psi, \phi\psi)$. The vectors*

$$\mathbf{b}_1 = (1, 0, b, c) \ , \qquad \mathbf{b}_2 = (0, 1, -cn_\phi, ct_\phi + b) \ ,$$
$$\mathbf{b}_3 = (-b, -c, 1, 0) \ , \qquad \mathbf{b}_4 = (cn_\phi, -ct_\phi - b, 0, 1)$$

generate a sublattice of determinant $\#\mathcal{E}(\mathbb{F}_q)$ in $\mathcal{L}$. If $\mathcal{G} = \mathcal{E}(\mathbb{F}_q)$, then $\mathcal{L} = \langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4 \rangle$.

Proof. Let λ_ϕ and λ_ψ be the eigenvalues of ϕ and ψ on $\mathcal{G}$, respectively. Applying Lemma 1 to the inclusion $\mathbb{Z}[\psi] \subset \mathbb{Z}[\phi]$, we obtain relations

$$\lambda_\psi - c\lambda_\phi - b \equiv 0 \pmod{N} \qquad \text{and}$$
$$\lambda_\psi\lambda_\phi - t_\phi\lambda_\psi - b\lambda_\phi + cn_\phi + bt_\phi \equiv 0 \pmod{N} \ ,$$

corresponding to the vectors $\mathbf{b}_3$ and $(cn_\phi + bt_\phi, -c, -t_\phi, 1) = \mathbf{b}_4 - t_\phi\mathbf{b}_3$. Multiplying the relations above through by $-\lambda_\psi$ and using $\lambda_\psi^2 = \lambda_{\psi^2} = -1 \pmod{N}$, we obtain new relations

$$1 + c\lambda_\phi\lambda_\psi + b\lambda_\psi \equiv 0 \pmod{N} \qquad \text{and}$$
$$\lambda_\phi - t_\phi + b\lambda_\phi\lambda_\psi - (cn_\phi + bt_\phi)\lambda_\psi \equiv 0 \pmod{N} \ ,$$

corresponding to the vectors $(1, 0, b, c) = \mathbf{b}_1$ and $(-t_\phi, 1, -cn_\phi - bt_\phi, -b) = \mathbf{b}_4 - t_\phi\mathbf{b}_3$, respectively. □

The vectors produced by Theorem 4 are short: ϕ is a GLV endomorphism, so both n_ϕ and t_ϕ are in $O(1)$. Hence, in view of Eq. (6), $\|\mathbf{b}_i\|_\infty$ is in $O(\sqrt{p})$ for $1 \leq i \leq 4$.

Remark 5. The assumption that $\mathbb{Z}[\psi]$ is contained in $\mathbb{Z}[\phi]$ is incompatible with the hypothesis of [**19**] (which supposes that $\mathbb{Q}(\phi) \cap \mathbb{Q}(\psi) = \mathbb{Q}$); but even without this assumption, $\mathbb{Q}(\phi) = \mathbb{Q}(\psi) = \mathbb{Q}(\pi')$ when $\mathcal{E}$ is ordinary, so the hypothesis of [**19**] is *never* satisfied for ordinary curves.

9. Decompositions for the Guillevic–Ionica construction

The Guillevic–Ionica construction [**12**] uses a modified CM method to search for elliptic curves $\mathcal{E}/\mathbb{F}_{p^2}$ such that $\mathcal{E}$ has endomorphisms ϕ and ψ such that ϕ is separable of very small degree d_1, and ψ is the composition of an inseparable p-isogeny and a separable isogeny of very small degree d_2. (In a sense, these curves are to Longa–Sica curves what reductions of $\mathbb{Q}$-curves are to GLS curves.) Once such $\mathcal{E}$ and p have been found (given d_1 and d_2), the ϕ and ψ are easily recovered using Vélu's formulæ [**31**]. If this construction is used, then (as with the standard CM method) the expression of π as an element of $\mathbb{Z}[\phi]$ is known:

$$\pi = c\phi + b \ .$$

Theorem 6. *With ϕ and ψ defined as above: Suppose we are in the situation of §1 with $(\phi_1, \phi_2, \phi_3, \phi_4) = (1, \phi, \psi, \phi\psi)$, and $\psi^2 = [\pm d]\pi$. The vectors*

