CONNECTING KANI'S LEMMA AND PATH-FINDING IN THE BRUHAT-TITS TREE TO COMPUTE SUPERSINGULAR ENDOMORPHISM RINGS

KIRSTEN EISENTRÄGER AND GABRIELLE SCULLARD

Appendix A. Using Higher-Dimensional Isogenies for Endomorphism-Testing

A.1. Isogenies between polarized abelian varieties and their degrees.

Definition A.1. [Mil86, p. 126] A *polarization* of an abelian variety X defined over a field k is an isogeny $\lambda : X \to X^\vee$ to the dual variety $X^\vee$ so that $\lambda_{\overline{k}} = \phi_{\mathcal{L}}$ for some ample invertible sheaf $\mathcal{L}$ on $X_{\overline{k}}$. Here $\phi_{\mathcal{L}} : A(k) \to \mathrm{Pic}(A)$ is the map given by $a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$ with t_a the translation-by-a map.

Definition A.2. Given a positive integer N, an *N-isogeny* $\Phi : (A, \lambda_A) \to (B, \lambda_B)$ between principally polarized abelian varieties (A, λ_A) and (B, λ_B) is an isogeny such that $\Phi^\vee \circ \lambda_B \circ \Phi = N\lambda_A$. Here $\Phi^\vee : B^\vee \to A^\vee$ is the dual isogeny. An (N, N)-isogeny $\Phi : (A, \lambda_A) \to (B, \lambda_B)$ of abelian varieties of dimension g is an N-isogeny whose kernel is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^g$.

Let A be an abelian variety with a polarization λ. Since λ is an isogeny $A \to \hat{A}$, it has an inverse in $\mathrm{Hom}(\hat{A}, A) \otimes \mathbb{Q}$. The *Rosati involution* on $\mathrm{Hom}(\hat{A}, A) \otimes \mathbb{Q}$ corresponding to λ is

$$a \mapsto a^\dagger = \lambda^{-1} \circ \hat{\alpha} \circ \lambda.$$

In this paper we will consider endomorphisms of products of elliptic curves and abelian varieties. Given an abelian variety A, an integer $r > 1$ and isogenies $\phi_{i,j} : A \to A$ for $1 \le i, j \le r$, the $r \times r$ matrix $M = (\phi_{i,j})$ represents the isogeny

$$\begin{aligned} &\Phi : A^r \to A^r \text{ sending} \\ &\quad (P_1, \dots, P_r) \text{ to } (\phi_{1,1}(P_1) + \cdots + \phi_{1,r}(P_r), \dots, \phi_{r,1}(P_1) + \cdots + \phi_{r,r}(P_r)). \end{aligned}$$

We refer to this as the *matrix form of* Φ.

Definition A.3. Let A be a principally polarized abelian variety. Consider $\Phi : A^r \to A^r$ given by its matrix form $M = (\phi_{i,j})_{i,j=1,\dots,r}$ as above. Let $\phi_{i,j}^\dagger : A \to A$ be the Rosati involution of $\phi_{i,j}$. Define $\hat{\Phi}$ to be the endomorphism represented by the matrix $\hat{M} = (\phi_{j,i}^\dagger)_{i,j=1,\dots,r}$.

Definition A.2 can also be rephrased as follows, see [Rob23, Section 3.1].

Proposition A.4. *Let A be principally polarized, and let $\Phi : A^r \to A^r$ be an isogeny with matrix form M. Then $\hat{M} \cdot M = N \cdot Id_r$ if and only if Φ is an N-isogeny with respect to the product polarization.*

Proposition A.5. *Let E be an elliptic curve. Let $\Phi : E^k \to E^k$ be an N-isogeny of principally-polarized abelian varieties whose matrix form is $M = (\phi_{i,j})$. Then the degrees of the isogenies $\phi_{i,j} : E \to E$ are bounded above by N.*

Proof. If Φ is an N-isogeny, then we write $\hat{M} \cdot M = N \cdot \mathrm{Id}$. In particular, the i-th diagonal entry of $\hat{M} \cdot M$ is given by $\sum_{j=1}^{k} \phi_{j,i}^{\dagger} \phi_{j,i} = N$. For elliptic curves, $\phi_{j,i}^{\dagger}$ is the dual of $\phi_{j,i}$, so we have $\sum_{j=1}^{k} \deg(\phi_{j,i}) = N$ (where we define the degree of the 0 map to be 0). As the degree of an isogeny is nonnegative, we have $\deg(\phi_{j,i}) \leq N$. ☐

A.2. **Isogeny Diamonds and Kani's Lemma.** We now give the definition of an isogeny diamond in the setting of abelian varieties. This was first introduced by Kani [Kan97] for elliptic curves and generalized in [Rob23] to principally polarized abelian varieties.

Definition A.6. A (d_1, d_2)-*isogeny diamond configuration* is a $d_1 \cdot d_2$-isogeny $f : A \to B$ between principally polarized abelian varieties of dimension g which has two factorizations $f = f_1' \circ f_1 = f_2' \circ f_2$ with f_1 a d_1-isogeny, f_2 a d_2-isogeny and d_1, d_2 relatively prime.

$$\begin{tikzcd} A \arrow[r, "f_1"'] \arrow[d, "f_2"'] & A_1 \arrow[d, "f_1'"'] \\ A_2 \arrow[r, "f_2'"'] & B \end{tikzcd}$$

Lemma A.7 (Kani's Lemma)**.** *Let $f = f_1' \circ f_1 = f_2' \circ f_2$ be a (d_1, d_2)-isogeny diamond configuration. Then $F = \begin{pmatrix} f_1 & \tilde{f}_1' \\ -f_2 & \tilde{f}_2' \end{pmatrix}$ is d-isogeny $F : A \times B \to A_1 \times A_2$ with $d = d_1 + d_2$ and kernel* $\operatorname{Ker} F = \{(\tilde{f}_1(P), f_1'(P)) : P \in A_1[d]\}$.

