IBM Research

Sieving for closest lattice vectors (with preprocessing)

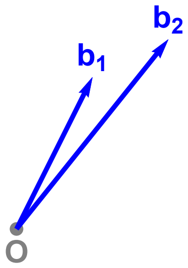
Thijs Laarhoven

mail@thijs.com
http://www.thijs.com/

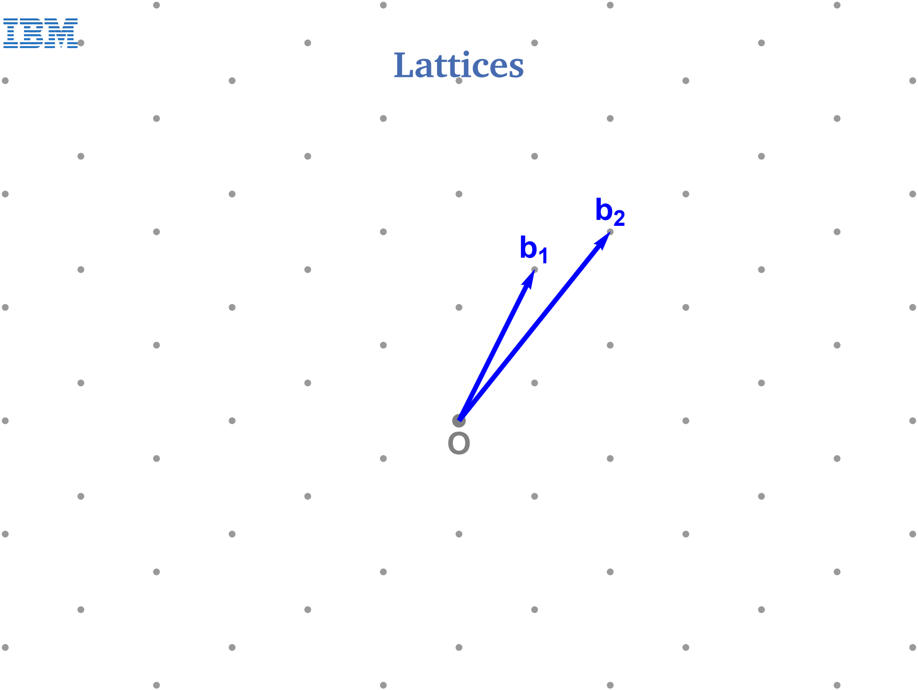
Lorentz Center 2016, Leiden, The Netherlands
(August 24, 2016)

Lattices

Lattices

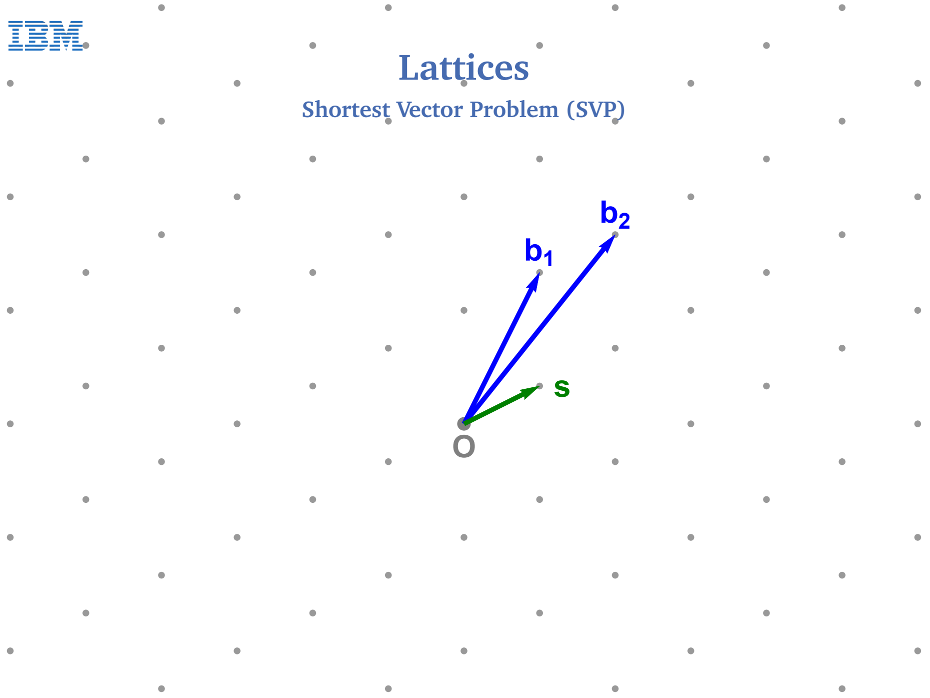


Lattices



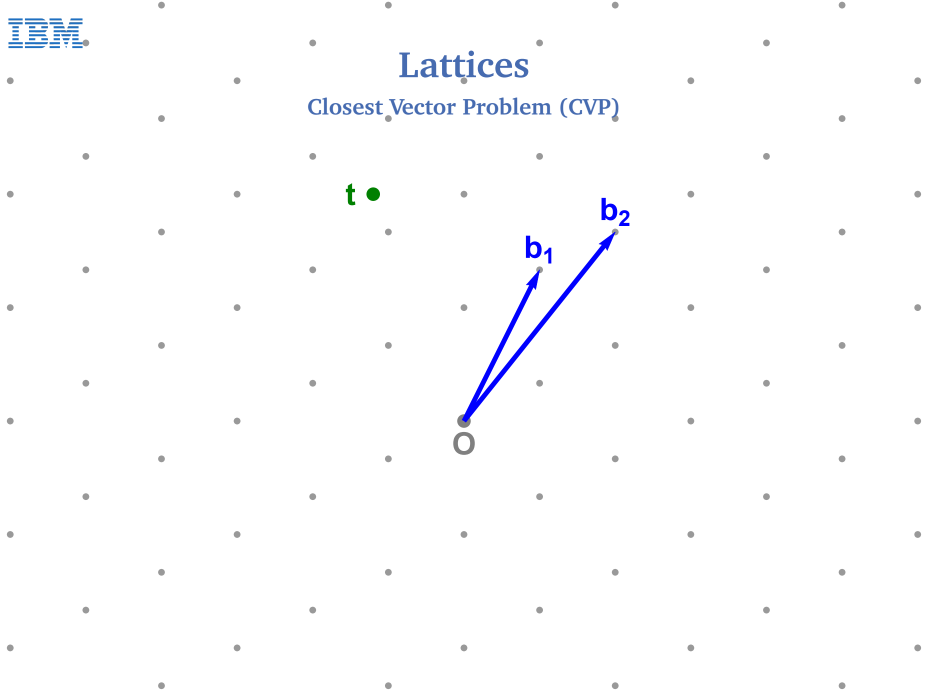
Lattices

Shortest Vector Problem (SVP)



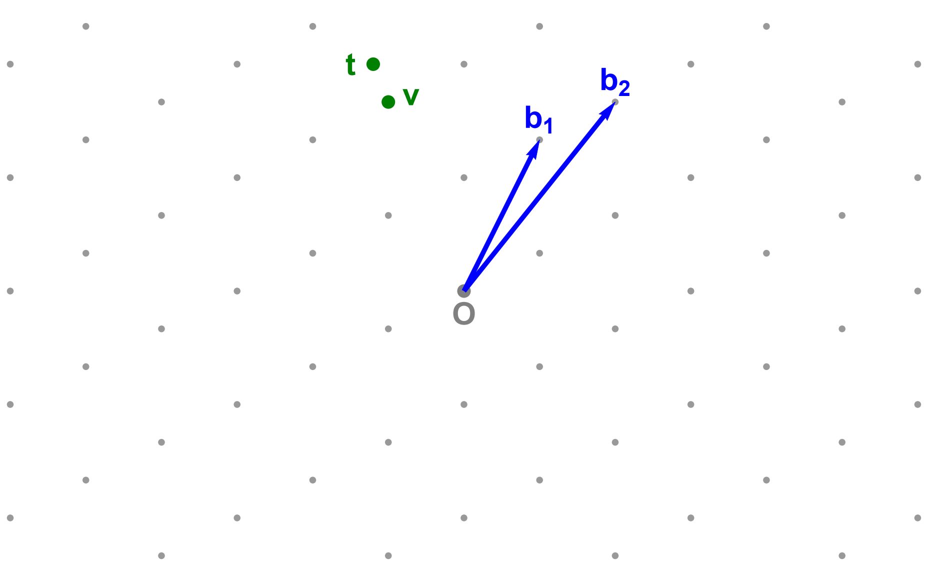
Lattices

Closest Vector Problem (CVP)



Lattices

Closest Vector Problem (CVP)



