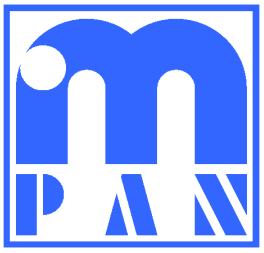
INSTITUTE OF MATHEMATICS
of the
Polish Academy of Sciences



ul. Śniadeckich 8, P.O.B. 21, 00-956 Warszawa 10, Poland http://www.impan.pl

IM PAN Preprint 715 (2010)

Robert Dryło

On Constructing Optimal Families of Pairing-friendly Elliptic Curves

Presented by Zbigniew Jelonek

Published as manuscript

Received 11 March 2010

ON CONSTRUCTING OPTIMAL FAMILIES OF PAIRING-FRIENDLY ELLIPTIC CURVES

ROBERT DRYŁO

Abstract. Pairing-friendly elliptic curves have the rare property that the Weil or Tate pairing on points of some large prime order can be efficiently computed. Thanks to this they are useful in cryptography for implementing protocols based on these pairings. To construct ordinary pairing-friendly curves one usually obtains parameters of a curve as values of certain polynomials, and then finds its equation via the complex multiplication method. Such polynomials are called families. There is essentially one general method for constructing the so-called complete families, which in the fullest generality is due to Brezing and Weng. No general methods have been proposed for constructing (i) arbitrary families, and (ii) families of curves of nearly prime group order. In this paper we propose two methods for the first purpose, which extend the Brezing-Weng method and the Dupont-Enge-Morain method for constructing individual pairing-friendly curves. Furthermore, we describe all arbitrary families $(r(x), t(x), q(x))$ with embedding degree k satisfying (ii) for which $\mathbb{Q}[x]/(r(x)) \cong K$, where K is a fixed number field containing kth roots of unity (in fact, we describe families with parameter $\rho \leq \rho_0$ for a given bound $1 \leq \rho_0 < 2$). This allows one to represent such families by rational solutions of certain systems of polynomial equations.

1. Introduction

Elliptic curves containing a subgroup of large prime order with a small embedding degree are commonly used for implementing cryptographic schemes based on bilinear pairings (see, e.g., [4, 5, 12]). However, such pairing-friendly curves are very rare [1, 14] and thus require special selection. Natural examples come from supersingular curves, whose embedding degrees are not greater than 6 [16]. All known methods for constructing suitable ordinary curves are based on the complex multiplication method, and either give individual curves or families of curves (see [10] for a survey). The former methods, however, usually produce curves for which the order of the desired subgroup is approximately equal to the square root of the curve order, while usually the most desirable curves for applications should have prime or nearly prime order. Curves with better parameters can be obtained by using families, although no general method is known for constructing families of pairing-friendly curves with nearly prime group order (see [5, Section 4.5], and [9, Problem 6.2]). According to the standard notation, such families are those with parameter $\rho = 1$, and are currently known only for embedding degrees $3, 4, 6, 10, 12$; see [3, 9, 11, 17, 18].

Another problem is that no general method has been proposed for constructing families of arbitrary types. Such methods have been developed for constructing so-called complete families, and all essentially work like the Brezing-Weng method [6]. The use of this method to construct families with desired properties has been extensively examined. The main goal was to minimize the

Key words and phrases. Pairing-friendly elliptic curves, systems of polynomial equations.
Research partially supported by the Polish Minister of Science as a project nr 0 R00 004307 in years 2009-2011.

ρ-value, and it seems that this was successfully achieved in many cases (see [10]). Sparse families, unlike complete families, have been much less studied. It is interesting that among the currently known families with $\rho = 1$ those with embedding degrees $3, 4, 6, 10$ are all sparse (in fact, it seems that those are also all currently known sparse families).

In this paper we describe two general methods for constructing arbitrary families (Section 4). They extend the Brezing-Weng method and the Dupont-Enge-Morain method [8] for constructing individual pairing-friendly curves. Note that the former method requires finding rational solutions of certain systems of polynomial equations, while the latter avoids this and allows constructing families with prescribed so-called CM equation. However, just as other methods, also these methods generically produce families with $\rho \approx 2$. To improve this, we focus on the problem of constructing, via the generalized Brezing-Weng method, families with $\rho \leq \rho_0$ for a given bound $1 \leq \rho_0 < 2$. More precisely, we characterize all families $(r(x), t(x), q(x))$ with embedding degree k and $\rho \leq \rho_0$ for which $\mathbb{Q}[x]/(r(x)) \cong K$, where K is a fixed number field containing kth roots of unity. This allows one to represent such families by rational solutions of certain systems of polynomial equations. Unfortunately, those systems rapidly become complicated when the degree $n = [K : \mathbb{Q}]$ increases (in fact, they come from minors of some matrices). For example, determining (up to a linear change of variables) complete families with $\rho = 1$ requires finding rational solutions in some open subset of $\mathbb{P}^{n-2}(\mathbb{C})$ of a certain system of forms of degree $n(n-1)/4$. We also give a lower bound on the dimension of the corresponding algebraic set if it is nonempty. For complete families with $\rho = 1$ this lower bound equals 0, when it is attained there are only finitely many equivalence classes of such families. The case of arbitrary families is more complicated and generally requires finding rational zeros in some open subset of $\mathbb{P}^{n-2}(\mathbb{C}) \times \mathbb{P}^{n-1}(\mathbb{C})$ of certain forms of degrees similar to the above. For families with $\rho = 1$ a lower bound on the dimension of the corresponding algebraic set equals 1. (See Sections 3 and 5 for the case of complete and arbitrary families, respectively.)

Notice that these results are of interest for families of degree greater than 2, as for quadratic families more precise methods, due to Miyaji et al. [17] and generalized by Scott and Barreto [18] and Galbraith et al. [11], allow one to parameterize all elliptic curves with embedding degrees $3, 4, 6$ and prescribed cofactors. For quartic families the resulting systems can be solved via standard methods (in particular, we explain how from this point of view the families of Barreto-Naehrig [3] and Freeman [9] arise; see Examples 3.2 and 5.2). However, it seems that for families of higher degrees more sophisticated methods should be used.

2. Framework

This section provides terminology and basic facts that will be used in this paper. For a detailed discussion of pairing-friendly elliptic curves and their applications we refer to the work of Freeman, Scott and Teske [10].

Let E be an elliptic curve over a finite field $\mathbb{F}_q$, and r be a prime number with $\gcd(r,q)=1$ dividing the order $\#E(\mathbb{F}_q)$. *The embedding degree of E with respect to r* is defined to be the smallest integer k such that $r \mid q^k-1$ (if $r \not| k$, this is equivalent to the condition that $r \mid \Phi_k(t-1)$, where $t=q+1-\#E(\mathbb{F}_q)$ is the trace of E, and Φ_k is the kth cyclotomic polynomial).

An elliptic curve is commonly called *pairing-friendly* if it can be used for secure and efficient implementation of cryptographic protocols based on the Weil or Tate pairings. This means that both in an r-order subgroup of E and in the multiplicative group of the field $\mathbb{F}_{q^k}$ the discrete logarithm problem is hard, but the arithmetic is efficient. For the latter purpose, the embedding degree k should be reasonably small, and r should have a relatively small cofactor with respect to $\#E(\mathbb{F}_q)$. By Hasse's theorem, the ratio of the bit sizes of $\#E(\mathbb{F}_q)$ and r is closely approximated by the parameter $\rho=\log q/\log r$.

