Finite Fields and Their Applications 55 (2019) 268–283

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On isogeny graphs of supersingular elliptic curves over finite fields

Gora Adj [a], Omran Ahmadi [b,*], Alfred Menezes [a]

[a] *Department of Combinatorics & Optimization, University of Waterloo, Canada*
[b] *Institute for Research in Fundamental Sciences (IPM), Tehran, Iran*

A R T I C L E I N F O

Article history:
Received 4 February 2018
Received in revised form 17 October 2018
Accepted 20 October 2018
Available online 5 November 2018
Communicated by Neal Koblitz

MSC:
11G20
11G15
14G15
14H52
94A60

Keywords:
Supersingular elliptic curves over finite fields
Isogeny graphs

A B S T R A C T

We study the isogeny graphs of supersingular elliptic curves over finite fields, with an emphasis on the vertices corresponding to elliptic curves of j-invariant 0 and 1728.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of order q and characteristic $p > 3$, and let $\overline{\mathbb{F}}_q$ denote its algebraic closure. Let ℓ be a prime different from p. The isogeny graph $\mathcal{H}_\ell(\overline{\mathbb{F}}_q)$ is a di-

* Corresponding author.
E-mail addresses: gora.adj@gmail.com (G. Adj), oahmadid@ipm.ir (O. Ahmadi), ajmeneze@uwaterloo.ca (A. Menezes).

https://doi.org/10.1016/j.ffa.2018.10.002
1071-5797/

rected graph whose vertices are the $\overline{\mathbb{F}}_q$-isomorphism classes of elliptic curves defined over $\mathbb{F}_q$, and whose directed arcs represent degree-ℓ $\overline{\mathbb{F}}_q$-isogenies (up to a certain equivalence) between elliptic curves in the isomorphism classes. See [10] and [15] for summaries of the theory behind isogeny graphs and for applications in computational number theory.

Every supersingular elliptic curve defined over $\overline{\mathbb{F}}_p$ is isomorphic to one defined over $\mathbb{F}_{p^2}$. Pizer [12] showed that the subgraph $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$ of $\mathcal{H}_\ell(\overline{\mathbb{F}}_{p^2})$ induced by the vertices corresponding to isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$ is an expander graph (and consequently is connected). This property of $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$ was exploited by Charles, Goren and Lauter [2] who proposed a cryptographic hash function whose security is based on the intractability of computing directed paths of a certain length between two vertices in $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$. In 2011, Jao and De Feo [8] (see also [4]) presented a key agreement scheme whose security is also based on the intractability of this problem for small ℓ (typically $\ell = 2, 3$). There have also been proposals for related signature schemes [19,6] and an undeniable signature scheme [9].

In this paper, we study the supersingular isogeny graph $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ whose vertices are (representatives of) the $\mathbb{F}_{p^2}$-isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, and whose directed arcs represent degree-ℓ $\mathbb{F}_{p^2}$-isogenies between the elliptic curves. Observe that the difference between the definitions of $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ and $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$ is that the isomorphisms and isogenies in the former are defined over $\mathbb{F}_{p^2}$ itself. This difference necessitates a careful treatment of the vertices corresponding to supersingular elliptic curves having j-invariant equal to 0 and 1728. We note that the security of the aforementioned cryptographic schemes relies on the difficulty of constructing certain directed paths in $\mathcal{G}_\ell(\mathbb{F}_{p^2})$. On the other hand, [2] and [4] state that security is based on the hardness of constructing certain directed paths in $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$. Thus, it is worthwhile to study the differences between $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ and $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$. We also note that Delfs and Galbraith [3] studied supersingular isogeny graphs $\mathcal{G}_\ell(\mathbb{F}_p)$, where the vertices are $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_p$ and the arcs are equivalence classes of degree-ℓ $\mathbb{F}_p$-isogenies. They observed that the graphs $\mathcal{G}_\ell(\mathbb{F}_p)$ have similar 'volcano' structures as the ordinary subgraphs of $\mathcal{H}_\ell(\overline{\mathbb{F}}_p)$ [5].

The remainder of the paper is organized as follows. In §2 we provide a concise summary of the relevant background on elliptic curves and isogenies between them. Standard references for the material in §2 are the books by Silverman [14] and Washington [17]. The supersingular isogeny graph $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ is defined in §3. In §4, we completely describe the three small subgraphs of $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ whose vertices correspond to supersingular elliptic curves E over $\mathbb{F}_{p^2}$ with $t = p^2 + 1 - \#E(\mathbb{F}_{p^2}) \in \{0, -p, p\}$; see Fig. 1. In §5, we study the two large subgraphs of $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ whose vertices correspond to supersingular elliptic curves E over $\mathbb{F}_{p^2}$ with $t = p^2 + 1 - \#E(\mathbb{F}_{p^2}) \in \{-2p, 2p\}$, and make some observations about the number of loops at the vertices corresponding to elliptic curves with j-invariant equal to 0 or 1728. We make some concluding remarks in §6.

2. Elliptic curves

In the remainder of this paper, p will denote a prime greater than 3. Let $k = \mathbb{F}_q$ be the finite field of order q and characteristic p, and let $\overline{k} = \cup_{n\geq 1}\mathbb{F}_{q^n}$ denote its algebraic closure. Let $\sigma : \alpha \mapsto \alpha^q$ denote the q-power Frobenius map. An elliptic curve E over k is defined by a Weierstrass equation $E/k : Y^2 = X^3 + aX + b$ where $a, b \in k$ and $4a^3 + 27b^2 \neq 0$. The j-invariant of E is $j(E) = 1728 \cdot 4a^3/(4a^3 + 27b^2)$. One can easily check that $j(E) = 0$ if and only if $a = 0$, and $j(E) = 1728$ if and only if $b = 0$. For any extension K of k, the set of K-rational points on E is $E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\infty\}$, where ∞ is the point at infinity; we write $E = E(\overline{k})$. The chord-and-tangent addition law transforms $E(K)$ into an abelian group. For any $n \geq 2$ with $p \nmid n$, the group of n-torsion points on E is isomorphic to $\mathbb{Z}_n \oplus \mathbb{Z}_n$. In particular, if n is prime then E has exactly $n + 1$ distinct order-n subgroups.

2.1. Isomorphisms and automorphisms

Two elliptic curves $E/k : Y^2 = X^3 + aX + b$ and $E'/k : Y^2 = X^3 + a'X + b'$ are isomorphic over the extension field K/k if there exists $u \in K^*$ such that $a' = u^4a$ and $b' = u^6b$. If such a u exists, then the corresponding isomorphism $f : E \to E'$ is defined by $(x, y) \mapsto (u^2x, u^3y)$. If E and E' are isomorphic over K, then $j(E) = j(E')$. Conversely, if $j(E) = j(E')$, then E and E' are isomorphic over $\overline{k}$. Elliptic curves E_1/k, E_2/k that are isomorphic over $\mathbb{F}_{q^d}$ for some $d > 1$, but are not isomorphic over any smaller extension of $\mathbb{F}_q$, are said to be degree-d twists of each other. In particular, a degree-2 (quadratic) twist of $E_1/k : Y^2 = X^3 + aX + b$ is $E_2/k : Y^2 = X^3 + c^2aX + c^3b$ where $c \in k^*$ is a non-square, and $\#E_1(k) + \#E_2(k) = 2q + 2$. If $j \in \overline{k} \setminus \{0, 1728\}$, then

$$E_j : Y^2 = X^3 + \frac{3j}{1728 - j}X + \frac{2j}{1728 - j} \tag{1}$$

is an elliptic curve with $j(E_j) = j$. Also, $E : Y^2 = X^3 + 1$ has $j(E) = 0$ and $Y^2 = X^3 + X$ has $j(E) = 1728$.

