Splittings and the isogeny problem in dimension 2

Sam Frengley (joint work with Maria Corte-Real Santos and Craig Costello)

The dimension 1 case

Isogenies

Isogeny-based cryptography is a type of post-quantum cryptography that has been considered in NIST's standardisation process.

The **general isogeny problem** (in dimension 1) underlies the security of many isogeny-based schemes (e.g., SQIsign)

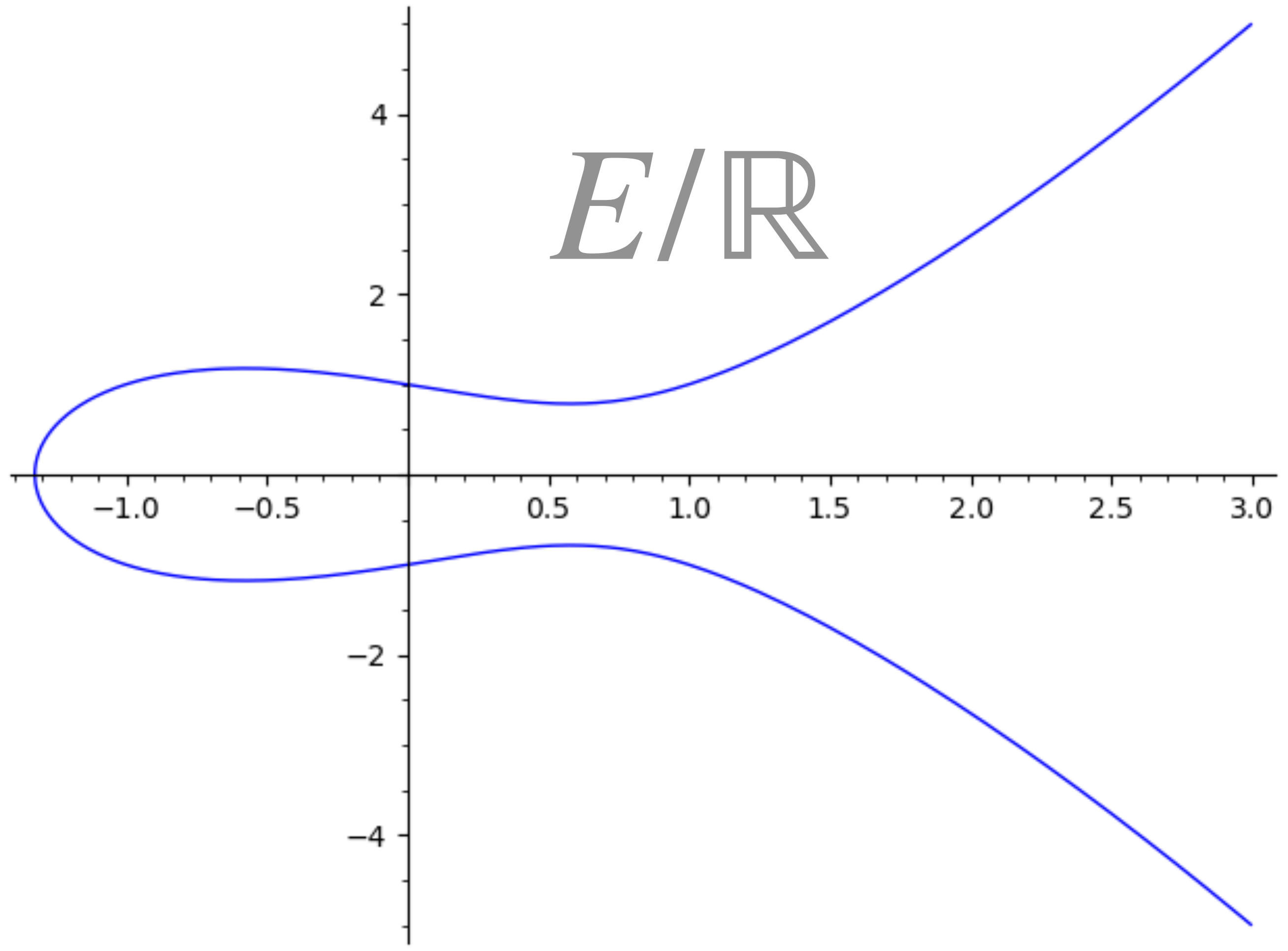
In this work we look at the problem in dimension 2 and decrease the concrete complexity of the best attack (due to Costello–Smith)

Isogenies

$4A^3 + 27B^2 \neq 0$

Let $E/\mathbb{F}_{p^2}$ be an elliptic curve ($p \neq 2,3$). You can write

$$E : y^2 = x^3 + Ax + B$$



where $A, B \in \mathbb{F}_{p^2}$.

Consider some other elliptic curve $E'/\mathbb{F}_{p^2}$

$$E' : y'^2 = x'^3 + A'x' + B'$$

where $A', B' \in \mathbb{F}_{p^2}$.

Isogenies

$$E : y^2 = x^3 + Ax + B \qquad \text{and} \qquad E' : y'^2 = x'^3 + A'x' + B'$$

An isogeny

$$\phi \colon E \to E'$$

is a pair of rational functions $\phi_1, \phi_2 \in \mathbb{F}_{p^2}(x, y)$ such that for every $P = (x_P, y_P) \in E(\bar{\mathbb{F}}_p)$ the point

$$\phi(P) = (\phi_1(x_P, y_P), \phi_2(x_P, y_P))$$

lies on E' (and $\phi(O) = O'$ for the point at infinity).

Isogenies

Fact. Any isogeny $\phi = (\phi_1, \phi_2)$ can be written with $\phi_1 \in \mathbb{F}_{p^2}(x)$.

Example: Over $\mathbb{F}_{23}$

$$E : y^2 = x^3 + x \qquad \text{and} \qquad E' : y'^2 = x'^3 - 4x'$$

given by the equations

$$\phi = \left(\underbrace{\frac{x^2+1}{x}}_{\text{Given only in terms of } x \text{ (no } y\text{)}}, \frac{y(x^2-1)}{x^2} \right)$$

Isogenies

Fact. Any isogeny $\phi = (\phi_1, \phi_2)$ can be written with $\phi_1 \in \mathbb{F}_{p^2}(x)$.

Example: Over $\mathbb{F}_{23}$

$$E : y^2 = x^3 + x \qquad \text{and} \qquad E' : y'^2 = x'^3 + 16x' + 10$$

given by the equations

$$\phi = \left(\underbrace{\frac{(x-10)(x-7)(x^2-8x+9)(x^2-6x-5)}{x(x+5)^2(x-9)^2}}_{\text{Given only in terms of } x \text{ (no } y\text{)}}, \dots \right)$$

Isogenies

Fact. Any isogeny $\phi = (\phi_1, \phi_2)$ can be written with $\phi_1 \in \mathbb{F}_{p^2}(x)$.

The **degree of ϕ** is

$$\deg(\phi) = \max\{\deg(\text{numerator } \phi_1), \deg(\text{denominator } \phi_1)\}$$

Example: Over $\mathbb{F}_{23}$

$$E : y^2 = x^3 + x \qquad \text{and} \qquad E' : y'^2 = x'^3 - 4x'$$

given by the equations

Degree 2

$$\phi = \left(\frac{x^2 + 1}{x}, \frac{y(x^2 - 1)}{x^2} \right)$$

Isogenies

Fact. Any isogeny $\phi = (\phi_1, \phi_2)$ can be written with $\phi_1 \in \mathbb{F}_{p^2}(x)$.

The **degree of ϕ** is

$$\deg(\phi) = \max\{\deg(\text{numerator } \phi_1), \deg(\text{denominator } \phi_1)\}$$

Example: Over $\mathbb{F}_{23}$

$$E : y^2 = x^3 + x \qquad \text{and} \qquad E' : y'^2 = x'^3 + 16x' + 10$$

given by the equations

Degree 6

$$\phi = \left(\frac{(x-10)(x-7)(x^2-8x+9)(x^2-6x-5)}{x(x+5)^2(x-9)^2}, \ldots \right)$$

j-invariant

Fact. A pair of elliptic curves are isomorphic (over $\bar{\mathbb{F}}_p$) if and only if

$$j(E) = j(E').$$

This $j(E)$ is known as the j-invariant of E and is defined by

$$j(E) = 2^8 \cdot 3^3 \cdot \frac{A^3}{4A^3 + 27B^2}$$

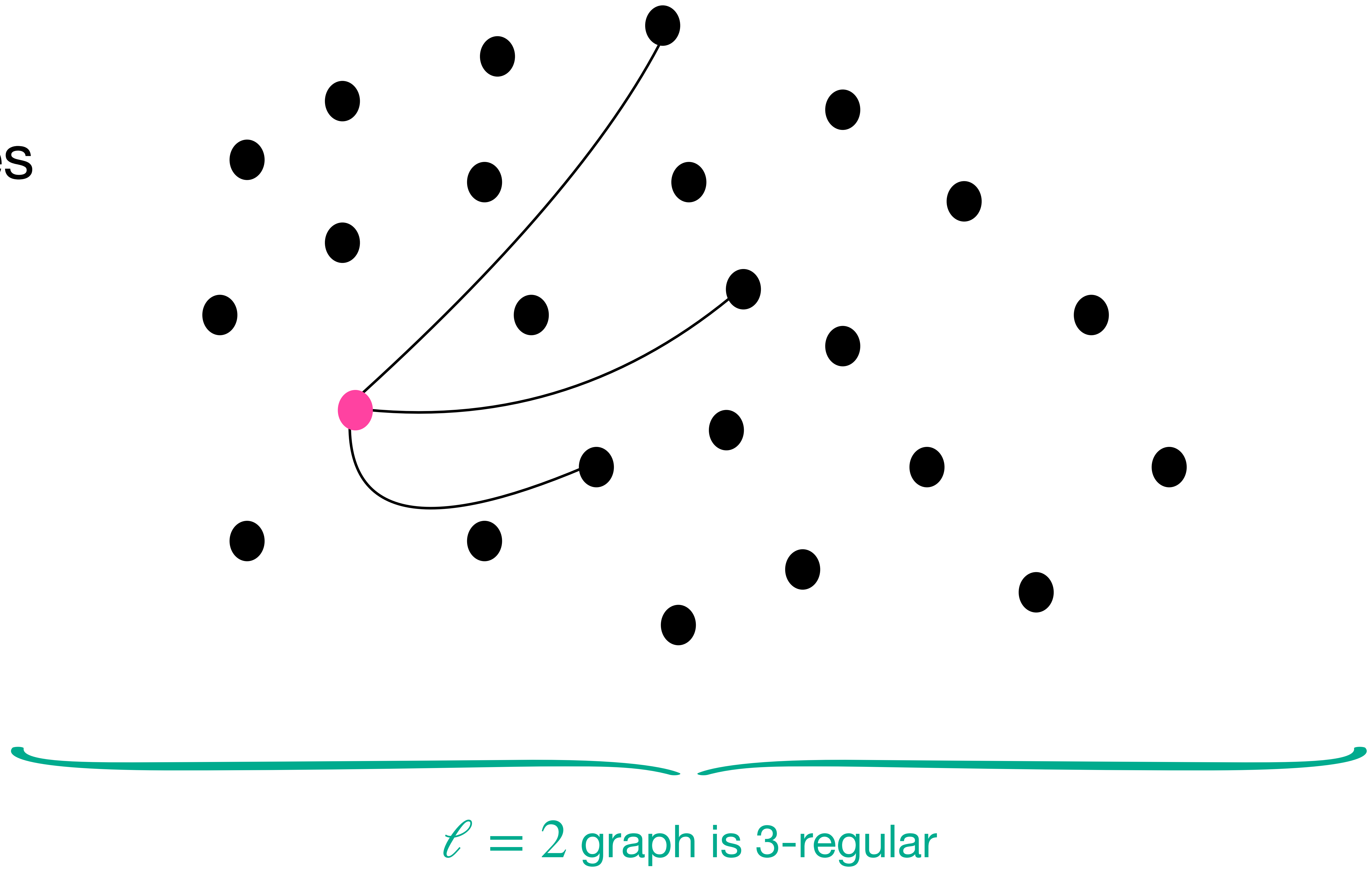
The isogeny problem in dimension 1

Problem (The isogeny problem in dimension 1). Given a pair of supersingular elliptic curves E_1 and E_2 over the finite field $\mathbb{F}_{p^2}$ find an isogeny $E_1 \to E_2$.

