



**HAL**  
open science

# Algebraic geometry codes over abelian surfaces containing no absolutely irreducible curves of low genus

Yves Aubry, Elena Berardini, Fabien Herbaut, Marc Perret

## ► To cite this version:

Yves Aubry, Elena Berardini, Fabien Herbaut, Marc Perret. Algebraic geometry codes over abelian surfaces containing no absolutely irreducible curves of low genus. *Finite Fields and Their Applications*, 2021, 10.1016/j.ffa.2020.101791 . hal-02100210v2

**HAL Id: hal-02100210**

**<https://hal.science/hal-02100210v2>**

Submitted on 31 Mar 2021

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# ALGEBRAIC GEOMETRY CODES OVER ABELIAN SURFACES CONTAINING NO ABSOLUTELY IRREDUCIBLE CURVES OF LOW GENUS

YVES AUBRY, ELENA BERARDINI, FABIEN HERBAUT AND MARC PERRET

ABSTRACT. We provide a theoretical study of Algebraic Geometry codes constructed from abelian surfaces defined over finite fields. We give a general bound on their minimum distance and we investigate how this estimation can be sharpened under the assumption that the abelian surface does not contain low genus curves. This approach naturally leads us to consider Weil restrictions of elliptic curves and abelian surfaces which do not admit a principal polarization.

## 1. INTRODUCTION

The success of Goppa construction ([5]) of codes over algebraic curves in breaking the Gilbert-Varshamov bound (see Tsfasman-Vlăduț-Zink bound in [18]) has been generating much interest over the last forty years. This gave birth to the field of Algebraic Geometry codes. It results a situation with a rich background and many examples of evaluation codes derived from algebraic curves (see for instance [19]). The study of Goppa construction from higher dimensional varieties has begun with few exceptions in the first decade of the twenty-first century. Although the construction holds in any dimension, the main focus has been put on algebraic surfaces.

The case of ruled surfaces is considered by Aubry in [1]. The case of toric surfaces is addressed among others by Little and Schenck in [13] and by Nardi in [16]. Voloch and Zarzar introduce the strategy of looking for surfaces with small Picard number ([21] and [23]). This approach is discussed in [12] and used by Couvreur in [2] to obtain very good codes over rational surfaces. In a parallel direction Little and Schenck ([12]) stress the influence of the sectional genus of the surface, that is the genus of a generic section. Finally, Haloui investigates the case of simple Jacobians of curves of genus 2 in [6].

The aim of this article is to study codes constructed from general abelian surfaces. While from the *geometric* point of view (i.e. over an algebraically closed field) a principally polarized abelian surface is isomorphic either to the Jacobian of a curve of genus 2 or to the product of two elliptic curves, the landscape turns

---

2010 *Mathematics Subject Classification.* 14K05, 14G50, 94B27.

*Key words and phrases.* Abelian surfaces, AG codes, Weil restrictions, finite fields.

to be richer from the *arithmetic* point of view. Weil proved that over a finite field  $k$  there is exactly one more possibility, that is the case of the Weil restriction of an elliptic curve defined over a quadratic extension of  $k$  (see for instance [8, Th.1.3]). Moreover, one can also consider abelian surfaces which do not admit a principal polarization.

The main contribution of this paper is twofold. First, we give a lower bound on the minimum distance of codes constructed over general abelian surfaces. Secondly, we sharpen this lower bound for abelian surfaces which do not contain absolutely irreducible curves defined over  $\mathbb{F}_q$  of arithmetic genus less or equal than a fixed integer  $\ell$ . In order to summarise our results in the following theorem, let us consider an ample divisor  $H$  on an abelian surface  $A$  and let us denote by  $\mathcal{C}(A, rH)$  the generalised evaluation code whose construction is recalled in Section 2.

**Theorem.** (*Theorem 2.2 and Theorem 3.3*) *Let  $A$  be an abelian surface defined over  $\mathbb{F}_q$  of trace  $\text{Tr}(A)$ . Let  $m = \lfloor 2\sqrt{q} \rfloor$ ,  $H$  be an ample divisor on  $A$  rational over  $\mathbb{F}_q$  and  $r$  be a positive integer large enough so that  $rH$  is very ample.*

*Then, the minimum distance  $d(A, rH)$  of the code  $\mathcal{C}(A, rH)$  satisfies*

$$(1) \quad d(A, rH) \geq \#A(\mathbb{F}_q) - rH^2(q + 1 - \text{Tr}(A) + m) - r^2m \frac{H^2}{2}.$$

*Moreover, if  $A$  is simple and contains no absolutely irreducible curves of arithmetic genus  $\ell$  or less for some positive integer  $\ell$ , then*

$$(2) \quad d(A, rH) \geq \#A(\mathbb{F}_q) - \max \left( \left\lfloor r\sqrt{\frac{H^2}{2}} \right\rfloor (\ell - 1), \varphi(1), \varphi \left( \left\lfloor r\sqrt{\frac{H^2}{2\ell}} \right\rfloor \right) \right),$$

where

$$\varphi(x) := m \left( r\sqrt{\frac{H^2}{2}} - x\sqrt{\ell} \right)^2 + 2m\sqrt{\ell} \left( r\sqrt{\frac{H^2}{2}} - x\sqrt{\ell} \right) + x \left( q + 1 - \text{Tr}(A) + (\ell - 1)(m - \sqrt{\ell}) \right) + r\sqrt{\frac{H^2}{2}}(\ell - 1).$$

If  $A$  is simple, then we can take  $\ell = 1$  and the lower bound (2) is nothing but Haloui's one [6] proved in the case of simple Jacobian surfaces  $\text{Jac}(C)$  with the choice  $H = C$  (see Remark 3.5).

It is worth to notice that the second bound is better for larger  $\ell$  (at least for  $q$  sufficiently large and  $1 < r < \sqrt{q}$ , see Remark 3.6). In particular, the bound obtained for  $\ell = 2$  improves the one obtained for  $\ell = 1$ . This leads us to investigate the case of abelian surfaces with no absolutely irreducible curves of genus 1 nor 2, which are necessarily either Weil restrictions of elliptic curves on a quadratic extension, either not principally polarizable abelian surfaces, from the classification given above. The following proposition lists all situations for which we can apply bound (2) with  $\ell = 2$ . The key point of the proof is a characterisation of isogeny classes of abelian surfaces containing Jacobians of curves of genus 2 obtained by Howe, Nart and Ritzenthaler ([8]).

**Proposition.** (Proposition 4.2 and Proposition 4.3) *The bound on the minimum distance (2) of the previous theorem holds when taking  $\ell = 2$  in the two following cases:*

- (i) *Let  $A$  be an abelian surface defined over  $\mathbb{F}_q$  which does not admit a principal polarization. Then  $A$  does not contain absolutely irreducible curves of arithmetic genus 0, 1 nor 2.*
- (ii) *Let  $q$  be a power of a prime  $p$ . Let  $E$  be an elliptic curve defined over  $\mathbb{F}_{q^2}$  of Weil polynomial  $f_{E/\mathbb{F}_{q^2}}(t) = t^2 - \text{Tr}(E/\mathbb{F}_{q^2})t + q^2$ . Let  $A$  be the  $\mathbb{F}_{q^2}/\mathbb{F}_q$ -Weil restriction of the elliptic curve  $E$ . Then  $A$  does not contain absolutely irreducible curves defined over  $\mathbb{F}_q$  of arithmetic genus 0, 1 nor 2 if and only if one of the following cases holds:*
  - (1)  $\text{Tr}(E/\mathbb{F}_{q^2}) = 2q - 1$ ;
  - (2)  $p > 2$  and  $\text{Tr}(E/\mathbb{F}_{q^2}) = 2q - 2$ ;
  - (3)  $p \equiv 11 \pmod{12}$  or  $p = 3$ ,  $q$  is a square and  $\text{Tr}(E/\mathbb{F}_{q^2}) = q$ ;
  - (4)  $p = 2$ ,  $q$  is nonsquare and  $\text{Tr}(E/\mathbb{F}_{q^2}) = q$ ;
  - (5)  $q = 2$  or  $q = 3$  and  $\text{Tr}(E/\mathbb{F}_{q^2}) = 2q$ .

