# Lattice-based cryptography II

## Enumeration attacks

Tanja Lange
(with some slides from Daniel J. Bersntein and Nadia Heninger)

Eindhoven University of Technology

SAC – Post-quantum cryptography

# LLL is just the beginning

Many more attacks

- Block Korkine-Zolotarev (BKZ)
  - Assumes we can solve SVP exactly in small dimension $m$.
  - Projects $m$ vectors to smaller space, solves SVP there, lifts back.
  - Chains these in a way and interleaves with LLL to obtain short basis.
  - Quality depends heavily on $m$.
- Enumeration algorithms
  - Search for absolutely shortest, with some smart ideas.
  - Finds shortest vector.
  - Can balance time and quality of basis by stopping early/pruning.
- Sieving algorithms
  - Asymptotically faster than enumeration; better than BKZ.
  - Needs more space.
  - No guarantee that short vector found is shortest.
  - Balances time and quality of basis.

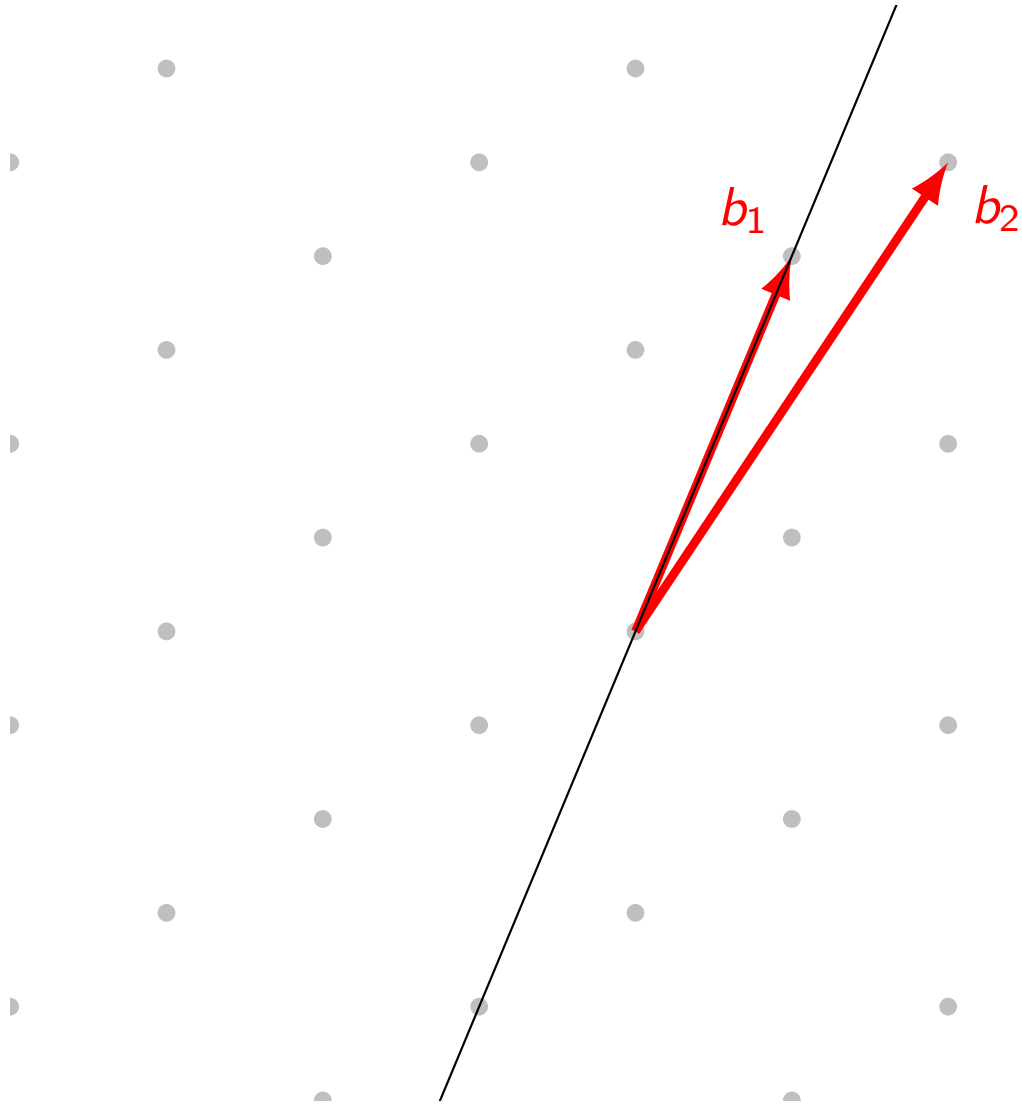
We cover enumeration. For sieving see slides 69 onwards of http://thijs.com/docs/lec2.pdf by Thijs Laarhoven.

# Enumeration


Visualization idea: Thijs Laarhoven.

# Enumeration

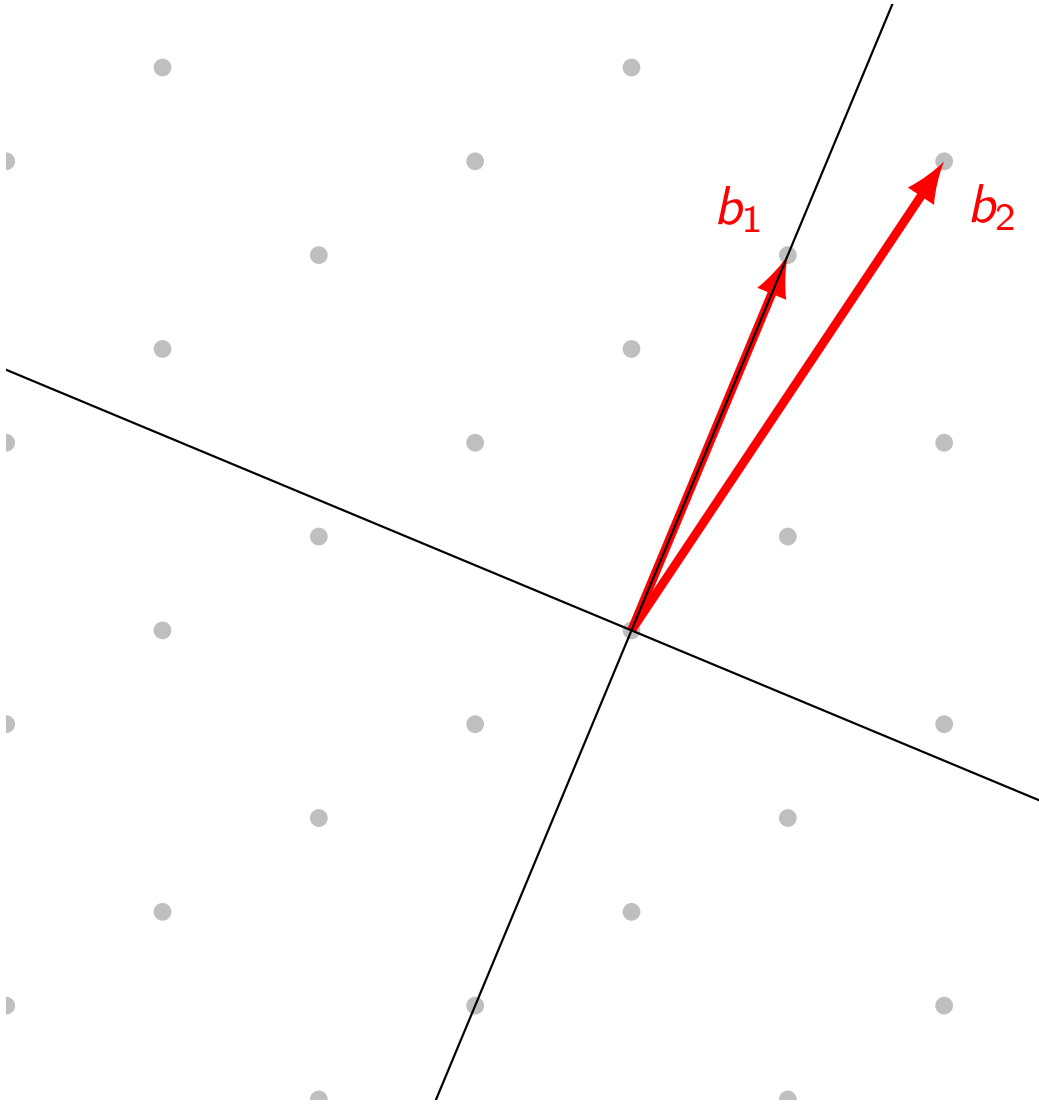
- Pick one direction, here $b_1$.




Visualization idea: Thijs Laarhoven.

