Products and polarizations of super-isolated abelian varieties

Stefano Marseglia¹ · Travis Scholl²

Received: 21 August 2020 / Accepted: 21 May 2021 / Published online: 22 June 2021
© The Author(s) 2021

Abstract
In this paper we study super-isolated abelian varieties, that is, abelian varieties over finite fields whose isogeny class contains a single isomorphism class. The goal of this paper is to (1) characterize whether a product of super-isolated varieties is super-isolated, and (2) characterize which super-isolated abelian varieties admit principal polarizations, and how many up to polarized isomorphisms.

1 Introduction

An abelian variety $A/F_q$ is super-isolated if its $F_q$-isogeny class contains only the isomorphism class of $A$. Hence a super-isolated $A/F_q$ is determined up to isomorphism by the characteristic polynomial of its Frobenius endomorphism. In [18], the second author introduced super-isolated elliptic curves and surfaces in the context of cryptography, and in [19] this was generalized to higher dimensional simple super-isolated abelian varieties. In this paper we continue on this path. In particular we focus on two questions:

1. When is the product of super-isolated varieties super-isolated?
2. When does a super-isolated variety admit a principal polarization and, if that is the case, how many are there up to polarized isomorphism?

In [18] it is shown that simple super-isolated abelian varieties are rare, in the sense that for most finite fields $F_q$ there are no super-isolated varieties over $F_q$. Trying to generalize this statement to non-simple abelian varieties leads to the first question. Our methods show that super-isolated products are even rarer and can be enumerated as efficiently as super-isolated simple varieties.

The second question is related to the problem of determining whether an abelian variety is the Jacobian of a curve. This is in general a difficult question, see [14] for the case of abelian surfaces. In the case of super-isolated abelian varieties all the arithmetic information is encoded in the Weil polynomial determining the isogeny class. Since every Jacobian admits
a canonical principal polarization, the second question is a first step towards characterizing super-isolated Jacobians.

In this paper, we first present some general results about products of super-isolated abelian varieties, see Sect. 3.1. Then, in order to give answers to our questions, we focus on a class of abelian varieties that we call ideal, see Definition 14. For the category of such abelian varieties, we have functorial descriptions in terms of finitely generated free $\mathbb{Z}$-modules with a “Frobenius-like” endomorphism, see [3,4]. In the ordinary case, we can describe also dual varieties and polarizations, see [8]. We exploit these descriptions in Theorem 16 where we exhibit a criterion to answer Question 1. It turns out that the technology developed to prove Theorem 16 in Sects. 2 and 3 allows us to show that, for any fixed dimension, there are only finitely many super-isolated ideal abelian varieties that are not simple, see Corollary 19. In Sect. 3.3 we give an algorithm to enumerate them and we produce complete lists of such abelian varieties that are a product of elliptic curves and surfaces, see Algorithm 1 and Table 1.

In Sect. 4, we characterize which simple ordinary super-isolated varieties admit a principal polarization, see Theorem 27. We also show that if such a polarization exists, then it is unique, see Theorem 35. Moreover in Corollary 36 and Remark 37 we discuss the product case. These results give an answer to Question 2.

In Sect. 5 we apply the theory developed in the previous sections to prove some properties of super-isolated Jacobians, see Proposition 38.

In this paper, all morphisms between abelian varieties over a field $k$ are defined over the same field $k$.

2 Products of Weil generators

Weil generators in CM fields have been studied in [18,19]. They represent the Frobenius endomorphism of a super-isolated abelian variety. The purpose of this section is to generalize the notion of a Weil generator to a product of CM fields and give quantitative results. For a CM field $K$ we will denote its CM involution by $\overline{\cdot}$.

**Definition 1** Let $K$ be a product of CM fields $K = K_1 \times \cdots \times K_n$. We say $\alpha \in K$ is a Weil generator for $K$ if $\alpha \overline{\alpha} \in \mathbb{Z}$ and $O_K = \mathbb{Z}[\alpha, \overline{\alpha}]$, where $O_K = \prod O_{K_i}$. That is, $\alpha \overline{\alpha}$ lies in the image of the diagonal embedding $\mathbb{Z} \to K$, and the subring generated by $\alpha$ and $\overline{\alpha}$ is the integral closure of $\mathbb{Z}$ in $K$.

Let $K$ be a CM-field. Denote by $F$ the fixed field of the CM involution of $K$. Fix $\gamma \in K$ satisfying $O_K = O_F[\gamma]$. Let $R$ be the set of all $\eta \in F$ such that $O_F = \mathbb{Z}[\eta]$. Choose a set $T \subset R$ of representatives of $R/ \sim$, where $\eta_1 \sim \eta_2$ if $\eta_1 - \eta_2 \in \mathbb{Z}$. If $\gamma$ does not exist or $T = \emptyset$, then $K$ has no Weil generators. Indeed, if $\alpha$ is a Weil generator for $K$ then we could choose $\gamma = \alpha$ and $(\alpha + \overline{\alpha}) \in R$, see [19, Lemma 3.13]. Given the order $O_F$, the set $T$ is always finite and can be effectively computed, see [5]. By [19, Lemma 3.15] every Weil generator $\alpha \in K$ can be written as

$$\alpha = u(\gamma - \overline{\gamma}) + \eta + a$$

for a unique triple $(u, \eta, a) \in O_F^\times \times T \times \mathbb{Z}$.

**Example 2** Let $K = \mathbb{Q}(i)$ and put $\gamma = i$ and $T = \{0\}$. Then every Weil generator is of the form $(\pm 2i + a)/2$ for some integer $a \in \mathbb{Z}$. Alternatively, every Weil generator can also be written as $b \pm i$ for some $b \in \mathbb{Z}$.
Example 3 Let $K = \mathbb{Q}(\xi)$ and put $\gamma = \xi$ and $T = \{(1 + \sqrt{5})/2, (1 - \sqrt{5})/2\}$. Then every generator can be expressed as $(u(\xi - \bar{\xi}) + (1 \pm \sqrt{5})/2 + a)/2$ for some $u \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}^\times$ and $a \in \mathbb{Z}$.

Lemma 4 Let $K$ be a CM field with maximal real subfield $F$, and $\alpha \in K$ a Weil generator of $K$. Fix $\eta \in T$ and $a \in \mathbb{Z}$ as in Eq. (1). If $q = \alpha \bar{\alpha}$, then
\[
\text{Norm}_{F/Q}((\eta + a)^2 - 4q) = \frac{\text{Disc}_{K/Q}(\alpha)}{\text{Disc}_{F/Q}^2}.
\]

**Proof** Let $g = \deg F$ and $\beta = \alpha + \bar{\alpha}$. By [11, Ch.2 Ex. 23],
\[
\text{Disc}_{K/Q}(1, \ldots, \beta g^{-1}, \alpha, \ldots, \alpha \beta g^{-1}) = \text{Disc}_{F/Q}(\beta)^2 \text{Norm}_{F/Q} \text{Disc}_{K/F}(\alpha).
\]
But $\{1, \alpha\}$ is a $\mathcal{O}_F$-basis for $\mathcal{O}_K$ and $\{1, \beta, \ldots, \beta g^{-1}\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_F$, so this reduces to
\[
\text{Disc}_{K} = \text{Disc}_{F}^2 \text{Norm}_{F/Q} \text{Disc}_{K/F}(\alpha).\]
The result follows because
\[
\text{Disc}_{K/F}(\alpha) = \text{det} \begin{pmatrix} \text{Trace}_{K/F}(1) & \text{Trace}_{K/F}(\alpha) \\ \text{Trace}_{K/F}(\alpha) & \text{Trace}_{K/F}(\alpha^2) \end{pmatrix} = (\alpha - \bar{\alpha})^2 = (\eta + a)^2 - 4q.
\]

The expression in Lemma 4 can be viewed as the equation of a plane curve by replacing $a$ and $4q$ with formal variables. Lemma 5 below together with the substitutions
\[
\text{Norm}_{F/Q}((\eta + a)^2 - 4q) = \prod_{\sigma:F \rightarrow \mathbb{C}} (a + \sigma(\eta))^2 - 4q
\]
and $t = -\text{Disc}_K / \text{Disc}_{F}^2$ shows that this curve is geometrically irreducible.

Lemma 5 Let $t, a_1, \ldots, a_n \in \mathbb{C}$ and
\[
P(x, y) = \prod_{i=1}^n ((x - a_i)^2 - y) + t.
\]
If the $a_i$ are distinct and $t \neq 0$, then $P(x, y)$ is irreducible.