$$\mathbf{b}_1 = (\pm d, 0, -b, -c) \ , \qquad \mathbf{b}_2 = (0, \pm d, cn_\phi, -ct_\phi - b) \ ,$$
$$\mathbf{b}_3 = (-b, -c, 1, 0) \ , \qquad \mathbf{b}_4 = (cn_\phi, -ct_\phi - b, 0, 1)$$

generate a sublattice of determinant $\#\mathcal{E}(\mathbb{F}_{p^2})$ in $\mathcal{L}$. If $\mathcal{G} = \mathcal{E}(\mathbb{F}_{p^2})$, then $\mathcal{L} = \langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4 \rangle$.

Proof. The proof is the same as for Theorem 4, but with $\lambda_\psi^2 = \pm d$. □

10. Two-dimensional decompositions in genus 2

Suppose $\mathcal{A}/\mathbb{F}_q$ is an ordinary principally polarized abelian surface (in our applications, $\mathcal{A}$ is either the Jacobian of a genus 2 curve, or the Weil restriction of an elliptic curve). The Frobenius endomorphism π of $\mathcal{A}$ generates a quartic CM field $\mathbb{Q}(\pi)$, and the Rosati involution of $\mathrm{End}(\mathcal{A})$ (exchanging an endomorphism with its Rosati dual) acts as complex conjugation on $\mathbb{Q}(\pi)$. Hence, the quadratic real subfield of $\mathbb{Q}(\pi)$ is $\mathbb{Q}(\pi + \pi^\dagger)$, and $\mathbb{Z}[\pi + \pi^\dagger]$ is a real quadratic order. We may identify $\pi^\dagger$ with q/π; the eigenvalue of $\pi + \pi^\dagger$ on subgroups of $\mathcal{A}(\mathbb{F}_q)$ is $1 + q$ (because π has eigenvalue 1).

The characteristic polynomial of Frobenius is

$$P_\pi(T) = T^4 - t_{(\pi+\pi^\dagger)}T^3 + (2q + n_{(\pi+\pi^\dagger)})T^2 - t_{(\pi+\pi^\dagger)}T + q^2 \ ,$$

so

$$\#\mathcal{A}(\mathbb{F}_q) = P_\pi(1) = P_{\pi+\pi^\dagger}(q+1) = (q+1)^2 - t_{(\pi+\pi^\dagger)}(q+1) + n_{(\pi+\pi^\dagger)} \ . \tag{7}$$

The Weil bounds yield

$$|t_{(\pi+\pi^\dagger)}| \leq 4\sqrt{q} \quad \text{and} \quad |n_{(\pi+\pi^\dagger)}| \leq 4q \ ,$$

while Rück [**24**] shows that

$$t_{(\pi+\pi^\dagger)}^2 - 4n_{(\pi+\pi^\dagger)} > 0 \quad \text{and} \quad n_{(\pi+\pi^\dagger)} + 4q > 2|t_{(\pi+\pi^\dagger)}|\sqrt{q} \ .$$

Theorem 7. *Suppose ϕ is a non-integer real multiplication endomorphism of an ordinary abelian surface $\mathcal{A}$ (ie, $\phi^\dagger = \phi$) such that $\mathbb{Z}[\pi + \pi^\dagger] \subseteq \mathbb{Z}[\phi]$, and assume that we are in the situation of §1 with $(\phi_1, \phi_2) = (1, \phi)$. If $\pi + \pi^\dagger = c\phi + b$, then the vectors*

$$\mathbf{b}_1 = (q + 1 - b, -c) \qquad \textit{and} \qquad \mathbf{b}_2 = (cn_\phi - (q + 1 - b)t_\phi, q + 1 - b)$$

generate a sublattice of determinant $\#\mathcal{A}(\mathbb{F}_q)$ in $\mathcal{L}$. If $\mathcal{G} = \mathcal{A}(\mathbb{F}_q)$, then $\mathcal{L} = \langle \mathbf{b}_1, \mathbf{b}_2 \rangle$.