# Enumeration

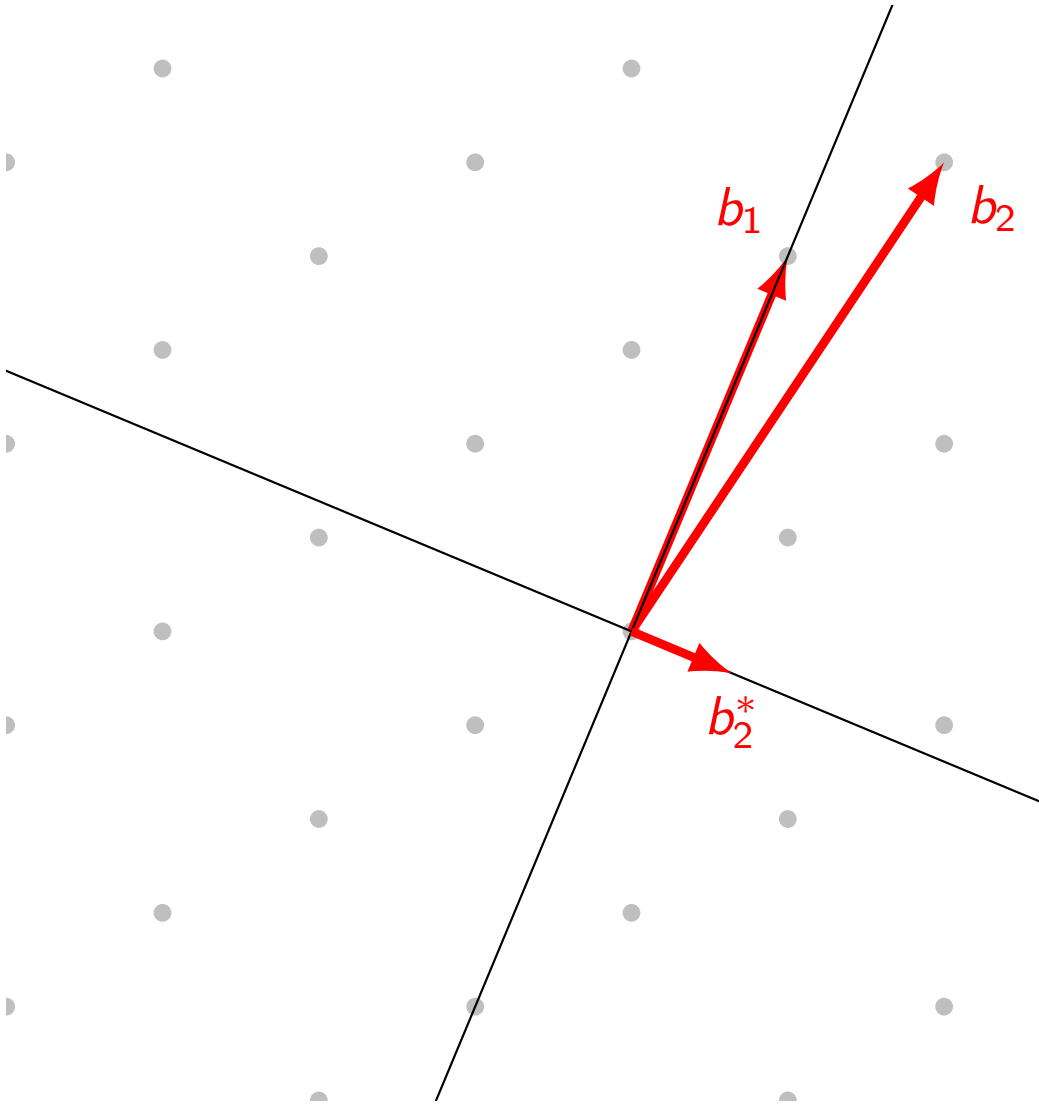
- Pick one direction, here $b_1$.
- Consider directions orthogonal to it.




Visualization idea: Thijs Laarhoven.

# Enumeration

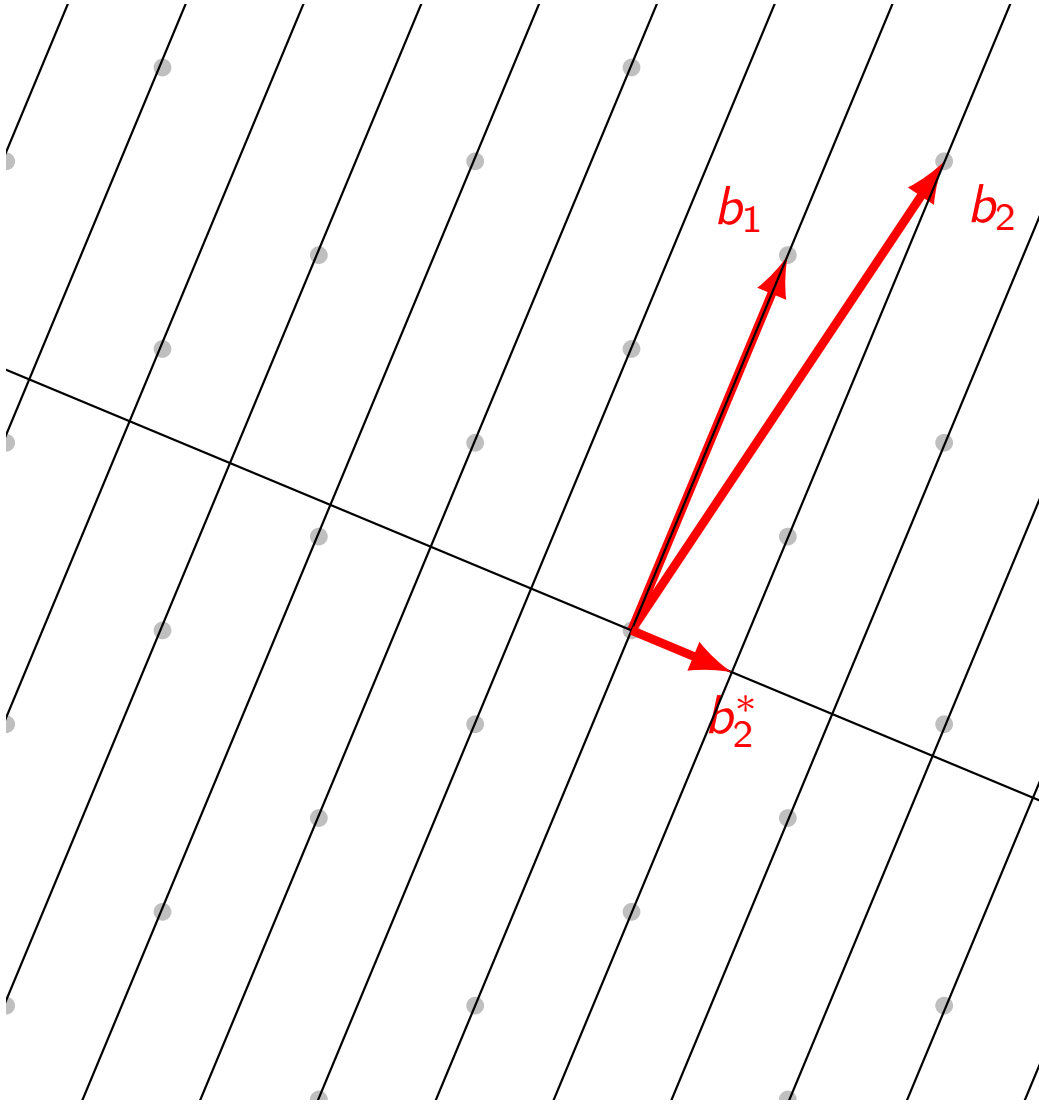
- Pick one direction, here $b_1$.
- Consider directions orthogonal to it.
- Project the other vector(s) on this orthogonal part.




Visualization idea: Thijs Laarhoven.

# Enumeration

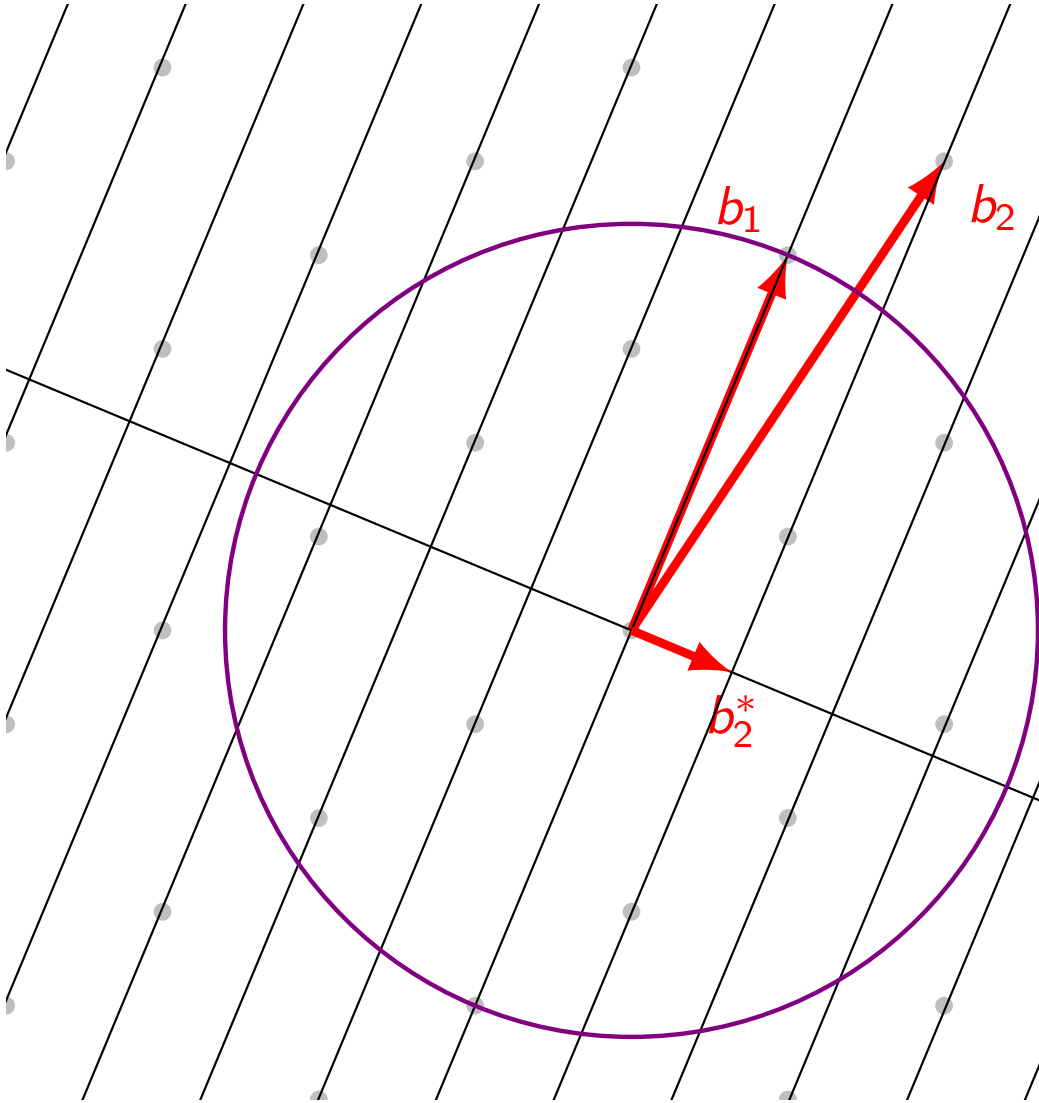
- Pick one direction, here $b_1$.
- Consider directions orthogonal to it.
- Project the other vector(s) on this orthogonal part.
- Make a grid parallel to $b_1$ spaced by the length of $B_2^*$.
- Consider points within the sphere of radius $||b_1||$.