Usually constructions of ordinary pairing-friendly curves proceed in two steps. First for a fixed embedding degree k one finds the curve parameters r,t,q, where r and q are prime numbers such that there exists an ordinary elliptic curve over the field $\mathbb{F}_q$ with trace t, that contains a subgroup of order r with embedding degree k. Then the equation of such a curve is found via the complex multiplication (CM) method. However, the CM method is efficient provided that the discriminant D of the curve (defined as the square-free part of the integer $4q-t^2>0$) is sufficiently small. Therefore, in practice one also fixes a discriminant D, and looks for the above parameters satisfying the equation $4q-t^2=Dy^2$ for some $y\in\mathbb{Z}$.

This can be done directly by using either the method of Cocks-Pinch [7] or Dupont-Enge-Morain [8]. However, these methods usually only achieve $\rho\approx 2$. Improvements are possible by obtaining such parameters as values of certain polynomials $r(x),t(x),q(x)\in\mathbb{Q}[x]$. This approach leads to the notion of a family of pairing-friendly elliptic curves, which in its final form was established by Freeman, Scott and Teske [10]. The definition requires two auxiliary notions. A polynomial $r(x)\in\mathbb{Q}[x]$ is said to *represent integers* (resp. *represent primes*) if $r(x)\in\mathbb{Z}$ for all $x\in\mathbb{Z}$ (resp. $r(x)$ is a prime number for infinitely many $x\in\mathbb{Z}$). The latter property is conjecturally equivalent to the following conditions: $r(x)$ is irreducible, has positive leading coefficient, $r(x)\in\mathbb{Z}$ for some $x\in\mathbb{Z}$, and $\gcd(\{r(x): x, r(x)\in\mathbb{Z}\})=1$.

Definition 2.1. Let k and D be positive integers, and assume D is square-free. A triple of polynomials $(r(x),t(x),q(x))$ in $\mathbb{Q}[x]$ is said to *represent a family of elliptic curves with embedding degree k and discriminant D* if the following conditions are satisfied:
(i) $r(x)$ is irreducible, has positive leading coefficient, and represents integers;
(ii) $q(x)$ represents primes;
(iii) $r(x)$ divides $q(x)+1-t(x)$ and $\Phi_k(t(x)-1)$;
(iv) the CM equation

$$4q(x)-t(x)^2=Dy^2$$

has infinitely many solutions $(x,y)\in\mathbb{Z}^2$.

Remark 2.2. Notice that the last and least explicit condition of this definition is actually very strong. It was observed by Freeman [9] that then the left-hand side of the CM equation is of the form $g(x)h(x)^2$, where $g(x), h(x) \in \mathbb{Q}[x]$ and $\deg g(x) \leq 2$ (this easily follows from Siegel's theorem [19, Theorem 4.3]).

To find parameters of an actual elliptic curve that occurs in a family, one starts with an integer solution (x_0, y_0) of the CM equation and checks whether the values $r(x_0), t(x_0), q(x_0)$ give such parameters. Notice that for large x_0 the ρ-values of the resulting curves are close to the ρ-value of a family, defined as

$$\rho = \lim_{x\to\infty} \frac{\log q(x)}{\log r(x)} = \frac{\deg q(x)}{\deg r(x)}.$$

The density of integer solutions of the CM equation and methods for determining them primarily depend on the degree of the polynomial $g(x)$ in the above remark. The ideal case occurs when the left-hand side of the CM equation is of the form $Dy(x)^2$ for $y(x) \in \mathbb{Q}[x]$. Then the family is called *complete*; otherwise the family is called *sparse* (see [10] for more details).

Methods for constructing families usually do not yield families exactly in the sense of the above definition, but only so-called potential families satisfying certain necessary conditions. For constructive purposes, a natural definition of such families is the following.

Definition 2.3. A triple of polynomials $(r(x), t(x), q(x))$ in $\mathbb{Q}[x]$ *represents a potential family of elliptic curves with embedding degree* k if:
(i) $r(x)$ is irreducible, and divides $q(x) + 1 - t(x)$ and $\Phi_k(t(x) - 1)$;
(ii) $4q(x) - t(x)^2 = g(x)h(x)^2$, where $g(x), h(x) \in \mathbb{Q}[x]$ and $\deg g(x) \leq 2$.

Similarly as above, we define the parameter ρ for potential families, and complete potential families. By a family we will usually understand a family in the sense of Definition 2.1.

Remark 2.4. Clearly a potential family (r, t, q) may be very far from being a family. For example, q may not represent primes, or q and t may never take simultaneously integer values for $x \in \mathbb{Z}$, or $4q - t^2$ may have negative leading coefficient (e.g., if $r \mid \Phi_k(t-1)$, then even the triple (r, t, q) with $q = t - 1$ is a potential family for which $q + 1 - t = 0$ and $4q - t^2 = -(t-2)^2$). However, in the first two cases it may happen that $(ar(x + b), t(x + b), q(x + b)$ will be a family for some $a, b \in \mathbb{Q}$. Checking this essentially comes down to checking whether for a given $f(x) \in \mathbb{Q}[x]$ there exists $x_0 \in \mathbb{Q}$ such that $f(x_0) \in \mathbb{Z}$. This is a finite calculation. If $Nf(x) \in \mathbb{Z}[x]$ for $N \in \mathbb{Z}$, then it suffices to check whether $Nf(r/s) \in N\mathbb{Z}$ for each divisor s of the leading coefficient of $Nf(x)$, and $0 \leq r < |Ns|$. (Indeed, if $Nf(a/s) \in N\mathbb{Z}$ and $\gcd(a, s) = 1$, then s divides the leading coefficient of $Nf(x)$, and if $a = Nsq + r$ for $q \in \mathbb{Z}$ and $0 \leq r < |Ns|$, then $Nf(r/s) \in N\mathbb{Z}$.)

Sometimes it is convenient to determine families up to the following equivalence relation.

Definition 2.5. Two potential families $(r_i(x), t_i(x), q_i(x))$, $i = 1, 2$, are *linearly equivalent* if $(r_1(x), t_1(x), q_1(x)) = (cr_2(ax + b), t_2(ax + b), q_2(ax + b))$ for some $a, b, c \in \mathbb{Q}$ with $ac \neq 0$.

Finally, we recall the Brezing-Weng method for constructing complete families.

Proposition 2.6. *Let K be a number field containing kth roots of unity and $\sqrt{-D}$ for a square-free integer $D > 0$. Suppose that $r(x) \in \mathbb{Q}[x]$ is an irreducible polynomial such that $\mathbb{Q}[x]/(r(x)) \cong K$. Let $t(x), y(x) \in \mathbb{Q}[x]$ be the lifts of degree less than $\deg r(x)$ of $\zeta+1$ and $(\zeta-1)/\sqrt{-D}$, respectively, where $\zeta \in \mathbb{Q}[x]/(r(x))$ is a kth primitive root of unity. Let $q(x) = \frac{1}{4}(t(x)^2+Dy(x)^2)$. Then the triple $(r(x), t(x), q(x))$ represents a complete (potential) family of elliptic curves with embedding degree k and discriminant D. The ρ-value of this family is $\rho = \max\{2\deg t(x), 2\deg y(x)\}/\deg r(x) < 2$.*

Clearly, in order to construct, via this method, families with small ρ-value, one must carefully choose the polynomial $r(x)$. In the first constructions of Barreto, Lynn and Scott [2] and Brezing and Weng [6], r was simply the lth cyclotomic polynomial for l divisible by k. This natural choice turned out to be very successful in some cases; it also allows one to carry out more general constructions with variable k for which ρ tends to 1 as k increases (see [10]).