Outline

Sieving for SVP

Sieving for CVP

Sieving for CVPP

Conclusion

Outline

Sieving for SVP

Sieving for CVP

Sieving for CVPP

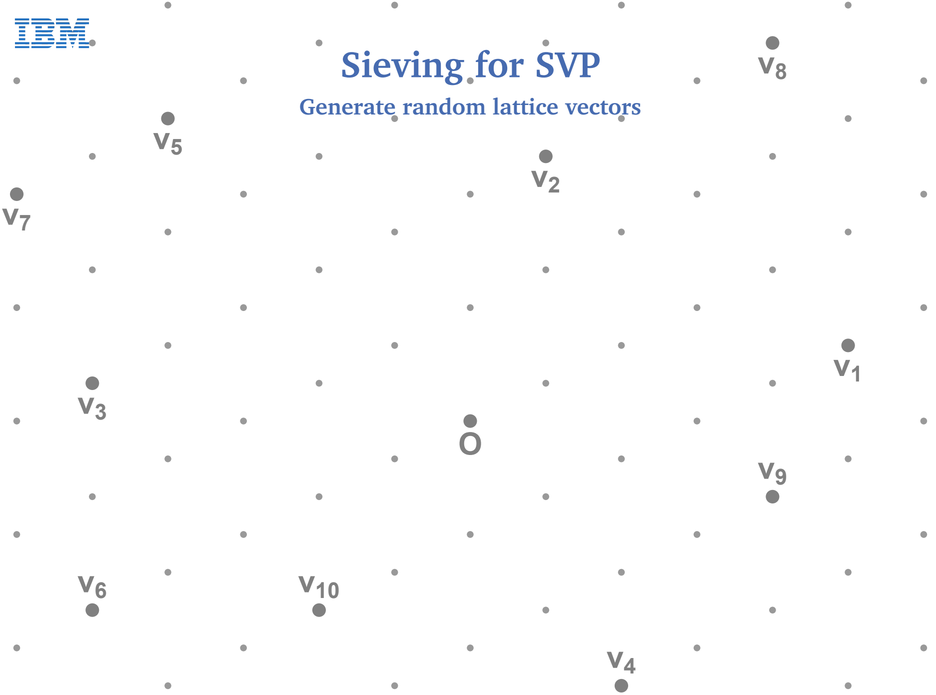
Conclusion

Sieving for SVP

Generate random lattice vectors

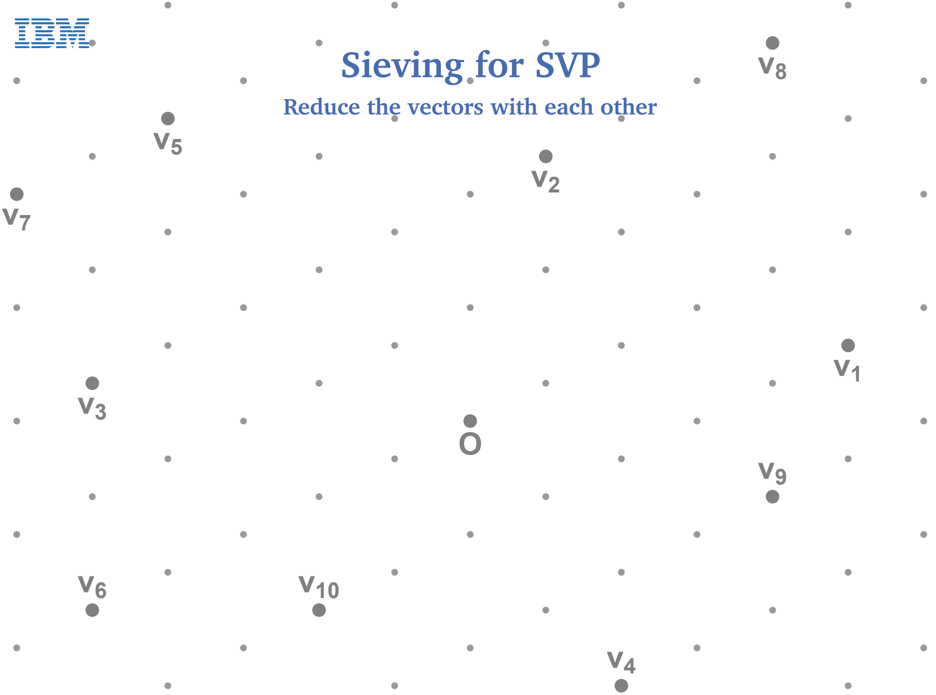
Sieving for SVP

Generate random lattice vectors



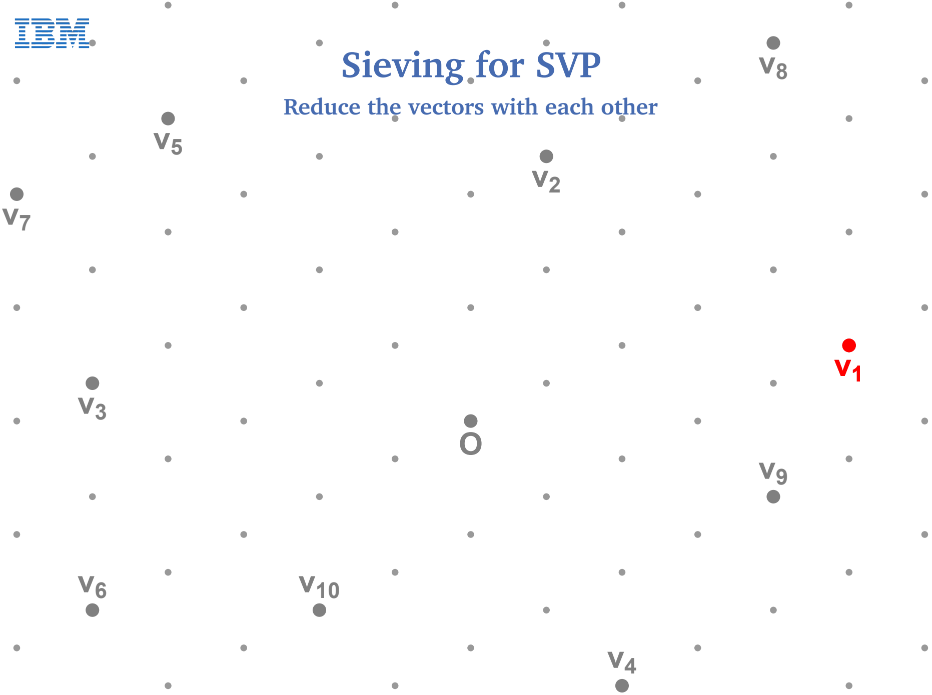
Sieving for SVP

Reduce the vectors with each other



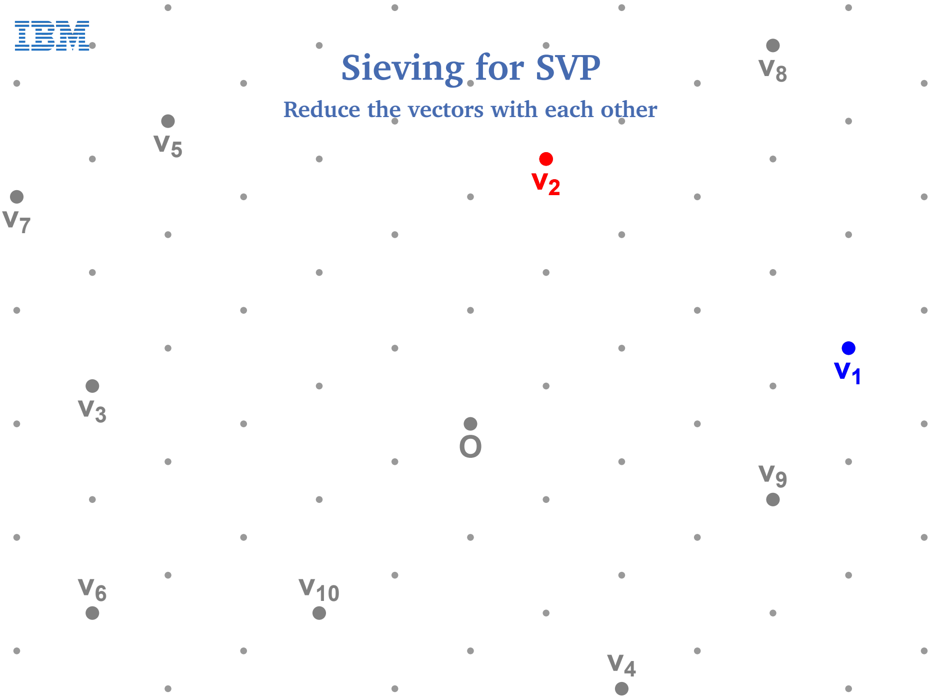
Sieving for SVP

Reduce the vectors with each other



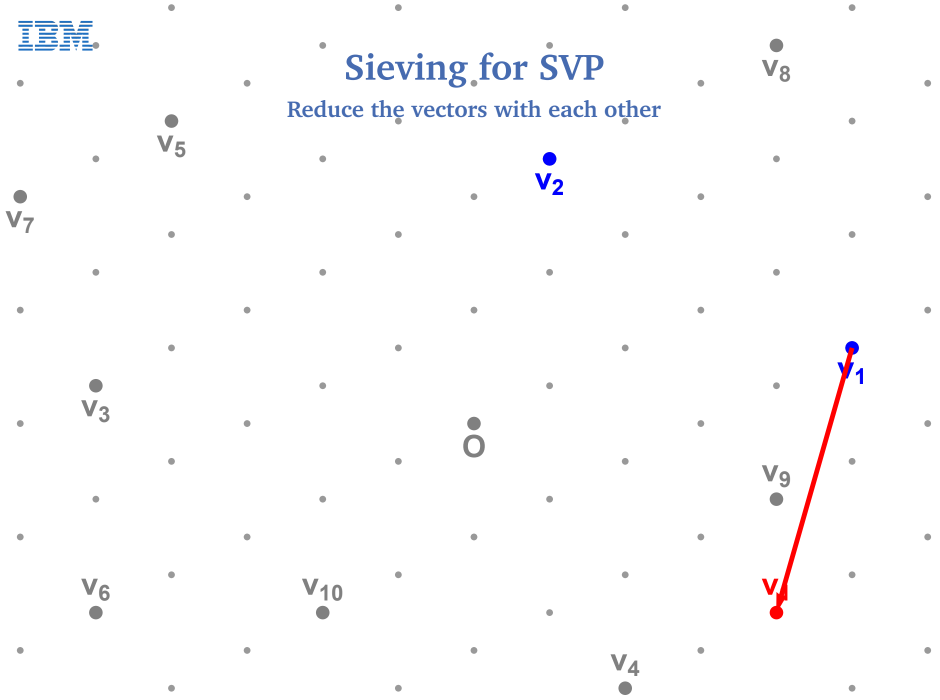
Sieving for SVP