Supersingular isogeny graph $\Gamma_1(p;\ell)$

We have:

1. Vertices: j-invariants of supersingular elliptic curves over $\mathbb{F}_{p^2}$
2. Edges: ℓ-isogenies

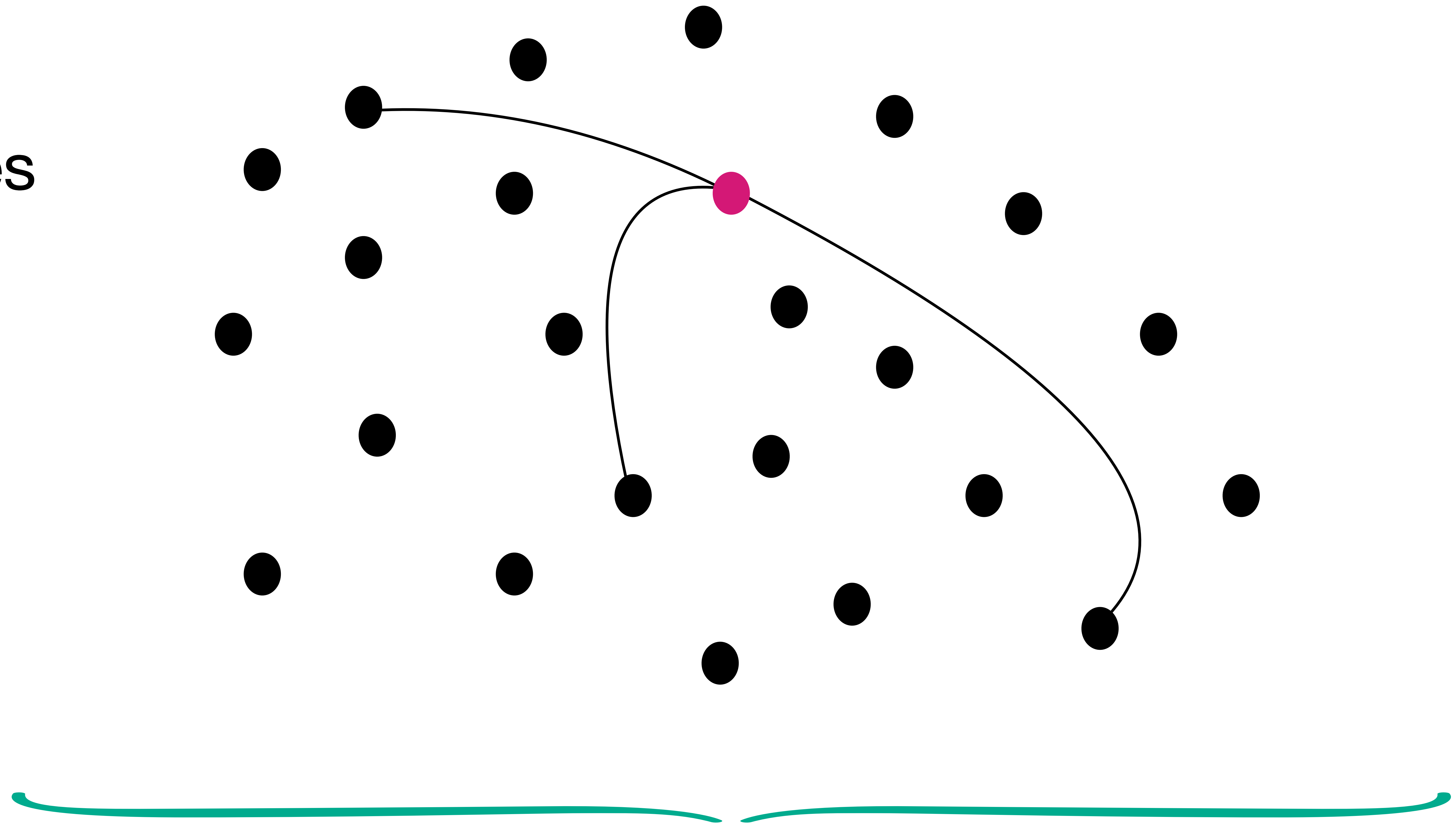


Supersingular isogeny graph $\Gamma_1(p;\ell)$

We have:

1. Vertices: j-invariants of supersingular elliptic curves over $\mathbb{F}_{p^2}$

2. Edges: ℓ-isogenies



$\ell = 2$ graph is 3-regular

Supersingular isogeny graph $\Gamma_1(p;\ell)$

We have:

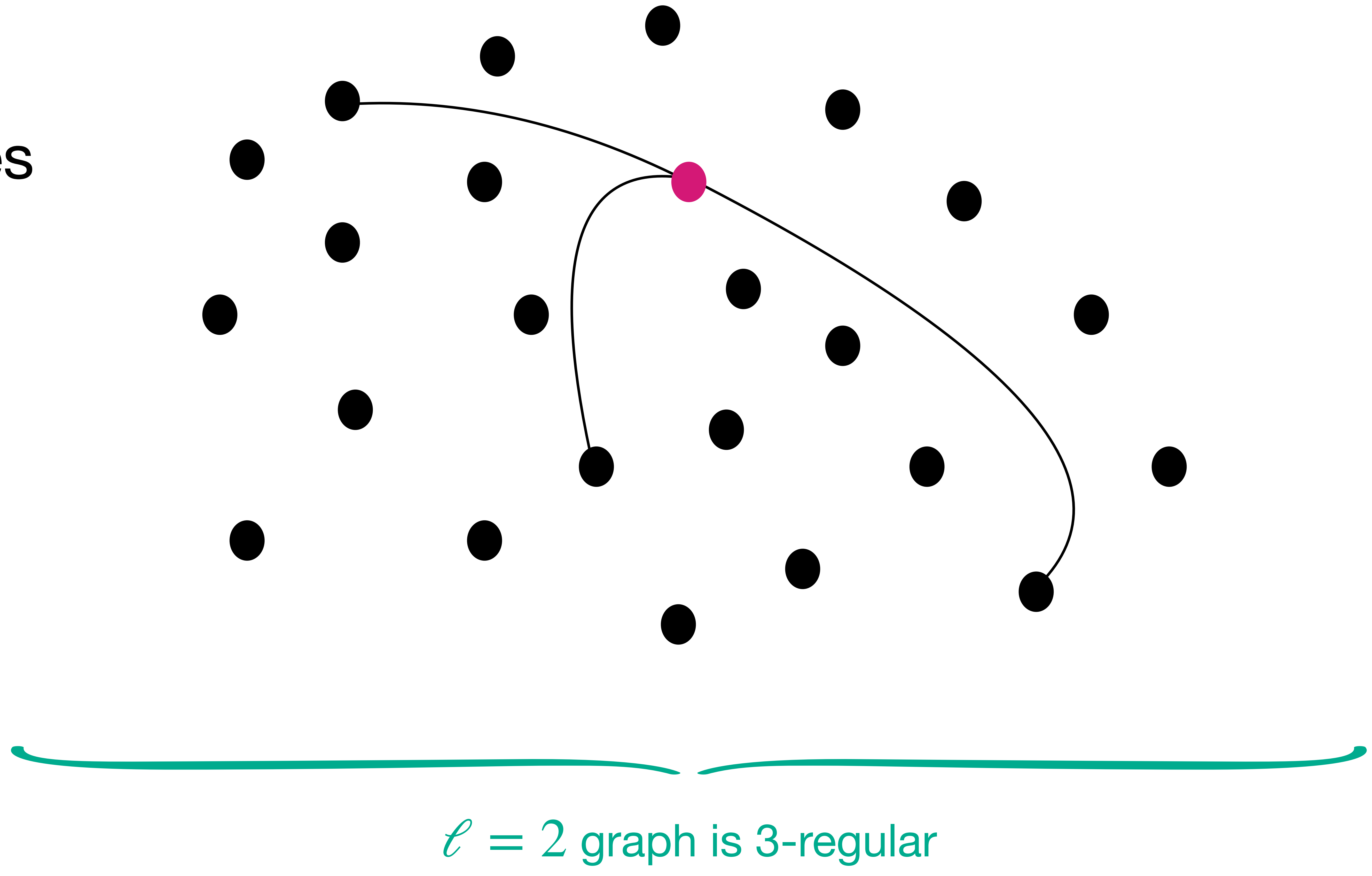
1. Vertices: j-invariants of supersingular elliptic curves over $\mathbb{F}_{p^2}$

2. Edges: ℓ-isogenies

Properties:

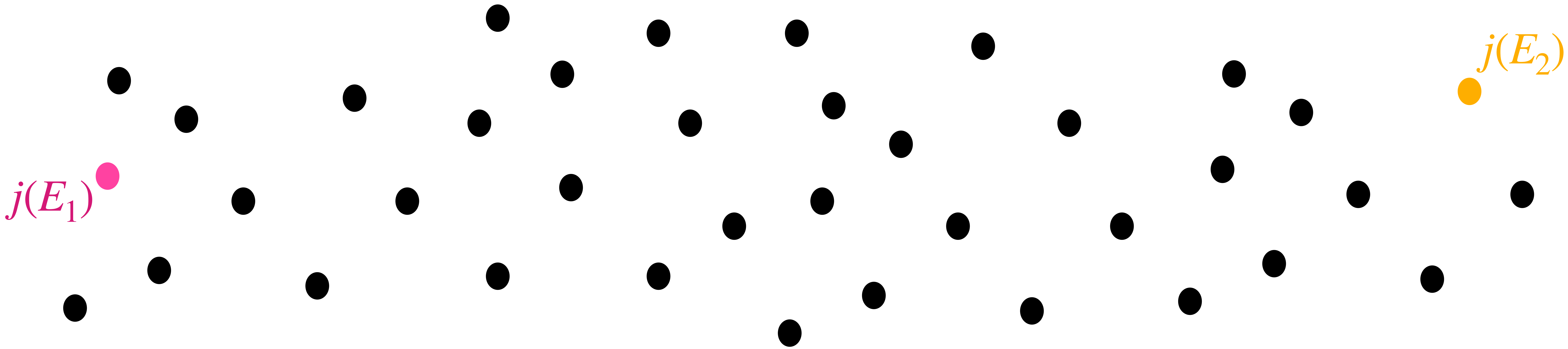
Large: $\sim p/12$ nodes

Great mixing
(Ramanujan graph!)



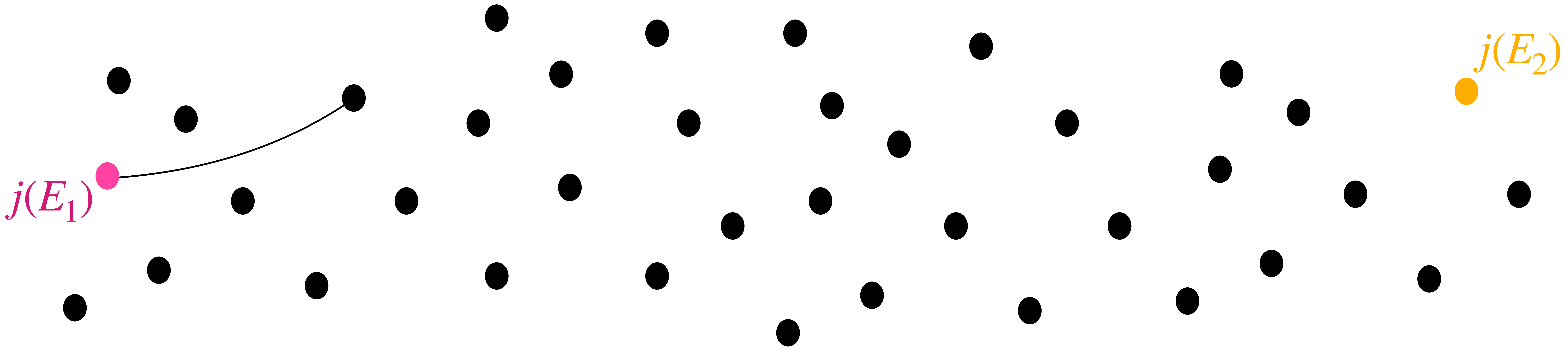
The isogeny problem in dimension 1

Problem (The isogeny problem in dimension 1). Given a pair of supersingular elliptic curves E_1 and E_2 over the finite field $\mathbb{F}_{p^2}$ find an isogeny $E_1 \to E_2$.



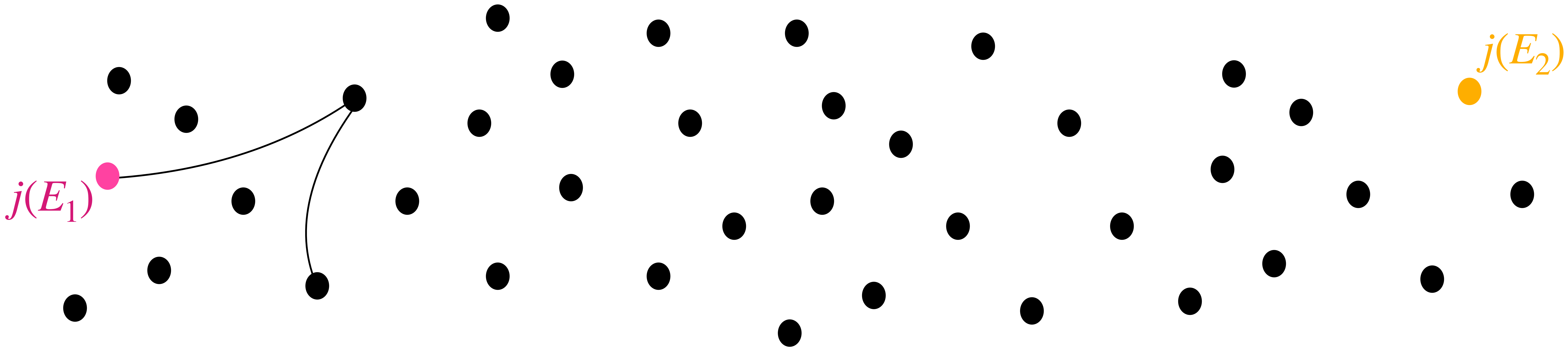
The isogeny problem in dimension 1

Problem (The isogeny problem in dimension 1). Given a pair of supersingular elliptic curves E_1 and E_2 over the finite field $\mathbb{F}_{p^2}$ find an isogeny $E_1 \to E_2$.