Proof. This is Lemma 6 in [Rob23], which generalizes Theorem 2.3 in [Kan97]. ☐

A.3. **Endomorphism-Testing Algorithm.**

Algorithm A.8. Endomorphism-Testing Algorithm

Input: Elliptic curve E defined over $\mathbb{F}_{p^k}$; $\beta \in \operatorname{End}(E)$ which is written as a sum $\beta = b_1\beta_1 + b_2\beta_2 + b_3\beta_3 + b_4\beta_4$ where β_i are endomorphisms which can be evaluated efficiently at powersmooth points of E and $b_i \in \mathbb{Z}$; n a positive integer; Q the norm form such that $Q(x_1, x_2, x_3, x_4) = \deg(\sum_{i=1}^{4} x_i \beta_i)$

Output: TRUE if $\frac{\beta}{n}$ is an endomorphism of E and FALSE if $\frac{\beta}{n}$ is not an endomorphism.

(1) Compute $\deg(\beta)$. If $n^2 \nmid \deg(\beta)$, conclude that $\frac{\beta}{n}$ is not an endomorphism and output FALSE. Otherwise, set $N := \deg(\beta)/n^2$.
(2) Choose $a \in \mathbb{Z}$ such that $N' := N + a$ is powersmooth and $\gcd(N', n) = 1$.
(3) Compute integers $a_1, a_2, a_3, a_4 \in \mathbb{Z}$ such that $a_1^2 + a_2^2 + a_3^2 + a_4^2 = a$. Let $\alpha \in \operatorname{End}(E^4)$ be the a-isogeny, given by the matrix
$$\begin{pmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & a_4 & -a_3 \\ a_3 & -a_4 & a_1 & a_2 \\ a_4 & a_3 & -a_2 & a_1 \end{pmatrix}.$$
(4) Compute $K := \{(\frac{\widehat{\beta}}{n} \cdot \mathrm{Id}_4(P), \alpha(P)) : P \in E^4[N + a]\}$. Note that K can be computed even if $\frac{\beta}{n}$ is not an endomorphism: we can compute $\widehat{\beta}$ on $E[N + a]$, and by choice of a, n is invertible mod $N + a$.

(5) Determine if $F : E^8 \to E^8/K$ is an endomorphism of principally polarized abelian varieties. (We do so by computing an appropriate theta structure for E^8/K and checking that the projective theta constant of E^8 is the same as the projective theta constant of E^8/K.) If not, then terminate and conclude that $\frac{\beta}{n}$ is not an endomorphism.
(6) Choose $M > \sqrt{\deg(\beta)} + \sqrt{n^2(N+a)}$ which is powersmooth. We check if $F_{ij}|_{E[M]} = \psi\frac{\beta}{n}|_{E[M]}$ for some $\psi \in \mathrm{Aut}(E)$, by evaluating the composition $E \xrightarrow{\iota_i} E^8 \xrightarrow{F} E^8 \xrightarrow{\pi_j} E$ on $E[M]$. If for some F_{ij} we have $F_{ij}|_{E[M]} = \psi\frac{\beta}{n}|_{E[M]}$, then we terminate and output TRUE. If no entry F_{ij} satisfies $F_{ij} = \psi\frac{\beta}{n}$, then terminate and output FALSE.

Proposition A.9. *Algorithm A.8 is correct and runs in time polynomial in* $\log(p^k)$ *and* $\log(\deg(\beta))$.

The proof of Proposition A.9 follows from Lemmas A.11, A.14, and A.15 below.

Lemma A.10. *Suppose $\psi \in \mathrm{Aut}(E^n, \lambda)$, where λ is the product polarization on E^n. Suppose ψ is written as an $n \times n$ matrix, as in the notation of Section 2. Then for each i, ψ_{ij} is nonzero for exactly one j; for each j, ψ_{ij} is nonzero for exactly one i; and whenever ψ_{ij} is nonzero, then ψ_{ij} is an automorphism of E.*

Proof. As ψ preserves the polarization on E^n, we have that $\lambda = \psi^\vee \lambda \psi$. Therefore $\psi^\dagger \psi = 1$, where $\psi^\dagger$ denotes the image of ψ under the Rosati involution.

If M denotes the matrix form of ψ, then the matrix form of $\psi^\dagger$ is the conjugate transpose M^* of M, so that $\psi^\dagger_{ij} = \widehat{\psi_{ji}}$, the dual of ψ_{ji} [Rob23, Lemma 3]. Thus $M^*M = \mathrm{Id}_n$.

Fix $1 \leq i \leq n$. We have $\sum_{k=1}^n \widehat{\psi_{ik}}\psi_{ik} = \sum_{k=1}^n \deg(\psi_{ik}) = 1$. As $\deg(\psi_{ik})$ is a positive integer whenever ψ_{ik} is nonzero, we have that $\deg(\psi_{ik}) \neq 0$ for exactly one k, and for this k, we have $\deg(\psi_{ik}) = 1$.

For $j \neq i$, we have $\sum_{k=1}^n \widehat{\psi_{ik}}\psi_{jk} = 0$. As $\psi_{ik} = 0$ for all but one k, we have, for this k, that $\widehat{\psi_{ik}}\psi_{jk} = 0$, which implies $\psi_{jk} = 0$.

This shows that there is a unique nonzero entry in the i-th row, and that it is the only nonzero entry in its column. As there are n rows and n columns, this shows that there is a unique nonzero entry in each column, which is necessarily an automorphism. ☐

Lemma A.11. *Let $\beta \in End(E)$ and n a positive integer. If $\frac{\beta}{n}$ is an endomorphism, then Algorithm A.8 outputs True.*

Proof. Let $\phi = \frac{\beta}{n} \in \mathrm{End}(E)$. Then $\deg(\phi) = \frac{\deg(\beta)}{n^2} = N$. By construction of α (which is built out of scalar multiplications), we have the following commutative diagram, which is an (N, a)-isogeny diamond configuration.

$$\begin{array}{ccc} E^4 & \xrightarrow{\phi\cdot\mathrm{Id}_4} & E^4 \\ \alpha\big\downarrow & & \big\downarrow\alpha \\ E^4 & \xrightarrow{\phi\cdot\mathrm{Id}_4} & E^4 \end{array}$$

By Kani's Lemma, there is an (N+a)-endomorphism $G : (E^8, \lambda) \to (E^8, \lambda)$, where λ is the product polarization, such that G is given by the matrix $\begin{pmatrix} \phi \cdot \mathrm{Id}_4 & \alpha^\dagger \\ -\alpha & \widehat{\phi} \cdot \mathrm{Id}_4 \end{pmatrix}$. Moreover, as a

was chosen such that $(N,a)=1$, we can write $\ker(G)=\{\widehat{\phi}\cdot \mathrm{Id}_4(P), \alpha(P) : P \in E^4[N+a]\}$, which is precisely K as constructed in Step 4.