An automorphism of E/k is an isomorphism from E to itself. The group of all automorphisms of E that are defined over K is denoted by $\mathrm{Aut}_K(E)$. If $j(E) \neq 0, 1728$, then $\mathrm{Aut}_{\overline{k}}(E)$ has order 2 with generator $(x, y) \mapsto (x, -y)$. If $j(E) = 1728$, then $\mathrm{Aut}_{\overline{k}}$ is cyclic of order 4 with generator $\psi : (x, y) \mapsto (-x, iy)$ where $i \in \overline{k}$ is a primitive fourth root of unity. If $j(E) = 0$, then $\mathrm{Aut}_{\overline{k}}$ is cyclic of order 6 with generator $\rho : (x, y) \mapsto (\eta x, -y)$ where $\eta \in \overline{k}$ is a primitive third root of unity.

2.2. Isogenies

Let E, E' be elliptic curves defined over $k = \mathbb{F}_q$. An isogeny $\phi : E \to E'$ is a non-constant rational map defined over $\overline{k}$ with $\phi(\infty) = \infty$. An endomorphism on E is an isogeny from E to itself; the zero map $P \mapsto \infty$ is also considered to be an endomorphism on E. If the field of definition of ϕ is the extension K of k, then ϕ is called a K-isogeny. If such an isogeny exists, then E and E' are said to be K-isogenous. Tate's theorem asserts that for finite K, E and E' are K-isogenous if and only if $\#E(K) = \#E'(K)$.

An isogeny ϕ is a morphism, is surjective, is a group homomorphism, and has finite kernel. Every K-isogeny ϕ can be represented as $\phi = (r_1(X), r_2(X) \cdot Y)$ where $r_1, r_2 \in K(X)$ (see p. 51 of [17]). Let $r_1(X) = p_1(X)/q_1(X)$, where $p_1, q_1 \in K[X]$ with $\gcd(p_1, q_1) = 1$. Then the degree of ϕ is $\max(\deg p_1, \deg q_1)$. Also, ϕ is said to be separable if $r_1'(X) \neq 0$; otherwise it is inseparable. In fact, ϕ is separable if and only if $\#\mathrm{Ker}\ \phi = \deg \phi$. Note that all isogenies of prime degree $\ell \neq p$ are separable.

For every $m \geq 1$, the multiplication-by-m map $[m] : E \to E$ is a k-isogeny of degree m^2. Every degree-m isogeny $\phi : E \to E'$ has a unique dual isogeny $\hat{\phi} : E' \to E$ satisfying $\hat{\phi} \circ \phi = [m]$ and $\phi \circ \hat{\phi} = [m]$. If ϕ is a K-isogeny, then so is $\hat{\phi}$. We have $\deg \hat{\phi} = \deg \phi$ and $\hat{\hat{\phi}} = \phi$. If E'' is an elliptic curve defined over k and $\psi : E' \to E''$ is an isogeny, then $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$.

2.3. Vélu's formula

Let E be an elliptic curve defined over $k = \mathbb{F}_q$. Let $\ell \neq p$ be a prime, and let G be an order-ℓ subgroup of E. Let $G^* = G \setminus \{\infty\}$. Then there exists an elliptic curve E' over $\overline{k}$ and a degree-ℓ isogeny $\phi : E \to E'$ with $\mathrm{Ker}\ \phi = G$. The elliptic curve E' and the isogeny ϕ are both defined over $K = \mathbb{F}_{q^t}$ where t is the smallest positive integer such that G is σ^t-invariant, i.e., $\{\sigma^t(P) : P \in G\} = G$ where σ is the q-power Frobenius map (so $\sigma(P) = (x^q, y^q)$ if $P = (x, y)$ and $\sigma(\infty) = \infty$). Furthermore, ϕ is unique in the following sense: if E'' is an elliptic curve defined over K and $\psi : E \to E''$ is a degree-ℓ K-isogeny with $\mathrm{Ker}\ \psi = G$, then there exists an isomorphism $f : E' \to E''$ defined over K such that $\psi = f \circ \phi$.

Given the Weierstrass equation $Y^2 = X^3 + aX + b$ for E/k and an order-ℓ subgroup G of E, Vélu's formula yields an elliptic curve E' defined over K and a degree-ℓ K-isogeny $\phi : E \to E'$ with $\mathrm{Ker}\ \phi = G$.

Suppose first that $\ell = 2$ and $G = \{\infty, (\alpha, 0)\}$. Then the Weierstrass equation for E' is

$$E' \ : \ Y^2 = X^3 - (4a + 15\alpha^2)X + (8b - 14\alpha^3), \tag{2}$$

and the isogeny ϕ is given by

$$\phi = \left(X + \frac{3\alpha^2 + a}{X - \alpha},\ Y - \frac{(3\alpha^2 + a)Y}{(X - \alpha)^2} \right). \tag{3}$$

Suppose now that ℓ is an odd prime. For $Q = (x_Q, y_Q) \in G^*$, define

$$t_Q = 3x_Q^2 + a, \quad u_Q = 2y_Q^2, \quad w_Q = u_Q + t_Q x_Q.$$

Furthermore, define

$$t = \sum_{Q \in G^*} t_Q, \quad w = \sum_{Q \in G^*} w_Q,$$

and

$$r(X) = X + \sum_{Q \in G^*} \left(\frac{t_Q}{X - x_Q} + \frac{u_Q}{(X - x_Q)^2} \right). \tag{4}$$

Then the Weierstrass equation for E' is

$$E' \;:\; Y^2 = X^3 + (a - 5t)X + (b - 7w), \tag{5}$$

and the isogeny ϕ is given by

$$\phi = (r(X), r'(X)Y). \tag{6}$$

We will henceforth denote the Vélu-generated elliptic curve E' by E^G.

2.4. Modular polynomials

Let ℓ be a prime. The modular polynomial $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$ is a symmetric polynomial of the form $\Phi_\ell(X, Y) = X^{\ell+1} + Y^{\ell+1} - X^\ell Y^\ell + \sum c_{ij} X^i Y^j$, where the sum is over pairs of integers (i, j) with $0 \le i, j \le \ell$ and $i + j < 2\ell$. Modular polynomials have the following remarkable property.