The paper is structured as follows. In Section 2 we consider evaluation codes on general abelian surfaces. We compute their dimension and prove the lower bound (1) on their minimum distance. Section 3 is devoted to the case of simple abelian surfaces, that is those for which we can choose some  $\ell \geq 1$ . We derive the lower bound (2) depending on the minimum arithmetic genus of absolutely irreducible curves lying on the surface. In Section 4 we consider abelian surfaces which do not admit a principal polarization and Weil restrictions of elliptic curves to find all abelian surfaces defined over a finite field containing no absolutely irreducible curves of arithmetic genus 0, 1 and 2. Finally, in Section 5, we make explicit the lower bounds for the minimum distance.

## 2. CODES FROM ABELIAN SURFACES

**2.1. Some facts on intersection theory.** One of the ingredients of the proofs of Theorems 2.2 and 3.3 is the classical inequality induced by the Hodge index theorem (3) in the context of intersection theory on surfaces. In this subsection, we briefly recall this context and the main properties we need. We refer the reader to [7, §V] for further details.

Let  $X$  be a nonsingular, projective, absolutely irreducible algebraic surface defined over  $\mathbb{F}_q$ . A divisor on  $X$  is an element of the free abelian group generated by the irreducible curves on  $X$ . Divisors associated to rational functions on  $X$  are called principal. Two divisors on  $X$  are said to be *linearly equivalent* if their difference is a principal divisor. We write  $\text{Pic}(X)$  for the group of divisors of  $X$  modulo linear equivalence. The Néron-Severi group of  $X$ , denoted by  $\text{NS}(X)$ , is obtained by considering the coarser *algebraic equivalence* we do not define here since it coincides for abelian varieties (see [11, §IV]) with the following *numerical equivalence*. A divisor  $D$  on  $X$  is said to be numerically equivalent to zero, which

we denote by  $D \equiv 0$ , if the intersection product  $C.D$  is zero for all curves  $C$  on  $X$ . This gives the coarsest equivalence relation on divisors on  $X$  and we denote the group of divisors modulo numerical equivalence by  $\text{Num}(X)$ . We have thus  $\text{Num}(X) = \text{NS}(X)$ , so we will refer to these two equivalence relations with no distinction. We write simply  $D$  for the class of a divisor  $D$  in  $\text{NS}(X)$ .

We recall the Nakai-Moishezon criterion in the context of surfaces: a divisor  $H$  is ample if and only if  $H^2 > 0$  and  $H.C > 0$  for all irreducible curves  $C$  on  $X$  ([7, §V, Th.1.10]). The Hodge index theorem states that the intersection pairing is negative definite on the orthogonal complement of the line generated by an ample divisor. From this, it easily follows that

$$(3) \quad H^2 D^2 \leq (H.D)^2$$

for any pair of divisors  $D, H$  with  $H$  ample, and that equality holds if and only if  $D$  and  $H$  are numerically proportional.

**2.2. Evaluation codes.** This subsection begins by a reminder about definitions of the evaluation code we study. To this end we consider again  $X$  a nonsingular, projective, absolutely irreducible algebraic surface defined over  $\mathbb{F}_q$  and  $G$  a divisor on  $X$ . The Riemann-Roch space  $L(G)$  is defined by

$$L(G) = \{f \in \mathbb{F}_q(X) \setminus \{0\} \mid (f) + G \geq 0\} \cup \{0\}.$$

The Algebraic Geometry code  $\mathcal{C}(X, G)$  is sometimes presented from a functional point of view as the image of the following linear evaluation map  $\text{ev}$

$$\begin{aligned} \text{ev} : L(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \dots, f(P_n)) \end{aligned}$$

which is clearly well defined when considering  $\{P_1, \dots, P_n\} \subset X(\mathbb{F}_q)$  a subset of rational points which are on  $X$  but not in the support of  $G$ . In fact, this construction naturally extends to the case where  $\{P_1, \dots, P_n\} = X(\mathbb{F}_q)$  is an enumeration of the whole set of the rational points on  $X$ , as noticed by Manin and Vlăduț in [20, §3.1]. Indeed, one can rather consider the image of the following map, where we denote by  $\mathcal{L}$  the line bundle associated to  $L(G)$ , by  $\mathcal{L}_{P_i}$  the stalks at the  $P_i$ 's, and by  $s_{P_i}$  the images of a global section  $s \in H^0(X, \mathcal{L})$  in the stalks

$$\begin{aligned} \text{ev} : H^0(X, \mathcal{L}) &\longrightarrow \bigoplus_{i=1}^n \mathcal{L}_{P_i} = \mathbb{F}_q^n \\ s &\longmapsto (s_{P_1}, \dots, s_{P_n}). \end{aligned}$$

Different choices of isomorphisms between the fibres  $\mathcal{L}_{P_i}$  and  $\mathbb{F}_q$  give rise to different maps but lead to equivalent codes. See also [10] or [1] for another constructive point of view.

Throughout the whole paper we associate to a nonzero function  $f \in L(G)$  an effective rational divisor

$$(4) \quad D := G + (f) = \sum_{i=1}^k n_i D_i,$$

where  $n_i > 0$  and where each  $D_i$  is an  $\mathbb{F}_q$ -irreducible curve whose arithmetic genus is denoted by  $\pi_i$ . The evaluation map  $\text{ev}$  is injective if and only if the number  $N(f)$  of zero coordinates of the codeword  $\text{ev}(f)$  satisfies

$$(5) \quad N(f) < \#X(\mathbb{F}_q)$$

for any  $f \in L(G) \setminus \{0\}$ . In this case the minimum distance  $d(X, G)$  of the code  $\mathcal{C}(X, G)$  satisfies

$$(6) \quad d(X, G) = \#X(\mathbb{F}_q) - \max_{f \in L(G) \setminus \{0\}} N(f).$$

Let us remark now that by (4) we have

$$(7) \quad N(f) \leq \sum_{i=1}^k \#D_i(\mathbb{F}_q)$$

for any  $f \in L(G) \setminus \{0\}$ . Therefore, to get a lower bound on the minimum distance of the code  $\mathcal{C}(X, G)$  it suffices to get two upper bounds:

- an upper bound on the number  $k$  of  $\mathbb{F}_q$ -irreducible components of an effective divisor linearly equivalent to  $G$

$$D = \sum_{i=1}^k n_i D_i \sim G;$$

- an upper bound on the number of rational points on each  $\mathbb{F}_q$ -irreducible curves  $D_i$  in the support of  $D$ .

**2.3. The parameters of codes over abelian surfaces.** In this subsection we begin the estimation of the parameters of the code in the context of our work.

Let  $A$  be an abelian surface defined over  $\mathbb{F}_q$ . We recall that the Weil polynomial of an abelian variety is the characteristic polynomial of the Frobenius endomorphism acting on its Tate module. Since  $A$  is here two-dimensional, it has by Weil theorem the shape

$$(8) \quad f_A(t) = t^4 - \text{Tr}(A)t^3 + a_2 t^2 - q \text{Tr}(A)t + q^2.$$

By the Riemann Hypothesis  $f_A(t) = (t - \omega_1)(t - \bar{\omega}_1)(t - \omega_2)(t - \bar{\omega}_2)$  where  $\omega_i$  are complex numbers of modulus  $\sqrt{q}$ . The number  $\text{Tr}(A) = \omega_1 + \bar{\omega}_1 + \omega_2 + \bar{\omega}_2$  is called the *trace of A*.

Let  $H$  be an ample divisor on  $A$  rational over  $\mathbb{F}_q$  and  $r$  large enough so that  $rH$  is very ample ( $r \geq 3$  is sufficient by [15, III, §17]). Our goal is to derive from (6) a lower bound on the minimum distance of the code  $\mathcal{C}(A, rH)$ .

If the evaluation map  $\text{ev}$  is injective, then the dimension of  $\mathcal{C}(A, rH)$  is equal to the dimension  $\ell(rH)$  of the Riemann-Roch space  $L(rH)$  which can be computed using the Riemann-Roch theorem for surfaces. In the general setting of a divisor  $D$  on a surface  $X$  it states that (see [7, V, §1])

$$\ell(D) - s(D) + \ell(K_X - D) = \frac{1}{2}D \cdot (D - K_X) + 1 + p_a(X)$$

where  $K_X$  is the canonical divisor of  $X$  and  $p_a(X)$  is the arithmetic genus of  $X$ , and where  $s(D) = \dim_{\mathbb{F}_q} H^1(X, \mathcal{L}(D))$  is the so-called *superabundance* of  $D$  in  $X$ .