**Proof** Suppose that $P(x, y) = h(x, y)g(x, y)$ and that $h(x, y)$ is non-constant. Let $L_i(x, y) = (x - a_i)^2 - y$ so that $P(x, y) = \prod_{i=1}^n L_i(x, y) + t$. For any point $Q$ with $L_i(Q) = 0$, we have $P(Q) = t$. Hence $h(x, (x - a_i)^2 - y)$ must be constant, say $c_i$. Because $L_i$ and $L_j$ both vanish at $((a_i + a_j)/2, ((a_i - a_j)/2)^2)$, it follows that $c_1 = c_2 = \cdots = c_n$. Let $c$ denote this value. Since $h(x, y) - c$ is zero whenever $L_i(x, y)$ is, it follows that $L_i(x, y)$ divides $h(x, y) - c$ for every $i = 1, \ldots, n$. As the $L_i(x, y)$ are distinct and irreducible, we must have that their product also divides $h(x, y) - c$. But $h(x, y)$ is non-constant, so $h(x, y) - c \neq 0$ and therefore $\deg h(x, y) = \deg P(x, y)$. It follows that $g(x, y)$ is constant.

Proposition 6 Let $K = K_1 \times \cdots \times K_n$ be a product of CM fields. For $i = 1, \ldots, n$ pick an algebraic integer $\alpha_i \in \mathcal{O}_{K_i}$ and put $\alpha = (\alpha_1, \ldots, \alpha_n)$. For each $i$ denote by $g_i(x) \in \mathbb{Z}[x]$ the minimal polynomial of $\alpha_i + \bar{\alpha}_i$. Then $\mathbb{Z}[\alpha, \bar{\alpha}] = \prod \mathbb{Z}[\alpha_i, \bar{\alpha}_i]$ if and only if $|\text{Res}(g_i, g_j)| = 1$ for all $i \neq j$. 

© Springer
Proof First we will show that $\mathbb{Z}[\alpha, \bar{\alpha}] = \prod_i \mathbb{Z}[\alpha_i, \bar{\alpha}_i]$ if and only if $\mathbb{Z}[\alpha + \bar{\alpha}] = \prod_i \mathbb{Z}[\alpha_i + \bar{\alpha}_i]$. Let $e_i$ be the $i$-th orthogonal idempotent of $K = \prod_i K_i$. Observe that $\mathbb{Z}[\alpha + \bar{\alpha}]$ is the subset of $\mathbb{Z}[\alpha, \bar{\alpha}]$ that is fixed by complex conjugation. Moreover, for every $i = 1, \ldots, n$, we have $e_i = \bar{e}_i$. The claim follows from the following chain of equivalences: we have $\mathbb{Z}[\alpha, \bar{\alpha}] = \prod_i \mathbb{Z}[\alpha_i, \bar{\alpha}_i]$ if and only if $e_i \in \mathbb{Z}[\alpha_i, \bar{\alpha}_i]$ for all $i = 1, \ldots, n$ if and only if $e_i \in \mathbb{Z}[\alpha + \bar{\alpha}]$ for all $i = 1, \ldots, n$ if and only if $\mathbb{Z}[\alpha + \bar{\alpha}] = \prod_i \mathbb{Z}[\alpha_i + \bar{\alpha}_i]$.

Next we claim that $\mathbb{Z}[\alpha + \bar{\alpha}] = \prod_i \mathbb{Z}[\alpha_i + \bar{\alpha}_i]$ if and only if $|\text{Res}(g_i, g_j)| = 1$ for all $i \neq j$. The map $\mathbb{Z}[x] \to \mathbb{Z}[\alpha + \bar{\alpha}]$ sending $x$ to $\alpha + \bar{\alpha}$ is surjective. Therefore, it is equivalent to show that $\mathbb{Z}[x]/\text{lcm}(g_i) \cong \prod_i \mathbb{Z}[x]/g_i$ if and only if $|\text{Res}(g_i, g_j)| = 1$. The former holds if and only if the ideals $g_i\mathbb{Z}[x]$ are coprime. By [24, Lem. 11.3] (see also [16, p. 420] for a slightly stronger version), this holds if and only if the pairwise resultants of the $g_i$ are units. □

Corollary 7 Let $K = K_1 \times \cdots \times K_n$ be a product of CM fields. Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in K$, and $g_i$ be the minimal polynomial for $\alpha_i + \bar{\alpha}_i$. Then $\alpha$ is a Weil generator for $K$ if and only if each $\alpha_i$ is a Weil generator for $K_i$, $\alpha_i\bar{\alpha}_i = \cdots = \alpha_n\bar{\alpha}_n$, and $|\text{Res}(g_i, g_j)| = 1$ for all $i \neq j$.

Proof Suppose that $\alpha$ is a Weil generator for $K$. Then $\alpha_1\bar{\alpha}_1 = \cdots = \alpha_n\bar{\alpha}_n \in \mathbb{Z}$. Moreover, $\mathcal{O}_K = \mathbb{Z}[\alpha, \bar{\alpha}]$. Because $\mathcal{O}_K = \prod_i \mathcal{O}_{K_i}$, it follows that $\mathcal{O}_{K_i} = \mathbb{Z}[\alpha_i, \bar{\alpha}_i]$ for all $i$. So the resultant condition in the statement follows from Proposition 6.

Suppose that the latter conditions hold. By Proposition 6, we have $\mathbb{Z}[\alpha, \bar{\alpha}] = \prod_i \mathbb{Z}[\alpha_i, \bar{\alpha}_i] = \prod_i \mathcal{O}_{K_i} = \mathcal{O}_K$. Since $\alpha_i\bar{\alpha}_i$ is the same for each $i$, we also have that $\alpha \bar{\alpha}$ lies in the diagonal $\mathbb{Z} \to K$. Therefore $\alpha$ is a Weil generator for $K$. □

Example 8 In Corollary 7, both the condition that $|\text{Res}(g_i, g_j)| = 1$ for all $i \neq j$, and the condition that $\alpha_1\bar{\alpha}_1 = \cdots = \alpha_n\bar{\alpha}_n$ are necessary. To see this, let $K_1 = \mathbb{Q}(\sqrt{-11})$ and $K_2 = \mathbb{Q}(\sqrt{-19})$. Then $\alpha_1 = (3 - \sqrt{-11})/2$ and $\alpha_2 = (1 - \sqrt{-19})/2$ are Weil generators with norm 5 for $K_1$ and $K_2$ respectively. However, $|\text{Res}(g_1, g_2)| = |\text{Res}(x - 3, x - 1)| = 2$. Therefore the ring $\mathbb{Z}[(\alpha_1, \alpha_2), (\bar{\alpha}_1, \bar{\alpha}_2)] \neq \mathcal{O}_{K_1 \times K_2}$, so $(\alpha_1, \alpha_2)$ is not a Weil generator for $K_1 \times K_2$.

If we instead set $K_2 = \mathbb{Q}(\sqrt{-13})$ and $\alpha_2 = 2 - i\sqrt{13}$ then $|\text{Res}(g_1, g_2)| = |\text{Res}(x - 3, x - 4)| = 1$ but $\text{Norm}(\alpha_2) = 17$. So in this case, $(\alpha_1, \alpha_2)$ is not a Weil generator because its norm does not lie in the diagonal embedding $\mathbb{Z} \to K_1 \times K_2$.

Lemma 9 Let $K_1$ and $K_2$ be CM fields. Then there are finitely many Weil generators in $K_1 \times K_2$.

Proof For $i = 1, 2$, choose $\gamma_i$ and $T_i$ for $K_i$ as in the beginning of Sect. 2. If for some $i$, $\gamma_i$ does not exist or $T_i = \emptyset$, then $K_i$ does not have any Weil generators and we are done. So we will assume that $\gamma_1, \gamma_2$ exist and both $T_1$ and $T_2$ are nonempty. Now we may write any Weil generator $\alpha_i$ in $K_i$ as in Eq. (1), that is, there is a unique triple $(u_i, \eta_i, a_i) \in \mathcal{O}_{K_i}^\times \times T_i \times \mathbb{Z}$ such that

\[\alpha_i = \frac{u_i (\gamma_i - \bar{\gamma}_i) + \eta_i + a_i}{2} \]
For each pair \((\eta_1, \eta_2)\) \(\in T_1 \times T_2\), let \(X_{\eta_1, \eta_2}\) denote the affine variety cut out by the following equations in \(\mathbb{Q}[x_1, x_2, y]\):

\[
\prod_{\sigma: F_1 \rightarrow C} ((\sigma(\eta_1) + x_1) - 4y) = \frac{\text{Disc}_{F_1} K_1}{\text{Disc}_{F_1}^2}.
\]

(2)

\[
\prod_{\tau: F_2 \rightarrow C} ((\tau(\eta_2) + x_2) - 4y) = \frac{\text{Disc}_{K_2}}{\text{Disc}_{F_2}^2}.
\]

(3)

\[
\prod_{\sigma: F_1 \rightarrow C \atop \tau: F_2 \rightarrow C} ((\sigma(\eta_1) + x_1) - (\tau(\eta_2) + x_2))^2 = 1.
\]

(4)

By [5] the sets \(T_i\) are finite, so there are a finite number of the \(X_{\eta_1, \eta_2}\). Let \(\mathcal{X}\) denote their union.