Visualization idea: Thijs Laarhoven.

# Enumeration

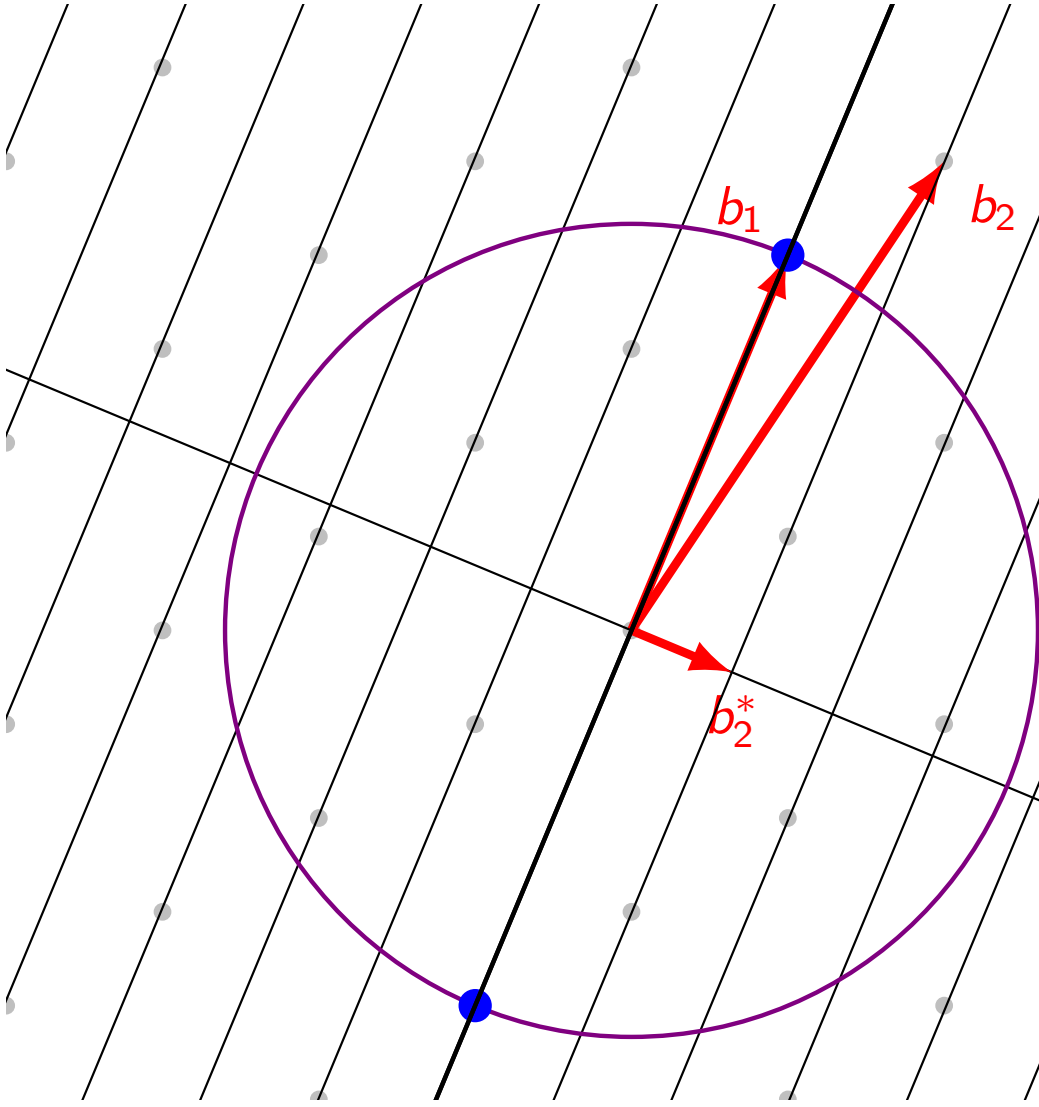
- Pick one direction, here $b_1$.
- Consider directions orthogonal to it.
- Project the other vector(s) on this orthogonal part.
- Make a grid parallel to $b_1$ spaced by the length of $B_2^*$.
- Consider points within the sphere of radius $||b_1||$.
- For each multiple of $||b_2^*||$ find all lattice points on that line.




Visualization idea: Thijs Laarhoven.

# Enumeration

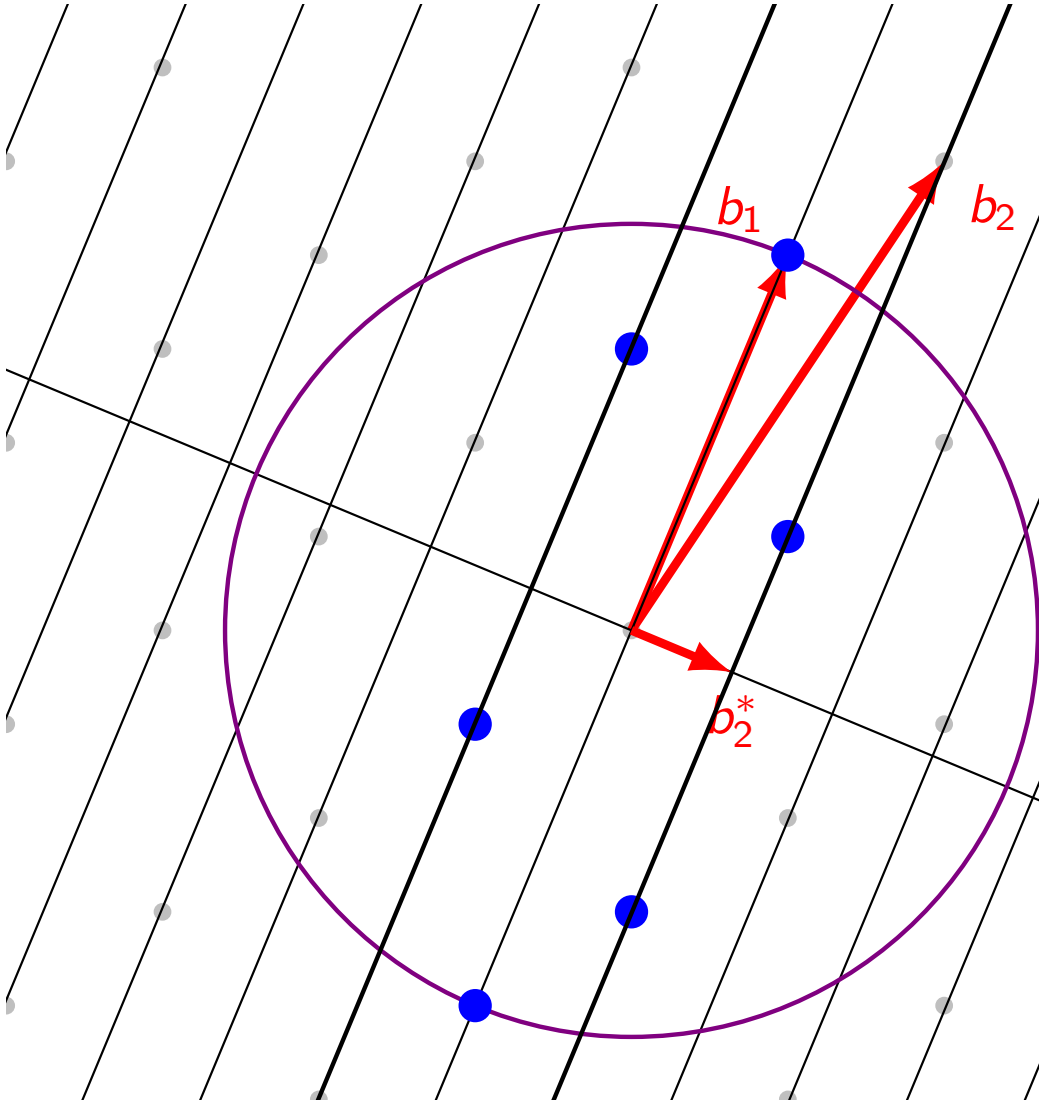
- Pick one direction, here $b_1$.
- Consider directions orthogonal to it.
- Project the other vector(s) on this orthogonal part.
- Make a grid parallel to $b_1$ spaced by the length of $B_2^*$.
- Consider points within the sphere of radius $||b_1||$.
- For each multiple of $||b_2^*||$ find all lattice points on that line.




Visualization idea: Thijs Laarhoven.