Theorem 1. *Suppose that the characteristic of $k = \mathbb{F}_q$ is different from ℓ. Let E/k be an elliptic curve with $j(E) = j$. Let $G_1, G_2, \ldots, G_{\ell+1}$ be the order-ℓ subgroups of E. Let $j_i = j(E^{G_i})$. Then the (possibly repeated) roots of $\Phi_\ell(j, Y)$ in $\overline{k}$ are precisely $j_1, j_2, \ldots, j_{\ell+1}$.*

2.5. Supersingular elliptic curves

Hasse's theorem states that if E is defined over $\mathbb{F}_q$, then $\#E(\mathbb{F}_q) = q + 1 - t$ where $|t| \le 2\sqrt{q}$. The integer t is called the trace of the q-power Frobenius map σ since the characteristic polynomial of σ acting on E is $Z^2 - tZ + q$. If $p \mid t$, then E is called supersingular; otherwise it is said to be ordinary. Every supersingular elliptic curve E over $\overline{\mathbb{F}}_q$ is isomorphic to one defined over $\mathbb{F}_{p^2}$; in particular, $j(E) \in \mathbb{F}_{p^2}$. Henceforth, we shall assume that $q = p^2$ (and $p > 3$).

Supersingularity of an elliptic curve depends only on its j-invariant. We say that $j \in \mathbb{F}_{p^2}$ is supersingular if there exists a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ with $j(E) = j$; if this is the case, then all elliptic curves with j-invariant equal to j are supersingular. Note that $j = 0$ is supersingular if and only if $p \equiv 2 \pmod 3$, and $j = 1728$ is supersingular if and only if $p \equiv 3 \pmod 4$.

Schoof [13, Theorem 4.6] determined the number of isomorphism classes of elliptic curves over a finite field. In particular, the number of isomorphism classes of supersingular elliptic curves E over $\mathbb{F}_{p^2}$ with $\#E(\mathbb{F}_{p^2}) = p^2 + 1 - t$ is

$$N(t) = \begin{cases} \left(p + 6 - 4\left(\frac{-3}{p}\right) - 3\left(\frac{-1}{p}\right)\right)/12, & \text{if } t = \pm 2p, \\ 1 - \left(\frac{-3}{p}\right), & \text{if } t = \pm p, \\ 1 - \left(\frac{-1}{p}\right), & \text{if } t = 0, \end{cases} \tag{7}$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. It follows that the total number of isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$ is $\lfloor p/6 \rfloor + \epsilon$, where $\epsilon = 0, 6, 3, 9$ if $p \equiv 1, 5, 7, 11 \pmod{12}$ respectively. Furthermore, if $t = 0$, $-p$ or p then $E(\mathbb{F}_{p^2})$ is cyclic [13, Lemma 4.8].

3. Supersingular isogeny graphs

Let $k = \mathbb{F}_q$ where $q = p^2$, and let $\ell \neq p$ be a prime. Recall that σ is the q-th power Frobenius map. The supersingular isogeny graph $\mathcal{G}_\ell(k)$ is a directed graph whose vertex set $V_\ell(k)$ consists of representatives (chosen below) of the k-isomorphism classes of supersingular elliptic curves defined over k. The (directed) arcs of $\mathcal{G}_\ell(k)$ are defined as follows. Let $E_1 \in V_\ell(k)$, and let G be a σ-invariant order-ℓ subgroup of E_1. Let $\phi : E_1 \to E_1^G$ be the Vélu isogeny with kernel G (recall that E_1^G and ϕ are both defined over k), and let E_2 be the representative of the k-isomorphism class of elliptic curves containing E_1^G. Then (E_1, E_2) is an arc; we call E_1 the tail and E_2 the head of the arc. Note that $\mathcal{G}_\ell(k)$ can have multiple arcs (more than one arc (E_1, E_2)) and loops (arcs of the form (E_1, E_1)).

Remark 1. The definition of arcs is independent of the choice of isogeny with kernel G. This is because, as noted in §2.3, if $\phi' : E_1 \to E_2'$ is any degree-ℓ isogeny with kernel G where both E_2' and ϕ' are defined over k, then E_2' and E_1^G are isomorphic over k and consequently ϕ and ϕ' yield the same arc (E_1, E_2).

Remark 2. The definition of $\mathcal{G}_\ell(k)$ is independent of the choice of representatives. Indeed, let $f : E_1' \to E_1$ be a k-isomorphism of elliptic curves, and suppose that E_1' was chosen as a representative instead of E_1. Let $\psi = \phi \circ f$. Then Ker $\psi = f^{-1}(G)$, and thus the σ-invariant order-ℓ subgroup $f^{-1}(G)$ of E_1' yields the arc (E_1', E_2). The claim now follows since f^{-1} yields a one-to-one correspondence between the σ-invariant order-ℓ subgroups of E_1 and E_1'.

A consequence of Tate's theorem is that the graph $\mathcal{G}_\ell(k)$ can be partitioned into subgraphs whose vertices are the k-isomorphism classes of supersingular elliptic curves E/k with trace $t = p^2 + 1 - \#E(k) \in \{0, -p, p, -2p, 2p\}$; we denote these subgraphs by

$\mathcal{G}_\ell(k,t)$. There are two such subgraphs ($t = \pm 2p$) when $p \equiv 1 \pmod{12}$, four subgraphs ($t = \pm p, \pm 2p$) when $p \equiv 5 \pmod{12}$, three subgraphs ($t = 0, \pm 2p$) when $p \equiv 7 \pmod{12}$, and five subgraphs ($t = 0, \pm p, \pm 2p$) when $p \equiv 11 \pmod{12}$. These subgraphs are further studied in §4 and §5. We first fix the representatives of the k-isomorphism classes of supersingular elliptic curves over k.

Suppose that $p \equiv 3 \pmod 4$, and let w be a generator of k^*. Munuera and Tena [11] showed that the representatives of the four isomorphism classes of elliptic curves E/k with $j(E) = 1728$ can be taken to be

$$E_{1728,w^i} : Y^2 = X^3 + w^i X \quad \text{for} \quad i \in [0,3]. \tag{8}$$

Of these curves, $E_{1728,w}$ and E_{1728,w^3} have p^2+1 $\mathbb{F}_{p^2}$-rational points, and so we choose them as the vertices of $\mathcal{G}_\ell(k,0)$. Furthermore, $\#E_{1728,1}(\mathbb{F}_{p^2}) = p^2+1+2p$ and $\#E_{1728,w^2}(\mathbb{F}_{p^2}) = p^2+1-2p$; hence, we select $E_{1728,1}$ and E_{1728,w^2} as the vertices of $\mathcal{G}_\ell(k,-2p)$ and $\mathcal{G}_\ell(k,2p)$, respectively.