If F is an isogeny with $\ker(F)=K$, then F is an $(N+a)$-endomorphism of principally polarized abelian varieties (and the computed theta constants are equal). Therefore, we proceed to Step 6.

By [Kan97, Proposition 1.1], there is an automorphism $\psi : E^8 \to E^8$ which preserves the product polarization and such that $F=\psi G$. By Lemma A.10 each row and each column of the matrix form of ψ has exactly one nonzero entry, which is an automorphism of E. Thus, the entries of the matrix form of F are precisely the entries of the matrix form of G, composed with an automorphism of E. In particular, four of the nonzero entries of F will be given by $\psi_{ij}\phi$ for some automorphism $\psi_{ij} \in \mathrm{End}(E)$. $\square$

Lemma A.12. *The subgroup K in Step 4 of Algorithm A.8 is a maximally isotropic subgroup of $E^8[N+a]$ (whether or not $\frac{\beta}{n}$ is an endomorphism). Thus, K is the kernel of an $(N+a)$-isogeny with respect to some polarization on E^8.*

Proof. Let K denote the subgroup in Step 4 of Algorithm A.8, which is precisely the image of $F^\dagger = \begin{pmatrix} \frac{1}{n}\widehat{\beta}\cdot \mathrm{Id}_4 & -\alpha^\dagger \\ \alpha & \frac{1}{n}\beta \cdot \mathrm{Id}_4 \end{pmatrix}$ on $(E^4\times E^4)[N+a]$

Let $m \in \mathbb{Z}$ such that $mn \equiv 1 \pmod{N+a}$. Consider the following isogeny factorization configuration:

$$\begin{array}{ccc} E^4 & \xrightarrow{m\beta\cdot \mathrm{Id}_4} & E^4 \\ {\scriptstyle mn\alpha}\downarrow & & \downarrow{\scriptstyle mn\alpha} \\ E^4 & \xrightarrow{m\beta\cdot \mathrm{Id}_4} & E^4 \end{array}$$

By Kani's Lemma, there is an $m^2n^2(N+a)$-endomorphism of E^8 with respect to the product polarization, given by $F' = \begin{pmatrix} m\beta\cdot \mathrm{Id}_4 & mn\alpha^\dagger \\ -mn\alpha & m\widehat{\beta}\cdot \mathrm{Id}_4 \end{pmatrix}$ and with kernel equal to the image of $F'^\dagger = \begin{pmatrix} m\widehat{\beta}\cdot \mathrm{Id}_4 & -mn\alpha^\dagger \\ mn\alpha & m\beta\cdot \mathrm{Id}_4 \end{pmatrix}$ on $(E^4\times E^4)[m^2n^2(N+a)]$. Let $K' = F'^\dagger(E^4\times E^4)[m^2n^2(N+a)]$. By Kani's Lemma, K' is a maximal isotropic subgroup of $E^8[m^2n^2(N+a)]$.

First, note that $K'\cap E^8[N+a]$ is a maximal isotropic subgroup of $E^8[N+a]$. If $e_{m^2n^2(N+a)}$ is the Weil pairing on $E^8[m^2n^2(N+a)]$ and $P,Q \in E^8[N+a]\cap K'$, then $1 = e_{m^2n^2(N+a)}(P,Q) = e_{N+a}(mnP, mnQ)$ by compatibility of the Weil pairing. By choice of m, we have $e_{N+a}(mnP,mnQ) = e_{N+a}(P,Q)$. Thus, $K'\cap E^8[N+a]$ is an isotropic subgroup of $E^8[N+a]$. Since K' is a maximal isotropic subgroup of $E^8[m^2n^2(N+a)]$, and $(m^2n^2, N+a)=1$, we have $K'\cap E^8[N+a]$ has order $(N+a)^8$ and is therefore a maximal isotropic subgroup of $E^8[N+a]$.

Finally, we have $K = K'\cap E^8[N+a]$. It is clear that $K \subset K'\cap E^8[N+a]$, since $F^\dagger = F'^\dagger$ on $E^8[N+a]$. Moreover, by the description of K as $\{(\frac{\widehat{\beta}}{n}\cdot \mathrm{Id}_4(P), \alpha(P)) : P \in E^4[N+a]\}$, where β and α have degrees coprime to $N+a$, it is clear that the order of $\#K = (N+a)^8 = \#(K'\cap E^8[N+a])$. Thus, K is a maximal isotropic subgroup of $E^8[N+a]$.

By [Kan97, Proposition 1.1], K is therefore the kernel of an $N+a$-isogeny with respect to some polarization. $\square$

The following lemma shows that an endomorphism is uniquely determined by its degree and its action on M-torsion, for suitably large M (depending on the degree).

Lemma A.13. *Let E be an elliptic curve and $\phi, \psi \in End(E)$. Let $M > \sqrt{\deg(\phi)} + \sqrt{\deg(\psi)}$. If $\psi|_{E[M]} = \phi|_{E[M]}$, then $\psi = \phi$.*

Proof. For contradiction, assume the hypotheses of the lemma and that $\phi - \psi$ is nonzero. Since $\psi|_{E[M]} = \phi|_{E[M]}$, $E[M] \subset \ker(\phi - \psi)$. Since $\phi - \psi$ is nonzero, we must have $\phi - \psi = M\gamma$ for some nonzero $\gamma \in \mathrm{End}(E)$. Thus, $\deg(\phi - \psi) = M^2 \deg(\gamma)$. By the Cauchy-Schwartz inequality, $\deg(\phi - \psi) \leq (\sqrt{\deg(\phi)} + \sqrt{\deg(\psi)})^2$. Hence $M^2 \leq M^2 \deg(\gamma) \leq (\sqrt{\deg(\phi)} + \sqrt{\deg(\psi)})^2$, which is a contradiction. $\square$

Lemma A.14. *If $\frac{\beta}{n}$ is not an endomorphism, Algorithm A.8 outputs False.*

Proof. Assume $F : E^8 \to E^8$ respects the product polarization and has kernel K as defined in Step 4. Let F_{ij} be an entry in the matrix form of F. Then $\deg(F_{ij}) \leq (N + a)$. If $F_{ij}|_{E[M]} = \frac{\psi\beta}{n}|_{E[M]}$ for some $M > \sqrt{\deg(\beta)} + \sqrt{n^2(N + a)}$ and an automorphism ψ, then $nF_{ij}|_{E[M]} = \psi\beta|_{E[M]}$. As we know $\psi\beta, nF_{ij}$ are endomorphisms, and $M > \sqrt{\deg(\beta)} + \sqrt{n^2(N + a)} > \sqrt{\deg(\psi\beta)} + \sqrt{n \deg(F_{ij})}$, Lemma A.13 implies that $\frac{\beta}{n} = \psi^{-1} F_{ij} \in \mathrm{End}(E)$. $\square$

Lemma A.15. *Algorithm A.8 runs in time polynomial in* $\log(p^k)$ *and* $\log(\deg(\beta))$.