We will now construct a finite-to-one map \(\psi\) from Weil generators of \(K_1 \times K_2\) to \(\mathcal{X}(\mathbb{Z})\). Let \((\alpha_1, \alpha_2)\) be a Weil generator in \(K_1 \times K_2\). Then \(\alpha_i\) corresponds to a unique triple \((u_i, \eta_i, a_i)\) \(\in \mathcal{O}_{F_i}^\times \times T_i \times \mathbb{Z}\). Let \(q = \alpha_1\alpha_1 = \alpha_2\alpha_2\). Define \(\psi\) by sending \((\alpha_1, \alpha_2) \mapsto (a_1, a_2, q)\). The image of \(\psi\) satisfies Eqs. (2) and (3) by Lemma 4, and Eq. (4) by Corollary 7. Next we will show that \(\psi\) is finite-to-one. It suffices to show that for a given \(a_i, q\) in \(\mathbb{Z}\), there are finitely many \(u_i \in \mathcal{O}_{F_i}^\times\) and \(\eta_i \in T_i\) such that \(\alpha_i = (u_i(\gamma_i - \overline{\gamma}_i) + \eta_i + a_i)/2\) is a Weil generator for \(K_i\) with \(a_i\overline{\alpha}_i = q\). Every such Weil generator satisfies \(4a_i\overline{a}_i = 4q = \text{Norm}_{K_i/F_i}(\gamma_i - \overline{\gamma}_i) + (\eta_i + a_i)^2\). In particular, \(u_i\) is determined up to sign by \(a_i, q\), and \(\eta_i\). Since \(T_i\) is finite, there are only finitely many possible \(\eta_i\). Hence there are only finitely many possible \(u_i\) as well.

It suffices to show that each component \(X_{\eta_1, \eta_2}\) has dimension 0, as this implies that \(\mathcal{X}(\mathbb{Z})\) is finite. Let \((\eta_1, \eta_2)\) \(\in T_1 \times T_2\), and let \(X = X_{\eta_1, \eta_2}\). Notice that Eq. (4) is a polynomial equation in \(x_1 - x_2\). Therefore there are complex numbers \(\beta_k\) for \(k = 1, \ldots, \tilde{k}\), with \(\tilde{k} = 2[K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]\), such that

\[
\prod_{\sigma: F_1 \rightarrow C \atop \tau: F_2 \rightarrow C} (x_1 - x_2 + \sigma(\eta_1) - \tau(\eta_2))^2 - 1 = \prod_{k=1}^{\tilde{k}} (x_1 - x_2 - \beta_k).
\]

Hence we can write \(X\) as a union of subvarieties \(X_k\), for \(k = 1, \ldots, \tilde{k}\), where \(X_k\) is the intersection of the geometrically irreducible surfaces (see Lemma 5) defined by Eqs. (2) and (3) and by

\[x_1 - x_2 - \beta_k = 0.\]

In particular we can eliminate \(x_2\) and describe \(X_k\) as the intersection of the two irreducible plane curves

\[
\prod_{\sigma: F_1 \rightarrow C} ((\sigma(\eta_1) + x_1) - 4y) = \frac{\text{Disc}_{F_1} K_1}{\text{Disc}_{F_1}^2} = 0,
\]

(6)

\[
\prod_{\tau: F_2 \rightarrow C} ((\tau(\eta_2) + x_1 - \beta_k) - 4y) = \frac{\text{Disc}_{K_2}}{\text{Disc}_{F_2}^2} = 0.
\]

(7)

By Bézout’s theorem, the intersection of two geometrically irreducible plane curves has dimension 0 as long as the curves are distinct. So it is sufficient to show that the polynomials in Eqs. (6) and (7) are not proportional. We will prove this by contradiction.
Suppose that the two polynomials in Eqs. (6) and (7) are proportional. By comparing the highest degree monomial in \( y \) we must have that Eqs. (6) and (7) are equal. Note that this also implies \([K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}]\). Setting \( x_1 = -(\sigma(\eta_1) + \tau(\eta_2) - \beta_k)/2 \) and \( y = (\sigma(\eta_1) + x_1)^2/4 \) for any choice of \( \sigma \) and \( \tau \) will zero out the products in Eqs. (6) and (7), which shows that \( \text{Disc}_{K_1}/\text{Disc}_{K_1}^2 = \text{Disc}_{K_2}/\text{Disc}_{K_2}^2 \). Setting \( y = 0 \) leads to

\[
\prod_{\sigma : F_1 \to \mathbb{C}} (\sigma(\eta_1) + x_1)^2 = \prod_{\tau : F_2 \to \mathbb{C}} (\tau(\eta_2) + x_1 - \beta_k)^2.
\]

By comparing the zeros we see that, for each \( k \), there is a bijection \( \sigma \mapsto \tau_{\sigma,k} \) such that \( \sigma(\eta_1) = \tau_{\sigma,k}(\eta_2) - \beta_k \). Fix a \( 1 \leq k_0 \leq k \) substituting \( \sigma(\eta_1) = \tau_{\sigma,k_0}(\eta_2) - \beta_{k_0} \) and \( x_2 = x_1 - \beta_{k_0} \) in Eq. (5) yields

\[
\prod_{k=1}^{k_0} (x_1 - (x_1 - \beta_{k_0}) - \beta_k)^2 = \left( \prod_{\sigma, \tau} x_1 - (x_1 - \beta_{k_0}) + \tau_{\sigma,k_0}(\eta_2) - \beta_{k_0} - \tau(\eta_2) \right)^2 - 1
\]

\[
0 = \left( \prod_{\sigma, \tau} (\tau_{\sigma,k}(\eta_2) - \tau(\eta_2))^2 \right) - 1
\]

Since the product is taken over all embeddings \( \sigma \) (and \( \tau \)) we have that the right hand side is equal to \(-1\), which is a contradiction. \( \square \)

**Theorem 10** Let \( K = K_1 \times \cdots \times K_n \) be a product of CM fields. If \( n > 1 \) then \( K \) has finitely many Weil generators.

**Proof** This follows directly from Lemma 9 and the fact that every Weil generator for \( K \) projects to a Weil generator for each product \( K_i \times K_j \), with \( i \neq j \). \( \square \)

### 3 Products of super-isolated varieties

In this section, we study products of super-isolated abelian varieties. Recall that the Weil polynomial \( h \) of a \( d \)-dimensional abelian variety \( A/\mathbb{F}_q \) is defined as the characteristic polynomial of the Frobenius endomorphism of \( A \). The polynomial \( h \) lies in \( \mathbb{Z}[x] \), it has degree \( 2d \) and all its complex roots have absolute value \( \sqrt{q} \). Also we define the real Weil polynomial of \( A \) the unique polynomial \( g \) in \( \mathbb{Z}[x] \) such that \( h(x) = x^d g(x + q/x) \). In particular if \( h \) is irreducible and \( \pi \) is a root of \( h \), then \( g \) is the minimal polynomial of \( \pi + q/\pi \).

#### 3.1 Glueing exponent and super isolated abelian varieties

**Lemma 11** Let \( A_1 \) and \( A_2 \) be abelian varieties over a finite field \( \mathbb{F}_q \). Assume that \( A_1 \) and \( A_2 \) have no isogeny factor in common. If the product \( A_1 \times A_2 \) is super-isolated, then both \( A_1 \) and \( A_2 \) are super-isolated.

**Proof** Let \( B_1 \) and \( B_2 \) be abelian varieties isogenous to \( A_1 \) and \( A_2 \), respectively. Since \( A_1 \times A_2 \) is super-isolated then there exists an isomorphism \( \varphi : A_1 \times A_2 \to B_1 \times B_2 \). Observe that

\[
\text{Hom}_{\mathbb{F}_q}(A_1 \times A_2, B_1 \times B_2) = \text{Hom}_{\mathbb{F}_q}(A_1, B_1) \times \text{Hom}_{\mathbb{F}_q}(A_2, B_2),
\]

because \( A_1 \) and \( A_2 \) have no isogeny factor in common. Hence there are isomorphisms \( \varphi_1 : A_1 \to B_1 \) and \( \varphi_2 : A_2 \to B_2 \) such that \( \varphi = \varphi_1 \times \varphi_2 \). In particular \( A_1 \) and \( A_2 \) are super-isolated. \( \square \)
**Definition 12** (cf. [6, Def. 2.1]) Let $A_1$ and $A_2$ be abelian varieties over $\mathbb{F}_q$. The **glueing exponent** $e(A_1, A_2)$ of $A_1$ and $A_2$ is the greatest common divisor of the exponent of $\Delta$, where $\Delta$ ranges over all finite group schemes that embed in both a variety isogenous to $A_1$ and a variety isogenous to $A_2$.

**Lemma 13** Let $A_1$ and $A_2$ be abelian varieties over a finite field $\mathbb{F}_q$. If $A_1$ and $A_2$ are super-isolated and $e(A_1, A_2) = 1$ then the product $A_1 \times A_2$ is super-isolated.

