LMS J. Comput. Math. 18 (1) (2015) 419–443
doi:10.1112/S1461157015000091

Heuristics on pairing-friendly abelian varieties

John Boxall and David Gruenewald

Abstract

We discuss heuristic asymptotic formulae for the number of isogeny classes of pairing-friendly abelian varieties of fixed dimension $g \geqslant 2$ over prime finite fields. In each formula, the embedding degree $k \geqslant 2$ is fixed and the rho-value is bounded above by a fixed real $\rho_0 > 1$. The first formula involves families of ordinary abelian varieties whose endomorphism ring contains an order in a fixed CM-field K of degree g and generalizes previous work of the first author when $g = 1$. It suggests that, when $\rho_0 < g$, there are only finitely many such isogeny classes. On the other hand, there should be infinitely many such isogeny classes when $\rho_0 > g$. The second formula involves families whose endomorphism ring contains an order in a fixed totally real field K_0^+ of degree g. It suggests that, when $\rho_0 > 2g/(g+2)$ (and in particular when $\rho_0 > 1$ if $g = 2$), there are infinitely many isogeny classes of g-dimensional abelian varieties over prime fields whose endomorphism ring contains an order of K_0^+. We also discuss the impact that polynomial families of pairing-friendly abelian varieties has on our heuristics, and review the known cases where they are expected to provide more isogeny classes than predicted by our heuristic formulae.

1. *Introduction*

Pairing-based cryptography uses non-degenerate pairings defined on a product $G_1 \times G_2$ of two abelian groups and taking values in a third abelian group G_3. Typically, G_1, G_2 and G_3 are cyclic groups of the same prime order r. An important source of suitable groups is elliptic curves over finite fields, and in recent years generalizations using higher-dimensional abelian varieties have been proposed.

As we shall recall briefly below, elliptic curves or abelian varieties possessing suitable subgroups for pairing-based cryptography satisfy very strong conditions, and are loosely referred to as pairing-friendly. These conditions suggest that they are very rare, and various estimates concerning their number (either unconditional or depending on certain hypotheses) have been discussed, both for elliptic curves [**1**, **15**, **19**] and also for Jacobians of genus two curves [**13**, **18**]. In [**5**], one of the authors investigated a heuristic asymptotic formula for the number of pairing-friendly elliptic curves over prime fields; the purpose of the present paper is to present and provide computational evidence for generalizations of this to higher-dimensional abelian varieties.

1.1. *Background*

Let q be a power of a prime p and let $\mathbb{F}_q$ denote a finite field with q elements. Let A be an abelian variety over $\mathbb{F}_q$ of dimension $g \geqslant 1$. Let π be the Frobenius endomorphism of A over $\mathbb{F}_q$, let $\ell \neq p$ be a prime and let C_π be the characteristic polynomial of the action π on the ℓ-adic

Received 7 October 2013; revised 20 February 2015.

2010 Mathematics Subject Classification 11G10, 11N45, 11T71 (primary), 14K15 (secondary).

Most of the work on this paper was undertaken while the authors participated in the project *Pairings and Advances in Cryptology for E-cash (PACE)* funded by the Agence Nationale de la Recherche (project reference ANR-07-TCOM-0013). The final version was completed when the first author participated in the ANR-funded project *SIM and PAiring Theory for Information and Communications Security (SIMPATIC)* (project reference ANR-12-INSE-0014).

Tate module of A. Then Weil [27] showed that C_π is a monic polynomial of degree $2g$ with integer coefficients that is independent of ℓ. Furthermore, he proved that the complex roots of C_π are *q-Weil numbers*, in other words algebraic integers of which any complex conjugate π satisfies $\pi\bar{\pi} = q$. In general, by a *q-Weil polynomial* we mean a monic polynomial with integer coefficients all of whose roots are q-Weil numbers. Thus, C_π is a q-Weil polynomial of degree $2g$, and Tate [24] showed that C_π depends only on the isogeny class of A. Furthermore, the order of the group $A(\mathbb{F}_q)$ is equal to $C(1)$, so that the order of $A(\mathbb{F}_q)$ is invariant under isogeny.

A classification result was proved by Honda and Tate [14, 25]. They proved that there is a bijection between the set of $\mathbb{F}_q$-isogeny classes of simple abelian varieties and the set of *irreducible* Weil polynomials. Explicitly, the bijection associates to the isogeny class of the simple abelian variety A the minimal polynomial M_π of the Frobenius endomorphism π of A. The characteristic polynomial C_π is then a suitable power of M_π, so that $2\dim A$ is an even multiple of the degree of M_π. For a detailed study of this and related questions, we refer to [26]. We simply mention the following result, which is part of [12, Lemma 2.2] and is proved using results in [26].

PROPOSITION 1.1. *Let $g \geqslant 1$ be an integer, let p be a prime and let C be an irreducible p-Weil polynomial of degree $2g$. Then the simple abelian varieties over $\mathbb{F}_p$ whose Frobenius endomorphism has minimal polynomial C have dimension g.*

In what follows, if $g_0 \geqslant 1$ is an integer, we understand by a *triple of degree g_0* (or simply a triple if the reference to g_0 is clear) a triple (r, C, q), where r is a prime, q a power of a prime, C a q-Weil polynomial of degree $2g_0$ and r divides $C(1)$. By our previous remarks, we can associate to (the isogeny class of) any pairing-friendly g-dimensional abelian variety A over $\mathbb{F}_q$ a triple (r, C, q) of degree g, where r is a prime such that $A(\mathbb{F}_q)$ contains a subgroup G_1 of order r and C is the characteristic polynomial of the Frobenius endomorphism of A over $\mathbb{F}_q$. Conversely, if $q = p$ is prime and C is irreducible of degree $2g$, Proposition 1.1 implies that if r is any prime dividing $C(1)$, then (r, C, p) corresponds to an isogeny class of simple abelian varieties A over $\mathbb{F}_p$ such that $A(\mathbb{F}_p)$ contains a subgroup G_1 of order r.

We now describe the conditions that a triple (r, C, q) as above must satisfy assuming that it is associated to an isogeny class of abelian varieties A that are pairing-friendly. We refer to [11] (in the case of elliptic curves) and [10] (in any dimension) for background and motivation.

By definition, the *rho-value* of the triple is $\rho = \rho(A) = \rho(r, C, q) = g \log q / \log r$, where A is any member of the corresponding isogeny class and g is the dimension of A.

(1) Since $\#A(\mathbb{F}_q) = C_\pi(1)$, it follows from the fact that the roots of C_π are q-Weil numbers that $(\sqrt{q} - 1)^{2g} \leqslant \#A(\mathbb{F}_q) \leqslant (\sqrt{q} + 1)^{2g}$. We deduce that, assuming that g is fixed and given any $\rho_0 < 1$, we must have $\rho > \rho_0$ whenever q is sufficiently large. In cryptographic applications, we want ρ to be as close to 1 as possible, since, for fixed r, computations in the field $\mathbb{F}_q$ will be faster.

(2) There exists an integer $k \geqslant 2$ such that r divides $\Phi_k(q)$. Here, Φ_k is the kth cyclotomic polynomial. (Some authors allow $k = 1$, but we shall exclude this case. See Remark 3.4.) Under some further mild restrictions, $A(\mathbb{F}_{q^k})$ contains a subgroup G_2 of order r different from G_1 and there is a computable non-degenerate pairing on $G_1 \times G_2$ that takes values in the rth roots of unity in $\mathbb{F}_{q^k}$ (see for example [1] when $g = 1$ and [21, Theorem 3.1]). We need to choose k in such a way that the discrete logarithm problem in the field generated over the prime field $\mathbb{F}_p$ by the rth roots of unity is unfeasible, but not so large that the computations in the field $\mathbb{F}_{q^k}$ become unwieldy. We call k the *embedding degree* and k/g the *security ratio* of the triple (or of any abelian variety in the corresponding isogeny class). At present, the security ratio is in practice bounded by about 50 when $g = 1$ (see [11]). Although larger values of k will be needed to maintain the same security level when g-dimensional abelian varieties are used, it is natural to consider k as constant.

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

Thus, when searching for abelian varieties of dimension g for use in pairing-based cryptography, we seek triples (r, C, q) with small embedding degree k and rho-value as close to 1 as possible. Once a suitable triple (r, C, q) has been found, it is necessary to compute equations for some member of the corresponding isogeny class, the groups G_1 and G_2 and to be able to compute the pairing. The only known method of constructing such abelian varieties is the CM-method, which is based on the reduction at primes above p of abelian varieties over number fields having complex multiplication, these being in turn constructed using theta functions or modular invariants. It is possible at present to construct elliptic curves with complex multiplication by the maximal order of an imaginary quadratic field whose discriminant is as large as about 10^{15} (see [**9**]). On the other hand, only a few thousand explicit equations of genus two curves whose Jacobians have complex multiplication are known at present (see [**16**]). Since this is computationally very heavy, it seems reasonable to consider triples that can be obtained from the reduction of a *fixed* abelian variety, at least up to twist.

1.2. *Presentation of the paper*

Until now, when $g > 1$, no examples of triples (r, C, q) of cryptographic interest with rho-value less than or equal to g have been found. When $g = 2$ and $k = 5$ or $k = 10$, a method discussed in [**13**] (see also Remark 7.8 below) does give rise to triples with rho-value close to 1, but the corresponding abelian varieties cannot be constructed using the CM-method. The motivation that led to the present paper was an attempt to understand the reasons for this, and our main purpose is to discuss two heuristic estimates (see Estimates 3.2 and 5.1) related to the asymptotic growth as $x \to \infty$ for the number of triples (r, C, p) of given degree g with $r \leqslant x$, under certain conditions on the rho-value $g(\log p/\log r)$ and the polynomial C.

In order to state these estimates formally, we need to consider triples of the form (r, π, q), where r is a prime and π is a q-Weil number such that, if K is any number field containing π, r divides the $K/\mathbb{Q}$-norm $\mathrm{N}_{K/\mathbb{Q}}(\pi - 1)$ of $\pi - 1$. This is because our heuristic arguments will be based mostly on the geometry of number fields. See Remarks 3.3 and 5.2 for how to interpret heuristics for triples (r, π, q) in terms of triples (r, C, q). We say that (r, π, q) has *embedding degree* k if r divides $\Phi_k(q)$. If $2g$ is an even multiple of the degree of the number field $\mathbb{Q}(\pi)$, we define the *degree* g *rho-value* of (r, π, q) to be $g(\log q/\log r)$. If $2g$ is equal to the degree of $\mathbb{Q}(\pi)$, we simply call this the rho-value.

From now on, we mostly restrict attention to triples (r, π, p) with p a prime. By Proposition 1.1, such triples do correspond to isogeny classes of abelian varieties over prime fields. We write a triple as (r, π, q) when we discuss matters in relation to arbitrary finite fields, it being understood that q is a power of the prime p.

To avoid repetition, we restrict attention to $g \neq 1$, referring the reader to [**5**, **22**] for discussions of the elliptic curves case.

In both estimates we fix integers $g \geqslant 2$, $k \geqslant 2$ and a real number $\rho_0 > 1$ and suppose that the rho-value $g(\log p/\log r)$ is bounded above by ρ_0. For a simple reason that will become clear in Lemma 3.1, we in fact need to suppose $\rho_0 > g/\varphi(k)$, where φ is Euler's totient function.

ESTIMATE 1.2. Let $g \geqslant 2$, $k \geqslant 2$ be integers and let $\rho_0 > \max(1, g/\varphi(k))$ be a real number such that $\rho_0 \neq g$. Fix a CM-field K of degree $2g$ and a CM-type Φ on K. Assume that we are not in the situation considered in Remark 7.7. Let $N(k, K, \Phi, \rho_0, x)$ denote the number of triples (r, π, p) with embedding degree k, with $\pi \in K$, with $r \leqslant x$ and with $p \leqslant r^{\rho_0/g}$ that come from Φ. Then there is an explicit constant $\alpha > 0$ depending only on k and K such that we have

$$N(k, K, \Phi, \rho_0, x) \sim \frac{\alpha}{\rho_0} \int_2^x \frac{u^{(\rho_0/g)-2}\, du}{(\log u)^2} \tag{1.1}$$

as $x \to \infty$.

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

Here and elsewhere in the paper, $\sim$ denotes asymptotic equivalence, in the sense that the ratio of the two terms tends to 1 as $x \to \infty$. A more precise statement giving the value of α is to be found in Estimate 3.2. We refer to § 2 for the definition of the notion that (r, π, p) comes from Φ. In addition, we have excluded the possibility $\rho_0 = g$ since this is a borderline case, the integral being bounded as $x \to \infty$ when $\rho_0 \leqslant g$ and unbounded when $\rho_0 > g$. This observation together with Proposition 1.1 and the fact that there are only finitely many CM-types on a given CM-field K implies the following corollary.

COROLLARY 1.3. *Let notation and hypotheses be as in Estimate 1.2 and assume that (1.1) is correct. If $\rho_0 < g$, then there are only finitely many isogeny classes of g-dimensional abelian varieties over prime finite fields whose endomorphism ring contains an order of K that have embedding degree k and rho-value bounded above by ρ_0. If $\rho_0 > g$ and if at least one of the CM-types on K is primitive, then there are infinitely many such isogeny classes.*

The proof of the final sentence also uses Proposition 2.3 below. In fact, the conclusion of Corollary 1.3 also holds in the situation considered in Remark 7.7, as we shall explain there.

Since our initial motivation was the search for abelian varieties with rho-value close to 1, we were led by the corollary to study asymptotics for triples (r, π, q) where the Weil numbers π were allowed to vary over larger sets.

