Forbidden isogenies

Bradley W. Brock[1] Everett W. Howe [2]

[1]IDA Center for Communications Research, Princeton

[2]Unaffiliated mathematician

14th Algorithmic Number Theory Symposium
Rump session
1 July 2020

Email: however@alumni.caltech.edu Web site: ewhowe.com Twitter: @howe

Graphs of Richelot isogenies

Richelot graphs

- *Vertices*: Principally polarized abelian surfaces over $\mathbb{F}_q$
- *Edges*: Richelot isogenies from one PPAS to another

One might choose to restrict to subgraphs:

- Supersingular abelian surfaces
- Super*special* abelian surfaces
- Jacobians
- $\ldots$

A few papers that discuss algorithms based on Richelot graphs

Wouter Castryck, Thomas Decru, Benjamin Smith:
Hash functions from superspecial genus-2 curves using Richelot isogenies

Craig Costello, Benjamin Smith:
The supersingular isogeny problem in genus 2 and beyond

E. V. Flynn, Yan Bo Ti:
Genus two isogeny cryptography

Toshiyuki Katsura, Katsuyuki Takashima:
Counting Richelot isogenies between superspecial abelian surfaces

Katsuyuki Takashima:
Efficient algorithms for isogeny sequences and their cryptographic applications

What do these graphs even *look* like?

Volcanos?

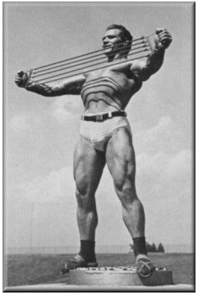
Mount Ngauruhoe, by Flickr user russellstreet

What do these graphs even *look* like?

Volcanos?

Mount Ngauruhoe, by Flickr user russellstreet

Expanders?



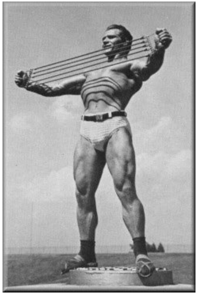
Olympic athlete John Grimek

What do these graphs even *look* like?

Volcanos?

Mount Ngauruhoe, by Flickr user russellstreet

Expanders?



Olympic athlete John Grimek

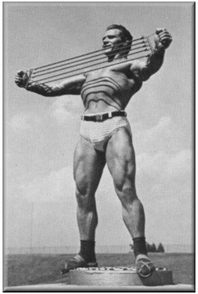
Are they connected? Are there short paths? What's the diameter?

What do these graphs even *look* like?

Volcanos?

Mount Ngauruhoe, by Flickr user russellstreet

Expanders?



Olympic athlete John Grimek

Are they connected? Are there short paths? What's the diameter?

Why are we stuck using *these* confusing graphs?

Humanistic mathematics

As the poet Mary Oliver writes in “The Summer Day”:

Tell me, what is it you plan to do
With your one wild and precious life?

Humanistic mathematics

As the poet Mary Oliver writes in “The Summer Day”:

Tell me, what is it you plan to do
With your one wild and precious life?

Will you wander, hopeless, lost
In a vast and undirected graph?

Humanistic mathematics

As the poet Mary Oliver writes in “The Summer Day”:

Tell me, what is it you plan to do
With your one wild and precious life?

Will you wander, hopeless, lost
In a vast and undirected graph?

If we want *meaning* and *hope* in our lives and in our math,
we need to find a better graph.

Where to look?

The answer is hidden in plain sight

Castryck/Decru/Smith: “Let K be a field of characteristic $p > 5$.”

Costello/Smith: “Throughout, p denotes a prime > 3, and ℓ a prime not equal to p.”

Flynn/Ti: “Let p and ℓ be distinct primes… We will use Richelot isogenies [$\ell = 2$].”

Katsura/Takashima: “Let k be an algebraically closed field of characteristic $p > 5$.”

Takashima: “Let p be an odd prime > 5.”

The answer is hidden in plain sight

Castryck/Decru/Smith: "Let K be a field of characteristic $p > 5$."

Costello/Smith: "Throughout, p denotes a prime > 3, and ℓ a prime not equal to p."

Flynn/Ti: "Let p and ℓ be distinct primes... We will use Richelot isogenies [$\ell = 2$]."

Katsura/Takashima: "Let k be an algebraically closed field of characteristic $p > 5$."

Takashima: "Let p be an odd prime > 5."

Conspiracy theory

What are these authors trying to keep from us?

The answer is hidden in plain sight

Castryck/Decru/Smith: “Let K be a field of characteristic $p > 5$.”

Costello/Smith: “Throughout, p denotes a prime > 3, and ℓ a prime not equal to p.”

Flynn/Ti: “Let p and ℓ be distinct primes... We will use Richelot isogenies [$\ell = 2$].”

Katsura/Takashima: “Let k be an algebraically closed field of characteristic $p > 5$.”

Takashima: “Let p be an odd prime > 5.”

Conspiracy theory

What are these authors trying to keep from us?
This studied focus on *odd* primes can hardly be a coincidence.

The answer is hidden in plain sight

Castryck/Decru/Smith: “Let K be a field of characteristic $p > 5$.”

Costello/Smith: “Throughout, p denotes a prime > 3, and ℓ a prime not equal to p.”

Flynn/Ti: “Let p and ℓ be distinct primes... We will use Richelot isogenies [$\ell = 2$].”

