A new post-quantum digital signature scheme

Chloe Martindale

University of Bristol

SIAM-AG TU/e
14th July, 2023

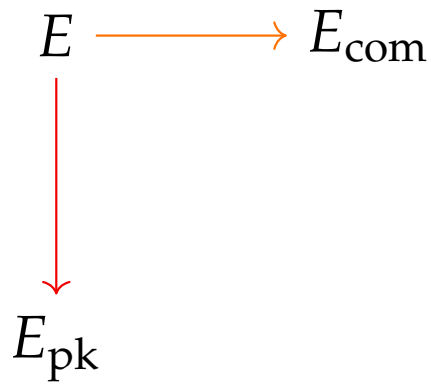
joint work (in progress) with Ross Bowden

Concept: Let's take the Q out of SQISign

public, secret, commitment, challenge, response

1

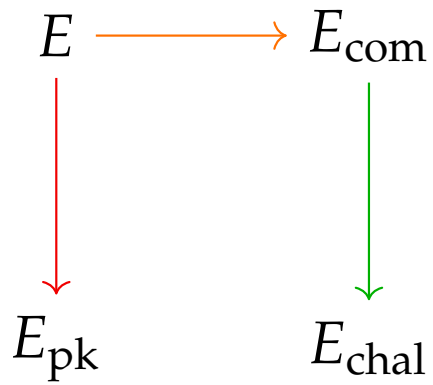
Concept: Let's take the Q out of SQISign



public, secret, commitment, challenge, response

1

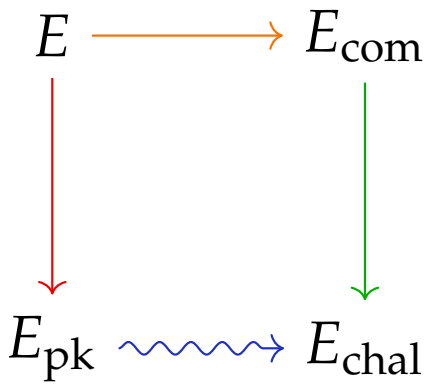
Concept: Let's take the Q out of SQISign



public, secret, commitment, challenge, response

1

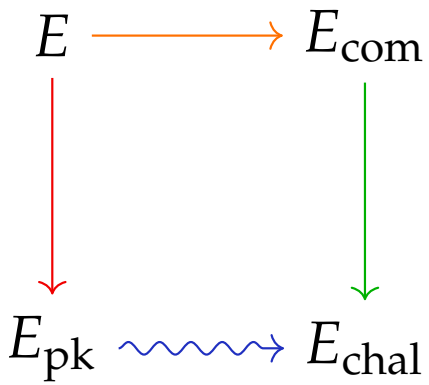
Concept: Let's take the Q out of SQISign



public, secret, commitment, challenge, response

1

Concept: Let's take the Q out of SQISign

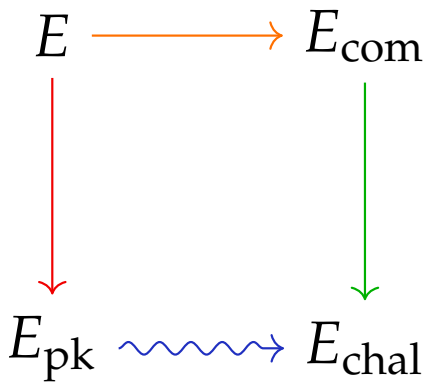


public, secret, commitment, challenge, response

- Bottleneck: response requires
  - Computing $\mathrm{End}(E_{\text{chal}})$
  - KLPT

1

Concept: Let's take the Q out of SQISign

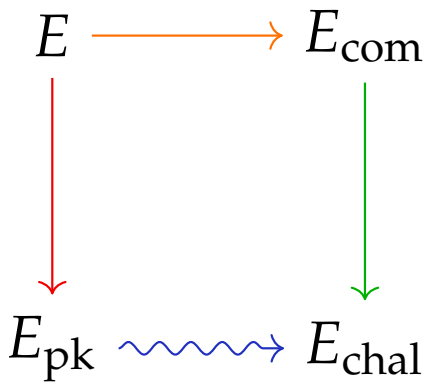


public, secret, commitment, challenge, response

- Bottleneck: response requires
  - Computing $\mathrm{End}(E_{\text{chal}})$
  - KLPT
- Idea: replace
  - Computing $\mathrm{End}(E_{\text{chal}}) \rightsquigarrow$ basis change on $T_2(E_{\text{pk}})$
  - KLPT $\rightsquigarrow$ once-for-each-E_{pk} computation[1]

[1] Hopefully. Work in progress, remember?

Concept: Let's take the Q out of SQISign



public, secret, commitment, challenge, response

- Bottleneck: response requires
  - Computing $\mathrm{End}(E_{\text{chal}})$
  - KLPT
- Idea: replace
  - Computing $\mathrm{End}(E_{\text{chal}}) \rightsquigarrow$ basis change on $T_2(E_{\text{pk}})$
  - KLPT $\rightsquigarrow$ once-for-each-E_{pk} computation[1]

How?!

[1] Hopefully. Work in progress, remember?

How: Bruhat-Tits trees and isogeny graphs

Quaternion Algebra graphs

Nodes:
Maximal orders / $\sim$

Edges:
Ideals of norm 2 / $\sim$

Supersingular isogeny graphs

Nodes:
j-invariants

Edges:
2-isogenies / $\sim$

Quotients of Bruhat-Tits trees

How: Bruhat-Tits trees and isogeny graphs

Quaternion Algebra graphs

Nodes:
Maximal orders / $\sim$

Edges:
Ideals of norm 2 / $\sim$

Supersingular isogeny graphs

Nodes:
j-invariants

Edges:
2-isogenies / $\sim$

Quotients of Bruhat-Tits trees

Nodes:

$$\left\{ \begin{pmatrix} 2^n & 0 \\ r & 2^m \end{pmatrix} : 0 \leq r < 2^m \right\} / \sim$$

Edges:

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

act on nodes via multiplication.

How: Bruhat-Tits trees and isogeny graphs

SIGs

Nodes:

j-invariants

Edges:

2-isogenies

(Quotients of)
Bruhat-Tits trees

Nodes:

$$\begin{pmatrix} 2^n & 0 \\ r & 2^m \end{pmatrix}_{0 \le r < 2^m} / \sim$$

Edges:

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{label}=\infty,$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \quad \text{label}=1,$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \quad \text{label}=0$$

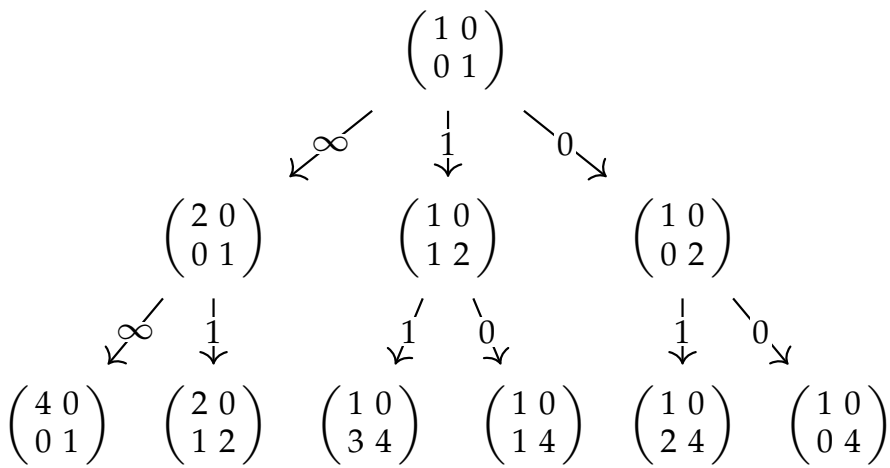
How: Bruhat-Tits trees and isogeny graphs

SIGs

Nodes:
j-invariants

Edges:
2-isogenies

1. Choose root of tree E_{pk}
   and basis $\{P, Q\}$ of $T_2(E_{\text{pk}})$.



(Quotients of)
Bruhat-Tits trees

Nodes:

$$\begin{pmatrix} 2^n & 0 \\ r & 2^m \end{pmatrix}_{0 \le r < 2^m} / \sim$$

Edges:

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{label}=\infty,$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \quad \text{label}=1,$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \quad \text{label}=0$$

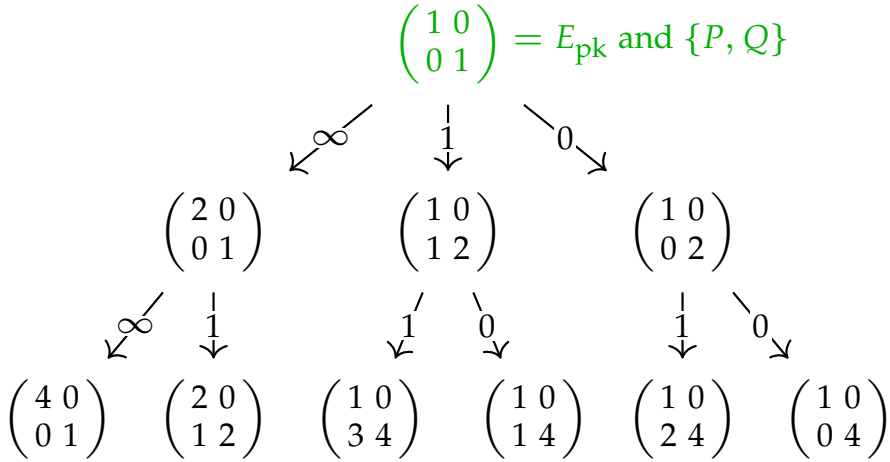
How: Bruhat-Tits trees and isogeny graphs

SIGs

Nodes:
j-invariants

Edges:
2-isogenies

1. Choose root of tree E_{pk}
   and basis $\{P, Q\}$ of $T_2(E_{\text{pk}})$.



(Quotients of) Bruhat-Tits trees

Nodes:

$$\begin{pmatrix} 2^n & 0 \\ r & 2^m \end{pmatrix}_{0 \le r < 2^m} / \sim$$

Edges:

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{label}=\infty,$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \quad \text{label}=1,$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \quad \text{label}=0$$