Suppose that $p \equiv 2 \pmod 3$, and let w be a generator of k^*. Munuera and Tena [11] also showed that the representatives of the six isomorphism classes of elliptic curves E/k with $j(E) = 0$ can be taken to be

$$E_{0,w^i} : Y^2 = X^3 + w^i \quad \text{for} \quad i \in [0,5]. \tag{9}$$

Of these curves, $E_{0,w}$ and E_{0,w^5} have p^2+1+p $\mathbb{F}_{p^2}$-rational points, and so we choose them as the vertices of $\mathcal{G}_\ell(k,-p)$. Similarly, E_{0,w^2} and E_{0,w^4} have p^2+1-p $\mathbb{F}_{p^2}$-rational points, and so we choose them as the vertices of $\mathcal{G}_\ell(k,p)$. Finally, $\#E_{0,1}(\mathbb{F}_{p^2}) = p^2+1+2p$ and $\#E_{0,w^3}(\mathbb{F}_{p^2}) = p^2+1-2p$; hence, we select $E_{0,1}$ and E_{0,w^3} as the vertices of $\mathcal{G}_\ell(k,-2p)$ and $\mathcal{G}_\ell(k,2p)$, respectively.

If $j \neq 0, 1728$ is supersingular, then E_j (defined in (1)) and a quadratic twist $\tilde{E}_j$ are representatives of the two isomorphism classes of elliptic curves with j-invariant equal to j. Furthermore, $\#E_j(\mathbb{F}_{p^2}) \in \{p^2+1-2p, p^2+1+2p\}$ and $\#\tilde{E}_j(\mathbb{F}_{p^2}) = 2p^2 + 2 - \#E_j(\mathbb{F}_{p^2})$. We select E_j as a vertex in either $\mathcal{G}_\ell(k,-2p)$ or $\mathcal{G}_\ell(k,2p)$ depending on whether $\#E_j(\mathbb{F}_{p^2}) = p^2+1+2p$ or p^2+1-2p, and $\tilde{E}_j$ as a vertex in the other graph.

4. The subgraphs $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$ and $\mathcal{G}_\ell(\mathbb{F}_{p^2} \pm p)$

For a supersingular elliptic curve E defined over a finite field $\mathbb{F}_q$ of characteristic > 3, we denote by $\mathrm{End}(E)$ the ring of endomorphisms of E defined over $\mathbb{F}_q$ and by $K = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ the corresponding endomorphism algebra. We will use the following classical result of Waterhouse [18] (see also Theorem 2.1 in [3]) to describe the arcs in the subgraphs $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$ and $\mathcal{G}_\ell(\mathbb{F}_{p^2} \pm p)$ as depicted in Fig. 1.

Theorem 2. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_q = \mathbb{F}_{p^n}$ with $p > 3$, and let $t = q + 1 - \#E(\mathbb{F}_q)$. Then one of the following holds:*

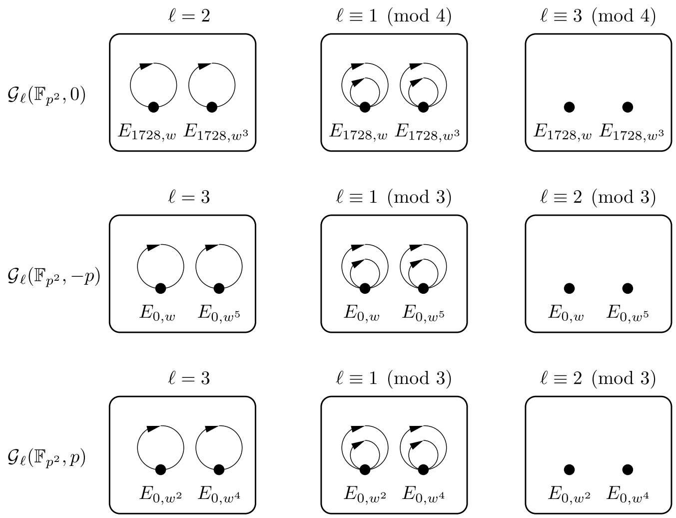

Fig. 1. The small subgraphs of $\mathcal{G}_\ell(\mathbb{F}_{p^2})$, $p \equiv 11 \pmod{12}$.

(i) *n is even and $t = \pm 2\sqrt{q}$;*
(ii) *n is even, $p \equiv 2 \pmod 3$ and $t = \pm\sqrt{q}$;*
(iii) *n is even, $p \equiv 3 \pmod 4$ and $t = 0$;*
(iv) *n is odd and $t = 0$.*

Let σ be the q-power Frobenius endomorphism of E. In case (i), K is a quaternion algebra over $\mathbb{Q}$, σ is a rational integer, and $\mathrm{End}(E)$ is a maximal order in K. In cases (ii), (iii) and (iv), $K = \mathbb{Q}(\sigma)$ is an imaginary quadratic number field and $\mathrm{End}(E)$ is an order in K with conductor coprime to p.

4.1. The subgraph $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$

Let $q = p^2$ where $p \equiv 3 \pmod 4$, w is a generator of $\mathbb{F}_q^*$, and $\ell \neq p$ is a prime. The graph $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$ has two vertices, $E_{1728,w}$ and E_{1728,w^3}; to ease the notation we will call them E_w and E_{w^3} in this section.

Theorem 3. *Let $p > 3$ and ℓ be primes with $p \equiv 3 \pmod 4$ and $\ell \neq p$.*

(i) *$\mathcal{G}_2(\mathbb{F}_{p^2}, 0)$ has exactly two arcs, one loop at each of its two vertices.*
(ii) *If $\ell \equiv 3 \pmod 4$, then $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$ has no arcs.*
(iii) *If $\ell \equiv 1 \pmod 4$, then $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$ has exactly four arcs, two loops at each of its two vertices.*

Proof. We describe the arcs originating at E_w. Notice that these arcs are exactly the degree-ℓ endomorphisms of E_w, i.e., the non-unit factors of ℓ in $\mathrm{End}(E_w)$. The case E_{w^3} case is similar.

Since $t = 0$, by Theorem 2, $\mathrm{End}(E_w)$ is an order in $K = \mathbb{Q}(\sigma)$ with conductor c coprime to p. The characteristic polynomial of the p^2-power Frobenius map σ is $Z^2 + p^2$, and so we have $K = \mathbb{Q}(\sqrt{-p^2}) = \mathbb{Q}(i)$ whose maximal order is $\mathbb{Z}[i]$, the Gaussian integers. Since σ and multiplication by integers are in $\mathrm{End}(E_w)$, we have

$$\mathbb{Z}[\sigma] = \mathbb{Z}[ip] \subseteq \mathrm{End}(E_w) \subseteq \mathbb{Z}[i].$$

Thus, the conductor c of $\mathrm{End}(E_w)$ divides the conductor p of $\mathbb{Z}[\sigma]$, whence $c = 1$ and $\mathrm{End}(E_w) = \mathbb{Z}[i]$. We have the following cases.