**Proof** It is a direct application of [6, Lemma 2.3].

Observe that $A_1$ and $A_2$ have no isogeny factor in common if and only if $e(A_1, A_2) < \infty$. See also [6, after Def. 2.1]. In view of this consideration, Lemmas 11 and 13 allow us to understand super-isolated products in terms of the glueing exponent. In general the glueing exponent is tricky to compute. Nevertheless one can use [6, Prop.2.8] to show that for abelian varieties $A$ and $B$ over $\mathbb{F}_q$ with no isogeny factor in common the glueing exponent divides the resultant of the radicals of the real Weil polynomials $g_A$ and $g_B$ of $A$ and $B$. In particular if such a resultant is 1 then also $e(A, B) = 1$. In particular Corollary 7 can be considered as a reformulation in terms of Weil generators (restricted to ideal abelian varieties, see Definition 14 below) of Lemma 13.

In what follows we will use a different strategy: We will restrict ourselves to a subcategory of abelian varieties and give conditions for them (and their products) to be super-isolated in terms of Weil generators. The upshot of this approach is that it is more computationally friendly, since Weil generators can be enumerated. Moreover, in such a subcategory, we will be able to study powers of super-isolated abelian varieties.

### 3.2 Weil generators and super isolated abelian varieties

From now on we will focus on squarefree varieties. That is, abelian varieties whose Weil polynomial is squarefree. Our main tool is the equivalence of categories between certain abelian varieties $A/\mathbb{F}_q$ and $\mathbb{Z}$-modules with extra structure.

**Definition 14** Let $A/\mathbb{F}_q$ be an abelian variety, and let $h$ denote its Weil polynomial. Let $p$ be the characteristic of $\mathbb{F}_q$. Then $A$ is **ideal** if the following holds:

1. the polynomial $h$ factors into distinct irreducible factors.
2. the polynomial $h$ has no real roots.
3. the polynomial $h$ is ordinary (meaning half of the roots of $h$ are $p$-adic units) or $q$ is prime.

Suppose that $A/\mathbb{F}_q$ is ideal. Then there is an isogeny

$$A \sim A_1 \times \cdots \times A_n,$$

where the $A_i$ are simple and pairwise non-isogenous abelian varieties. By Honda–Tate theory, see [7] and [22], the Weil polynomial factors into $h = h_1 \cdots h_n$, where $h_i$ is the Weil polynomial of $A_i$. Because of the ordinary condition (or the condition that $q$ is prime), the polynomials $h_i$ are irreducible. In particular, if we let $\pi_i$ denote a root of $h_i$ and put $K_i = \mathbb{Q}(\pi_i)$, then $K_i$ is a CM field of degree $2 \dim A_i$. Let $K = \prod K_i$ and consider the subring $\mathbb{Z}[[\pi, \pi]] \subseteq K$ where $\pi = (\pi_1, \ldots, \pi_n)$ and $\pi_i = (\pi_1, \ldots, \pi_n)$ with $\pi_i = q/\pi_i$. We will identify $K$ with $\text{End } A \otimes \mathbb{Q}$. Let $\mathcal{O}_K = \prod \mathcal{O}_{K_i}$, that is, the integral closure of $\mathbb{Z}$ in $K$. Note that $\mathcal{O}_K$ and $\mathbb{Z}[\pi, \pi]$ are free finitely generated $\mathbb{Z}$-modules of rank $\dim_{\mathbb{Q}}(K)$. In particular we have a finite-index inclusion $\mathbb{Z}[\pi, \pi] \subseteq \mathcal{O}_K$ and one can show that $\mathbb{Z}[\pi, \pi] \subseteq \text{End } A \subseteq \mathcal{O}_K$. 

\[\text{Springer}\]
By [13, Thm. 4.3] the ideal abelian varieties can be functorially described in terms of fractional \( \mathbb{Z}[\pi, \bar{\pi}] \)-ideals. Such a description builds on the equivalences of categories established in [3,4].

**Theorem 15** If \( A/\mathbb{F}_q \) is ideal and simple, then \( A \) is super-isolated if and only if \( K \) has class number 1 and \( \mathbb{Z}[\pi, \bar{\pi}] = \mathcal{O}_K \). Equivalently, \( A \) is super-isolated if and only if \( \text{Pic}(\mathcal{O}_K) \) is trivial and \( \pi \) is a Weil generator for \( K \).

**Proof** The result for ordinary varieties is given in [19, Thm. 7.4]. The extension to the case where \( q \) is prime is [18, Thm. 16]. \( \square \)

**Theorem 16** If \( A/\mathbb{F}_q \) is ideal, then \( A \) is super-isolated if and only if each \( A_i \) is super-isolated and \( \mathbb{Z}[\pi, \bar{\pi}] = \mathcal{O}_{K_i} \). Equivalently, \( A \) is super-isolated if and only if \( \text{Pic}(\mathcal{O}_{K_i}) \) is trivial and \( \pi \) is a Weil generator for \( K_i \).

**Proof** By [13, Thm. 4.3] we have that \( A \) is super-isolated if and only if \( \mathbb{Z}[\pi, \bar{\pi}] = \mathcal{O}_K \) and \( \text{Pic}(\mathcal{O}_K) \) is trivial. Moreover by Theorem 15 we have that each simple factor \( A_i \) is super-isolated if and only if \( \mathbb{Z}[\pi_i, \bar{\pi}_i] = \mathcal{O}_{K_i} \) and \( \text{Pic}(\mathcal{O}_{K_i}) \) is trivial. The result follows from the equality \( \text{Pic}(\mathcal{O}_K) = \prod \text{Pic}(\mathcal{O}_{K_i}) \).

By using Theorem 16 it is easy to construct super-isolated products of big dimension as shown in the following example.

**Example 17** Consider the polynomials

\[
\begin{align*}
  h_1(x) &= (x^4 - 2x^3 + 3x^2 - 4x + 4), \\
  h_2(x) &= (x^6 - 4x^5 + 9x^4 - 15x^3 + 18x^2 - 16x + 8), \\
  h_3(x) &= (x^6 - 3x^5 + 6x^4 - 9x^3 + 12x^2 - 12x + 8), \\
  h_4(x) &= (x^8 - 5x^7 + 12x^6 - 20x^5 + 29x^4 + 40x^3 + 48x^2 - 40x + 16), \\
  h_5(x) &= (x^8 - 5x^7 + 13x^6 - 25x^5 + 39x^4 - 50x^3 + 52x^2 - 40x + 16), \\
  h_6(x) &= (x^8 - 4x^7 + 5x^6 + 2x^5 - 11x^4 + 4x^3 + 20x^2 - 32x + 16).
\end{align*}
\]

One can check that each factor \( h_i \) determines a Weil generator \( \alpha_i \) for a CM field \( K_i = \mathbb{Q}[x]/h_i \), and that \( (\alpha_1, \ldots, \alpha_6) \) is a Weil generator for the product \( K_1 \times \cdots \times K_6 \). Therefore \( h = \prod_i h_i \) is the Weil polynomial for a 20-dimensional super-isolated variety over \( \mathbb{F}_2 \).

**Example 18** Let \( A/\mathbb{F}_5 \) be the product of the elliptic curves \( E_1 : y^2 = x^3 + 4x + 2 \) and \( E_2 : y^2 = x^3 + 3x + 2 \). The Weil polynomials of \( E_1 \) and \( E_2 \) are \( h_1 = x^2 - 3x + 5 \) and \( h_2 = x^2 - x + 5 \), respectively. Using Corollary 7 and Theorem 16, it is straightforward to check that \( E_1 \) and \( E_2 \) are super-isolated, but \( A \) is not, see also Example 8. Therefore \( A \) must be isogeneous, but not isomorphic, to some other abelian surface over \( \mathbb{F}_5 \). One way to verify this claim is to observe that \( \mathbb{Z}[\pi, \bar{\pi}] \not\subseteq \mathcal{O}_K = \mathbb{Z}[\pi_1] \times \mathbb{Z}[\pi_2] = \text{End}_{\mathbb{F}_5}(A) \). By [13, Thm. 4.3] we have that there exists an abelian variety \( A' \) isogenous to \( A \) with \( \text{End}_{\mathbb{F}_5}(A') = \mathbb{Z}[\pi, \bar{\pi}] \). In particular \( A \) is not isomorphic to \( A' \). More precisely, since \( \mathcal{O}_K \) is the unique order of \( \mathbb{Z}[\pi, \bar{\pi}] \) and \( \text{Pic}(\mathbb{Z}[\pi, \bar{\pi}]) \simeq \mathbb{Z}/2\mathbb{Z} \), by using [13, Thm. 4.3] we can conclude that the isogeny class of \( A \) contains exactly 4 isomorphism classes of abelian varieties, 3 of which have endomorphism ring \( \mathbb{Z}[\pi, \bar{\pi}] \).