Reduce the vectors with each other



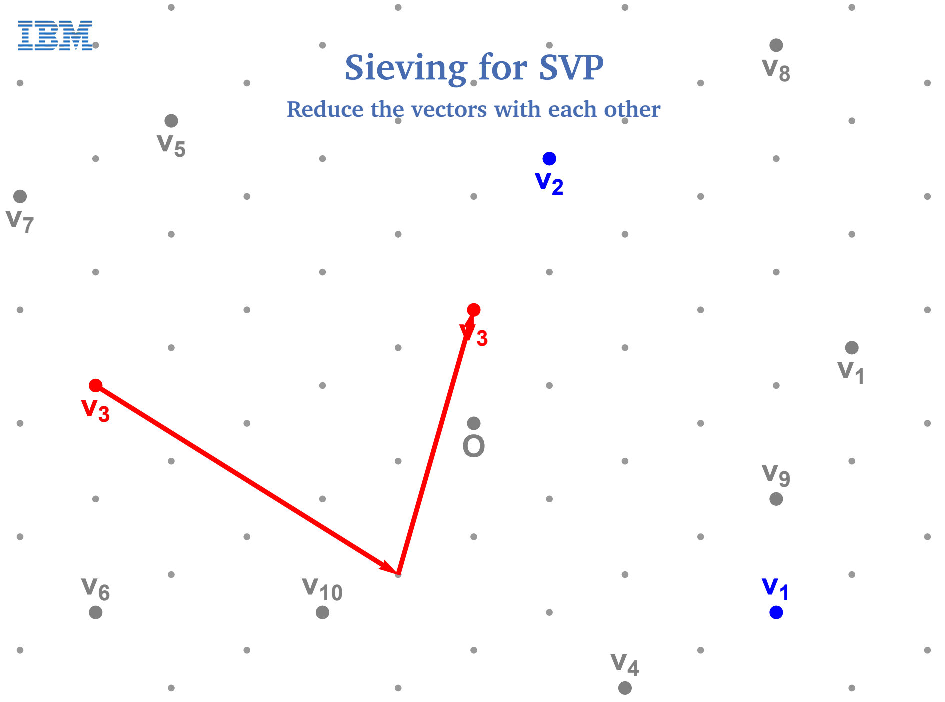
Sieving for SVP

Reduce the vectors with each other



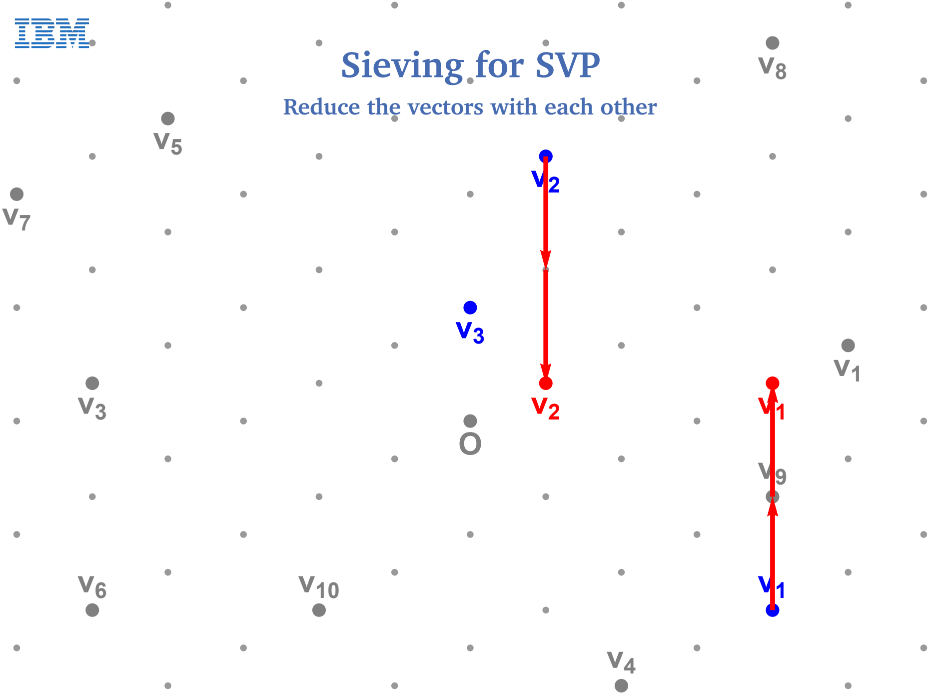
Sieving for SVP

Reduce the vectors with each other



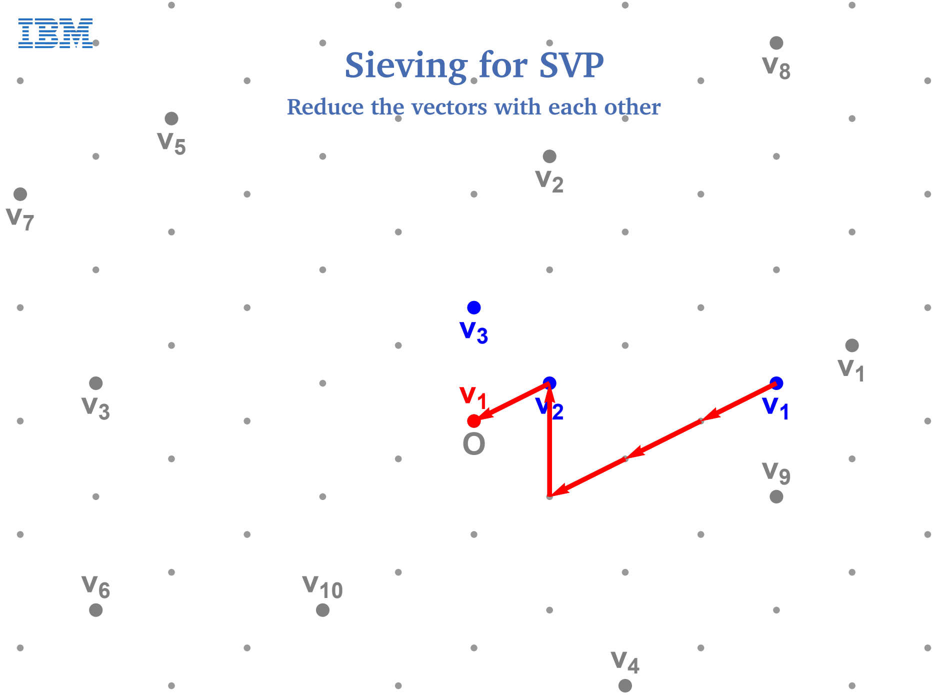
Sieving for SVP

Reduce the vectors with each other



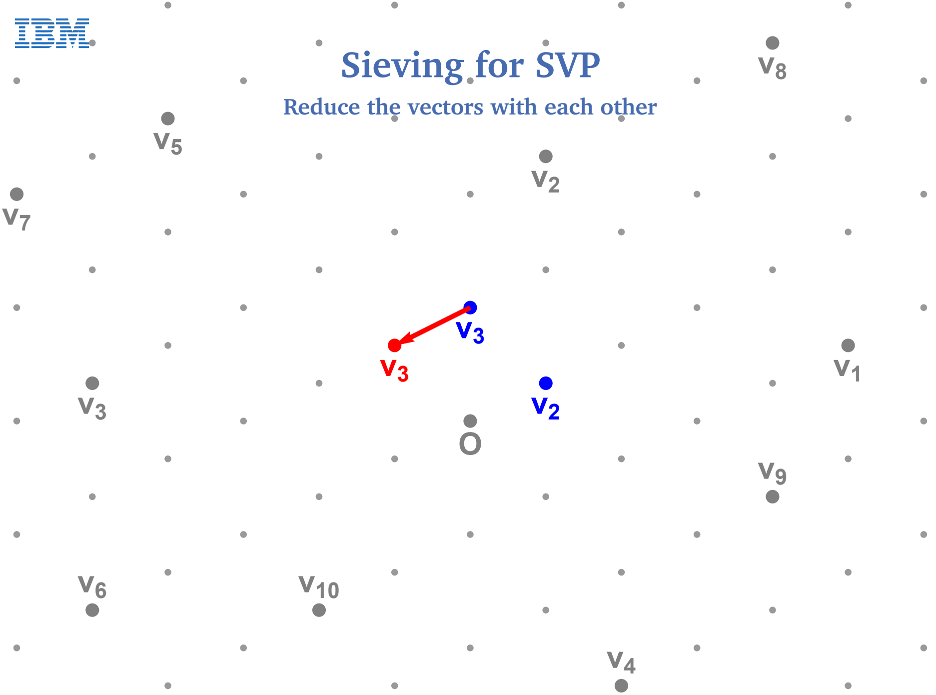
Sieving for SVP

Reduce the vectors with each other



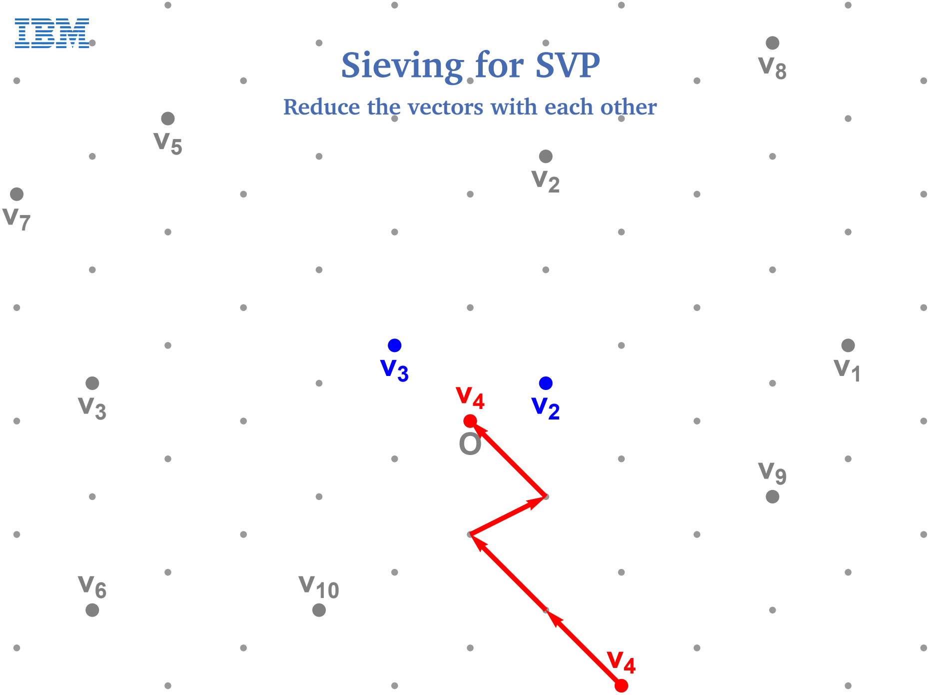
Sieving for SVP

Reduce the vectors with each other



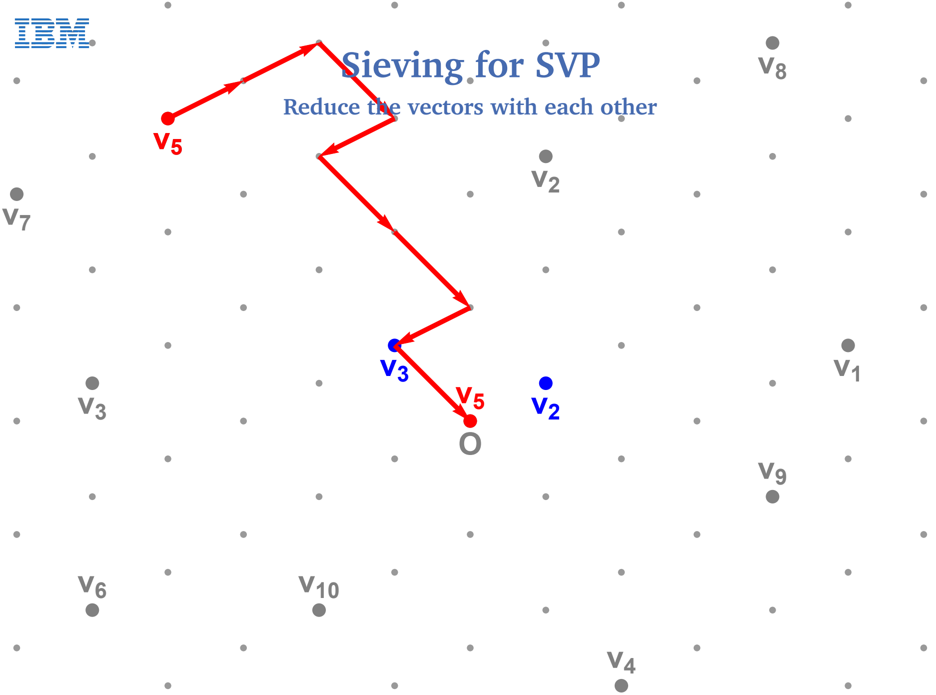
Sieving for SVP

