

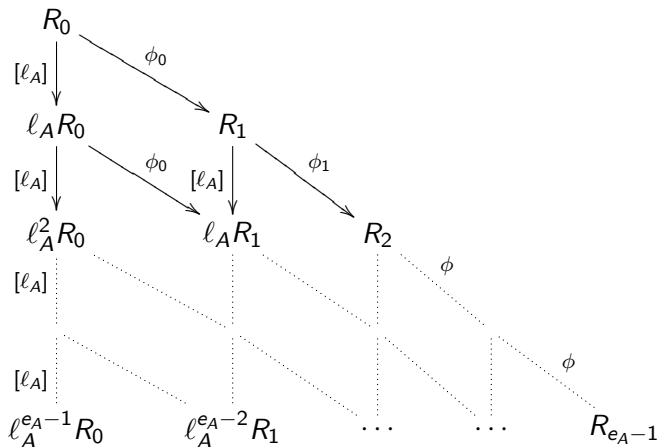
Faster isogenies in a quantum world

Luca De Feo and Jérôme Plût

Université de Versailles

September 19, 2011

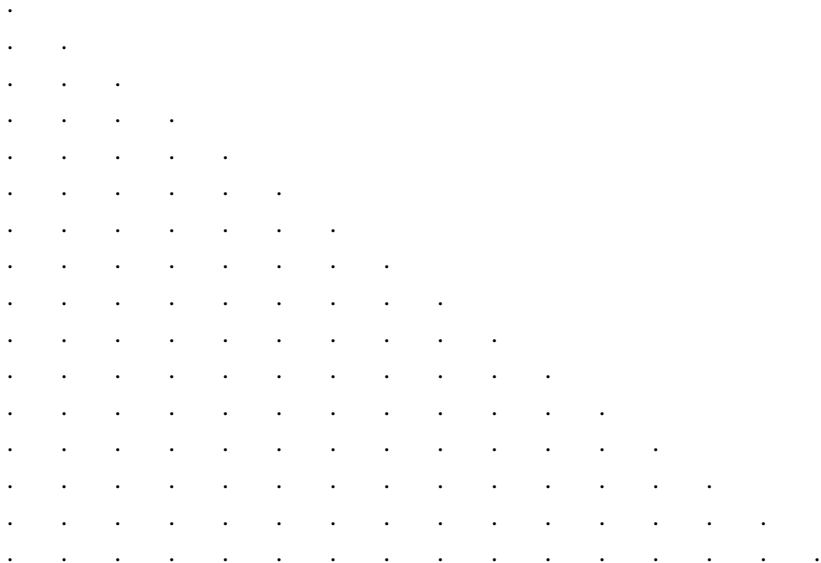
Computational strategies



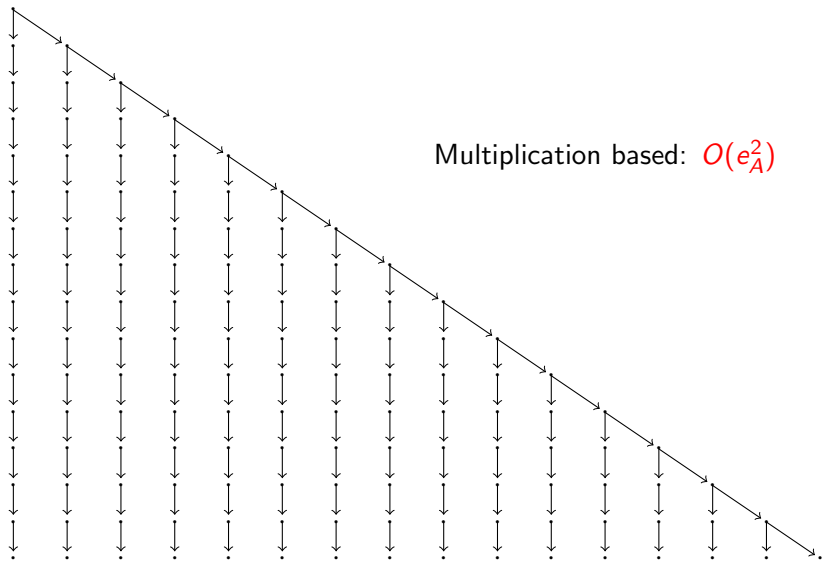
The outer edges are always needed. For the inner nodes, one can:

- ▶ Compute *vertical* arrows (multiplication-based strategy)
- ▶ Compute *diagonal* arrows (isogeny-based strategy)

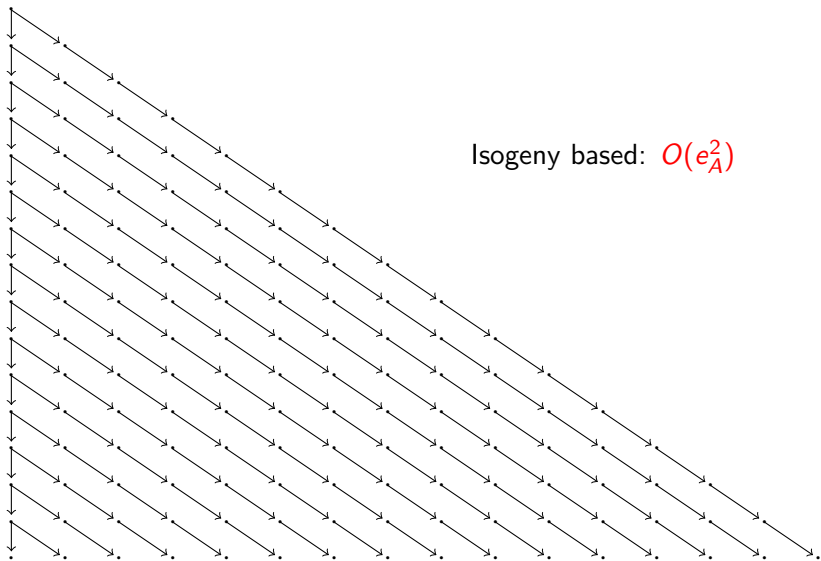
Navigating the triangle



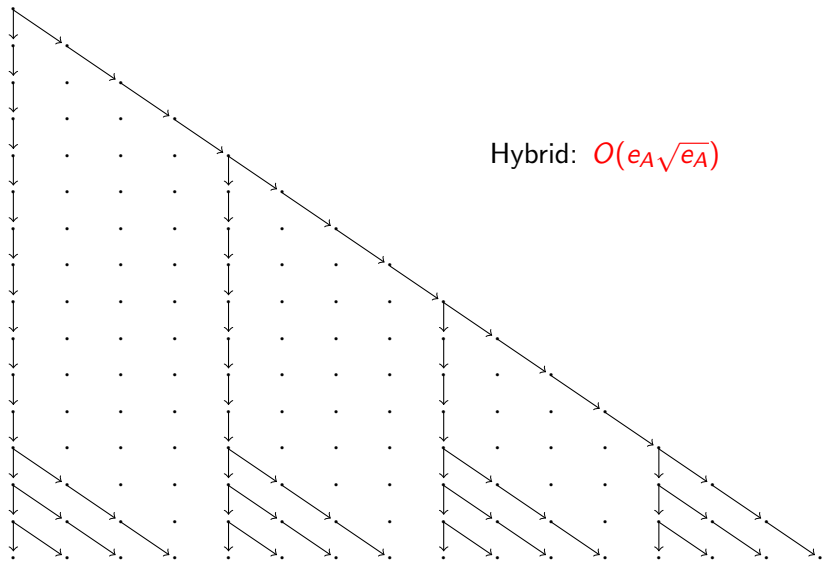
Navigating the triangle



Navigating the triangle



Navigating the triangle



Navigating the triangle