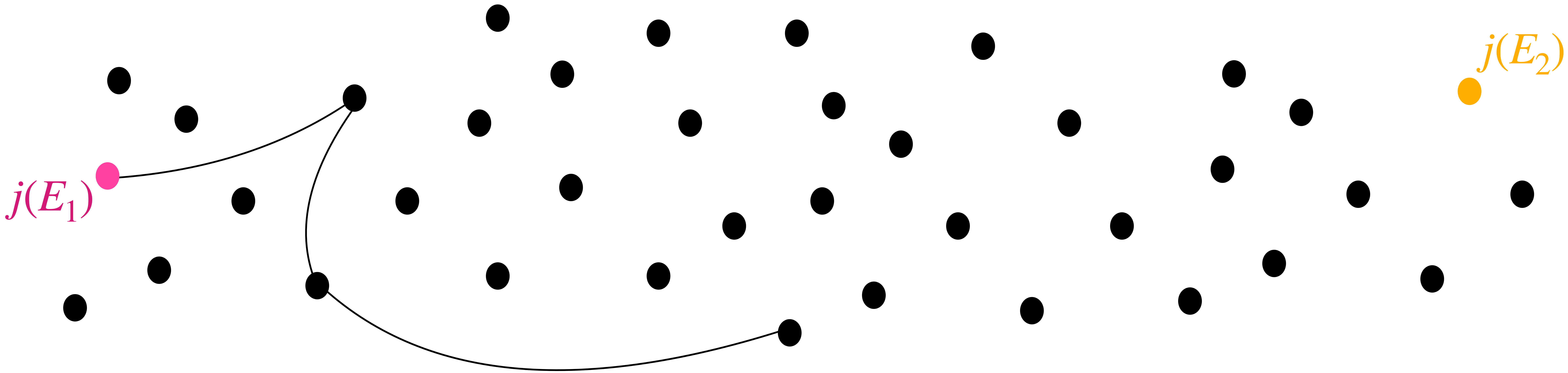
The isogeny problem in dimension 1

Problem (The isogeny problem in dimension 1). Given a pair of supersingular elliptic curves E_1 and E_2 over the finite field $\mathbb{F}_{p^2}$ find an isogeny $E_1 \to E_2$.



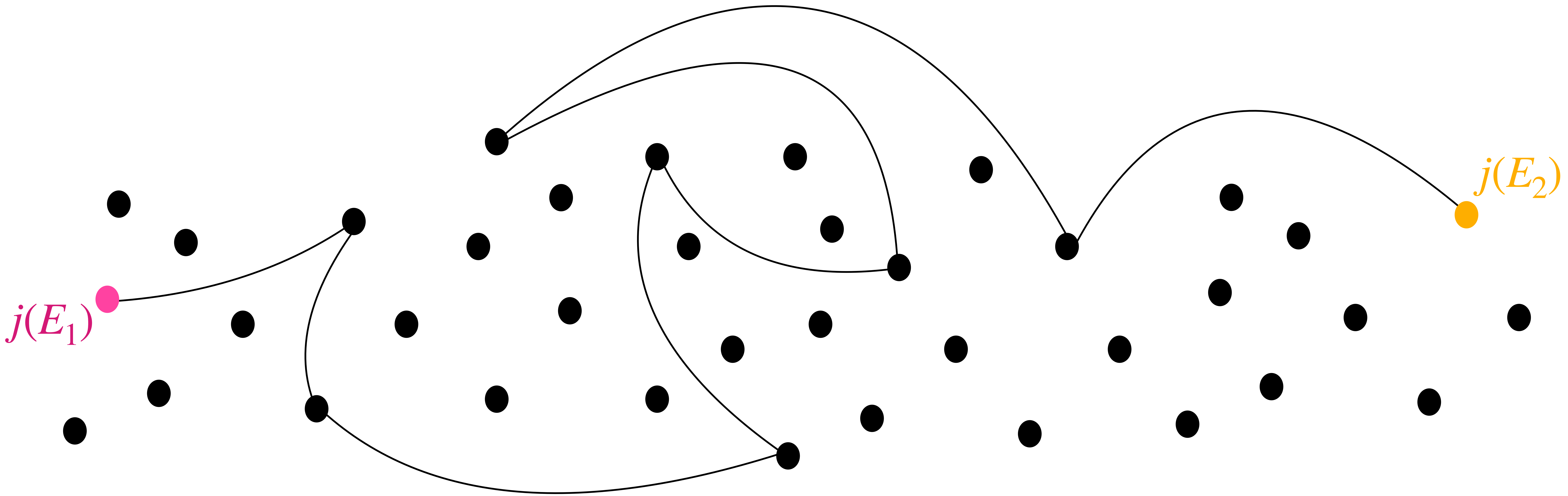
The isogeny problem in dimension 1

Problem (The isogeny problem in dimension 1). Given a pair of supersingular elliptic curves E_1 and E_2 over the finite field $\mathbb{F}_{p^2}$ find an isogeny $E_1 \to E_2$.



The isogeny problem in dimension 1

Problem (The isogeny problem in dimension 1). Given a pair of supersingular elliptic curves E_1 and E_2 over the finite field $\mathbb{F}_{p^2}$ find an isogeny $E_1 \to E_2$.



The isogeny problem in dimension 1

Problem (The isogeny problem in dimension 1). Given a pair of supersingular elliptic curves E_1 and E_2 over the finite field $\mathbb{F}_{p^2}$ find an isogeny $E_1 \to E_2$.

Theorem (Delfs—Galbraith). There exists a $\widetilde{O}(\sqrt{p})$ algorithm to solve the supersingular isogeny problem in dimension 1.

The dimension 2 case

Why dimension 2?

The SIDH attacks showed that **understanding higher dimensional isogenies appears to be crucial** in navigating the supersingular isogeny graph in dimension 1.

However comparatively little is actually known about the (superspecial) isogeny graph in dimension 2!

Abelian surfaces

Abelian surfaces come in 2 flavours

- Products of elliptic curves $E_1 \times E_2$
- Jacobians of genus 2 curves $\mathrm{Jac}(C)$

The isogeny problem in dimension 2

Problem (The isogeny problem in dimension 2). Given a pair of superspecial (p.p.) abelian surfaces A_1 and A_2 over the finite field $\mathbb{F}_{p^2}$ find an isogeny $A_1 \to A_2$.

Superspecial isogeny graph $\Gamma_2(p; \ell)$

We have:

1. Vertices: ($\bar{\mathbb{F}}_p$-isomorphism classes of p.p.) superspecial abelian surfaces over $\mathbb{F}_{p^2}$

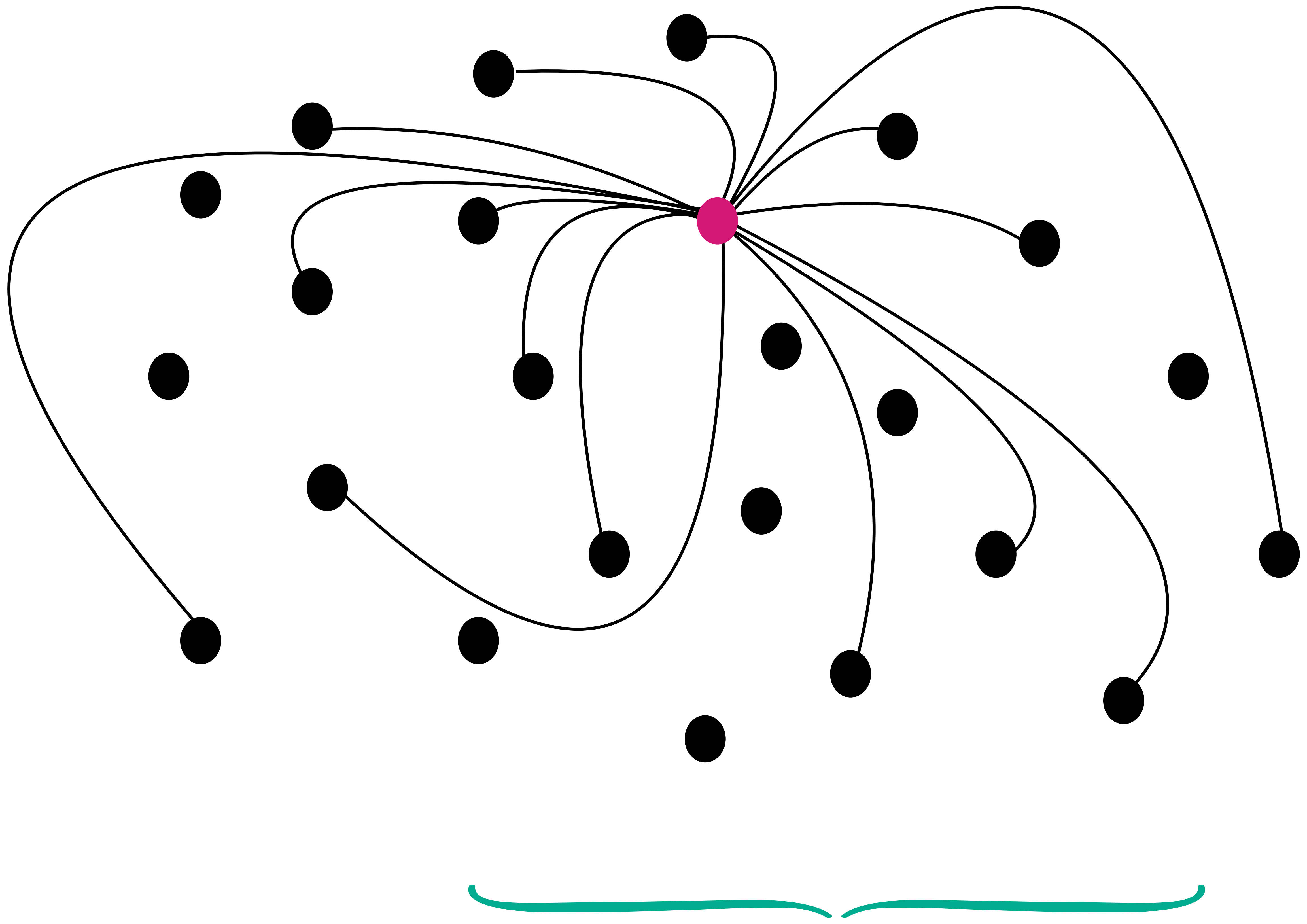
2. Edges: (ℓ, ℓ)-isogenies

Superspecial isogeny graph $\Gamma_2(p;\ell)$

We have:

1. Vertices: ($\bar{\mathbb{F}}_p$-isomorphism classes of p.p.) superspecial abelian surfaces over $\mathbb{F}_{p^2}$

2. Edges: (ℓ,ℓ)-isogenies



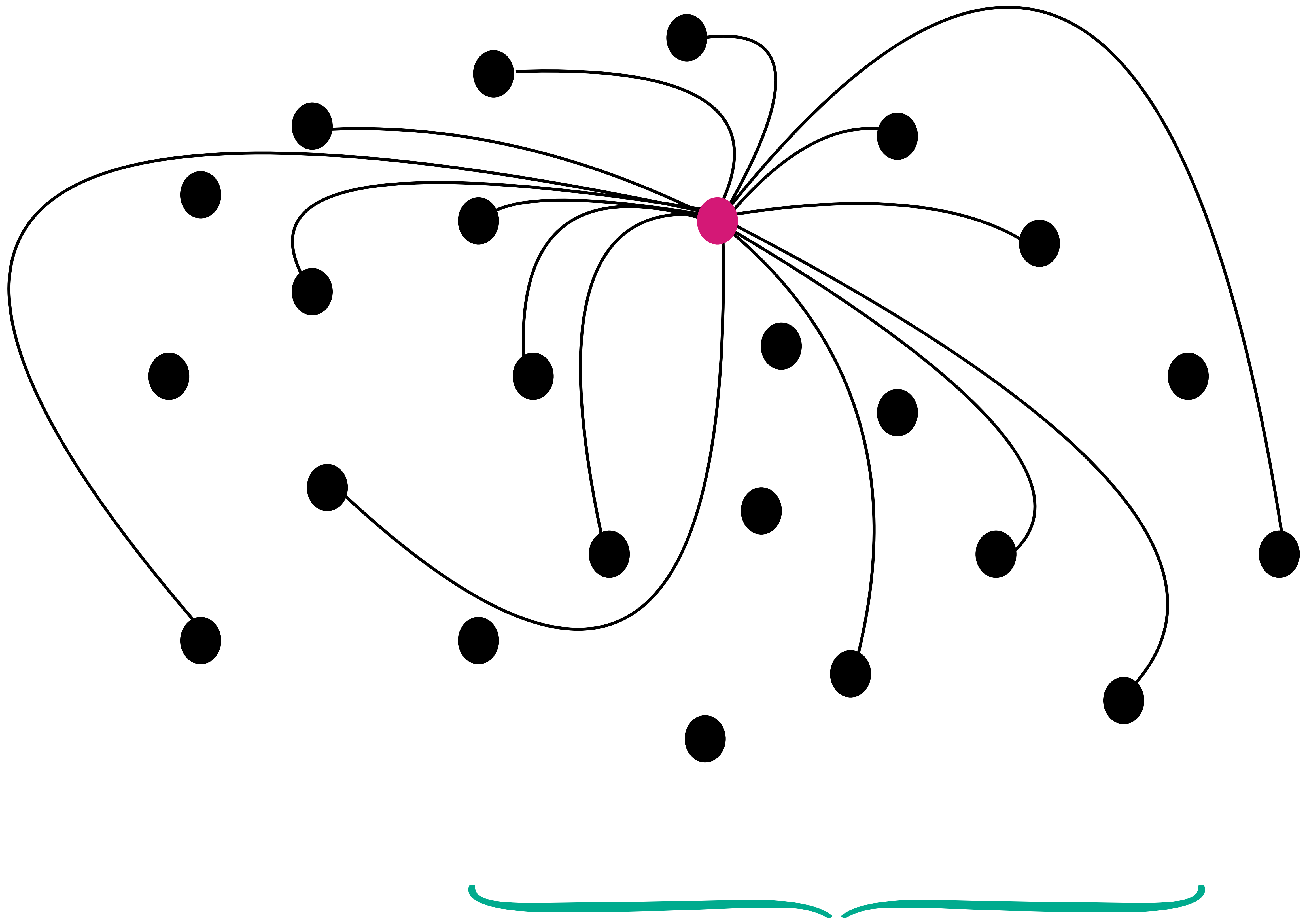
$\ell = 2$ graph is 15-regular

Superspecial isogeny graph $\Gamma_2(p;\ell)$

We have:

1. Vertices: ($\bar{\mathbb{F}}_p$-isomorphism classes of p.p.) superspecial abelian surfaces over $\mathbb{F}_{p^2}$

2. Edges: (ℓ,ℓ)-isogenies



Properties:

Large: $O(p^3)$ nodes

Great mixing!