The advantage of using another representation of cyclotomic fields was first demonstrated by Barreto and Naehrig [3] by constructing a complete family with $k = 12$ and $\rho = 1$. They used the fact that evaluating the 12th cyclotomic polynomial at $u(x) = 6x^2$ yields the reducible polynomial $\Phi_{12}(u(x)) = r(x)r(-x)$ with irreducible $r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$. Then the desired family is represented by $r(x)$, $t(x) = u(x) + 1$, and $q(x) = r(x) + t(x) - 1$.

A useful way to look for suitable polynomials $r(x)$ is to generate them as minimal polynomials of primitive elements of K; this method was used by Kachisa, Schaefer and Scott [13]. In the next section we describe all primitive elements of K that determine complete families with $\rho \le \rho_0$ for a given bound $1 \le \rho_0 < 2$.

3. Complete families with $\rho \le \rho_0$

Let K be a number field of degree $n = [K : \mathbb{Q}]$ containing kth roots of unity and $\sqrt{-D} \in K$ for a positive square-free integer D. For a given bound $1 \le \rho_0 < 2$, we describe all families with $\rho \le \rho_0$ satisfying the following condition

(3.1) (r, t, q) is a complete potential family with embedding degree k, discriminant D, such that $\mathbb{Q}[x]/(r) \cong K$.

It will be convenient to represent such families with $\rho < 2$ by the following pairs from K.

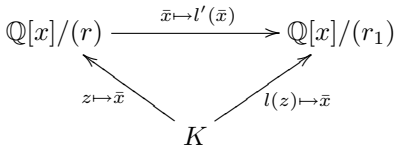
(3.2) $(z, \zeta) \in K^2$, z is a primitive element of K, and ζ is a kth primitive root of unity.

According to Proposition 2.6, such a pair (z, ζ) determines the family (r, t, q), where r is the minimal polynomial of z, $q = \frac{1}{4}(t^2 + Dy^2)$, and $t, y \in \mathbb{Q}[x]$ are the lifts of degree less than n of $\varphi(\zeta) + 1$ and $(\varphi(\zeta) - 1)/\sqrt{-D}$, respectively, where $\varphi : K \to \mathbb{Q}[x]/(r)$ is the isomorphism $z \mapsto \bar{x}$. Obviously, every family (3.1) with r monic and $\rho < 2$ arises in this way, and two pairs (z_1, ζ_1), (z_2, ζ_2) determine the same family iff $(z_2, \zeta_2) = (\varphi(z_1), \varphi(\zeta_1))$ for an automorphism φ of K.

We also introduce an equivalence relation in the set of all pairs (3.2), which corresponds to linear equivalence of families (Definition 2.5). We declare (z_1, ζ_1) and (z_2, ζ_2) to be equivalent if $z_2 = a\varphi(z_1) + b$ and $\zeta_2 = \varphi(\zeta_1)$ for an automorphism φ of K and $a, b \in \mathbb{Q}$ with $a \neq 0$. Then there is the induced bijection

$$\{\text{pairs (3.2)}\}/\sim \longrightarrow \{\text{families (3.1) with } \rho < 2\}/\sim. \tag{3.3}$$

Proof. Let us check that this map is well defined. Let (r, t, q) and (r_1, t_1, q_1) be two families determined by equivalent pairs (z, ζ) and $(l(\varphi(z)), \varphi(\zeta))$, respectively, where $l(x) \in \mathbb{Q}[x]$ is of degree one and $\varphi \in \mathrm{Aut}(K)$. We may assume $\varphi = \mathrm{id}$, since conjugate pairs determine the same family. Since r and r_1 are minimal polynomials of z nad $l(z)$, respectively, we have $r_1(x) = cr(l'(x))$ for some $c \in \mathbb{Q}$, and $l' \in \mathbb{Q}[x]$ satisfying $l'(l(x)) = x$. Hence the following diagram of fields isomorphisms is commutative



From this it follows that $t_1(x) = t(l'(x))$, and $q_1(x) = q(l'(x))$, so these families are equivalent. Surjectivity of the map (3.3) is obvious. Its injectivity is also easily seen from the above diagram. □

In order to express the ρ-value of a family in terms of such pairs, denote by $\deg_z a$, where z is a primitive element of K and $a \in K^*$, the smallest integer $i \geq 0$ such that a belongs to the subspace generated by $1, z, \ldots, z^i$. Then it is easy to see that a pair (z, ζ) determines the family with

$$\rho = \tfrac{1}{n} \max\{2 \deg_z \zeta, 2 \deg_z(\zeta - 1)/\sqrt{-D}\}. \tag{3.4}$$

Now for a fixed kth primitive root of unity $\zeta \in K$, a basis $b_1, \ldots, b_n$ of $K/\mathbb{Q}$, and a bound $1 \leq \rho_0 < 2$, we derive conditions on coordinates in this basis of all primitive elements $z \in K$ for which the pairs (z, ζ) determine families with $\rho \leq \rho_0$. Notice that we may assume $\rho_0 = 2B/n$ for an integer $n/2 \leq B < n$, since ρ-values of the families in question are of such form.

Writing $b_i b_j = \sum_l a_{ij}^{(l)} b_l$ with rational numbers $(a_{ij}^{(l)})_{i,j,l=1,\ldots,n}$, one can compute homogeneous polynomials $f_{ij} \in \mathbb{Q}[X_1, \ldots, X_n]$, $i = 1, \ldots, n, j = 0, \ldots, n-1$, such that

$$\Big(\sum_i x_i b_i\Big)^j = \sum_i f_{ij}(x) b_i$$

for all $x = (x_1, \ldots, x_n) \in \mathbb{Q}^n$. Let $u_{l1}, \ldots, u_{ln} \in \mathbb{Q}$ for $l = 1, 2$ be the coordinates in our basis of ζ and $(\zeta - 1)/\sqrt{-D}$, respectively. Consider the two $n \times (B+2)$ matrices

$$M_l = \begin{bmatrix} f_{10} & \cdots & f_{1B} & u_{l1} \\ \vdots & \ddots & \vdots & \vdots \\ f_{n0} & \cdots & f_{nB} & u_{ln} \end{bmatrix} \text{ for } l = 1, 2,$$

and the $n \times n$ matrix $M = [f_{ij}]$. For $x \in \mathbb{Q}^n$ denote by $M(x)$ and $M_l(x)$ the matrices obtained from M and M_l by evaluating their entries at x. Using (3.4), we now find the following.

(3.5) *Let* $x = (x_1, \dots, x_n) \in \mathbb{Q}^n$ *and* $z = \sum_{i=1}^n x_i b_i$. *Then* z *is a primitive element of* K *and the pair* (z, ζ) *determines the family with parameter* $\rho \le \rho_0$ *if and only if* $\det M(x) \neq 0$ *and* $\operatorname{rank} M_1(x) = \operatorname{rank} M_2(x) \le B + 1$*; or equivalently, if* x *is a solution of the system* $F_1 = \cdots = F_m = 0,\ F \neq 0$, *where* $F_1, \dots, F_m$ *are all the maximal minors of* M_1, M_2, *and* $F = \det M$.