Proof. Let B be a powersmoothness bound for $N + a$ (as in Step 2), and let C be a powersmoothness bound for M (as in Step 6). Given Q, computing the degree $\deg(\beta)$ amounts to evaluating the quaternary quadratic form Q at (b_1, b_2, b_3, b_4). Finding a_1, a_2, a_3, a_4 can be done in time $O((\log(a))^2 (\log\log(a))^{-1})$, see [RS86, PT18].

Computing a basis for K means first computing a basis for $E[N+a]$; decomposing into at most $\log(N+a)$ prime power parts, this can be done in $O(B^2 \log(p^k)^2 \log(N+a))$ operations [Rob23, Lemma 7]. Evaluating $\widehat{\beta}$ on a basis for $E[N + a]$ and α on the induced basis for $E^4[N + a]$ can be done efficiently by our assumption on β and powersmoothness of $N + a$.

For Step 5, we need to check that F is truly an endomorphism. We place the additional data of a symmetric theta structure of level 2 on E^8, by taking an appropriate symplectic basis of $E[4]$ if $N + a$ is odd, or $E[2^{m+2}]$ where 2^m is the largest power of 2 dividing $N + a$ otherwise. (See Proposition C.2.6 of [DLRW23] and the preceding remark about how to choose a basis which is compatible with K in different cases.) Decomposing K into prime components and using the previous data, we can compute the theta null point of E^8/K with the induced theta structure in $O(\ell_{N+a}^8 \log(N+a))$ operations, where ℓ_{N+a} is the largest prime dividing $N+a$. (See Theorem C.2.2 and Theorem C.2.5 of [DLRW23].) Finally, as F may not preserve the product theta structure even if it is the desired endomorphism, we need to act on the theta null point by a polarization-preserving matrix in order to directly compare theta null points. When $N + a$ is odd, this matrix is computed explicitly [DLRW23, Proposition C.2.4] from the action of F on $E[4]$, which can also be evaluated in $O(\ell_{N+a}^8 \log(N + a))$ operations. This gives $O(B^8 \log(N + a))$ operations for this step.

In Step 6, computing a basis for the prime-power parts of $E[M]$ takes $O(C^2 \log(p^k)^2 \log(M))$ operations. If F is an endomorphism, then having already computed theta coordinates for E^8 and E^8/K in the previous step, we can evaluate F in terms of theta coordinates [DLRW23, Theorem C.2.2, Theorem C.2.5] and translate back to Weierstrass coordinates to check the equality. Note that there are only finitely many, and usually two, automorphisms to consider.

Each evaluation costs $O(\ell_{N+a}^8 \log(N+a))$ operations where ℓ_{N+a} is the largest prime dividing $N+a$. There are 64 entries F_{ij} to check, by checking the equality on at most $2\log(M)$ points. Thus, this step requires at most $O(C^2 \log(p^k)^2 \log(M) + B^8 \log(N+a)\log(M))$ operations.

Now, we show that B and C can be taken polynomially sized in $\deg(\beta)$, that $N+a$ is $\tilde{O}(\deg(\beta))$, and that M is $\tilde{O}(1+n)\sqrt{\log(\deg(\beta))\deg(\beta)}$. Here, $\tilde{O}$ ignores logarithmic factors.

M and C are easier to analyze, as we have no restrictions on the primes which can divide M. When $k \geq 6$, we have that the k-th prime p_k satisfies $k\log(k) < p_k < k(\log(k) + \log\log(k))$ [RS62, Corollary of Theorem 3]. Therefore, we can take M to be a product of the first k primes where k is at most $\log(\sqrt{\deg(\beta)} + \sqrt{n^2(N+a)})$ and $C = \tilde{O}(\log(\sqrt{\deg(\beta)} + \sqrt{n^2(N+a)})$. Such a product is bounded by $\tilde{O}((\log(\sqrt{\deg(\beta)} + \sqrt{n^2(N+a)})(\sqrt{\deg(\beta)} + \sqrt{n^2(N+a)}))$.

We can bound $N+a$ and B similarly. However, $N+a$ is chosen to be coprime to Nn (equivalently, coprime to $\deg(\beta)$), so we instead take $N+a$ to be the product of the first at most $\log(N)$ primes which are coprime to Nn. Then we can take $B = \tilde{O}(\log(\deg(\beta)))$, noting that Nn has at most $\log(\deg(\beta))$ prime factors, so the largest prime we use is the k-th prime for $k \leq 2\log(\deg(\beta))$. The smallest such product which is larger than N is at most $\tilde{O}(\log(\deg(\beta))N)$. Thus, we have $N+a = \tilde{O}(\deg(\beta))$.

Returning to M and C, we get $\sqrt{\deg(\beta)} + \sqrt{n^2(N+a)} \leq \tilde{O}((1+n)\sqrt{\log(\deg(\beta))\deg(\beta)})$. Hence $M = \tilde{O}((1+n)\sqrt{\log(\deg(\beta))\deg\beta})$ and $C = \tilde{O}(\log((1+n)\sqrt{\log(\deg(\beta)\deg(\beta)}))$. □

One can get speedups by replacing E^8 by E^4 and tweaking parameters as discussed by Robert in [Rob23, Section 6]; for simplicity and for a proven complexity we don't go into those details here.

Appendix B. An Explicit Isomorphism with the Matrix Ring

Proof of Proposition 5.1. in [ES25].