Superspecial isogeny graph $\Gamma_2(p;\ell)$

We have:

1. Vertices: ($\bar{\mathbb{F}}_p$-isomorphism classes of p.p.) superspecial abelian surfaces over $\mathbb{F}_{p^2}$

2. Edges: (ℓ,ℓ)-isogenies

Writing $\mathcal{S}_2(p)$ for the vertex set of $\Gamma_2(p;\ell)$ we get

$$\mathcal{S}_2(p) = \mathcal{J}_2(p) \sqcup \mathcal{E}_2(p)$$

Jacobians $\sim O(p^3)$

Elliptic products $\sim O(p^2)$

Properties:

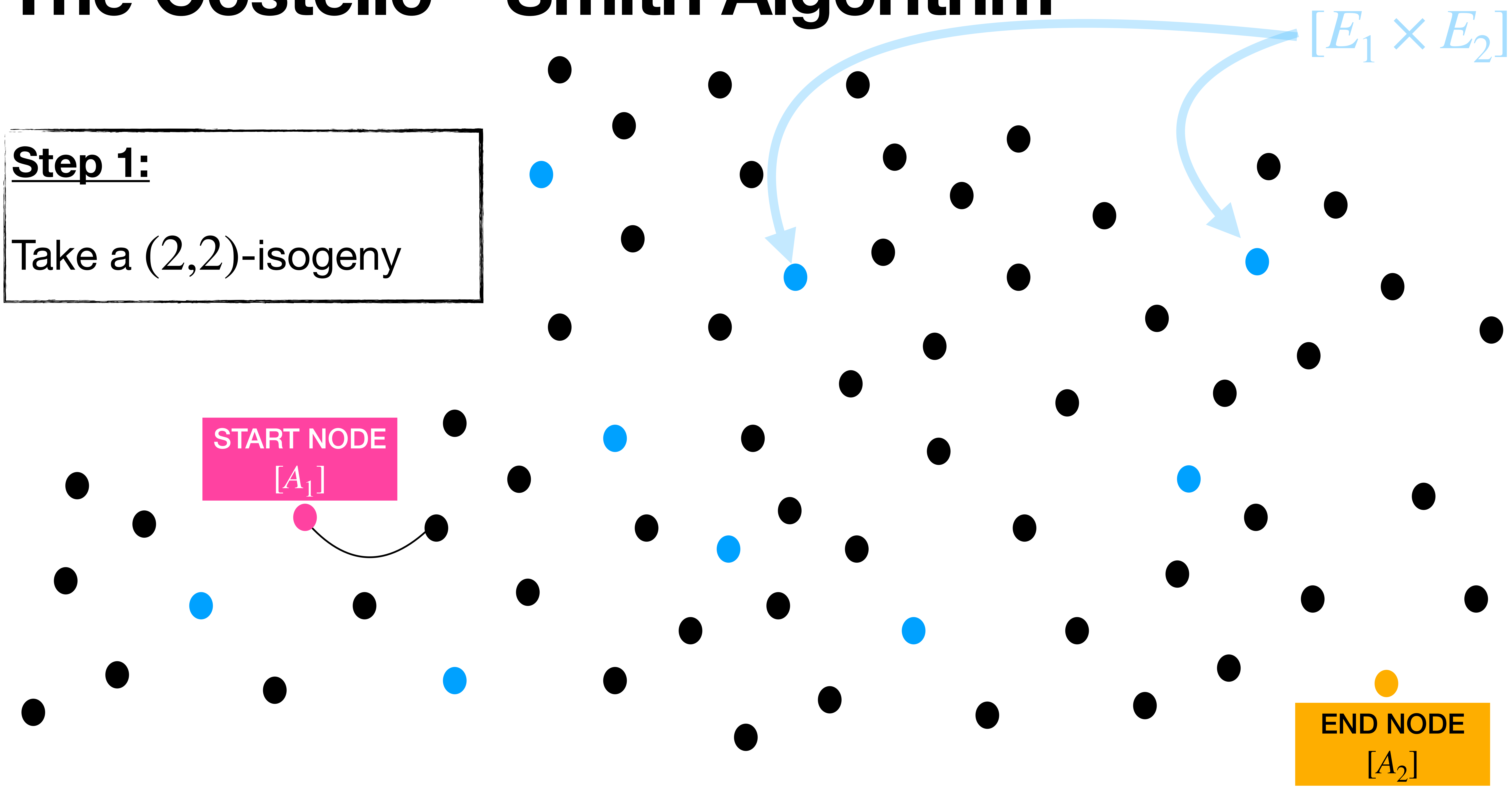
Large: $O(p^3)$ nodes

Great mixing!

The Costello—Smith Algorithm

Step 1:

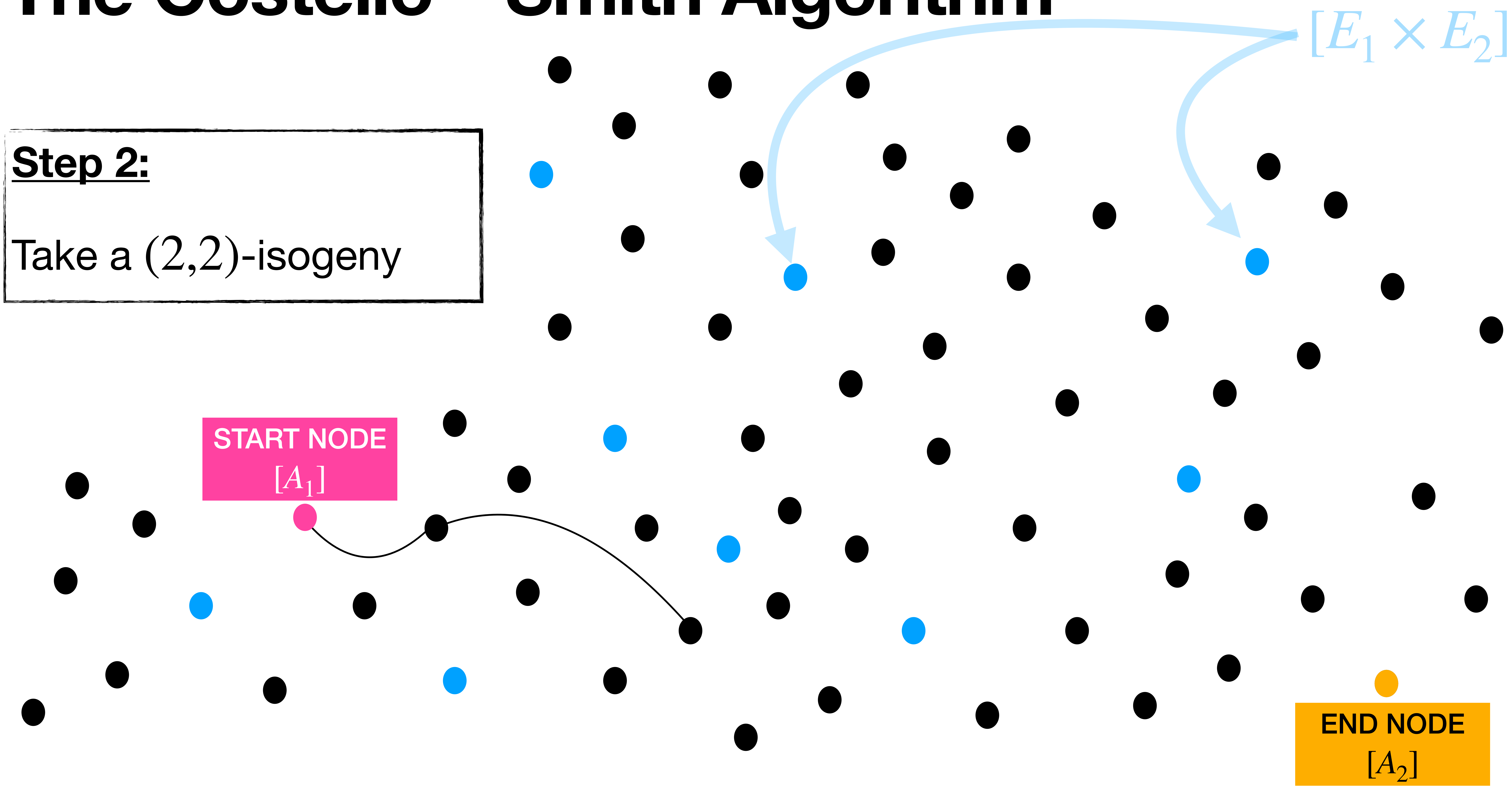
Take a $(2,2)$-isogeny



The Costello—Smith Algorithm

Step 2:

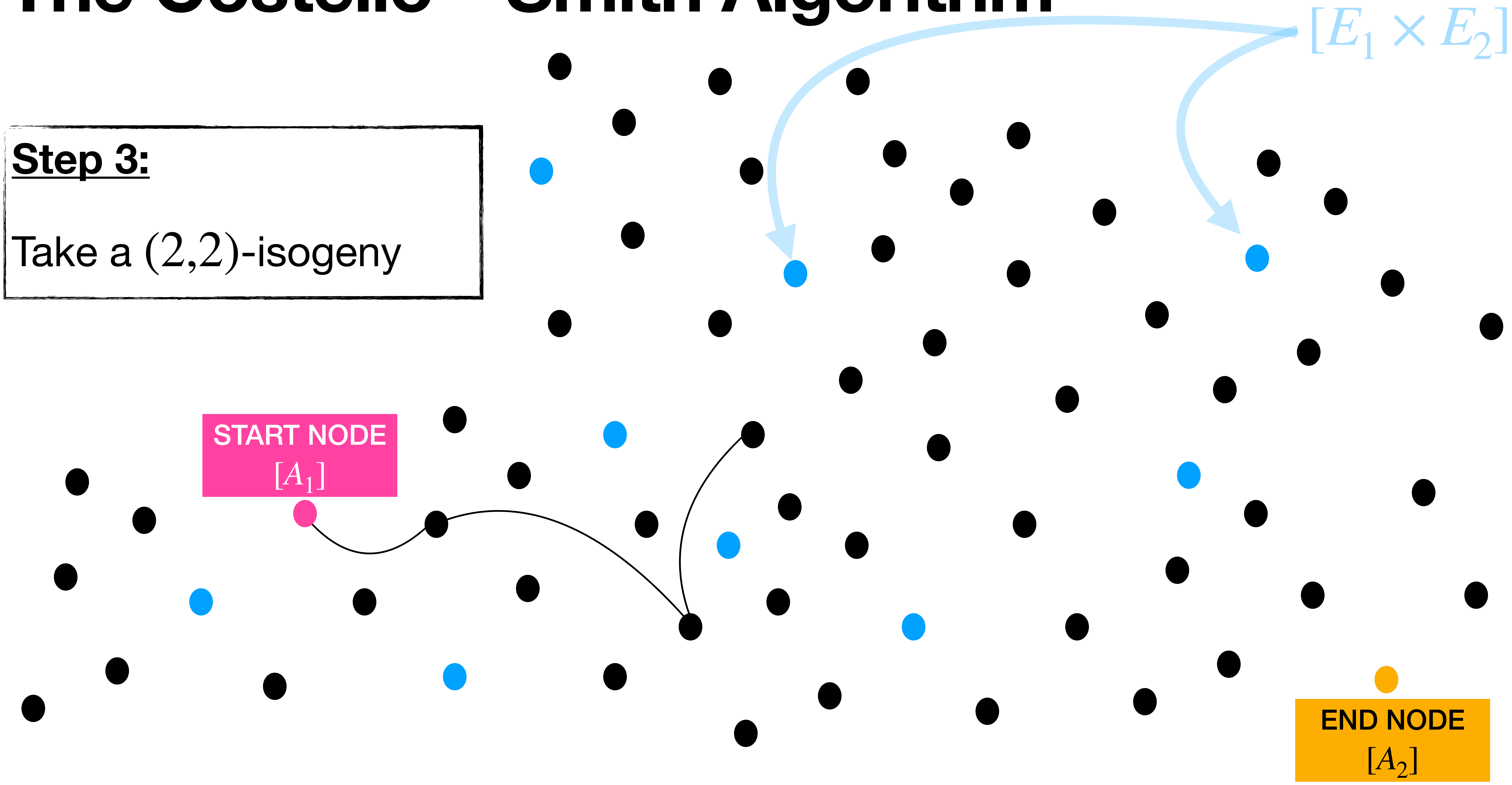
Take a $(2,2)$-isogeny



The Costello—Smith Algorithm

Step 3:

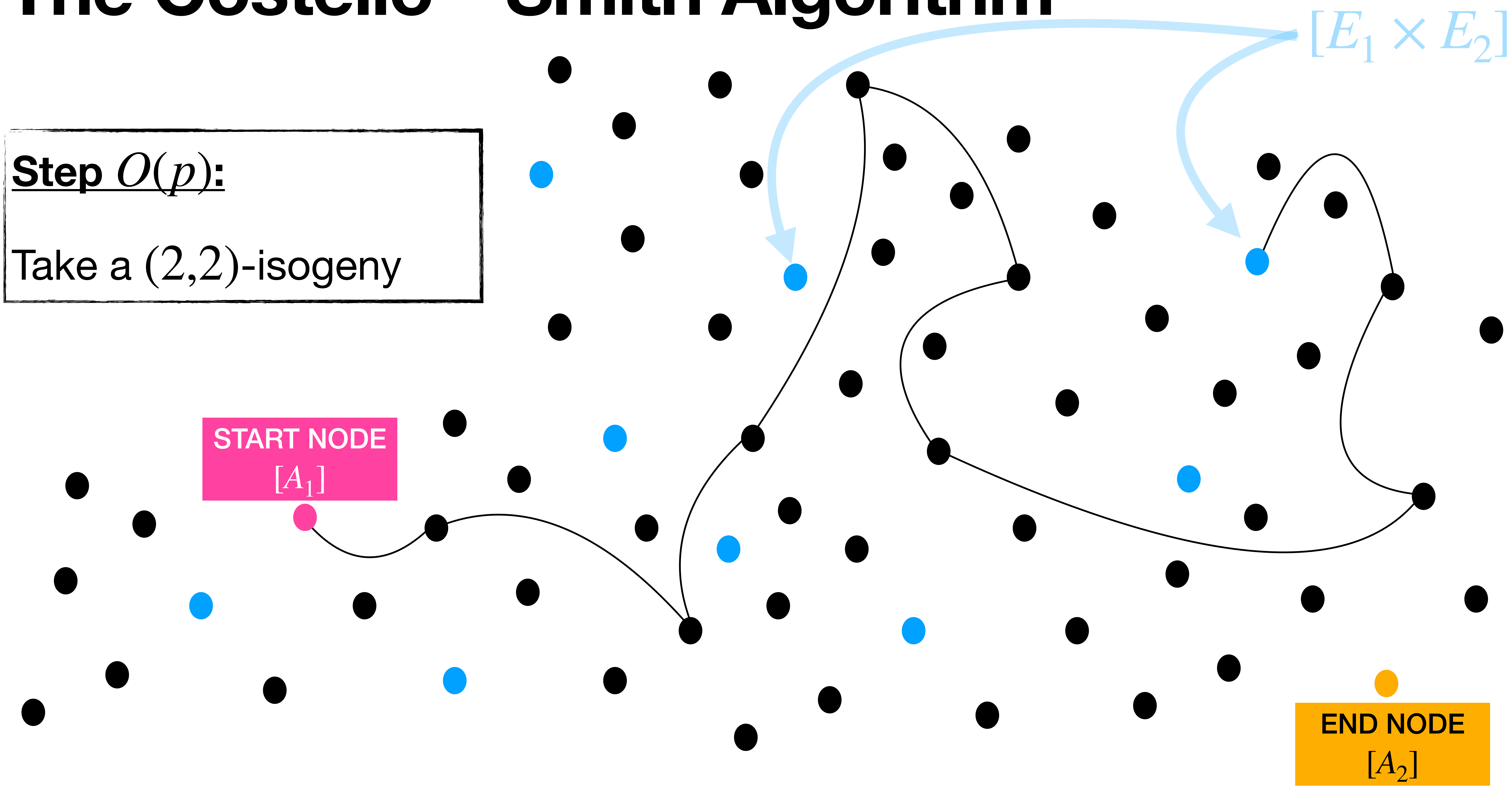
Take a $(2{,}2)$-isogeny



The Costello—Smith Algorithm

Step $O(p)$:

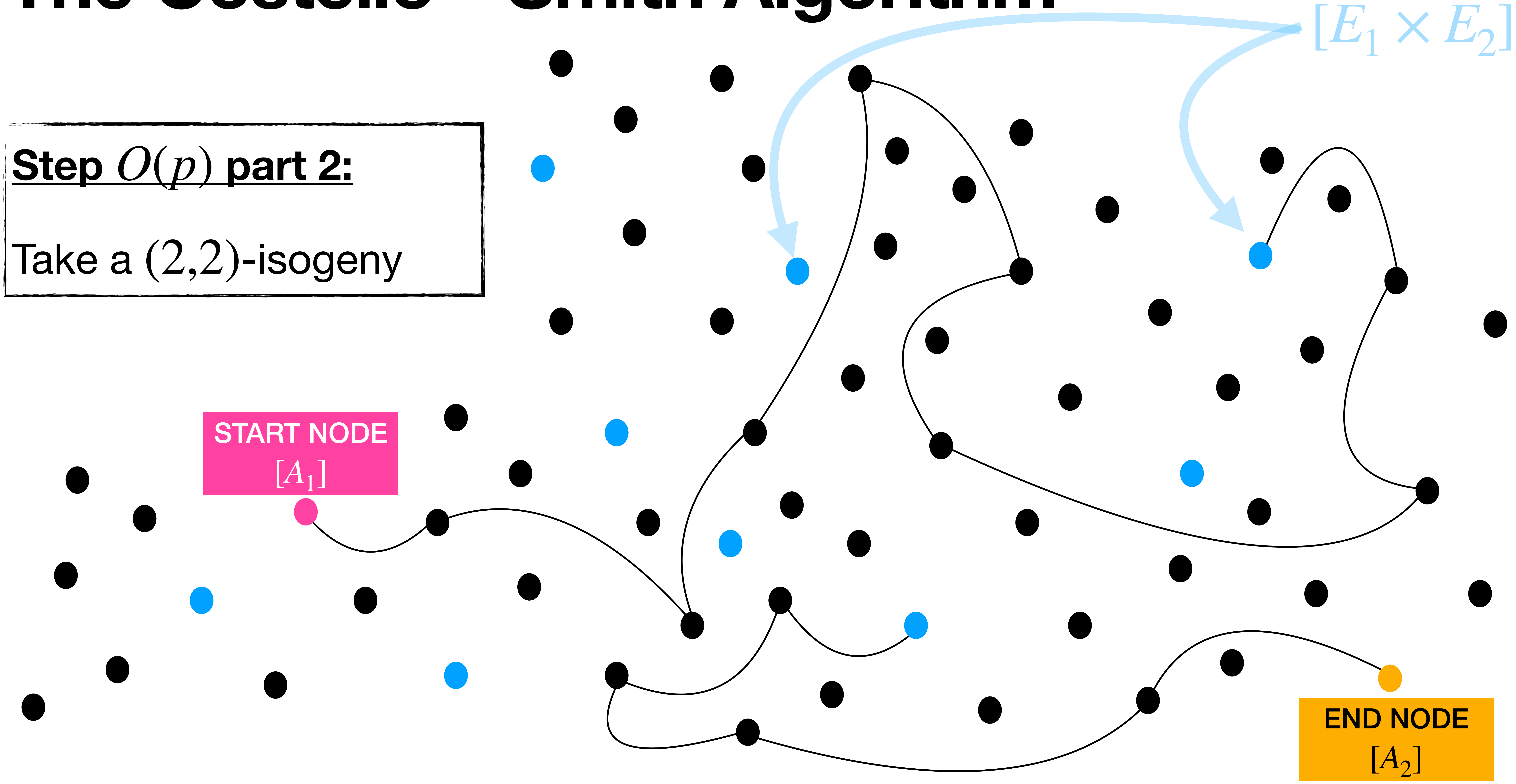
Take a $(2,2)$-isogeny



The Costello—Smith Algorithm

Step $O(p)$ part 2:

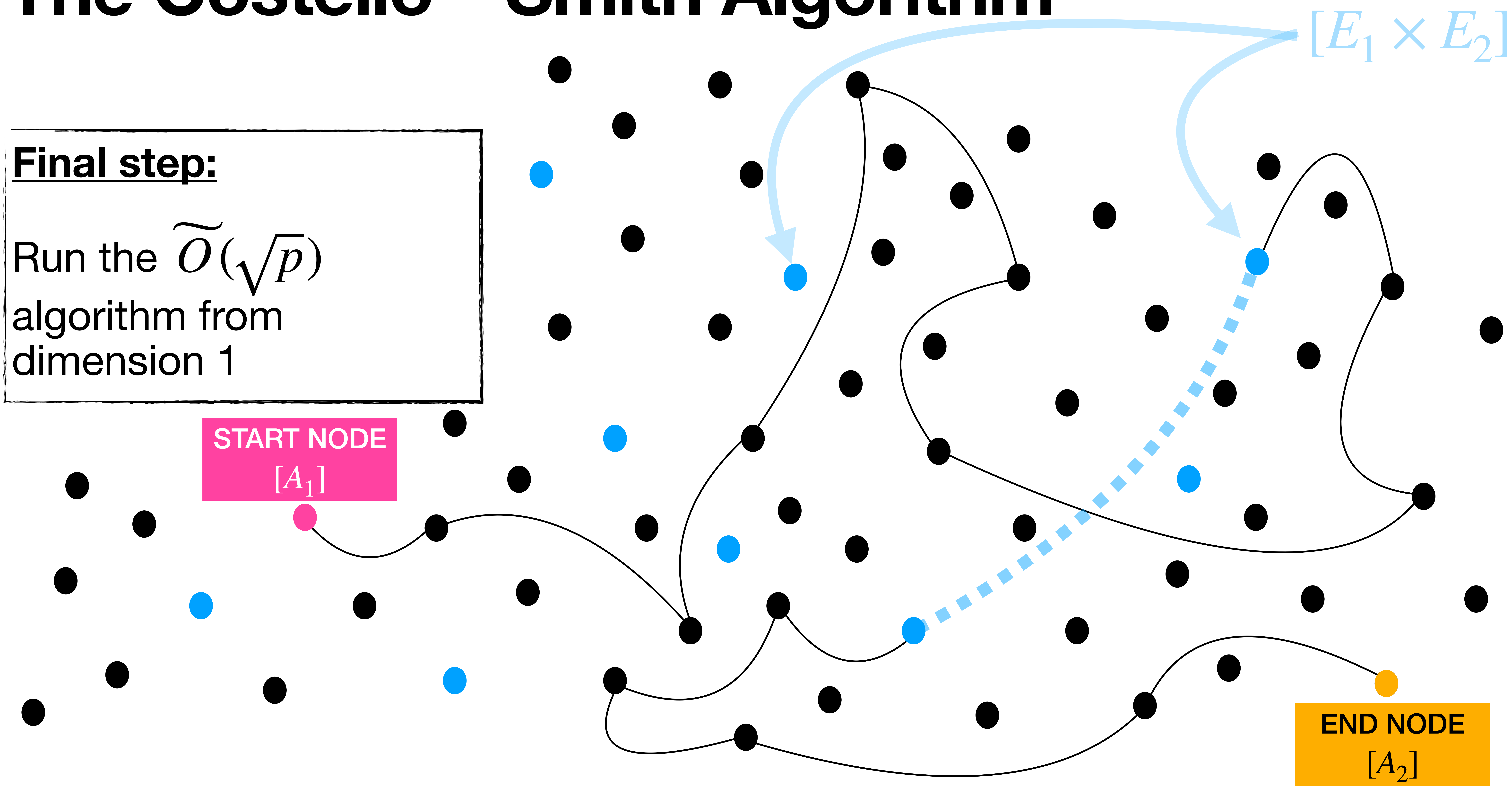
Take a $(2,2)$-isogeny



The Costello—Smith Algorithm

Final step:

Run the $\widetilde{O}(\sqrt{p})$ algorithm from dimension 1



The Costello—Smith Algorithm

To summarise the Costello—Smith Algorithm:

1. Walk from the start vertex in $\Gamma_2(p; 2)$ until we hit a vertex in $\mathcal{E}_2(p)$

The Costello—Smith Algorithm

To summarise the Costello—Smith Algorithm:

1. Walk from the start vertex in $\Gamma_2(p; 2)$ until we hit a vertex in $\mathscr{E}_2(p)$

There are $O(p^3)$ total vertices in $\Gamma_2(p; 2)$ and $O(p^2)$ are in $\mathscr{E}_2(p)$ so this takes $O(p)$ steps

Assuming mild conjecture about distribution of $\mathscr{E}_2(p)$ in the graph

The Costello—Smith Algorithm

To summarise the Costello—Smith Algorithm:

1. Walk from the start vertex in $\Gamma_2(p; 2)$ until we hit a vertex in $\mathscr{E}_2(p)$ $\widetilde{O}(p)$
2. Walk from the end vertex in $\Gamma_2(p; 2)$ until we hit a vertex in $\mathscr{E}_2(p)$ $\widetilde{O}(p)$
3. Run the algorithm in dimension 1 $\widetilde{O}(\sqrt{p})$
4. Return the path.

Theorem (Costello—Smith). There exists a $\widetilde{O}(p)$ algorithm to solve the isogeny problem in dimension 2.

Splittings and accelerating Costello—Smith

(N, N)—splittings

Every (p.p.) superspecial abelian surface has

$$D_N = N^3 \prod_{\ell | N} \frac{1}{\ell^3} (\ell + 1)(\ell^2 + 1)$$

(N, N)-isogenous neighbours. This is $\sim N^3$.

Compute all (N, N)—isogenous neighbours for big N.

Very expensive to compute (N, N)—isogeny.

(N, N)—splittings

Every (p.p.) superspecial abelian surface has

$$D_N = N^3 \prod_{\ell | N} \frac{1}{\ell^3}(\ell + 1)(\ell^2 + 1)$$

(N, N)-isogenous neighbours. This is $\sim N^3$.