(i) If $\ell = 2$, then ℓ factors as $2 = i(i-1)^2$. Hence, since $\mathbb{Z}[i]$ is a unique factorization domain, there is a unique degree-ℓ endomorphism of E_w.
(ii) If $\ell \equiv 3 \pmod 4$, then ℓ is prime in $\mathbb{Z}[i]$. Thus, there are no degree-ℓ endomorphisms.
(iii) If $\ell \equiv 1 \pmod 4$, then ℓ splits as $\ell = \alpha\overline{\alpha}$ for some Gaussian prime α. Hence, there are exactly two degree-ℓ endomorphisms of E_w. □

4.2. The subgraphs $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm p)$

Let $q = p^2$ where $p \equiv 2 \pmod 3$, w is a generator of $\mathbb{F}_q^*$, and $\ell \neq p$ is a prime. The graph $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -p)$ has two vertices, $E_{0,w}$ and E_{0,w^5}; to ease the notation we will call them E_w and E_{w^5} in this section.

Theorem 4. *Let $p > 3$ and ℓ be primes with $p \equiv 2 \pmod 3$ and $\ell \neq p$.*

(i) *$\mathcal{G}_3(\mathbb{F}_{p^2}, -p)$ has exactly two arcs, one loop at each of its two vertices.*
(ii) *If $\ell \equiv 2 \pmod 3$, then $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -p)$ has no arcs.*
(iii) *If $\ell \equiv 1 \pmod 3$, then $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -p)$ has exactly four arcs, two loops at each of its two vertices.*

Proof. We describe the arcs originating at E_w. Notice that these arcs are exactly the degree-ℓ endomorphisms of E_w, i.e., the non-unit factors of ℓ in $\mathrm{End}(E_w)$. The E_{w^5} case is similar.

Since $t = -p$, by Theorem 2, $\mathrm{End}(E_w)$ is an order in $K = \mathbb{Q}(\sigma)$ with conductor c coprime to p. The characteristic polynomial of the p^2-power Frobenius map σ is $Z^2 + pZ + p^2$, and thus we have $K = \mathbb{Q}(\sqrt{-3})$. Hence, the maximal order of K is Eisentein integers $\mathbb{Z}[\lambda]$ where $\lambda = (-1 + \sqrt{3})/2$. Since σ and multiplication by integers are in $\mathrm{End}(E_w)$, we have

$$\mathbb{Z}[\sigma] = \mathbb{Z}[\lambda p] \subseteq \mathrm{End}(E_w) \subseteq \mathbb{Z}[\lambda].$$

Thus, the conductor c of $\mathrm{End}(E_w)$ divides the conductor p of $\mathbb{Z}[\sigma]$, whence $c = 1$ and $\mathrm{End}(E_w) = \mathbb{Z}[\lambda]$. We have the following cases.

(i) If $\ell = 3$, then ℓ factors as $3 = -\lambda^2(1-\lambda)^2$. Hence, since $\mathbb{Z}[\lambda]$ is a unique factorization domain, there is a unique degree-ℓ endomorphism of E_w.
(ii) If $\ell \equiv 2 \pmod 3$, then ℓ is prime in $\mathbb{Z}[\lambda]$. Thus there are no degree-ℓ endomorphisms.
(iii) If $\ell \equiv 1 \pmod 3$, then ℓ splits as $\ell = \alpha\overline{\alpha}$ for some Eisentein prime α. Hence, there are exactly two degree-ℓ endomorphisms of E_w. $\square$

The proof of Theorem 5 is similar to that of Theorem 4.

Theorem 5. *Let $p > 3$ and ℓ be primes with $p \equiv 2 \pmod 3$ and $\ell \neq p$.*

(i) *$\mathcal{G}_3(\mathbb{F}_{p^2}, p)$ has exactly two arcs, one loop at each of its two vertices.*
(ii) *If $\ell \equiv 2 \pmod 3$, then $\mathcal{G}_\ell(\mathbb{F}_{p^2}, p)$ has no arcs.*
(iii) *If $\ell \equiv 1 \pmod 3$, then $\mathcal{G}_\ell(\mathbb{F}_{p^2}, p)$ has exactly four arcs, two loops at each of its two vertices.*

5. The subgraphs $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p)$

As noted in §3, the vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ have distinct j-invariants. Moreover, there is a one-to-one correspondence between the vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ and the vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 2p)$; namely, if E is a vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ then the chosen quadratic twist $\tilde{E}$ is a vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 2p)$. Now, the characteristic polynomial of the q-power Frobenius map σ acting on any vertex E in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ is $Z^2+2pZ+p^2 = (Z+p)^2$, so $(\sigma+[p])^2 = 0$. Since nonzero endomorphisms are surjective, we must have $\sigma + [p] = 0$. Hence $\sigma = [-p]$ and all order-ℓ subgroups of E are σ-invariant. It follows that every vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ has outdegree $\ell + 1$. Similarly, every vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 2p)$ has outdegree $\ell + 1$.

By Theorem 1, the j-invariants of the heads of arcs with tail E in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ are precisely the roots of $\Phi_\ell(j(E), Y)$ (all $\ell + 1$ of which lie in $\mathbb{F}_{p^2}$). These roots are also the j-invariants of the heads of arcs with tail $\tilde{E}$ in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 2p)$. Hence the directed graphs $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ and $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 2p)$ are isomorphic.

Sutherland [15] defines the isogeny graph $\mathcal{H}_\ell(\overline{\mathbb{F}}_{p^2})$ to have vertex set $\overline{\mathbb{F}}_{p^2}$ and arcs (j_1, j_2) present with multiplicity equal to the multiplicity of j_2 as a root of $\Phi_\ell(j_1, Y)$ in $\overline{\mathbb{F}}_{p^2}$. The following folklore result shows that $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$, the supersingular component of $\mathcal{H}_\ell(\overline{\mathbb{F}}_{p^2})$, is isomorphic to $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$.

Theorem 6. *$\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ and $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$ are isomorphic.*

Proof. Recall that every supersingular elliptic curves over $\overline{\mathbb{F}}_{p^2}$ is isomorphic to one defined over $\mathbb{F}_{p^2}$. Hence the map $\beta : E \mapsto j(E)$ is a bijection between the vertex sets of $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ and $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$. Now, let (E_1, E_2) be an arc of multiplicity $c \geq 0$ in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$. By Theorem 1, $j(E_2)$ is a root of multiplicity c of $\Phi_\ell(j(E_1), Y)$. Hence $(j(E_1), j(E_2))$ is an arc of multiplicity c in $\mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$. Thus, β preserves arcs and $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p) \cong \mathcal{G}_\ell(\overline{\mathbb{F}}_{p^2})$. $\square$

5.1. Indegree

Suppose that p is prime and let E be a vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$. Then all automorphisms of E are defined over $\mathbb{F}_{p^2}$; we denote the group of all automorphisms of E by $\mathrm{Aut}(E)$. Recall from §2.1 that $\#\mathrm{Aut}(E) = 4, 6$ or 2 depending on whether $j(E) = 1728$, $j(E) = 0$ or $j(E) \neq 0, 1728$.