ESTIMATE 1.4. Let $g \geqslant 1$ be an integer, let K_0^+ be a totally real field of degree g, let $k \geqslant 2$ be an integer and let $\rho_0 > \max(1, g/\varphi(k))$ be a real number with $\rho_0 \neq 2g/(g+2)$. Assume that we are not in the situation considered in Remark 7.8 below. Let $R(k, K_0^+, \rho_0, x)$ denote the number of triples (r, π, p) with embedding degree k, with π a root of an equation of the form $x^2 - \tau x + p$, where τ is an algebraic integer of K_0^+ all of whose conjugates satisfy $|\tau| \leqslant 2\sqrt{p}$, and $r \leqslant x$. Then there is a constant $\beta > 0$ such that, as $x \to \infty$, we have the asymptotic equivalence

$$R(k, K_0^+, \rho_0, x) \sim \frac{\beta}{\rho_0} \int_2^x \frac{u^{\rho_0(1/2+1/g)-2}\, du}{(\log u)^2}. \tag{1.2}$$

The precise value of β will be given in Estimate 5.1. The integral in (1.2) remains bounded as $x \to \infty$ if and only if $\rho_0 \leqslant 2g/(g+2)$, which explains why we exclude the boundary case $\rho_0 = 2g/(g+2)$. A glance at formulae (1.1) and (1.2) shows that the contribution from all the quadratic CM-extensions of K_0^+ is greater than that of one such extension K, as would be expected.

COROLLARY 1.5. *Let notation and hypotheses be as in Estimate 1.4 and suppose that (1.2) is correct. If $\rho_0 < 2g/(g+2)$, then there are only finitely many isogeny classes of g-dimensional abelian varieties over prime finite fields whose endomorphism ring contains an order of K_0^+ that have embedding degree k and rho-value bounded above by ρ_0. If $\rho_0 > 2g/(g+2)$, then there are infinitely many such isogeny classes provided that there is an infinite subset of the triples (r, π, p) of Estimate 1.4 for which π is of degree $2g$ over $\mathbb{Q}$ and the extension $\mathbb{Q}(\pi)/\mathbb{Q}$ is unramified at p.*

Again, the last sentence follows from Proposition 2.3 and Corollary 2.2. The hypothesis that there are infinitely many triples with π of degree $2g$ over $\mathbb{Q}$ and $\mathbb{Q}(\pi)/\mathbb{Q}$ unramified at p is a reasonable one; in fact it is reasonable to suppose that the proportion of triples with $r \leqslant x$ which do not satisfy this property tends to 0 as $x \to \infty$.

By definition, polynomial families parametrize the primes r and p appearing in triples (r, π, p) using values at integers of polynomials r_0 and p_0 of degrees $\deg r_0$ and $\deg p_0$ with

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

rational coefficients. A well-known example is the Barreto–Naehrig family that parametrizes a family of elliptic curves (see [**2**] and Remark 7.7 below). The *generic rho-value* is by definition $g(\deg p_0/\deg r_0)$ and, as the parameter w tends to infinity, the rho-values of the triples in the family tend to the generic rho-value. Detailed definitions are given in § 7, the discussion there being similar to that of [**5**, § 3]. As in the case of elliptic curves, polynomial families of dimension g having generic rho-value less than $g(1 + (1/\deg r_0))$ can be expected to contain more triples (r, π, p) than predicted by the heuristics of § 3 and those with generic rho-value less than $(2g/(g + 2))(1+(1/\deg r_0))$ should contain more triples than predicted by the heuristics of § 5. These statements are made precise in § 7 and Remarks 7.7 and 7.8 contain a discussion of the only known cases where this occurs.

1.3. *Contents of the paper and outline of the methods involved*

We now outline briefly the contents of the paper. In § 2, we recall some basic properties of CM-fields, CM-types and Weil numbers, and define the notion of a Weil number that comes from a given CM-type. In particular, we prove Theorem 2.4 on the asymptotic growth of the number of Weil numbers in a CM-field. In § 3, we state Estimate 3.2 and give a heuristic argument in favour of it. Numerical computations in relation to Estimate 3.2 are discussed in § 4. In § 5, we state Estimate 5.1 and present a heuristic argument that leads to it. The following § 6 presents numerical computations in relation to the heuristics of § 5. In the final § 7, we discuss the effect of polynomial families on the asymptotic formulae discussed in §§ 3 and 5.

We end the introduction with a few brief remarks on the nature of the heuristic arguments used. The argument leading to Estimate 3.2 is inspired by well-known generalizations to number fields of Dirichlet's theorem on arithmetic progressions and the prime number theorem (see for example [**20**, Chapter VII, § 2]). In particular, we use Theorem 2.4. In addition to methods from analytic number theory, the heuristic leading to Estimate 5.1 is based on simple properties of K_0^+ coming from the geometry of numbers. Also, implicit in both estimates are very strong uniformity hypotheses on the distribution of the roots of cyclotomic polynomials modulo primes that go far beyond what is currently known at least when ρ_0 is small.

Similarly, the arguments in § 7 on the asymptotic growth of the number of triples belonging to a polynomial family are heuristic, since they depend on the heuristics of Bateman and Horn [**3**] and Conrad [**8**] on the asymptotic growth of the number of integers at which a given finite set of polynomials simultaneously takes simultaneously prime values.

2. *Notation and review of CM-types and Weil numbers*

2.1. *Notation and review of CM-types*

We begin by fixing some notation and reviewing some simple properties of CM-types. Let ζ_k denote a primitive kth root of unity. If F is a number field, we denote by $e(k, F)$ the degree of the number field $F \cap \mathbb{Q}(\zeta_k)$. This is well defined since $\mathbb{Q}(\zeta_k)$ is a Galois extension of $\mathbb{Q}$. Let w_F denote the number of roots of unity in F and h_F the class number of F. We write $\mathrm{N}_{F/\mathbb{Q}}$ for the absolute norm from F to $\mathbb{Q}$, applied to elements or to ideals. If $\alpha \in F$ and if σ is an embedding of F in another field or an automorphism of F, we write α^σ for the image of α under σ. If F is a CM-field, we denote by F^+ the maximal real subfield of F and by c the non-trivial automorphism of F that fixes F^+. We often write $\overline{\alpha}$ for the image of $\alpha \in F$ under c.

We briefly review the notion of CM-types, referring to [**23**, Chapter 2] for details. A *CM-type* is a pair (K, Φ) (or simply Φ if the reference to K is clear) consisting of a CM-field K and a set Φ of g embeddings $\phi : K \to \mathbb{C}$ such that $\Phi \cup c\Phi$ is the set of all embeddings of K in $\mathbb{C}$. Let L denote a fixed Galois closure of K, so that L is also a CM-field. Then, fixing an embedding of L in $\mathbb{C}$, we can view a CM-type Φ as a set of embeddings of K in L.

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

Let (K, Φ) and (M, Ψ) be two CM-types. We say that (K, Φ) and (M, Ψ) are *equivalent* if there exist an isomorphism of fields $\delta : K \to M$ and an automorphism ι of $\mathbb{C}$ such that $\Psi = \{\iota \circ \phi \circ \delta^{-1} \mid \phi \in \Phi\}$. If M is also a subfield of the Galois closure L of K and we view CM-types on CM-subfields of L as embeddings in L as above, this definition is equivalent to asking that $\Psi = \{\iota \circ \phi \circ \delta^{-1} \mid \phi \in \Phi\}$ for some automorphisms δ, ι of L.

Write G for the Galois group of L over $\mathbb{Q}$ and H for the subgroup of G corresponding to K. Any embedding ϕ of K in L can be extended to an automorphism of L and, if we also denote by ϕ one such extension, then all the extensions form a coset ϕH of H. Let S denote the set of all extensions of elements of Φ to automorphisms of L. Then S is a CM-type on L and the subgroup $H' = \{\gamma \in G \mid \gamma S = S\}$ contains H; we say that Φ is *primitive* if $H' = H$.

Put $S^* = \{\sigma^{-1} \mid \sigma \in S\}$ and let $\hat{H} = \{\gamma \in G \mid \gamma S^* = S^*\}$. Then $\hat{H}$ is a subgroup of G and the corresponding subfield $\hat{K}$ of L is a CM-field, known as the *reflex field* of K. Furthermore, the set $\hat{\Phi}$ of embeddings of $\hat{K}$ in $\mathbb{C}$ obtained by restriction of elements of S^* is a CM-type on $\hat{K}$, known as the *reflex* of Φ. Note that $\hat{\Phi}$ is always primitive.

By definition, the Φ-*trace* is the map $\mathrm{Tr}_\Phi : K \to L$ that sends $\alpha \in K$ to $\sum_{\phi \in \Phi} \alpha^\phi$. One can show that the field $\hat{K}$ is generated over $\mathbb{Q}$ by the set $\{\mathrm{Tr}_\Phi(\alpha) \mid \alpha \in K\}$, so that Tr_Φ actually takes values in $\hat{K}$. It follows that the Φ-*norm* N_Φ, which is defined by $\mathrm{N}_\Phi(\alpha) = \prod_{\phi \in \Phi} \alpha^\phi$ for all $\alpha \in K$, also takes values in $\hat{K}$. We define the $\hat{\Phi}$-*trace* $\mathrm{Tr}_{\hat{\Phi}}$ and $\hat{\Phi}$-*norm* $\mathrm{N}_{\hat{\Phi}}$ similarly; these maps are defined on $\hat{K}$ and take values in the subfield K' of K corresponding to the subgroup H' of G. The norm maps extend in an obvious way to maps on ideals $\mathrm{N}_\Phi : I_K \to I_{\hat{K}}$ and $\mathrm{N}_{\hat{\Phi}} : I_{\hat{K}} \to I_{K'}$, where I_F denotes the group of fractional ideals of the number field F.

Let $Cl_{\hat{K}}$ be the ideal class group of $\hat{K}$ and denote by $Cl(\hat{\Phi})$ the subgroup of $Cl_{\hat{K}}$ consisting of the ideal classes γ such that $\mathrm{N}_{\hat{\Phi}}(\gamma)$ is the principal ideal class of K and, if $\mathfrak{A} \in \gamma$, then the ideal $\mathrm{N}_{\hat{\Phi}}(\mathfrak{A})$ of K has a generator α such that $\alpha\overline{\alpha}$ is rational. (This makes sense as a class group since if $\mathfrak{A}$ is a principal ideal of $\hat{K}$ with generator β, then $\mathrm{N}_{\hat{\Phi}}(\beta)$ is a generator of $\mathrm{N}_{\hat{\Phi}}(\mathfrak{A})$ and $\mathrm{N}_{\hat{\Phi}}(\beta)\overline{\mathrm{N}_{\hat{\Phi}}(\beta)} = \mathrm{N}_{\hat{K}/\mathbb{Q}}(\beta)$ is rational.) Let $h_{\hat{\Phi}}$ be the order of $Cl(\hat{\Phi})$.

2.2. *Weil numbers and characteristic polynomials*

Recall from the Introduction that if q is a power of a prime p, a q-*Weil number* is an algebraic integer all of whose complex conjugates π satisfy $\pi\bar{\pi} = q$.

Let π be a q-Weil number, where $q = p^a$. If π has a real conjugate, then $\pi^2 = q$ and so $\pi = \pm\sqrt{q}$ and π is totally real and belongs to $\mathbb{Q}$ if a is even and is real quadratic if a is odd. On the other hand, if π has no real conjugate, then q/π is also a conjugate and π is a root of the polynomial $X^2 - \tau X + q$, where $\tau = \pi + q/\pi$ is a totally real algebraic integer. It follows that $\mathbb{Q}(\pi)$ is a CM-field. Furthermore, every real conjugate of τ satisfies $|\tau| \leqslant 2\sqrt{q}$. Conversely, if τ is a totally real algebraic integer all of whose real conjugates satisfy this inequality, then the roots of $X^2 - \tau X + q$ are q-Weil numbers.

Recall that an abelian variety A over $\mathbb{F}_q$ of dimension g is said to be *ordinary* if the group $A[p](\overline{\mathbb{F}}_q)$ of p-torsion points over an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ has p-rank g. We refer to [**26**, § 7] for the following result.

PROPOSITION 2.1. *Let A be a simple abelian variety over $\mathbb{F}_q$ of dimension g, let π be the Frobenius endomorphism of A and let $\tau = \pi + q/\pi$. Then the following are equivalent.*

(i) *A is ordinary.*
(ii) *π and q/π are coprime algebraic integers.*
(iii) *τ and q are coprime algebraic integers.*

Furthermore, if these conditions are satisfied, $\mathrm{End}(A) \otimes \mathbb{Q} = \mathbb{Q}(\pi)$ *is a CM-field.*

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

The fact that $\mathbb{Q}(\pi)$ is a CM-field follows from the previous discussion. We deduce the following Corollary to Proposition 1.1, already remarked in [**12**].

COROLLARY 2.2. *Let $g \geqslant 1$ be an integer and let K be a CM-field of degree $2g$. Let p be a prime and let C be an irreducible p-Weil polynomial of degree $2g$ such that $K \simeq \mathbb{Q}[X]/C(X)$. If p is unramified in K, then the abelian varieties over $\mathbb{F}_p$ belonging to the isogeny class corresponding to C are ordinary.*

Proof. Indeed, if p is such that the abelian varieties are not ordinary, then π and p/π have a common prime ideal factor $\mathfrak{p}$. But then $\mathfrak{p}^2$ divides p, so p is ramified in K. □

Inspired by this result, we say that the q-Weil number π is *ordinary* if it satisfies the equivalent conditions (ii) and (iii) of the proposition.

Let π be a q-Weil number belonging to the CM-field K of degree $2g$. Then, by the *characteristic polynomial of* π, denoted by C_π, we mean the characteristic polynomial of the endomorphism multiplication-by-π of the $\mathbb{Q}$-vector space K. Then C_π is a power of the minimal polynomial of π and depends only on g and not on K. In particular, if π' is another q-Weil number belonging to K, then $C_{\pi'} = C_\pi$ if and only if π' is a conjugate of π. Furthermore, if $K = \mathbb{Q}(\pi)$, then C_π is the minimal polynomial of π and, if $\mathrm{Aut}(K)$ denotes the automorphism group of K, then the number of conjugates of an element of K is equal to the order of $\mathrm{Aut}(K)$. Thus, $\#\,\mathrm{Aut}(K)$ triples of the form (r, π, q) give rise to the same triple (r, C, q).

2.3. *Weil numbers coming from a given CM-type*

Let (K, Φ) be a CM-type. If $\pi \in K$ is a Weil number, we say that π *comes from* Φ if there is an ideal $\mathfrak{A} \in I_{\hat{K}}$ such that $\mathrm{N}_{\hat{\Phi}}(\mathfrak{A})$ is a principal ideal of K, generated by π. Similarly, we say that the triple of one of the forms (r, C, q) and (r, π, q) as above comes from Φ if π comes from Φ.