Reduce the vectors with each other



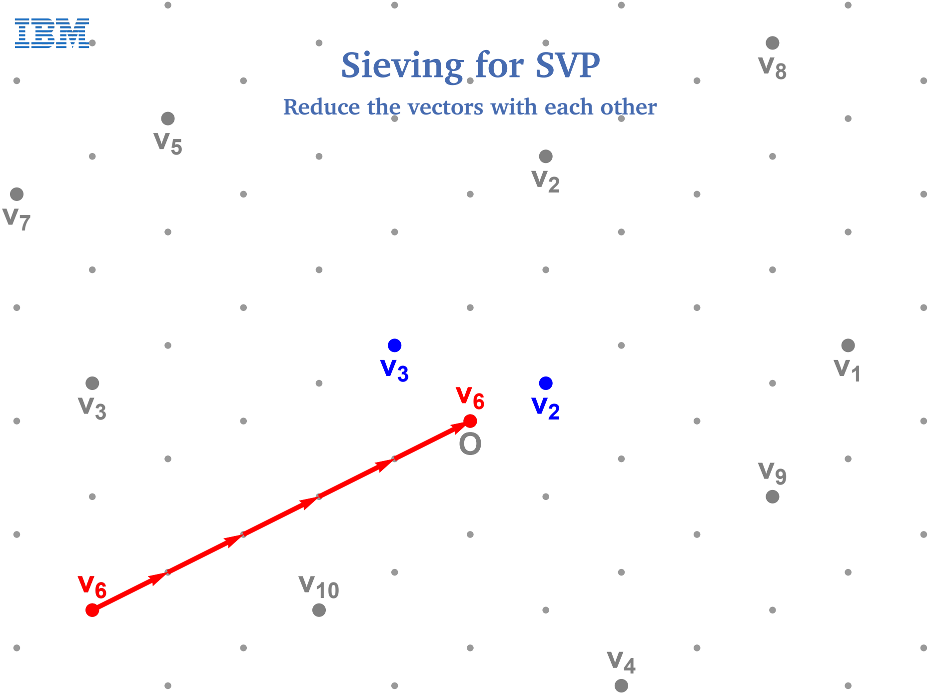
Sieving for SVP

Reduce the vectors with each other



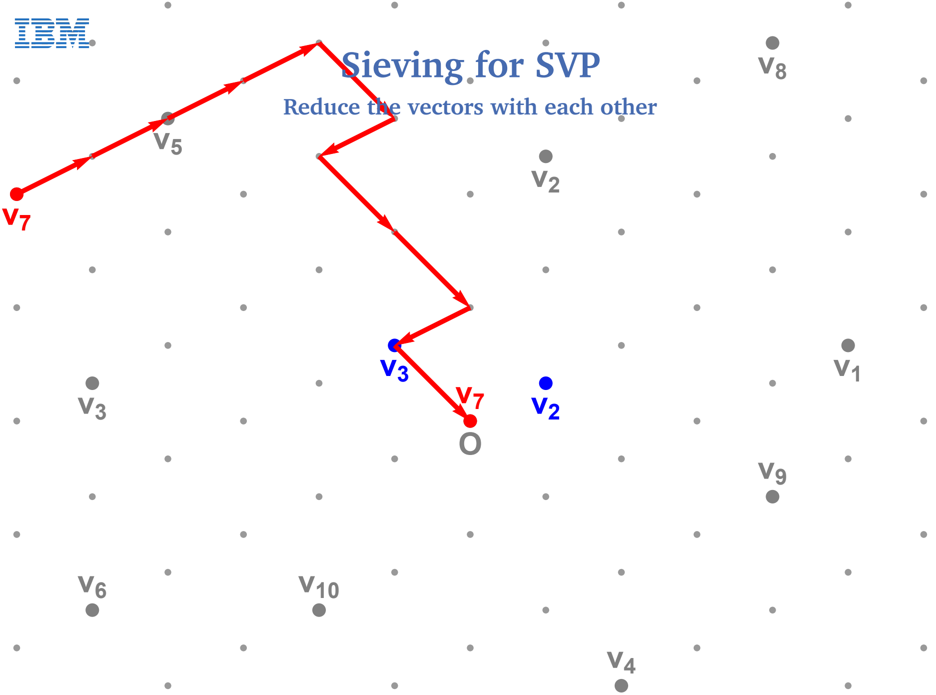
Sieving for SVP

Reduce the vectors with each other



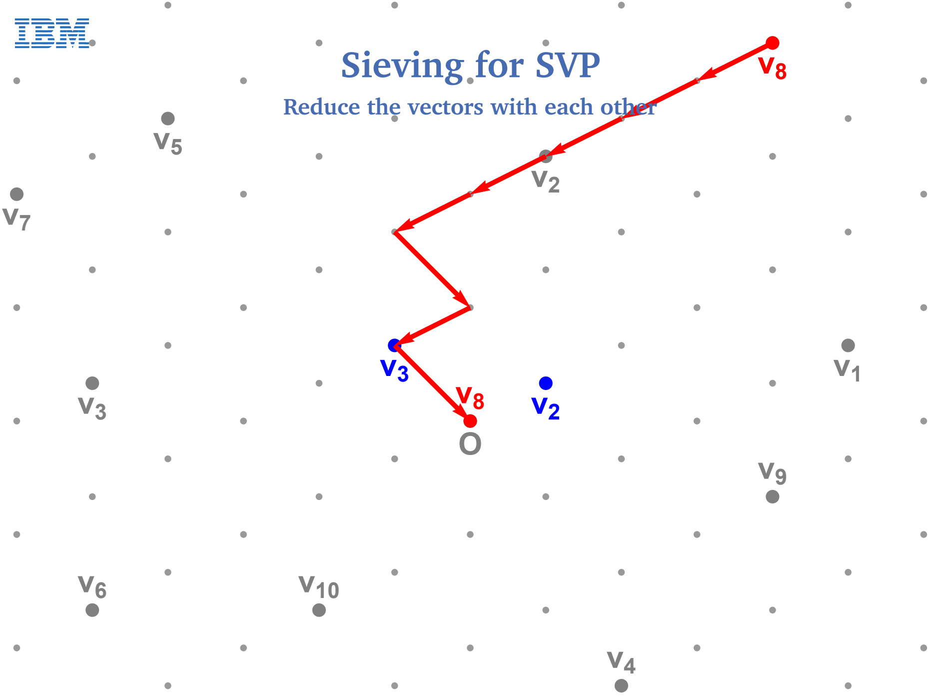
Sieving for SVP

Reduce the vectors with each other



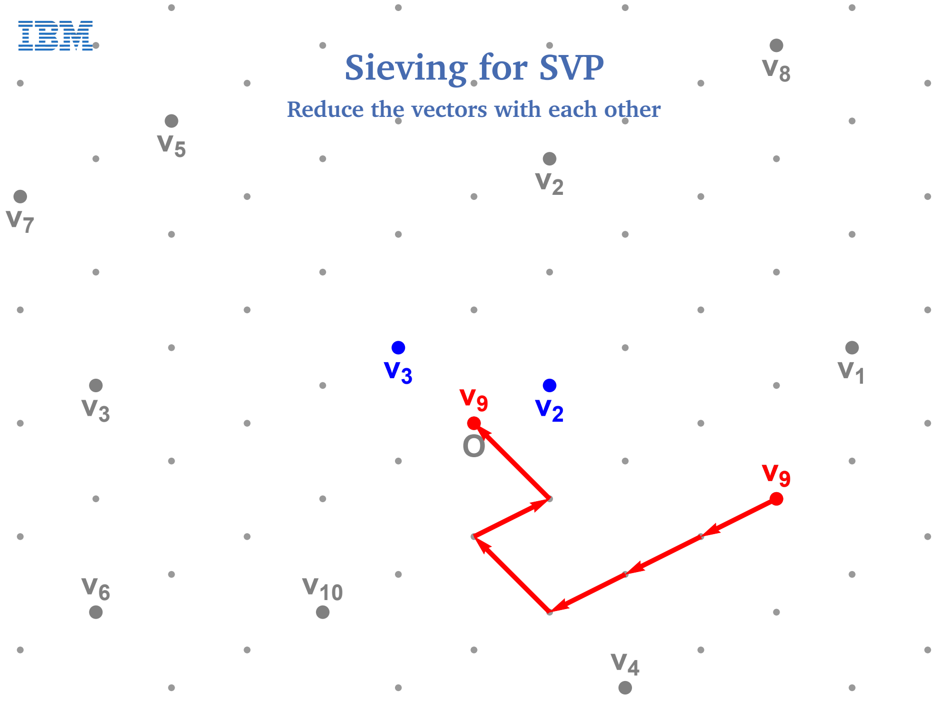
Sieving for SVP

Reduce the vectors with each other



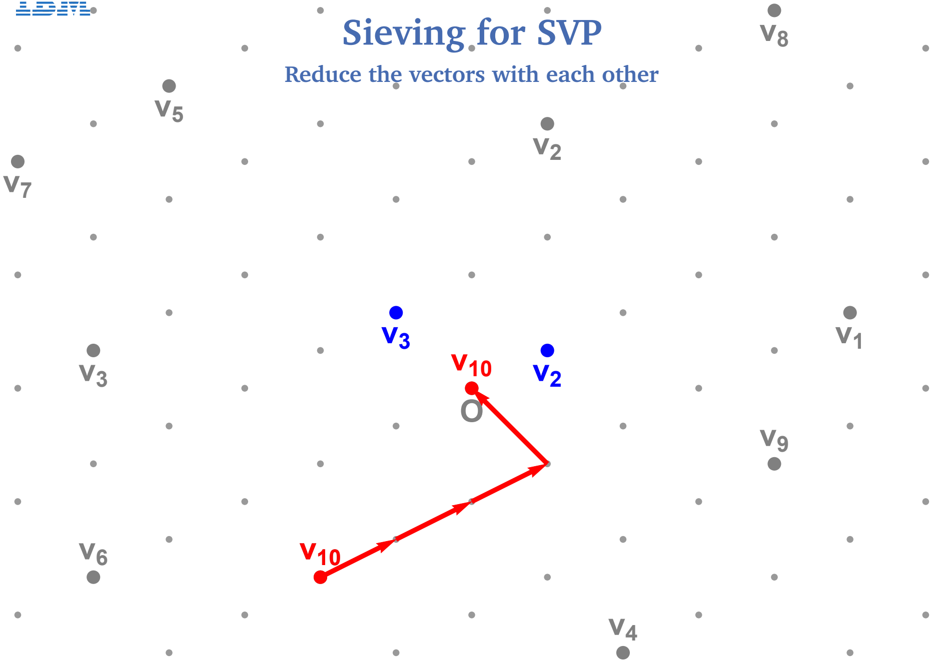
Sieving for SVP

Reduce the vectors with each other



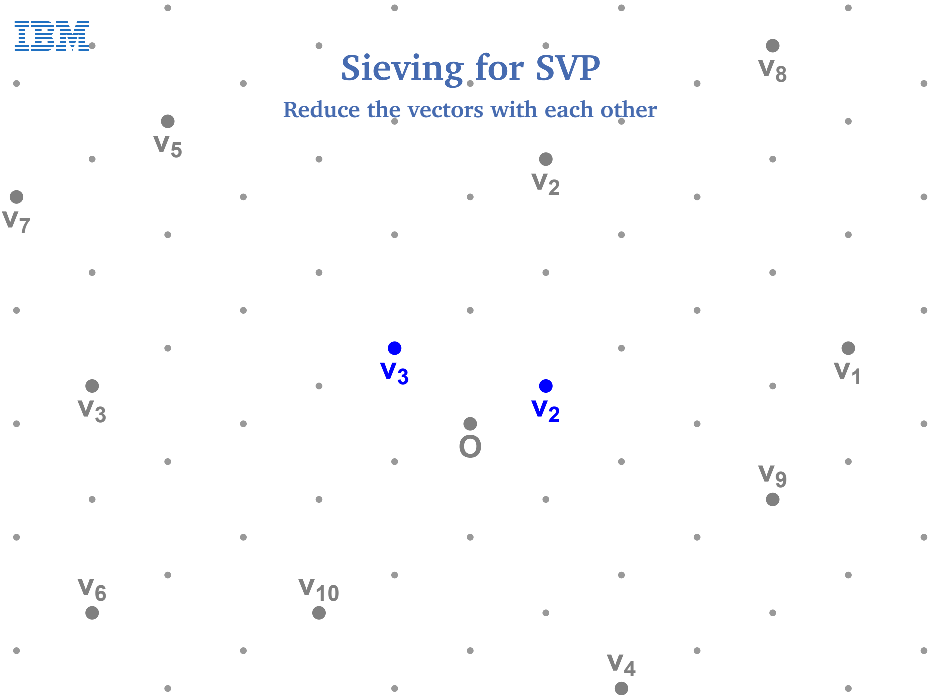
Sieving for SVP

Reduce the vectors with each other