Proof. The proof is almost exactly the same as that of Theorem 2. As we noted above, $(\pi + \pi^\dagger)$ has eigenvalue $q + 1$ on $\mathcal{G}$. Applying Lemma 1 to $\mathbb{Z}[\pi + \pi^\dagger] \subset \mathbb{Z}[\phi]$, we obtain relations

$$\begin{aligned} (q + 1 - b) \cdot 1 - c \cdot \lambda_\phi &\equiv 0 \pmod{N} \qquad \text{and} \\ (cn_\phi - (q + 1 - b)t_\phi) \cdot 1 + (q + 1 - b) \cdot \lambda_\phi &\equiv 0 \pmod{N} \ . \end{aligned}$$

The first implies that $\mathbf{b}_1$ is in $\mathcal{L}$, the second that $\mathbf{b}_2$ is in $\mathcal{L}$. The determinant of $\langle \mathbf{b}_1, \mathbf{b}_2 \rangle$ is

$$(q + 1 - b)^2 + c^2 n_\phi - (q + 1 - b)ct_\phi = \#\mathcal{A}(\mathbb{F}_q) \ ,$$

using Eq. (7), $t_{(\pi+\pi^\dagger)} = ct_\phi + 2b$, and $t_\phi^2 - 4n_\phi = c^2(t_{(\pi+\pi^\dagger)}^2 - 4n_{(\pi+\pi^\dagger)})$. □

We apply Theorem 7 to the explicit real multiplication families treated in [**28, 17, 11**]. In each case, the assumption $\mathbb{Z}[\pi + \pi^\dagger] \subseteq \mathbb{Z}[\phi]$ is fulfilled because $\mathbb{Z}[\phi]$ is the maximal order of the real subfield of the endomorphism algebra.

Example 7 (Explicit RM by $\mathbb{Q}(\sqrt{5})$). Brumer [4], Hashimoto [**13**], Mestre [**20**], and Tautz, Top, and Verberkmoes [**29**] have given explicit constructions of families of genus 2 curves whose Jacobians have explicit real multiplication by $\mathbb{Z}[(1 + \sqrt{5})/2]$, which is the maximal order of $\mathbb{Q}(\sqrt{5})$ (see Wilson's thesis [**30**] for a full characterization of all such curves). In each case, the curve is equipped with a correspondence inducing an explicit endomorphism ϕ on the Jacobian satisfying $P_\phi(T) = T^2 + T - 1$; these endomorphisms have been exploited for fast scalar multiplication in [**17**] and [**28**].

Let $\mathcal{C}/\mathbb{F}_q$ be the reduction mod p of a curve taken from one of these families; then $\mathcal{J}_\mathcal{C}$ inherits the explicit endomorphism ϕ, and $\mathbb{Z}[\phi] \cong \mathbb{Z}[(1 + \sqrt{5})/2]$. Since $\mathbb{Z}[(1 + \sqrt{5})/2]$ is the maximal order of $\mathbb{Q}(\sqrt{5})$, we must have $\mathbb{Z}[\pi + \pi^\dagger] \subseteq \mathbb{Z}[\phi]$; so

$$\pi + \pi^\dagger = c\phi + b$$

where $b = \frac{1}{2}(t_{(\pi+\pi^\dagger)} + c)$ and $5c^2 = \Delta(\pi + \pi^\dagger)$.

Putting ourselves in the situation of §1 with $(\phi_1, \phi_2) = (1, \phi)$, Theorem 7 yields vectors

$$\mathbf{b}_1 = (q + 1 - b, -c) \qquad \text{and} \qquad \mathbf{b}_2 = (-c - (q + 1 - b), q + 1 - b)$$

in $\mathcal{L}$. Note that $|c| < 4\sqrt{q/5}$, so $|b| < (2 + 2/\sqrt{5})\sqrt{q}$, and

$$\sigma(\mathbf{b}_1) = \sigma(\mathbf{b}_2) = \log_2(q + 1).$$

Example 8. Mestre [**21**] has constructed a two-parameter family of genus 2 curves whose Jacobians have explicit real multiplication by $\mathbb{Z}[\sqrt{2}]$ (an alternative presentation of these curves for cryptographic applications is developed in [**11**]; see Bending's thesis [**2**] for a full characterization of curves with RM by $\mathbb{Z}[\sqrt{2}]$). The efficient endomorphism ϕ satisfies $P_\phi(T) = T^2 - 2$ in this case, so $\Delta(\phi) = 8$.