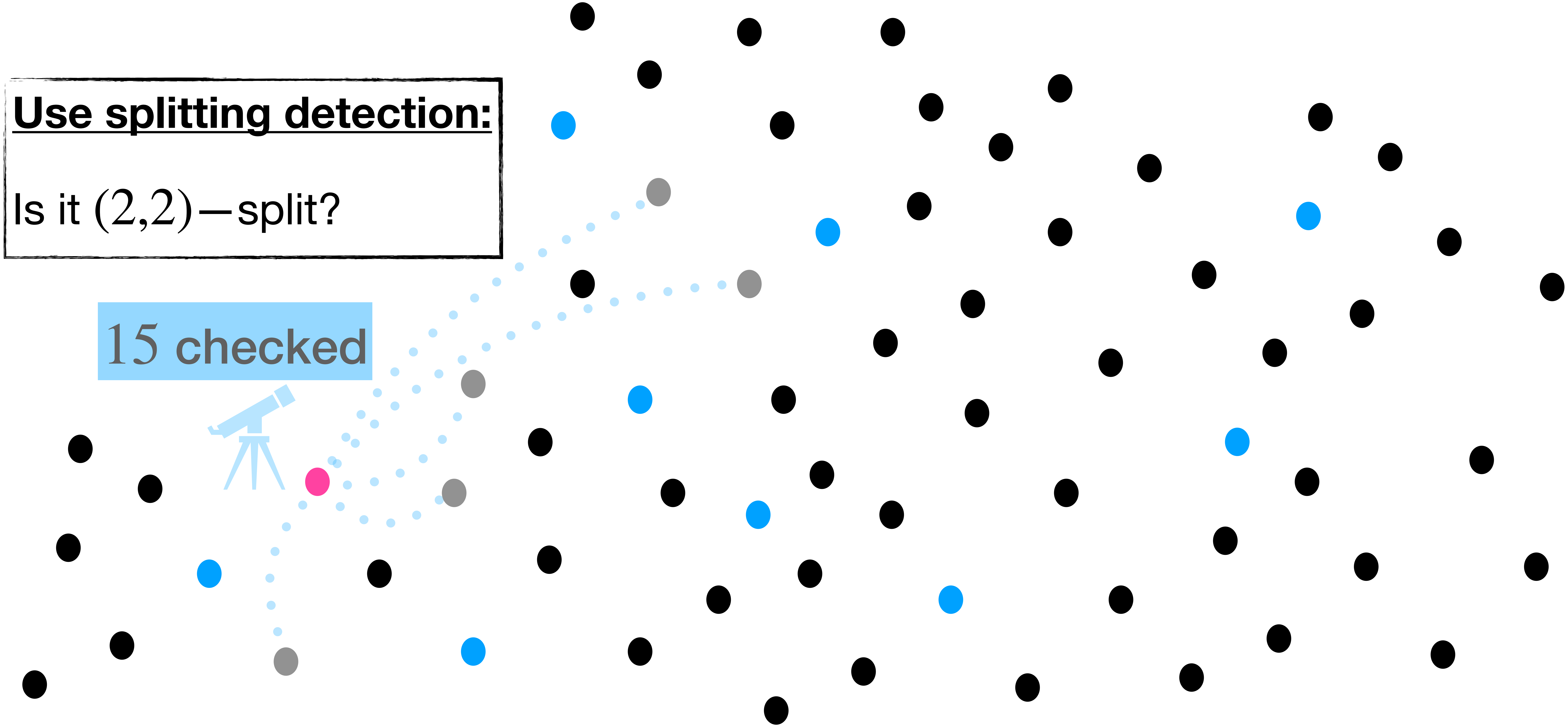
Detect if any (N, N)—isogenous neighbour is $E \times E'$ in one go!

(N, N)—split

Accelerated Costello—Smith Algorithm

Use splitting detection:

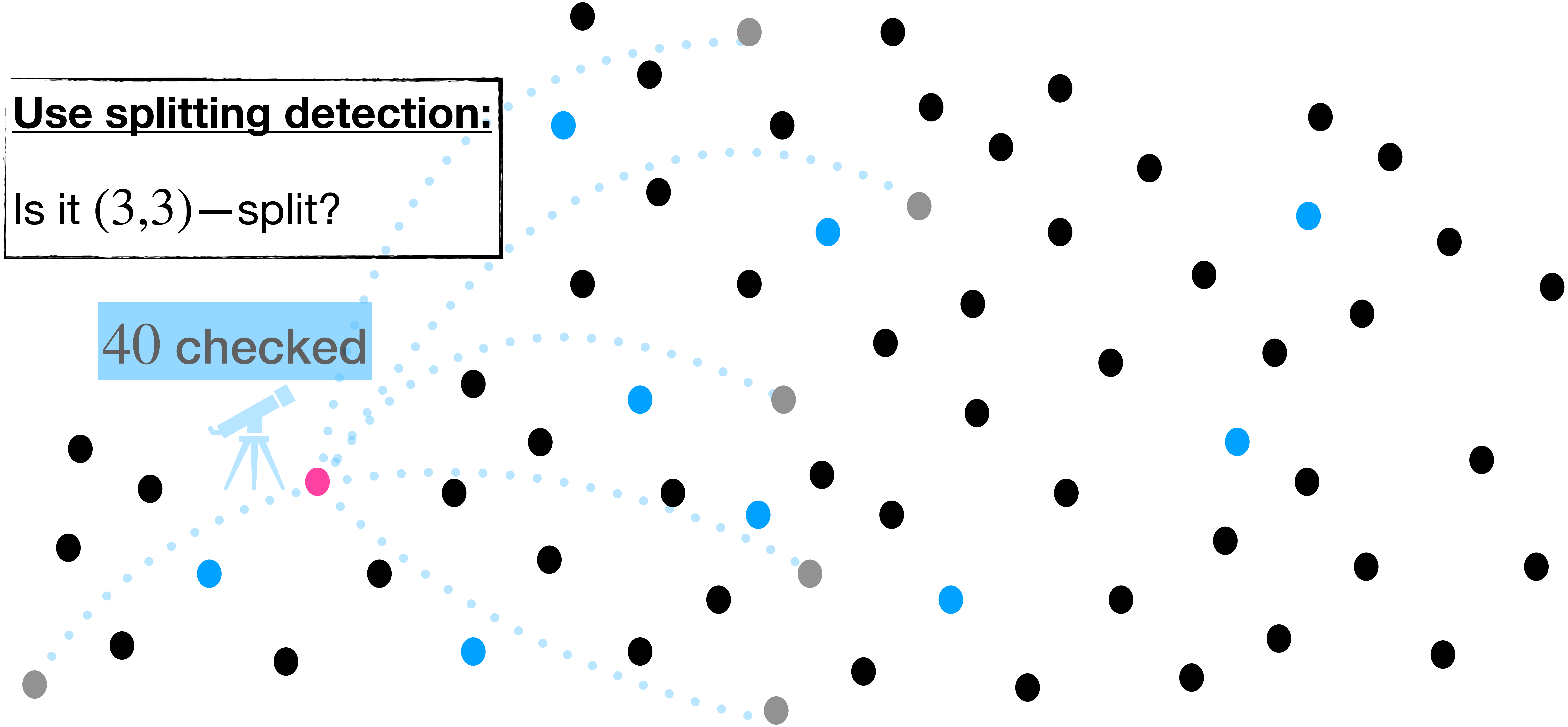
Is it $(2,2)$—split?



Accelerated Costello—Smith Algorithm

Use splitting detection:

Is it $(3,3)$—split?



Accelerated Costello—Smith Algorithm

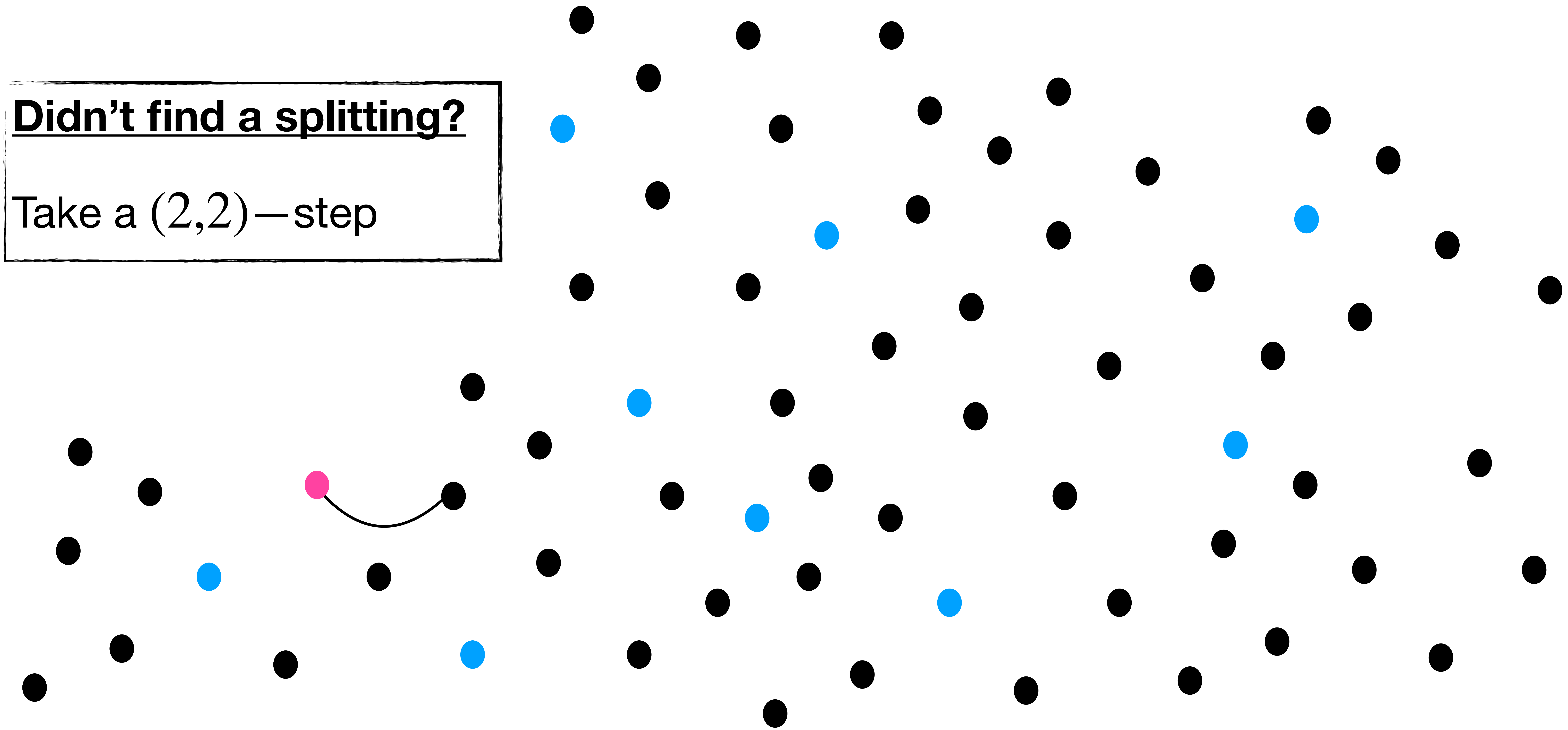
Etc, etc, etc, for appropriate N

Appropriate is an interesting question. The bigger the telescope the costlier it will be to build

Accelerated Costello—Smith Algorithm

Didn't find a splitting?

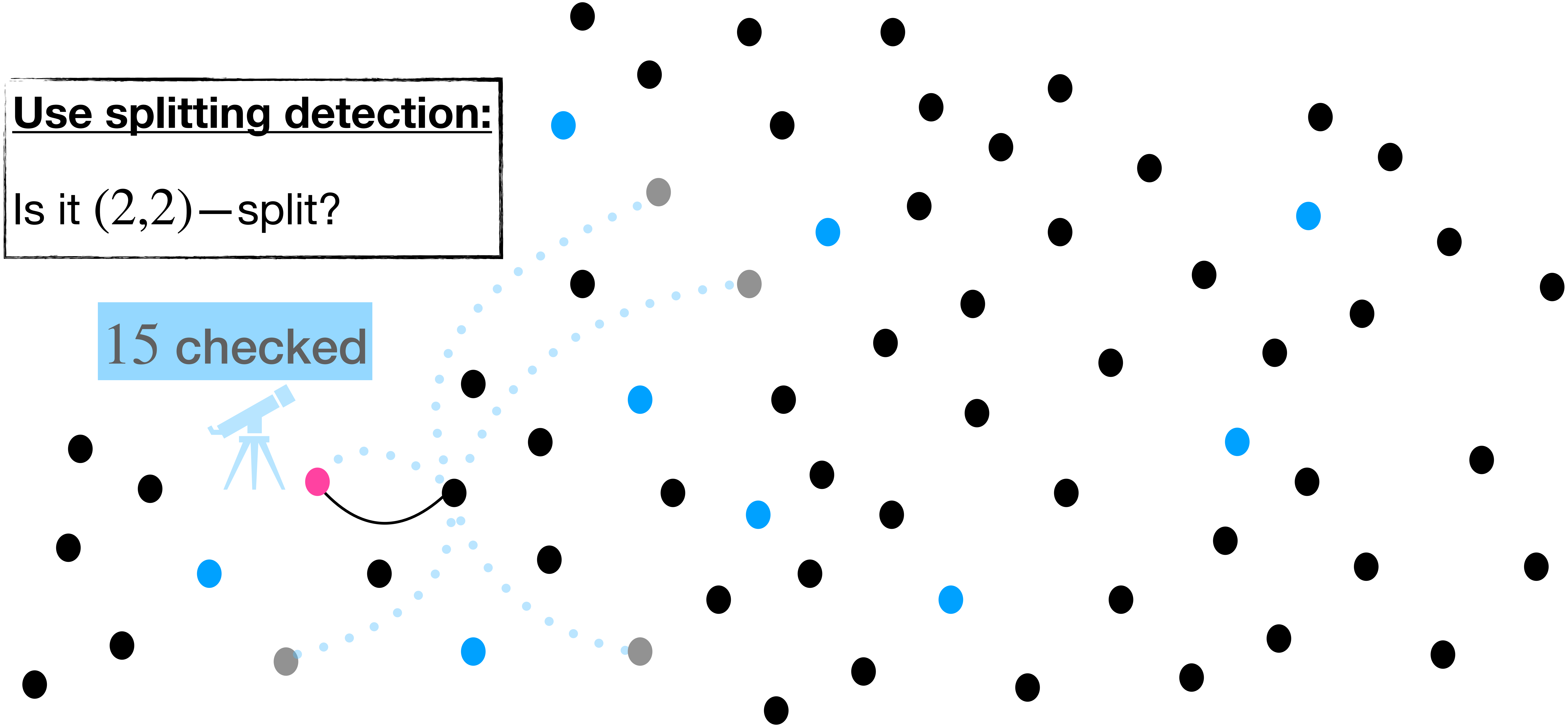
Take a $(2,2)$—step



Accelerated Costello—Smith Algorithm

Use splitting detection:

Is it $(2,2)$—split?