# Enumeration

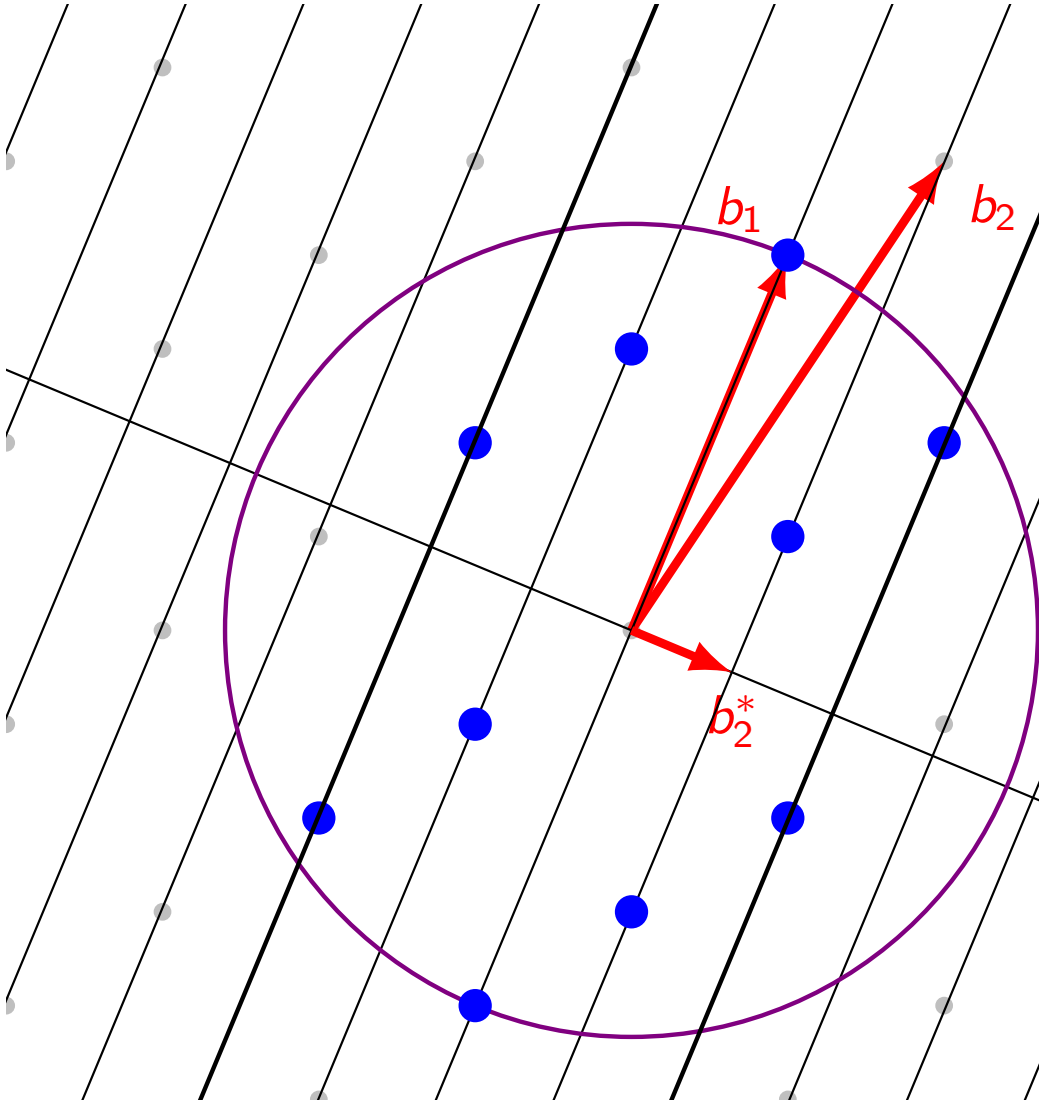
- Pick one direction, here $b_1$.
- Consider directions orthogonal to it.
- Project the other vector(s) on this orthogonal part.
- Make a grid parallel to $b_1$ spaced by the length of $B_2^*$.
- Consider points within the sphere of radius $||b_1||$.
- For each multiple of $||b_2^*||$ find all lattice points on that line.




Visualization idea: Thijs Laarhoven.

# Enumeration

- Pick one direction, here $b_1$.
- Consider directions orthogonal to it.
- Project the other vector(s) on this orthogonal part.
- Make a grid parallel to $b_1$ spaced by the length of $B_2^*$.
- Consider points within the sphere of radius $||b_1||$.
- For each multiple of $||b_2^*||$ find all lattice points on that line.

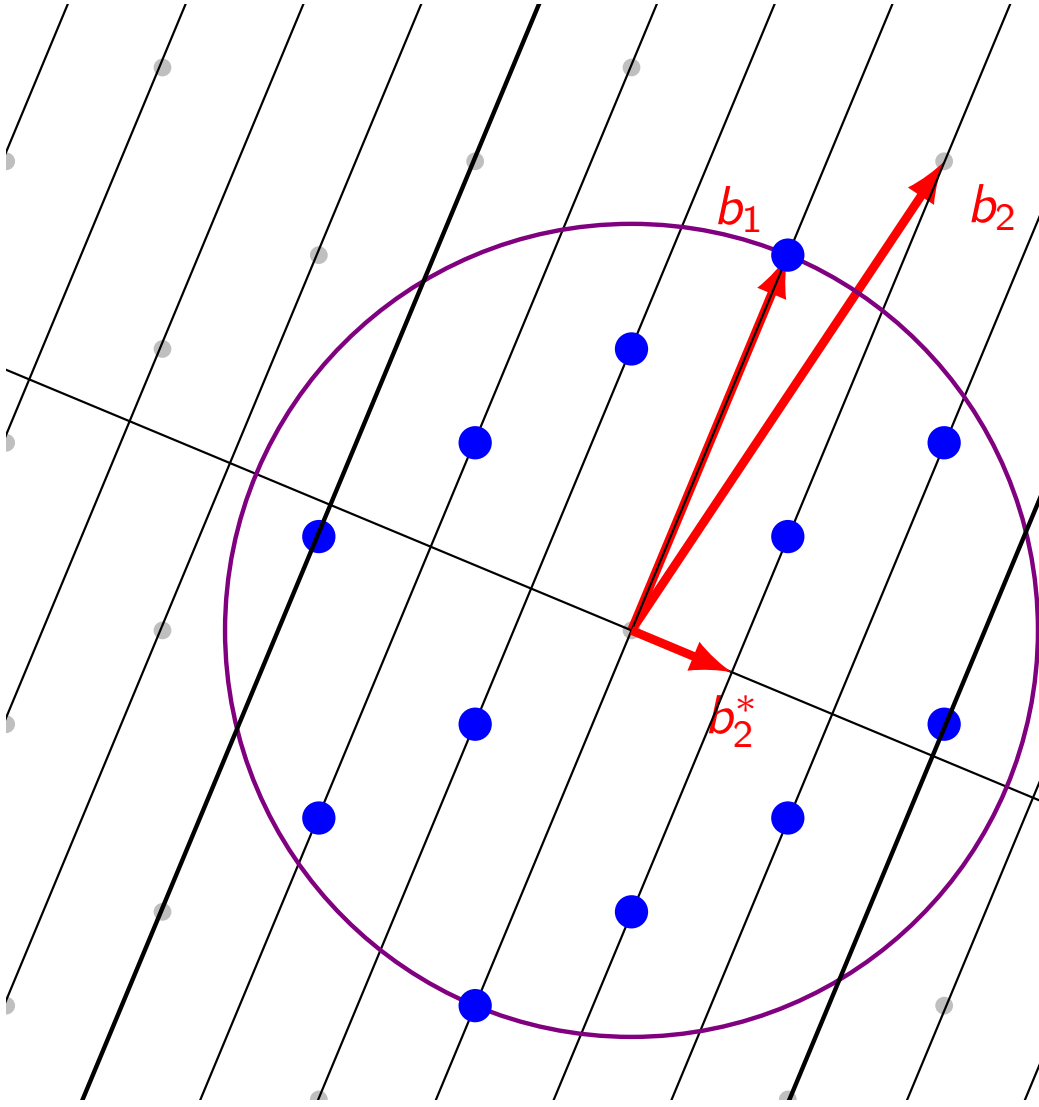



Visualization idea: Thijs Laarhoven.

# Enumeration

- Pick one direction, here $b_1$.
- Consider directions orthogonal to it.
- Project the other vector(s) on this orthogonal part.
- Make a grid parallel to $b_1$ spaced by the length of $B_2^*$.
- Consider points within the sphere of radius $||b_1||$.
- For each multiple of $||b_2^*||$ find all lattice points on that line.
- Output the shortest vector in the sphere.

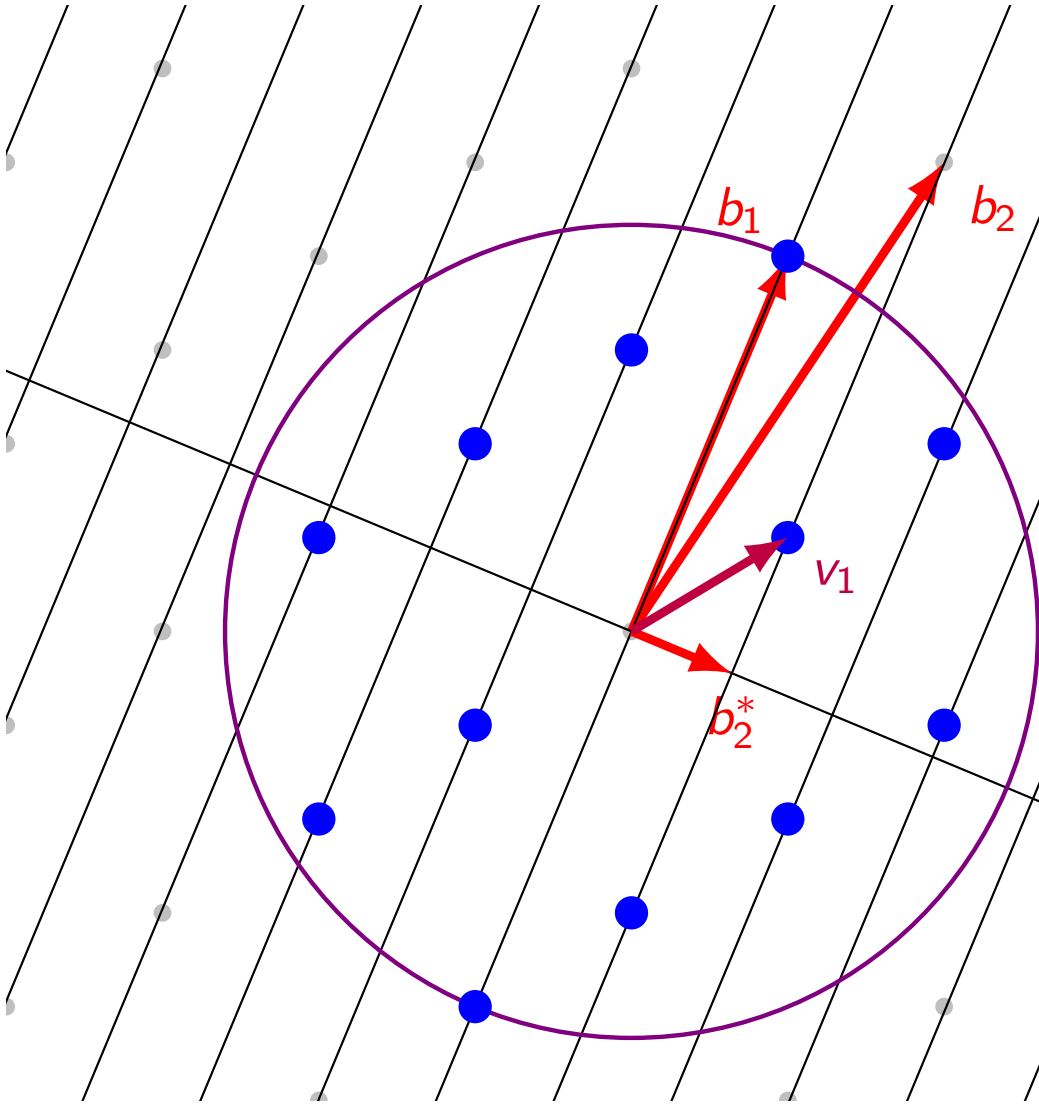
Visualization idea: Thijs Laarhoven.