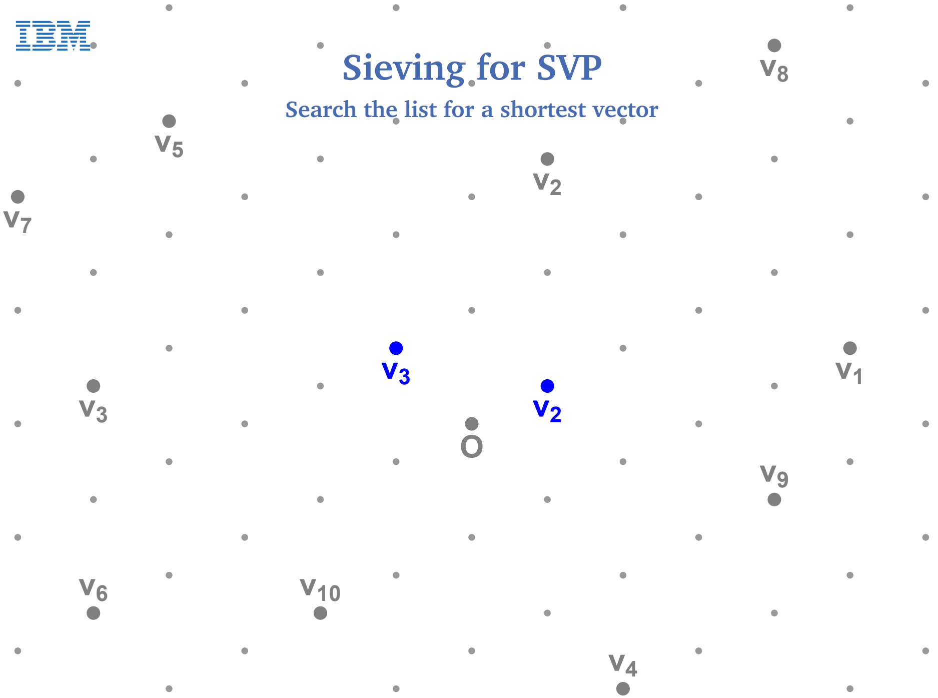
Sieving for SVP

Reduce the vectors with each other



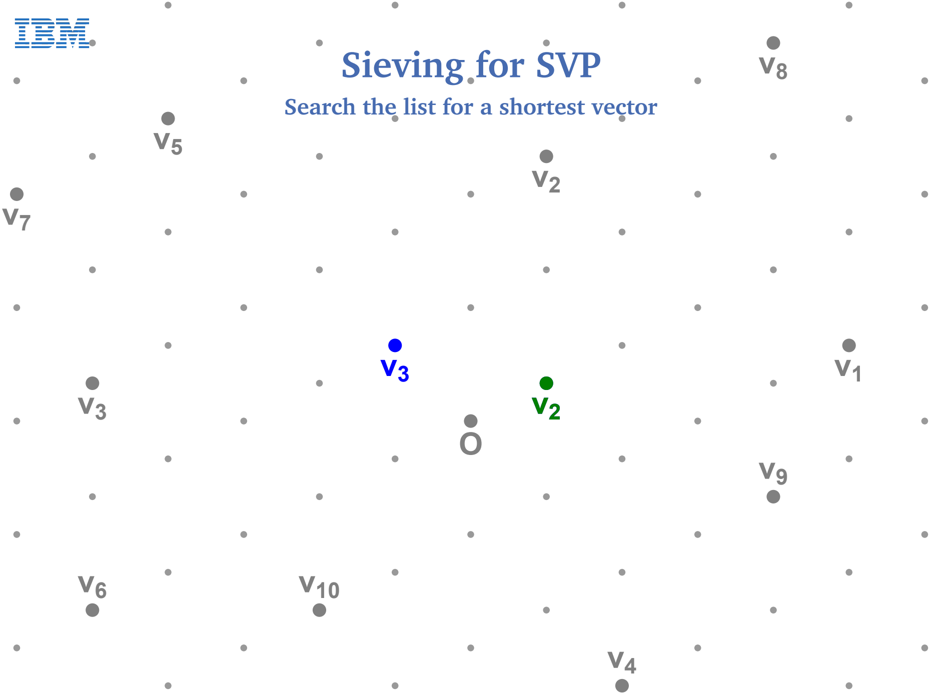
Sieving for SVP

Search the list for a shortest vector



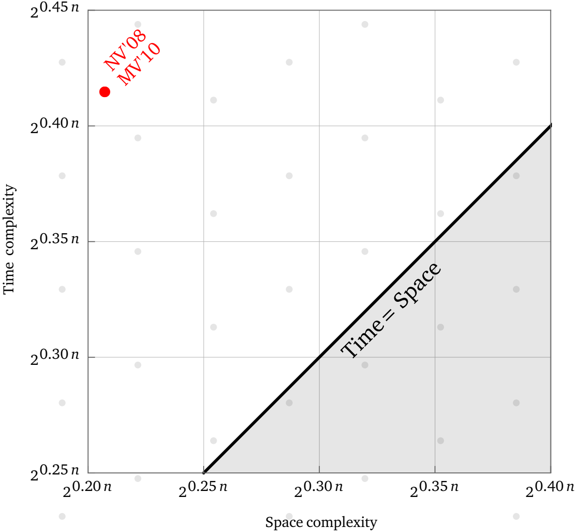
Sieving for SVP

Search the list for a shortest vector



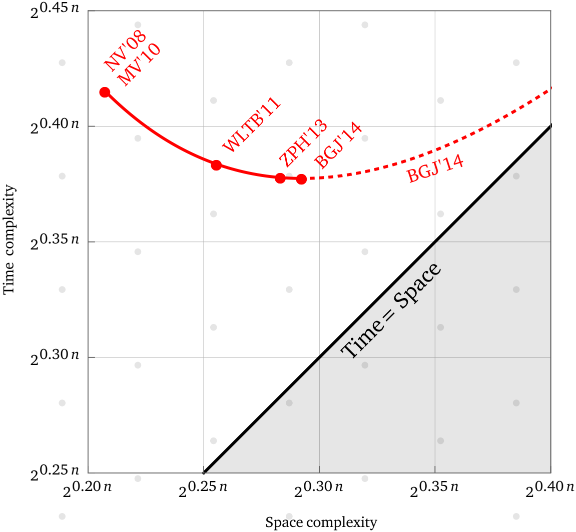
Sieving for SVP

The GaussSieve and Nguyen-Vidick sieve



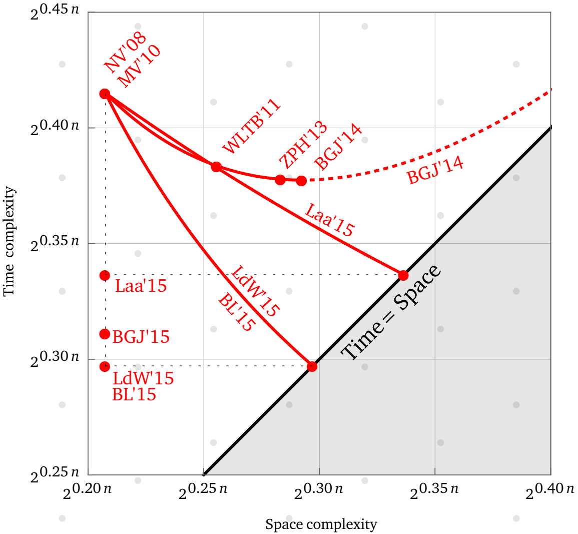
Sieving for SVP

Leveled sieving approaches



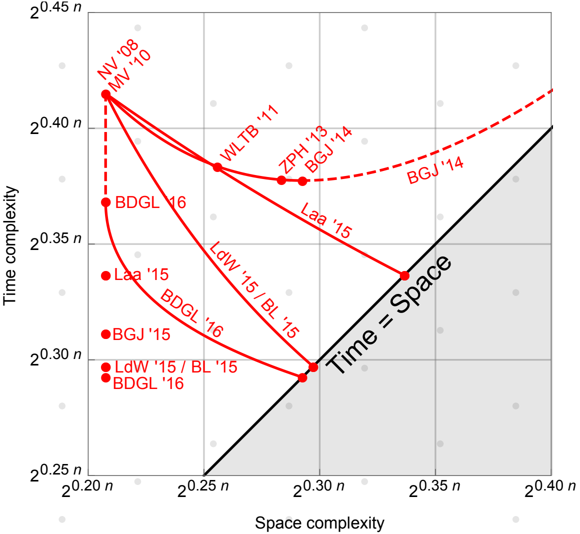
Sieving for SVP

Locality-Sensitive Hashing (LSH)