How: Bruhat-Tits trees and isogeny graphs

SIGs

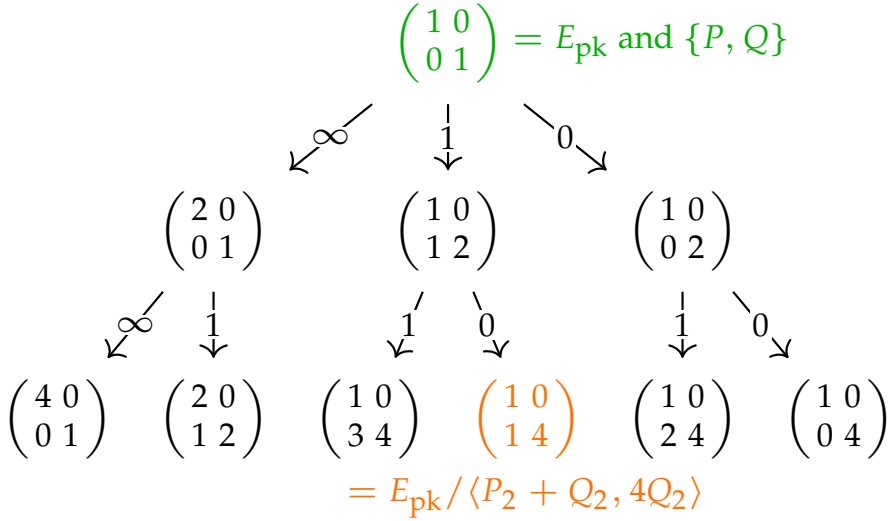
Nodes:

j-invariants

Edges:

2-isogenies

1. Choose root of tree E_{pk} and basis $\{P, Q\}$ of $T_2(E_{\text{pk}})$.
2. Call P_d, Q_d canonical lifts of P, Q that generate $E_{\text{pk}}[2^d]$.



(Quotients of) Bruhat-Tits trees

Nodes:

$$\begin{pmatrix} 2^n & 0 \\ r & 2^m \end{pmatrix}_{0 \le r < 2^m} / \sim$$

Edges:

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{label}=\infty,$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \quad \text{label}=1,$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \quad \text{label}=0$$

How: Bruhat-Tits trees and isogeny graphs

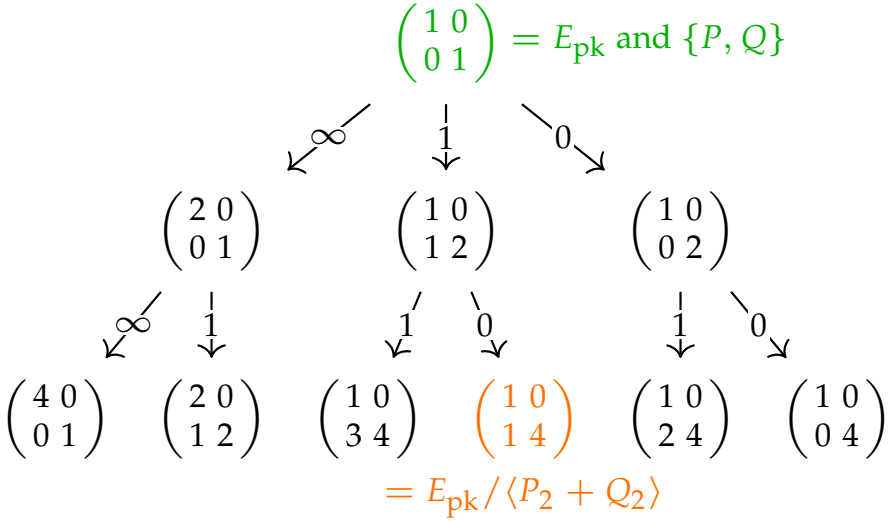
SIGs

Nodes:
j-invariants

Edges:
2-isogenies

1. Choose root of tree E_{pk} and basis $\{P, Q\}$ of $T_2(E_{\text{pk}})$.
2. Call P_d, Q_d canonical lifts of P, Q that generate $E_{\text{pk}}[2^d]$.
3. A matrix node M at depth d is

$$E_{\text{pk}}/\langle (P_d, Q_d) \cdot M \rangle.$$



(Quotients of) Bruhat-Tits trees

Nodes:

$$\begin{pmatrix} 2^n & 0 \\ r & 2^m \end{pmatrix}_{0 \le r < 2^m} / \sim$$

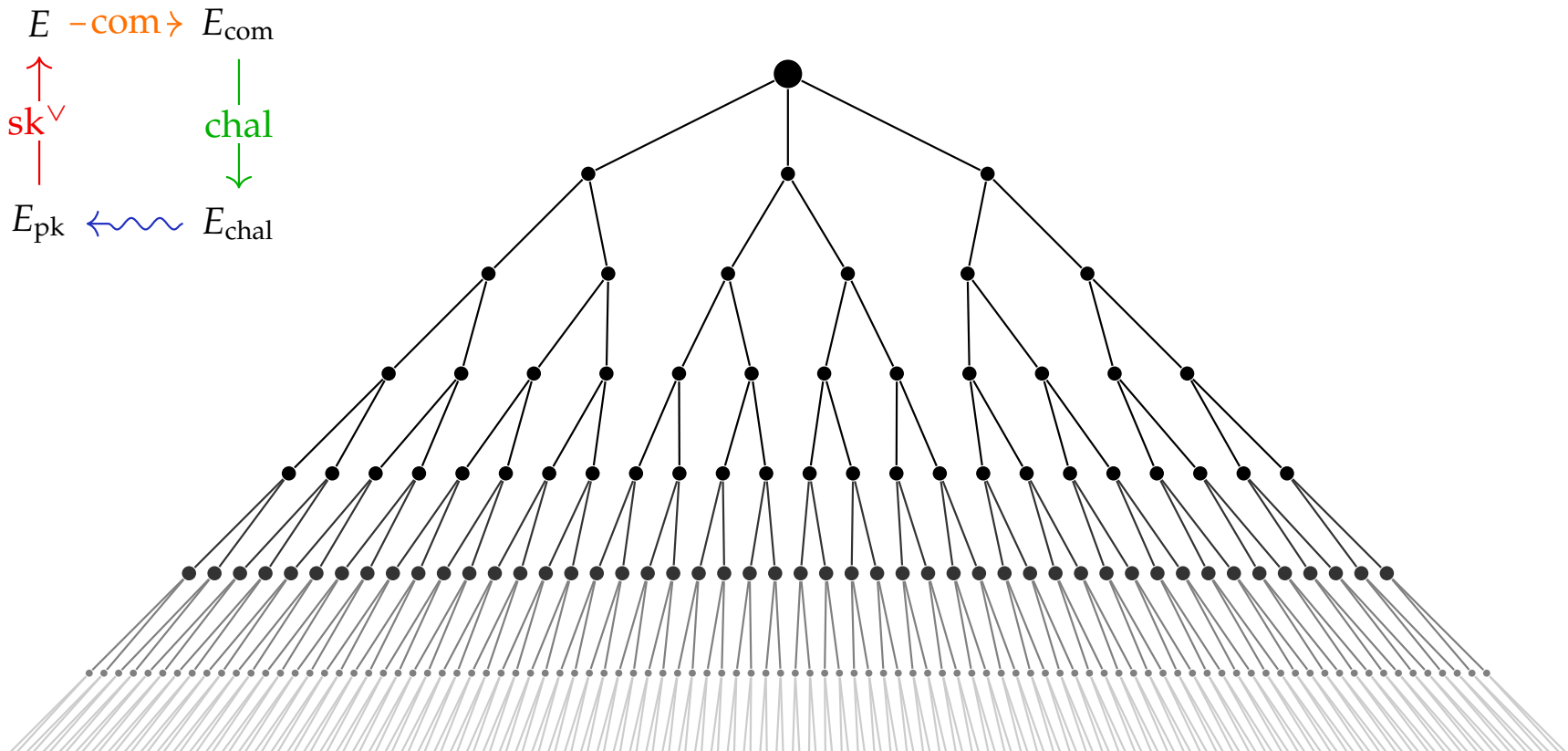
Edges:

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{label}=\infty,$$

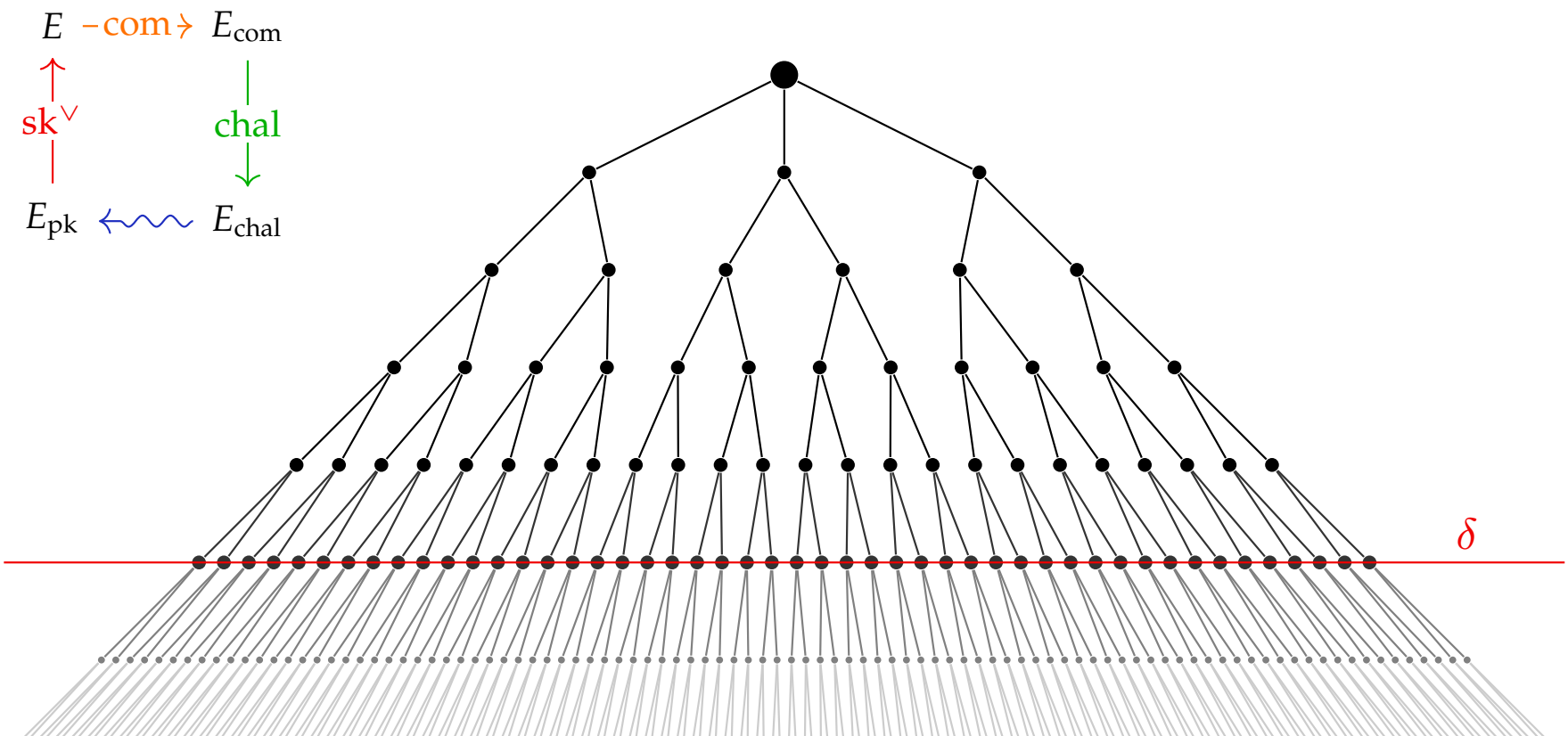
$$\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \quad \text{label}=1,$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \quad \text{label}=0$$