Now an obvious approach would be to solve this system over $\mathbb{C}$, and then try to find some its rational solutions (note that the condition $F \neq 0$ can be replaced by the equation $YF = 1$, where Y is a new variable). Unfortunately, this may be difficult even for quite small n, because these systems rapidly become complicated (e.g., since $\deg f_{ij} = j$, we have $\deg F_i = B(B+1)/2$, and $\deg F = n(n-1)/2$). The situation slightly simplifies when we consider families up to linear equivalence. Suppose that $b_1 = 1$, and put $G_i = F_i(0, X_1, \dots, X_{n-1})$, $G = F(0, X_1, \dots, X_{n-1})$.

Theorem 3.1. *Let* V *be the set of all solutions of the system* $G_1 = \cdots = G_m = 0,\ G \neq 0$ *in the projective space* $\mathbb{P}^{n-2}(\mathbb{C})$.
(i) Then the rational points on V *determine all equivalence classes of families characterized by (3.5), and each class is represented by at most* $[K : \mathbb{Q}(\zeta)]$ *such points. Furthermore, if* $K/\mathbb{Q}$ *is Galois, then all equivalence classes of families (3.1) with* $\rho \le \rho_0$ *are represented in this way.*
(ii) If V *is nonempty, then all its irreducible components have dimension* $\ge 2B - n$.

Proof. (i) By (3.3), it suffices to show this for equivalence classes of pairs (3.2). If $(x_1, \dots, x_n) \in \mathbb{Q}^n$ is a solution of the system $F_1 = \cdots = F_m = 0,\ F \neq 0$, then the pairs $(\sum_{i=1}^n x_i b_i, \zeta)$ and $(\sum_{i=2}^n x_i b_i, \zeta)$ are equivalent (since $b_1 = 1$) and their class is determined by the point $x = (x_2 : \cdots : x_n) \in V$. Furthermore, if for $y = (y_2 : \cdots : y_n) \in V$ the pairs $(\sum_{i=2}^n y_i b_i, \zeta)$ and $(\sum_{i=2}^n x_i b_i, \zeta)$ are equivalent, then $\sum_{i=2}^n y_i b_i = \varphi(\sum_{i=2}^n \lambda x_i b_i)$ for $\lambda \in \mathbb{Q}^*$ and $\varphi \in \operatorname{Aut}(K/\mathbb{Q}(\zeta))$. Thus rational points on V representing the same class are all conjugate by the action of the automorphism group $\operatorname{Aut}(K/\mathbb{Q}(\zeta))$ on V, hence there are at most $[K : \mathbb{Q}(\zeta)]$ such points. Finally, if K is Galois, then each pair (3.2) is equivalent to (z, ζ) for some $z \in K$.
(ii) We show that V is the intersection of $2(n - (B+1))$ hypersurfaces, which implies that $\dim V \ge n - 2 - 2(n - (B+1)) = 2B - n$, if $V \neq \emptyset$ (see, e.g., [15, Corollary 3.14]). Consider the inverse matrix $M^{-1} = \frac{1}{F}[M_{ij}]^T$, where $M_{ij} = (-1)^{i+j}$ times the (i,j)th minor of M. Then for each $x = (x_1, \dots, x_n) \in \mathbb{Q}^n$ with $F(x) \neq 0$, the matrix $M^{-1}(x)$ is the transition matrix from the basis $b_1, \dots, b_n$ to the basis $1, z, \dots, z^{n-1}$ for $z = \sum x_i b_i$. Hence, (z, ζ) represents the family with $\rho \le \rho_0$ iff $\sum_{j=1}^n u_{lj} M_{ji}(x) = 0$ for $i = B+2, \dots, n$ and $l = 1, 2$. Thus $V = \{\sum_{j=1}^n u_{lj} M_{ji}(0, X_1, \dots, X_{n-1}) = 0 : i = B+2, \dots, n, l = 1, 2\} \cap \{G \neq 0\}$, which concludes the proof. □

Notice that if the forms from the proof of (ii) behave on the open set $G \neq 0$ like generic forms, then one might expect that $\dim V = 2B - n$. In particular, if this is the case for $\rho_0 = 1$, then $\dim V = 0$, and consequently, there are only finitely many classes of complete families. However, note that the forms $G_1, \dots, G_m$ have usually many zeros on the hypersurface $G = 0$. For example,

they vanish on all rational points of this hypersurface, since such points determine elements from proper subfields of K, so satisfy conditions $\operatorname{rank} M_i \leq B+1$, $i=1,2$.

Example 3.2. For an example of how the above theorem works, let us determine all complete families (r,t,q) with $k=12$, $\rho=1$, and such that $\mathbb{Q}[x]/(r) \cong K$, where K is the 12th cyclotomic field (a well known example of such a family is the Barreto-Naehrig family). Then $[K:\mathbb{Q}]=4$ and $\sqrt{-3} \in K$. Let $\zeta \in K$ be a 12th primitive root of unity. The coordinates of ζ and $(\zeta-1)/\sqrt{-3}$ in the standard basis $1,\zeta,\zeta^2,\zeta^3$ are $(0,1,0,0)$ and $(-1/3,1/3,2/3,-2/3)$. Then the matrices M_1 and M_2 are quadratic, and the corresponding polynomials G_1, G_2, and G are the following
$G_1 = -X_1^2X_3 + 2X_1X_2^2 - 2X_1X_3^2 + X_2^2X_3$,
$G_2 = -2/3X_1^3 - 4/3X_1^2X_2 - 5/3X_1^2X_3 - 4/3X_1X_2X_3 - 2/3X_1X_3^2 - X_2^2X_3 - 4/3X_2X_3^2$,
$G = X_1^6 + 5X_1^5X_3 - 2X_1^4X_2^2 + 9X_1^4X_3^2 + 2X_1^3X_2^2X_3 + 8X_1^3X_3^3 - 3X_1^2X_2^4 + 6X_1^2X_2^2X_3^2 + 4X_1^2X_3^4 - 3X_1X_2^4X_3 + 8X_1X_2^2X_3^3 - 3X_2^4X_3^2 + 4X_2^2X_3^4$.
The curves $G_1=0, G_2=0 \subset \mathbb{P}^2(\mathbb{C})$ have the following common rational points: $(-2:0:1), (-1:-1:1), (0:0:1), (1:-1:1), (0:1:0)$, but $G \neq 0$ only for $(1:-1:1)$ and $(-1:-1:1)$. The first point, determines the class of the family $r = x^4+2x^3+6x^2-4x+4$, $t = 1/6x^2+2/3x+5/3$, $q = 1/36x^4+1/18x^3+1/3x^2+5/9x+7/9$, which is equivalent to the Barreto-Naehrig family. The second point determines the class of the family $r = x^4+2x^3+2x^2+4x+4$, $t = 1/2x^2+1$, $q = 1/12x^4+1/6x^3+2/3x^2+1/3x+1/3$, but $q(x) \notin \mathbb{Z}$ for any $x \in \mathbb{Q}$ (see Remark 2.4).