We next derive some unconditional results about Weil numbers coming from a given CM-type.

PROPOSITION 2.3. *Let (K, Φ) be a CM-type, let p be a prime unramified in K and let $\pi \in K$ be a p-Weil number coming from Φ.*

(i) *There is a unique prime ideal $\mathfrak{P}$ of $\hat{K}$ such that π generates the ideal $\mathrm{N}_{\hat{\Phi}}\mathfrak{P}$ of K. Furthermore, $\mathfrak{P}$ is of degree one, and its ideal class belongs to $Cl(\hat{\Phi})$.*

(ii) *If (K, Φ) is primitive, then $K = \mathbb{Q}(\pi)$.*

Proof. (i) By considering the factorization of p as a product of prime ideals in L and K, and using $\pi\overline{\pi} = p$, one sees that there is an integral ideal $\mathfrak{P}$ of $\hat{K}$ such that $\mathrm{N}_{\hat{\Phi}}\mathfrak{P}$ is equal to the ideal generated by π. Furthermore, one necessarily has $\mathrm{N}_{\hat{K}/\mathbb{Q}}(\mathfrak{P}) = p$, so that since p is prime $\mathfrak{P}$ is necessarily a prime ideal of degree one. It is clear from the definitions that the ideal class of $\mathfrak{P}$ must belong to $Cl(\hat{\Phi})$.

Suppose that $\mathfrak{P}'$ is a second prime ideal of $\hat{K}$ such that $\mathrm{N}_{\hat{\Phi}}\mathfrak{P}'$ is equal to the ideal generated by π. Let $\mathfrak{Q}$ and $\mathfrak{Q}'$ denote respectively prime ideals of L dividing $\mathfrak{P}$ and $\mathfrak{P}'$. Since p divides both $\mathfrak{Q}$ and $\mathfrak{Q}'$, there is an element $\tau \in G$ such that $\mathfrak{Q}' = \mathfrak{Q}^\tau$. Let $G_\mathfrak{Q}$ be the decomposition group of $\mathfrak{Q}$ and recall that $\hat{H}$ is the subgroup of G corresponding to $\hat{K}$. Since $\mathfrak{P}$ has degree one, $G_\mathfrak{Q}$ is a subgroup of $\hat{H}$. Since L is the Galois closure of K, p is unramified in L and the ideal factorization of $\mathfrak{P}$ in L is $\prod_{\sigma \in G_\mathfrak{Q}\backslash\hat{H}} \mathfrak{Q}^\sigma$. From the definition of $\mathrm{N}_{\hat{\Phi}}$, we see that the ideal factorization of π in L is equal to $\prod_{\sigma \in G_\mathfrak{Q}\backslash S^*} \mathfrak{Q}^\sigma$. By hypothesis, it is also equal to $\prod_{\sigma \in G_{\mathfrak{P}^\tau}\backslash S^*} \mathfrak{Q}^{\tau\sigma}$. It follows that $\tau S^* = S^*$, so that $\tau \in \hat{H}$. But then $\mathfrak{Q}$ and $\mathfrak{Q}'$ divide the same prime ideal of $\hat{K}$, so that $\mathfrak{P}' = \mathfrak{P}$.

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

(ii) It suffices to prove that if $\gamma \in G$ is such that π^γ and π have the same ideal factorization in L, then $\gamma \in H$. To do this, we return to the ideal factorization $\prod_{\sigma \in G_{\mathfrak{Q}} \backslash S^*} \mathfrak{Q}^\sigma$ of π. The ideal factorization of π^γ is then $\prod_{\sigma \in G_{\mathfrak{Q}} \backslash S^*} \mathfrak{Q}^{\sigma\gamma}$, and this can only coincide with that of π if $S^*\gamma = S^*$ or, equivalently, if $\gamma S = S$. Since Φ is primitive, this implies $\gamma \in H$. □

Despite its simple proof, we have been unable to find a reference to the following result in the literature.

THEOREM 2.4. *Let Φ be a CM-type on K. Then the number $\pi_\Phi(x)$ of p-Weil numbers coming from Φ with p prime and $p \leqslant x$ is asymptotically equal to*

$$\pi_\Phi(x) \sim \frac{w_K h_{\hat{\Phi}}}{h_{\hat{K}}} \int_2^x \frac{du}{\log u} \tag{2.1}$$

as $x \to \infty$.

Proof. Let π be a p-Weil number coming from Φ. Since only finitely many primes ramify in K, we can suppose p unramified. By Proposition 2.3(i), there is a unique prime ideal of degree one $\mathfrak{P}$ of $\hat{K}$ such that $\mathrm{N}_{\hat{\Phi}}(\mathfrak{P})$ is equal to the ideal of K generated by π. Now, if π' is another p-Weil number that generates the same ideal as π, then $\pi' = \zeta\pi$ for some invertible element ζ of the ring of integers of K. Since π and π' are p-Weil numbers, all the complex conjugates of ζ have absolute value 1. It follows from Kronecker's lemma on roots of unity (see for example [**20**, Chapter II, Theorem 2.1]) that ζ is a root of unity. Conversely, if ζ is a root of unity in K and π is a p-Weil number in K, then $\zeta\pi$ is also a p-Weil number in K. We deduce that $\pi_\Phi(x)$ is equal to w_K times the number of degree one prime ideals $\mathfrak{P}$ of $\hat{K}$ with $\mathrm{N}_{\hat{K}/\mathbb{Q}}(\mathfrak{P}) \leqslant x$. Since the ideal class of $\mathfrak{P}$ must belong to $Cl(\hat{\Phi})$, the result thus follows by applying the prime ideal theorem in number fields (see for example [**20**, Chapter VII]). □

3. *A heuristic asymptotic formula for a fixed CM-type*

In this section, we fix the embedding degree k and the CM-field K of degree $2g$ and we propose an asymptotic heuristic estimate as $x \to \infty$ for the number of triples (r, π, p) using an approach similar to that already used for elliptic curves in [**5**]. See also [**12**, § 3]. Before discussing Estimate 3.2, we begin with the following simple observation. As before, φ denotes Euler's totient function. Also, we allow triples (r, π, q) with q a prime power.

LEMMA 3.1. *Let g and $k \geqslant 1$ be fixed. If $\rho_0 < g/\varphi(k)$, then there are only finitely many triples (r, π, q) of genus g with embedding degree k and g-degree rho-value $\leqslant \rho_0$.*

Proof. Suppose that there are infinitely many triples (r, π, q) with embedding degree k and rho-value $\rho \leqslant \rho_0$. For any fixed r, since $q \leqslant r^{\rho_0/g}$, there are only finitely many possibilities for the prime power q such that (r, π, q) is a triple whose first member is r. On the other hand, by considering the ideal factorization of q in K and using Kronecker's lemma on roots of unity, we deduce that for fixed q there are only finitely many q-Weil numbers belonging to K. Hence, the set of values r that appear as first members of triples is unbounded. Recall that the kth cyclotomic polynomial Φ_k is a monic polynomial of degree $\varphi(k)$. Since r divides $\Phi_k(q)$, we have $r \leqslant \Phi_k(q)$. On the other hand, $\Phi_k(q) \sim q^{\varphi(k)}$ and $q^{\varphi(k)} \leqslant r^{\varphi(k)\rho/g}$, so that $\Phi_k(q) \leqslant 2r^{\varphi(k)\rho/g} \leqslant 2r^{\varphi(k)\rho_0/g}$ if r is large enough. We deduce that $r \leqslant 2r^{\varphi(k)\rho_0/g}$ if r is large enough. Since $\rho_0 < g/\varphi(k)$, this is impossible. □

The purpose of the rest of this section is to give a heuristic argument in support of the following refined version of Estimate 1.2.

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

ESTIMATE 3.2. Estimate 1.2 holds with

$$\alpha = \frac{e(k,K)gw_K h_{\hat{\Phi}}}{\rho_0 h_{\hat{K}}}.$$

REMARK 3.3. It follows from Proposition 2.3(ii) and the discussion at the end of 2.2 that, when Φ is primitive, the number of triples (r, C, p) with $K \simeq \mathbb{Q}[x]/C(x)$ is expected to be asymptotically equivalent to

$$\frac{e(k,K)gw_K h_{\hat{\Phi}}}{\#(\mathrm{Aut}(K))\rho_0 h_{\hat{K}}} \int_2^x \frac{du}{u^{2-(\rho_0/g)}(\log u)^2}$$

as $x \to \infty$. Also, when p is unramified in K, the triple is ordinary.

We now complete the heuristic argument which will lead to Estimate 3.2, in a manner similar to [5].

Let r be given. The probability that r is prime and splits completely in $\mathbb{Q}(\zeta_k)$ is equal to the probability that r is prime and that $r \equiv 1 \pmod{k}$, which is $1/(\varphi(k)\log r)$. On the other hand, when $r \equiv 1 \pmod{k}$, Φ_k has $\varphi(k)$ distinct roots $\pmod{r}$. Thus, if p is any integer, the probability that $\Phi_k(p) \equiv 0 \pmod{r}$ is roughly $\varphi(k)/r$. Hence, the probability that r is prime and divides $\Phi_k(p)$ is roughly

$$\frac{1}{\varphi(k)\log r}\frac{\varphi(k)}{r} = \frac{1}{r\log r}.$$

On the other hand, we want p to be a prime and $\pi \in K$ to be a p-Weil number such that r divides $\mathrm{N}_{K/\mathbb{Q}}(\pi - 1)$. We assume that the probability that r divides $\mathrm{N}_{K/\mathbb{Q}}(\pi - 1)$ is $1/r$. To justify this, suppose first that Φ is primitive, so that $K = \mathbb{Q}(\pi)$ by Proposition 2.3(ii). Then we can ignore the case where r^2 divides $\mathrm{N}_{K/\mathbb{Q}}(\pi - 1)$, assuming that as r increases it occurs with negligible frequency. This means that there is a unique degree one prime ideal $\mathfrak{r}$ dividing r that also divides $\pi - 1$. We assume that the Weil numbers π behave randomly with respect to division by a non-zero ideal of K. This means that the probability that $\pi - 1$ is divisible by $\mathfrak{r}$ is $1/r$. In any number field, the average number of primes of degree one dividing a given rational prime is one, so that this is equivalent to the probability that r divides $\mathrm{N}_{K/\mathbb{Q}}(\pi - 1)$ being equal to $1/r$. A similar argument works when Φ is not primitive, replacing K by suitable CM-subfields of K.

On the other hand, the probability that r is a prime, that it splits completely in $\mathbb{Q}(\zeta_k)$ and that there exists a degree one prime in K dividing r is equal to $e(k,K)/(r^2\log r)$.

Finally, from Theorem 2.4, we see that the expected number of p-Weil numbers coming from Φ with prime $p \leqslant r^{\rho_0/g}$ is about $(w_K h_{\hat{\Phi}}/h_{\hat{K}})(r^{\rho_0/g}/(\log r^{\rho_0/g}))$, so that the total number of triples (r, π, p) satisfying the hypotheses of Estimate 3.2 is expected to be asymptotically equivalent to

$$\sum_{2\leqslant r\leqslant x} \frac{e(k,K)}{r^2(\log r)} \frac{w_K h_{\hat{\Phi}}}{h_{\hat{K}}} \frac{r^{\rho_0/g}}{\log r^{\rho_0/g}} = \frac{e(k,K)gw_K h_{\hat{\Phi}}}{\rho_0 h_{\hat{K}}} \sum_{2\leqslant r\leqslant x} \frac{1}{r^{2-(\rho_0/g)}(\log r)^2},$$

where the sums are over all integers r between 2 and x. Replacing the sum by an integral leads to Estimate 3.2.

REMARK 3.4. Suppose that $\mathbb{F}_q$ contains the rth roots of unity. Let $A/\mathbb{F}_q$ be a simple ordinary abelian variety of dimension g and suppose that the prime $r \neq p$ divides the order of $A(\mathbb{F}_q)$. Then $q \equiv 1 \pmod{r}$ and hence $1 \pmod{r}$ is a root of multiplicity at least two of the characteristic polynomial of the Frobenius endomorphism π of A acting on the $\mathbb{F}_r$-vector

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

space $A[r]$ of points of order dividing r of A. Suppose that r is prime to the discriminant of the order $\mathbb{Z}[\pi, p/\pi]$, which is contained in $\mathrm{End}(A)$. Then r can be factored as a product of distinct proper $\mathrm{End}(A)$-ideals, say $r\,\mathrm{End}(A) = \mathfrak{r}_1\mathfrak{r}_2\ldots\mathfrak{r}_h$. We can then write $A[r]$ as a direct sum

$$A[r] = A[\mathfrak{r}_1] \oplus A[\mathfrak{r}_2] \oplus \ldots \oplus A[\mathfrak{r}_h],$$

where, for each i, $A[\mathfrak{r}_i]$ denotes the subgroup of $A[r]$ killed by all the elements of $\mathfrak{r}_i$. We deduce that the action of π on $A[r]$ is semi-simple, so that the 1-eigenspace of π in $A[r]$ viewed as a $\mathbb{F}_r$-vector space is of dimension at least two. It follows that r^2 necessarily divides the order of $A(\mathbb{F}_q)$. Thus, the assumption made in the study of Estimate 3.2 that we can ignore cases where r^2 divides the order $A(\mathbb{F}_q)$ is not justified when $k = 1$.

4. *Numerical evidence in the fixed CM-field case*

In this section, we report on numerical evidence for Estimate 3.2.

4.1. *Examples in genus two and three*

For the convenience of the reader, we summarize briefly all possible CM-types up to equivalence for $g = 2$ and 3. Recall that K denotes a CM-field of degree $2g$, K^+ the maximal real subfield of K, L a fixed Galois closure of K and G the Galois group of L over $\mathbb{Q}$. If F is a subfield of L, we denote by G^F the subgroup of G that fixes F. We fix an embedding of L into $\mathbb{C}$. When we write a CM-type Φ on K as a set $\{\tau_1, \tau_2, \ldots\}$ of elements of G, we mean that Φ is the restriction to K of these elements, and similarly for the reflex type $\hat{\Phi}$.