**Corollary 19** Let \( g \) be a positive integer. There are only finitely many ideal super-isolated abelian varieties of dimension \( g \) that are not simple. In particular, there are only finitely many finite fields \( \mathbb{F}_q \) for which such a variety may exist.
Proof By Theorem 16 it is sufficient to count Weil generators in products of CM fields with class number 1. In [20, Thm. 2, p. 136], Stark showed that for any fixed degree, there are finitely many CM fields with class number 1 with that degree. Hence there are finitely many products $K_1 \times \cdots \times K_n$ with $\sum \deg K_i = 2g$ such that each $K_i$ is a CM field with class number 1. By Theorem 10, any such product of fields contains only finitely many Weil generators.

\[ \square \]

3.3 Products of super-isolated elliptic curves and abelian surfaces

In this section we outline a general strategy to enumerate certain products of super-isolated varieties.

Algorithm 1 Enumerate Weil Generators

Require: A product $K$ of CM fields $K_1$ and $K_2$, with maximal totally real subfields $F_1$ and $F_2$, respectively.

Ensure: All Weil generators for $K$.

1: $F \leftarrow F_1 \times F_2$
2: Find $\gamma_i$ such that $\mathcal{O}_K = \mathcal{O}_F[\gamma_i]$
3: $T_i \leftarrow$ a complete set of $\eta_j \in F_i$ such that $\mathcal{O}_{F_i} = \mathbb{Z}[\eta_j]$ up to integer translation
4: for all $(\eta_1, \eta_2) \in T_1 \times T_2$ do
5: $X_{\eta_1, \eta_2} \leftarrow$ the variety defined in the proof of Lemma 9
6: for all $P \in X_{\eta_1, \eta_2}(\mathbb{Q})$ do
7: for all $u_i \in \mathcal{O}_{F_i}$ with $u_i^2 \operatorname{Norm}_{K/F}(\gamma_i - \overline{\gamma}_i) + (\eta_i + P_{x_i})^2 = 4P_y$ do
8: $\alpha_i \leftarrow (u_i(\gamma_i - \overline{\gamma}_i) + \eta_i + P_{x_i})/2$
9: if $\alpha_1 \in \mathcal{O}_{K_1}$ and $\alpha_2 \in \mathcal{O}_{K_2}$ then
10: print $(\alpha_1, \alpha_2)$
11: end if
12: end for
13: end for
14: end for

Proposition 20 Let $K$ be a product of CM fields $K_1$ and $K_2$, with maximal totally real subfields $F_1$ and $F_2$, respectively. Algorithm 1 exactly outputs all Weil generators for $K_1 \times K_2$.

Proof As seen in the proof of Lemma 9, every Weil generator $(\alpha_1, \alpha_2)$ of $K$ corresponds to a rational point on one of the varieties $X_{\eta_1, \eta_2}$ for some $\eta_1, \eta_2 \in T_1 \times T_2$. The algorithm ranges over all rational points on all such varieties and finds all possible pairs $(\alpha_1, \alpha_2)$ which could be Weil generators. This means that the output will include all Weil generators.

It remains to show that everything the algorithm outputs is a Weil generator for $K_1 \times K_2$. Suppose that the algorithm outputs $(\alpha_1, \alpha_2)$ from a point on $X_{\eta_1, \eta_2}$ for some $(\eta_1, \eta_2) \in T_1 \times T_2$. It is straightforward to check that if $\alpha_i \in \mathcal{O}_{K_i}$ then it is indeed a Weil generator for $K_i$ using [19, Lem. 3.13]. By construction of $X_{\eta_1, \eta_2}$, it follows that $(\alpha_1, \alpha_2)$ satisfies the resultant condition in Corollary 7. Therefore $(\alpha_1, \alpha_2)$ is a Weil generator for $K_1 \times K_2$.

Remark 21 Algorithm 1 can be extended to arbitrary products $K_1 \times \cdots \times K_n$ in a straightforward way: First compute the set $W_{i,j}$ of all Weil generators in the sub-product $K_i \times K_j$ for all $1 \leq i, j \leq n$. Then search for tuples $(\alpha_1, \ldots, \alpha_n)$ with $(\alpha_i, \alpha_j) \in W_{i,j}$ for all $1 \leq i, j \leq n$.

Using Tables of CM fields of degree 2 and 4 with class number one, we can enumerate all ideal superisolated abelian varieties that factor into products of elliptic curves and surfaces.
Table 1 The number of ideal super-isolated products of elliptic curves and abelian surfaces over each finite field $\mathbb{F}_q$

| $q$ | $1 \times 1$ | $1 \times 2$ | $1 \times 1 \times 2$ | $1 \times 2 \times 2$ | $2 \times 2$ |
|-----|--------------|--------------|----------------------|---------------------|-------------|
| 2   | 4            | 24           | 10                   | 12                  | 18          |
| 3   | 4            | 24           | 6                    | 12                  | 18          |
| 4   | 2            |              |                      |                     |             |
| 5   | 2            | 12           |                      | 2                   | 6           |
| 7   |              | 8            |                      |                     |             |
| 8   | 2            |              |                      |                     |             |
| 9   | 2            |              |                      |                     |             |
| 11  | 2            | 8            | 2                    | 4                   | 4           |
| 13  |              | 6            |                      |                     |             |
| 17  | 2            | 8            | 2                    |                     |             |
| 19  |              |              |                      |                     | 2           |
| 32  |              | 2            |                      |                     |             |
| 41  |              | 2            |                      |                     |             |
| 47  |              | 4            |                      |                     |             |
| 59  |              | 2            |                      |                     |             |
| 61  |              | 2            |                      |                     |             |
| 83  | 2            |              |                      |                     |             |
| 101 |              | 2            |                      |                     |             |
| 173 |              | 2            |                      |                     |             |
| 227 | 2            |              |                      |                     |             |
| 257 | 2            |              |                      |                     |             |
| 283 |              | 2            |                      |                     |             |
| 383 |              | 2            |                      |                     |             |
| 1523| 2            |              |                      |                     |             |
| 1601| 2            |              |                      |                     |             |
| 18131|             |              |                      |                     | 2           |

Each column represents a decomposition type, so for example $1 \times 1$ represents the product of two non-isogenous elliptic curves. If the cell is empty, it means there is no super-isolated abelian variety over $\mathbb{F}_q$ with the prescribed decomposition type.

**Corollary 22** There are 240 ideal super-isolated abelian varieties that factor into a product of curves and surfaces. A summary of some of their characteristics are given in Table 1.  

**Proof** We implemented Algorithm 1 in Sage and found all ideal super-isolated abelian varieties that decompose into a product of curves and surfaces. This was done by first finding a complete list of CM fields with class number 1 and degree $\leq 4$ (see [19, Tbl. 3] for references). For each pair $K_i, K_j$ of such fields, we computed the set of Weil generators $W_{i,j}$ in $K_i \times K_j$. We filtered the Weil generators whose minimal polynomials satisfy the conditions in Definition 14, as these correspond to simple ideal varieties. Next we organized the data into a graph $\mathcal{G}$ as follows. The vertex set of $\mathcal{G}$ is given by all Weil generators appearing as part of a pair in some $W_{i,j}$. We add an edge between $\alpha_1$ and $\alpha_2$ if $(\alpha_1, \alpha_2) \in W_{i,j}$ for some $i, j$. That is, the edge set of $\mathcal{G}$ is the union of the $W_{i,j}$. Finally, we used standard methods to enumerate all complete subgraphs (cliques) of size $\geq 2$ in $\mathcal{G}$. \[\square\]

**Remark 23** Observe that by [19, Cor. 7.6], for every fixed dimension $g > 2$ we have only finitely many (ordinary) super-isolated abelian varieties. This was shown by mapping Weil

1 The raw data collected and source code can be found at https://github.com/tscholl2/siav-polarizations-products.

Springer
generators to integral points on degree $g$ plane curves. Given a way to enumerate the integral points on such a curve, it is straightforward to enumerate super-isolated abelian varieties of dimension $g$. However, computing integral points on high degree curves (which often have high genus) is a difficult problem. If instead we restrict to enumerating non-trivial products of super-isolated $g$-folds, then Algorithm 1 only requires enumerating points on a dimension $0$ variety (of degree $\approx g^3$). This seems to suggest that finding products of super-isolated varieties is easier than finding singletons.

3.4 Powers of super-isolated abelian varieties

In the case where $A$ is isogenous to a power, we can apply the results from [12] to prove the following Theorem.

**Theorem 24** Let $A/P_q$ be an ideal abelian variety. If $A$ is super-isolated, then $A^n$ is super-isolated for every $n \geq 1$. Conversely, if there exists $n \geq 1$ such that $A^n$ is super-isolated then $A$ is super-isolated.