Remark 3.3. If K is the kth cyclotomic field of degree $n=\varphi(k)$, and $\zeta \in K$ is a kth primitive root of unity, then the points $x \in \mathbb{Q}^n$ such that $\operatorname{rank} M_1(x) \leq \frac{n}{2}+1$ and $\det M(x) \neq 0$ determine all primitive elements $z \in K$ satisfying $\deg_z \zeta \leq n/2$, or equivalently, polynomials $r(x), t(x) \in \mathbb{Q}[x]$ satisfying $\deg r(x) = n$, $r(x) \mid \Phi_k(t(x)-1)$ and $\deg t(x) \leq n/2$. Such polynomials have been first examined by Galbraith et al. [11], who represented them by rational points of some elliptic curves when $\varphi(k)=4$, i.e., $k=5,8,10,12$ (for example, for $k=12$ such a curve is given by the equation $G_1=0$ in the above example). (Note that original constructions of quartic families with $k=10,12$, and $\rho=1$ were based on this result.)

4. Constructing arbitrary families

In this section we describe two methods for constructing arbitrary families. The first extends the Brezing-Weng method and requires finding rational solutions of certain systems of polynomial equations. The second is based on the Dupont-Enge-Morain method [8] for constructing individual pairing-friendly curves, and yields families with prescribed left-hand side of the CM equation.

4.1. **Extension of the Brezing-Weng method.** We start with the following observation. If (r,t,q) is a family of elliptic curves with embedding degree k, then one can write $4q-t^2 = gh^2$ with $g,h \in \mathbb{Q}[x]$ and $\deg g \leq 2$. Reducing this modulo r and using the fact that r divides both $q+1-t$ and $\Phi_k(t-1)$ we get $\bar{g}\bar{h}^2 = 4\bar{q}-\bar{t}^2 = 4(\bar{t}-1)-\bar{t}^2 = -(\bar{t}-2)^2 = -(\zeta-1)^2$, where the bar denotes taking the residue class, and $\zeta \in K = \mathbb{Q}[x]/(r)$ is a kth primitive root of unity. Thus

$-\bar{g} = (\zeta-1)^2/\bar{h}^2$ is a square in K, and $\bar{h} = \pm(\zeta-1)/\sqrt{-g}$. This suggests that to construct another family we should find an element $g' \in K$ such that $-g'$ is a square in K, and which has the lift in $\mathbb{Q}[x]$ of degree ≤ 2. Then a new family will be formed from the lifts of g' and $h' = \pm(\zeta-1)/\sqrt{-g'}$. Elements g' with such properties are determined by rational solutions of some system of quadratic forms. In detail, the method is as follows.

Proposition 4.1. *Let $r \in \mathbb{Q}[x]$ be an irreducible polynomial of degree n such that the residue field $K = \mathbb{Q}[x]/(r)$ contains a kth primitive root of unity ζ. Let $g_1, \ldots, g_n \in \mathbb{Q}[X_1, \ldots, X_n]$ be quadratic forms such that $(\sum_{i=1}^n a_i \bar{x}^{i-1})^2 = \sum_{i=1}^n g_i(a)\bar{x}^{i-1}$ for all $a = (a_1, \ldots, a_n) \in \mathbb{Q}^n$. Assume that $a = (a_1, \ldots, a_n) \in \mathbb{Q}^n$ is a non-zero solution of the system $g_4 = \cdots = g_n = 0$. Put $\gamma = \sum_{i=1}^n a_i \bar{x}^{i-1}$, $g' = -\gamma^2$, and $h' = (\zeta-1)/\sqrt{-g'} = (\zeta-1)/\gamma$. Let $g, h, t \in \mathbb{Q}[x]$ be the lifts of degree less than n of g', h' and $\zeta+1$, respectively, and let $q = \frac{1}{4}(t^2 + gh^2)$. Then the triple (r, t, q) represents a potential family of elliptic curves with embedding degree k.*

The family produced via this method has $\rho \leq \max\{2\deg t, \deg g + 2\deg h\}/n$ (≤ 2), and the equality holds if $4q - t^2$ has positive leading coefficient. Furthermore, for $n \geq 4$ every potential family with $\rho < 2$ such that $4q - t^2$ has positive leading coefficient arises in this way. Notice that the trivial solution $\gamma = 1$ leads to the pathological family $(r, t, t-1)$. Furthermore, two non-zero solutions $a, a' \in \mathbb{Q}^n$ of the system $g_4 = \cdots = g_n = 0$ such that $a = \lambda a'$ for $\lambda \in \mathbb{Q}$ determine the same family. Thus one may consider solutions of this system in the projective space $\mathbb{P}^{n-1}(\mathbb{Q})$. However, one may expect that random solutions will usually give families with ρ-value close to 2. To improve this we can add some new equations, but unfortunately of higher degrees. Suppose that r and t are chosen so that $2\deg t/n \leq \rho_0$ for a given bound $1 \leq \rho_0 < 2$ (according to the previous section such r, t are characterized by conditions $\operatorname{rank} M_1 \leq B+1$, $\det M \neq 0$). Observe that one can compute homogeneous polynomials $h_0, h_1, \ldots, h_n \in \mathbb{Q}[X_1, \ldots, X_n]$ with $\deg h_0 = n$ and $\deg h_i = n-1$, $1 \leq i \leq n$, such that $(\sum_{i=1}^n a_i \bar{x}^{i-1})^{-1} = (\sum_{i=1}^n h_i(a)\bar{x}^{i-1})/h_0(a)$ for all $a = (a_1, \ldots, a_n) \in \mathbb{Q}^n \setminus \{0\}$ (this easily follows from Cramer's rule, since inversion in a fixed basis of $K/\mathbb{Q}$ can be done by solving a system of linear equations). Consequently, one can also compute homogeneous polynomials $h_0, h_1, \ldots, h_n \in \mathbb{Q}[X_1, \ldots, X_n]$ such that $(\zeta-1)(\sum_{i=1}^n a_i \bar{x}^{i-1})^{-1} = (\sum_{i=1}^n h_i(a)\bar{x}^{i-1})/h_0(a)$ for all $a = (a_1, \ldots, a_n) \in \mathbb{Q}^n \setminus \{0\}$. Then a solution $a \in \mathbb{P}^{n-1}(\mathbb{Q})$ of the system $g_4 = \cdots = g_n = 0$ determines the family with $\rho \leq \rho_0$ if $h_i(a) = 0$ for sufficiently large i. In detail, this is as follows.

Proposition 4.2. *Assume that $n \geq 4$. Let $r, \zeta, t, g_1, \ldots, g_n$ be as in Proposition 4.1, and suppose $2\deg t/n \leq \rho_0$ for $1 \leq \rho_0 < 2$. Let $h_0, h_1, , \ldots, h_n \in \mathbb{Q}[X_1, \ldots, X_n]$ be homogeneous polynomials with $\deg h_0 = n$, $\deg h_i = n-1$, $1 \leq i \leq n$, such that $(\zeta-1)(\sum_{i=1}^n a_i \bar{x}^{i-1})^{-1} = (\sum_{i=1}^n h_i(a)\bar{x}^{i-1})/h_0(a)$ for all $a = (a_1, \ldots, a_n) \in \mathbb{Q}^n \setminus \{0\}$. For $c = 0, 1, 2$, let d_c be the largest integer such that $(c+2d_c)/n \leq \rho_0$. Then all potential families (r, t, q) with $\rho \leq \rho_0$ such that $4q - t^2$ has positive leading coefficient are represented by points from the algebraic set*

$$\bigcup_{c=0,1,2} \{a \in \mathbb{P}^{n-1}(\mathbb{Q}) : g_{c+2} = \cdots = g_n = h_{d_c+2} = \cdots = h_n = 0\}.$$

However, assuming that for varying r, for example, the forms $g_4, \ldots, g_n, h_{n-2}, h_{n-1}, h_n$ behave like generic forms, we should not expect to obtain in general families with ρ-value smaller than $2(n-2)/n$. Therefore, to essentially improve ρ, one must carefully choose r, which will be discussed in the next section.