$g = 2$ (cf. [**23**, pp. 64 and 65]). There are three possibilities for K.

(i) $K = L$ is a Galois biquadratic extension of $\mathbb{Q}$. Let K_0 be an imaginary quadratic subfield of K and let τ be the non-trivial element of G^{K_0}. Then $\Phi = \{\mathrm{id}, \tau\}$ is a CM-type on K extending the CM-type $\{\mathrm{id}\}$ of K_0. We have $\hat{K} = K_0$ and $\hat{\Phi} = \{\mathrm{id}\}$. Hence, there are two equivalence classes of CM-types on K corresponding to the two imaginary quadratic subfields. Neither of them is primitive.

(ii) $K = L$ is a Galois cyclic extension of $\mathbb{Q}$. If τ is a generator of G, then every CM-type is equivalent to $\Phi = \{\mathrm{id}, \tau\}$. This is a primitive CM-type, $\hat{K} = K$ and $\hat{\Phi} = \{\mathrm{id}, \tau^{-1}\}$.

(iii) K is not Galois over $\mathbb{Q}$, and G is a dihedral group generated by σ and τ with σ of order two having K as fixed field and τ of order four. Every CM-type is equivalent to $\Phi = \{\mathrm{id}, \tau\}$. Again this is a primitive CM-type, $\hat{K}$ is the field fixed by $\tau\sigma$ and $\hat{\Phi} = \{\mathrm{id}, \sigma\}$.

$g = 3$. There are four possibilities for K.

(iv) $K = L$ is a degree six Galois cyclic extension of $\mathbb{Q}$. Then K contains a unique imaginary quadratic subfield K_1. Every imprimitive CM-type on K is equivalent to $\Phi = G^{K_1}$. We have $\hat{K} = K_1$ and $\hat{\Phi} = \{\mathrm{id}\}$. There is a unique equivalence class of primitive CM-type. If τ is a generator of $\mathrm{Gal}(K/\mathbb{Q})$, a representative is $\Phi = \{\mathrm{id}, \tau, \tau^2\}$. We have $\hat{K} = K$ and $\hat{\Phi} = \{\mathrm{id}, \tau^{-1}, \tau^{-2}\}$.

(v) K is not Galois over $\mathbb{Q}$ but $K = K^+(\sqrt{-D})$ for some square-free integer $D > 0$. Then G is a dihedral group of order twelve. There is an imprimitive equivalence class as in case (iv), taking $K_1 = \mathbb{Q}(\sqrt{-D})$. There are primitive CM-types all of which are equivalent to the following one. Let τ be a generator of the unique cyclic subgroup of order six of G, and put $\Phi = \{\mathrm{id}, \tau, \tau^2\}$. Then $\hat{K} = K$ and $\hat{\Phi} = \{\mathrm{id}, \tau^{-1}, \tau^{-2}\}$.

In the remaining two cases, K is not Galois over $\mathbb{Q}$ and does not contain an imaginary quadratic subfield. Up to equivalence, there is a unique CM-type and it primitive. We always have $[\hat{K} : \mathbb{Q}] = 8$.

(vi) K^+ is Galois over $\mathbb{Q}$. Then $[L : \mathbb{Q}] = 24$, G is the direct product of a cyclic group of order two and an alternating group on four letters, and G^K is a Klein 4-group. Furthermore, G

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

has four Sylow 3-subgroups, and the restriction of the elements of any one of them to K gives a CM-type $\Phi = \{\mathrm{id}, \tau, \tau^2\}$. Then $\hat{K}$ is the corresponding fixed field and $\hat{\Phi}$ is the restriction of the elements of G^K to $\hat{K}$.

(vii) K^+ is not Galois over $\mathbb{Q}$. In this case, $[L : \mathbb{Q}] = 48$ and G is the direct product of a cyclic group of order two and a symmetric group on four letters. Now G^K is a dihedral group of order eight and we can take Φ to be the set of restrictions to K of the elements $\{\mathrm{id}, \tau, \tau^2\}$ of one of the four Sylow 3-subgroups of G. Then $G^{\hat{K}}$ is the unique subgroup of G containing τ that is isomorphic to the symmetric group of degree three. Again $\hat{\Phi}$ is the set of restrictions to $\hat{K}$ of the elements of G^K.

Since there is only one primitive CM-type up to equivalence, we can test Estimate 3.2 by determining all possible Weil numbers in the field K without explicitly dealing with a reflex field, and then dividing out by the order of the automorphism group of K (see Remark 3.3).

We wrote a program in Magma [4] to compute the number $N(k, K, \rho_0, (a, b))$ of characteristic polynomials C_π coming from triples (r, π, p) with $a \leqslant r \leqslant b$ and $p \leqslant r^{\rho_0/g}$, and compared it with the value

$$I(k, K, \rho_0, (a, b)) = \frac{e(k, K) g w_K h_{\hat{\Phi}}}{\#(\mathrm{Aut}(K)) \rho_0 h_{\hat{K}}} \int_a^b \frac{du}{u^{2-(\rho_0/g)} (\log u)^2} \tag{4.1}$$

predicted by Estimate 3.2. Looping over r, for each such prime pair (r, p) satisfying $r \equiv 1 \pmod{k}$ and p a primitive kth root of unity mod r, we search for p-Weil numbers in the following way.

(1) Factorize $p\mathcal{O}_K$ into prime ideals and make a list $D(p)$ of all possible ideal decompositions of the form $\mathfrak{a}\bar{\mathfrak{a}} = p\mathcal{O}_K$ which are *primitive*, that is, those for which there is no decomposition of the form $(\mathfrak{a} \cap K^0)(\bar{\mathfrak{a}} \cap K^0) = p\mathcal{O}_{K^0}$ for any proper CM-subfield K^0.

(2) For each pair $(\mathfrak{a}, \bar{\mathfrak{a}}) \in D(p)$, test whether $\mathfrak{a}$ is principal and if so find a generator γ. Such an element satisfies $\gamma\bar{\gamma} = p\eta$ for some unit η of $\mathcal{O}_K$. Determine whether $\eta = \gamma\bar{\gamma}/p$ can be written in the form $\varepsilon\bar{\varepsilon}$. If so, then $\pi = \gamma/\varepsilon$ is a p-Weil number and $\Gamma_{\mathfrak{a}} = \{\eta\pi : \eta \in U_K\}$ is the complete set of p-Weil numbers corresponding to $(\mathfrak{a}, \bar{\mathfrak{a}})$.

For each Weil number π found, we check whether r divides $\mathrm{N}_{K/\mathbb{Q}}(\pi - 1)$ and store the minimal polynomial C_π (and its associated data $(r, p, \rho = g(\log p/\log r))$) for those π satisfying this condition.

Since p-Weil numbers are generators of principal ideals of the form $\mathrm{N}_{\hat{\Phi}}(\mathfrak{P})$, where $\mathfrak{P}$ has norm p, we need only consider those p for which there is a degree one prime above p in $\hat{K}$. We obtain necessary conditions by working in the maximal abelian subfield M of the Galois closure L of K. We require that the decomposition field of a prime of M above p contains $F = \hat{K} \cap M$. The Kronecker–Weber theorem tells us that F is contained in $\mathbb{Q}(\zeta_f)$, where f is the conductor of F and the decomposition group $\mathrm{Gal}(\mathbb{Q}(\zeta_f)/F) \triangleleft \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q}) \cong (\mathbb{Z}/f\mathbb{Z})^*$ gives us congruence conditions on $p \pmod{f}$ for such a decomposition to occur. For non-Galois CM-fields in genus two or three, F is a quadratic field and hence we need only compute ideal decompositions for half the congruence classes modulo f. For Galois CM-fields of degree $2g \leqslant 6$, the Galois group is abelian and $\hat{K} = K = F$, so the proportion of primes we deal with is even smaller, namely $1/2g$. In a similar manner, since we require that r splits completely in K, we obtain further congruence restrictions on r when the maximal abelian subextension of K is not contained in $\mathbb{Q}(\zeta_k)$.

We ran this program on a selection of quartic and sextic CM-fields for several values of k. The field invariants making up the constant term in the heuristic formula of Estimate 3.2 are varied in our sample.

For Galois CM-fields of degrees four and six, we computed the type norm map explicitly to determine the unique decomposition (up to the Galois action). This approach of using the type norm map, while possible for other non-Galois fields, was slower than computing the ideal decompositions due to requiring us to perform calculations in the larger Galois closure.

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

The tables have been placed together near the end of the paper for ease of use.

Table 1 gives the values of $N(k, K, \rho_0, (10^4, 5 \times 10^5))$ with rho-values $\rho_0 \leqslant 3.5$ and with several values of k, for the class number one CM-field $K = \mathbb{Q}[X]/(X^4 + 4X^4 + 2)$, which is a cyclic Galois extension of $\mathbb{Q}$. Table 2 presents a similar table for the field $\mathbb{Q}(\zeta_5)$, which is another Galois cyclic CM-field of class number one. Table 3 presents a table in the same format, this time for a non-Galois quartic CM-field. The cyclic examples took between 5000 and 10 000 s to compute, whereas the non-Galois example took 20 000–30 000 s.

Tables 4–6 give the values of $N(k, K, \rho_0, (10^4, 5 \times 10^5))$ with $\rho_0 \leqslant 5.1$ for several values of k for some sextic CM-fields belonging to cases (iv), (v) and (vi) above. It proved computationally too challenging to compute the heuristic value for a generic sextic field having Galois group of order 48, so we did not produce any data for such a field.

TABLE 1. *Values of* $N(k, K, \rho_0, (10^4, 5 \times 10^5))$ *for* $K = \mathbb{Q}[X]/(X^4 + 4X^2 + 2)$. *Invariants:* $w_K = 2$, $h_{\hat{\Phi}} = h_{\hat{K}} = 1$, *G cyclic.*

ρ_0	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	I	$k=8$	$k=24$	I	$k=16$	$k=32$	I
2.8	2	3	1	0	0	0	1.02	7	1	2.03	3	4	4.07
2.9	4	3	2	0	3	1	1.74	8	1	3.48	7	5	6.97
3.0	8	3	6	1	5	2	3.00	16	3	6.00	10	11	11.99
3.1	14	5	8	2	10	3	5.18	20	5	10.36	22	17	20.73
3.2	22	9	9	6	13	5	8.99	23	15	17.98	43	33	35.96
3.3	30	14	15	12	26	14	15.66	36	30	31.31	63	58	62.62
3.4	46	27	26	23	40	31	27.37	61	55	54.73	112	104	109.46
3.5	68	51	59	38	59	49	48.00	99	110	96.00	178	187	192.00

TABLE 2. *Values of* $N(k, K, \rho_0, (10^4, 5 \times 10^5))$ *for* $K = \mathbb{Q}(\zeta_5)$. *Invariants:* $w_K = 10$, $h_{\hat{\Phi}} = h_{\hat{K}} = 1$, *G cyclic.*

ρ_0	$k=2$	$k=3$	$k=4$	$k=12$	$k=24$	$k=36$	I	$k=5$	$k=10$	$k=15$	$k=20$	$k=25$	I
2.5	0	3	0	2	2	2	1.04	2	4	9	2	4	4.15
2.6	2	3	2	3	2	6	1.75	6	10	12	3	6	7.01
2.7	2	5	2	3	4	7	2.98	10	22	17	5	6	11.91
2.8	2	6	2	6	6	10	5.08	14	26	29	14	9	20.33
2.9	6	9	8	8	9	10	8.71	26	46	45	32	22	34.84
3.0	10	15	14	18	17	18	14.99	64	70	72	49	51	59.97
3.1	16	27	20	32	24	27	25.91	106	124	125	83	93	103.63
3.2	26	44	43	52	35	50	44.95	176	168	210	150	162	179.79
3.3	70	76	72	82	72	87	78.28	302	302	335	282	319	313.12
3.4	112	142	140	143	130	141	136.83	574	560	597	534	578	547.30
3.5	212	250	241	258	235	251	240.00	1000	1000	1049	977	1006	959.99

TABLE 3. *Values of* $N(k, K, \rho_0, (10^4, 5 \times 10^5))$ *for* $K = \mathbb{Q}[X]/(X^4 + 8X^2 + 13)$. *Invariants:* $w_K = 2$, $h_{\hat{\Phi}} = h_{\hat{K}} = 2$, *G dihedral.*

ρ_0	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	I	$k=12$	$k=24$	$k=36$	I
2.7	2	0	0	1	2	2	1.19	2	2	2	2.38
2.8	2	2	2	4	3	3	2.03	2	4	6	4.07
2.9	6	5	3	6	3	4	3.48	8	8	9	6.97
3.0	6	8	6	10	6	7	6.00	17	14	11	11.99
3.1	8	13	11	11	10	14	10.36	25	25	17	20.73
3.2	16	23	19	20	17	25	17.98	44	43	36	35.96
3.3	32	31	26	34	27	39	31.31	65	71	64	62.62
3.4	58	59	56	57	54	66	54.73	116	116	115	109.46
3.5	100	97	93	93	96	117	96.00	206	195	191	192.00

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

The data for the Galois sextic CM-field examples was computed relatively quickly: approximately 2300 s for each value of k. The sextic fields with G of order 12 took between 20 000 and 60 000 s each; the examples with G of order 24 took under 15 000 s. An explanation for why the order 24 examples were quicker to compute than the order twelve examples is that the latter have a proper CM-subfield (of degree two), so we must identify and discard the non-primitive ideal decompositions.