Since  $A$  is an abelian surface we have ([15, III, §16])  $K_A = 0$  and  $p_a(A) = -1$ . Moreover, if  $rH$  is very ample, then we can deduce from [7, V, Lemma 1.7] that  $\ell(K - rH) = \ell(-rH) = 0$  and that  $s(rH) = 0$  ([15, III, §16]). So finally if the evaluation map  $\text{ev}$  is injective, i.e. if inequality (5) holds, we get the dimension of the code  $\mathcal{C}(A, rH)$ :

$$\dim_{\mathbb{F}_q} L(rH) = r^2 \frac{H^2}{2}.$$

We are now going to give a lower bound on the minimum distance of  $\mathcal{C}(A, rH)$  using (6) and (7). Theorem 4 of [6] states that the number of rational points on a projective  $\mathbb{F}_q$ -irreducible curve  $D$  defined over  $\mathbb{F}_q$  of arithmetic genus  $\pi$  lying on an abelian surface  $A$  of trace  $\text{Tr}(A)$  is bounded by

$$\#D(\mathbb{F}_q) \leq q + 1 - \text{Tr}(A) + |\pi - 2| \lfloor 2\sqrt{q} \rfloor.$$

Hence, if we set  $m := \lfloor 2\sqrt{q} \rfloor$ , where  $\lfloor x \rfloor$  denotes the integer part of the real number  $x$ , from inequality (7) we get

$$(9) \quad N(f) \leq k(q + 1 - \text{Tr}(A)) + m \sum_{i=1}^k |\pi_i - 2|.$$

With no hypotheses on the abelian surface nor on the arithmetic genera  $\pi_i$ , we can only say that  $\pi_i = 0$  cannot occur and since  $\pi_i \geq |\pi_i - 2|$  for  $\pi_i \geq 1$ , we have

$$(10) \quad N(f) \leq k(q + 1 - \text{Tr}(A)) + m \sum_{i=1}^k \pi_i.$$

In order to use (10) to bound the minimum distance of the code  $\mathcal{C}(A, rH)$ , we need Lemma 2.1 below, giving upper bounds on the number  $k$  of irreducible components of the effective divisor  $D$  linearly equivalent to  $rH$  and on the sum of the arithmetic genera of its components  $D_i$ . We recall for this purpose a generalisation of the adjunction formula which states that for a curve  $D$  of arithmetic genus  $\pi$  on a surface  $X$  we have  $D \cdot (D + K_X) = 2\pi - 2$  ([7, §V, Exercise 1.3]). In the case of an abelian surface  $A$  for which  $K_A = 0$ , this says that for any curve  $D$  of arithmetic genus  $\pi$  lying on  $A$  we have  $D^2 = 2\pi - 2$ .

**Lemma 2.1.** *Let  $D$  be an effective divisor linearly equivalent to  $rH$ , let  $D = \sum_{i=1}^k n_i D_i$  be its decomposition as a sum of  $\mathbb{F}_q$ -irreducible curves and let  $\pi_i$  be the arithmetic genus of  $D_i$  for  $i = 1, \dots, k$ . Then we have*

$$\sum_{i=1}^k \pi_i \leq r^2 \frac{H^2}{2} + k \quad \text{and} \quad k \leq rH^2.$$

*Proof.* Applying Formula (3) to  $H$  and  $D_i$  for every  $i$ , we get  $D_i^2 H^2 \leq (D_i \cdot H)^2$ . By the adjunction formula we have

$$(11) \quad \pi_i - 1 \leq (D_i \cdot H)^2 / (2H^2).$$

Indeed  $H^2 > 0$  by the Nakai-Moishezon criterion since  $H$  is ample.

Summing from  $i = 1$  to  $k$ , we obtain

$$(12) \quad \sum_{i=1}^k \pi_i - k \leq \frac{1}{2H^2} \sum_{i=1}^k (D_i \cdot H)^2.$$

We have also

$$(13) \quad \begin{aligned} \sum_{i=1}^k (D_i \cdot H)^2 &= \left( \sum_{i=1}^k D_i \cdot H \right)^2 - \sum_{i \neq j} (D_i \cdot H)(D_j \cdot H) \\ &\leq \left( \sum_{i=1}^k n_i D_i \cdot H \right)^2 - \sum_{i \neq j} (D_i \cdot H)(D_j \cdot H) \\ &\leq r^2 (H^2)^2, \end{aligned}$$

where we used the facts that  $n_i > 0$ , that  $D = \sum_{i=1}^k n_i D_i$  is linearly (and hence numerically) equivalent to  $rH$  and that  $D_i \cdot H > 0$  for every  $i = 1, \dots, k$ , thanks to Nakai-Moishezon criterion since  $H$  is ample. Now applying inequality (13) to inequality (12), we get

$$\sum_{i=1}^k \pi_i \leq \frac{r^2 (H^2)^2}{2H^2} + k = \frac{r^2 H^2}{2} + k$$

which completes the proof of the first statement. Using that  $k \leq \sum_{i=1}^k n_i D_i \cdot H = rH^2$  we get the second one.  $\square$

As a consequence of Lemma 2.1 we can state the following theorem.

**Theorem 2.2.** *Let  $A$  be an abelian surface defined over  $\mathbb{F}_q$  of trace  $\text{Tr}(A)$ . Let  $m = \lfloor 2\sqrt{q} \rfloor$ ,  $H$  be an ample divisor on  $A$  rational over  $\mathbb{F}_q$  and  $r$  be a positive integer large enough so that  $rH$  is very ample.*



Then the minimum distance  $d(A, rH)$  of the code  $\mathcal{C}(A, rH)$  satisfies

$$d(A, rH) \geq \#A(\mathbb{F}_q) - rH^2(q + 1 - \text{Tr}(A) + m) - r^2m \frac{H^2}{2}.$$

*Proof.* Using Lemma 2.1 together with (10) we get  $N(f) \leq \phi(k)$  with  $\phi(k) := k(q + 1 - \text{Tr}(A) + m) + mr^2H^2/2$  and  $k \in [1, rH^2]$ . This means that  $N(f) \leq \max_{k \in [1, rH^2]} \{\phi(k)\}$ . Now remark that  $\phi$  is an increasing linear function since  $|\text{Tr}(A)| \leq 4\sqrt{q}$ , and hence gets its maximum when  $k = rH^2$ . Therefore we have  $N(f) \leq \phi(rH^2)$ , which implies  $d(A, rH) = \#A(\mathbb{F}_q) - \max\{N(f), f \in L(rH) \setminus \{0\}\} \geq \#A(\mathbb{F}_q) - \phi(rH^2)$ . The theorem is proved since  $\phi(rH^2) = rH^2(q + 1 - \text{Tr}(A) + m) + mr^2H^2/2$ .  $\square$

**Remark 2.3.** Let  $H$  be an ample divisor. Suppose that  $H$  is irreducible over  $\mathbb{F}_q$ , but reducible on a Galois extension of prime degree  $e$ . Then  $H$  is a sum of  $e$  conjugate irreducible components such that the intersection points are also conjugates under the Galois group. Then, by Lemma 2.3 of [21], we have

$$k \leq r \frac{H^2}{e}.$$

Hence under this hypothesis we get a sharper bound on the number of irreducible components of a divisor linearly equivalent to  $rH$ , thus a sharper bound for Theorem 2.2.

### 3. CODES FROM ABELIAN SURFACES WITH NO SMALL GENUS CURVES

We consider now evaluation codes  $\mathcal{C}(A, rH)$  on abelian surfaces which contain no absolutely irreducible curves defined over  $\mathbb{F}_q$  of arithmetic genus smaller than or equal to an integer  $\ell$ .

Throughout this section  $A$  denotes a *simple* abelian surface defined over  $\mathbb{F}_q$ . Let us remark that by Proposition 5 of [6] a simple abelian surface contains no irreducible curves of arithmetic genus 0 nor 1 defined over  $\mathbb{F}_q$ . In particular, every absolutely irreducible curve on  $A$  has arithmetic genus greater than or equal to 2 and thus it is relevant to take  $\ell \geq 1$ .

**Lemma 3.1.** *Let  $A$  be a simple abelian surface defined over  $\mathbb{F}_q$  of trace  $\text{Tr}(A)$ . Let  $\ell$  be a positive integer such that for every absolutely irreducible curves of arithmetic genus  $\pi$  lying on  $A$  we have  $\pi > \ell$ . Let  $f$  be a nonzero function in  $L(rH)$  with associated effective rational divisor  $D = \sum_{i=1}^k n_i D_i$  as given in equation (4). Write  $k = k_1 + k_2$  where  $k_1$  is the number of  $D_i$  which have arithmetic genus  $\pi_i > \ell$  and  $k_2$  is the number of  $D_i$  which have arithmetic genus  $\pi_i \leq \ell$ . Then*

$$(14) \quad N(f) \leq k_1(q + 1 - \text{Tr}(A) - 2m) + m \sum_{i=1}^{k_1} \pi_i + k_2(\ell - 1),$$

where  $\pi_i > \ell$  and where  $\sum_{i=1}^{k_1} \pi_i$  is supposed to be zero if  $k_1 = 0$ .