Let $\ell \neq p$ be a prime. Let E_1, E_2 be two vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$, and let $\phi_1, \phi_2 : E_1 \to E_2$ be two degree-ℓ $\mathbb{F}_{p^2}$-isogenies. We say that ϕ_1 and ϕ_2 are *equivalent* if they have the same kernel, or, equivalently, if there exists $\rho_2 \in \mathrm{Aut}(E_2)$ such that $\phi_2 = \rho_2 \circ \phi_1$. Thus, the arcs (E_1, E_2) in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ can be seen as the classes of equivalent degree-ℓ $\mathbb{F}_{p^2}$-isogenies from E_1 to E_2. We define ϕ_1 and ϕ_2 to be *automorphic* if there exists $\rho_1 \in \mathrm{Aut}(E_1)$ such that ϕ_2 and $\phi_1 \circ \rho_1$ are equivalent. Hence, if ϕ_1 and ϕ_2 are automorphic then there exist $\rho_1 \in \mathrm{Aut}(E_1)$ and $\rho_2 \in \mathrm{Aut}(E_2)$ such that $\phi_2 = \rho_2 \circ \phi_1 \circ \rho_1$. Since $\hat{\phi}_2 = \rho_1^{-1} \circ \hat{\phi}_1 \circ \rho_2^{-1}$, it follows that the duals of automorphic isogenies are automorphic.

Theorem 7. *Let E be a vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ and let $n = \#\mathrm{Aut}(E)/2$. Let a and b denote the number of arcs (E, E_{1728}) and arcs (E, E_0) in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$, respectively. Then the indegree of E is $(\ell + a + 2b + 1)/n$.*

Proof. Let E_1, E_2 be two vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$, and let $\mathrm{Aut}(E_i) = \langle \rho_i \rangle$ and $n_i = \#\mathrm{Aut}(E_i)/2$ for $i = 1, 2$. Let $\phi : E_1 \to E_2$ be a degree-ℓ $\mathbb{F}_{p^2}$-isogeny.

Suppose first that the kernel of ϕ is not an eigenspace of ρ_1. Consider the set

$$\mathcal{A} = \{\rho_2^j \circ \phi \circ \rho_1^i \ : \ 0 \leq i < 2n_1,\ 0 \leq j < 2n_2\}$$

of isogenies automorphic to ϕ. Since $\rho_i^{n_i} = -1$ for $i \in \{1, 2\}$, we have

$$\mathcal{A} = \{\rho_2^j \circ \phi \circ \rho_1^i \ : \ 0 \leq i < n_1,\ 0 \leq j < 2n_2\}.$$

One can check that if $(i, j) \neq (i', j')$ where $0 \leq i, i' < n_1$ and $0 \leq j, j' < 2n_2$, then $\rho_2^j \circ \phi \circ \rho_1^i = \rho_2^{j'} \circ \phi \circ \rho_1^{i'}$ implies that the kernel of ϕ is an eigenspace of ρ_1. Hence the set $\mathcal{A}$ has size exactly $2n_1n_2$ and the isogenies in $\mathcal{A}$ can be partitioned into n_1 classes of equivalent isogenies, each class comprised of $2n_2$ isogenies. Similarly, the set

$$\hat{\mathcal{A}} = \{\rho_1^i \circ \hat{\phi} \circ \rho_2^j \ : \ 0 \leq i < 2n_1,\ 0 \leq j < 2n_2\}$$

of dual isogenies can be partitioned into n_2 classes of equivalent isogenies, each class comprised of $2n_1$ isogenies. Consequently, ϕ generates n_1 different arcs (E_1, E_2) and $\hat{\phi}$ generates n_2 different arcs (E_2, E_1). Because duals of automorphic isogenies are automorphic, if there is another degree-ℓ $\mathbb{F}_{p^2}$-isogeny ψ from E_1 to E_2 not automorphic to ϕ, then ψ (resp. $\hat{\psi}$) generates a set of n_1 (resp. n_2) arcs (E_1, E_2) (resp. (E_2, E_1)) disjoint from those generated by ϕ (resp. $\hat{\phi}$). Therefore, the number r_{out} of arcs (E_1, E_2) generated by isogenies whose kernels are not eigenspaces of ρ_1 and the number r_{in} of arcs

(E_2, E_1) generated by their duals are multiples of n_1 and n_2, respectively. Moreover, we have

$$r_{\text{in}} = \frac{n_2 \cdot r_{\text{out}}}{n_1}. \tag{10}$$

Suppose now that the kernel of ϕ is an eigenspace of ρ_1. This scenario occurs only if E_1 has j-invariant 1728 or 0. Suppose E_1 has j-invariant 1728, and let ρ_1 be the automorphism $(x, y) \mapsto (-x, iy)$ where $i \in \mathbb{F}_{p^2}$ satisfies $i^2 = -1$. Denote by G the kernel of ϕ, and let $\phi' : E_1 \to E_1^G$ denote the Vélu isogeny. By (5), E_1^G has equation $Y^2 = X^3 + aX - 7w$ for some $a \in \mathbb{F}_{p^2}$ and $w = \sum_{Q \in G^*}(5x_Q^3 + 3x_Q)$. Since $\rho_1(G) = G$, if $(x, y) \in G$ then $(-x, iy) \in G$. Hence $w = 0$ and we conclude that E_1^G is isomorphic to E_1 over $\mathbb{F}_{p^2}$, i.e., $E_2 = E_1$. A similar argument using the automorphism $(x, y) \mapsto (\eta x, -y)$ with $\eta \in \mathbb{F}_{p^2}$ satisfying $\eta^2 + \eta + 1 = 0$ shows that we also have $E_2 = E_1$ when the j-invariant of E_1 is 0. Thus, if the kernel of ϕ is an eigenspace of ρ_1, the arcs generated by ϕ are loops at E_1. Therefore, we can generalize (10) to the total number t_{out} of arcs (E_1, E_2) and the total number t_{in} of arcs (E_2, E_1) and obtain

$$t_{\text{in}} = \frac{n_2 \cdot t_{\text{out}}}{n_1}. \tag{11}$$

Now, let E be a vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ and $n = \#\text{Aut}(E)/2$. Denote by E_j the vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ having j-invariant $j \in \mathbb{F}_{p^2}$. Let a be the number of arcs (E, E_{1728}) and b the number of arcs (E, E_0). Note that the number of arcs (E, E_j), $j \notin \{0, 1728\}$, is $c = \ell - a - b + 1$. From (11) we have

$$\text{indegree}(E) = \frac{c}{n} + \frac{2a}{n} + \frac{3b}{n},$$

whence

$$\text{indegree}(E) = \frac{\ell + a + 2b + 1}{n}. \quad \square$$

5.2. Loops

Let E_{1728} and E_0 denote the vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ with j-invariants 1728 and 0. In §5.2.1 and §5.2.2 we investigate the number of loops at E_{1728} and E_0 in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$. In particular, we determine upper bounds on p for which E_0 and E_{1728} have unexpected loops, i.e., loops not arising from eigenspaces of the primitive automorphisms of E_0 and E_{1728}.