TABLE 4. *Values of* $N(k, K, \rho_0, (10^4, 5 \times 10^5))$ *for* $K = \mathbb{Q}(\zeta_9)$. *Invariants:* $w_K = 18$, $h_{\hat{\Phi}} = h_{\hat{K}} = 1$, G *cyclic.*

ρ_0	$k=2$	$k=4$	$k=5$	I	$k=3$	$k=6$	I	$k=9$	$k=18$	I
4.0	6	3	0	2.99	2	4	5.99	22	18	17.97
4.1	8	6	2	4.27	6	8	8.54	34	24	25.62
4.2	10	6	6	6.10	10	18	12.20	46	44	36.60
4.3	14	10	8	8.73	14	22	17.46	64	54	52.38
4.4	16	11	13	12.52	20	30	25.04	82	72	75.13
4.5	24	15	23	17.99	30	38	35.98	124	116	107.94
4.6	32	24	30	25.90	50	62	51.79	180	160	155.37
4.7	44	34	42	37.34	80	80	74.68	260	236	224.05
4.8	68	51	62	53.94	114	116	107.88	390	330	323.63
4.9	90	71	82	78.04	166	162	156.09	568	454	468.27
5.0	136	104	114	113.11	250	224	226.22	812	658	678.66
5.1	224	169	159	164.19	380	328	328.38	1238	944	985.15

TABLE 5. *Values of* $N(k, K, \rho_0, (10^4, 5 \times 10^5))$ *for* $K = \mathbb{Q}[X]/(X^6 + 24X^4 + 144X^2 + 27)$. *Invariants:* $w_K = 6$, $h_{\hat{\Phi}} = 1$, $h_{\hat{K}} = 2$, G *of order* 12.

ρ_0	$k=2$	$k=4$	$k=5$	$k=32$	I	$k=3$	$k=6$	$k=24$	I
3.9	0	3	0	0	1.05	2	4	3	2.10
4.0	0	3	0	0	1.50	2	4	5	2.99
4.1	0	3	0	1	2.13	4	6	7	4.27
4.2	2	3	0	2	3.05	6	6	10	6.10
4.3	4	5	0	4	4.37	8	6	15	8.73
4.4	6	5	2	6	6.26	14	8	21	12.52
4.5	12	8	6	9	9.00	20	14	32	17.99
4.6	16	12	9	13	12.95	22	24	53	25.90
4.7	22	15	13	20	18.67	32	34	67	37.34
4.8	40	23	24	30	26.97	44	50	84	53.94
4.9	50	35	32	42	39.02	62	80	119	78.04
5.0	64	52	57	58	56.55	110	118	160	113.11
5.1	88	74	96	84	82.10	164	170	214	164.19

TABLE 6. *Values of* $N(k, K, \rho_0, (10^4, 5 \times 10^5))$ *for* $K = \mathbb{Q}[X]/(X^6 + 35X^4 + 364X^2 + 1183)$. *Invariants:* $w_K = 2$, $h_{\hat{\Phi}} = 4$, $h_{\hat{K}} = 16$, G *of order* 24.

ρ_0	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	I	$k=7$	$k=14$	$k=35$	I
4.4	0	2	0	2	3	1.04	5	2	4	3.13
4.5	0	2	0	2	4	1.50	10	4	4	4.50
4.6	2	2	0	3	5	2.16	11	5	6	6.47
4.7	2	3	0	4	6	3.11	15	7	10	9.34
4.8	2	6	3	6	8	4.49	16	14	11	13.48
4.9	2	8	4	8	8	6.50	23	23	17	19.51
5.0	8	13	6	15	10	9.43	37	37	25	28.28
5.1	12	14	9	18	14	13.68	48	49	40	41.05

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

We would have liked to have extended the range of r, but the unavoidable large number of ideal factorizations in number fields prevented us from taking an interval for r too large or high up.

In almost all the cases we computed, there is good agreement between the computed value of $N(k, K, \rho_0, (a, b))$ and the expected value $I(k, K, \rho_0, (a, b))$. Noticeable exceptions occur in Table 1 when $k = 2$ and $k = 8$ and in Table 5 when $k = 24$, when the integral seems to seriously underestimate the actual number of triples found. To check whether the phenomenon persisted, we extended the computation to larger r (up to 2×10^7 in the cases $k = 2$ and $k = 8$ of Table 1) and found that the computed values were in much closer agreement with the expected ones.

4.2. *An example in genus four*

We also computed pairing-friendly Weil polynomials for the non-Galois octic CM-field

$$K = \mathbb{Q}[X]/(X^8 + 78X^6 + 1323X^4 + 7401X^2 + 9801).$$

Let L be a Galois closure of K. Then $[L : \mathbb{Q}] = 24$ and L contains a non-Galois sextic CM-field K_6 with Galois closure L. Thus, the Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$ is that of case (vi) above. It follows that the primitive CM-type on K_6 is a reflex CM-type for K. Up to equivalence, there are two primitive CM-types on K: Φ_6 with reflex field K_6 and Φ_8 with reflex field $K_8 \cong K$. There is also an imprimitive class of CM-types corresponding to extending the CM-type Φ_2 of the imaginary quadratic field $K_2 \cong \mathbb{Q}(\zeta_3)$ contained in K.

Using the same method as described earlier, we computed pairing-friendly primitive Weil polynomials of K. We sorted them by CM-type Φ_i in order to compare the number $N_{\Phi_i}(k, K, \rho_0, (a, b))$ of pairing-friendly examples coming from Φ_i with the heuristic from Estimate 3.2:

$$I_{\Phi_i}(k, K, \rho_0, (a, b)) = \frac{e(k, K) g w_K h_{\hat{\Phi}_i}}{\#(\mathrm{Aut}(K)) \rho_0 h_{K_i}} \int_a^b \frac{du}{u^{2-(\rho_0/g)} (\log u)^2}$$

(similar notation to before, now with Φ_i as a subscript).

Table 7 gives the values of $N_{\Phi_i}(k, K, \rho_0, (10^4, 5 \times 10^5))$ with $\rho_0 \leqslant 7.0$ for several values of k. It turns out that $h_{\hat{\Phi}_6}/h_{K_6} = h_{\hat{\Phi}_8}/h_{K_8}$ in this example, so in fact $I_{\Phi_i}(k, K, \rho_0, (a, b))$ is the same for both primitive CM-types.

REMARK 4.1. Since $w_K = w_{K_2}$, all imprimitive Weil numbers of K are in K_2, and so an imprimitive Weil polynomial of K with rho-value ρ is a fourth power of a Weil polynomial of

TABLE 7. *Values of* $N_{\Phi_i}(k, K, \rho_0, (10^4, 5 \times 10^5))$ *for the field* $K = \mathbb{Q}[X]/(X^8 + 78X^6 + 1323X^4 + 7401X^2 + 9801)$. *Invariants:* $w_K = 6$, $h_{\hat{\Phi}_6} = 4, h_{\hat{K}_6} = 8$, $h_{\hat{\Phi}_8} = 2, h_{\hat{K}_8} = 4$.

	$k = 4$		$k = 5$		Heuristic	$k = 3$		$k = 6$		Heuristic
ρ_0	N_{Φ_6}	N_{Φ_8}	N_{Φ_6}	N_{Φ_8}	$I_{\Phi_6} = I_{\Phi_8}$	N_{Φ_6}	N_{Φ_8}	N_{Φ_6}	N_{Φ_8}	$I_{\Phi_6} = I_{\Phi_8}$
6.0	5	9	16	12	9.00	16	20	18	14	18.00
6.1	6	11	18	19	11.82	20	24	26	20	23.64
6.2	12	14	21	26	15.54	30	28	36	28	31.09
6.3	21	25	27	32	20.47	42	38	56	38	40.93
6.4	31	39	32	37	26.97	56	62	74	50	53.94
6.5	40	51	41	46	35.57	68	74	94	62	71.15
6.6	49	64	53	55	46.96	90	96	128	82	93.94
6.7	62	81	74	72	62.07	136	130	152	116	124.14
6.8	85	104	89	94	82.10	176	176	196	152	164.19
6.9	117	133	118	131	108.68	240	216	236	222	217.36
7.0	157	167	159	171	144.00	300	286	300	314	288.00

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

K_2 with rho-value $\rho/4$. As one would hope, the genus one heuristic integral $I(k, K_2, \rho_0/4, (a, b))$ equals $I_{\Phi_2}(k, K, \rho_0, (a, b))$. We confirmed that the imprimitive counts agree well with the heuristic estimates for $k = 4, 5$. No pairing-friendly examples were found when $k = 3$ or 6. These are two of the three 'exceptional' cases, where the independence hypotheses are not satisfied and hence the heuristics do not apply. See [5] for details.

5. *Asymptotics for a fixed maximal real subfield*

When $\rho_0 < g$, the integral

$$\int_2^\infty \frac{du}{u^{2-(\rho_0/g)}(\log u)^2}$$

converges. Thus, Estimate 3.2 suggests that, if K is any CM-field of degree $2g$ and if $\rho_0 < g$, there are only finitely many triples (r, π, p) with rho-value less than ρ_0.

In order to try to understand where triples with rho-value less than g might be located, we now develop a heuristic formula for the asymptotic growth of the number of triples with rho-value bounded above by ρ_0 and the CM-field K varies but with a fixed maximal real subfield K_0^+. Thus, we fix k, ρ_0 and a totally real field K_0^+ of degree g and seek an estimate for the number of triples (r, π, p) with $r \leqslant x$, $p \leqslant r^{\rho_0/g}$ and π is a p-Weil number lying in some CM-field whose maximal real subfield is K_0^+. We denote by $\mathcal{O}_0^+$ the ring of integers of K_0^+. Furthermore, if $\alpha \in K_0^+$, we denote by $\{\alpha_i \mid 1 \leqslant i \leqslant g\}$ the set of real embeddings of α.

Let (r, π, p) be such a triple and write $\tau = \pi + p/\pi$. Then $\tau \in \mathcal{O}_0^+$ and (X denoting a variable)

$$(X - \pi)(X - p/\pi) = X^2 - \tau X + p \in \mathcal{O}_0^+[X] \quad \text{and} \quad |\tau_i| \leqslant 2\sqrt{p} \quad \text{for all } i \in \{1, 2, \ldots, g\},$$

the last inequalities being a consequence of the Weil bounds. Furthermore, the characteristic polynomial $C_\pi(X)$ of π factors over $\mathbb{R}[X]$ as

$$C_\pi(X) = \prod_{i=1}^{g} (X^2 - \tau_i X + p). \tag{5.1}$$

Conversely, if $\tau \in \mathcal{O}_0^+$ is such that $|\tau_i| \leqslant 2\sqrt{p}$ for all i, then $X^2 - \tau X + p$ has two roots π and p/π which are p-Weil numbers such that, if $\tau \neq \pm 2\sqrt{p}$, $K_0^+(\pi)$ is a CM-field with maximal real subfield K_0^+.

Estimate 5.1. Estimate 1.4 holds with

$$\beta = \frac{g 4^{g+1} e(k, K_0^+)}{\rho_0 (g+2) d_0^{1/2}}.$$

Here d_0 denotes the discriminant of K_0^+ and $e(k, K_0^+)$ the degree of $K_0^+ \cap \mathbb{Q}(\zeta_k)$ over $\mathbb{Q}$.

Remark 5.2. Let (r, π, p) be a triple as above, and let $\tau = \pi + p/\pi$. If π is real, then $\pi = \pm\sqrt{p}$ and π must belong to K_0^+. This can occur for only finitely many p. Otherwise, $K_0^+(\pi)$ is uniquely determined by π, and τ arises from the two p-Weil numbers π and p/π. It follows that the number of triples (r, π, p) that correspond to the same triple (r, C, p) with C a characteristic polynomial is equal to twice the number of conjugates of τ; in particular, if $K_0^+ = \mathbb{Q}(\tau)$, it is equal to $2\#(\mathrm{Aut}(K_0^+))$. The triples are ordinary when p is unramified in $K_0^+(\pi)$.

We now indicate a heuristic argument that leads to Estimate 5.1. From elementary results about the geometry of algebraic number fields, we know that as $T \to \infty$, the number $R(K_0^+, T)$

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

of $\tau \in \mathcal{O}_0^+$ such that $|\tau_i| \leqslant T$ for all i satisfies

$$R_0(K_0^+, T) \sim (2T)^g d_0^{-1/2}.$$

As before, the probability that r divides $\Phi_k(p)$ with r prime is $1/(r \log r)$. On the other hand, by the prime ideal theorem, in number fields the expected number of degree one prime ideals of K_0^+ dividing r given that r splits in $\mathbb{Q}(\zeta_k)$ is equal to $e(k, K_0^+)$. In view of this, we assume that the probability that an integer r is prime and divides both $\Phi_k(p)$ and $\mathrm{N}_{K_0^+(\pi)/\mathbb{Q}}(\pi - 1)$ is equal to $e(k, K_0^+)/(r^2 \log r)$.

Thus, we expect the number $R(k, K_0^+, \rho_0, x)$ of triples (r, π, p) with $r \leqslant x$ and $p \leqslant r^{\rho_0/g}$ to be asymptotically equivalent to

$$\sum_{r \leqslant x} \frac{e(k, K_0^+)}{r^2 \log r} \sum_{p \leqslant r^{\rho_0/g}} 2R_0(K_0^+, 2\sqrt{p}), \tag{5.2}$$

where the sum over r is over integers and that over p is over primes, and the 2 appears before the $R_0(K_0^+, 2\sqrt{p})$ because we distinguish between π and p/π. Hence,

$$R(k, K_0^+, \rho_0, x) \sim \frac{2 \cdot 4^g e(k, K_0^+)}{d_0^{1/2}} \sum_{r \leqslant x} \frac{1}{r^2 \log r} \sum_{p \leqslant r^{\rho_0/g}} p^{g/2}. \tag{5.3}$$

Now, it follows from the prime number theorem by an easy argument using Abel summation that, if $\alpha \geqslant 0$, then the sum over primes $\sum_{p \leqslant U} p^\alpha$ is asymptotically equivalent to $U^{\alpha+1}/((\alpha+1)\log U)$ as $U \to \infty$ (see for example [**17**, pp. 203–205] for a more general statement). Applying this with $\alpha = g/2$ and $U = r^{\rho_0/g}$, (5.3) becomes

$$R(k, K_0^+, \rho_0, x) \sim \frac{g 4^{g+1} e(k, K_0^+)}{\rho_0 (g+2) d_0^{1/2}} \sum_{r \leqslant x} \frac{r^{\rho_0(1/2+1/g)-2}}{(\log r)^2}. \tag{5.4}$$

Replacing the sum by an integral and rearranging slightly leads to Estimate 5.1.