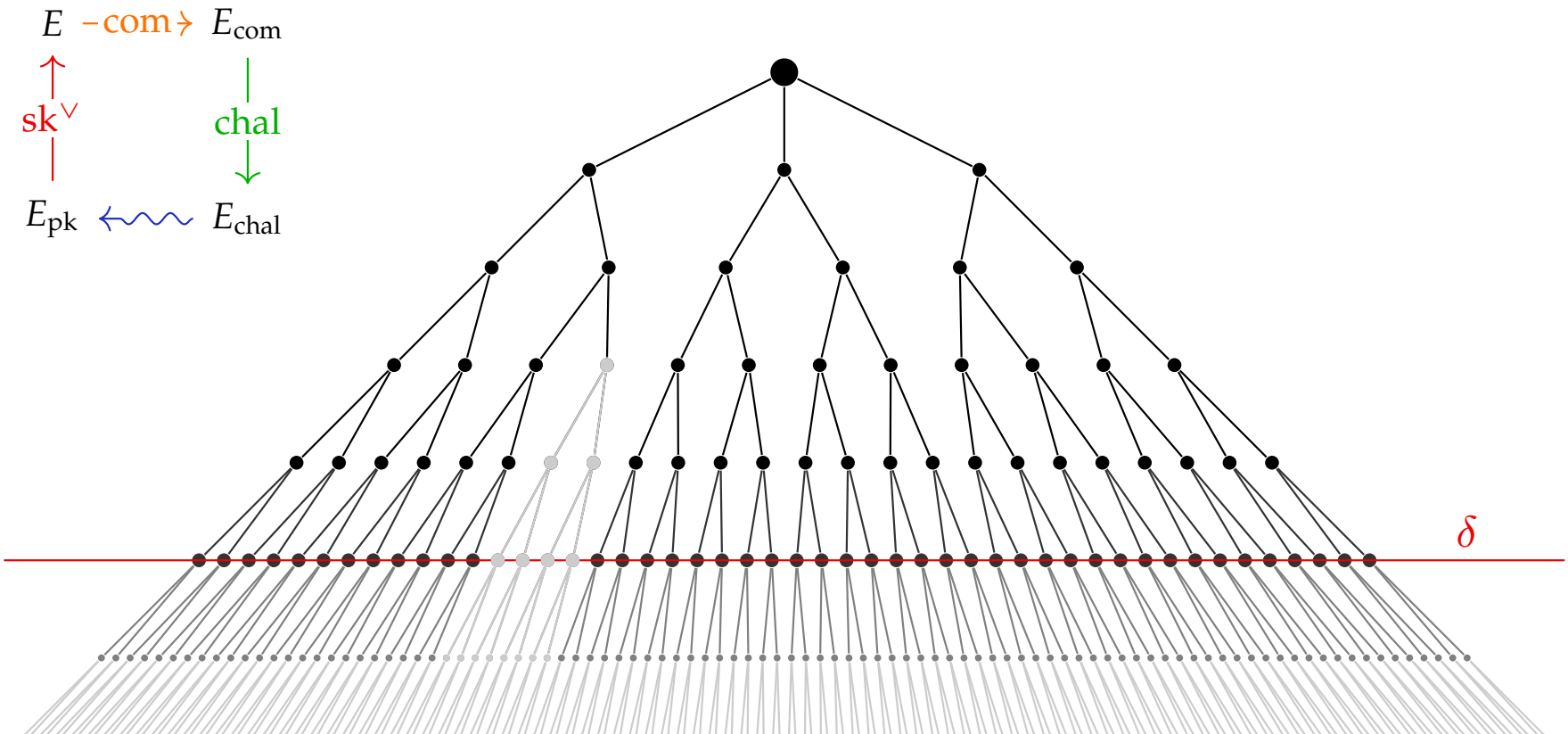
From KLPT to Bruhat-Tits quotients



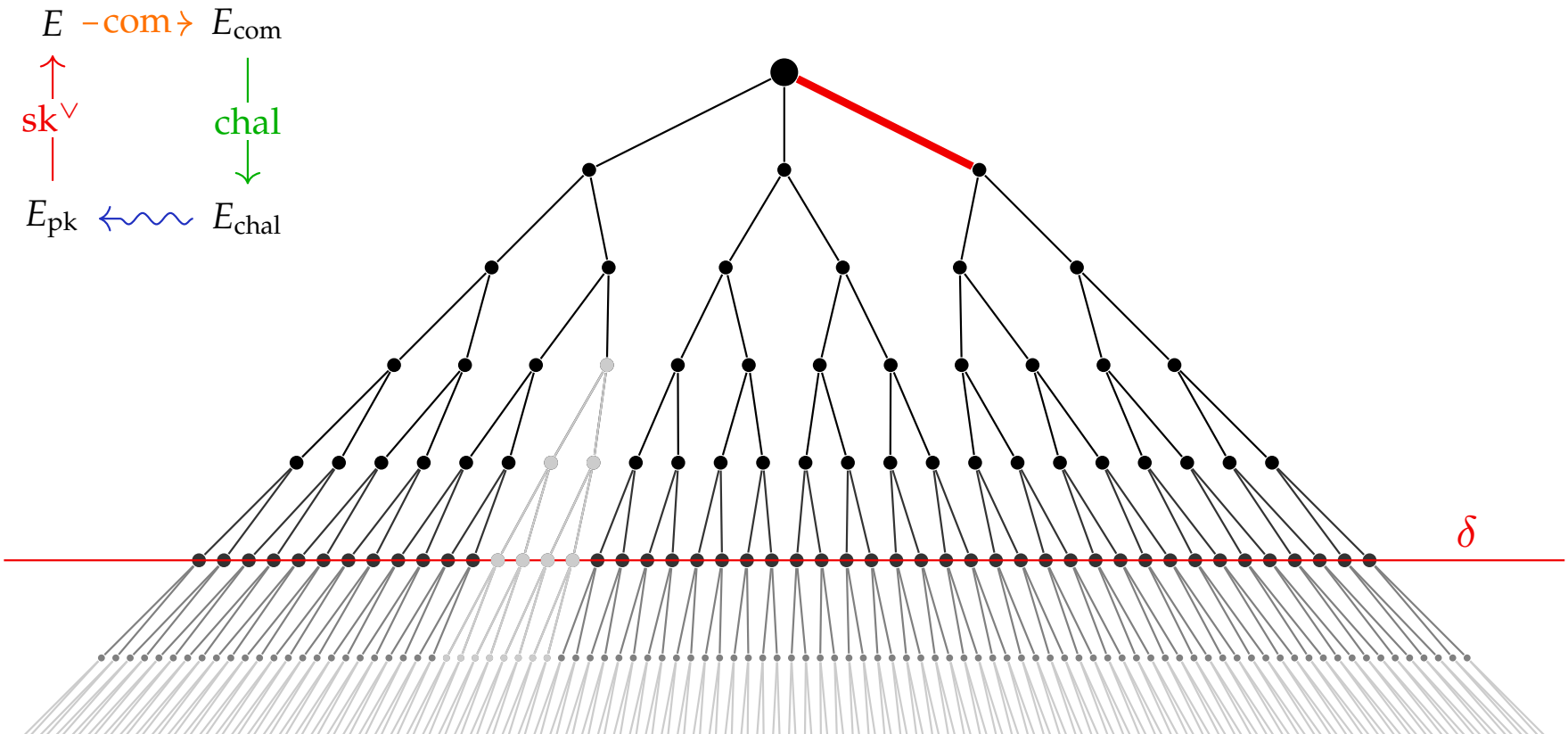
From KLPT to Bruhat-Tits quotients



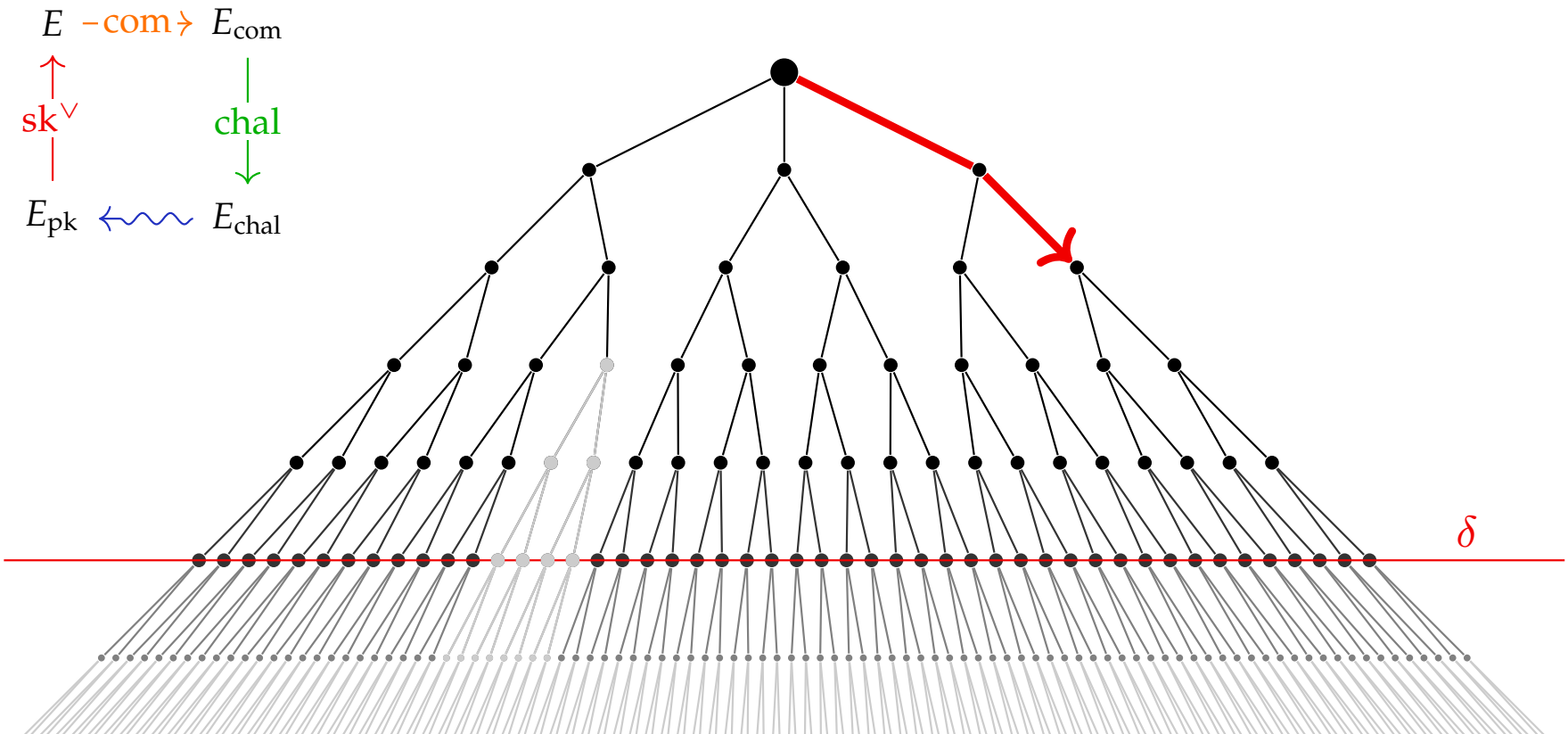
From KLPT to Bruhat-Tits quotients