# Enumeration

- Pick one direction, here $b_1$.
- Consider directions orthogonal to it.
- Project the other vector(s) on this orthogonal part.
- Make a grid parallel to $b_1$ spaced by the length of $B_2^*$.
- Consider points within the sphere of radius $||b_1||$.
- For each multiple of $||b_2^*||$ find all lattice points on that line.
- Output the shortest vector in the sphere.

Visualization idea: Thijs Laarhoven.



# Enumeration with pruning

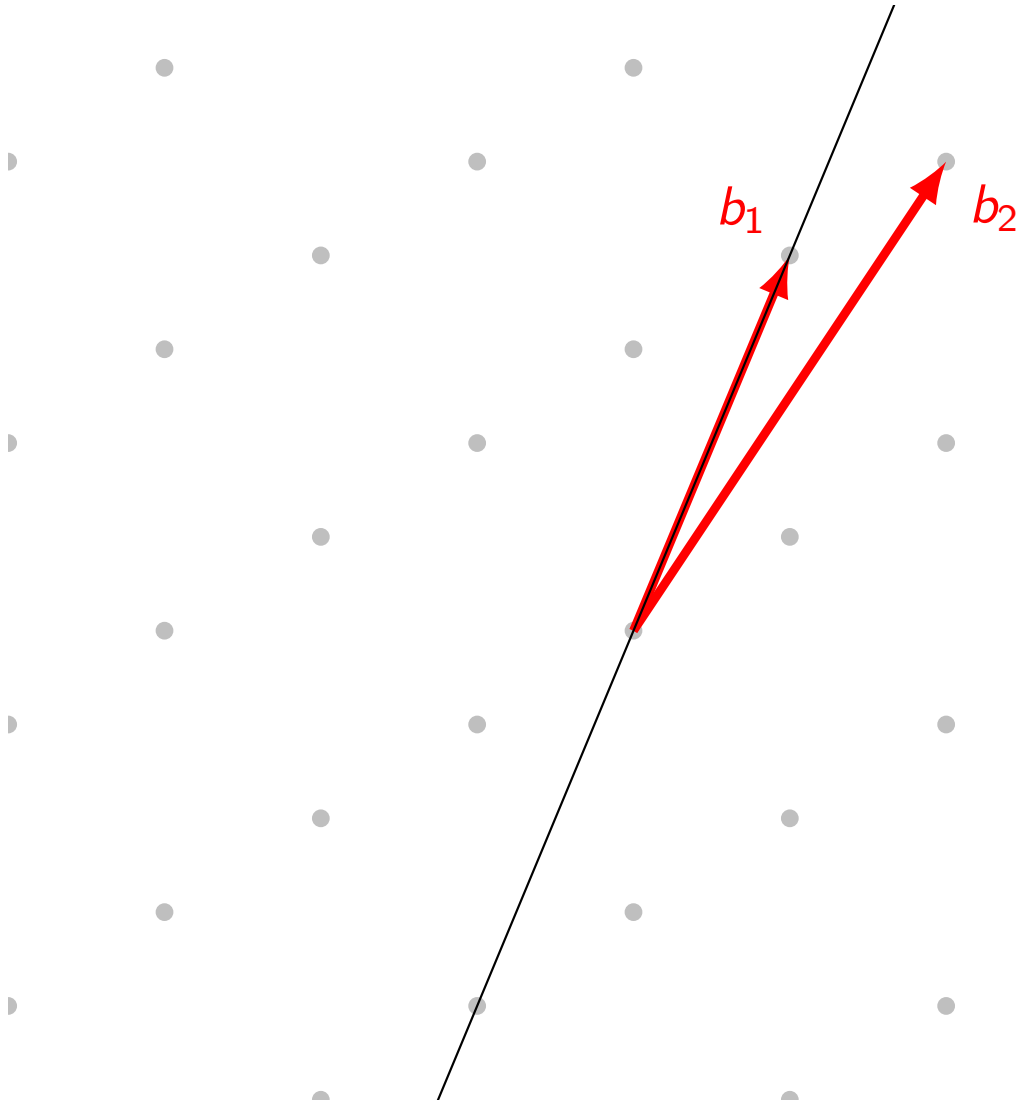
- Follow the steps for enumeration.


Visualization idea: Thijs Laarhoven.

# Enumeration with pruning

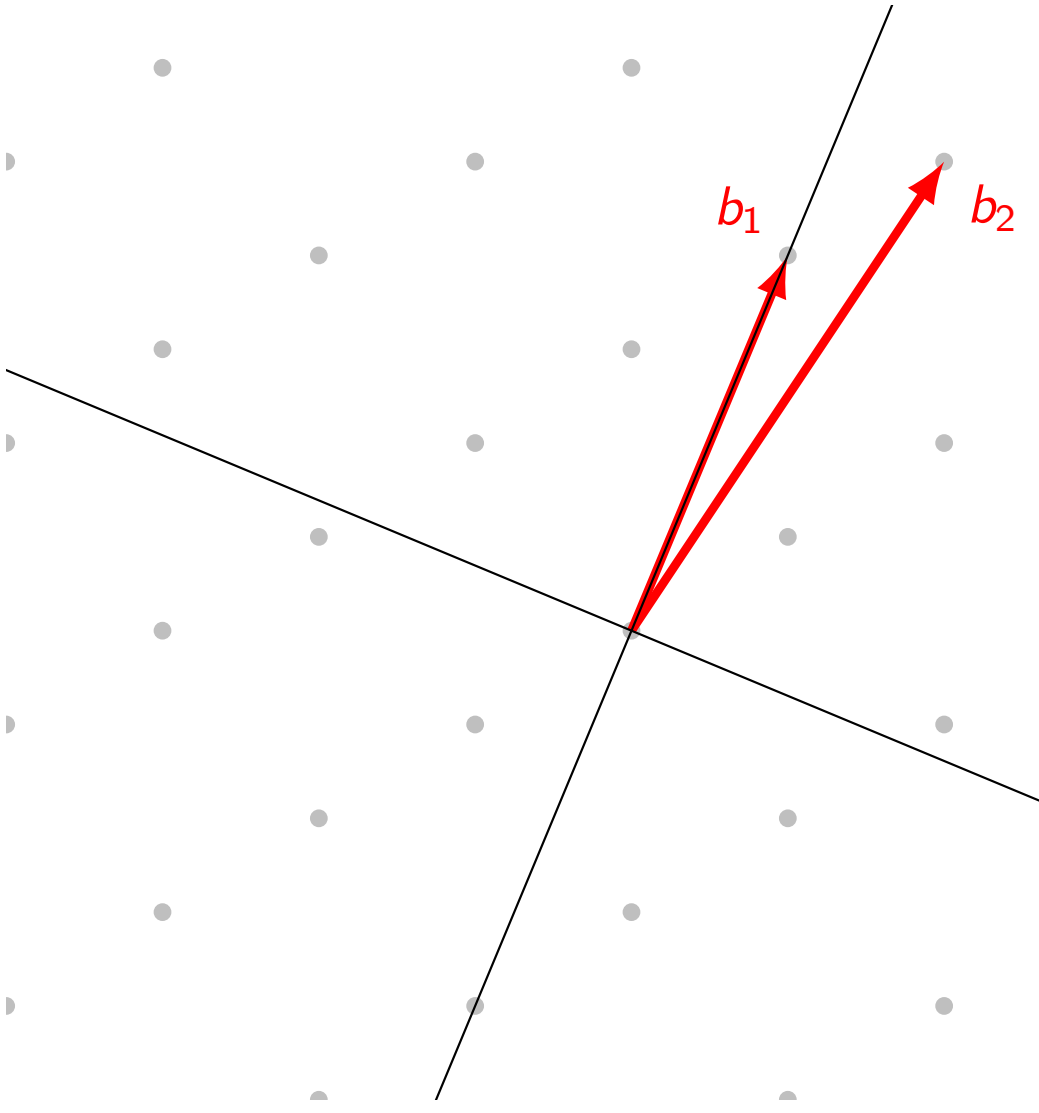
- Follow the steps for enumeration.

Visualization idea: Thijs Laarhoven.