Remark 5.3. Suppose that there are C prime ideals of norm r in K_0^+ (where $0 \leqslant C \leqslant g$). Then the number of $\tau \in \mathcal{O}_0^+$ with $|\tau|_i \leqslant 2\sqrt{p}$ for all embeddings i of τ in $\mathbb{R}$ is asymptotically equivalent to

$$4^g p^{g/2} d_0^{-1/2}.$$

On the other hand, if $\mathfrak{r}^+$ is a prime ideal of norm r in K_0^+, the probability that $\tau \equiv p + 1 \pmod{\mathfrak{r}^+}$ is $1/r$. Hence, the number of elements τ in this range and $\mathfrak{r}^+$ a degree one prime ideal of K_0^+ dividing r such that $\tau \equiv p + 1 \pmod{\mathfrak{r}^+}$ should be roughly

$$4^g p^{g/2} C r^{-1} d_0^{-1/2}.$$

In particular, if p is close to $r^{\rho_0/g}$, this is close to

$$4^g r^{\rho_0/2-1} C d_0^{-1/2}. \tag{5.5}$$

Thus, if $\rho_0 > 2$, we expect that when r is large and p is a prime close to $r^{\rho_0/g}$, the number of p-Weil numbers π with $\pi + p/\pi \in K_0^+$ is close to (5.5), which tends to infinity with r.

For a numerical illustration, see Remark 6.2.

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

6. *Numerical evidence in the fixed maximal real subfield case*

We continue to use the notation introduced in the previous section. For small x and ρ_0, we can compute $R(k, K_0^+, \rho_0, x)$ as follows. Since $r \leqslant x$, we know that $|\tau_i| \leqslant 2\sqrt{p} \leqslant 2r^{\rho_0/2g} \leqslant 2x^{\rho_0/2g}$. Hence, we need to carry out the following steps.

(1) Make a list $\mathcal{L}$ of all $\tau \in \mathcal{O}_0^+$ such that $|\tau_i| \leqslant 2x^{\rho_0/2g}$ for all i.
(2) For each $\tau \in \mathcal{L}$, factor $\Phi_k(\tau - 1)$ into prime ideals in K_0^+ and make a list $\mathcal{M}(\tau)$ of all degree one primes $\mathfrak{r}^+$ dividing $\Phi_k(\tau - 1)$ of norm r such that $x \geqslant r \geqslant (|\tau_i|/2)^{2g/\rho_0}$ for all i.
(3) For each $\mathfrak{r}^+ \in M(\tau)$, search for primes $p \leqslant x^{\rho_0/g}$ such that $p \equiv \tau - 1 \pmod{\mathfrak{r}^+}$ and $|\tau_i| \leqslant 2\sqrt{p}$ for all i.

The condition $p \equiv \tau - 1 \pmod{\mathfrak{r}^+}$ of (3) ensures that r divides $\Phi_k(p)$. Thus, for any $\tau \in \mathcal{L}$, $\mathfrak{r}^+ \in M(\tau)$ and prime p as in (3), the triples (r, π, p) and $(r, p/\pi, p)$ with π and p/π the roots of $X^2 - \tau X + p$ contribute towards the total $R(k, K_0^+, \rho_0, x)$.

Conversely, if (r, π, p) is a triple with $r \leqslant x$ and $p \leqslant r^{\rho_0/g}$, and if $\tau = \pi + p/\pi$, then $\tau \in \mathcal{L}$. Since r divides $\mathrm{N}_{K/\mathbb{Q}}(\pi - 1)$, some prime ideal $\mathfrak{r}^+$ of K^+ above r must divide $p + 1 - \tau$. Then $\mathfrak{r}^+ \in M(\tau)$ and p satisfies (3), so that (r, π, p) will be detected by the above search.

Of course, the major drawback of this approach is the need to factor $\Phi_k(\tau - 1)$. Since the size of $\Phi_k(\tau - 1)$ depends on the degree of Φ_k, it is necessary to choose k with $\varphi(k)$ small. On the other hand, decreasing ρ reduces the size of the list $\mathcal{L}$ of step (1). In any case, in practice it is only possible to make meaningful computations when $\varphi(k)$ and x are small.

Using this method, we computed a few tables with ρ_0 at most equal to g.

Let $R_c(k, K_0^+, \rho_0, (a, b))$ be the number of distinct irreducible characteristic polynomials (5.1) associated to Weil numbers π belonging to triples (r, π, p) with $a \leqslant r \leqslant b$, $\pi + p/\pi \in K_0^+$ and $p \leqslant r^{\rho_0/g}$. Tables 8–10 compare the values of $R_c(k, K_0^+, \rho_0, (a, b))$ with the heuristic estimate

$$J = J(k, K_0^+, \rho_0, (a, b)) = \frac{g 4^{g+1} e(k, K_0^+)}{2\#(\mathrm{Aut}(K_0^+))\rho_0(g+2)d_0^{1/2}} \int_a^b \frac{u^{\rho_0(1/2+1/g)-2}\, du}{(\log u)^2}. \tag{6.1}$$

Table 8 shows the values of $R_c(k, \mathbb{Q}(\sqrt{2}), \rho_0, (10^3, 10^5))$ for $k \in \{3, 4, 5, 6, 7, 8, 12\}$ and values of ρ_0 between 1 and 2. On the other hand, Table 9 presents the values of $R_c(k, \mathbb{Q}(\sqrt{d}), 2.0, (10^3, 10^5))$ for $k \in \{3, 4, 5, 6, 12\}$ and for square-free $d \leqslant 50$. The entries for which $e(k, \mathbb{Q}(\sqrt{d})) = 2$ are marked with an asterisk; the predicted value for these entries is $2J$. In all other cases, $e(k, \mathbb{Q}(\sqrt{d})) = 1$ and the predicted value is J. Finally, Table 10 shows the values of $R_c(k, \mathbb{Q}(\zeta_7 + \zeta_7^{-1}), \rho_0, (10^3, 10^4))$ for $k \in \{3, 4, 5, 6, 7\}$ and values of ρ_0 between 1.5 and 3.

TABLE 8. *Values of* $R_c(k, K_0^+, \rho_0, (10^3, 10^5))$ *for* $K_0^+ = \mathbb{Q}(\sqrt{2})$.

ρ_0	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=12$	J	$k=8$	J
1.0	1	0	0	0	0	1	0.16	0	0.33
1.1	1	0	0	1	0	1	0.36	0	0.73
1.2	2	0	0	1	2	2	0.83	1	1.65
1.3	4	1	0	1	3	3	1.92	1	3.85
1.4	7	2	5	5	4	6	4.59	7	9.18
1.5	15	11	14	15	12	17	11.21	22	22.42
1.6	36	22	28	34	25	37	27.95	62	55.90
1.7	81	68	62	88	62	80	71.04	157	142.09
1.8	200	194	192	219	161	210	183.80	384	367.60
1.9	493	518	467	496	534	543	483.16	940	966.33
2.0	1346	1418	1267	1331	1295	1321	1288.45	2572	2576.91

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

The running times in Table 9 were dependent on the size of $\varphi(k)$, the degree of the kth cyclotomic polynomial. For $k \neq 5, 12$, each table entry took under 10 min to compute. The value which took the most time to compute was $k = 5$ for the field $\mathbb{Q}(\sqrt{5})$, which took just under $3\frac{1}{2}$ hours. The computations in Table 10 took under three hours when $k \in \{3, 4, 6\}$ but over ten times longer when $k = 5$ and $k = 7$.

REMARK 6.1. In almost all cases in Tables 8–10, the CM-field $K_0^+(\pi)$ has Galois closure of maximal size. For instance, over 10^4 examples are listed in Table 8, but in only 58 of them is the field $\mathbb{Q}(\sqrt{2}, \pi)$ Galois; in 54 cases the field is biquadratic and in the other four it is cyclic.

REMARK 6.2. We can also use Table 10 to illustrate Remark 5.3. When $K_0^+ = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ and $k = 5$, the table shows that there are no triples with rho-value between 2.3 and 2.4, and 183 with rho-value between 2.4 and 2.5. However, only three values of (r, p) account for all

TABLE 9. *Values of* $R_c(k, \mathbb{Q}(\sqrt{d}), 2.0, (10^3, 10^5))$ *for* $k \in \{3, 4, 5, 6, 12\}$ *and* $d \leqslant 50$ *square-free. Asterisks indicate the cases where* $e(k, \mathbb{Q}(\sqrt{d}) = 2$.

d	$k=3$	$k=4$	$k=5$	$k=6$	$k=12$	J	d	$k=3$	$k=4$	$k=5$	$k=6$	$k=12$	J
2	1346	1418	1267	1331	1321	1288.45	26	365	408	368	374	358	357.35
3	1144	1093	1049	1103	2199*	1052.02	29	675	718	688	662	660	676.73
5	1650	1808	3306*	1670	1703	1629.78	30	356	338	322	346	354	332.68
6	789	794	774	753	751	743.89	31	351	351	333	345	328	327.27
7	755	718	634	667	708	688.71	33	643	687	621	664	640	634.39
10	659	635	573	599	616	576.21	34	325	324	336	287	291	312.50
11	574	580	534	553	567	549.40	35	319	341	285	311	349	308.00
13	1090	1043	1064	975	1084	1010.75	37	634	596	654	614	609	599.12
14	521	526	494	491	432	486.99	38	309	320	299	313	302	295.59
15	486	460	487	443	475	470.48	39	325	334	280	307	306	291.78
17	967	954	952	880	902	883.87	41	609	651	580	537	602	569.14
19	422	480	450	395	412	418.03	42	320	280	316	303	255	281.16
21	883	753	799	798	810	795.25	43	302	300	296	274	300	277.88
22	396	415	405	379	414	388.48	46	307	289	258	300	253	268.66
23	377	393	418	378	396	379.94	47	273	258	311	257	252	265.79

TABLE 10. *Values of* $R_c(k, K_0^+, \rho_0, (10^3, 10^4))$ *for* $K_0^+ = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$.

ρ_0	$k=3$	$k=4$	$k=5$	$k=6$	J	$k=7$	J
1.5	3	0	1	0	0.65	2	1.96
1.6	3	0	1	1	1.20	2	3.60
1.7	10	11	1	3	2.22	6	6.66
1.8	10	11	1	5	4.14	9	12.41
1.9	10	28	1	9	7.75	24	23.26
2.0	18	42	1	15	14.61	30	43.84
2.1	32	53	12	35	27.70	77	83.10
2.2	144	82	40	68	52.78	230	158.33
2.3	197	82	97	160	101.05	324	303.15
2.4	244	232	97	236	194.37	716	583.11
2.5	354	519	280	362	375.53	1 028	1 126.60
2.6	557	1 048	714	865	728.59	1 647	2 185.76
2.7	1211	1 654	1314	1 132	1 419.19	3 267	4 257.58
2.8	2474	3 050	2640	1 598	2 774.87	9 820	8 324.62
2.9	5136	5 527	5330	3 993	5 445.06	19 124	16 335.18
3.0	9378	10 116	8179	11 699	10 721.16	35 287	32 163.49

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

these triples: $(1051, 307)$, $(5741, 1229)$ and $(6091, 1321)$, which give rise respectively to 46, 66 and 74 triples with corresponding rho-values 2.469, 2.466 and 2.474. If we substitute $r = 1051$, 5741 or 6091 in (5.5) with $g = 3$, $C = 3$ and divide by $\#\operatorname{Aut}(\mathbb{Q}(\zeta_7 + \zeta_7^{-1})) = 3$, we find that the predicted number of triples is respectively 46.9, 68.7 and 72.1.

7. *The influence of polynomial families*

As was already noted in [**5**, § 3] in the genus one case, polynomial families with small generic rho-value can be expected to produce more triples than predicted by Estimate 3.2. For elliptic curves over prime fields, the only case where this is known to happen occurs when $k = 12$, where the family involved is the well-known Barreto–Naehrig family, which is recalled below. In this section, we investigate under what circumstances polynomial families might produce counterexamples to Estimates 3.2 and 5.1 in higher genus, and list all the known examples. In defining polynomial families, it is more convenient to consider triples involving characteristic polynomials rather than Weil numbers.

Definition 7.1. Let $g \geqslant 1$, $k \geqslant 2$ be integers with $k \geqslant 3$ if $g = 1$. By a *polynomial family of dimension g with embedding degree k* of triples, we mean a collection of polynomials $\mathcal{P} = \{r_0(w), p_0(w), a_i(w) \mid 0 \leqslant i \leqslant 2g\}$ with rational coefficients with the following properties:

(i) the polynomials r_0 and p_0 are irreducible. In addition, we suppose that there exists an infinite set $\mathcal{W}_0$ of integers such that $r_0(w_0)$ and $p_0(w_0)$ are prime numbers for all $w_0 \in \mathcal{W}_0$;

(ii) we have $a_{2g}(w) = 1$ and $a_i(w) = a_{2g-i}(w)p_0(w)^i$ for all $i \in \{0, 1, \ldots, g-1\}$. We further suppose $a_i(w_0) \in \mathbb{Z}$ for all i and for all $w_0 \in \mathcal{W}_0$;

(iii) define $C_w(X) = \sum_{i=0}^{2g} a_i(w)X^i$, an element of $\mathbb{Q}[X, w]$. We suppose that, for all $w_0 \in \mathcal{W}_0$ with $|w_0|$ sufficiently large, the roots of $C_{w_0}(X)$ are $p_0(w_0)$-Weil numbers;

(iv) we have that $r_0(w)$ divides both $C_w(1)$ and $\Phi_k(p_0(w))$.

The *generic rho-value* of $\mathcal{P}$ is $g(\deg p_0/\deg r_0)$.

By removing a finite number of integers from $\mathcal{W}_0$, we can suppose that all $w_0 \in \mathcal{W}_0$ satisfy (iii). Similarly, if w_0 is such that $r_0(w_0)$ does not divide the denominators of any of the coefficients of r_0, p_0 and the a_i, then condition (iv) implies that $r_0(w_0)$ divides $C_{w_0}(1)$ and $\Phi_k(p_0(w_0))$, so that $(r_0(w_0), C_{w_0}(X), p_0(w_0))$ is a triple as in the Introduction. We therefore suppose from now on that all the elements of $\mathcal{W}_0$ satisfy (iii). Similarly, in the case of an ordinary family, we can suppose that when $w_0 \in \mathcal{W}_0$, $p_0(w_0)$ does not divide $a_g(w_0)$. Clearly, we can suppose that the leading coefficients of r_0 and w_0 are positive, so that $\mathcal{W}_0$ contains arbitrarily large *positive* integers. We usually tacitly assume that $\mathcal{W}_0$ consists of *all* the integers with the prescribed properties.