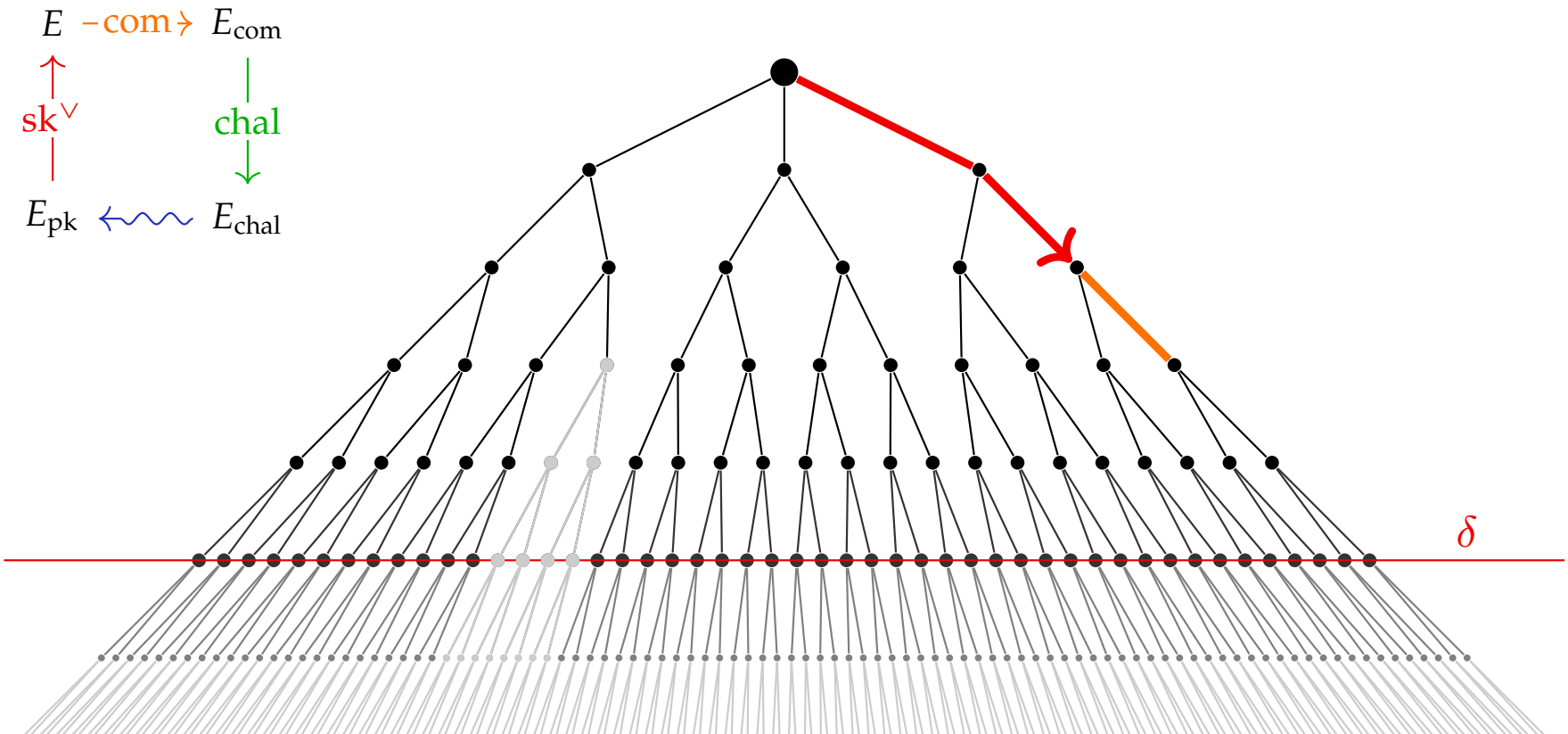
From KLPT to Bruhat-Tits quotients



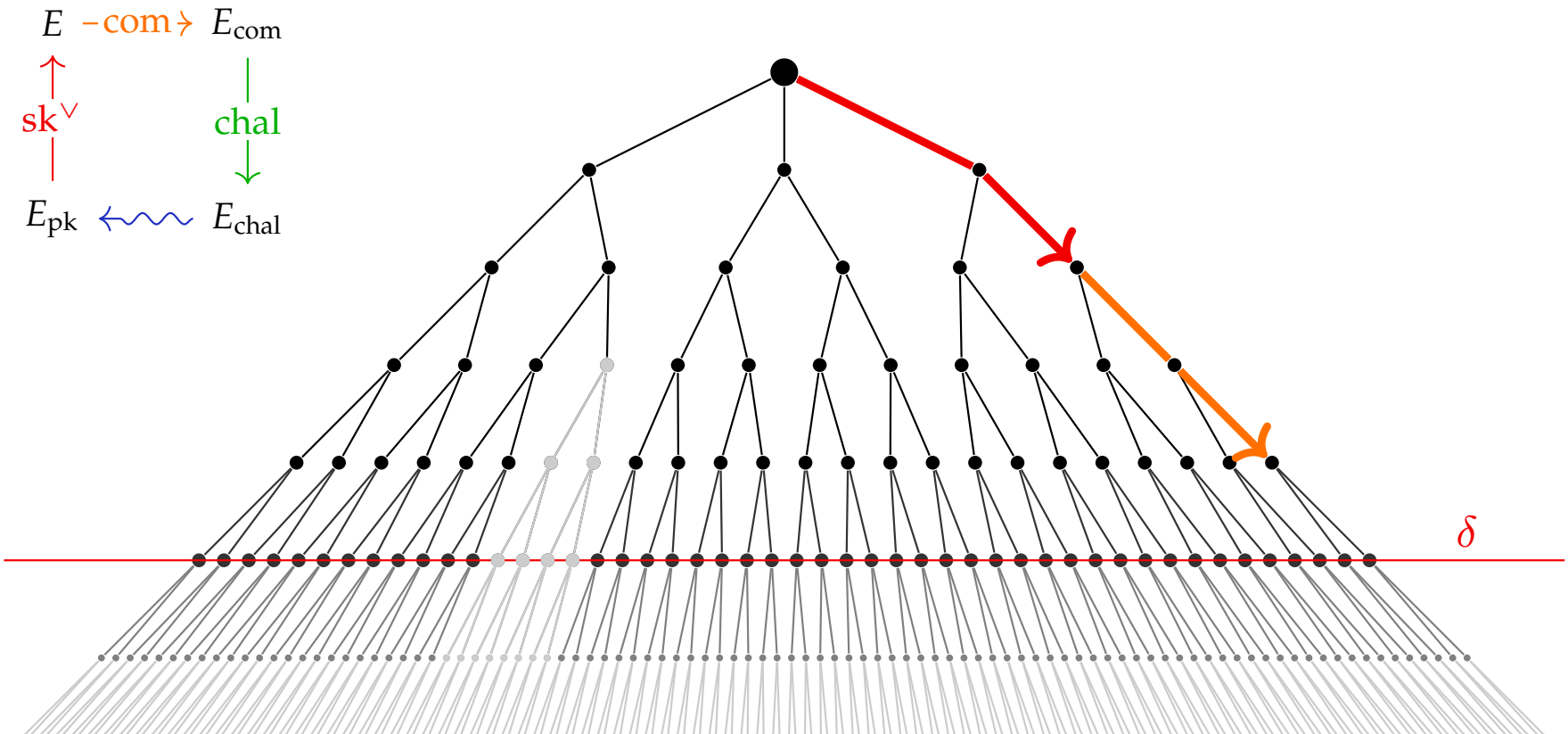
From KLPT to Bruhat-Tits quotients



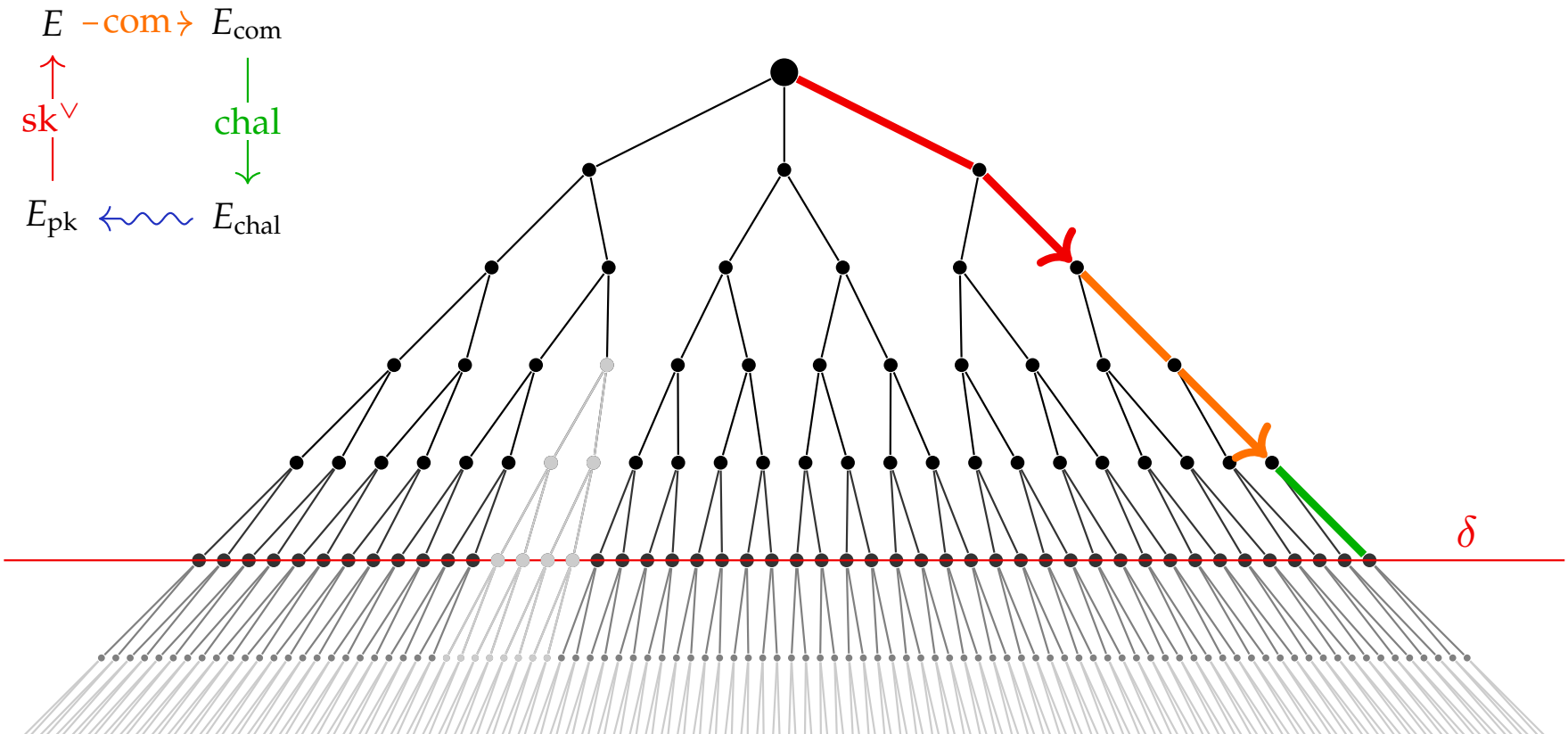
From KLPT to Bruhat-Tits quotients



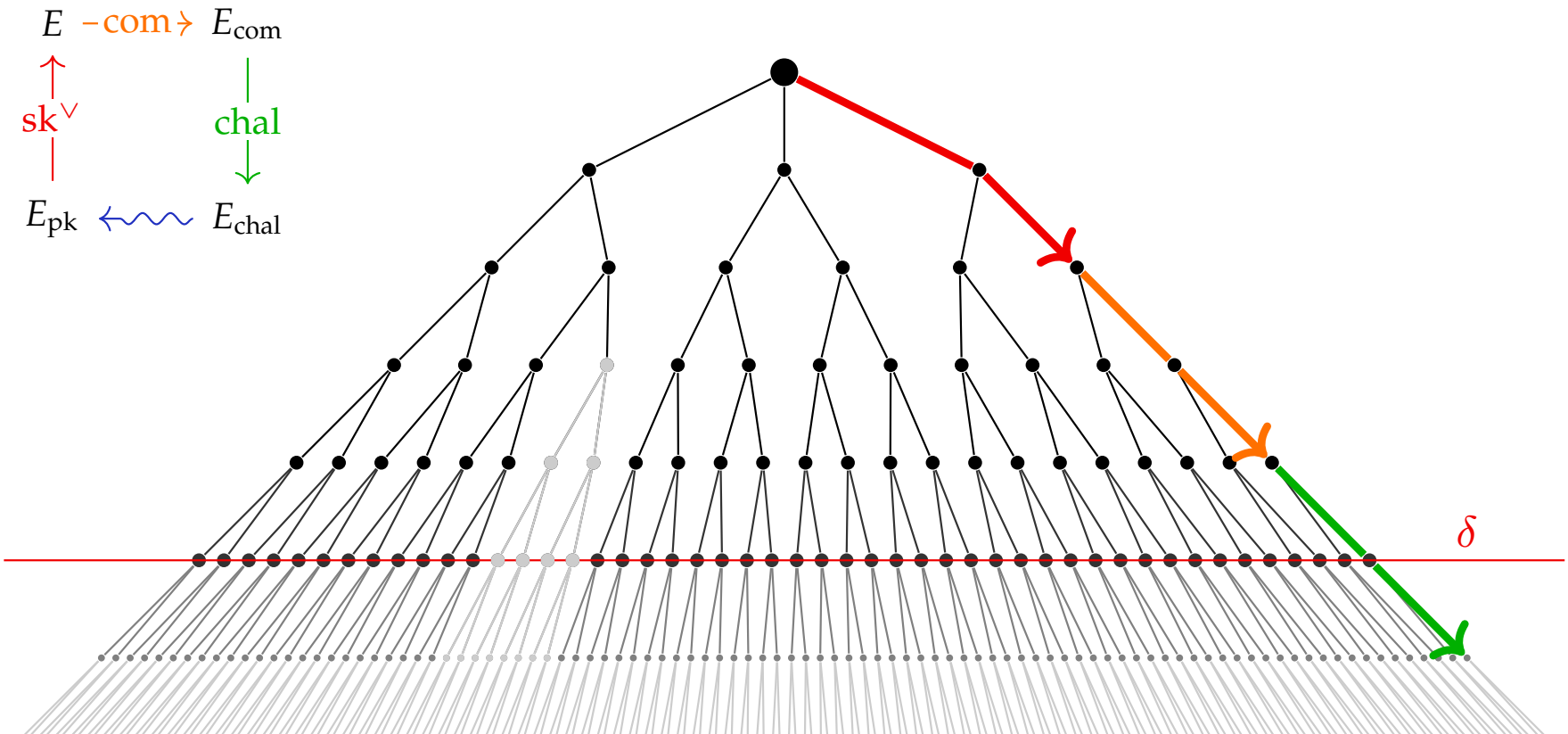