*Proof.* In order to prove the statement, let us recall that by Theorem 4 of [6] the number of rational points on an irreducible curve  $D_i$  on  $A$  of arithmetic genus  $\pi_i$  satisfies  $\#D_i(\mathbb{F}_q) \leq q + 1 - \text{Tr}(A) + m|\pi_i - 2|$ . Since  $A$  is simple and hence  $\pi_i \geq 2$ , we get  $\#D_i(\mathbb{F}_q) \leq q + 1 - \text{Tr}(A) - 2m + m\pi_i$ . Without loss of generality we consider  $\{D_1, \dots, D_{k_1}\}$  to be the set of the  $D_i$  which have arithmetic genus  $\pi_i > \ell$  and  $\{D_{k_1+1}, \dots, D_k\}$  to be the set of the  $k_2$  curves which have arithmetic genus  $\pi_i \leq \ell$ . Thus, we get

$$\sum_{i=1}^{k_1} \#D_i(\mathbb{F}_q) \leq k_1(q + 1 - \text{Tr}(A) - 2m) + m \sum_{i=1}^{k_1} \pi_i$$

where  $\pi_i > \ell$ . Under the hypothesis that any absolutely irreducible curve on  $A$  has arithmetic genus  $> \ell$ , we have that the  $k_2$  curves that have arithmetic genus  $\pi_i \leq \ell$  are necessarily non absolutely irreducible. It is well-known (see for example the proof of Theorem 4 of [6]) that if  $D_i$  is a non absolutely irreducible curve of arithmetic genus  $\pi_i$  lying on an abelian surface, its number of rational points satisfies  $\#D_i(\mathbb{F}_q) \leq \pi_i - 1$ . Hence summing on  $k_2$  we get

$$\sum_{i=k_1+1}^k \#D_i(\mathbb{F}_q) \leq \sum_{i=k_1+1}^k (\pi_i - 1) \leq k_2(\ell - 1).$$

The proof is now complete using inequality (7).  $\square$

In order to use inequality (14) to deduce a lower bound on the minimum distance of the code  $\mathcal{C}(A, rH)$ , it is sufficient to bound the numbers  $k_1$  and  $k_2$  and the sum  $\sum_{i=1}^{k_1} \pi_i$ .

**Lemma 3.2.** *With the same notations and under the same hypotheses as Lemma 3.1 we have:*

- (1)  $k_1\sqrt{\ell} + k_2 \leq r\sqrt{\frac{H^2}{2}}$ ,
- (2)  $\sum_{i=1}^{k_1} \pi_i \leq \alpha^2 + 2\sqrt{\ell}\alpha + (\ell + 1)k_1$ , where  $\alpha := r\sqrt{\frac{H^2}{2}} - k_1\sqrt{\ell} - k_2$ .

*Proof.* Let us prove the first assertion. Since  $H$  is ample, by Nakai-Moishezon criterion we have that  $D_i \cdot H > 0$  for every  $i = 1, \dots, k$  and  $H^2 > 0$ . Thus, we can take the square root of inequality (11) in the proof of Lemma 2.1 and get  $\sqrt{\pi_i - 1} \leq D_i \cdot H / \sqrt{2H^2}$ . Now taking into account that  $1 \leq \pi_i - 1$  since  $A$  is assumed to be simple, summing for  $i \in \{1, \dots, k\}$ , using that  $n_i > 0$  and that

$\sum_{i=1}^k n_i D_i \cdot H = rH^2$ , we obtain

$$\begin{aligned} \sum_{i=1}^{k_1} \sqrt{\pi_i - 1} &= \sum_{i=1}^k \sqrt{\pi_i - 1} - \sum_{i=k_1+1}^k \sqrt{\pi_i - 1} \\ &\leq \sum_{i=1}^k \sqrt{\pi_i - 1} - k_2 \\ &\leq \frac{1}{\sqrt{2H^2}} \sum_{i=1}^k n_i D_i \cdot H - k_2 \\ &= r\sqrt{\frac{H^2}{2}} - k_2. \end{aligned}$$

Considering the  $k_1$  curves that have arithmetic genus  $\pi_i > \ell$ , we have  $\sqrt{\ell} \leq \sqrt{\pi_i - 1}$  and so  $k_1\sqrt{\ell} \leq \sum_{i=1}^{k_1} \sqrt{\pi_i - 1}$ . Thus we get

$$k_1\sqrt{\ell} + k_2 \leq r\sqrt{\frac{H^2}{2}}.$$

Let us now prove the last statement. For  $i = 1, \dots, k_1$ , set  $s_i = \sqrt{\pi_i - 1} - \sqrt{\ell}$ . Under the hypothesis that  $\pi_i \geq \ell + 1$ , the  $s_i$  are non-negative real numbers. Thus

$$\sum_{i=1}^{k_1} s_i^2 \leq \left( \sum_{i=1}^{k_1} s_i \right)^2.$$

Moreover, we have seen above that

$$\sum_{i=1}^{k_1} s_i = \sum_{i=1}^{k_1} \sqrt{\pi_i - 1} - k_1\sqrt{\ell} \leq r\sqrt{\frac{H^2}{2}} - k_1\sqrt{\ell} - k_2 = \alpha.$$

Therefore, since  $\pi_i = (s_i + \sqrt{\ell})^2 + 1 = s_i^2 + 2s_i\sqrt{\ell} + \ell + 1$  for  $i \in \{1, \dots, k_1\}$ , we have

$$\begin{aligned} \sum_{i=1}^{k_1} \pi_i &= \sum_{i=1}^{k_1} s_i^2 + 2\sqrt{\ell} \sum_{i=1}^{k_1} s_i + (\ell + 1)k_1 \\ (15) \quad &\leq \left( \sum_{i=1}^{k_1} s_i \right)^2 + 2\sqrt{\ell} \sum_{i=1}^{k_1} s_i + (\ell + 1)k_1 \\ &\leq \alpha^2 + 2\sqrt{\ell}\alpha + (\ell + 1)k_1, \end{aligned}$$

which completes the proof of the lemma.  $\square$

We can now prove the following theorem.

**Theorem 3.3.** *Let  $A$  be a simple abelian surface defined over  $\mathbb{F}_q$  of trace  $\text{Tr}(A)$ . Let  $m = \lfloor 2\sqrt{q} \rfloor$ ,  $H$  be an ample divisor on  $A$  rational over  $\mathbb{F}_q$  and  $r$  be a positive integer large enough so that  $rH$  is very ample. Moreover, let  $\ell$  be a positive integer such that for every absolutely irreducible curves of arithmetic genus  $\pi$  lying on  $A$  we have  $\pi > \ell$ . Then the minimum distance  $d(A, rH)$  of the code  $\mathcal{C}(A, rH)$  satisfies*

$$d(A, rH) \geq \#A(\mathbb{F}_q) - \max \left( \left\lfloor r\sqrt{\frac{H^2}{2}} \right\rfloor (\ell - 1), \varphi(1), \varphi \left( \left\lfloor r\sqrt{\frac{H^2}{2\ell}} \right\rfloor \right) \right),$$

where

$$\varphi(x) := m \left( r\sqrt{\frac{H^2}{2}} - x\sqrt{\ell} \right)^2 + 2m\sqrt{\ell} \left( r\sqrt{\frac{H^2}{2}} - x\sqrt{\ell} \right) + x \left( q+1 - \text{Tr}(A) + (\ell-1)(m - \sqrt{\ell}) \right) + r\sqrt{\frac{H^2}{2}}(\ell-1).$$

*Proof.* Recall that  $d(A, rH) = \#A(\mathbb{F}_q) - \max\{N(f), f \in L(rH) \setminus \{0\}\}$ . The point of departure is the inequality (14). When  $k_1 = 0$ , it simply implies that  $N(f)$  is less than or equal to  $k_2(\ell - 1)$ . If  $k_1 > 0$  we use point (2) of Lemma 3.2 to get (16)

$$N(f) \leq k_1 \left( q+1 - \text{Tr}(A) + (\ell-1)(m - \sqrt{\ell}) \right) + m\alpha^2 + 2m\sqrt{\ell}\alpha + r\sqrt{\frac{H^2}{2}}(\ell-1) - \alpha(\ell-1)$$