**Proof** By Theorem 15 we have that $A$ is super-isolated if and only if $K$ has class number 1 and $\mathbb{Z}[\pi, \pi] = \mathcal{O}_K$. By Steinitz theory, see [21], this is equivalent to having a unique isomorphism class of torsion-free $\mathbb{Z}[\pi, \pi]$-modules of rank $n$ (for any $n \geq 1$), which is represented by

$$\mathcal{O}_K^n = \mathcal{O}_K \oplus \ldots \oplus \mathcal{O}_K.$$ 

Using the classification given in [12, Theorem 4.1], one sees that this happens if and only if $A^n$ is super-isolated. $\square$

4 Principal polarizations

In general, (principal) polarizations of abelian varieties in an ordinary square-free isogeny class can be computed up to polarized isomorphisms using [13, Alg. 3]. However, in this section we show that if the isogeny class is super-isolated, then the situation is much simpler. For a CM type $\Phi$ of a CM field $K$ we denote by $N_{\Phi}$ the associated norm, that is,

$$N_{\Phi}(\alpha) = \prod_{\phi \in \Phi} \phi(\alpha),$$

for every $\alpha \in K$.

4.1 Existence of principal polarizations

**Lemma 25** Let $K$ be a CM field of degree $2g$ with maximal totally real subfield $F$. Let $\Phi$ be a CM type of $K$, and $\alpha \in K$ satisfying $\mathcal{O}_K = \mathcal{O}_F[\alpha]$. Then the following statements are equivalent:

1. $K/F$ is unramified at all finite primes.
2. $\alpha - \overline{\alpha} \in \mathcal{O}_K^\times$.
3. $\text{Norm}_{K/Q}(\alpha - \overline{\alpha}) = 1$.
4. $N_{\Phi}(\alpha - \overline{\alpha}) = \pm 1$.

Moreover, if any of the statements holds then $g$ is even.
**Proof** Observe that we have

\[
\text{Norm}_{K/Q}(\alpha - \overline{\alpha}) = N_{\Phi}(\alpha - \overline{\alpha})N_{\Phi}(\overline{\alpha} - \alpha) = (-1)^g N_{\Phi}(\alpha - \overline{\alpha})^2.
\]  

(8)

By [17, Ch. III, Prop. 2.4], \((\alpha - \overline{\alpha})O_K\) is the relative different ideal \(\text{Diff}_{K/F}\). So \(K/F\) is unramified at all finite primes if and only if \(\alpha - \overline{\alpha} \in O_K^\times\). As all norms in CM fields are non-negative, this is equivalent to \(\text{Norm}_{K/Q}(\alpha - \overline{\alpha}) = 1\). Hence we have proved that (1), (2) and (3) are equivalent. Using Eq. (8) we get that (3) is also equivalent to

\[1 = (-1)^g N_{\Phi}(\alpha - \overline{\alpha})^2.\]

If \(K/F\) is unramified at all finite primes, then \(g\) is even by [8, Lem. 10.2] and we get that \(N_{\Phi}(\alpha - \overline{\alpha}) = \pm 1\). Conversely if \(N_{\Phi}(\alpha - \overline{\alpha}) = \pm 1\) then by Eq. (8) we get \(\text{Norm}_{K/Q}(\alpha - \overline{\alpha}) = (-1)^g\). Since norms are positive in CM-fields, we deduce that \(g\) is even and \(K/F\) is unramified. This concludes the proof. \(\square\)

Let \(A/\mathbb{F}_q\) be a simple ordinary super-isolated abelian variety of dimension \(g\). Let \(h\) be the Weil polynomial of \(A\). Put \(K = \mathbb{Q}[x]/h = \mathbb{Q}(\pi)\). Fix an isomorphism \(j : \overline{\mathbb{Q}}_p \simeq \mathbb{C}\) and let \(\Phi\) be the set of embeddings \(\phi : K \rightarrow \mathbb{C}\) such that \(\nu(\phi(\pi)) > 0\), where \(\nu\) is the \(p\)-adic valuation on \(\mathbb{C}\) induced by \(j\). Since \(A\) is ordinary, precisely half of the roots of \(h\) are \(p\)-adic units. Therefore \(\Phi\) is a CM-type of \(K\).

**Lemma 26** The abelian variety \(A\) does not admit a principal polarization if and only if \(N_{\Phi}(\pi - \overline{\pi}) = -1\).

**Proof** Suppose \(A\) does not admit a principal polarization. Then by [8, Cor. 11.4] we have that \(K/F\) is unramified at all finite primes and \(N_{\Phi}(\pi - \overline{\pi}) < 0\). Because \(\pi\) is a Weil generator for \(K\), it follows that \(O_K = O_F[\pi]\) by [19, Lem. 3.13]. So by Lemma 25, we have \(N_{\Phi}(\pi - \overline{\pi}) = -1\).

Conversely, suppose that \(N_{\Phi}(\pi - \overline{\pi}) = -1\). By Lemma 25 it follows that \(K/F\) is unramified at all finite primes, and that \((\pi - \overline{\pi}) \in O_K^\times\). In particular there is no prime of \(F\) dividing \((\pi - \overline{\pi})\) which is inert in \(K/F\). It now follows from [8, Cor. 11.4] that \(A\) does not admit a principal polarization. \(\square\)

**Theorem 27** The abelian variety \(A\) does not admit a principal polarization if and only if \(\text{Norm}_{K/F}(\pi - \overline{\pi}) = 1\) and the middle coefficient \(a_g\) of the Weil polynomial is \(-1\) mod \(q\) if \(q > 2\) and \(-1\) mod 4 if \(q = 2\).

**Proof** By Lemmas 25 and 26, it is enough to show that if \(K/Q\) is unramified at all finite primes, then \(N_{\Phi}(\pi - \overline{\pi}) = -1\) if and only if \(a_g\) satisfies the congruence condition in the statement. By [8, Prop. 11.5], if \(K/F\) is unramified at all finite primes then \(N_{\Phi}(\pi - \overline{\pi}) \equiv a_g \mod q\) if \(q > 2\) and \(N_{\Phi}(\pi - \overline{\pi}) \equiv a_g \mod 4\) if \(q = 2\). As these moduli are enough to distinguish \(\pm 1\), the result follows. \(\square\)

**Example 28** Let \(\pi\) denote a root of \(h(x) = x^8 + x^7 - 3x^6 - x^5 + 7x^4 - 2x^3 - 12x^2 + 8x + 16\). Then \(\pi\) is a Weil generator for the CM field \(K = \mathbb{Q}(\pi)\) of degree 8. So \(\pi\) corresponds to a super-isolated abelian fourfold \(A\) over \(\mathbb{F}_2\). One can check that \(\text{Norm}_{K/Q}(\pi - \overline{\pi}) = 1\). Also, the middle coefficient of \(h(x)\) is \(7 \equiv -1 \mod 4\), so \(A\) does not admit a principal polarization.

**Example 29** We will show that the two conditions in Theorem 27 are independent. Let \(\alpha_1\) denote a root of \(h_1 = x^2 - x + 3\) and \(\alpha_2\) a root of \(h_2 = x^4 - 5x^2 + 9\). Then \(\alpha_1\) and \(\alpha_2\) are Weil generators for the CM fields \(K_i = \mathbb{Q}(\alpha_i)\). Let \(q_i = \alpha_i\overline{\alpha_i}\). One can compute that
Norm$_{K_1/Q}(\alpha_1 - \alpha_1) = 11$ and Norm$_{K_2/Q}(\alpha_2 - \alpha_2) = 1$. The middle coefficients of $h_1$ and $h_2$ are $-1$ mod $q_1$ and $1$ mod $q_2$ respectively. Therefore $\alpha_1$ satisfies the second hypothesis but not the first of Theorem 27, while $\alpha_2$ satisfies the first but not the second.

**Remark 30** One can show that any abelian variety admits a principal polarization if and only if its quadratic twist does. But for super-isolated varieties, this follows almost immediately from Theorem 27. If $h(x)$ is the Weil polynomial of $A/F_q$, then $h(-x)$ is the Weil polynomial for its twist. Then because Norm$_{K_i/Q}(\pi - \pi) = \text{Norm}_{K_i/Q}((-\pi) - (-\pi))$ and $h(x)$ and $h(-x)$ share the same middle coefficient, the criterion in Theorem 27 holds for one if and only if it holds for the other.

Given any super-isolated abelian variety $A$, we can always construct one with a principal polarization using Zarhin’s trick and Theorem 24.

**Proposition 31** Let $A$ be a super-isolated abelian variety. Then $A^8$ is principally polarized.

**Proof** Since $A$ is super-isolated it is isomorphic to its dual $A^\vee$. Hence there is an isomorphism $\varphi : A^8 \to (A \times A^\vee)^4$. By Zarhin’s trick (see [26]), the product $(A \times A^\vee)^4$ admits a principal polarization $\mu$. Then $\varphi^* \mu = \varphi^\vee \circ \mu \circ \varphi$ is a principal polarization of $A^8$, see for example [15, p.143].