From KLPT to Bruhat-Tits quotients



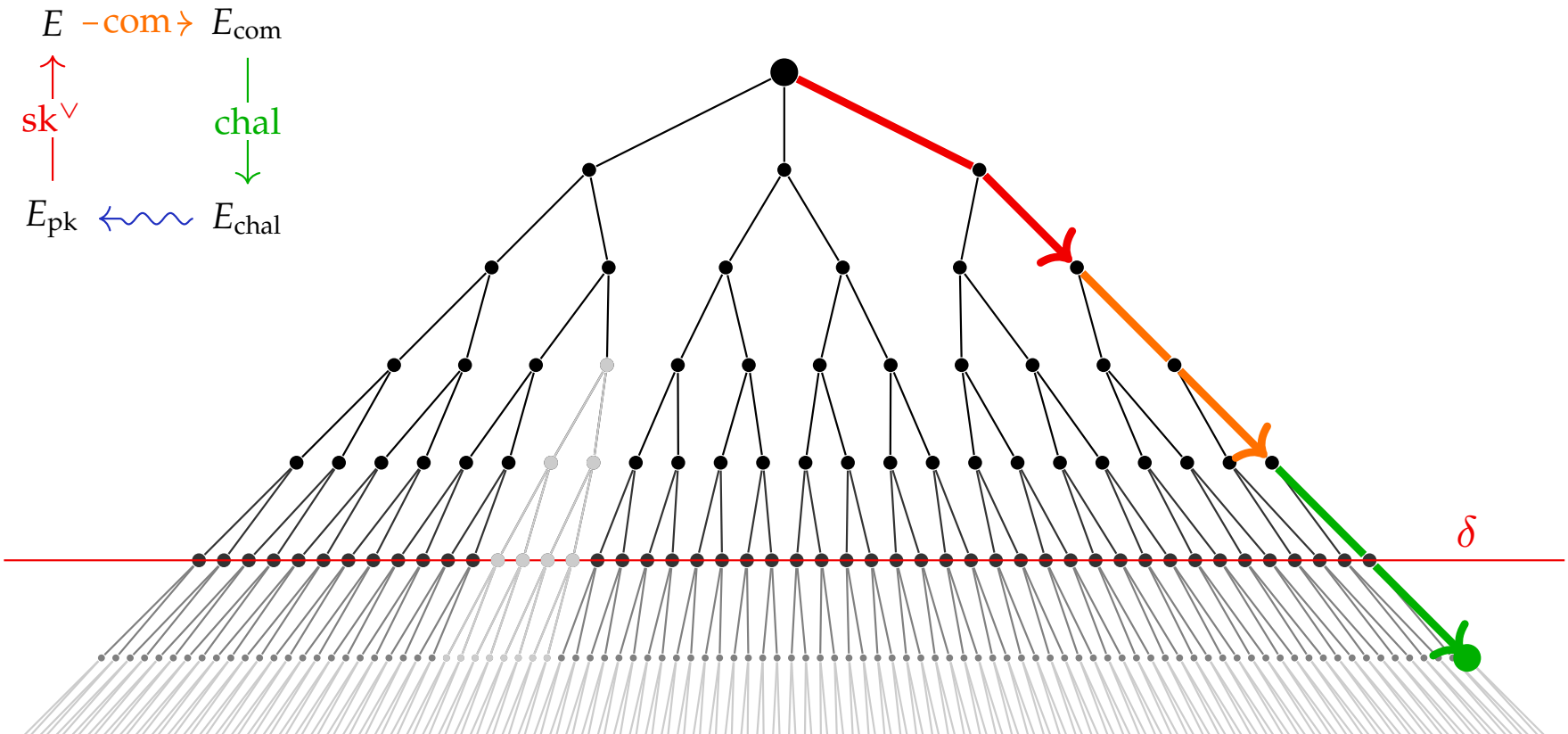
From KLPT to Bruhat-Tits quotients



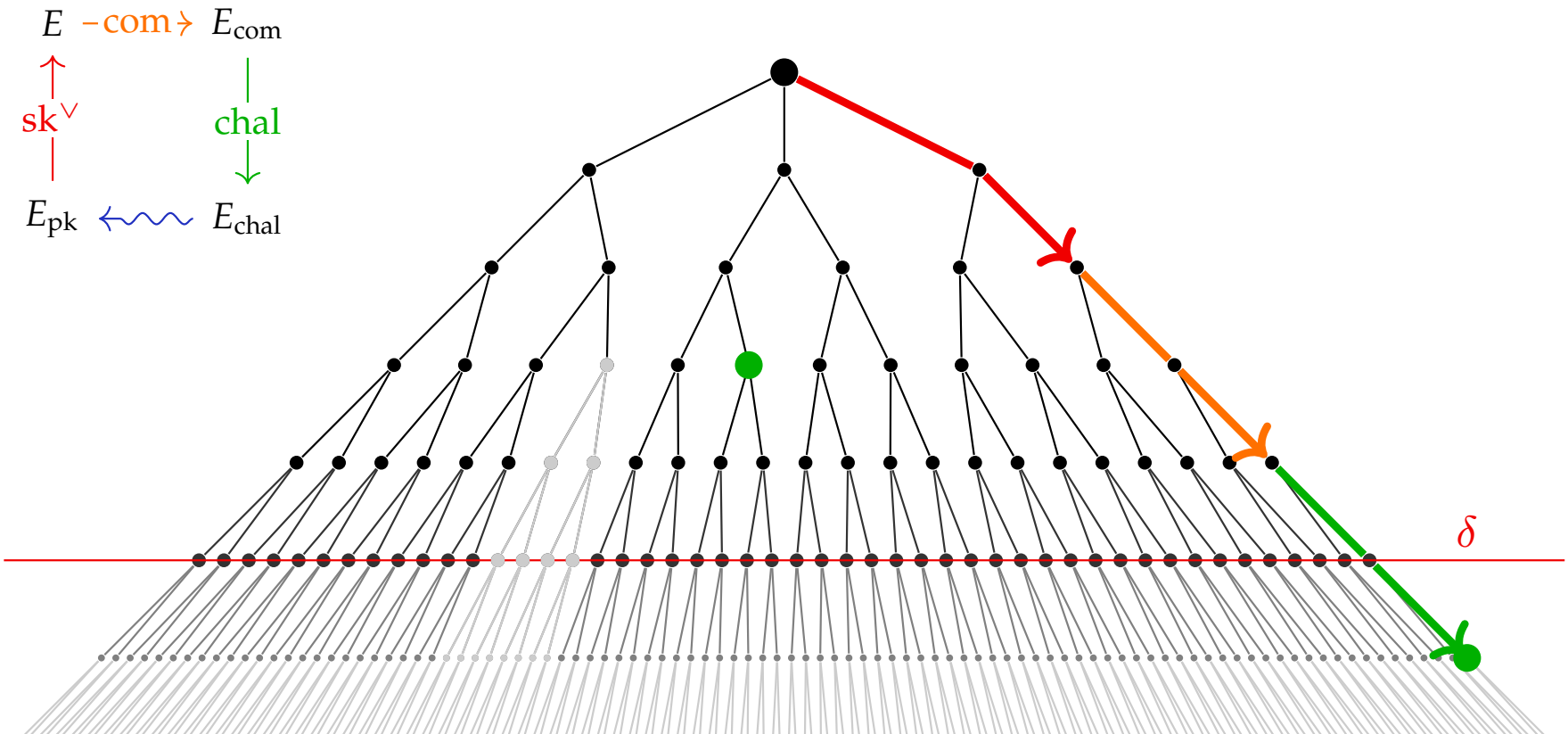
From KLPT to Bruhat-Tits quotients



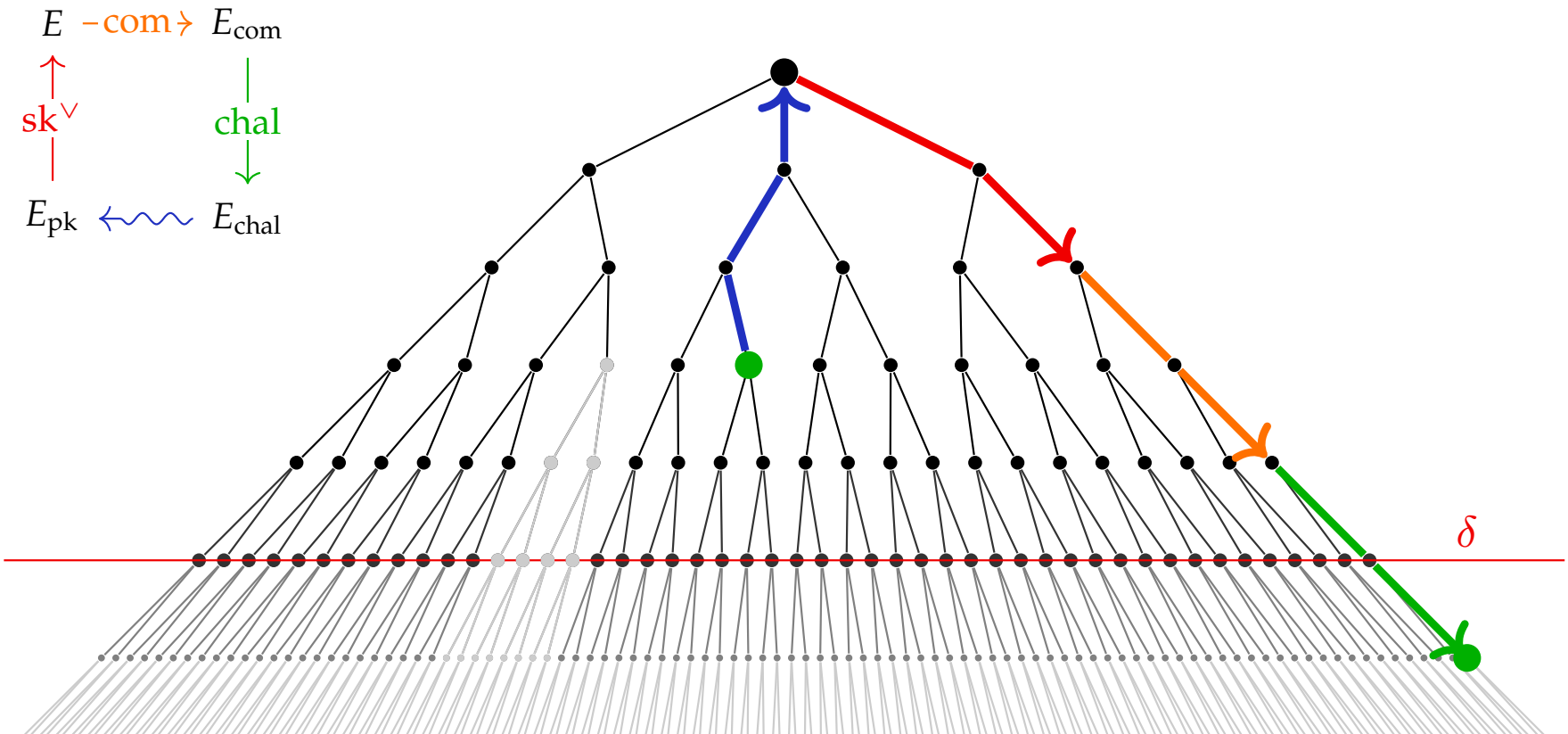