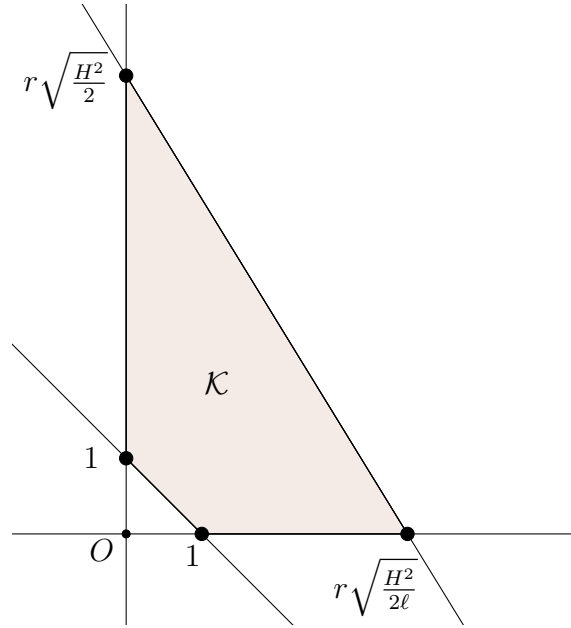
where we have set  $\alpha := r\sqrt{\frac{H^2}{2}} - k_1\sqrt{\ell} - k_2$ . Now point (1) of Lemma 3.2 ensures that  $\alpha \geq 0$  which enables to conclude that  $N(f) \leq \phi(k_1, k_2)$  where  $\phi(k_1, k_2)$  is defined by

$$\phi(k_1, k_2) = \begin{cases} k_2(\ell - 1) & \text{if } k_1 = 0 \\ k_1 \left( q+1 - \text{Tr}(A) + (\ell-1)(m - \sqrt{\ell}) \right) \\ \quad + m\alpha^2 + 2m\sqrt{\ell}\alpha + r\sqrt{\frac{H^2}{2}}(\ell-1) & \text{if } k_1 > 0. \end{cases}$$

It thus remains to maximise the function  $\phi(k_1, k_2)$  on the integer points inside the polygon  $\mathcal{K}$  defined by

$$\mathcal{K} = \left\{ (k_1, k_2) \mid 0 \leq k_1, 0 \leq k_2, 1 \leq k_1 + k_2, \sqrt{\ell}k_1 + k_2 \leq r\sqrt{\frac{H^2}{2}} \right\}$$

and represented below.



First, in the case where  $k_1 = 0$  we notice that  $k_2 \leq \left\lfloor r\sqrt{\frac{H^2}{2}} \right\rfloor$ , which implies  $\phi(0, k_2) \leq \left\lfloor r\sqrt{\frac{H^2}{2}} \right\rfloor (\ell - 1)$ . Second, for a fixed positive value of  $k_1$  less than or equal to  $r\sqrt{\frac{H^2}{2}}$  we can consider  $\phi$  as a degree-2 polynomial in  $\alpha \geq 0$ , namely  $\phi(k_1, k_2) = m\alpha(\alpha + 2\sqrt{\ell}) + \text{constant}$ . This way, it is clear that the maximum of  $\phi$  is reached for the maximal value of  $\alpha$ , that is for the minimal value of  $k_2$  such that  $(k_1, k_2) \in \mathcal{K}$ . Hence, for this second case we are reduced to maximise  $\phi$  on the segment  $\left[ (1, 0), \left( r\sqrt{\frac{H^2}{2\ell}}, 0 \right) \right]$ . As easily checked,  $\phi$  is a convex function on this segment, so the maximum is reached at an extremal integer point,  $(1, 0)$  or  $\left( \left\lfloor r\sqrt{\frac{H^2}{2\ell}} \right\rfloor, 0 \right)$ . Finally, note that we have  $\phi(x, 0) = \varphi(x)$ , and the theorem is proved.  $\square$

**Remark 3.4.** Taking into account the term  $-\alpha(\ell - 1)$  in the inequality (16) one sometimes obtains a slightly better bound than the one of Theorem 3.3 but whose expression is even more complicated.

**Remark 3.5.** The bound in Theorem 3.3 applies with  $\ell = 1$  on simple abelian surfaces since they do not contain absolutely irreducible curves of arithmetic genus 0 nor 1, as remarked at the beginning of this section. Note that for  $\ell = 1$  we have  $\left\lfloor r\sqrt{\frac{H^2}{2}} \right\rfloor (\ell - 1) = 0$  and thus in this context we are reduced to

consider the maximum between  $\varphi(1)$  and  $\varphi\left(\left\lfloor r\sqrt{\frac{H^2}{2}} \right\rfloor\right)$  in Theorem 3.3. In order to easily compare these two values, let us consider a weaker version of our theorem by removing the integer part. Indeed,  $\varphi\left(\left\lfloor r\sqrt{\frac{H^2}{2}} \right\rfloor\right) \leq \varphi\left(r\sqrt{\frac{H^2}{2}}\right)$ . Consequently we have  $d(A, rH) \geq \#A(\mathbb{F}_q) - \max\left(\varphi(1), \varphi\left(r\sqrt{\frac{H^2}{2}}\right)\right)$  and after some calculations we get

$$d(A, rH) \geq \begin{cases} \#A(\mathbb{F}_q) - r\sqrt{\frac{H^2}{2}}(q+1 - \text{Tr}(A)) & \text{if } r \leq \frac{\sqrt{2}(q+1 - \text{Tr}(A) - m)}{m\sqrt{H^2}}, \\ \#A(\mathbb{F}_q) - (q+1 - \text{Tr}(A) - m) - mr^2\frac{H^2}{2} & \text{otherwise.} \end{cases}$$

In particular if  $A = \text{Jac}(C)$  is the Jacobian of a curve  $C$  of genus 2 which is simple, then by setting  $H = C$  with  $H^2 = C^2 = 2\pi_C - 2 = 2$  by the adjunction formula, we obtain

$$d(\text{Jac}(C), rC) \geq \begin{cases} \#\text{Jac}(C)(\mathbb{F}_q) - r\#C(\mathbb{F}_q) & \text{if } r \leq \frac{q+1 - \text{Tr}(A) - 2m}{m}, \\ \#\text{Jac}(C)(\mathbb{F}_q) - \#C(\mathbb{F}_q) - m(r^2 - 1) & \text{otherwise.} \end{cases}$$

This bound coincides with the bound in the main theorem of [6].

**Remark 3.6.** We point out, using an elementary asymptotic analysis for large  $q$  and  $r$ , that our estimation of the minimum distance is better for larger  $\ell$ . We assume that  $\ell$  is small (for example  $\ell$  is a fixed value) and that  $r = q^\rho$  for some  $\rho > 0$ . For simplicity, we also assume that  $H^2 = 2$  (see Section 5) and remove the integer part. Taking into account that  $|\text{Tr}(A)| \leq 4\sqrt{q}$  yields to

$$\begin{cases} r(\ell - 1)\sqrt{\frac{H^2}{2}} & \underset{q \rightarrow \infty}{\sim} & (\ell - 1)q^\rho, \\ \varphi(1) & \underset{q \rightarrow \infty}{\sim} & cq^{\max\{1, 2\rho + \frac{1}{2}\}}, \\ \varphi\left(r\sqrt{\frac{H^2}{2\ell}}\right) & \underset{q \rightarrow \infty}{\sim} & \frac{1}{\sqrt{\ell}}q^{1+\rho}, \end{cases}$$

where  $c = 1, 3$  or  $2$  depending on whether  $\rho < 1/4, \rho = 1/4$  or  $\rho > 1/4$ . Consequently, in this setting, the lower bound  $d^*$  obtained in Theorem 3.3 satisfies

$$\begin{cases} \#A(\mathbb{F}_q) - d^* & \underset{q \rightarrow \infty}{\sim} & 2q^{2\rho + \frac{1}{2}} \text{ if } \rho \geq \frac{1}{2}, \\ \#A(\mathbb{F}_q) - d^* & \underset{q \rightarrow \infty}{\sim} & \frac{1}{\sqrt{\ell}}q^{1+\rho} \text{ if } 0 < \rho < \frac{1}{2}. \end{cases}$$

So for  $q$  sufficiently large and  $r = q^\rho$  with  $0 < \rho < \frac{1}{2}$ , the bound in Theorem 3.3 obtained for  $\ell = 2$  for instance is better than the one obtained for  $\ell = 1$ , that is for any simple abelian variety. We thus focus in the next section on the existence of simple abelian surfaces which do not contain absolutely irreducible curves of arithmetic genus 2.