Remark 4.3. Observe that for $\rho_0 = 1$ one can avoid solving the above systems. Then q must be of the form $q = cr + t - 1$ for some nonzero $c \in \mathbb{Q}$, and $4q - t^2 = gh^2$ for $g, h \in \mathbb{Q}[x]$ with $\deg g \leq 2$. Thus, if $f(x,y) = 4(yr(x) + t(x) - 1) - t(x)^2 = f_n(y)x^n + \cdots + f_0(y)$, then either c is a root of $f_n(y)$, or $f_n(c) \neq 0$ and $f(x,c)$ is not square-free, and so c is a root of the discriminant of $f(x,y)$ with respect to x. For each such c we check by factorizing $f(x,c)$ whether it is suitable.

4.2. **Extension of the Dupont-Enge-Morain method.** Both methods for constructing individual pairing-friendly curves due to Cocks and Pinch [7] and Dupont, Enge and Morain [8] can be adapted for constructing families. The former is extended by the Brezing-Weng method. To extend the latter, let us first recall how it works.

If $r, t, q \in \mathbb{Z}$ are parameters of an elliptic curve with embedding degree k and discriminant D, then $r \mid \gcd(q + 1 - t, \Phi_k(t-1))$ and $4q - t^2 = Dy^2$, $y \in \mathbb{Z}$. Hence, $\bar{t} \in \mathbb{F}_r$ is a common root of the reduced (mod r) polynomials $\bar{N}(X, Dy^2), \bar{\Phi}_k(X-1) \in \mathbb{F}_r[X]$, where

$$N(X,Y) = (X-2)^2 + Y.$$

In particular, $r \mid R_k(Dy^2)$, where

$$R_k(Y) = \mathrm{Resultant}_X(N(X,Y), \Phi_k(X-1)).$$

To compute the desired parameters, the Dupont-Enge-Morain method follows these lines in the backward direction, which leads to the following algorithm:
- choose $y \in \mathbb{Z}$ and try to find the largest prime factor r of $R_k(Dy^2)$ (one can show that the polynomial $R_k(Y)$ represents primes (see [10, Lemma 4.5]), so one can test whether $R_k(Dy^2)$ is a prime number);
- find a common root $t' \in \mathbb{F}_r$ of $\bar{N}(x, Dy^2), \bar{\Phi}_k(X-1) \in \mathbb{F}_r[X]$;
- take the lift $t \in \{0, \ldots, r-1\}$ of that root, and check whether $q = \frac{1}{4}(t^2 + Dy^2)$ is a prime number.

Clearly, we can repeat these steps working with polynomials, which will allow us to find families with prescribed left-hand side of the CM equation $f(x) = Dy^2$. Notice that in this setting we will be able to find irreducible factors of $R_k(f(x))$, since factorization in $\mathbb{Q}[x]$ is efficient. More specifically, the method is as follows.

Proposition 4.4. *Let $g(x), h(x) \in \mathbb{Q}[x]$ and $\deg g(x) \leq 2$. Put $f(x) = g(x)h(x)^2$. Let $r(x) \in \mathbb{Q}[x]$ be an irreducible factor of $R_k(f(x))$, and let $K = \mathbb{Q}[x]/(r(x))$. Suppose that the polynomials $\bar{N}(X, f(x)), \bar{\Phi}_k(X-1) \in K[X]$ have a common root in K. Let $t(x) \in \mathbb{Q}[x]$ be the lift of degree $< \deg r(x)$ of that root, and let $q(x) = \frac{1}{4}(t(x)^2 + f(x))$. Then the triple $(r(x), t(x), q(x))$ represents a potential family with embedding degree k.*

Note that the above family has $\rho \le 2$ if either $R_k(f(x))$ is irreducible or $\deg f(x) \le 2\varphi(k)$, where $\varphi(k) = \deg \Phi_k(X)$. The former is obvious; the latter follows from the inequality $\deg r(x) \ge \varphi(k)$, which holds because K contains kth roots of unity.

5. Arbitrary families with $\rho \le \rho_0$

Here we extend the results from Section 3 on arbitrary families. Let K be a number field of degree $n = [K : \mathbb{Q}]$ containing kth roots of unity, and assume $n \ge 4$. We will consider the following families

(5.1) (r, t, q) is a potential family with embedding degree k such that $\mathbb{Q}[x]/(r) \cong K$.

It will be convenient to represent such families by the following triples from K.

(5.2) $(z, \zeta, \gamma) \in K^3$, z is a primitive element of K, ζ is a kth primitive root of unity, and $\gamma \ne 0$ with $\deg_z \gamma^2 \le 2$.

More precisely, such triples determine families satisfying the following additional condition.

(5.3) (r, t, q) satisfies (5.1), and one can write $4q - t^2 = gh^2$, where $g, h \in \mathbb{Q}[x]$, $\deg g \le 2$, and $\deg h < n$.

According to Proposition 4.1, such a triple (z, ζ, γ) determines the family (r, t, q), where r is the minimal polynomial of z, $q = \frac{1}{4}(t^2 + gh^2)$, and t, g, h are the lifts of degree less than n of $\varphi(\zeta + 1)$, $\varphi(-\gamma^2)$ and $\varphi((\zeta_k - 1)/\gamma)$, respectively, where $\varphi : K \to \mathbb{Q}[x]/(r)$ is the isomorphism $z \mapsto \bar{x}$.

An equivalence relation in the set of all triples (5.2), which corresponds to linear equivalence of families is defined as follows. We identify (z, ζ, γ) and (z', ζ', γ'), if $z' = a\varphi(z) + b$, $\zeta' = \varphi(\zeta)$, and $\gamma' = c\varphi(\gamma)$ for $\varphi \in \mathrm{Aut}(K)$ and $a, b, c \in \mathbb{Q}$ with $ac \ne 0$.

(5.4) *There is the induced surjection*

$$\Phi : \{\textit{triples (5.2)}\}/\!\sim \;\longrightarrow\; \{\textit{families (5.3)}\}/\!\sim,$$

which is 'almost bijective', i.e., if $\Phi^{-1}([(r, t, q)])$ has more than one element, then $q = \frac{1}{4}(t^2 + Dy^2)$ for some $D \in \mathbb{Z}$, and the cardinality of $\Phi^{-1}([(r, t, q)])$ is equal to the number of distinct linear factors of y in $\mathbb{Q}[x]$.