Fix a polynomial family $\mathcal{P}$. If $x > 0$, denote by $\nu(x) = \nu(\mathcal{P}, x)$ the cardinality of the set of triples $(r_0(w_0), C_{w_0}(1), p_0(w_0))$ with $w_0 \in \mathcal{W}_0$ and $r_0(w_0) \leqslant x$. We want a simple asymptotic equivalent for $\nu(x)$ as $x \to \infty$, which can then be compared with Estimates 3.2 and 5.1. This can only be done heuristically, using the formulae of Bateman and Horn [**3**] and Conrad [**8**] for the asymptotic growth of the number of integers at which a finite set of polynomials simultaneously take prime values, and we recall the special case we need. Let $\mu(x)$ denote the cardinality of the set of $w_0 \in \mathcal{W}_0$ with $|w_0| \leqslant x$. Then there exists a strictly positive constant A_0 such that

$$\mu(x) \sim A_0 \int_2^x \frac{du}{(\log u)^2} \sim A_0 \frac{x}{(\log x)^2} \tag{7.1}$$

as $x \to \infty$. (The papers [**3**, **8**] only consider the case when $r_0(\mathbb{Z}) \subseteq \mathbb{Z}$ and $p_0(\mathbb{Z}) \subseteq \mathbb{Z}$, but one can reduce to this case using an affine change of variables. We refer to [**3**, **8**] for the value of A_0.)

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

Here the expression on the right is obtained from the one in the middle by integrating by parts. In what follows, A_1, A_2 and A_3 denote strictly positive constants.

LEMMA 7.2. *Let $\mathcal{P}$ be a polynomial family of triples. Then, assuming the heuristics in* [**3**, **8**], *there exists a constant $A_1 > 0$ such that*

$$\nu(x) \sim A_1 \frac{x^{1/\deg r_0}}{(\log x)^2} \quad \text{as } x \to \infty. \tag{7.2}$$

Proof. Let $r_1 > 0$ denote the leading coefficient of r_0 and put $d = \deg r_0$. Then $r_0(y) \sim r_1 y^d$ as $y \to \infty$ and, from this, one sees using (7.1) that $\nu(r_1 y^d) \sim \mu(y) \sim A_0 y/(\log y)^2$. To conclude, it suffices to substitute $x = r_1 y^d$. □

Now let $\rho_0 > 1$. If $g(\deg p_0/\deg r_0) > \rho_0$, then there are only finitely many $w_0 \in \mathcal{W}_0$ and the triple $(r_0(w_0), C_{w_0}(w_0), p_0(w_0))$ has rho-value at most ρ_0. On the other hand, if $g(\deg p_0/\deg r_0) < \rho_0$, then for all sufficiently large $w_0 \in \mathcal{W}_0$, $(r_0(w_0), C_{w_0}(w_0), p_0(w_0))$ always has rho-value at most ρ_0, so if the exponent $1/\deg r_0$ in (7.2) is sufficiently large, $\nu(x)$ might grow faster than the total number of triples predicted by Estimates 3.2 or 5.1. The following lemma makes this precise.

LEMMA 7.3. *Let $\mathcal{P}$ be a polynomial family of triples. Let $I(k, K, \rho_0, (a, b))$ be as in* (4.1) *and $J(k, K_0^+, \rho_0, (a, b))$ be as in* (6.1). *Then, assuming the heuristics in* [**3**, **8**], *we have*

$$\lim_{x\to\infty} \frac{\nu(x)}{I(k, K, \rho_0, (2, x))} = \begin{cases} \infty & \text{if } \rho_0 < g(1 + (1/\deg r_0)), \\ A_2 & \text{if } \rho_0 = g(1 + (1/\deg r_0)), \\ 0 & \text{if } \rho_0 > g(1 + (1/\deg r_0)) \end{cases} \tag{7.3}$$

and

$$\lim_{x\to\infty} \frac{\nu(x)}{J(k, K_0^+, \rho_0, (2, x))} = \begin{cases} \infty & \text{if } \rho_0 < (2g/(g+2))(1 + (1/\deg r_0)), \\ A_3 & \text{if } \rho_0 = (2g/(g+2))(1 + (1/\deg r_0)), \\ 0 & \text{if } \rho_0 > (2g/(g+2))(1 + (1/\deg r_0)). \end{cases} \tag{7.4}$$

Proof. The first statement is clear when $\rho_0 \leqslant g$, since then $I(k, K, \rho_0, (2, x))$ remains bounded, $\rho_0 < g(1 + (1/\deg r_0))$ and $\nu(x) \to \infty$ by (7.2). If $\rho_0 > g$, we have

$$I(k, K, \rho_0, (2, x)) = \frac{e(k, K) g w_K h_{\tilde{\Phi}}}{\#(\mathrm{Aut}(K)) \rho_0 h_{\tilde{K}}} \int_2^x \frac{u^{(\rho_0/g)-2}\, du}{(\log u)^2} \sim \frac{e(k, K) g^2 w_K h_{\tilde{\Phi}}}{\#(\mathrm{Aut}(K)) \rho_0 (\rho_0 - g) h_{\tilde{K}}} \frac{x^{(\rho_0/g)-1}}{(\log x)^2},$$

as one sees by integrating by parts. The first statement in the lemma then follows by comparing the exponent $(\rho_0/g) - 1$ with the exponent $1/\deg r_0$ appearing in (7.2). The proof of the second statement is similar. □

DEFINITION 7.4. Let $\mathcal{P}$ be a polynomial family of triples of dimension g. If K is a CM-field of degree $2g$, we say that $\mathcal{P}$ has *constant CM-field K* if, for all $w_0 \in \mathcal{W}_0$, $\mathbb{Q}[X]/C_{w_0}(X)$ is isomorphic to K. Similarly, if K_0^+ is a totally real field of degree g, we say that $\mathcal{P}$ has a *constant maximal totally real subfield K_0^+* if, for all $w_0 \in \mathcal{W}_0$, $\mathbb{Q}[X]/C_{w_0}(X)$ contains a subfield isomorphic to K_0^+.

THEOREM 7.5. *Let g, k and $\rho_0 > 1$ be fixed.*

(i) *Let K be a CM-field of degree $2g$. Suppose that there exists a polynomial family of triples with fixed CM-field K such that $g(\deg p_0/\deg r_0) < \rho_0$ and $\rho_0 < g(1 + (1/\deg r_0))$. Then,*

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

assuming the Bateman–Horn–Conrad heuristics [**3**, **8**], *Estimate* 3.2 *is incorrect for at least one CM-type on* K.

(ii) *Let* K_0^+ *be a totally real field of degree* g. *Suppose that there exists a polynomial family of triples with constant maximal totally real subfield* K_0^+ *such that* $g(\deg p_0/\deg r_0) < \rho_0$ *and either*
(a) $\rho_0 < (2g/(g+2))(1+(1/\deg r_0))$ *or*
(b) $\rho_0 = (2g/(g+2))(1+(1/\deg r_0))$ *and the constant* A_3 *of Lemma* 7.3 *satisfies* $A_3 > 1$.
Then, assuming the Bateman–Horn–Conrad heuristics, Estimate 5.1 *is incorrect.*

(iii) *No other polynomial family is incompatible with Estimate* 3.2 *or* 5.1, *with the following possible exceptions:*
in (i), *families with either* $g(\deg p_0/\deg r_0) = \rho_0$ *and* $\rho_0 \leqslant g(1+(1/\deg r_0))$ *or* $g(\deg p_0/\deg r_0) < \rho_0$ *and* $\rho_0 = g(1+(1/\deg r_0))$;
in (ii), *families with* $g(\deg p_0/\deg r_0) = \rho_0$ *and* $\rho_0 \leqslant (2g/(g+2))(1+(1/\deg r_0))$.

Proof. (i) This follows from the first case of (7.3). (ii) Similarly, this follows using the first two cases of (7.4). (iii) If $g(\deg p_0/\deg r_0) > \rho_0$, then there can be only finitely many triples $(r_0(w_0), C_{w_0}, p_0(w_0))$ that have rho-value at most ρ_0, so the family cannot affect the asymptotics of Estimates 3.2 and 5.1. Similarly, if $\rho_0 > g(1+(1/\deg r_0))$, the third case of (7.3) shows that $\nu(x)$ grows too slowly to affect Estimate 3.2 and a similar argument works for Estimate 5.1 when $\rho_0 > (2g/(g+2))(1+(1/\deg r_0))$. We are left with the exceptional cases indicated. □

REMARK 7.6. The exceptional cases seem difficult to handle. If $g(\deg p_0/\deg r_0) = \rho_0$, it seems difficult to determine whether there are infinitely many triples in the family with rho-value at most ρ_0. In the fixed CM-field case (i), we cannot argue as in (ii) when $\rho_0 = g(1+(1/\deg r_0))$, since there is no reason for all the triples in a family to belong to the same CM-type.

REMARK 7.7. When $g=1$ and $k=12$, Theorem 7.5 predicts that the well-known Barreto–Naehrig family is inconsistent with Estimate 3.2 (or, rather, with its analogue for $g=1$). The Barreto–Naehrig family [**2**] has $r_0(w) = 36w^4+36w^3+18w^2+6w+1$, $p_0(w) = 36w^4+36w^3+24w^2+6w+1$ and $a_1(w) = -(6w^2+1)$. The field K is $\mathbb{Q}(\sqrt{-3})$, as one checks by computing the discriminant of $C_w(X)$, which is -3 times the square of a polynomial with rational coefficients. The generic rho-value is 1, and this is inconsistent with Estimate 3.2 when $1 < \rho_0 < \frac{5}{4}$. We obtain families inconsistent with Estimate 3.2 for any g by taking the isogeny classes of the gth powers of Barreto–Naehrig curves, with K being a CM-field containing $\mathbb{Q}(\sqrt{-3})$ and Φ being any CM-type on K whose restriction to $\mathbb{Q}(\sqrt{-3})$ is the identity. The inconsistency occurs when $g < \rho_0 < \frac{5}{4}g$, so that Corollary 1.3 holds in this case as well.

REMARK 7.8. The only cases where there are known to exist families of the form described in Theorem 7.5 and inconsistent with Estimate 5.1 occur when $g=2$ and $k=5$ or $k=10$. Four of the families listed in [**13**, Table 4] have this property. These are listed on Table 11.

See [**13**] for details of why these are polynomial families, and in particular how to check that the roots of $C_{w_0}(X)$ are Weil numbers when $w_0 \in \mathcal{W}_0$. If $w_0 \in \mathcal{W}_0$, the real quadratic subfield

TABLE 11. *Polynomial families inconsistent with Estimate* 5.1.

k	$r_0(w)$	$a_3(w)$	$a_2(w)$	$p_0(w)$
5	$2525w^4+2575w^3+990w^2+170w+11$	$-20w-6$	$1515w^2+780w+102$	$1010w^2+525w+69$
10	$25w^4+25w^3+15w^2+5w+1$	-2	$15w^2+10w+5$	$10w^2+5w+2$
10	$11w^4+21w^3+16w^2+6w+1$	$w-1$	$11w^2+12w+5$	$11w^2+10w+3$
10	$275w^4+475w^3+315w^2+95w+11$	$15w+4$	$165w^2+110w+20$	$55w^2+40w+8$

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

of $C_{w_0}(X)$ is generated by a root of $X^2 + a_3(w_0)X + a_2(w_0) - 2p_0(w_0)$. In each of the four families in the table, one sees that the discriminant of this polynomial in X has the form five times a square. This shows that the real quadratic subfield is always $\mathbb{Q}(\sqrt{5})$. In each case, the generic rho-value is 1, and again this is inconsistent with Estimate 5.1 when $1 < \rho_0 < \frac{5}{4}$.

The fact that polynomial families might provide sufficiently many triples to contradict the fixed maximal real subfield heuristics was only noticed as a result of a remark by the referee on the first version of this paper. When the above examples were found, a search was made for other families for other values of g and k. Let $\mathcal{P}$ be a polynomial family. Since the generic rho-value is at least 1, one has $\deg r_0 \leqslant g \deg p_0$. Since $r_0(w)$ divides $\Phi_k(p_0(w))$, we also have $\deg r_0 \leqslant \varphi(k)\deg p_0$. Also, the image of $p_0(w)$ under the canonical map $\mathbb{Q}[w]/r_0(w)$ is a primitive kth root of unity, which implies that $\varphi(k)$ divides $\deg r_0$. When $g = 1$, one deduces that no family can contradict Estimate 5.1. Suppose from now on that $g \geqslant 2$ and that the generic rho-value is 1. We shall see in Lemma 7.12 below that $\deg p_0 \geqslant 2$. A search was run when $g = 2$ and $g = 3$ for prime-representing polynomials p_0 with $\deg p_0 \geqslant 2$ and $\Phi_k(p_0(w))$ reducible, using both systematic searching by varying the coefficients of p_0 and using a method similar to that of [**13**], but, up to affine transformation, none were found except those appearing on the table. In conclusion, although the existence of other families that contradict Estimates 3.2 or 5.1 cannot be excluded, we believe that they are few and far between.

When the data in support of Estimate 5.1 was prepared, computations were made with $K_0^+ = \mathbb{Q}(\sqrt{5})$, $k = 5$ and $k = 10$, with r in the range $10^3 \leqslant r \leqslant 10^5$ (see Table 9 for the case $k = 5$). There are no members of the family with $k = 5$ in this range, one member of the first family with $k = 10$, no members of the second and two members of the third. The numerical rho-values are 1.17475, 1.26640 and 1.31191. On the other hand, when the complete lists of all triples with $\rho_0 \leqslant 1.3$, fixed maximal real subfield $\mathbb{Q}(\sqrt{5})$ and $10^3 \leqslant r \leqslant 10^5$ are examined, we find four triples when $k = 5$ and three triples when $k = 10$, while Estimate 5.1 predicts that in both cases there should be 4.866 triples. So, when the data was examined we were not led to suspect the existence of families such as those in Table 11.