## 4. ABELIAN SURFACES WITHOUT CURVES OF GENUS 1 NOR 2

In light of Remark 3.6, considering abelian surfaces without absolutely irreducible curves of small arithmetic genus will lead to a sharper lower bound on the minimum distance of the evaluation code  $\mathcal{C}(A, rH)$ . Hence in this section we look for abelian surfaces which satisfy the property not to contain absolutely irreducible curves defined over  $\mathbb{F}_q$  of arithmetic genus 0, 1 nor 2.

By the theorem of classification of Weil (see for instance [8, Th.1.3]), a principally polarized abelian surface defined over  $\mathbb{F}_q$  is isomorphic to either the polarized Jacobian of a curve of genus 2 over  $\mathbb{F}_q$ , either the product of two polarized elliptic curves over  $\mathbb{F}_q$  or either the Weil restriction from  $\mathbb{F}_{q^2}$  to  $\mathbb{F}_q$  of a polarized elliptic curve defined over  $\mathbb{F}_{q^2}$ . It is straightforward to see that the Jacobian of a curve of genus 2 contains the curve itself and that the product of two elliptic curves contains copies of each of them.

It therefore remains two cases to consider. First, there is the case of abelian surfaces which do not admit a principal polarization. We prove in Proposition 4.2 that they always satisfy the desired property. Secondly, we give in Proposition 4.3 necessary and sufficient conditions for Weil restrictions of elliptic curves to satisfy the same property.

Throughout this section we will make use of the two following well-known results. An abelian surface contains a *smooth* absolutely irreducible curve of genus 1 if and only if it is isogenous to the product of two elliptic curves. Moreover, a simple abelian surface contains a *smooth* absolutely irreducible curve of genus 2 if and only if it is isogenous to the Jacobian of a curve of genus 2 (see [4, Proposition 2]). The following lemma gives necessarily and sufficient conditions to avoid the presence of *non necessarily smooth* absolutely irreducible curves of low arithmetic genus.

**Lemma 4.1.** *Let  $A$  be an abelian surface. Then the three following statements are equivalent:*

- (1)  *$A$  is simple and not isogenous to a Jacobian surface;*
- (2)  *$A$  does not contain absolutely irreducible curves of arithmetic genus 0, 1 nor 2;*
- (3)  *$A$  does not contain absolutely irreducible smooth curves of genus 0, 1 nor 2.*

*Proof.* Let us prove that (1)  $\Rightarrow$  (2). Let  $A$  be a simple abelian surface which is not isogenous to the Jacobian of a curve of genus 2. Let  $C$  be an absolutely irreducible curve lying on  $A$  and let  $\nu : \tilde{C} \mapsto C$  be its normalisation map. The case of genus 0 and 1 is treated in [6, §2]. For the genus 2 case, assume by contradiction that  $\pi(C) = 2$ . We get  $g(\tilde{C}) = \pi(C) = 2$  so  $\tilde{C} = C$  is smooth and thus by Proposition 2 of [4]  $A$  is isogenous to the Jacobian of  $C$ , in contradiction with the hypotheses.

The implication (2)  $\Rightarrow$  (3) is trivial since for smooth curves the geometric and arithmetic genus coincide.

Finally let us prove that (3)  $\Rightarrow$  (1). Assume by contradiction that  $A$  is not simple, hence  $A$  is isogenous to the product of two elliptic curves and thus it contains at least a smooth absolutely irreducible curve of genus 1, in contradiction with (3). Now assume that  $A$  is simple and isogenous to a Jacobian surface. Then by Proposition 2 of [4],  $A$  contains a smooth absolutely irreducible curve of genus 2, again in contradiction with (3). This concludes the proof.  $\square$

**4.1. Non-principally polarized abelian surfaces.** An isogeny class of abelian varieties over  $\mathbb{F}_q$  is said to be not principally polarizable if it does not contain a principally polarizable abelian variety over  $\mathbb{F}_q$ . The following proposition states that abelian surfaces which do not admit a principal polarization have naturally the property we are searching for.

**Proposition 4.2.** *Let  $A$  be an abelian surface in a not principally polarizable isogeny class. Then  $A$  does not contain absolutely irreducible curves of arithmetic genus 0, 1 nor 2.*

*Proof.* It is well-known that an abelian variety contains no curves of genus 0. Since  $A$  is not isogenous to a principally polarizable abelian surface, it follows that it is not isogenous to a product of two elliptic curves nor to a Jacobian surface. By Lemma 4.1 we conclude the proof.  $\square$

To be concrete, let us recall here a characterisation of non-principally polarized isogeny class of abelian surfaces ([9, Th.1]) for which Theorem 3.3 applies with  $\ell = 2$ . An isogeny class of abelian surfaces defined over  $\mathbb{F}_q$  with Weil polynomial  $f(t) = t^4 + at^3 + bt^2 + qat + q^2$  is not principally polarizable if and only if the following three conditions are satisfied:

- (1)  $a^2 - b = q$ ;
- (2)  $b < 0$ ;
- (3) all prime divisors of  $b$  are congruent to 1 mod 3.

**4.2. Weil restrictions of elliptic curves.** Let  $k = \mathbb{F}_q$  and  $K$  denotes an extension of finite degree  $[K : k]$  of  $k$ . Let  $E$  be an elliptic curve defined over  $K$ . The  $K/k$ -Weil restriction of scalars of  $E$  is an abelian variety  $W_{K/k}(E)$  of dimension  $[K : k]$  defined over  $k$  (see [14, §16] for a presentation in terms of universal property and see [4, §3] for a constructive approach). We consider here the  $\mathbb{F}_{q^2}/\mathbb{F}_q$ -Weil restriction of an elliptic curve  $E$  defined over  $\mathbb{F}_{q^2}$  which is an abelian surface  $A$  defined over  $\mathbb{F}_q$ .

Let  $f_{E/\mathbb{F}_{q^2}}(t)$  be the Weil polynomial of the elliptic curve  $E$  defined over  $\mathbb{F}_{q^2}$ . Then the Weil polynomial of  $A$  over  $\mathbb{F}_q$  is given (see [3, Prop 3.1]) by

$$(17) \quad f_{A/\mathbb{F}_q}(t) = f_{E/\mathbb{F}_{q^2}}(t^2).$$

Since  $f_{E/\mathbb{F}_{q^2}}(t) = t^3 - \text{Tr}(E/\mathbb{F}_{q^2})t + q^2$  we have  $f_A(t) = t^6 - \text{Tr}(E/\mathbb{F}_{q^2})t^4 + q^2t^2$ , thus it follows from (8) that the trace of  $A$  over  $\mathbb{F}_q$  is equal to 0. Moreover,



since the number of  $\mathbb{F}_q$ -rational points on an abelian variety  $A$  defined over  $\mathbb{F}_q$  equals  $f_{A/\mathbb{F}_q}(1)$ , we get that the number of rational points on  $A = W_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E)$  over  $\mathbb{F}_q$  is the same as the number of rational points on  $E$  over  $\mathbb{F}_{q^2}$ , i.e. we have  $\#A(\mathbb{F}_q) = f_{A/\mathbb{F}_q}(1) = f_{E/\mathbb{F}_{q^2}}(1) = \#E(\mathbb{F}_{q^2})$ .

**Proposition 4.3.** *Let  $q$  be a power of a prime  $p$ . Let  $E$  be an elliptic curve defined over  $\mathbb{F}_{q^2}$  of Weil polynomial  $f_{E/\mathbb{F}_{q^2}}(t) = t^2 - \text{Tr}(E/\mathbb{F}_{q^2})t + q^2$ . Let  $A$  be the  $\mathbb{F}_{q^2}/\mathbb{F}_q$ -Weil restriction of the elliptic curve  $E$ . Then  $A$  does not contain absolutely irreducible curves defined over  $\mathbb{F}_q$  of arithmetic genus 0, 1 nor 2 if and only if one of the following conditions holds*

- (1)  $\text{Tr}(E/\mathbb{F}_{q^2}) = 2q - 1$ ;
- (2)  $p > 2$  and  $\text{Tr}(E/\mathbb{F}_{q^2}) = 2q - 2$ ;
- (3)  $p \equiv 11 \pmod{12}$  or  $p = 3$ ,  $q$  is a square and  $\text{Tr}(E/\mathbb{F}_{q^2}) = q$ ;
- (4)  $p = 2$ ,  $q$  is nonsquare and  $\text{Tr}(E/\mathbb{F}_{q^2}) = q$ ;
- (5)  $q = 2$  or  $q = 3$  and  $\text{Tr}(E/\mathbb{F}_{q^2}) = 2q$ .