Proof. Similarly to (3.3) we check that Φ is well defined. To find triples representing a family (r, t, q), write $4q - t^2 = gh^2$ as in (5.3). Then this family is represented by all triples $(\varphi(z), \varphi(\zeta), c\varphi(\gamma))$, where $c \in \mathbb{Q}^*$, $\varphi \in \mathrm{Aut}(K)$, $z \in K$ is a root of r, and $\zeta = \psi(\bar{t} - 1)$, $\gamma = \psi(\sqrt{-\bar{g}})$, where $\psi : \mathbb{Q}[x]/(r) \to K$ is the isomorphism $\bar{x} \mapsto z$. Other triples representing this family must come from another factorization $4q - t^2 = g_1 h_1^2$ as in (5.2) such that $g/g_1 \notin \mathbb{Q}$. Such factorization may exist only if $4q - t^2 = Dy^2$ for $D \in \mathbb{Z}$ and $y \in \mathbb{Q}[x]$. Then g and g_1 must be squares of distinct linear factors of y in $\mathbb{Q}[x]$. Now the assertion easily follows. □

Define the parameter ρ for a triple (5.2) to be

$$\rho(z,\zeta,\gamma)=\frac{1}{n}\max\{2\deg_z\zeta,\deg_z\gamma^2+2\deg_z(\zeta-1)/\gamma\}.$$

Then a triple (z,ζ,γ) determines the family (r,t,q) with $\rho\le\rho(z,\zeta,\gamma)$, and the equality holds if $4q-t^2$ has positive leading coefficient.

Now for a fixed kth primitive root of unity $\zeta\in K$, a basis $b_1,\dots,b_n$ of $K/\mathbb{Q}$, and a bound $1\le\rho_0<2$, we derive conditions on coordinates in this basis of all elements $z,\gamma\in K$ such that the triple (z,ζ,γ) satisfies (5.2) and has $\rho(z,\zeta,\gamma)\le\rho_0$. To parameterize coordinates of such z and γ we use variables $X_1,\dots,X_n$ and $Y_1,\dots,Y_n$, respectively. Compute the following polynomials:
- homogeneous polynomials $f_{ij}\in\mathbb{Q}[X_1,\dots,X_n]$, $i=1,\dots,n, j=0,\dots,n-1$, with $\deg f_{ij}=j$ such that $(\sum_i x_ib_i)^j=\sum_i f_{ij}(x)b_i$ for all $x=(x_1,\dots,x_n)\in\mathbb{Q}^n$;
- quadratic forms $g_1,\dots,g_n\in\mathbb{Q}[Y_1,\dots,Y_n]$ such that $(\sum y_ib_i)^2=\sum g_i(y)b_i$ for all $y=(y_1,\dots,y_n)\in\mathbb{Q}^n$;
- homogeneous polynomials $h_0,h_1,\dots,h_n\in\mathbb{Q}[Y_1,\dots,Y_n]$ with $\deg h_i=n-1$, $1\le i\le n$, and $\deg h_0=n$, such that $(\zeta-1)(\sum y_ib_i)^{-1}=(\sum h_i(y)b_i)/h_0(y)$ for all $y=(y_1,\dots,y_n)\in\mathbb{Q}^n\setminus\{0\}$ (see the discussion preceding Proposition 4.2).

Let B be the largest integer such that $2B/n\le\rho_0$. For $c=0,1,2$, let d_c be the largest integer such that $(c+2d_c)/n\le\rho_0$. Then $\rho(z,\zeta,\gamma)\le\rho_0$ iff $\deg_z\zeta\le B$, $\deg_z\gamma^2\le c$, and $\deg_z(\zeta-1)/\gamma\le d_c$ for some $c=0,1,2$. We express these conditions in terms of the following matrices. Let $u_1,\dots,u_n\in\mathbb{Q}$ be the coordinates of ζ in our basis. For $c=0,1,2$, let

$$M_1=\begin{bmatrix}f_{10}&\cdots&f_{1B}&u_1\\ \vdots&\ddots&\vdots&\vdots\\ f_{n0}&\cdots&f_{nB}&u_n\end{bmatrix},\quad M_{2c}=\begin{bmatrix}f_{10}&f_{11}&f_{1c}&g_1\\ \vdots&\vdots&\vdots&\vdots\\ f_{n0}&f_{n1}&f_{nc}&g_n\end{bmatrix},\quad M_{3c}=\begin{bmatrix}f_{10}&\cdots&f_{1d_c}&h_1\\ \vdots&\ddots&\vdots&\vdots\\ f_{n0}&\cdots&f_{nd_c}&h_n\end{bmatrix},$$

and let $M=[f_{ij}]$ be the $n\times n$ matrix. For $x,y\in\mathbb{Q}^n$, denote by $M_{ic}(x,y)$ the matrix obtained from M_{ic} by evaluating its entries in the last column at y, and evaluating the remaining entries at x. We now find the following.

(5.5) *Let $x=(x_1,\dots,x_n),y=(y_1,\dots,y_n)\in\mathbb{Q}^n\setminus\{0\}$, and let $z=\sum x_ib_i$ and $\gamma=\sum y_ib_i$. Then the triple (z,ζ,γ) satisfies (5.2) and has $\rho(z,\zeta,\gamma)\le\rho_0$ iff* $\det M(x)\ne0$, $\operatorname{rank}M_1(x)\le B+1$, $\operatorname{rank}M_{2c}(x,y)\le c+1$, *and* $\operatorname{rank}M_{3c}\le d_c+1$ *for some $c=0,1,2$; or equivalently, if (x,y) is a solution of the system $F_{c1}=\cdots=F_{cm_c}=0$, $F\ne0$ for some $c=0,1,2$, where $F_{c1},\dots,F_{cm_c}$ are all the maximal minors of the matrices M_1,M_{2c},M_{3c}, and $F=\det M$.*

In order to describe families up to linear equivalence, suppose that $b_1=1$, and put $G_{ci}=F_{ci}(0,X_1,\dots,X_{n-1},Y_1,\dots,Y_n)$, and $G=F(0,X_1,\dots,X_{n-1})$. (Notice that these polynomials are homogeneous with respect to $X_1,\dots,X_n$ and $Y_1,\dots,Y_n$, so determine an algebraic set in $\mathbb{P}^{n-2}(\mathbb{C})\times\mathbb{P}^{n-1}(\mathbb{C})$.)

Theorem 5.1. *For $c=0,1,2$, let V_c be the set of all solutions in $\mathbb{P}^{n-2}(\mathbb{C})\times\mathbb{P}^{n-1}(\mathbb{C})$ of the system $G_{c1}=\cdots=G_{cm_c}=0$, $G\ne0$. Put $V=V_0\cup V_1\cup V_2$.*
(i) If $K/\mathbb{Q}$ is Galois, then all equivalence classes of families (5.1) with $\rho\le\rho_0$, such that $4q-t^2$

has positive leading coefficient are represented by rational points on V.
(ii) If V_c is non-empty, then $\dim V_c \geq B + c + d_c - n$. *In particular, if $\rho_0 = 1$ and $V_2 \neq \emptyset$, then $dim V \geq 1$.*

Proof. The proof is similar to that of Theorem 3.1. We only note that here V_c can be described by the following equations
$\sum_{j=1}^{n} u_{1j} M_{ji}(0, X_1, \ldots, X_{n-1}) = 0$ for $i = B+2, \ldots, n$,
$\sum_{j=1}^{n} M_{ji}(0, X_1, \ldots, X_{n-1}) g_j(Y_1, \ldots, Y_n) = 0$ for $i = c+2, \ldots, n$,
$\sum_{j=1}^{n} u_{1j} M_{ji}(0, X_1, \ldots, X_{n-1}) h_j(Y_1, \ldots, Y_n) = 0$ for $i = d_c+2, \ldots, n$.
Thus, if $V_c \neq \emptyset$, then $\dim V_c \geq 2n - 3 - (n - B - 1 + n - c - 1 + n - d_c - 1) = B + c + d_c - n$. □

Example 5.2. For an example of how the above methods work, we determine all quartic families (r, t, q) with $k = 10$, $\rho = 1$, and such that $4q - t^2$ is of degree 2. Freeman's family $r(x) = 25x^4 + 25x^3 + 25x^2 + 5x + 1$, $t(x) = 10x^2 + 5x + 3$, $q(x) = 25x^4 + 25x^3 + 25x^2 + 10x + 3$ is a well known example of this type, and in fact, a unique example, as we will see below.

