Available online at www.sciencedirect.com

ScienceDirect

Applied Mathematics and Computation 196 (2008) 67–76

APPLIED MATHEMATICS AND COMPUTATION

www.elsevier.com/locate/amc

Computing the height of volcanoes of ℓ-isogenies of elliptic curves over finite fields [☆]

J. Miret [a], R. Moreno [a], D. Sadornil [b], J. Tena [c], M. Valls [a,*]

[a] *Dept. de Matemàtica, Universitat de Lleida, Spain*
[b] *Dept. de Matemáticas, Universidad de Salamanca, Spain*
[c] *Dept. de Álgebra, Geometría y Topología, Universidad de Valladolid, Spain*

Abstract

The structure of the volcano of ℓ-isogenies, ℓ-prime, of elliptic curves over finite fields has been extensively studied over recent years. Previous works present some results and algorithms concerning the height of such volcanoes in the case of isogenies whose kernels are generated by a rational point. The main goal of this paper is to extend such works to the case of ℓ-isogenies whose kernels are defined by a rational subgroup. In particular, the height of such volcanoes is completely characterized and can be computationally obtained.

Keywords: Elliptic curves; Finite fields; Isogenies; Volcanoes

1. Introduction

Along the last decade, several works concerning the properties of isogenies of elliptic curves over a finite field $\mathbb{F}_q$ have been undertaken. This study was firstly faced by Kohel [6], who characterized the relation of ℓ-isogeny, ℓ-prime, as a graph, whose nodes represent isomorphism classes of elliptic curves, and adjacent nodes correspond to ℓ-isogenous curves. Each connex component of this graph was named *volcano* due to its distinctive structure: it consists of a cycle at the top level (called *crater*), from whose nodes hang $\ell - 1$ trees which are ℓ-ary complete (see Section 3).

Lately, volcanoes of isogenies were further reviewed by Fouquet and Morain [3]. They were interested in this structure to introduce computational improvements to the SEA algorithm that computes the cardinal of a given elliptic curve [1]. Their approach provides the height of the volcano of that curve, by taking benefit of an exhaustive search algorithm to go through the nodes over several paths of the volcano. This algorithm involves computing the roots of ℓ-modular polynomials to visit adjacent nodes.

[☆] Partially supported by the Grants MTM2007-66842-C02-02, MTM2004-008076 and TIN2006-15662-C02-02 (Spain).

[*] Corresponding author. Address: Jaume II, 69, 25001-Lleida, Spain.
E-mail addresses: miret@eps.udl.es (J. Miret), ramiro@eps.udl.es (R. Moreno), sadornil@usal.es (D. Sadornil), tena@agt.uva.es (J. Tena), magda@eps.udl.es (M. Valls).

0096-3003/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.amc.2007.05.037

Recently, several papers have devoted their interest in the study of the properties of these volcanoes. Firstly, an algorithm to determine the structure of the volcano of 2-isogenies of an ordinary elliptic curve has been reported in [10]. The core of such an algorithm relies, on the one hand, on the relationship between the 2-Sylow group of the curves with their corresponding level in the volcano and, on the other hand, on the usage of the Vélu formulae for the computation of the isogenous curves. This procedure has been recently extended [11] to the case $\ell = 3$. Furthermore, some results concerning the height of the volcano are also provided in that paper for the case of ℓ-isogenies, for any prime ℓ, in the particular case of isogenies defined by a rational point of order ℓ.

The goal of the present paper is to broaden this approach, extending the study to the general case of ℓ-isogenies defined by rational subgroups of elliptic curves over $\mathbb{F}_q$, with characteristic different from 2 and 3. The paper is organized in three further sections. Section 2 briefly collects some basic notations and previous results concerning isogenies. Section 3 is mainly devoted to develop different results that allow us to characterize the height of the volcano of ℓ-isogenies of a given elliptic curve. Finally, Section 4 concerns computational aspects, as well as provides some examples, which have been found by taking advantage of the parametrization of the elliptic curves endowed with an ℓ-rational subgroup by means of the modular curve $X_0(\ell)$.

2. Isogenies of elliptic curves

In this section we will introduce the notations that will be used in the sequel concerning isogenies and rational subgroups of an elliptic curve. As well, we also report some results describing the relationship between the ℓ-isogenies and the action of the Frobenius endomorphism on the ℓ-torsion group.

Let E and E' be two elliptic curves over a field K. An isogeny between E and E' over K is a morphism

$$\begin{aligned} \mathscr{I} &: E \to E', \\ (x,y) &\mapsto (R_1(x), R_2(x,y)), \end{aligned}$$

where $R_1(x)$ and $R_2(x,y)$ are rational functions, i.e., $R_1(x) \in K(x)$, and $R_2(x,y) \in K(x,y)$ (see [14]) and such that $\mathscr{I}(\mathcal{O}_E) = \mathcal{O}_{E'}$, being $\mathcal{O}_E$ and $\mathcal{O}_{E'}$ the points at infinity of the curves.

If G is a finite non trivial subgroup of $E(\overline{K})$, there is a unique elliptic curve E' and an isogeny $E \xrightarrow{\mathscr{I}} E'$ such that $\ker \mathscr{I} = G$ [13]. More precisely, when the cardinal of G is d we say that it is an isogeny of degree d or a d-isogeny. In fact, since any isogeny of degree $d = d_1 d_2$ can be constructed as a composition of isogenies of degrees d_1 and d_2, it is enough to consider isogenies with prime degree ℓ.

If E is defined over K and G is $\mathrm{Gal}(\overline{K}/K)$ invariant, i.e., if G is K-rational, then the elliptic curve E' and the isogeny $\mathscr{I}$ are also defined over K.

When considering elliptic curves over a finite field $\mathbb{F}_q$, the number of rational ℓ-isogenies is closely related with the action of the Frobenius endomorphism on the ℓ-torsion group $E[\ell]$.

Hence, let $E/\mathbb{F}_q$ be an elliptic curve over a finite field $\mathbb{F}_q$, $q = p^r$, with a rational ℓ-isogeny, $\ell \neq p$, and let π be its Frobenius endomorphism. It is known that π satisfies

$$\pi^2 - t\pi + q = 0,$$

where $m = q + 1 - t$ is the cardinal of $E(\mathbb{F}_q)$. Since the subgroup $E[\ell]$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, the action of π on $E[\ell]$ can be seen as a 2×2 matrix with coefficients in $\mathbb{F}_q$, whose characteristic polynomial is

$$X^2 - (t \bmod \ell)X + (q \bmod \ell).$$

Then, the number of rational ℓ-isogenies of $E/\mathbb{F}_q$ (either 1, 2 or $\ell + 1$) and the structure of this matrix are related as follows [12].

Proposition 1. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve over $\mathbb{F}_q$ such that $j(E) \neq 0$, 1728. Then*

(i) *$E/\mathbb{F}_q$ has a unique rational ℓ-isogeny if and only if π has a unique one-dimensional eigenspace in $E[\ell]$.*
(ii) *$E/\mathbb{F}_q$ has exactly two rational ℓ-isogenies if and only if π acts on $E[\ell]$ as a non-scalar diagonal matrix.*
(iii) *$E/\mathbb{F}_q$ has $\ell + 1$ rational ℓ-isogenies if and only if π acts as a scalar matrix on $E[\ell]$.*