Sieving for SVP

Locality-Sensitive Filters (LSF)



Outline

Sieving for SVP

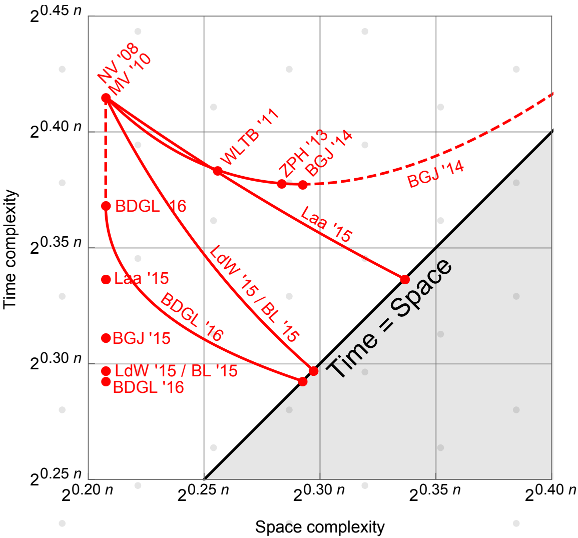
Sieving for CVP

Sieving for CVPP

Conclusion

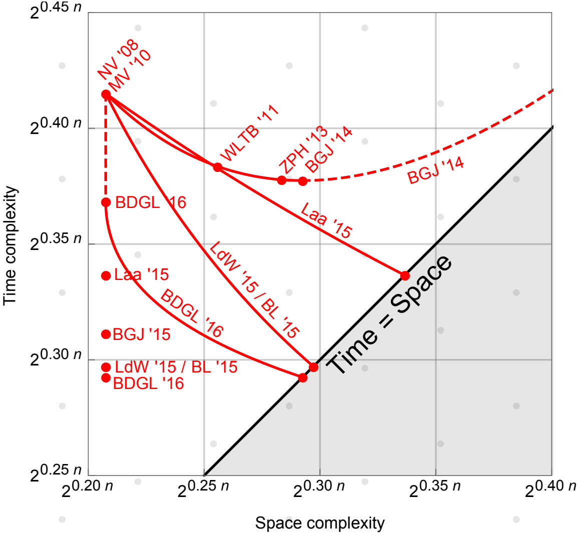
Sieving for SVP

Space/time trade-offs



Sieving for CVP

Space/time trade-offs



Outline

Sieving for SVP

Sieving for CVP

Sieving for CVPP

Conclusion

Sieving for CVPP

Run a GaussSieve as preprocessing

Sieving for CVPP

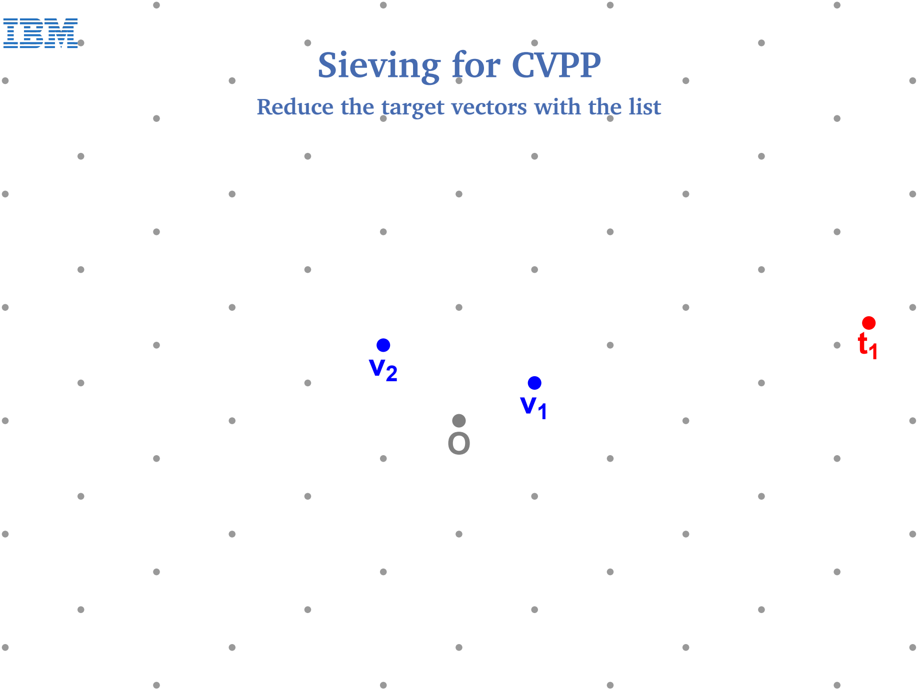
Run a GaussSieve as preprocessing

Sieving for CVPP

Reduce the target vectors with the list

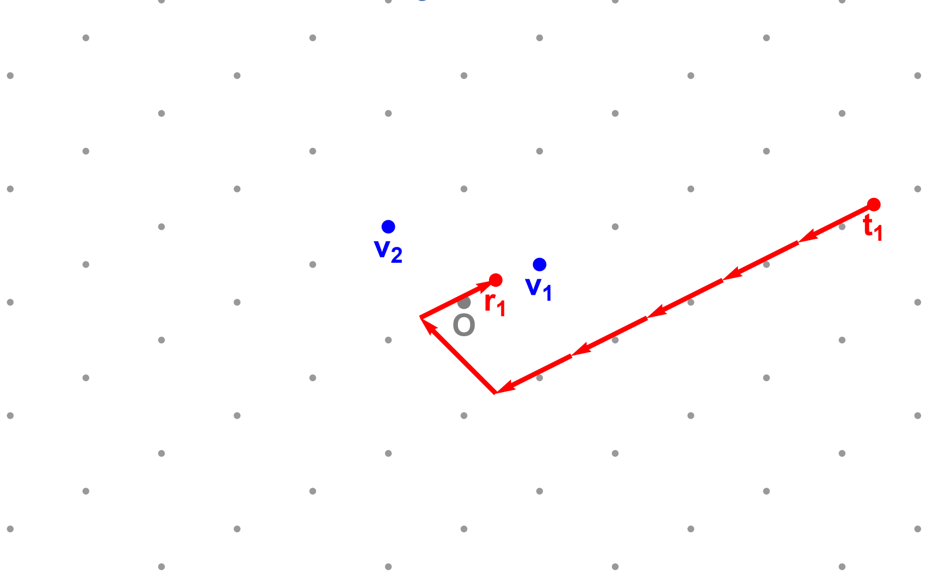
Sieving for CVPP

Reduce the target vectors with the list