Proof. We first compute the degree map Q, such that $Q(a_1, a_2, a_3, a_4) = \deg(a_1 + a_2\alpha + a_3\gamma + a_4\alpha\gamma)$, extending $\mathbb{Z}$-scalars of the usual degree map to $\mathbb{Z}_q$. The coefficients are specified by the value of the reduced traces $\mathrm{Trd}(\beta_i\hat{\beta}_j)$ where β_i and β_j range over all elements of the basis; this can be done in time polynomial in $\log(\deg(\alpha)\deg(\gamma))$ and $\log(p)$ via a modified Schoof's algorithm, by evaluating the products on sufficiently large torsion.

On input $\mathcal{O}_0$, specified by the multiplication table and Q, we compute a q-maximal q-enlargement of $\mathcal{O}_0$, denoted $\tilde{\mathcal{O}}$ [Voi13, Algorithms 3.12, 7.9, 7.10]. More specifically, Algorithm 3.12 produces a basis for $\mathcal{O}_0 \otimes \mathbb{Z}_q$ such that the norm form is normalized. Algorithm 7.9 gives a basis for a potentially larger "q-saturated" order, whose elements are of the form $\frac{x}{q^k}$. Here, x has coefficients in terms of the original basis of size at most $\max(\mathrm{Trd}(\beta_i\hat{\beta}_j))^4$, where β_i and β_j range over basis elements of the original basis. The power k in the denominator is at most $\lfloor j/2 \rfloor$ where j is the valuation of the atomic form corresponding to the basis element, and hence $k \leq e = v_q(\mathrm{discrd}(\mathcal{O}_0))$.

Since $|\mathrm{Trd}(\beta_i\hat{\beta}_j)| \leq 2\sqrt{\deg(\beta_i)\deg(\beta_j)}$, the coefficients are of size at most $16\deg(\alpha)^2\deg(\gamma)^2$. Applying Algorithm 7.10 adjoins a zero divisor mod q, which is of the form $\frac{x}{q}$; here, x is expressed as linear combinations of the basis with coefficients of size at most $16q^2\deg(\alpha)^2\deg(\gamma)^2$. Thus, the basis which is output for $\tilde{\mathcal{O}}$ has coefficients (in terms of the basis $\{1, \alpha, \gamma, \alpha\gamma\}$)

which are polynomially-sized in $\deg(\alpha)$, $\deg(\gamma)$, and q. Therefore, a basis element $\frac{\beta}{q^k}$ satisfies $\log(\deg(\beta))$ is at most polynomially-sized in $\log(\deg(\alpha))$, $\log(\deg(\gamma))$, and $\log(q)$. $\square$

Proposition B.1. *Given a basis and multiplication table for a q-maximal order $\tilde{\mathcal{O}}$, and a precision q^r, there is an algorithm which computes a zero divisor $x \in \tilde{\mathcal{O}} \otimes \mathbb{Z}_q$, up to precision q^r. In other words, there is an algorithm to compute an element $x \in \tilde{\mathcal{O}} \otimes \mathbb{Z}_{(q)}$ such that there exists a zero divisor $x' \in \tilde{\mathcal{O}} \otimes \mathbb{Z}_q$ with $v_q(x - x') \geq r$. The element x is expressed as a linear combination of the given basis such that coefficients are polynomially-sized in q^r and $\deg(\beta_i)\deg(\beta_j)$, where β_i and β_j range over elements of the given basis. The runtime is polynomial in $\log(q^r)$ and the size of $\tilde{\mathcal{O}}$.*

Proof. First, use [Voi13, Algorithm 3.12] on $\tilde{\mathcal{O}} \otimes \mathbb{Z}_q$ to obtain a normalized basis $\{f_1, f_2, f_3, f_4\}$ for $\tilde{\mathcal{O}} \otimes \mathbb{Z}_q$. Note that, clearing denominators by units in $\mathbb{Z}_q$ if necessary, we can ensure $f_i \in \mathcal{O}_0 \otimes \mathbb{Z}_{(q)}$.

As $\tilde{\mathcal{O}}$ is q-maximal, the output basis being normalized means that the reduced norm form $Q(x_1, x_2, x_3, x_4) = \mathrm{Nrd}(\sum_{i=1}^4 x_i f_i)$ is given by a sum of atomic forms.

When q is odd, this means that $Q(x_1, x_2, x_3, x_4) = \sum_{i=1}^4 a_i x_i^2$ where $a_i \in (\mathbb{Z}_q)^\times$ and $\mathrm{Trd}(f_i \hat{f}_j) = 0$ when $i \neq j$. When $q = 2$, atomic forms are of one of the two following types: (i) ax^2 for $a \in (\mathbb{Z}_q)^\times$ or (ii) $a_i x_i^2 + a_{ij} x_i x_j + a_j x_i^2$ such that $v_2(a_{ij}) \leq v_2(a_i) \leq v_2(a_j)$ and $v_2(a_i)v_2(a_{ij}) = 0$. Up to reordering basis elements if necessary, we may therefore write $Q(x_1, x_2, x_3, x_4) = A_{12}(x_1, x_2) + A_{34}(x_3, x_4)$, where A_{ij} is either atomic of type (ii) or a sum of atomic forms of type (i).

We split up rest of the proof into the case that q is odd and $q = 2$: We first produce a nonzero element $x \in (\mathbb{Z}/q\mathbb{Z})^4$ such that $Q(x) \equiv 0 \pmod{q}$. Then, we show that there exists a lift x' in $\tilde{\mathcal{O}} \otimes \mathbb{Z}_q$, and we compute and output a lift of x in $\tilde{\mathcal{O}} \otimes \mathbb{Q}$ up to our desired precision q^r. In each case, the coefficients (in terms of the f_i) x_1, x_2, x_3, x_4 will be chosen mod q^r, so the resulting output coefficients (in terms of the input basis) is polynomially-sized in q^r and $\deg(\beta_i)\deg(\beta_j)$.

Case 1: q is odd. Then the resulting reduced norm form is given by $Q(x_1, x_2, x_3, x_4) = \mathrm{Nrd}(\sum_{i=1}^4 x_i f_i) = \sum_{i=1}^4 a_i x_i^2$. The coefficients a_i may be rational, but $v_q(a_i) = 0$, so we may replace a_i by an integer mod q^r. Then there is a nonzero solution $(x_1, x_2, x_3) \in (\mathbb{F}_q)^3$ to the equation $\sum_{i=1}^3 a_i x_i^2 \equiv 0$, which can be found by a deterministic algorithm running in polynomial time in $\log(q)$ [vdW05]. Reindexing the basis elements f_i and the corresponding a_i as necessary, we can assume $x_1 \neq 0$, so that the quadratic polynomial $Q_1(x) = Q(x, x_2, x_3, 0)$ has a nonzero solution, x_1, mod q. Furthermore, $Q_1'(x_1) = 2a_1 x_1$, which is nonzero mod q. Thus, by Hensel's Lemma, x can be lifted to a solution to $Q_1(x) = 0$ over $\mathbb{Z}_q$. A solution mod q^r can be recovered in (at most) $r - 1$ Hensel lifts, each running in polynomial time in $\log(q)$ (see [vzGG13, Algorithm 15.10 and Theorem 15.11] or [Coh93, Theorem 3.5.3]).