# Enumeration with pruning

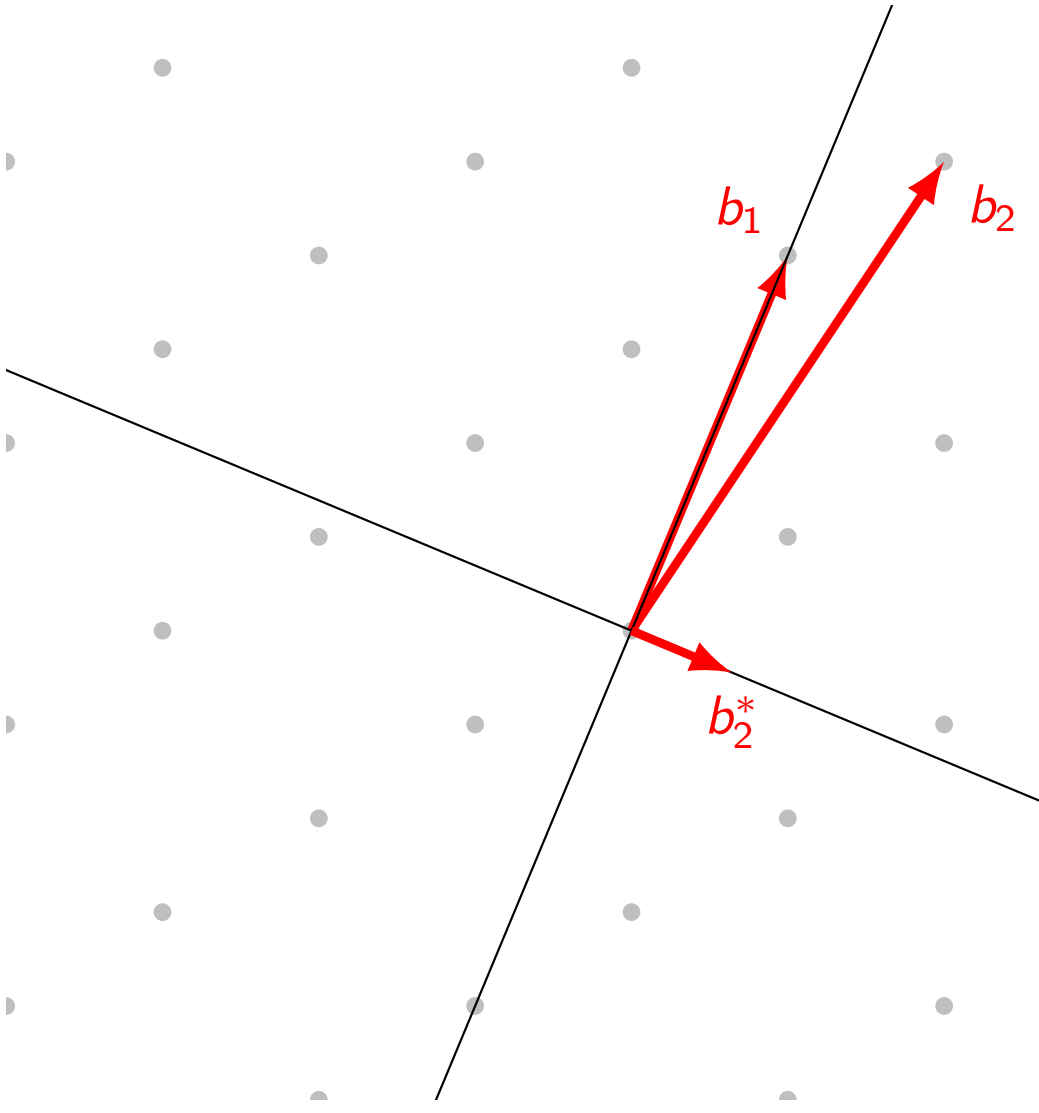
- Follow the steps for enumeration.




Visualization idea: Thijs Laarhoven.

# Enumeration with pruning

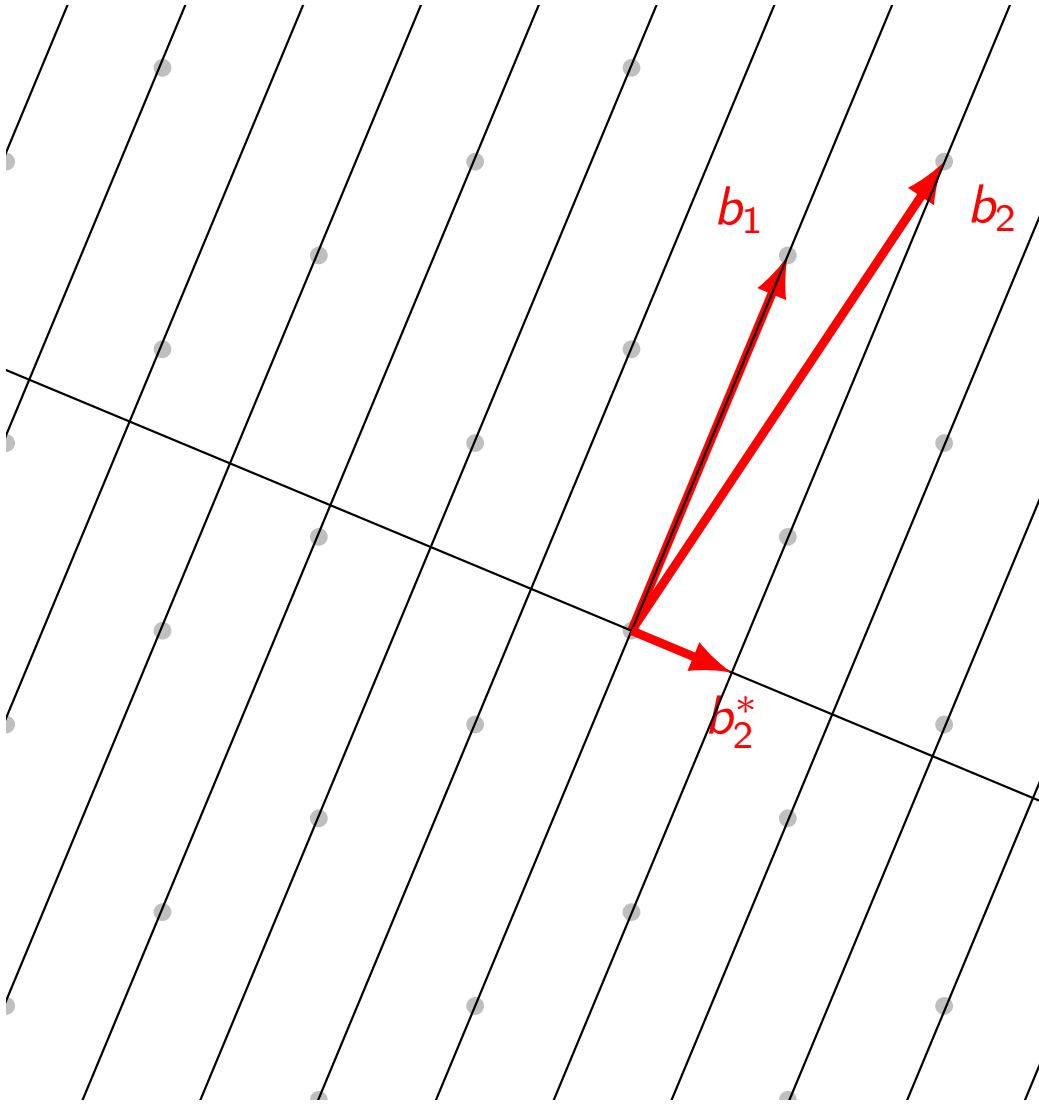
- Follow the steps for enumeration.




Visualization idea: Thijs Laarhoven.

# Enumeration with pruning

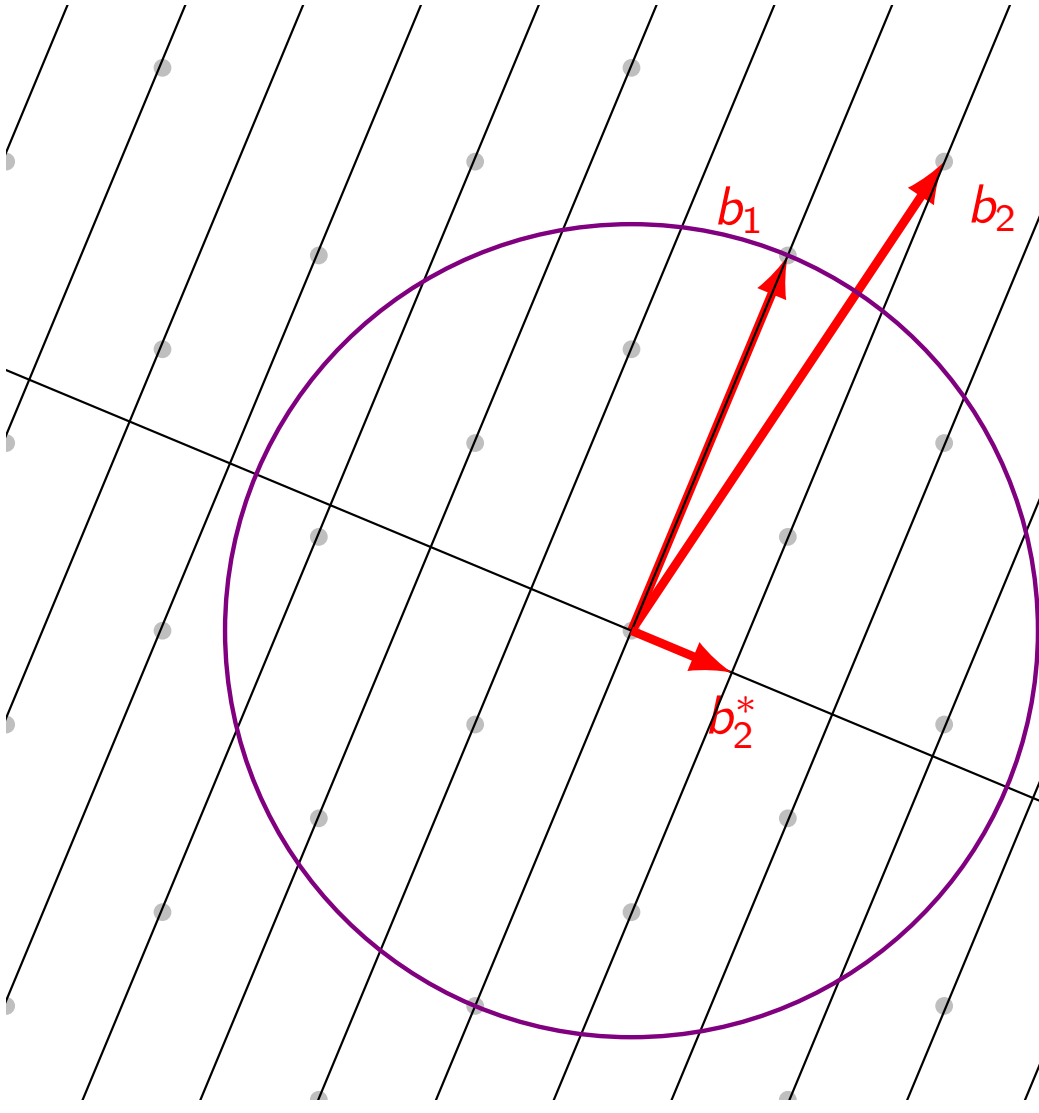
- Follow the steps for enumeration.