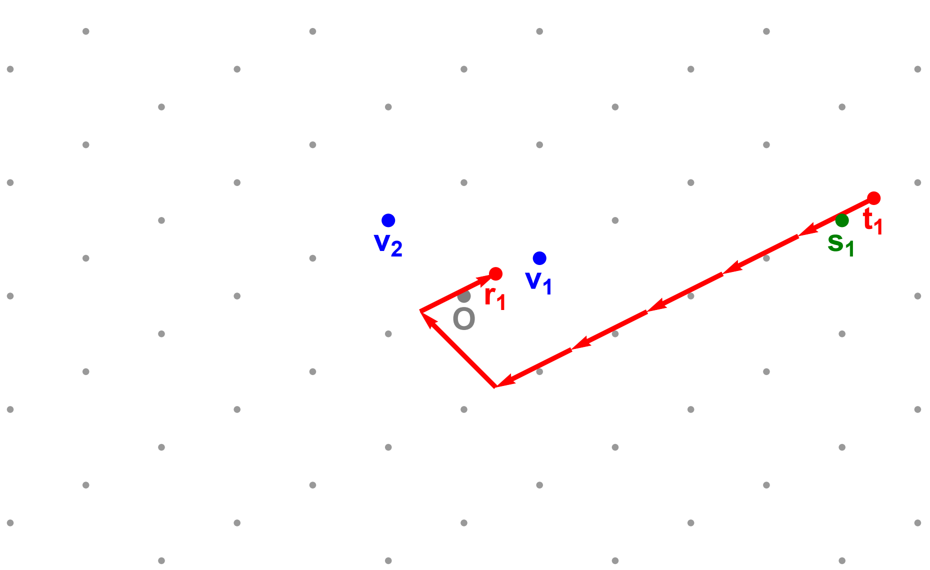
Sieving for CVPP

Reduce the target vectors with the list



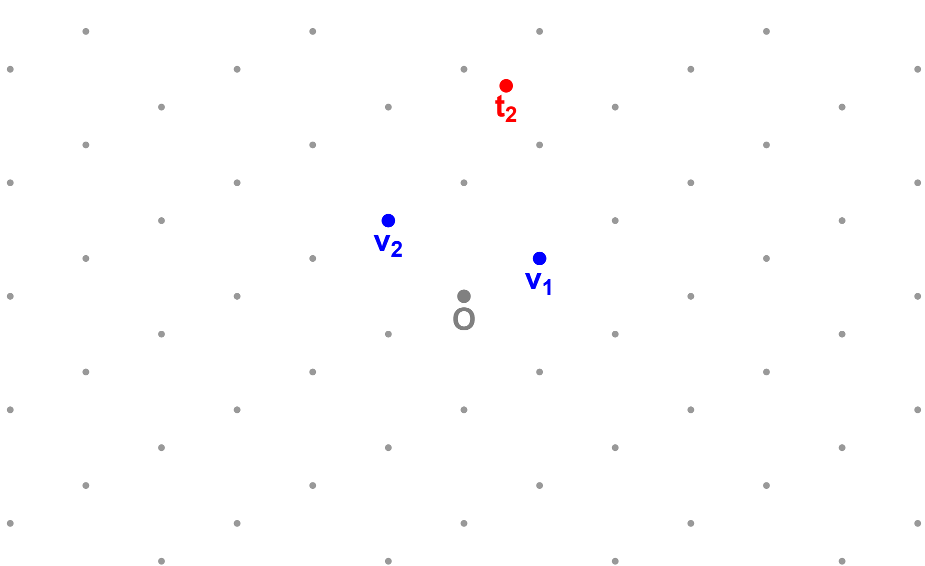
Sieving for CVPP

Reduce the target vectors with the list



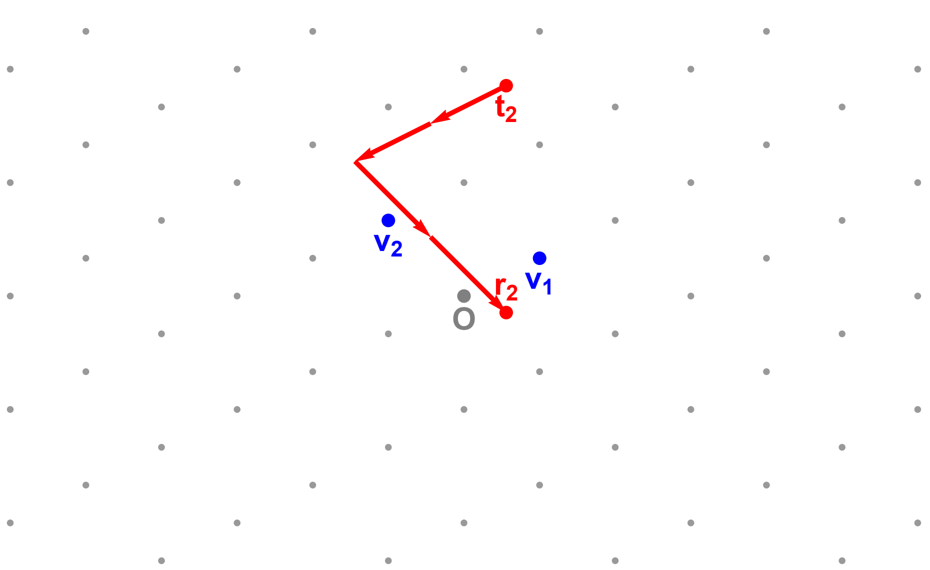
Sieving for CVPP

Reduce the target vectors with the list



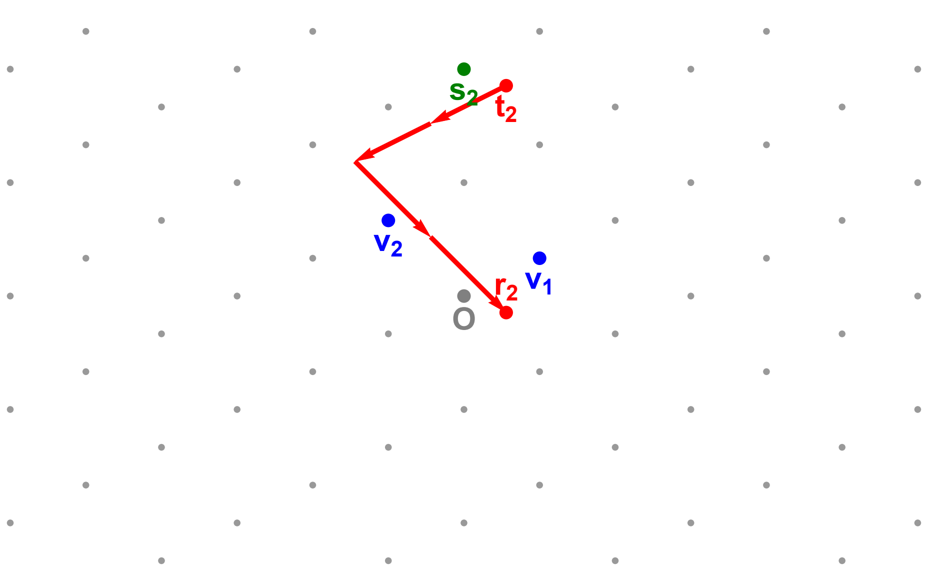
Sieving for CVPP

Reduce the target vectors with the list



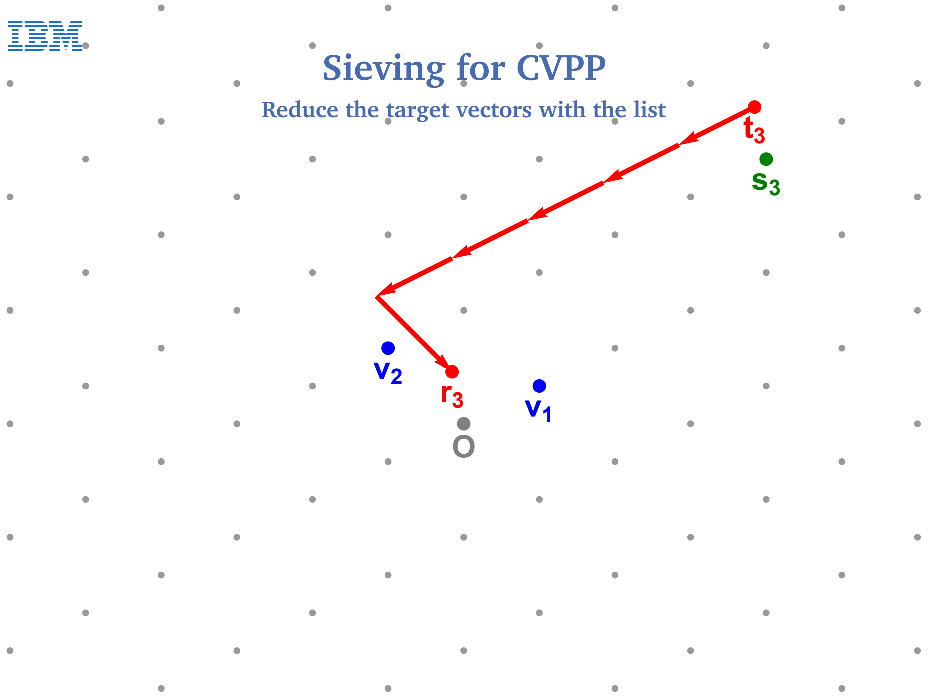
Sieving for CVPP

Reduce the target vectors with the list



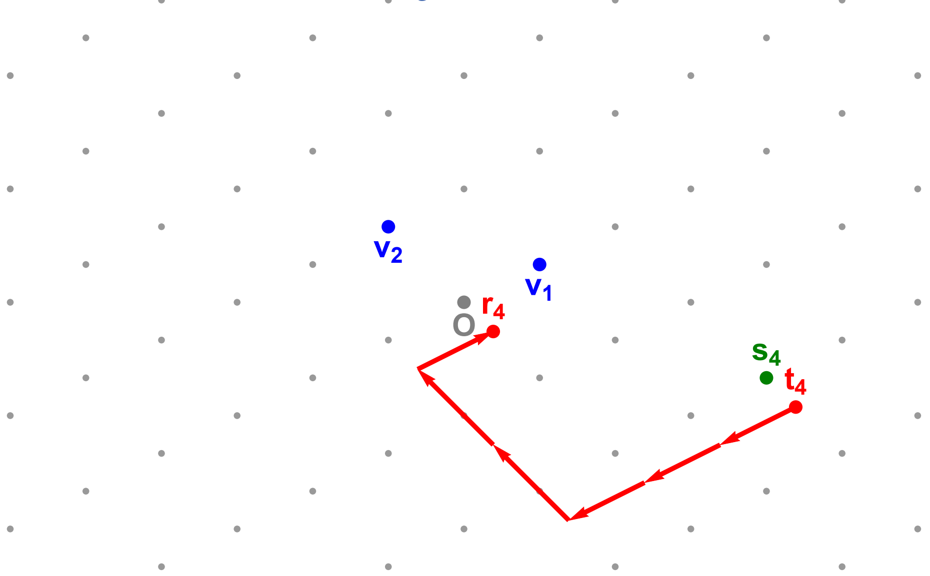
Sieving for CVPP

Reduce the target vectors with the list



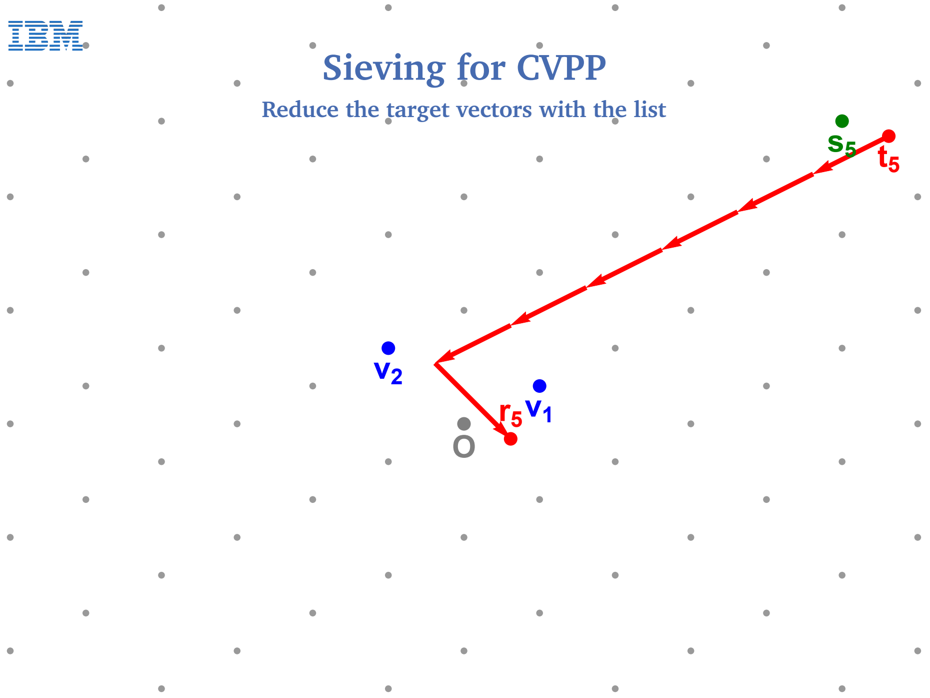
Sieving for CVPP