Case 2: $q = 2$. In this case, the resulting reduced norm form is given by the normalized form $Q(x_1, x_2, x_3, x_4) = A_{1,2}(x_1, x_2) + A_{3,4}(x_3, x_4)$. Here $A_{i,j}(x_i, x_j) = a_i x_i^2 + a_{i,j} x_i x_j + a_j x_j^2$. The discriminant of Q, and therefore of $\tilde{\mathcal{O}} \otimes \mathbb{Z}_q$, is $(4a_1a_2 - a_{1,2}^2)(4a_3a_4 - a_{ij})^2$. As $\tilde{\mathcal{O}} \otimes \mathbb{Z}_q$ is 2-maximal, $a_{i,2}$ and $a_{3,4}$ are necessarily nonzero (mod 2).

Let $A(y, z)$ be an atomic form of type (ii), say $A(y, z) = ay^2 + byz + cz^2$ such that $v_2(b) \leq v_2(a) \leq v_2(c)$. Further assume $v_2(b) = 0$. We show that we can choose $y_0, z_0 \in \mathbb{Z}/2\mathbb{Z}$ such that $A(y_0, z_0) \equiv 1 \pmod{2}$ and at least one of y_0 or z_0 is odd. If $v_2(a) \geq 1$ (and therefore $v_2(c) \geq 1$ as well), or if $v_2(a) = v_2(c) = 0$, we can set $y_0 \equiv z_0 \equiv 1 \pmod 2$. Otherwise, in the case that $v_2(a) = 0$ and $v_2(c) > 0$, we can set $y_0 \equiv 1 \pmod 2$ and $z_0 \equiv 0 \pmod 2$.

The quadratic form $Q(x_1, x_2, x_3, x_4)$ is the sum of two atomic quadratic forms $A_{1,2}$ and $A_{3,4}$ as above. We obtain a solution mod 2 by choosing x_1, x_2, x_3, x_4 mod 2 as just described. If x_1 and x_2 are both odd, i.e. in the case that a_1 and a_2 are of the same parity, we lift x_2, x_3, x_4 to $\mathbb{Z}/q^r\mathbb{Z}$ to obtain a quadratic polynomial $Q_1(x) = Q(x, x_2, x_3, x_4)$ with a solution mod 2 at $x \equiv 1 \pmod 2$. Then the derivative $Q_1'(1) = 2a_1 + a_{1,2}x_2$ is a unit in $\mathbb{Z}_2$. Otherwise, in the case that x_1 is odd and x_2 is even, we fix integers $x_1, x_3, x_4 \in \mathbb{Z}/q^r\mathbb{Z}$ to obtain a quadratic polynomial $Q_2(x) = Q(x_1, x, x_3, x_4)$ with a solution mod 2 at $x \equiv 0 \pmod 2$. Then the derivative $Q_2'(0) = a_{1,2}x_1$ is a unit in $\mathbb{Z}_2$. In either case, we obtain a solution to $Q = 0$ mod 2 which can be lifted to a solution in $\mathbb{Z}_q^4$ via Hensel's Lemma. As in the case that q is odd, a solution mod q^r can be recovered in $r - 1$ lifts, running in polynomial time in $\log(q)$. $\square$

Proof of Prop 5.2. in [ES25].

Proof. By Proposition B.1, there is an algorithm to compute $x \in \tilde{\mathcal{O}} \otimes \mathbb{Z}_{(q)}$ such that $\mathrm{Nrd}(x) \equiv 0 \pmod{q^r}$. We first use x as input for [Voi13, Algorithm 4.2]to compute nonzero $e \in \tilde{\mathcal{O}} \otimes \mathbb{Z}_q$ such that $e^2 = 0$. As before, we only specify e up to precision q^r and can therefore approximate e with an element of $\tilde{\mathcal{O}} \otimes \mathbb{Z}$. Furthermore, we can choose $e = \sum_{i=1}^4 e_i f_i$ such that for some i, $q \nmid e_i$.

Then, on input e, we use [Voi13, Algorithm 4.3] to compute i' and j' as a $\mathbb{Z}$-linear combination of $\frac{1}{s}e$ and $\frac{1}{s}f_i e$, for a basis element f_i such that $s = \mathrm{Trd}(f_i e)$ is nonzero.

In fact, we will modify the algorithm by choosing f_i such that $\mathrm{Trd}(f_i e)$ is nonzero mod q. If no such i exists, then $\mathrm{Trd}(ye) = 0$ for all $y \in \tilde{\mathcal{O}}$, so we show this cannot happen. Write $y = \sum_{j=1}^4 y_j f_j$ and $e = \sum_{i=1}^4 e_i f_i$, and consider the expression for $\mathrm{Trd}(ye) = -\mathrm{Trd}(y\bar{e})$ given by $\sum_{j=1}^4 \sum_{i=1}^4 -y_i e_j \mathrm{Trd}(f_i \hat{f}_j)$. As $\{f_1, f_2, f_3, f_4\}$ is a normalized basis, the equation simplifies in the following ways, depending on if q is even or odd.

If q is odd, then the expression simplifies to $\sum_{i=1}^4 -e_i \mathrm{Trd}(f_i \hat{f}_i) y_i$. This is identically 0 mod q if and only if q divides $e_i \mathrm{Trd}(f_i \hat{f}_i)$ for all i. In the notation of the proof of Proposition B.1, $\mathrm{Trd}(f_i \hat{f}_i)$ is exactly $2a_i$ and hence is not divisible by q by q-maximality. Hence, this expression is identically 0 mod q if and only if q divides e_i for all i, we chose e such that this does not happen.