Katsura/Takashima: “Let k be an algebraically closed field of characteristic $p > 5$.”

Takashima: “Let p be an odd prime > 5.”

Conspiracy theory

What are these authors trying to keep from us?
This studied focus on *odd* primes can hardly be a coincidence.
Wake up, sheeple!

My colleague Brad Brock and I:

Why not Richelot isogenies. . . *in characteristic two*

My colleague Brad Brock and I:

- Mavericks

Why not Richelot isogenies. . . *in characteristic two*

My colleague Brad Brock and I:

- Mavericks
- Unconstrained by “convention”. . .

Why not Richelot isogenies. . . *in characteristic two*

My colleague Brad Brock and I:

- Mavericks
- Unconstrained by "convention". . .
- . . . or bourgeois mathematical "proprieties". . .

Why not Richelot isogenies. . . *in characteristic two*

My colleague Brad Brock and I:

- Mavericks
- Unconstrained by “convention”. . .
- . . . or bourgeois mathematical “proprieties”. . .
- . . . or “common sense”

Why not Richelot isogenies... *in characteristic two*

My colleague Brad Brock and I:

- Mavericks
- Unconstrained by "convention"...
- ...or bourgeois mathematical "proprieties"...
- ...or "common sense"

We plunged straight into the belly of the beast:

We studied *purely inseparable Richelot isogenies.*

Supersingular genus-2 curves in characteristic 2

For every $t \in \overline{\mathbb{F}}_2$ let C_t be the curve

$$C_t\colon\, y^2 + y = \begin{cases} t(x^5 + x^3) & \text{if } t \neq 0; \\ x^5 & \text{if } t = 0. \end{cases}$$

These curves are supersingular, and every supersingular genus-2 curve over $\overline{\mathbb{F}}_2$ is isomorphic to exactly one of them.

Supersingular genus-2 curves in characteristic 2

For every $t \in \overline{\mathbb{F}}_2$ let C_t be the curve

$$C_t\colon\ y^2 + y = \begin{cases} t(x^5 + x^3) & \text{if } t \neq 0; \\ x^5 & \text{if } t = 0. \end{cases}$$

These curves are supersingular, and every supersingular genus-2 curve over $\overline{\mathbb{F}}_2$ is isomorphic to exactly one of them.

Let $\mathcal{G}$ be the graph of Richelot isogenies on the curves C_t.

Is the world *ready* for these results?

Theorem

The graph $\mathcal{G}$ *is connected.*

Is the world *ready* for these results?

Theorem

The graph $\mathcal{G}$ is connected.

Theorem

Suppose $s \in \mathbb{F}_{2^m}$ and $t \in \mathbb{F}_{2^n}$. Then the shortest path in $\mathcal{G}$ connecting C_s and C_t has length bounded above by the following expression in m and n:

Is the world *ready* for these results?

Theorem

The graph $\mathcal{G}$ is connected.

Theorem

Suppose $s \in \mathbb{F}_{2^m}$ and $t \in \mathbb{F}_{2^n}$. Then the shortest path in $\mathcal{G}$ connecting C_s and C_t has length bounded above by the following expression in m and n:

$$1.$$

Is the world *ready* for these results?

Theorem

The graph $\mathcal{G}$ is connected.

Theorem

Suppose $s \in \mathbb{F}_{2^m}$ and $t \in \mathbb{F}_{2^n}$. Then the shortest path in $\mathcal{G}$ connecting C_s and C_t has length bounded above by the following expression in m and n:

$$1.$$

Note: We have examples showing that the bound is sharp.

Is the world *ready* for these results?

Theorem

The graph $\mathcal{G}$ is connected.

Theorem

Suppose $s \in \mathbb{F}_{2^m}$ and $t \in \mathbb{F}_{2^n}$. Then the shortest path in $\mathcal{G}$ connecting C_s and C_t has length bounded above by the following expression in m and n:

$$1.$$

Note: We have examples showing that the bound is sharp.
We can classify the pairs (s, t) for which it is not sharp.

Further results

Let $R(s,t)$ denote the number of non-isomorphic Richelot isogenies from C_s to C_t.

Theorem

We have

$$R(s,t) = \begin{cases} 60 & \text{if } s \text{ and } t \text{ are both nonzero;} \\ 12 & \text{if exactly one of } s \text{ and } t \text{ is zero;} \\ 4 & \text{if } s = t = 0. \end{cases}$$

We give contructions that allow one to compute all of these isogenies.

If you dare think outside the box, why not use this graph for your next algorithm?

Advantages

Submitted for your consideration

If you dare think outside the box, why not use this graph for your next algorithm?

Advantages

- Efficient!

Submitted for your consideration

If you dare think outside the box, why not use this graph for your next algorithm?

Advantages

- Efficient!
- Easy-to-understand graph structure.

Submitted for your consideration

If you dare think outside the box, why not use this graph for your next algorithm?

Advantages

- Efficient!
- Easy-to-understand graph structure.
- Strong upper and lower bounds on path lengths.

Submitted for your consideration

If you dare think outside the box, why not use this graph for your next algorithm?

Advantages

- Efficient!
- Easy-to-understand graph structure.
- Strong upper and lower bounds on path lengths.

You're welcome.

arXiv:2002.02122 [math.AG]