Let K be the 10th cyclotomic field, and $\zeta \in K$ be a 10th primitive root of unity. For such families we can eliminate variables $Y_1, \ldots, Y_4$, since they are represented by triples (z, ζ, γ) such that $\deg_z \zeta \leq 2$, $\deg_z \gamma^2 \leq 2$, and $(\zeta - 1)/\gamma \in \mathbb{Q}$. The last two conditions yield $\deg_z (\zeta - 1)^2 \leq 2$. Thus we first compute all primitive elements $z \in K$ such that $\deg_z \zeta \leq 2$ and $\deg_z (\zeta - 1)^2 \leq 2$, and then determine the corresponding families according to Remark 4.3. Let M_1, M_2, and M be quadratic matrices whose the first three columns are formed from the coordinates of $1, z, z^2$ in the standard basis $1, \zeta, \zeta^2, \zeta^3$, and the last column is formed from the coordinates of ζ, $(\zeta - 1)^2$ and z^3, respectively. Their determinants evaluated at $(0, X_1, X_2, X_3)$ are the following:
$G_1 = -X_1^2 X_3 + 2X_1 X_2^2 + 2X_1 X_2 X_3 + 2X_1 X_3^2 + X_2^3 + X_2^2 X_3$,
$G_2 = -2X_1^2 X_2 - 5X_1 X_2^2 - 4X_1 X_2 X_3 - 2X_1 X_3^2 - 2X_2^3 - X2^2 X_3 - X_3^3$,
$G = X_1^6 + 3X_1^5 X_2 - 2X_1^5 X_3 + 5X_1^4 X_2^2 - 5X_1^4 X_2 X_3 + 5X_1^3 X_2^3 + 10X_1^3 X_2 X_3^2 + 5X_1^3 X_3^3 - 5X_1^2 X_2^3 X_3 - 5X_1^2 X_2 X_3^3 - 5X_1^2 X_3^4 - 2X_1 X_2^5 - 5X_1 X_2^4 X_3 - 5X_1 X_2^3 X_3^2 - 5X_1 X_2^2 X_3^3 + 3X_1 X_3^5 - X_2^6 - X_2^5 X_3 - X_2 X_3^5 - X_3^6$.
The curves $G_1 = 0, G_2 = 0 \subset \mathbb{P}^2(\mathbb{C})$ have the following common rational points: $(0 : -1 : 1), (-1/2 : 1 : 0), (1 : 0 : 0)$, but $G \neq 0$ only for the last two points. The point $(-1/2 : 1 : 0)$ determines the class of the family $r = x^4 + 3/2x^3 + 9/4x^2 + 7/8x + 11/16$, $t = 8/5x^2 + 6/5x + 13/5$, $q = 16/25x^4 + 24/25x^3 + 76/25x^2 + 44/25x + 51/25$, which is equivalent to Freeman's family. The last point does not determine any family with $\rho = 1$.

Note that for $k = 5$ there are no families of the above type. The corresponding equations for z are in fact the same as above (since $\zeta_5 = -\zeta_{10}$), but $4q - t^2$ has negative leading coefficient for the resulting family.

References

[1] R. Balasubramanian, N. Koblitz, The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *J. Cryptol.* **11**, 141-145 (1998)

[2] P.S.L.M. Barreto, B. Lynn, M. Scott, Constructing elliptic curves with prescribed embedding degrees, in *Security in Communication Networks–SCN 2002.* Lecture Notes in Computer Science, vol. 2576 (Springer, Berlin, 2002), pp. 263-273.
[3] P.S.L.M. Barreto, M. Naehrig, Pairing-friendly elliptic curves of prime order, in *Selected Areas in Cryptography –SAC 2005.* Lecture Notes in Computer Science, vol. 3897 (Springer, Berlin, 2006), pp. 319-331.
[4] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, in *Advances in Cryptology–Crytpo 2001.* Lecture Note in Computer Science, vol. 2139 (Springer, Berlin, 2001), pp. 213 229. Full version: *SIAM J. Comput.*, **32**, 586-615 (2003)
[5] D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, in *Advances in Cryptology–Asiacrypt 2001.* Lecture Notes in Computer Science, vol. 2248, (Springer, Berlin, 2002), pp. 514-532. Full version: *J. Cryptol.* **17**, 297-319 (2004)
[6] F. Brezing, A. Weng, Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptogr.* **37**, 133-141 (2005)
[7] C. Cocks, R.G.E. Pinch, Identity-based cryptosystems based on the Weil pairing. Unpublished manuscript, 2001
[8] R. Dupont, A. Enge, F. Morain, Building elliptic curves with arbitrary small MOV degree over finite prime fields. *J. Cryptol.* **18**, 79-89 (2005)
[9] D. Freeman, Constructing pairing-friendly elliptic curves with embedding degree 10, in *Algorithmic Number Theory Symposium–ANTS-VII.* Lecture Notes in Computer Science, vol. 4076 (Springer, Berlin, 2006), pp. 452-465
[10] D. Freeman, M. Scott, E. Teske, A taxonomy of pairing-friendly elliptic curves. *J. Cryptol.* **23**, 224-280 (2010)
[11] S. Galbraith, J. McKee, P. Valença, Ordinary abelian varieties having small embedding degree. *Finite Fields Appl.* **13**, 800-814 (2007)
[12] A. Joux, A one round protocol for tripartite Diffie-Hellman, in *Algorithmic Number Theory Symposium–ANTS-IV.* Lecture Notes in Computer Science, vol. 1838 (Springer, Berlin, 2000), pp. 385-393. Full version: *J. Cryptol.* **17**, 263-276 (2004)
[13] E. Kachisa, E. Schaefer, M. Scott, Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field, in *Pairing-Based Cryptography–Pairing 2008.* Lecture Notes in Computer Science, vol. 5209 (Springer, Berlin, 2008), pp. 126-135
[14] F. Luca, I. Shparlinski, Elliptic curves with low embedding degree. *J. Cryptol.* **19**, 553-562 (2006)
[15] D. Mumford, *Algebraic Geometry I Complex Projective Varieties* (Springer, Berlin, 1976)
[16] A. Menezes, T. Okamoto, S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inf. Theory* **39**,1639-1646 (1993)
[17] A. Miyaji, M. Nakabayashi, S. Takano, New explicit conditions of elliptic curves traces for FR-reduction. *IEICE Trans. Fundam.* **E84-A**, 1234-1243 (2001)
[18] M. Scott, P.S.L.M. Barreto, Generating more MNT elliptic curves. *Des. Codes Cryptogr.* **38**, 209-217 (2006)
[19] J. Silverman, *The Arithmetic of Elliptic Curves* (Springer, Berlin, 1986)

Institute of Mathematics, Polish Academy of Sciences, ul. Śniadeckich 8, 00-956 Warszawa, Poland
E-mail address: r.drylo@impan.gov.pl