*Proof.* Let  $E$  be an elliptic curve defined over  $\mathbb{F}_{q^2}$  and let  $A$  be the  $\mathbb{F}_{q^2}/\mathbb{F}_q$ -Weil restriction of  $E$ . Let  $f_A(t) = t^4 + at^3 + bt^2 + qat + q^2$  be the Weil polynomial of  $A$ . Recall that we have  $f_A(t) = t^4 - \text{Tr}(E/\mathbb{F}_{q^2})t^2 + q^2$  by (17) and thus  $(a, b) = (0, -\text{Tr}(E/\mathbb{F}_{q^2}))$ . Theorem 1.2-(2) with Table 1.2 in [8] gives necessary and sufficient conditions on the couple  $(a, b)$  for a simple abelian surface with the corresponding Weil polynomial not to be isogenous to the Jacobian of a smooth curve of genus 2.

Let us suppose that the trace of the elliptic curve  $E$  over  $\mathbb{F}_{q^2}$  does not fit one of the conditions (1) – (5). Let us remark that by Theorem 1.4 in [8] the first case of Table 1.2 in [8, Theorem 1.2-(2)] corresponds to all simple abelian surfaces which do not admit a principal polarization. Moreover the cases (1) – (5) cover the remaining cases of Table 1.2. Then  $f_A(t)$  does not represent an isogeny class of simple principally polarizable abelian surfaces not containing a Jacobian surface. Hence  $A$  is either not principally polarizable, or not simple or isogenous to the Jacobian of a curve of genus 2. In the first case  $A$  would not be a Weil restriction of an elliptic curve since these last one admit a principal polarization. In the second case,  $A$  would contain a curve of genus 1 and finally in the third case it would contain a curve of genus 2. Thus we proved that if  $A$  does not contain absolutely irreducible curves defined over  $\mathbb{F}_q$  of arithmetic genus 0, 1 nor 2 then one of conditions (1) – (5) holds.

Conversely, using again Table 1.2 in [8, Theorem 1.2-(2)] we get that in each case from (1) to (5) of our proposition, the couple  $(0, -\text{Tr}(E/\mathbb{F}_{q^2}))$  corresponds to simple abelian surfaces not isogenous to the Jacobian of a curve of genus 2. Therefore in these cases  $A$  does not contain absolutely irreducible *smooth* curves of geometric genus 0, 1 nor 2, and thus by Lemma 4.1,  $A$  does not contain absolutely irreducible curves of arithmetic genus 0, 1 nor 2.  $\square$

**Remark 4.4.** Let us mention two cases in which Weil restrictions of elliptic curves do contain curves of genus 1 or 2. First, if the elliptic curve  $E$  is defined over  $\mathbb{F}_q$ , it is clearly a subvariety of  $A$ . Note that in Proposition 4.3 we do not need to suppose that the elliptic curve  $E$  defined over  $\mathbb{F}_{q^2}$  is not defined over  $\mathbb{F}_q$  because none of the the elliptic curves with trace over  $\mathbb{F}_{q^2}$  as in cases (1)-(5) is defined over  $\mathbb{F}_q$ . Secondly, it is well-known that there are Weil restrictions of elliptic curves that are isogenous to Jacobian surfaces (see for example [17]) which thus contain smooth curves of genus 2.

**Remark 4.5.** Let  $q^2 = p^{2n}$  with  $p$  prime. By Deuring theorem (see for instance [22, Th. 4.1]) for every integer  $\beta$  satisfying  $|\beta| \leq 2q$  such that  $\gcd(\beta, p) = 1$ , or  $\beta = \pm 2q$ , or  $\beta = \pm q$  and  $p \not\equiv 1 \pmod{3}$ , there exists an elliptic curve of trace  $\beta$  over  $\mathbb{F}_{q^2}$ . Using Deuring theorem it is easy to check the existence of an elliptic curve with the given trace for each of the five cases in the previous theorem.

**Remark 4.6.** Let us remark that the first bound in Theorem 3.3 becomes relevant for  $q \geq B$  with  $B \approx 4(\sqrt{H^2 + 1})^2$  and it is non-relevant for small  $q$ . Therefore case (5) of Proposition 4.3 does not give rise to practical cases.

Let us briefly outline the results obtained in the last sections. The surfaces arising in Propositions 4.2 and 4.3 give rise to codes for which the lower bound on the minimum distance of Theorem 3.3 applies with  $\ell = 2$ . This is exactly the purpose of the proposition stated in the introduction.

We have exploited the fact that, for  $q$  sufficiently large and  $r = q^\rho$  with  $0 < \rho < \frac{1}{2}$ , the bound obtained for  $\ell = 2$  improves the one obtained for  $\ell = 1$ . Note also that under the same hypotheses the bound for  $\ell = 3$  improves the one for  $\ell = 2$ . Hence it would be interesting in the future to investigate on the existence of abelian surfaces without absolutely irreducible curves of genus  $\leq 3$  lying on them.

## 5. TO MAKE EXPLICIT THE LOWER BOUNDS FOR THE MINIMUM DISTANCE

We now show how the terms  $\#A(\mathbb{F}_q)$ ,  $\text{Tr}(A)$  and  $H^2$  appearing in the lower bounds for the minimum distance  $d(A, rH)$  given in Theorems 2.2 and 3.3 can be computed in many cases. As already said in the introduction of Section 4, three cases have to be distinguished in the case of principally polarized abelian surfaces, according to Weil classification.

Let  $A$  be a principally polarized abelian surface defined over  $\mathbb{F}_q$  with Weil polynomial  $f_A(t) = (t - \omega_1)(t - \bar{\omega}_1)(t - \omega_2)(t - \bar{\omega}_2)$  where the  $\omega_i$ 's are complex numbers of modulus  $\sqrt{q}$ . Then we get:

$$\#A(\mathbb{F}_q) = f_A(1) = (1 - \omega_1)(1 - \bar{\omega}_1)(1 - \omega_2)(1 - \bar{\omega}_2).$$

From formula (8), we obtain:

$$\text{Tr}(A) = \omega_1 + \bar{\omega}_1 + \omega_2 + \bar{\omega}_2.$$

Moreover, for any divisor  $H$  on  $A$ , the adjunction formula gives

$$H^2 = 2\pi_H - 2.$$

As recalled in Section 2, if the divisor  $H$  is ample then  $rH$  is very ample as soon as  $r \geq 3$ .

- (1) In case  $A$  is the Jacobian  $\text{Jac}(C)$  of a genus-2 curve  $C$  defined over  $\mathbb{F}_q$ , the numerator  $P_C(t)$  of the zeta function of  $C$  is equal to the reciprocal polynomial of the Weil polynomial  $f_{\text{Jac}(C)}(t)$ :

$$P_C(t) = t^4 f_{\text{Jac}(C)}\left(\frac{1}{t}\right) = (1 - \omega_1 t)(1 - \bar{\omega}_1 t)(1 - \omega_2 t)(1 - \bar{\omega}_2 t).$$

Hence we obtain

$$\begin{cases} \#C(\mathbb{F}_q) &= q + 1 - (\omega_1 + \bar{\omega}_1 + \omega_2 + \bar{\omega}_2) \\ \#C(\mathbb{F}_{q^2}) &= q^2 + 1 - (\omega_1^2 + \bar{\omega}_1^2 + \omega_2^2 + \bar{\omega}_2^2) \end{cases}$$

and thus

$$\#\text{Jac}(C)(\mathbb{F}_q) = \frac{1}{2}(\#C(\mathbb{F}_{q^2}) + \#C(\mathbb{F}_q)^2) - q.$$

Now, choosing  $H = C$  for instance, we get an ample divisor with  $H^2 = C^2 = 2\pi_C - 2 = 2$ .

- (2) In case  $A$  is the product  $E_1 \times E_2$  of two elliptic curves  $E_1$  and  $E_2$  each partial trace  $\text{Tr}(E_i) = \omega_i + \bar{\omega}_i$  is determined by  $\#E_i(\mathbb{F}_q) = q + 1 - \text{Tr}(E_i)$ . So we have  $\#A(\mathbb{F}_q) = \#E_1(\mathbb{F}_q) \times \#E_2(\mathbb{F}_q)$  and  $\text{Tr}(A) = \text{Tr}(E_1) + \text{Tr}(E_2)$ .

