Finite Fields and Their Applications 49 (2018) 108–125

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Distorting the volcano

Mireille Fouquet [a], Josep M. Miret [b], Javier Valera [b,*]

[a] *Institut de Mathématiques de Jussieu – Paris Rive Gauche, Université Paris Diderot – Paris 7, France*
[b] *Departament de Matemàtica, Universitat de Lleida, Spain*

ARTICLE INFO

Article history:
Received 18 December 2015
Received in revised form 8 June 2017
Accepted 13 September 2017
Available online xxxx
Communicated by Olga Polverino

MSC:
14H52
14K02

Keywords:
Finite field
Elliptic curve
Isogeny
Volcano
Distortion map

ABSTRACT

Volcanoes of ℓ-isogenies of elliptic curves are a special case of graphs with a cycle called crater. In this paper, given an elliptic curve E of a volcano of ℓ-isogenies, we present a condition over an endomorphism φ of E in order to determine which ℓ-isogenies of E are non-descending. The endomorphism φ is defined as the crater cycle of an m-volcano where E is located, with $m \neq \ell$. The condition is feasible when φ is a distortion map for a subgroup of order ℓ of E. We also provide some relationships among the crater sizes of volcanoes of m-isogenies whose elliptic curves belong to a volcano of ℓ-isogenies.

1. Introduction

Ordinary elliptic curves over a finite field $\mathbb{F}_q$ with the same cardinality together with ℓ-isogenies among them, where ℓ is a prime such that $\ell \nmid q$, can be represented in special graphs called volcanoes of ℓ-isogenies. These structures have interesting applications such

* Corresponding author.
E-mail addresses: fouquet@math.univ-paris-diderot.fr (M. Fouquet), miret@matematica.udl.cat (J.M. Miret), jvalera@matematica.udl.cat (J. Valera).

http://dx.doi.org/10.1016/j.ffa.2017.09.006
1071-5797/

as determining the endomorphism ring of an elliptic curve [16] or computing its group order in the SEA algorithm [22].

In a volcano of ℓ-isogenies the vertices are distributed in levels and the arcs represent ℓ-isogenies [12,16]. The number of levels of a volcano minus one is its height. The vertices located in the highest level belong to a cycle called crater. An arc which goes out from a vertex of the level k can only go inwards to a vertex of the level $k+1$, k or $k-1$. Moreover, horizontal arcs can only occur at the crater. In each case it is said that the arc is, respectively, descending, horizontal or ascending.

Fouquet and Morain [12] gave an algorithm to compute the height of a volcano of ℓ-isogenies using an exhaustive search of several paths in the volcano. As a consequence, some computational improvements were obtained for the SEA algorithm. Later, Ionica and Joux [15], using a symmetric pairing on the ℓ-Sylow subgroup of an elliptic curve, proposed a method to determine the direction of an ℓ-isogeny, that is, descending, horizontal or ascending. This allows us to calculate the height of a volcano more efficiently. Volcanoes of ℓ-isogenies have also been used by Sutherland [24] for the computation of Hilbert class polynomials. Other applications have been provided by Bisson and Sutherland [1] to compute the endomorphism ring of an ordinary elliptic curve and by Bröker, Lauter and Sutherland [3] to compute modular polynomials. Recently, Moody [20] has studied how to compute a volcano of ℓ-isogenies from the knowledge of volcanoes of m-isogenies, $m \neq \ell$.

In this paper, given an ordinary elliptic curve E over $\mathbb{F}_q$, we give a condition for determining which ℓ-isogenies of E are non-descending. For this purpose we consider an endomorphism of E which acts as a distortion map. As a consequence, we present an algorithm which returns an ascending path from E in the volcano of ℓ-isogenies where it belongs.

The paper is structured as follows. Section 2 introduces some concepts and notations about volcanoes of ℓ-isogenies. Section 3 provides some preliminary results concerning the existence and direction of isogenies. In Section 4 we give a characterization for the kernels of the non-descending ℓ-isogenies. In Section 5 we present some relationships among the crater sizes of volcanoes of m-isogenies whose elliptic curves belong to a volcano of ℓ-isogenies. In Section 6 we propose an algorithm for computing an ascending path in a volcano of ℓ-isogenies and we study its complexity. Section 7 is devoted to showing several examples. Finally, in Section 8 we give our conclusions about this paper.

Throughout this paper we consider elliptic curves over a finite field $\mathbb{F}_q$ of characteristic p, with j-invariant different from 0 and 1728. Furthermore, we denote by ℓ and m two distinct primes different from p.

2. Volcanoes of ℓ-isogenies

In this section we introduce the concept of volcano of ℓ-isogenies and we provide some notations and some of their properties.