5.2.1. E_{1728} loops

We begin by noting that

$$\Phi_2(X, 1728) = (X - 1728)(X - 287496)^2.$$

Since $287496-1728 = 2^3 \cdot 3^6 \cdot 7^2$, we see that 1728 is a triple root of $\Phi_2(X, 1728)$ in $\mathbb{Z}_p[X]$ if $p = 7$ and a single root if $p > 7$. Hence the number of loops at E_{1728} in $\mathcal{G}_2(\mathbb{F}_{p^2}, -2p)$ is three if $p = 7$ and one if $p > 7$ (and $p \equiv 3 \pmod 4$).

Lemma 8. *Let $p \equiv 3 \pmod 4$ be a prime, and let $\ell \neq p$ be an odd prime. Then the number of loops at E_{1728} is even. Moreover, if $\ell \equiv 1 \pmod 4$ then there are at least two loops at E_{1728}.*

Proof. Let ρ denote the automorphism $(x, y) \mapsto (-x, iy)$ of E_{1728} where $i \in \mathbb{F}_{p^2}$ satisfies $i^2 = -1$. Since $\#\mathrm{Aut}(E_{1728})/2 = 2$ we have from the first part of the proof of Theorem 7 that the number of loops at E_{1728} generated by isogenies whose kernels are not eigenspaces of ρ is even.

The characteristic polynomial Z^2+1 of ρ splits modulo ℓ if and only if $\ell \equiv 1 \pmod 4$. Hence, if $\ell \equiv 3 \pmod 4$ then all the loops at E_{1728} are generated by isogenies whose kernels are not eigenspaces of ρ and thus the number of loops is even. Now suppose that $\ell \equiv 1 \pmod 4$. The eigenspaces of ρ modulo ℓ are two different order-ℓ subgroups of E_{1728}. The second part of the proof of Theorem 7 shows that the arcs generated by these subgroups are loops at E_{1728}. $\square$

Let p be a prime and let $B_{p,\infty}$ denote the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞ with trace Tr and norm N. From [7, Lemma 2.1.1], we have the following result.

Lemma 9. *Let R be a maximal order of $B_{p,\infty}$, and let K_1, K_2 be distinct imaginary quadratic subfields of $B_{p,\infty}$. Furthermore, suppose that there exist $k_i \in R$, $i = 1, 2$, such that $\{1, k_i\}$ is a $\mathbb{Q}$-basis for K_i. Then $p \leq 4N(k_1)N(k_2)$.*

Theorem 10. *Let ℓ be a fixed prime, and let $p \equiv 3 \pmod 4$ be a prime distinct from ℓ. Suppose that E_{1728} has at least one loop in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ when $\ell \equiv 3 \pmod 4$, and at least three loops when $\ell \equiv 1 \pmod 4$. Then $p < 4\ell$.*

Proof. Let $\mathrm{End}(E_{1728})$ be the endomorphism ring of E_{1728}. It is known that $\mathrm{End}(E_{1728})$ is a maximal order in $B_{p,\infty}$ [18]. Since $\mathrm{End}(E_{1728})$ contains the order-4 automorphism $\rho : (x, y) \mapsto (-x, iy)$, where $i \in \mathbb{F}_{p^2}$ satisfies $i^2 = -1$, we have $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{-1}) \subset \mathrm{End}(E_{1728})$. Suppose that E_{1728} has a loop in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$, whence there exists $\alpha \in \mathrm{End}(E_{1728})$ such that $\mathrm{N}(\alpha) = \ell$. If $\ell \equiv 3 \pmod 4$, then $\alpha \notin \mathbb{Q}(\rho)$ since ℓ is prime in $\mathbb{Z}[\rho]$. On the other hand, if $\ell \equiv 1 \pmod 4$, then ℓ splits uniquely in $\mathbb{Z}[\rho]$ up to multiplication by units as $\ell = \delta\bar{\delta}$. If E_{1728} has at least three loops in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$, then we can further assume that $\alpha \neq u\delta$ for all units $u \in \mathbb{Z}[\rho]$ and again we conclude that $\alpha \notin \mathbb{Q}(\rho)$.

Every element $b \in B_{p,\infty}$ satisfies $b^2 - \mathrm{Tr}(b)b + \mathrm{N}(b) = 0$. Now, let $\gamma = 2\alpha - \mathrm{Tr}(\alpha)$. Since $\mathrm{Tr}(\gamma) = 0$, we have $\gamma^2 = -\mathrm{N}(\gamma) < 0$. Hence $\mathbb{Q}(\alpha) = \mathbb{Q}(\gamma)$ is an imaginary quadratic field different from $\mathbb{Q}(\rho)$. Considering the bases $\{1, \rho\}$, $\{1, \alpha\}$ for $\mathbb{Q}(\rho)$, $\mathbb{Q}(\alpha)$, respectively, Lemma 9 yields $p \leq 4\ell$, and as p is a prime number, we conclude that $p < 4l$. $\square$

5.2.2. E_0 loops

We have

$$\Phi_2(X,0) = (X - 2^4 \cdot 3^3 \cdot 5^3)^3,$$

whence 0 is a triple root of $\Phi_2(X,0)$ in $\mathbb{Z}_p[X]$ if $p = 5$ and not a root if $p > 5$. Hence the number of loops at E_0 in $\mathcal{G}_2(\mathbb{F}_{p^2}, -2p)$ is three if $p = 5$ and zero if $p > 5$ (and $p \equiv 2 \pmod 3$). Similarly, since

$$\Phi_3(X,0) = X(X - 2^{15} \cdot 3 \cdot 5^3)^3,$$

we conclude that the number of loops at E_0 in $\mathcal{G}_3(\mathbb{F}_{p^2}, -2p)$ is four if $p = 5$ and one if $p > 5$ (and $p \equiv 2 \pmod 3$).

Lemma 11. *Let $p \equiv 2 \pmod 3$ be a prime, and let $\ell \neq 3, p$ be an odd prime. If $\ell \equiv 2 \pmod 3$, then the number of loops at E_0 is $\equiv 0 \pmod 3$. If $\ell \equiv 1 \pmod 3$, then the number of loops at E_0 is $\equiv 2 \pmod 3$.*

Proof. Similar to the proof of Lemma 8. □

Theorem 12. *Let ℓ be a fixed prime. Let $p \equiv 2 \pmod 3$, $p \neq \ell$, be a prime for which E_0 has at least one loop in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ if $\ell \equiv 2 \pmod 3$ or at least three loops if $\ell \equiv 1 \pmod 3$. Then $p < 4\ell$.*