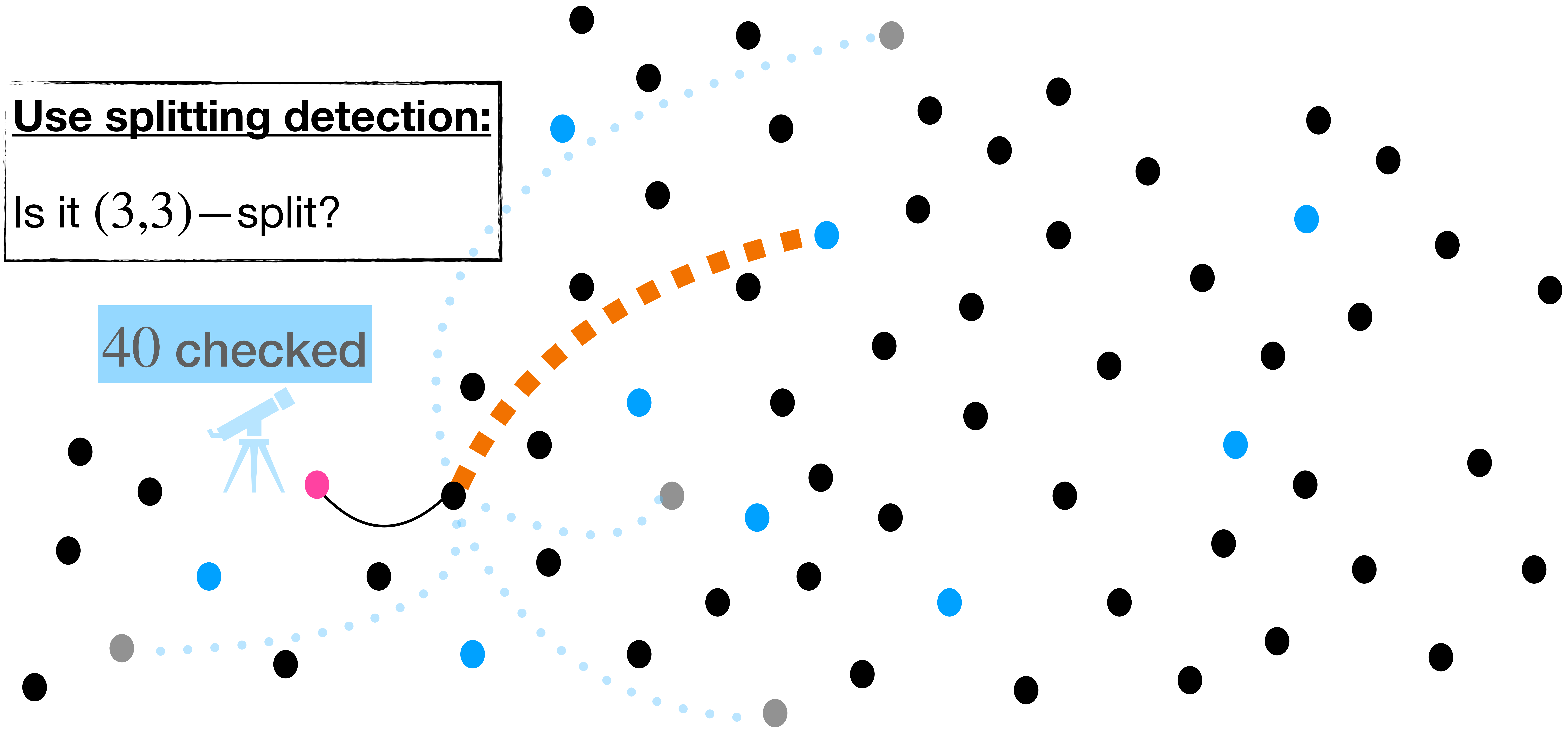


Accelerated Costello—Smith Algorithm

Use splitting detection:

Is it $(3,3)$—split?

40 checked



Detecting $(N, N)-$splittings

Detecting (N, N)—splittings

Detect if $\mathrm{Jac}(C)$ is (N, N)—split.

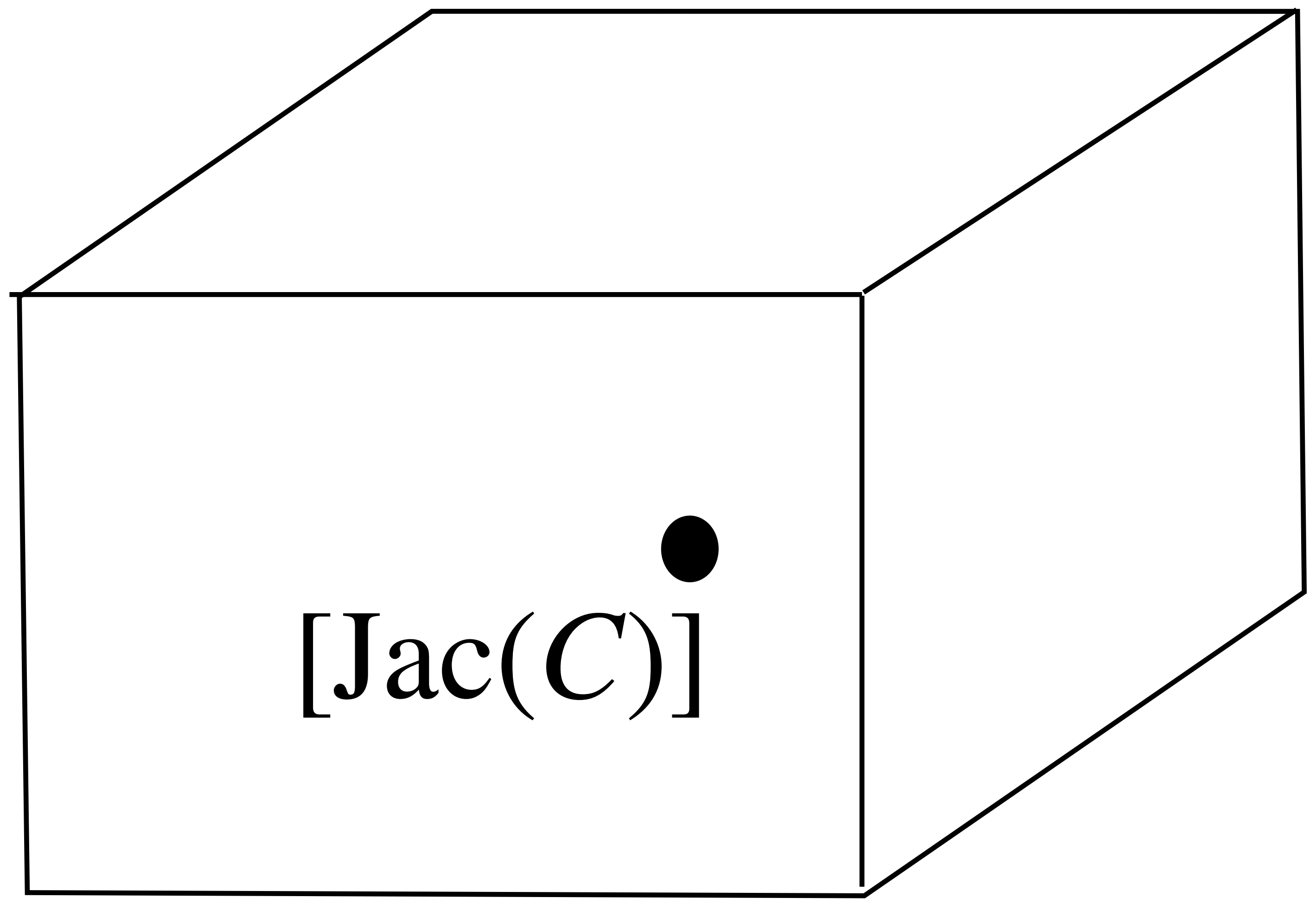
Fact 1. There exist 3 (normalised) "Igusa—Clebsch invariants" $j_1(C), j_2(C), j_3(C)$ which uniquely determine isomorphism classes $[\mathrm{Jac}(C)]$.

Like the j-invariant these are a few multiplications to compute

Detecting (N, N)—splittings

Detect if $\mathrm{Jac}(C)$ is (N, N)—split.

<u>Fact 1</u>. There exist 3 (normalised) "Igusa—Clebsch invariants" $j_1(C), j_2(C), j_3(C)$ which uniquely determine isomorphism classes $[\mathrm{Jac}(C)]$.

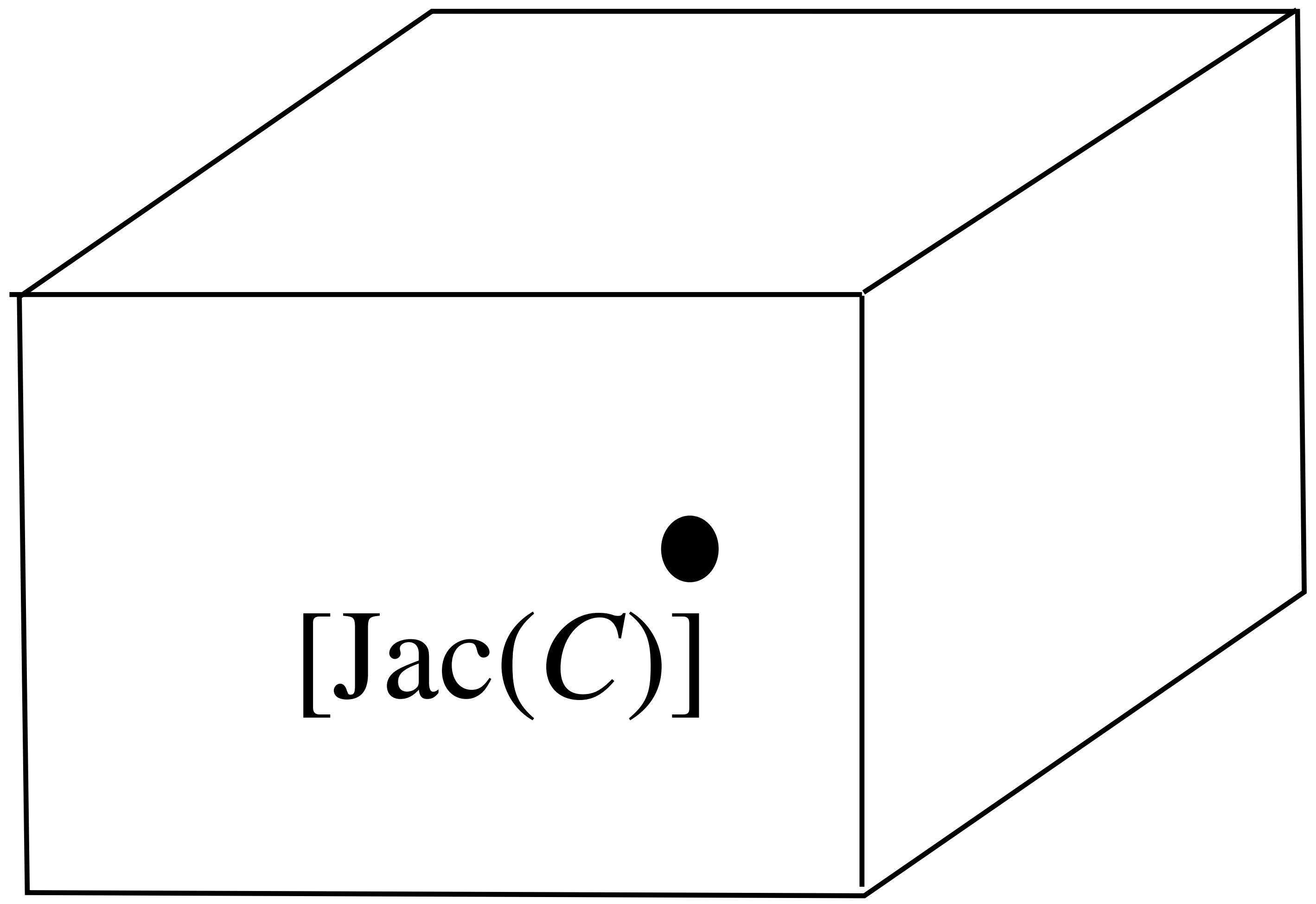


$\mathscr{A}_2 \approx$ {p.p. ab. surfaces}$/\sim$

Detecting (N, N)—splittings

Detect if $\mathrm{Jac}(C)$ is (N, N)—split.

Fact 2. There exists a "Humbert surface" $\mathscr{H}(N^2) \subset \mathscr{A}_2$ such that $\mathrm{Jac}(C)$ is (N, N)—split if and only if the point $[\mathrm{Jac}(C)] \in \mathscr{H}(N^2) \subset \mathscr{A}_2$.