### 4.2 Uniqueness of principal polarizations

In this section, we prove that if a super-isolated abelian variety admits a principal polarization, then such a polarization is unique up to polarized isomorphism.

First, we set the following notation. For a number field $L$, we let $U_L$ denote the group of units of $O_L$, and the group of totally positive units is $U_L^+$. The Hilbert class field of $L$ is denoted by $H_L$, and the narrow Hilbert class field is $H_L^+$. Recall that $H_L$ is the maximal unramified abelian extension of $L$ and that $H_L^+$ is the maximal abelian extension of $L$ unramified outside of the infinite primes (see [2, Ch. 5.C, Thm. 5.18] and [11, Ch. 8, p. 167]). Moreover, the Galois group $\text{Gal}(H_L/L)$ is isomorphic to the class group of $L$, see [2, Ch. 5.C, Thm. 5.23].

**Lemma 32** If $F$ is a totally real field, then

$$[U_F^+ : U_F^2] = [H_F^+ : H_F].$$

**Proof** If $r$ is the number of real embeddings of $F$, then $2^r = [U_F : U_F^+] [H_F^+ : H_F]$ by [10, Thm. 3.1, p. 242]. Since $F$ is totally real, $2^r = [U_F : U_F^2]$ as $U_F \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^r-1$.

**Lemma 33** Let $K$ be a CM field with class number 1, and let $F$ be the maximal totally real subfield of $K$. Then Norm$_{K/F}(U_K) = U_F^+.$

**Proof** By [11, Ch. 8, Ex. 27, p. 176], $H_K^+ K \subseteq H_K^+$. Since $K$ has no real embeddings because it is a CM field, we have $H_K^+ = H_K$ because the infinite primes of $K$ are unramified in every extension. Moreover, the assumption that $K$ has class number 1 means that $H_K = K$. Therefore we have that $F \subseteq H_K^+ F \subseteq K$, and either $H_K^+ F = F$ or $H_K^+ F = K$. By Lemma 32, $U_F^2$ has index 1 or 2 in $U_F^+$ depending on which equality holds.

If $K/F$ is ramified at a finite prime, then $H_K^+ = F$. Hence by Lemma 32 we have $U_F^+ = U_F^2$, and the conclusion follows from the fact that

$$U_F^2 \subseteq \text{Norm}_{K/F}(U_K) \subseteq U_F^+.$$

---

2 A real archimedean prime ramifies in an extension if it extends to a non-real embedding [2, Ch. 5.C, p. 94].
It remains to consider the case where $K/F$ is unramified. Here we have that $H_F^+ = K$, so $[U_F^+ : U_F^2] = 2$. To prove the claim, we will show that there is a unit $u \in U_K$ such that $\text{Norm}_{K/F}(u) \neq U_F^2$.

By Kummer theory, $K = F(\sqrt{-\varepsilon})$ for some totally positive element $\varepsilon \in F$. We claim that for every prime $p$ of $F$, the valuation $v_p(\varepsilon)$ is even. To see this, let $\mathfrak{p}$ be a prime of $K$ lying over $p$. Since $p$ is unramified in $K/F$, then we have $v_p(\varepsilon) = v_{\mathfrak{p}}(\varepsilon)$. The latter is even because $v_{\mathfrak{p}}(\varepsilon) = 2v_{\mathfrak{p}}(\sqrt{-\varepsilon})$.

By above, we can write $\varepsilon \mathcal{O}_F = \mathfrak{p}_1^{2e_1} \cdots \mathfrak{p}_k^{2e_k}$ for primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ of $F$. Because $K$ has class number 1, so does $F$, see [25, Thm. 4.10]. In particular, it remains to consider the case where $K = F(\sqrt{-1})$.

Let $\zeta$ be a primitive $2^n$th root of unity in $K$ such that $n$ is maximal (by above we know that $n \geq 2$). Then we have a tower of the form

$$
\begin{array}{c}
\mathbb{Q}(\zeta) \\
\mathbb{Q}(\zeta + \overline{\zeta}).
\end{array}
\begin{array}{c}
K \\
F
\end{array}
\begin{array}{c}
\mathbb{Q}(\sqrt{1 - \zeta}).
\end{array}
$$

Recall that since $\zeta$ is a primitive $2^n$th root of unity, the rational prime 2 is totally ramified in $\mathbb{Q}(\zeta)$. Moreover, $2\mathcal{O}_{\mathbb{Q}(\zeta)} = b^{2^{n-1}}$ where $b$ is the prime ideal generated by $b = 1 - \zeta$ [11, Ch. 2, Ex. 34, p. 34]. In particular $b = \overline{b}$. Put $a = b \cap \mathbb{Q}(\zeta + \overline{\zeta})$, which is the unique prime ideal of $\mathbb{Q}(\zeta + \overline{\zeta})$ above 2. Let $a = bb$. Observe that $a \in \mathbb{Q}(\zeta + \overline{\zeta})$ and that $a$ is a generator of $a\mathcal{O}_{\mathbb{Q}(\zeta)} = b^2$. Therefore $v_b(a) = 2v_a(a)$, and $v_b(a) = 2$ by construction. Hence $a$ is a generator of $a$. As mentioned above, the ramification index $e(b/a) = 2$. So, since $K/F$ is unramified, we deduce that there exists an ideal $c$ of $F$ such that $c^2 = a\mathcal{O}_F$. Moreover since $F$ has class number 1, the ideal $c$ admits a generator $c \in F$. Then $c^2 = au$ for some $u \in U_F$.

Moreover we have that

$$
c^2\mathcal{O}_K = c^2\mathcal{O}_K = a\mathcal{O}_K = b^2\mathcal{O}_K = b^2\mathcal{O}_K.
$$

Hence $c/b \in U_K$. Also, by construction,

$$
\text{Norm}_{K/F}\left(\frac{c}{b}\right) = \frac{au}{a} = u.
$$

We conclude the proof by proving that $u \notin U_F^2$. Indeed, assume that $u = u_0^2$ for some $u_0 \in U_F$. Then

$$
\left(\frac{bu_0}{c}\right)^2 = \frac{b^2}{a} = \frac{bb(-\zeta)}{a} = -\zeta.
$$

This implies that $bu_0/c$ is a primitive $2^{n+1}$ root of unity in $K$, contradicting the maximality of $n$. \qed
In the next example we show that the assumption on the class number of $K$ is necessary for Lemma 33 to hold.

**Example 34** Let $K = \mathbb{Q}[x]/(x^4 - x^3 + x^2 - 3x + 9)$, which has class number 2. Then $K$ is a CM field with maximal totally real subfield $F = \mathbb{Q}(\sqrt{21})$. A fundamental unit of $F$ is $\epsilon = (5 - \sqrt{21})/2$, which is totally positive. One can show that $U_K = U_F$. Therefore $\epsilon \notin \text{Norm}_{K/F}(U_K) = \langle \epsilon^2 \rangle$, so $U_F^+ / \text{Norm}_{K/F}(U_K) \cong \mathbb{Z}/2\mathbb{Z}$.

**Theorem 35** Let $A$ be a simple super-isolated ordinary abelian variety over $\mathbb{F}_q$ which admits a principal polarization. Then the polarization is unique up to polarized isomorphism.

**Proof** We have that $\text{End}(A) = \mathcal{O}_K$ for a CM-number field $K$ with class number 1. By [13, Thm. 5.4.(a)], two principal polarizations of $A$ differ by a totally positive unit in $U_F$. By [13, Thm. 5.4.(b)], two principal polarizations of $A$ are isomorphic if and only if they differ by an element of the form $v\overline{v}$ for a unit $v \in U_K$. In other words, the number of principal polarizations of $A$ up to isomorphism is given by the size of the quotient

$$\frac{U_F^+}{\text{Norm}_{K/F}(U_K)},$$

and this is trivial by Lemma 33.

\[\Box\]

### 4.3 Products of principal polarizations

Let $K$ be a CM field. Recall that for a CM type $\Phi$ of $K$ we say that a totally imaginary element $\lambda \in K$ is $\Phi$-positive if $\Im(\varphi(\lambda)) > 0$ for every $\varphi \in \Phi$. Also, for a fractional ideal $I$ of some order $R$ in $K$, we denote by $I'$ its trace dual ideal, which is defined as

$$I' = \{z \in K : \text{Trace}_{K/\mathbb{Q}}(xI) \subseteq \mathbb{Z}\}.$$

Also, we define $\overline{I}$ as the image of $I$ by the CM involution of $K$.

**Corollary 36** Let $A$ be an ordinary squarefree super-isolated abelian variety, say $A = \prod A_i$ with $A_i$ simple. Then $A$ admits a principal polarization if and only if each $A_i$ does. If this is the case, the principal polarization is unique up to polarized isomorphism.