Proof. Similar to the proof of Theorem 10. □

For primes $\ell \equiv 1 \pmod 4$ (resp. $\ell \equiv 3 \pmod 4$), let $p^1_{1728}(\ell)$ (resp. $p^3_{1728}(\ell)$) denote the largest prime $p \equiv 3 \pmod 4$, $p \neq \ell$, for which E_{1728} has at least three loops (resp. at least one loop) in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$. Similarly, for odd primes $\ell \equiv 1 \pmod 3$ (resp. $\ell \equiv 2 \pmod 3$), let $p^1_0(\ell)$ (resp. $p^2_0(\ell)$) denote the largest prime $p \equiv 2 \pmod 3$, $p \neq \ell$, for which E_0 has at least three loops (resp. at least one loop) in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$. Table 1 lists $p^1_{1728}(\ell)$, $p^3_{1728}(\ell)$, $p^1_0(\ell)$, $p^2_0(\ell)$ for all primes $\ell \leq 283$. These values were obtained by factoring the relevant values of the modular polynomial Φ_ℓ; the modular polynomials were obtained from Sutherland's database [1,16]. For example, $p^3_{1728}(\ell)$ is the largest prime factor of $\Phi_\ell(1728, 1728)$ that is congruent to 3 modulo 4. Table 1 indicates that the bounds $p^1_{1728}(\ell) < 4\ell$ and $p^3_{1728}(\ell) < 4\ell$ are tight, and suggests a tighter upper bound of 3ℓ for $p^1_0(\ell)$ and $p^2_0(\ell)$.

6. Concluding remarks

We defined the supersingular isogeny graph $\mathcal{G}_\ell(\mathbb{F}_{p^2})$, and described the arcs of its small subgraphs $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$ and $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm p)$. We also investigated the existence of loops at vertices E_0 and E_{1728} in the large subgraph $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$, and determined upper bounds on primes p for which E_0 and E_{1728} have unexpected loops in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$.

Table 1
The values $p^1_{1728}(\ell)$, $p^3_{1728}(\ell)$, $p^1_0(\ell)$, $p^2_0(\ell)$ for all odd primes $\ell \leq 283$.

ℓ	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
$p^1_{1728}(\ell)$	–	19	–	–	47	67	–	–	107	–	139	163	–	–	211
$p^3_{1728}(\ell)$	11	–	23	–	–	–	71	83	–	107	–	–	167	179	–
$p^1_0(\ell)$	–	–	17	–	23	–	53	–	–	89	107	–	113	–	–
$p^2_0(\ell)$	–	11	–	–	–	47	–	53	83	–	–	107	–	137	131

ℓ	59	61	67	71	73	79	83	89	97	101	103	107	109	113	127
$p^1_{1728}(\ell)$	–	239	–	–	283	–	–	347	383	379	–	–	431	443	–
$p^3_{1728}(\ell)$	227	–	263	239	–	311	331	–	–	–	383	419	–	–	503
$p^1_0(\ell)$	–	179	197	–	191	233	–	–	263	–	293	–	311	–	353
$p^2_0(\ell)$	173	–	–	197	–	–	233	263	–	251	–	317	–	311	–

ℓ	131	137	139	149	151	157	163	167	173	179	181	191	193	197	199
$p^1_{1728}(\ell)$	–	547	–	587	–	619	–	–	691	–	719	–	743	787	–
$p^3_{1728}(\ell)$	523	–	547	–	599	–	647	659	–	691	–	751	–	–	787
$p^1_0(\ell)$	–	–	401	–	449	467	461	–	–	–	491	–	563	–	593
$p^2_0(\ell)$	389	383	–	443	–	–	–	449	503	521	–	569	–	587	–

ℓ	211	223	227	229	233	239	241	251	257	263	269	271	277	281	283
$p^1_{1728}(\ell)$	–	–	–	911	919	–	947	–	1019	–	1063	–	1103	1123	–
$p^3_{1728}(\ell)$	839	887	907	–	–	947	–	991	–	1051	–	1039	–	–	1123
$p^1_0(\ell)$	617	653	–	683	–	–	719	–	–	–	–	809	827	–	821
$p^2_0(\ell)$	–	–	677	–	683	701	–	701	743	773	743	–	–	839	–

Acknowledgments

We are grateful the anonymous referees for their comments, one of which led to simplified proofs of Theorems 3 and 4, and another which yielded tighter bounds in Theorems 10 and 12.

References

[1] R. Bröker, K. Lauter, A. Sutherland, Modular polynomials via isogeny volcanoes, Math. Comput. 278 (2012) 1201–1231.
[2] D. Charles, E. Goren, K. Lauter, Cryptographic hash functions from expander graphs, J. Cryptol. 22 (2009) 93–113.
[3] C. Delfs, S. Galbraith, Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$, Des. Codes Cryptogr. 78 (2016) 425–440.
[4] L. De Feo, D. Jao, J. Plût, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, J. Math. Cryptol. 8 (2014) 209–247.
[5] M. Fouquet, F. Morain, Isogeny volcanoes and the SEA algorithm, in: Algorithmic Number Theory, ANTS 2002, in: LNCS, vol. 2369, 2002, pp. 276–291.
[6] S. Galbraith, C. Petit, J. Silva, Identification protocols and signature schemes based on supersingular isogeny problems, in: Advances in Cryptology, ASIACRYPT 2017, in: LNCS, vol. 10624, 2017, pp. 3–33.
[7] E. Goren, C. Lauter, Class invariants for quartic CM fields, Ann. Inst. Fourier 57 (2007) 457–480.
[8] D. Jao, L. De Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, in: Post-Quantum Cryptography, PQCrypto 2011, in: LNCS, vol. 7071, 2011, pp. 19–34.
[9] D. Jao, V. Soukharev, Isogeny-based quantum-resistant undeniable signatures, in: Post-Quantum Cryptography, PQCrypto 2014, in: LNCS, vol. 8772, 2014, pp. 160–179.
[10] D. Kohel, Endomorphism Rings of Elliptic Curves over Finite Fields, Ph.D. thesis, UC Berkeley, 1996.
[11] C. Munuera, J. Tena, An algorithm to compute the number of points on elliptic curves of j-invariant 0 or 1728 over a finite fields, Rend. Circ. Mat. Palermo, Ser. II XLII (1993) 106–116.
[12] A. Pizer, Ramanujan graphs and Hecke operators, Bull. Am. Math. Soc. 23 (1990) 127–137.
[13] R. Schoof, Nonsingular plane cubic curves over finite fields, J. Comb. Theory, Ser. A 46 (1987) 183–211.
[14] J. Silverman, The Arithmetic of Elliptic Curves, second edition, Springer, 2009.
[15] A. Sutherland, Isogeny volcanoes, in: Algorithmic Number Theory, ANTS 2013, in: MSP Open Book Series, vol. 1, 2013, pp. 507–530.
[16] A. Sutherland, Modular polynomials, math.mit.edu/~drew/ClassicalModPolys.html.
[17] L. Washington, Elliptic Curves: Number Theory and Cryptography, second edition, Chapman & Hall/CRC, 2008.
[18] W. Waterhouse, Abelian varieties over finite fields, Ann. Sci. Éc. Norm. Supér. 2 (1969) 521–560.
[19] Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao, V. Soukharev, A post-quantum digital signature scheme based on supersingular isogenies, in: Financial Cryptography and Data Security, FC 2017, in: LNCS, vol. 10322, 2018, pp. 163–181.