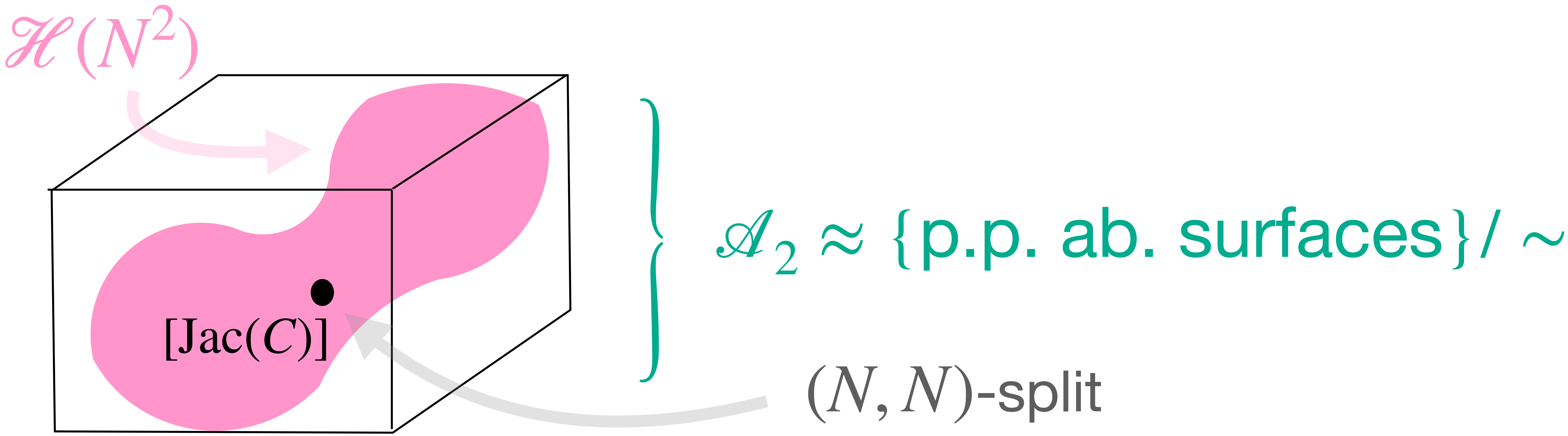


$\mathscr{A}_2 \approx$ {p.p. ab. surfaces}$/ \sim$

Detecting (N, N)—splittings

Detect if $\mathrm{Jac}(C)$ is (N, N)—split.

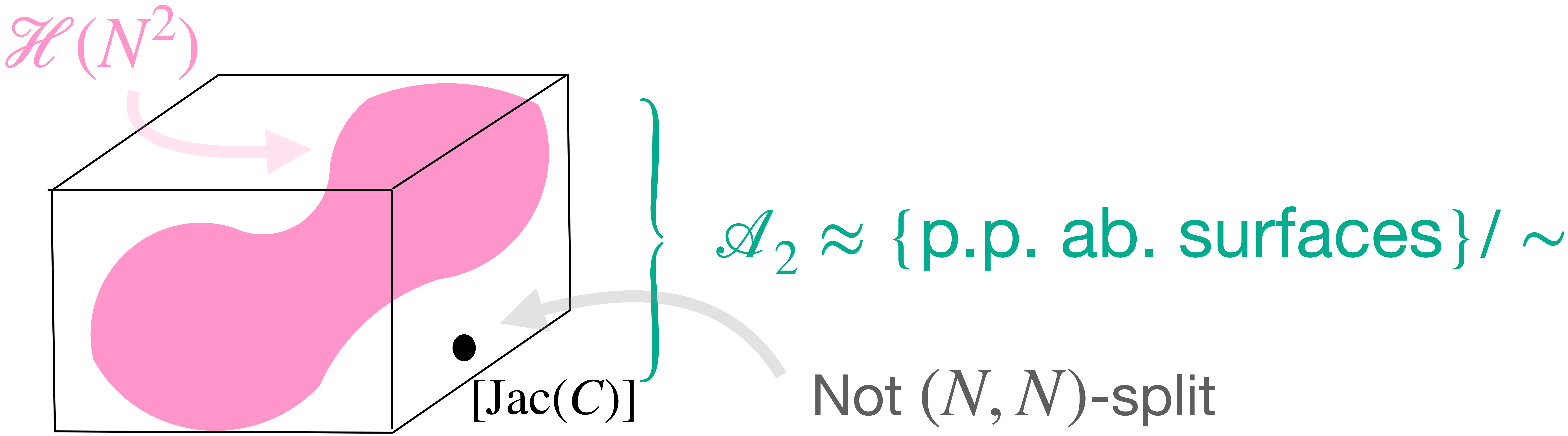
Fact 2. There exists a "Humbert surface" $\mathscr{H}(N^2) \subset \mathscr{A}_2$ such that $\mathrm{Jac}(C)$ is (N, N)—split if and only if the point $[\mathrm{Jac}(C)] \in \mathscr{H}(N^2) \subset \mathscr{A}_2$.



Detecting (N, N)—splittings

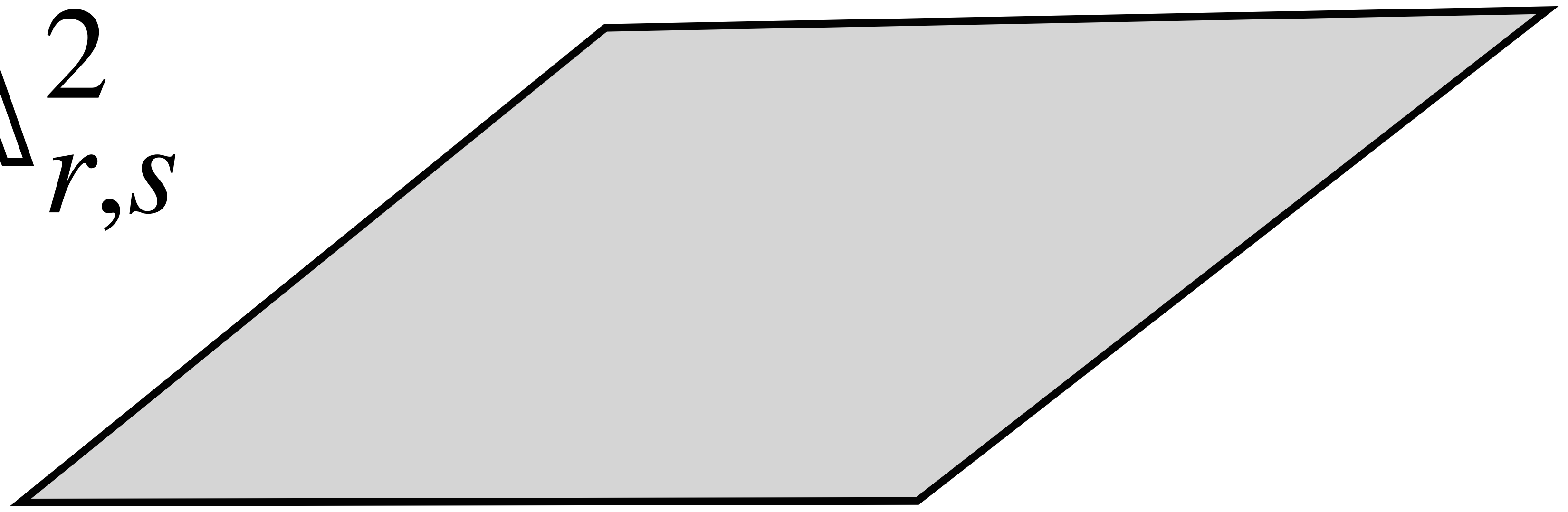
Detect if $\mathrm{Jac}(C)$ is (N, N)—split.

Fact 2. There exists a "Humbert surface" $\mathscr{H}(N^2) \subset \mathscr{A}_2$ such that $\mathrm{Jac}(C)$ is (N, N)—split if and only if the point $[\mathrm{Jac}(C)] \in \mathscr{H}(N^2) \subset \mathscr{A}_2$.



Detecting (N, N)—splittings

$\mathbb{A}^2_{r,s}$

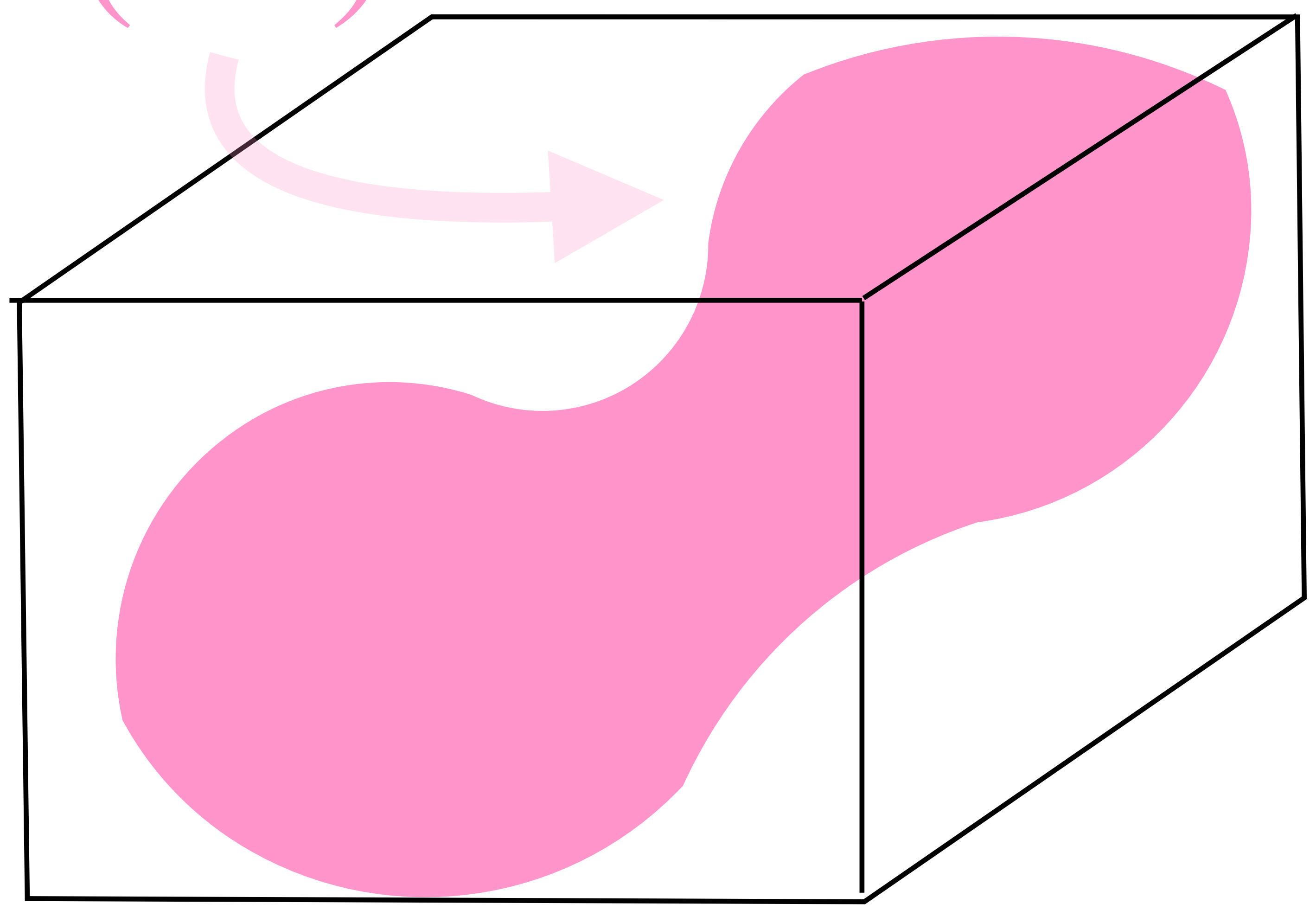


Theorem (Kumar). For $N \leq 11$

$$\varphi_{N^2} = (\alpha_1, \alpha_2, \alpha_3)$$

Explicit polynomials!

$\mathscr{H}(N^2)$



$\mathscr{A}_2 \approx \{\text{p.p. ab. surfaces}\}/\sim$

Detecting (N, N)—splittings

Approach:

Jac(C) is (N, N)—split $\Leftrightarrow \exists r, s \in \bar{\mathbb{F}}_p$ such that

$$\alpha_1(r,s) = j_1(C) \quad \text{and} \quad \alpha_2(r,s) = j_2(C) \quad \text{and} \quad \alpha_3(r,s) = j_3(C)$$

Only a handful of multiplications for small N

Check if there is a solution to the equations

$$\alpha_1(r,s) - j_1(C) = 0$$
$$\alpha_2(r,s) - j_2(C) = 0$$
$$\alpha_3(r,s) - j_3(C) = 0$$

Use techniques like resultants, polynomial gcd

What's the speed-up?

Speed-up

N	Total $\#\mathbb{F}_p$ mults.	Total $\#\mathbb{F}_p$ mults. per node revealed
2	175	12.5
3	767	19.2
4	4882	46.9
5	18818	120.6
6	29188	52.1
7	182641	456.6
8	325606	395.2
9	582474	539.3
10	1082007	495.4
11	3237198	2211.2

Cost of a $(2,2)$—step

p (bits)	$\mathbb{F}_p$-mults. per node
50	579
100	1176
150	1575
⋮	⋮
950	9772
1000	11346

Speed-up

	Walks in $\Gamma_2(2;p)$ without additional searching [17] (optimised in Section 3)	Walks in $\Gamma_2(2;p)$ w. split searching in $\Gamma_2(N;p)$ **This work**		
p (bits)	$\mathbb{F}_p$-mults. per node	set $N \in \{\dots\}$	$\mathbb{F}_p$-mults. per node	**improv. factor**
50	579	$\{2,3\}$	35	**16.5x**
100	1176	$\{2,3\}$	48	**24.5x**
150	1575	$\{3,4\}$	54	**29.2x**
⋮	⋮	⋮	⋮	⋮
950	9772	$\{4,6\}$	69	**141.6x**
1000	11346	$\{4,6\}$	71	**159.8x**

Further work

Endomorphisms

Humbert surfaces exist for discriminants all discriminants D and parametrise abelian surfaces with an endomorphism of degree D. The same techniques work!

Question. If you know that A_1 and A_2 endomorphisms of small degree, can you give an algorithm better than the $\widetilde{O}(p)$ Costello—Smith algorithm to solve the superspecial isogeny problem?