**Proof** Let $h$ (resp. $h_i$) be the Weil polynomial of $A$ (resp. $A_i$). Put $K = \mathbb{Q}[x]/h$ and $K_i = \mathbb{Q}[x]/h_i$ for each $i$, so that $K = \prod_{i=1}^n K_i$. For each $i$ let $F_i$ be the maximal totally real subfield of $K_i$ and put $F = \prod_i F_i$. Since the abelian variety $A$ is ordinary, by [13, Thm. 5.4] we have that $A$ is principally polarized if and only there exist a $\lambda \in K^*$ which is totally imaginary, $\Phi$-positive, and such that

$$\lambda \mathcal{O}_K = \overline{\mathcal{O}_K'},$$

(9)

Since $\mathcal{O}_K = \oplus_i \mathcal{O}_{K_i}$ and $\overline{\mathcal{O}_K'} = \oplus_i \overline{\mathcal{O}_{K_i}}$, if we write $\lambda = (\lambda_1, \ldots, \lambda_n)$ with $\lambda_i$ in $K_i$, then $\lambda$ is totally imaginary and $\Phi$-positive if and only if the same holds for each $\lambda_i$. Also, Eq. (9) holds if and only if

$$\lambda_i \mathcal{O}_{K_i} = \overline{\mathcal{O}_{K_i}}$$

for each $i$. The statement about the uniqueness follows from the equality

$$\frac{U^+_F}{\text{Norm}_{K/F}(U_K)} = \prod_{i=1}^n \frac{U^+_F / \text{Norm}_{K_i/F_i}(U_{K_i})}{\text{Norm}_{K_i/F_i}(U_{K_i})}.\]
\[ \theta \]

Denote by two non-isomorphic polarizations: indeed by [13, Thm. 5.4] the number of non-isomorphic see [12, Ex. 6.5, Ex. 6.6].

\[ \text{Jac} \]

abelian varieties.

\[ \pi \]

the same isogeny class, which is determined by the Weil polynomial by the minimal polynomial of \( \pi \). For more examples and a general method to construct such curves see [9].

\[ \text{Example 39} \]

Consider the hyperelliptic curves over \( \mathbb{F}_3 \) defined by

\[ C_1 : y^2 = 2x^5 + 2x^4 + x^3 + 2x^2 + 1 \quad \text{and} \quad C_2 : y^2 = 2x^5 + x^4 + x + 1. \]

Observe (or use Magma to verify) that \( C_1 \) and \( C_2 \) are not isomorphic. Their Jacobians lie in the same isogeny class, which is determined by the Weil polynomial

\[ h = x^4 - x^3 + x^2 - 3x + 9. \]

Let \( K = \mathbb{Q}[x]/(h) = \mathbb{Q}(\pi) \), which is the same field as in Example 34. Note that \( \pi \) is a Weil generator for \( K \) but that the isogeny class is not super-isolated because the class group of \( K \) has order two. Using [13, Thm. 4.3] we deduce that there are two isomorphism classes of abelian varieties in the isogeny class, represented by say \( A \) and \( B \). Using [13, Thm. 5.4], we compute that one of the isomorphism classes admits two non-isomorphic principal polarizations, say \( (A, \theta_1) \) and \( (A, \theta_2) \), while \( B \) is not principally polarized. Note that it is not surprising that \( A \) has two non-isomorphic polarizations: indeed by [13, Thm. 5.4] the number of non-isomorphic polarizations equals the size of \( U_{\mathcal{P}}^+ / \text{Norm}_{K/F}(U) \) and in Example 34 we showed that it is 2. Denote by \( \theta'_1 \) (resp. \( \theta'_2 \)) the canonical polarization of \( \text{Jac}(C_1) \) (resp. \( \text{Jac}(C_2) \)). We deduce that, after possibly relabelling \( \theta_1 \) and \( \theta_2 \), we have isomorphisms \( \text{Jac}(C_1), \text{Jac}(C_2) \simeq (A, \theta_1) \) and \( \text{Jac}(C_1), \text{Jac}(C_2) \simeq (A, \theta_2) \). In particular we have \( \text{Jac}(C_1) \simeq \text{Jac}(C_2) \simeq A \) as unpolarized abelian varieties.

**Acknowledgements** The first author was partially supported by the Max Planck Society (Postdoctoral Fellowship) and by the Dutch Research Council (NWO grant 613.001.651). The second author was partially supported by Alfred P. Sloan Foundation (grant number G-2014-13575). The second author would also like to thank Alice Silverberg and Karl Rubin for helpful discussions on abelian varieties and class field theory. The authors thank Jonas Bergström, Valentijn Karemaker, Christophe Ritzenthaler and Shahed Sharif for comments, and Everett Howe helpful discussion that lead to the results contained in Sect. 3.1. The authors are grateful to the anonymous reviewer for helpful suggestions and comments.
References

1. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. 24(3-4), 235–265 (1997) [Computational algebra and number theory (London, 1993)]
2. Cox, D.A.: Primes of the form \(x^2 + ny^2\). Pure and Applied Mathematics (Hoboken). Fermat, Class Field Theory, and Complex Multiplication, 2nd edn. Wiley, Hoboken (2013)
3. CENTILEGHE, T.G., STIX, J.: Categories of abelian varieties over finite fields, I: Abelian varieties over \(\mathbb{F}_p\). Algebra Number Theory 9(1), 225–265 (2015)
4. Deligne, P.: Variétés abéliennes ordinaires sur un corps fini. Invent. Math. 8, 238–243 (1969)
5. Györy, K.: Sur les polynômes à coefficients entiers et de discriminant donné. III. Publ. Math. Debrecen 23(1–2), 141–165 (1976)
6. Howe, E.W., Lauter, K.E.: New methods for bounding the number of points on curves over finite fields. In: Geometry and Arithmetic, EMS Ser. Congr. Rep., pp. 173–212. Eur. Math. Soc., Zürich (2012)
7. Honda, T.: Isogeny classes of abelian varieties over finite fields: Honda, Taira. J. Math. Soc. Jpn. 20, 83–95 (1968)
8. Howe, E.W.: Principally polarized ordinary abelian varieties over finite fields. Trans. Am. Math. Soc. 347(7), 2361–2401 (1995)
9. Howe, E.W.: Constructing distinct curves with isomorphic Jacobians. J. Number Theory 56(2), 381–390 (1996)
10. Janusz, G.J.: Algebraic Number Fields, vol. 7 of Graduate Studies in Mathematics, 2nd, edn. American Mathematical Society, Providence, RI (1996)
11. Marcus, D.A.: Number Fields. Second edition of [ MR0457396], With a foreword by Barry Mazur. Universitext. Springer, Cham (2018)
12. Marseglia, S.: Computing abelian varieties over finite fields isogenous to a power. Res. Number Theory 5(4), 17 (2019) (Paper No. 35)
13. Marseglia, S.: Computing square-free polarized abelian varieties over finite fields. Math. Comput. 90(328), 953–971 (2021)
14. Mainsner, D., Nart, E.: Abelian surfaces over finite fields as Jacobians. Exp. Math. 11(3), 321–337 (2002) (with an appendix by Everett W. Howe)
15. David, M.: Abelian varieties, volume 5 of Tata Institute of Fundamental Research Studies in Mathematics. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second edition (1974)
16. Myerson, G.: On resultants. Proc. Am. Math. Soc. 89(3), 419–420 (1983)
17. Neukirch, J.: Algebraic number theory, vol. 322 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer, Berlin (1999) [Translated from the 1992 German original with a note by Norbert Schappacher. With a foreword by G. Harder (1999)]
18. Scholl, T.: Super-isolated elliptic curves and abelian surfaces in cryptography. Exp. Math. 28(4), 385–397 (2019)
19. Scholl, T.: Super-isolated abelian varieties. J. Number Theory 206, 138–168 (2020)
20. Stark, H.M.: Some effective cases of the Brauer–Siegel theorem. Invent. Math. 23, 135–152 (1974)
21. Steinitz, E.: Rechteckige Systeme und Moduln in algebraischen Zahlkörpern. I. Math. Ann. 71(3), 328–354 (1911)
22. Tate, J.: Endomorphisms of abelian varieties over finite fields. Invent. Math. 2, 134–144 (1966)
23. The Sage Developers: SageMath, the Sage Mathematics Software System (version 8.7) (2019). https://www.sagemath.org
24. Vaseršte˘ın, L.N., Suslin, A.A.: Serre’s problem on projective modules over polynomial rings, and algebraic \(K\)-theory. Izv. Akad. Nauk SSSR Ser. Mat. 40(5), 993–1054, 1199 (1976)
25. Washington, L.C.: Introduction to cyclotomic fields, vol. 83 of Graduate Texts in Mathematics, 2nd edn. Springer, New York (1997)
26. Zarhin, J.G.: A remark on endomorphisms of abelian varieties over function fields of finite characteristic. Izv. Akad. Nauk SSSR Ser. Mat. 38, 471–474 (1974)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.