Let $\mathcal{C}/\mathbb{F}_q$ be the reduction mod p of a curve taken from one of these families; $\mathcal{J}_\mathcal{C}$ inherits the explicit endomorphism ϕ, and $\mathbb{Z}[\phi] \cong \mathbb{Z}[\sqrt{2}]$. Since $\mathbb{Z}[\sqrt{2}]$ is the maximal order of $\mathbb{Q}(\sqrt{2})$, we must have $\mathbb{Z}[\pi + \pi^\dagger] \subseteq \mathbb{Z}[\phi]$; so

$$\pi + \pi^\dagger = c\phi + b$$

where $b = \frac{1}{2}(t_{(\pi+\pi^\dagger)} + c)$ and $2c^2 = \Delta(\pi + \pi^\dagger)$.

Putting ourselves in the situation of §1 with $(\phi_1, \phi_2) = (1, \phi)$, Theorem 7 yields vectors

$$\mathbf{b}_1 = (q + 1 - b, -c) \qquad \text{and} \qquad \mathbf{b}_2 = (-2c, q + 1 - b)$$

in $\mathcal{L}$. For this family, $|c| < 2\sqrt{q/2}$ and $|b| < (2 + 1/2\sqrt{2})\sqrt{q}$; each is much smaller than $q + 1$, so as before we have

$$\sigma(\mathbf{b}_1) = \sigma(\mathbf{b}_2) = \log_2(q + 1).$$

References

[1] L. Babai, "On Lovasz' lattice reduction and the nearest lattice point problem". Combinatorica **6** (1986) 1–13

[2] P. R. Bending, "Curves of genus 2 with $\sqrt{2}$ multiplication". Ph. D. Thesis, University of Oxford (1998)

[3] J. W. Bos, C. Costello, H. Hisil, and K. Lauter, "High-Performance Scalar Multiplication using 8-Dimensional GLV/GLS Decomposition". In G. Bertoni and J.-S. Coron, Cryptographic Hardware and Embedded Systems - CHES 2013. Lecture Notes in Comput. Sci. **8086** (2013) 331–348

[4] A. Brumer, "The rank of $J_0(N)$". Asterisque **228** (1995) 41–68

[5] D. Cadé, X. Pujol, and D. Stehlé, fpLLL. `http://perso.ens-lyon.fr/damien.stehle/fplll/`

[6] M. Ciet, F. Sica, and J.-J. Quisquater, "Analysis of the Gallant–Lambert–Vanstone method based on efficient endomorphisms: Elliptic and hyperelliptic curves". In K. Nyberg and H. M. Heys (eds), Selected Areas in Cryptography: SAC 2002 Lecture Notes in Comput. Sci. **2595** (2003) 21–36

[7] H. Cohen and G. Frey (eds.) Handbook of elliptic and hyperelliptic curve cryptography. Chapman & Hall / CRC (2006)

[8] S. D. Galbraith, Mathematics of public key cryptography. Cambridge University Press (2012)

[9] S. D. Galbraith, X. Lin, and M. Scott, "Endomorphisms for faster elliptic curve cryptography on a large class of curves". J. Crypt. **24** #3 (2011) 446–469

[10] R. P. Gallant, R. J. Lambert, and S. A. Vanstone, "Faster point multiplication on elliptic curves with efficient endomorphisms". In J. Kilian (ed.), Advances in Cryptology: CRYPTO 2001, Lecture Notes in Comput. Sci. **2139** (2001) 190–200

[11] P. Gaudry, D. R. Kohel, and B. Smith, "Counting Points on Genus 2 Curves with Real Multiplication". In D. Lee and X. Wang (eds), Advances in Cryptology: ASIACRYPT 2011, Lecture Notes in Comput. Sci. **7073** (2011) 504-519