If $q = 2$, we have that $\mathrm{Trd}(f_i \hat{f}_i) = 2\,\mathrm{Nrd}(f_i) \equiv 0 \pmod q$ for all i, so the only nonzero terms are $-e_1 \mathrm{Trd}(f_2 \hat{f}_1), -e_2 \mathrm{Trd}(f_1 \hat{f}_2), -e_3 \mathrm{Trd}(f_4 \hat{f}_3), -e_4 \mathrm{Trd}(f_3 \hat{f}_4)$. We have $\mathrm{Trd}(f_1 \hat{f}_2) = Trd(f_2 \hat{f}_1) = a_{1,2}$ and $\mathrm{Trd}(f_3 \hat{f}_4) = \mathrm{Trd}(f_4 \hat{f}_3) = a_{3,4}$, which are not divisible by q as we showed in the proof of Proposition B.1. Hence this expression is identically 0 mod q if and only if q divides e_i for all i, but we chose e such that this does not happen.

This shows that $v_q(\mathrm{Trd}(ef_i)) = 0$ for some i, so that $\frac{1}{s} \in \mathbb{Z}_q$, and the elements i' and j' output by Algorithm 4.3 (with this modification) are elements of $\tilde{\mathcal{O}} \otimes \mathbb{Z}_q$ and furnish an isomorphism of $\tilde{\mathcal{O}} \otimes \mathbb{Z}_q \to M_2(\mathbb{Z}_q)$. To get i' and j' in $\tilde{\mathcal{O}}$ rather than in $\tilde{\mathcal{O}} \otimes \mathbb{Q}$, replace $\frac{1}{s}$ by an integer $m \equiv s^{-1} \pmod{q^r}$. $\square$

Appendix C. Known Subgraph

C.1. **Known Subgraph of the Bruhat-Tits Tree.** In the general case, the order Λ_0 may not be Bass. We have just shown how to recover Λ_E without having to list each of the local maximal orders containing Λ_0. Our approach is to determine the distance of Λ_E from $M_2(\mathbb{Z}_q)$, which is the only vertex we know to containing Λ_0, and then to recover the path from $M_2(\mathbb{Z}_q)$ to Λ_E one step at a time. This second step is the most costly, requiring at most $4(q+1)$ applications of Algorithm A.8 for each step in the path. In the worst case, Λ_E is e steps from $M_2(\mathbb{Z}_q)$.

If we can describe the set of maximal orders containing Λ_0 as $N_\ell(P)$ for a path P and an integer $\ell \geq 0$, we can obtain Λ_E more efficiently. First, we compute the distance r of Λ_E from the path P; next, we compute the order Λ' in P which is closest to Λ_E; finally, we recover the path from Λ' to Λ_E, one step at a time. As before, this last step is the most costly, but in the worst case, we only need to recover ℓ steps, where $\ell \leq \frac{e}{3}$.

Algorithm C.1. Finding Λ_E When the Subgraph is Known

Input: An order $\mathcal{O}_0 \subset \mathrm{End}(E)$; $e = v_q(\mathrm{discrd}(\mathcal{O}_0))$; a q-maximal q-enlargement $\tilde{O}$ of $\mathcal{O}_0$; an isomorphism $f : \mathcal{O}_0 \otimes \mathbb{Q}_q \to M_2(\mathbb{Q}_q)$ such that $f(\tilde{O} \otimes \mathbb{Z}_q) = M_2(\mathbb{Z}_q)$, given up to precision q^{e+1}; matrices T_1' and T_2' corresponding to endpoints of a path P and an integer $\ell \geq 0$ such that $\cap_{\Lambda \supset f(\mathcal{O}_0 \otimes \mathbb{Z}_q)} \Lambda = \cap_{\Lambda \in N_\ell(P)} \Lambda$.

Output: γ such that $\Lambda_E = \gamma^{-1} M_2(\mathbb{Z}_q)\gamma$

(1) Compute the least $r \leq \ell$ such that $\cap_{\Lambda \in N_r(P)} \Lambda \subset \Lambda_E$.
(2) Partition P into two disjoint paths P_0 and P_1 of equal length, and check if P_0 satisfies $\Lambda_E \in N_r(P_0)$. Set $P' = P_0$ if $\Lambda_E \in N_r(P_0)$ and $P' = P_1$ otherwise. Then replace P by P' and continue until P consists of a single order $T^{-1}M_2(\mathbb{Z}_q)T$.
(3) Recover the matrix path $d_1, d_2, \ldots, d_r$ of length r from $T^{-1}M_2(\mathbb{Z}_q)T$ to Λ_E, so that $\Lambda_E = (d_r \cdots d_2 d_1 T)^{-1} M_2(\mathbb{Z}_q) d_r \cdots d_2 d_1 T$. Output $d_r \cdots d_2 d_1 T$.

Proposition C.2. *Algorithm C.1 requires at most* $4(\ell + \log(|P|) + \ell q + 1)$ *applications of Algorithm A.8.*

Proof sketch:

The extra information about the graph structure allows us to replace $M_2(\mathbb{Z}_q)$ with an order whose which is close to Λ_E, thus minimizing the most costly step (recovering the path step-by-step). However, we stress that it is not clear how to efficiently obtain Λ_1, Λ_2, and Λ_3 from Λ_0.

C.2. **Possible Subgraphs.** We can use Tu's results to describe the subgraph of maximal orders containing any order in $M_2(\mathbb{Q}_q)$. We summarize the possible subgraphs in the following corollary.

Corollary C.3. *Suppose Λ is an order in $M_2(\mathbb{Q}_q)$. Let $S = \{\Lambda'$ maximal $: \Lambda \subset \Lambda'\}$. Then there exists a path $P$and an integer $\ell \geq 0$ such that $S = N_\ell(P)$.*

Proof. By Lemma 3.8 in [ES25], Λ, is contained in only finitely many maximal orders even when Λ is not a finite intersection of maximal orders. Hence the set S of maximal orders containing Λ is a finite set. Let $\Lambda'' = \cap_{\Lambda' \in S} \Lambda'$. The set of maximal orders containing Λ is precisely the set of maximal orders containing Λ''. Thus, it suffices to prove the statement in the case that Λ is equal to a finite intersection of maximal orders.