From KLPT to Bruhat-Tits quotients



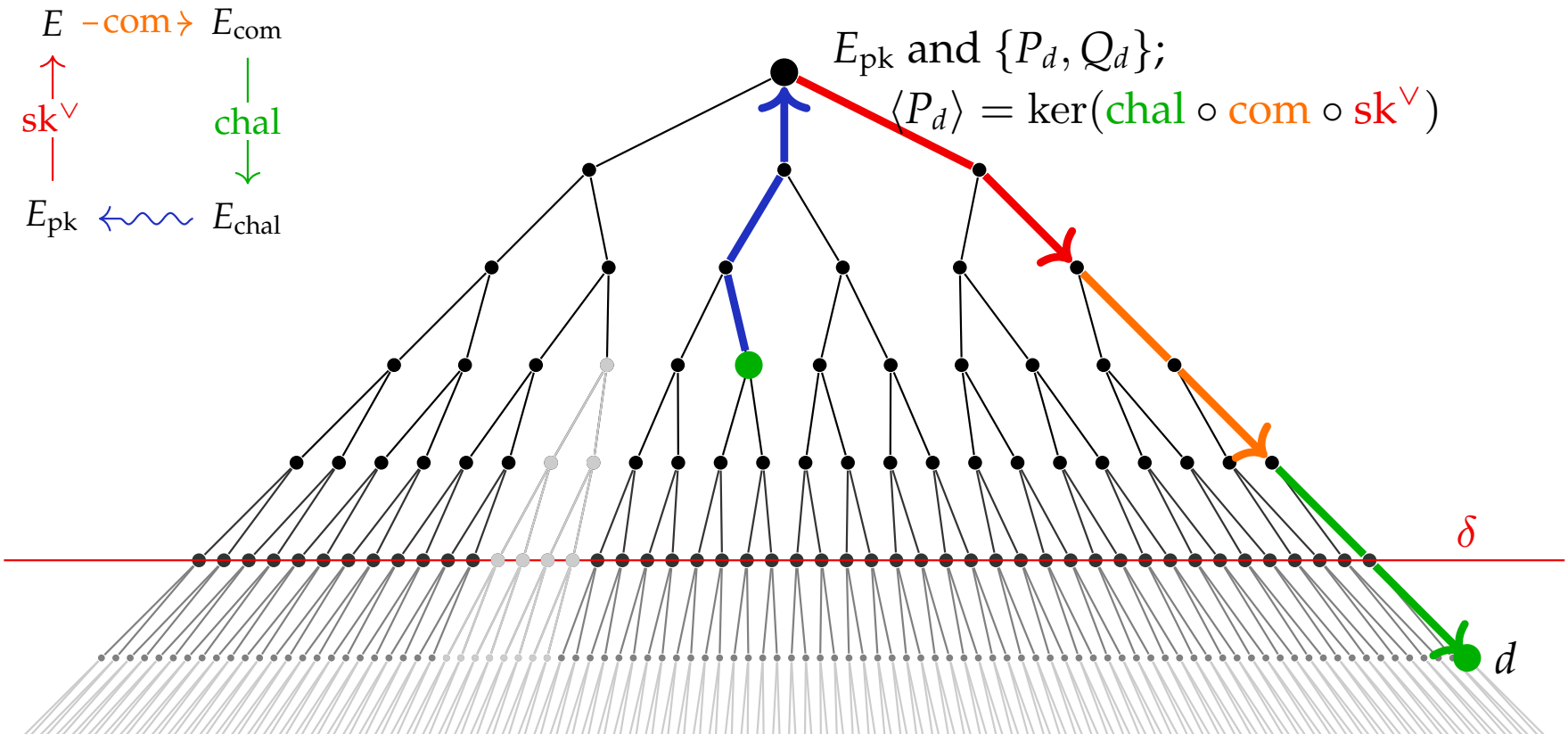
From KLPT to Bruhat-Tits quotients



From KLPT to Bruhat-Tits quotients



From KLPT to Bruhat-Tits quotients



The dream: A Bruhat-Tits identification protocol

Setup:

1. Starting at $j(E_0) = 1728$, compute a chain of 2-isogenies sk; publish codomain E_{pk} as public key.

The dream: A Bruhat-Tits identification protocol

Setup:

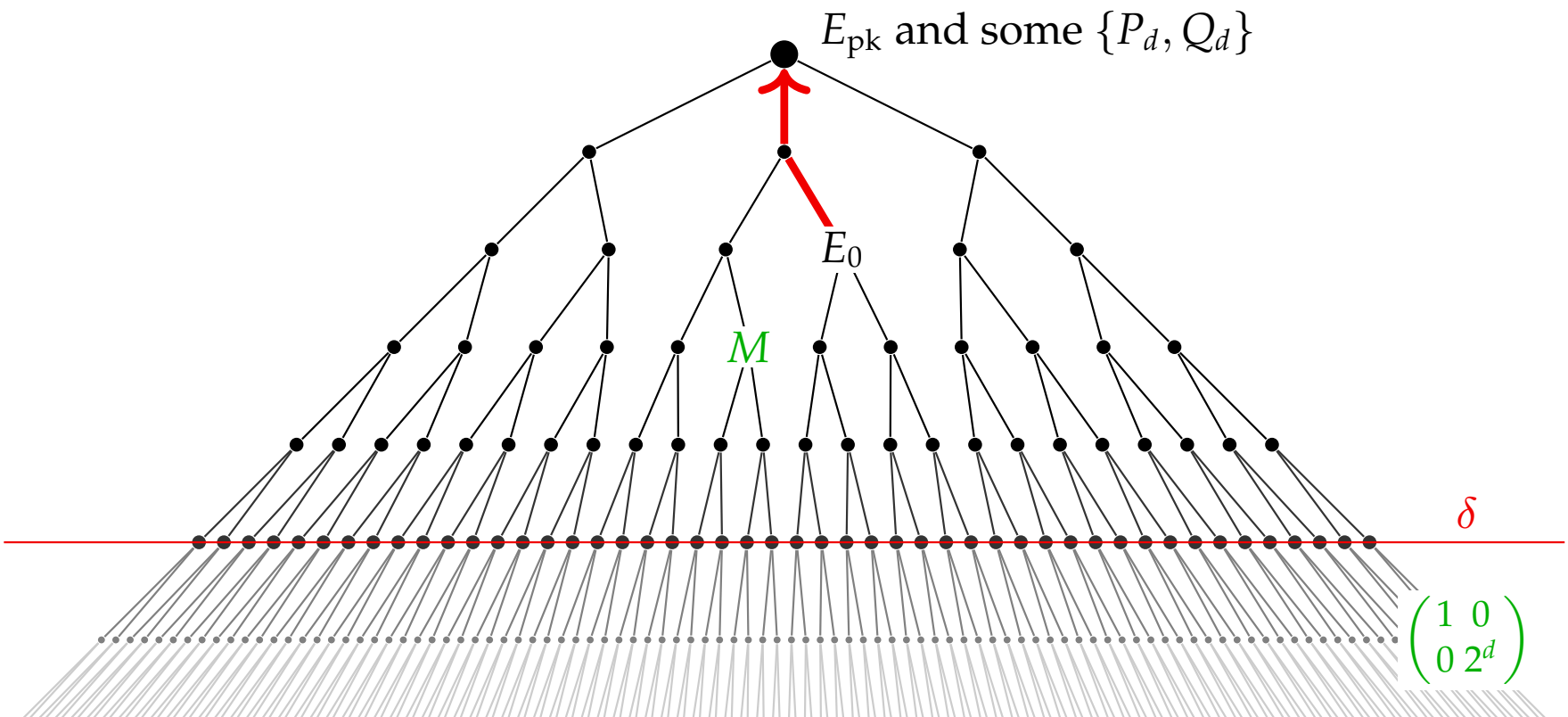
1. Starting at $j(E_0) = 1728$, compute a chain of 2-isogenies sk; publish codomain E_{pk} as public key.
2. Compute $\text{End}(E_{\text{pk}})$ and choose any basis P_d, Q_d of $E_{\text{pk}}[2^d]$, where $d > \delta$ is prescribed.

The dream: A Bruhat-Tits identification protocol

Setup:

1. Starting at $j(E_0) = 1728$, compute a chain of 2-isogenies sk; publish codomain E_{pk} as public key.
2. Compute $\text{End}(E_{\text{pk}})$ and choose any basis P_d, Q_d of $E_{\text{pk}}[2^d]$, where $d > \delta$ is prescribed.
3. Compute, for these choices, the matrix node M of depth $< \delta$ equivalent to $\begin{pmatrix} 1 & 0 \\ 0 & 2^d \end{pmatrix}$ in the quotient of the Bruhat-Tits tree with root E_{pk} and basis $\{P_d, Q_d\}$ of $T_2(E_{\text{pk}})$ at precision 2^d.

The dream: A Bruhat-Tits identification protocol



The dream: A Bruhat-Tits identification protocol

Commitment:

1. Starting at $j(E_0) = 1728$, compute a secret chain of 2-isogenies

$$\text{com} : E_0 \longrightarrow E_{\text{com}};$$

publicly commit to E_{com}.

The dream: A Bruhat-Tits identification protocol

Commitment:

1. Starting at $j(E_0) = 1728$, compute a secret chain of 2-isogenies
$$\text{com} : E_0 \longrightarrow E_{\text{com}};$$
publicly commit to E_{com}.

Challenge:

1. Send a challenge 2-isogeny chain
$$\text{chal} : E_{\text{com}} \longrightarrow E_{\text{ver}}.$$

The dream: A Bruhat-Tits identification protocol

Commitment:

1. Starting at $j(E_0) = 1728$, compute a secret chain of 2-isogenies
$$\text{com} : E_0 \longrightarrow E_{\text{com}};$$
publicly commit to E_{com}.

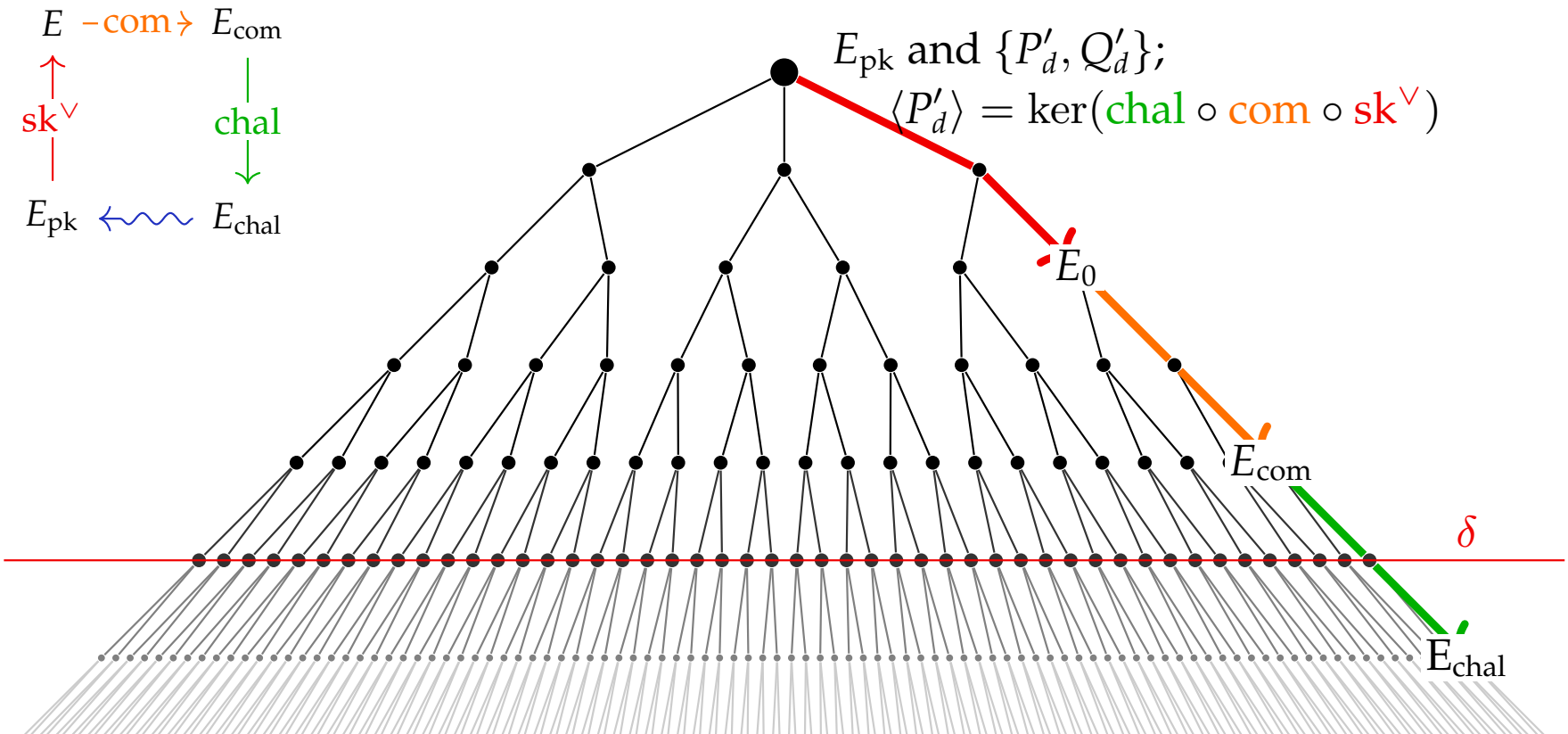
Challenge:

1. Send a challenge 2-isogeny chain
$$\text{chal} : E_{\text{com}} \longrightarrow E_{\text{ver}}.$$

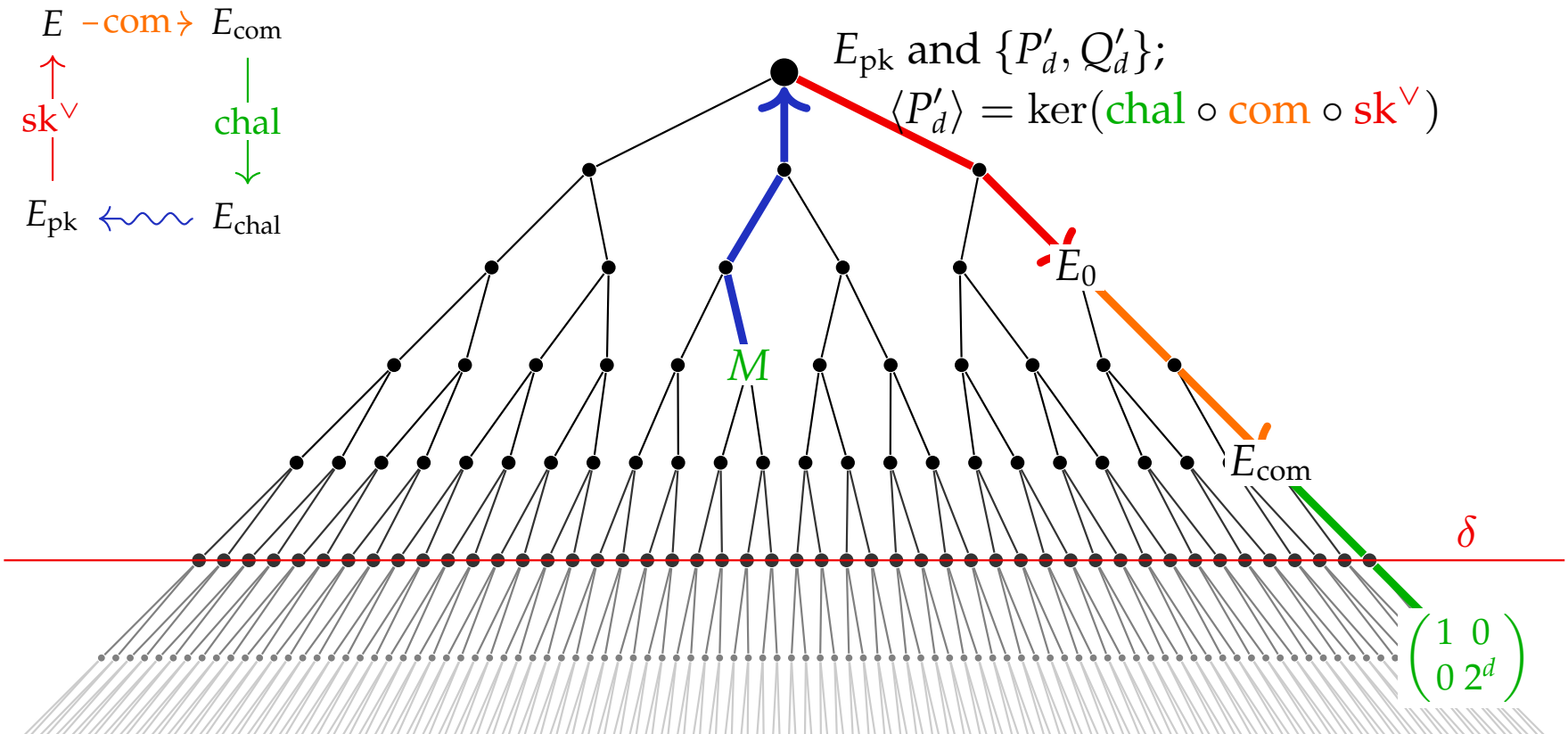
Response:

1. Compute the base change to basis $\{P'_d, Q'_d\}$ such that
$$\langle P'_d \rangle = \ker(\text{chal} \circ \text{esk} \circ \text{sk}^\vee).$$
2. Using M, read off a shorter path back to the root, reveal the corresponding 2-isogeny chain.

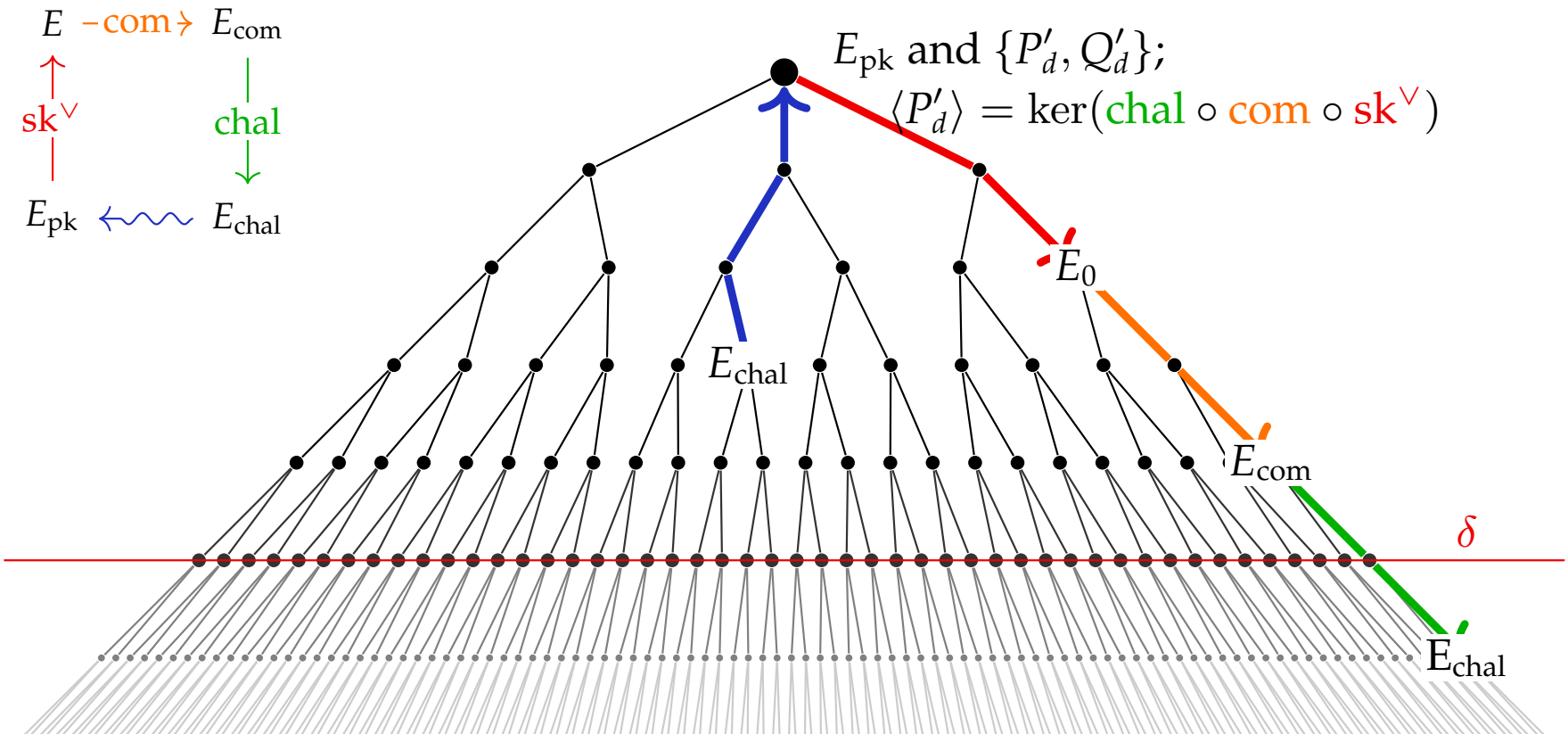
The dream: A Bruhat-Tits identification protocol



The dream: A Bruhat-Tits identification protocol



The dream: A Bruhat-Tits identification protocol



In progress: computing quotients

- We can't yet compute $M \sim \begin{pmatrix} 1 & 0 \\ 0 & 2^d \end{pmatrix}$.
- Only existing algorithm: Franc-Masdeu.
- Adapting F-M leads to:

Open question:

Find the shortest vector of

$$\begin{pmatrix} N \\ 2^n I \end{pmatrix} \in \mathrm{Mat}_{4\times 8}(\mathbb{Z}[x])$$

with respect to length

$$||\underline{v}(x)|| = \min_{x\in[0,r]}\{||\underline{v}(x)\cdot\underline{v}(x)||_\infty\}.$$

In progress: computing quotients

- We can't yet compute $M \sim \begin{pmatrix} 1 & 0 \\ 0 & 2^d \end{pmatrix}$.
- Only existing algorithm: Franc-Masdeu.
- Adapting F-M leads to:

Open question:

Find the shortest vector of

$$\begin{pmatrix} N \\ 2^n I \end{pmatrix} \in \mathrm{Mat}_{4\times 8}(\mathbb{Z}[x])$$

with respect to length

$$||\underline{v}(x)|| = \min_{x\in[0,r]}\{||\underline{v}(x)\cdot\underline{v}(x)||_\infty\}.$$

Questions? Answers?

References

AILMS Amorós, Iezzi, Lauter, Martindale, and Sotáková *Explicit connections between supersingular isogeny graphs and Bruhat-Tits trees*
`https://ia.cr/2021/372`

DKLPW De Feo, Kohel, Leroux, Petit, and Wesolowski, *SQISign: compact post-quantum signatures from quaternions and isogenies*
`https://ia.cr/2020/1240`

FM Franc and Masdeu, *Computing fundamental domains for the Bruhat-Tits tree for $GL_2(\mathbb{Q}_p)$, p-adic automorphic forms, and the canonical embedding of Shimura curves*
`https://arxiv.org/abs/1201.0356`
`https://github.com/mmasdeu/btquotients`