[12] A. Guillevic and S. Ionica, "Four dimensional GLV via the Weil restriction". To appear in ASIACRYPT 2013. `http://eprint.iacr.org/2013/311`

[13] K. Hashimoto, "On Brumer's family of RM-curves of genus two". Tohoku Math. J. (2) **52** #4 (2000) 475–488

[14] H. Hisil, K. Wong, G. Carter, and E. Dawson, "Twisted Edwards curves revisited". In: J. Pieprzyk (ed.), Advances in Cryptology: ASIACRYPT 2008. Lecture Notes in Comput. Sci. **5350** (2008) 326–343

[15] M. Kaib, "The Gauss lattice basis reduction algorithm succeeds with any norm". In L. Budach (ed.), Fundamentals of Computation Theory. Lecture Notes in Comput. Sci. **529** (1991) 275–286

[16] D. R. Kohel, "Endomorphism rings of elliptic curves over finite fields". Ph. D. thesis, University of California at Berkeley (1996)

[17] D. R. Kohel and B. Smith, "Efficiently computable endomorphisms for hyperelliptic curves". In F. Hess, S. Pauli, and M. Pohst (eds), Algorithmic number theory: ANTS-VII, Lecture Notes in Comput. Sci. **4076** (2006) 495–509

[18] H. W. Lenstra, Jr., "Complex multiplication structure of elliptic curves". J. Number Theory **56** #2 (1996) 227–241

[19] P. Longa and F. Sica, "Four-dimensional Gallant–Lambert–Vanstone scalar multiplication". In X. Wang and K. Sako (eds), Advances in Cryptology – ASIACRYPT 2012, Lecture Notes in Comput. Sci. **7658** (2012) 718–739

[20] J.-F. Mestre, "Familles de courbes hyperelliptiques à multiplications réelles". Progr. Math. **89** (1991) 313–334

[21] J.-F. Mestre, "Une généralisation d'une construction de Richelot". J. Algebraic Geom. **22** (2013) 575–580

[22] P. L. Montgomery, "Speeding the Pollard and Elliptic Curve Methods of factorization". Math. Comp. **48** #177 (1987) 243–264

[23] G. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance." IEEE Trans. Info. Theory **24** (1978) 106–110

[24] H.-G. Ruck, "Abelian surfaces and jacobian varieties over finite fields". Compositio Math. **76** #3 (1990) 351–366

[25] R. Schoof, "Counting points on elliptic curves over finite fields". J. Théor. Nombres Bordeaux **7** (1995) 219–254

[26] B. Smith, "Families of fast elliptic curves from $\mathbb{Q}$-curves". To appear in ASIACRYPT 2013. `http://hal.inria.fr/hal-00825287`

[27] H. P. F. Swinnerton-Dyer, A Brief Guide to Algebraic Number Theory. LMS Student Texts **50**, Cambridge University Press (2001)

[28] K. Takashima, "A new type of fast endomorphisms on Jacobians of hyperelliptic curves and their cryptographic application". IEICE Trans. Fundamentals **E89-A** #1 (2006) 124–133

[29] W. Tautz, J. Top, and A. Verberkmoes, "Explicit hyperelliptic curves with real multiplication and permutation polynomials". Can. J. Math. **43** #5 (1991) 1055–1064

[30] J. Wilson, "Curves of genus 2 with real multiplication by a square root of 5". Ph. D. Thesis, University of Oxford, 1998

[31] J. Vélu, "Isogénies entre courbes elliptiques". C. R. Math. Acad. Sci. Paris **273** (1971) 238–241

[32] Z. Zhou, Z. Hu, M. Xu, and W. Song, "Efficient 3-dimensional GLV method for faster point multiplication on some GLS elliptic curves". Inf. Process. Lett. **110** #22 (2010) 1003–1006

INRIA & École polytechnique. Équipe-Projet GRACE, INRIA Saclay – Île-de-France. Laboratoire d'Informatique (LIX), 1 rue Honoré d'Estienne d'Orves, Campus de l'École polytechnique, 91120 Palaiseau, France