Visualization idea: Thijs Laarhoven.

# Enumeration with pruning

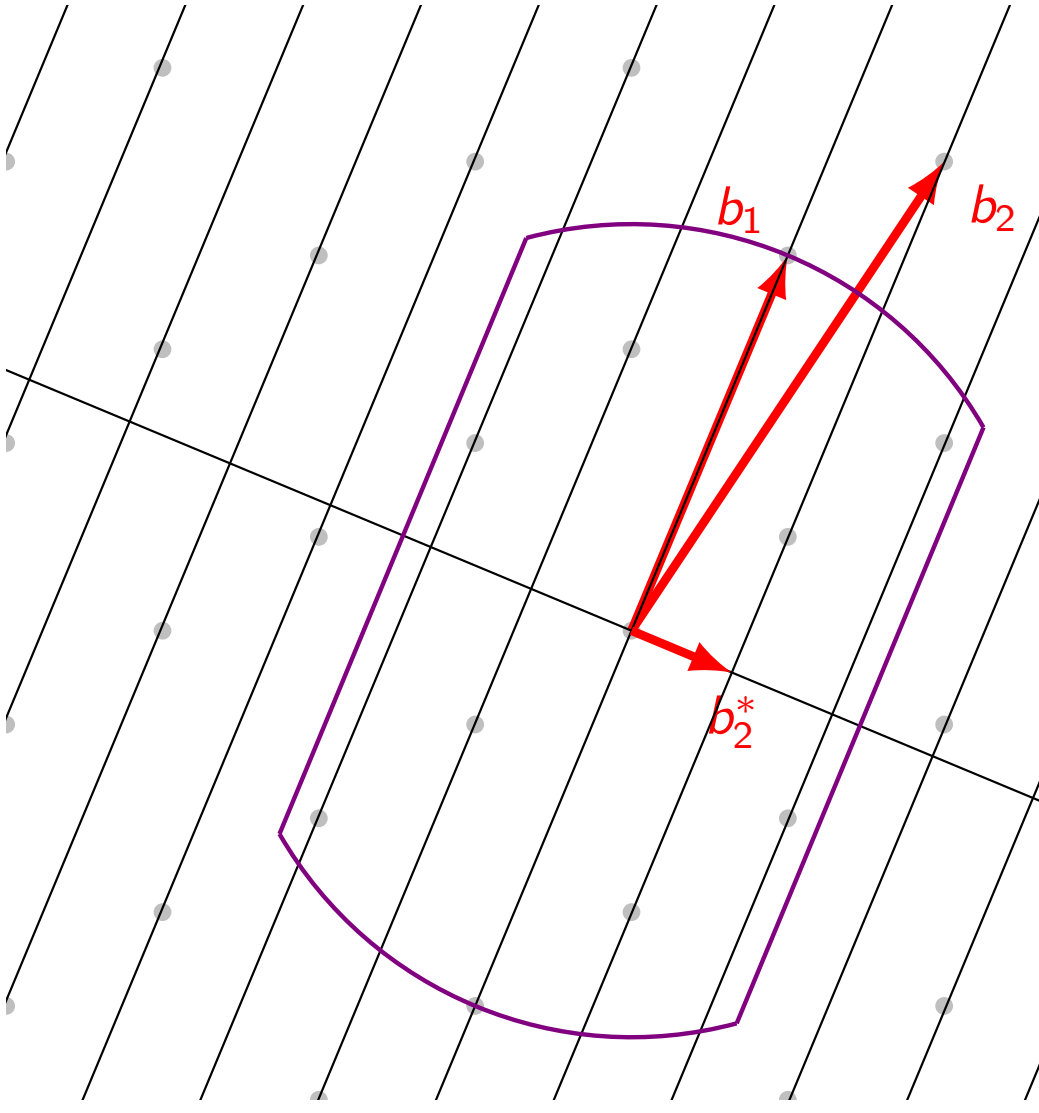
- Follow the steps for enumeration.
- Restrict the multiples of $b_2^*$.




Visualization idea: Thijs Laarhoven.

# Enumeration with pruning

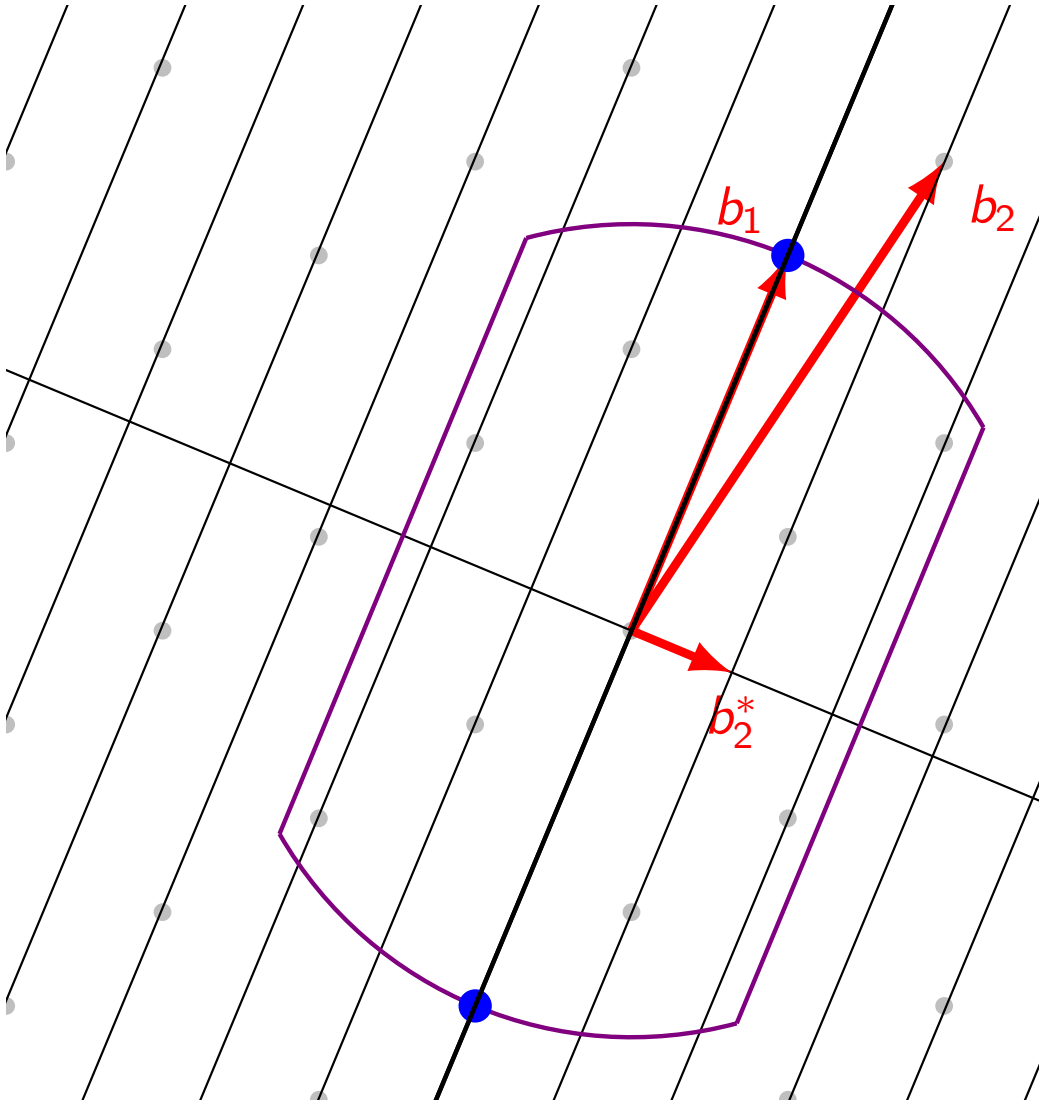
- Follow the steps for enumeration.
- Restrict the multiples of $b_2^*$.
- Continue as in enumeration




Visualization idea: Thijs Laarhoven.

# Enumeration with pruning

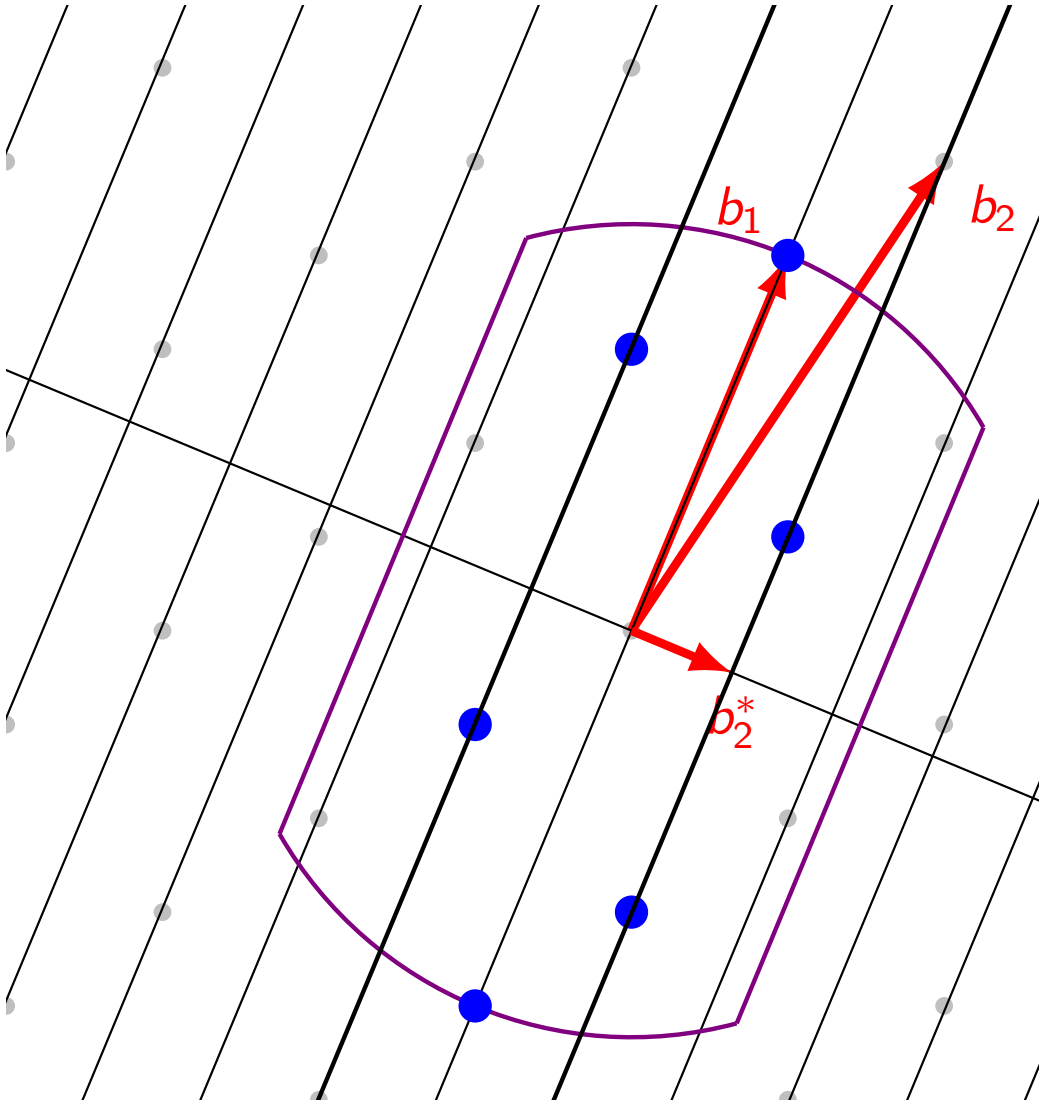
- Follow the steps for enumeration.
- Restrict the multiples of $b_2^*$.
- Continue as in enumeration