For the rest of the proof, assume Λ is a finite intersection of maximal orders. By Theorem [Tu11, Theorem 8], we can choose $\Lambda_1, \Lambda_2, \Lambda_3 \in S$ such that $\Lambda = \Lambda_1 \cap \Lambda_2 \cap \Lambda_3$. We need to construct a path P and an integer $\ell \geq 0$ such that for a maximal order Λ', we have $\Lambda_1 \cap \Lambda_2 \cap \Lambda_3 \subset \Lambda'$ if and only if $\Lambda' \in N_\ell(P)$.

By reindexing if necessary, let Λ_1 and Λ_2 be such that $d(\Lambda_1, \Lambda_2)$ is maximal among $d(\Lambda_i, \Lambda_j)$. Let P' denote the path from Λ_1 to Λ_2, and let $\ell = d(\Lambda_3, P')$.

By maximality of $d(\Lambda_1, \Lambda_2)$, the path P' has length at least 2ℓ. For $i = 1, 2$, let Λ_i' denote the vertex on the path P' such that $d(\Lambda_i', \Lambda_i) = \ell$. Let P be the path of vertices from Λ_1' to Λ_2'. We will show that $S = N_\ell(P)$.

First, note that $\ell = d(\Lambda_3, P)$. Suppose not. Then the closest vertex v' of P' to Λ_3 lies between Λ_i' and Λ_i for some i, and $v' \neq \Lambda_i'$. Then for $j \neq i, j \neq 3$, we have $d(\Lambda_j, \Lambda_i) = d(\Lambda_j, \Lambda_i') + d(\Lambda_i', \Lambda_i) = d(\Lambda_j, \Lambda_i') + d(\Lambda_i', v') + d(v', \Lambda_i)$. Since $d(v', \Lambda_i) < \ell = d(v', \Lambda_3)$, we have $d(\Lambda_j, \Lambda_i) \leq d(\Lambda_j, v') + d(v', \Lambda_3)$. But $d(\Lambda_j, v') + d(v', \Lambda_3) = d(\Lambda_j, \Lambda_3)$. This contradicts maximality of $d(\Lambda_1, \Lambda_2)$.

Let Λ_4 be a maximal order, and let $m = d(\Lambda_4, P)$. We need to show that $\Lambda_4 \in S$ if and only if $m \leq \ell$. By Lemmas 3.15 and 3.16 in [ES25], this is the same as showing that $d_3(S) = d_3(S \cup \{\Lambda_4\})$ if and only if $m \leq \ell$.

We have $d(\Lambda_1, \Lambda_2) + d(\Lambda_2, \Lambda_4) + d(\Lambda_4, \Lambda_1) = 2d(\Lambda_1, \Lambda_2) + 2m$. We will show that $d_3(S \cup \{\Lambda_4\}) = 2d(\Lambda_1, \Lambda_2) + 2\max\{\ell, m\}$.

If $i = 1$ or $i = 2$, let P_i denote the path between Λ_3 and Λ_i, and let $n_i = d(\Lambda_4, P_i)$.. We have $d(\Lambda_i, \Lambda_4) + d(\Lambda_4, \Lambda_3) + d(\Lambda_3, \Lambda_i) = 2d(\Lambda_i, \Lambda_3) + 2n_i$. If $n_i \leq m$, then this is clearly at most $2d(\Lambda_1, \Lambda_2) + 2m$. Let v_i denote the vertex of P_i which is closest to Λ_4, so $d(\Lambda_4, v_i) = n_i$ If $n_i > m$, the path P_i does not contain the closest vertex v on P to Λ_4 and $d(v, v_i) = n_i - m$. In this case, it follows that v_i lies on the path P, as otherwise $v_i = v$ and $n_i = m$, and that v_i is the closest vertex of P to Λ_3. Thus, $d(\Lambda_1, \Lambda_2) = d(\Lambda_i, v_i) + n_i - m + d(v, \Lambda_j)$, where $j \neq i, 3, 4$. We also have $d(\Lambda_i, \Lambda_3) = d(\Lambda_i, v_i) + d(v_i, \Lambda_3)$. Thus $2d(\Lambda_i, \Lambda_3) + 2n_i = 2(d(\Lambda_i, v_i) + n_i - m) + 2m \leq 2d(\Lambda_1, \Lambda_2) + 2m$.

We have shown that $d_3(S \cup \{\Lambda_4\}) = 2d(\Lambda_1, \Lambda_2) + 2\max\{\ell, m\}$. This is equal to $d_3(S)$ if and only if $m \leq \ell$, and hence Λ_4 is in S if and only if $\Lambda_4 \in N_\ell(P)$. $\square$

References

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[DLRW23] Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. SQISignHD: New dimensions in cryptography. Cryptology ePrint Archive, Paper 2023/436, 2023. `https://eprint.iacr.org/2023/436`.

[ES25] Kirsten Eisenträger and Gabrielle Scullard. Connecting Kani's lemma and path-finding in the Bruhat-Tits tree to compute supersingular endomorphism rings, 2025. Preprint.

[Kan97] Ernst Kani. The number of curves of genus two with elliptic differentials. *J. Reine Angew. Math.*, 485:93–121, 1997.

[Mil86] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.

[PT18] Paul Pollack and Enrique Treviño. Finding the four squares in lagrange's theorem. *Integers*, 18A:A15, 2018.

[Rob23] Damien Robert. Breaking SIDH in polynomial time. In *Advances in cryptology—EUROCRYPT 2023. Part V*, volume 14008 of *Lecture Notes in Comput. Sci.*, pages 472–503. Springer, Cham, [2023] ©2023.

[RS62] J. Barkley Rosser and Lowell Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois Journal of Mathematics*, 6:64–94, 1962.

[RS86] Michael O. Rabin and Jeffery O. Shallit. Randomized algorithms in number theory. *Communications on Pure and Applied Mathematics*, 39(S1):S239–S256, 1986.

[Tu11] Fang-Ting Tu. On orders of $M(2, K)$ over a non-Archimedean local field. *Int. J. Number Theory*, 7(5):1137–1149, 2011.

[vdW05] Christiaan E. van de Woestijne. Deterministic equation solving over finite fields. In *International Symposium on Symbolic and Algebraic Computation*, 2005.

[Voi13] John Voight. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. In *Quadratic and higher degree forms*, volume 31 of *Dev. Math.*, pages 255–298. Springer, New York, 2013.

[vzGG13] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, third edition, 2013.

Kirsten Eisenträger, Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, USA, eisentra@math.psu.edu

Gabrielle Scullard, Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, USA, gns49@psu.edu