Finally, we recall that, since the CM-field is variable, we cannot construct the abelian varieties corresponding to triples belonging to the families in Table 11 using the CM-method.

We end the paper with a brief discussion of the relationship between our Definition 7.1 of polynomial families and the definitions appearing in the work of other people. We also prove Lemma 7.12. For simplicity, we restrict our attention, as in Definition 7.1, to the case where $p_0(w)$ represents primes and not more general prime powers, although many other authors allow prime powers in their definitions in order to take account of families over non-prime fields.

Suppose first that $g = 1$. Then the most important polynomial families are the *Brezing–Weng* or *complete* families, first studied in a special case in [**6**] and discussed in detail in [**11**]; see in particular [**11**, Theorem 6.1]. The Barreto–Naehrig family mentioned in Remark 7.7 is an example. We have $C_w(X) = X^2 + a_1(w)X + p_0(w)$ and the family defines curves having CM by the same imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$, $D \geqslant 1$ a square-free integer, if and only if the discriminant $a_1^2(w) - 4p_0(w)$ of $C_w(X)$ is of the form $-Dy(w)^2$, with $y(w) \in \mathbb{Q}[w]$. If this is the case, and if we write $t(w) = -a_1(w)$, $q(w) = p_0(w)$ and $r_0(w) = r(w)$, it is not hard to see that our family becomes a family in the notation of [**11**, Theorem 6.1]. Note also that families defining curves with CM by varying fields give rise to sparse families as discussed in [**11**, § 5].

To handle the case $g \geqslant 2$, we use the following proposition, which is a consequence of a suitable explicit form of Hilbert's irreducibility theorem.

PROPOSITION 7.9. *Let F be a number field, let $f(X, w) \in F[X, w]$ be irreducible and let $\omega(x)$ denote the cardinality of the set of $w_0 \in \mathbb{Z}$ with $|w_0| \leqslant x$ and $f(X, w_0)$ reducible in $F[X]$. Then $\omega(x) = O(x^{1/2} \log x)$ as $x \to \infty$.*

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

Proof. This is just part of the special case $r = s = 1$, $k = \mathbb{Q}$ and $K = F$ of [**7**, Theorem 2.5]. □

Using Proposition 7.9 with $f(X, w) = C_w(X)$ and (7.1), we see that the number of $x_0 \in \mathcal{W}_0$ with $|x_0| \leqslant x$ and $C_{w_0}(X)$ reducible is $o(\mu(x))$, where μ is defined just before (7.1). Hence, we can suppose that $C_{w_0}(X)$ is irreducible for all $w_0 \in \mathcal{W}_0$ without affecting the heuristic estimates leading to Theorem 7.5.

LEMMA 7.10. *Let F be a finite extension of $\mathbb{Q}$ and let e be the degree of F over $\mathbb{Q}$. Suppose that $f(X, w)$ is an irreducible element of $\mathbb{Q}[X, w]$ of degree $d \geqslant 1$ in X. Then the following conditions are equivalent.*

(i) *There is a subset $\mathcal{W}$ of $\mathbb{Z}$ such that:*
   (a) *there exist $\alpha > \frac{1}{2}$ and $C > 0$ such that $\#(\mathcal{W} \cap [-x, x]) \geqslant Cx^{\alpha}$ for all sufficiently large x; and*
   (b) *for all $w_0 \in \mathcal{W}$, $f(X, w_0)$ is irreducible and $\mathbb{Q}[X]/f(X, w_0)$ contains a subfield isomorphic to F.*

(ii) *e divides d and $f(X, w)$ has an irreducible factor in $F[X, w]$ of degree d/e in X.*

Proof. Suppose that (i) holds. Since F is a subfield of $\mathbb{Q}[X]/f(X, w_0)$ which is of degree d over $\mathbb{Q}$, we see that e divides d. On the other hand, comparing Proposition 7.9 and the growth condition (a) of (i) shows that $f(X, w)$ must be reducible in $F[X, w]$. Since $f(X, w)$ has only finitely many irreducible factors, it follows that at least one of them (call it $g(X, w)$) has the property that the fields $F[X]/g(X, w_0)$ and $\mathbb{Q}[X]/f(X, w_0)$ are isomorphic for a positive proportion of $w_0 \in \mathcal{W}$. It follows that $g(X, w_0)$ is of degree d/e in X, as claimed. This proves that (i) implies (ii). To prove the converse, note that if $g(X, w)$ is an irreducible factor of $f(X, w)$ in $F[X, w]$ of degree d/e in X, then $f(X, w)$ is just the image of $g(X, w)$ under the norm map from F to $\mathbb{Q}$ extended in the usual way to a map from $F[X, w]$ to $\mathbb{Q}[X, w]$. □

REMARK 7.11. Let K be a CM-field of degree $2g$, let $\pi_0(w) \in K[w]$, $r_0(w) \in \mathbb{Q}[w]$ and let $k \geqslant 2$ be an integer. We say that (π_0, r_0) *represents a family of g-dimensional varieties with embedding degree k and complex multiplication by K* if:

(i) $p_0(w) = \pi_0(w)\overline{\pi}_0(w)$ lies in $\mathbb{Q}[w]$;

(ii) there is an infinite set $\mathcal{W}_0$ of integers such that $p_0(w_0)$ and $r_0(w_0)$ are prime numbers for all $w_0 \in \mathcal{W}_0$;

(iii) $\mathrm{N}_{K/\mathbb{Q}}(\pi_0(w) - 1)$ and $\Phi_k(p_0(w))$ are both divisible by $r_0(w)$. Here $\mathrm{N}_{K/\mathbb{Q}}$ denotes the map $K[w] \to \mathbb{Q}[w]$ induced by the norm map from K to $\mathbb{Q}$.

Assuming a weak form of the Bateman–Horn–Conrad heuristics, this definition is essentially equivalent to Definition 3.6 in Freeman's paper [**10**]. Let $C_w(X) = \mathrm{N}_{K/\mathbb{Q}}(X - \pi_0(w))$ and suppose that $C_w(X)$ is irreducible. If $w_0 \in \mathcal{W}_0$, then $C_{w_0}(X)$ is the characteristic polynomial of the corresponding abelian variety, and we obtain a polynomial family in the sense of Definition 7.1 with fixed CM-field K.

Conversely, let $\mathcal{P}$ be a polynomial family in the sense of Definition 7.1 with fixed CM-field K. Then, assuming the Bateman–Horn–Conrad heuristics, we can suppose that $\mathcal{W}_0$ satisfies the condition on $\mathcal{W}$ in (i) of Lemma 7.10. We deduce that $C_w(X)$ has a factor of degree one in X in $K[X, w]$, which we can write as $X - \pi_0(w)$ with $\pi_0(w) \in K[w]$. Using the fact that, when $w_0 \in \mathcal{W}_0$, the roots of $C_{w_0}(X)$ are $p_0(w_0)$-Weil numbers, we conclude that $\pi_0(w)\overline{\pi}_0(w) = p_0(w)$. Thus, Freeman's definition is essentially equivalent to our Definition 7.1 of families $\mathcal{P}$ having fixed CM-field K.

Finally, we use Lemma 7.10 to prove Lemma 7.12, which was used in Remark 7.8.

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press

LEMMA 7.12. *When $g \geqslant 2$, there are no polynomial families with constant maximal real subfield, generic rho-value equal to* 1 *and* $\deg p_0 = 1$.

Proof. When $g \geqslant 2$, one finds that if $\deg p_0 = 1$, then $\deg r_0 = \varphi(k)$. Furthermore, $g = \varphi(k)$ since the generic rho-value is 1. Let K_0^+ denote the fixed maximal real subfield, which is of degree g. Using Lemma 7.10 and the fact that the roots of the $C_{w_0}(X)$ are $p_0(w_0)$-Weil numbers, we see that $C_w(X)$ has a factor of the form $X^2 - \tau_0(w)X + p_0(w)$ in $K_0^+[X, w]$. Up to affine transformation, we can suppose that $p_0(w) = w$ and $r_0(w) = \Phi_k(w)$. Now the roots of $X^2 - \tau_0(w_0)X + w_0$ generate a quadratic CM-extension of K_0^+; by looking at the discriminant $\tau_0(w)^2 - 4w$ of $X^2 - \tau_0(w)X + w$, we deduce that $\tau_0(w)$ is a constant polynomial, equal to $\beta \in K_0^+$, say. It follows that $C_w(1)$ is divisible by $w - \beta + 1$ in $K_0^+[w]$. But $r_0(w)$ divides $C_w(1)$ in $\mathbb{Q}[w]$, and both polynomials are of degree g. It follows that $C_w(1)$ is a constant multiple of $r_0(w)$, so that $r_0(w)$ has a factor of degree one in $K_0^+[w]$. But $r_0(w) = \Phi_k(w)$, and this implies that K_0^+ contains a primitive kth root of unity ζ_k. Since $g = \varphi(k) \geqslant 2$, ζ_k is imaginary, so cannot belong to the totally real field K_0^+. This contradiction concludes the proof. □

Acknowledgements. We would like to thank the referee for his/her comments which have helped us to much improve the paper, and in particular make us realize that suitable polynomial families could provide counterexamples to our heuristics for a fixed maximal totally real subfield.

References

1. R. BALASUBRAMANIAN and N. KOBLITZ, 'The improbability that an elliptic curve has subexponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm', *J. Cryptology* 11 (1998) 141–145.
2. P. BARRETO and M. NAEHRIG, 'Pairing-friendly elliptic curves of prime order', *Selected areas in cryptography (SAC 2005)*, Lecture Notes in Computer Science 3897 (Springer, Berlin, 2006) 319–331.
3. P. T. BATEMAN and R. A. HORN, 'A heuristic asymptotic formula concerning the distribution of prime numbers', *Math. Comp.* 16 (1962) 363–367.
4. W. BOSMA, J. CANNON and C. PLAYOUST, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* 24 (1997) 235–265.
5. J. BOXALL, 'Heuristics on pairing-friendly elliptic curves', *J. Math. Cryptol.* 6 (2012) 81–104.
6. F. BREZING and A. WENG, 'Elliptic curves suitable for pairing based cryptography', *Des. Codes Cryptogr.* 37 (2005) 133–141.
7. S. D. COHEN, 'The distribution of Galois groups and Hilbert's irreducibility theorem', *Proc. Lond. Math. Soc.* 43 (1981) 227–250.
8. K. CONRAD, 'Hardy–Littlewood constants', *Mathematical properties of sequences and other combinatorical structures (Los Angeles, CA, 2002)* (Kluwer Academic, Boston, MA, 2003) 133–154.
9. A. ENGE and A. V. SUTHERLAND, 'Class invariants by the CRT method', *Algorithmic number theory (ANTS 9)*, Lecture Notes in Computer Science 6197 (Springer, Berlin, 2010) 142–156.
10. D. FREEMAN, 'A generalized Brezing–Weng method for constructing pairing-friendly ordinary abelian varieties', *Pairing-based cryptography: Pairing 2008*, Lecture Notes in Computer Science 5209 (Springer, Berlin, 2008) 146–163.
11. D. FREEMAN, M. SCOTT and E. TESKE, 'A taxonomy of pairing-friendly elliptic curves', *J. Cryptology* 23 (2010) 224–280.
12. D. FREEMAN, P. STEVENHAGEN and M. STRENG, 'Abelian varieties with prescribed embedding degree', *Algorithmic number theory (ANTS 8)*, Lecture Notes in Computer Science 5011 (Springer, Berlin, 2008) 60–73.
13. S. GALBRAITH, J. MCKEE and P. C. VALENÇA, 'Ordinary abelian varieties having small embedding degree', *Finite Fields Appl.* 13 (2007) 800–814.
14. T. HONDA, 'Isogeny classes of abelian varieties over finite fields', *J. Math. Soc. Japan* 20 (1968) 83–95.
15. J. JIMÉNEZ URROZ, F. LUCA and I. SHPARLINSKI, 'On the number of isogeny classes and pairing-friendly elliptic curves and statistics for MNT curves', *Math. Comp.* 81 (2012) 1093–1110.
16. D. KOHEL, 'Echidna databases. Databases for elliptic curves and higher dimensional analogues', http://echidna.maths.usyd.edu.au/∼kohel/dbs/.
17. E. LANDAU, *Handbuch der Lehre von der Verteilung der Primzahlen* (Teubner, Leipzig, 1909).
18. K. LAUTER and N. SHANG, 'Generating pairing-friendly parameters for the CM construction of genus 2 curves over prime fields', *Des. Codes Cryptogr.* 67 (2013) no. 3, 341–355.

19. F. Luca and I. Shparlinski, 'Elliptic curves of low embedding degree', *J. Cryptology* 19 (2006) 553–562.
20. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers* (Polish Scientific, Warsaw, 1974).
21. K. Rubin and A. Silverberg, 'Using abelian varieties to improve pairing-based cryptography', *J. Cryptology* 22 (2009) 330–364.
22. M. Sha, 'Heuristics of the Cocks–Pinch method', *Adv. Math. Commun.* 8 (2014) 103–118.
23. G. Shimura, 'Abelian varieties with complex multiplication and modular functions', Princeton Mathematical Series 46 (Princeton University Press, Princeton, NJ, 1997).
24. J. T. Tate, 'Endomorphisms of abelian varieties over finite fields', *Invent. Math.* 2 (1966) 134–144.
25. J. T. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'aprés T. Honda), Séminaire Bourbaki, vol. 1968/69: Exposés 347–363*, Lecture Notes in Mathematics 179 (Springer, Berlin, 1971) 95–110. Exp. 352.
26. W. C. Waterhouse, 'Abelian varieties over finite fields', *Ann. Sci. Éc. Norm. Supér.* (4) 2 (1969) 521–560.
27. A. Weil, *Courbes algébriques et variétés abéliennes* (Hermann, Paris, 1948).

John Boxall
Laboratoire de Mathématiques Nicolas Oresme, CNRS, UMR 6139
Université de Caen Basse-Normandie
Esplanade de la Paix
14032 Caen cedex 5
France
john.boxall@unicaen.fr

David Gruenewald
School of Mathematics and Statistics
University of Sydney, NSW 2006
Australia
davidg@maths.usyd.edu.au

https://doi.org/10.1112/S1461157015000091 Published online by Cambridge University Press