Visualization idea: Thijs Laarhoven.

# Enumeration with pruning

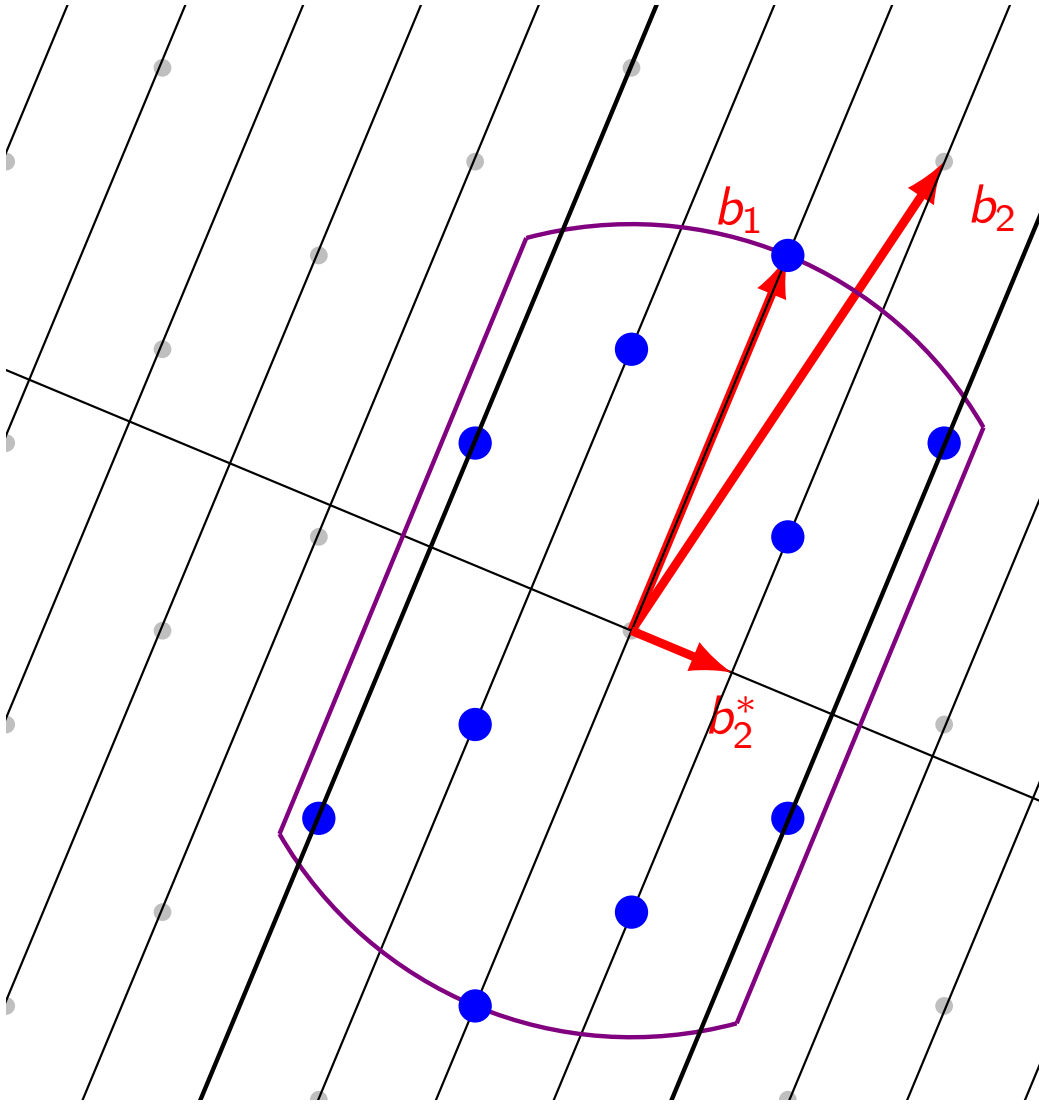
- Follow the steps for enumeration.
- Restrict the multiples of $b_2^*$.
- Continue as in enumeration




Visualization idea: Thijs Laarhoven.

# Enumeration with pruning

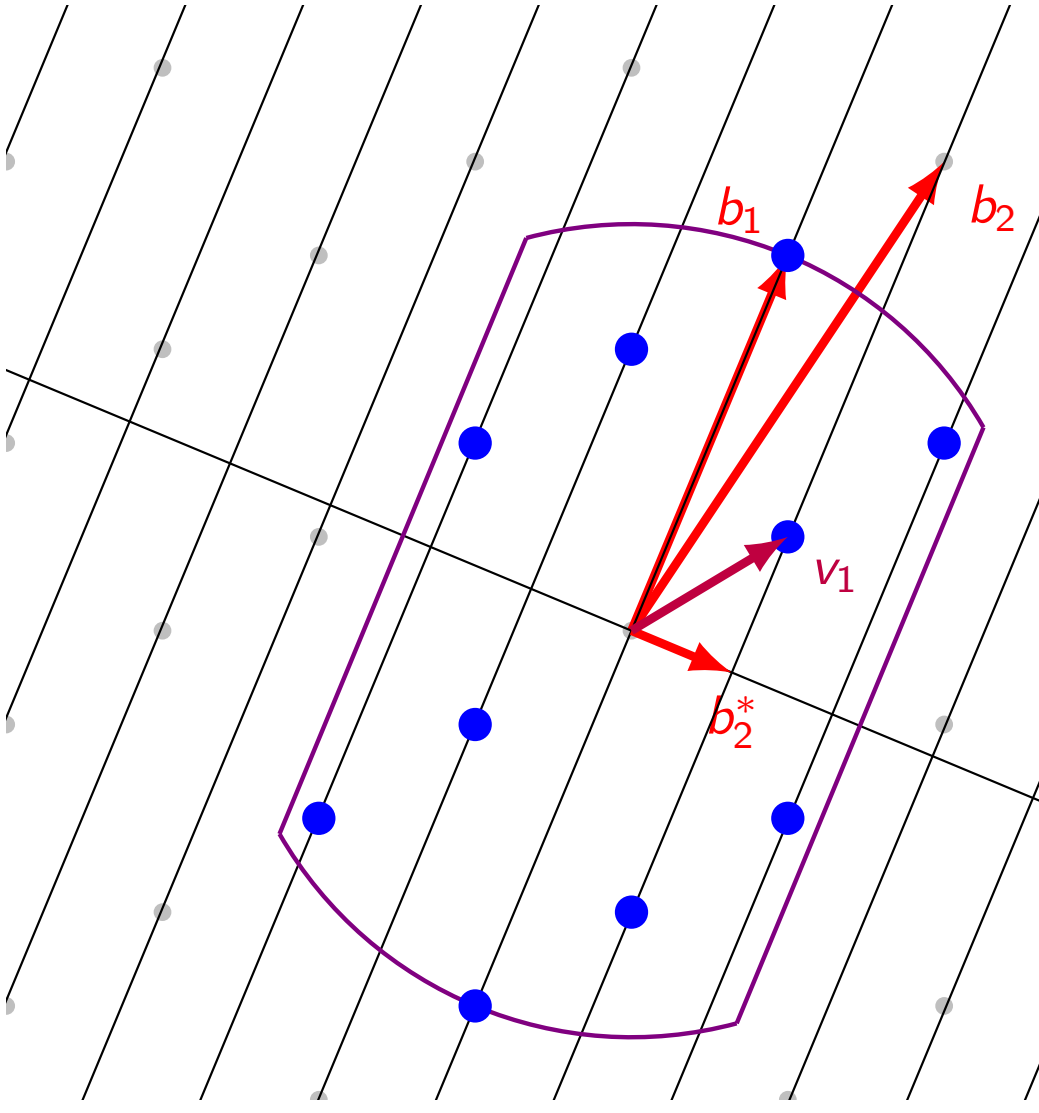
- Follow the steps for enumeration.
- Restrict the multiples of $b_2^*$.
- Continue as in enumeration




Visualization idea: Thijs Laarhoven.

# Enumeration with pruning

- Follow the steps for enumeration.
- Restrict the multiples of $b_2^*$.
- Continue as in enumeration
- Output the shortest vector in the sphere.




Visualization idea: Thijs Laarhoven.

# Enumeration with pruning

- Follow the steps for enumeration.
- Restrict the multiples of $b_2^*$.
- Continue as in enumeration
- Output the shortest vector in the sphere.
- Benefit is that search space gets smaller;
  usually shortest vector is in pruned space.

Visualization idea: Thijs Laarhoven.