Any choice of rational points  $P_i \in E_i$  leads to an ample divisor  $H = E_1 \times \{P_2\} + \{P_1\} \times E_2$  such that  $H^2 = (E_1 \times \{P_2\})^2 + (\{P_1\} \times E_2)^2 + 2(E_1 \times \{P_2\}) \cdot (\{P_1\} \times E_2) = 0 + 0 + 2 \times 1 = 2$ .

- (3) In the last case where  $A = W_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E)$  is the  $\mathbb{F}_{q^2}/\mathbb{F}_q$ -Weil restriction of an elliptic curve  $E$  defined over  $\mathbb{F}_{q^2}$ , then we have already seen in Subsection 4.2 that  $\#A(\mathbb{F}_q) = \#E(\mathbb{F}_{q^2})$  and that  $\text{Tr}(A) = 0$ .

As an ample divisor on  $A$ , one can choose for instance  $H = E + E^q$  where  $E^q$  is the image of  $E$  by the generator  $\sigma : x \mapsto x^q$  of the Galois group  $\text{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ . We thus have  $H^2 = E^2 + (E^q)^2 + 2E \cdot E^q = 0 + 0 + 2 \times 1 = 2$ .

**Acknowledgments:** The authors would like to thank the anonymous referee for relevant observations and in particular for advices which have led to a sharper form of Theorem 3.3.

## REFERENCES

- [1] Y. Aubry. “Algebraic geometric codes on surfaces”. Talk at Eurocode’92 - International symposium on coding theory and applications (1992, Udine, Italie), in Ph.D. thesis of the University of Aix-Marseille II, France (1993), hal-00979000. 1992.
- [2] A. Couvreur. “Construction of rational surfaces yielding good codes”. In: *Finite Fields Appl.* 17.5 (2011), pp. 424–441. ISSN: 1071-5797. DOI: [10.1016/j.ffa.2011.02.007](https://doi.org/10.1016/j.ffa.2011.02.007).
- [3] S. D. Galbraith. “Limitations of constructive Weil descent”. In: *Public-key cryptography and computational number theory (Warsaw, 2000)*. de Gruyter, Berlin, 2001, pp. 59–70.
- [4] S. D. Galbraith and N. P. Smart. “A cryptographic application of Weil descent”. In: *Cryptography and coding (Cirencester, 1999)*. Vol. 1746. Lecture Notes in Comput. Sci. Springer, Berlin, 1999, pp. 191–200. DOI: [10.1007/3-540-46665-7\\_23](https://doi.org/10.1007/3-540-46665-7_23).
- [5] V. D. Goppa. “Codes on algebraic curves”. In: *Dokl. Akad. Nauk SSSR* 259.6 (1981), pp. 1289–1290. ISSN: 0002-3264.
- [6] S. Haloui. “Codes from Jacobian surfaces”. In: *Arithmetic, geometry, cryptography and coding theory*. Vol. 686. Contemp. Math. Amer. Math. Soc., Providence, RI, 2017, pp. 123–135.
- [7] R. Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.
- [8] E. W. Howe, E. Nart, and C. Ritzenthaler. “Jacobians in isogeny classes of abelian surfaces over finite fields”. In: *Ann. Inst. Fourier (Grenoble)* 59.1 (2009), pp. 239–289. ISSN: 0373-0956.
- [9] E. W. Howe et al. “Principally polarizable isogeny classes of abelian surfaces over finite fields”. In: *Math. Res. Lett.* 15.1 (2008), pp. 121–127. ISSN: 1073-2780. DOI: [10.4310/MRL.2008.v15.n1.a11](https://doi.org/10.4310/MRL.2008.v15.n1.a11).
- [10] G. Lachaud. “Number of points of plane sections and linear codes defined on algebraic varieties”. In: *Arithmetic, geometry and coding theory (Luminy, 1993)* (1996), pp. 77–104.
- [11] S. Lang. *Abelian varieties*. Reprint of the 1959 original. Springer-Verlag, New York-Berlin, 1983, pp. xii+256. ISBN: 0-387-90875-7.
- [12] J. Little and H. Schenck. “Codes from surfaces with small Picard number”. In: *SIAM J. Appl. Algebra Geom.* 2.2 (2018), pp. 242–258. ISSN: 2470-6566. DOI: [10.1137/17M1128277](https://doi.org/10.1137/17M1128277).
- [13] J. Little and H. Schenck. “Toric surface codes and Minkowski sums”. In: *SIAM J. Discrete Math.* 20.4 (2006), pp. 999–1014. ISSN: 0895-4801. DOI: [10.1137/050637054](https://doi.org/10.1137/050637054).
- [14] J. S. Milne. *Algebraic Geometry (v6.02)*. Available at [www.jmilne.org/math/](http://www.jmilne.org/math/). 2017.

- [15] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970, pp. viii+242.
- [16] J. Nardi. “Algebraic geometric codes on minimal Hirzebruch surfaces”. In: *J. Algebra* 535 (2019), pp. 556–597. ISSN: 0021-8693. DOI: [10.1016/j.jalgebra.2019.06.022](https://doi.org/10.1016/j.jalgebra.2019.06.022).
- [17] J. Scholten. “Weil restriction of an elliptic curve over a quadratic extension”. Preprint. 2003.
- [18] M. A. Tsfasman, S. G. Vlăduț, and T. Zink. “Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound”. In: *Math. Nachr.* 109 (1982), pp. 21–28. ISSN: 0025-584X. DOI: [10.1002/mana.19821090103](https://doi.org/10.1002/mana.19821090103).
- [19] M. Tsfasman, S. G. Vlăduț, and D. Nogin. *Algebraic geometric codes: basic notions*. Vol. 139. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, 2007, pp. xx+338. ISBN: 978-0-8218-4306-2. DOI: [10.1090/surv/139](https://doi.org/10.1090/surv/139).
- [20] S. G. Vlăduț and Y. I. Manin. “Linear codes and modular curves”. In: *Journal of Soviet Mathematics* 30.6 (1985), pp. 2611–2643. ISSN: 1573-8795. DOI: [10.1007/BF02249124](https://doi.org/10.1007/BF02249124).
- [21] J. F. Voloch and M. Zarzar. “Algebraic geometric codes on surfaces”. In: *Arithmetics, geometry, and coding theory (AGCT 2005)*. Vol. 21. Sémin. Congr. Soc. Math. France, Paris, 2010, pp. 211–216.
- [22] W. C. Waterhouse. *Abelian varieties over finite fields*. Thesis (Ph.D.)—Harvard University. ProQuest LLC, Ann Arbor, MI, 1968.
- [23] M. Zarzar. “Error-correcting codes on low rank surfaces”. In: *Finite Fields Appl.* 13.4 (2007), pp. 727–737. ISSN: 1071-5797. DOI: [10.1016/j.ffa.2007.05.001](https://doi.org/10.1016/j.ffa.2007.05.001).

Yves Aubry, INSTITUT DE MATHÉMATIQUES DE TOULON - IMATH,  
UNIVERSITÉ DE TOULON AND INSTITUT DE MATHÉMATIQUES DE MARSEILLE - I2M,  
AIX MARSEILLE UNIVERSITÉ, CNRS, CENTRALE MARSEILLE, UMR 7373, FRANCE  
*E-mail address:* [yves.aubry@univ-tln.fr](mailto:yves.aubry@univ-tln.fr)

Elena Berardini, INSTITUT DE MATHÉMATIQUES DE MARSEILLE - I2M,  
AIX MARSEILLE UNIVERSITÉ, CNRS, CENTRALE MARSEILLE, UMR 7373, FRANCE  
*E-mail address:* [elena\\_berardini@hotmail.it](mailto:elena_berardini@hotmail.it)

Fabien Herbaut, INSPE NICE-TOULON, UNIVERSITÉ CÔTE D’AZUR,  
INSTITUT DE MATHÉMATIQUES DE TOULON - IMATH, UNIVERSITÉ DE TOULON, FRANCE  
*E-mail address:* [fabien.herbaut@univ-cotedazur.fr](mailto:fabien.herbaut@univ-cotedazur.fr)

Marc Perret, INSTITUT DE MATHÉMATIQUES DE TOULOUSE, UMR 5219,  
UNIVERSITÉ DE TOULOUSE, CNRS, UT2J, F-31058 TOULOUSE, FRANCE  
*E-mail address:* [perret@univ-tlse2.fr](mailto:perret@univ-tlse2.fr)