Reduce the target vectors with the list



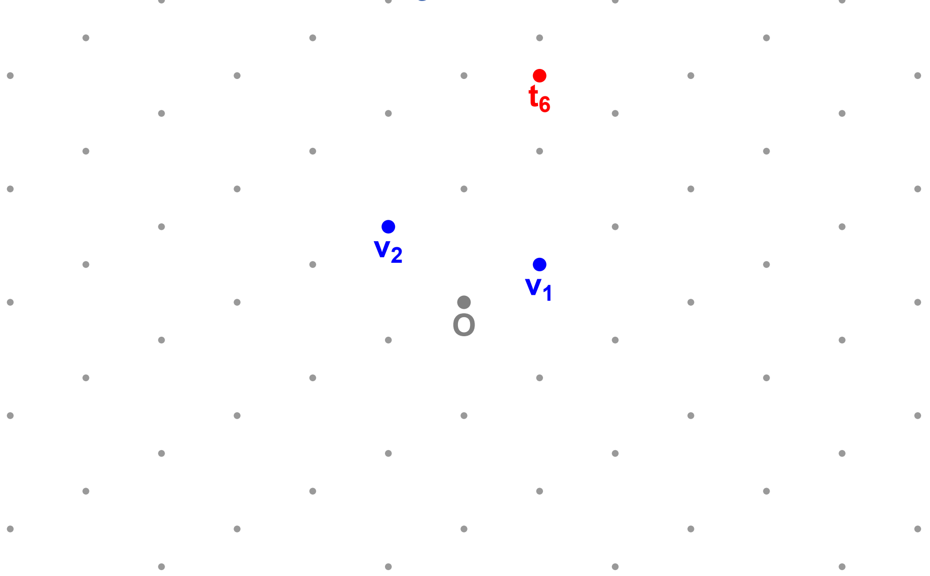
Sieving for CVPP

Reduce the target vectors with the list



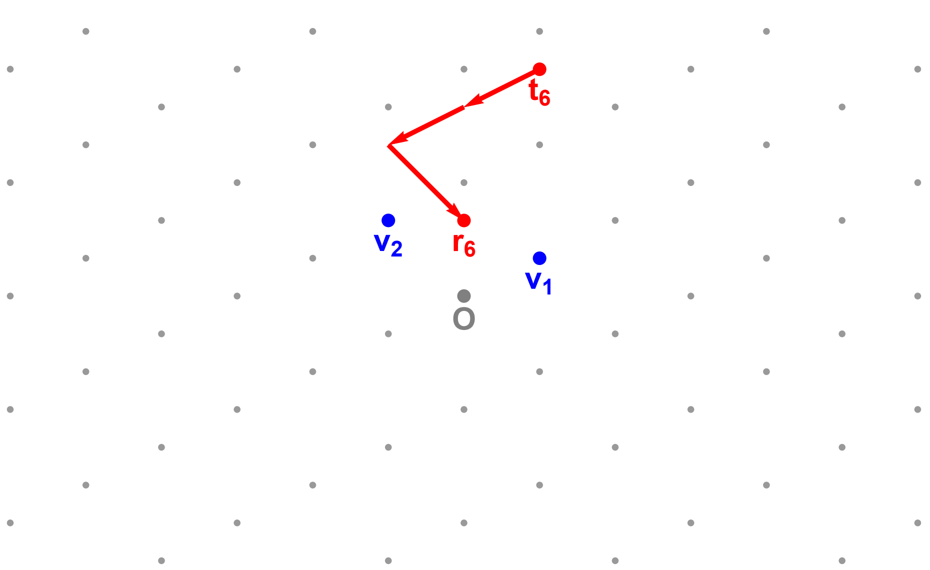
Sieving for CVPP

Reduce the target vectors with the list



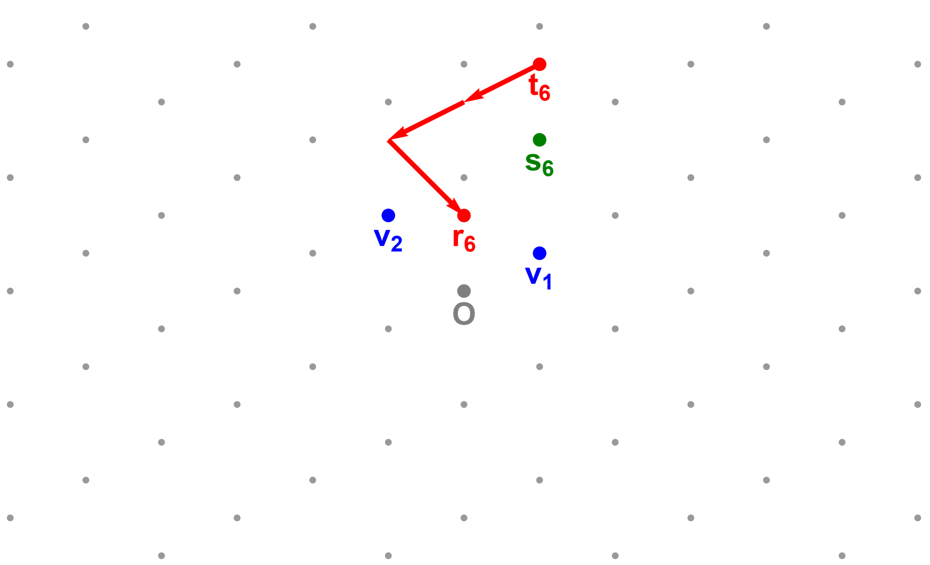
Sieving for CVPP

Reduce the target vectors with the list



Sieving for CVPP

Reduce the target vectors with the list

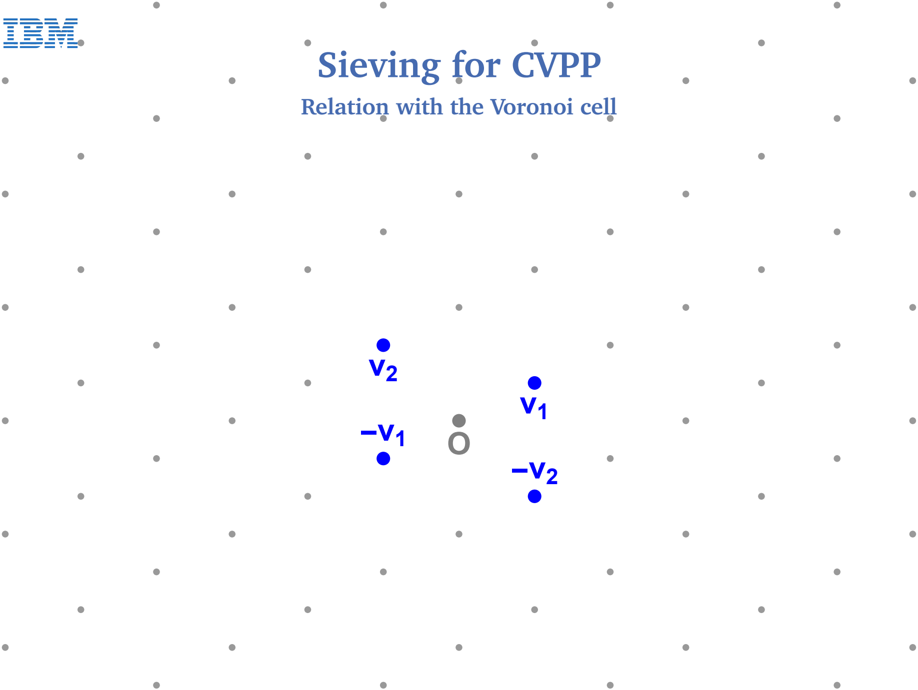


Sieving for CVPP

Relation with the Voronoi cell

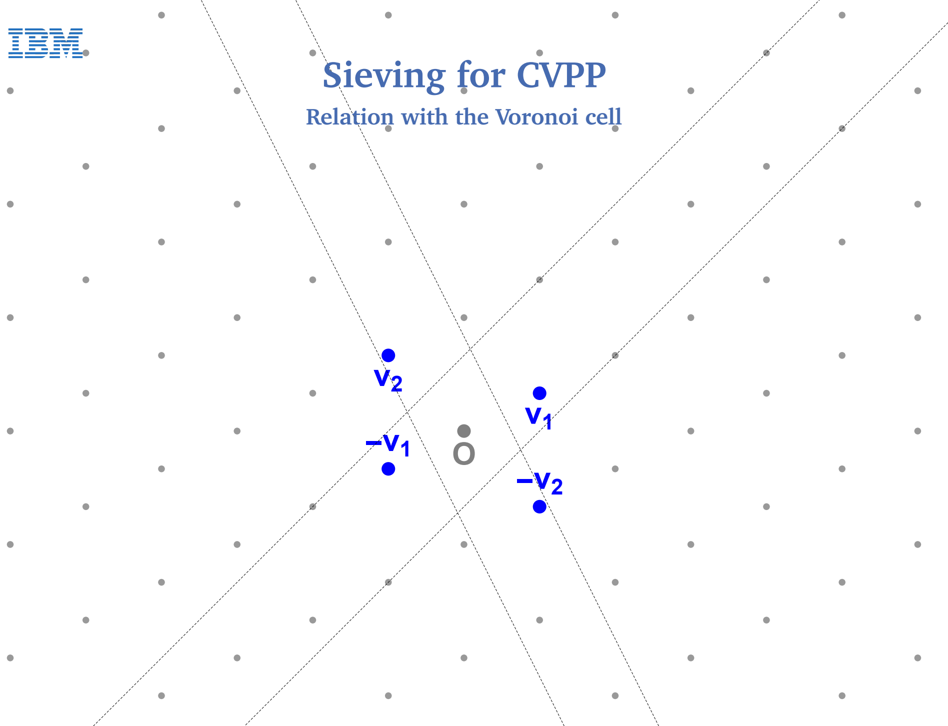
Sieving for CVPP

Relation with the Voronoi cell



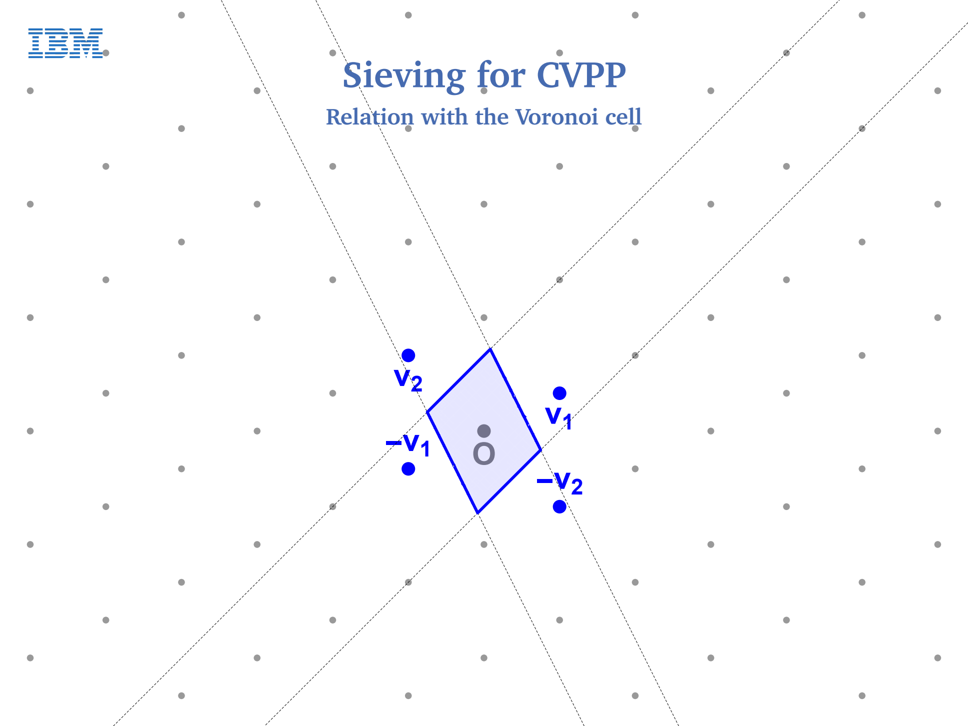
Sieving for CVPP

Relation with the Voronoi cell



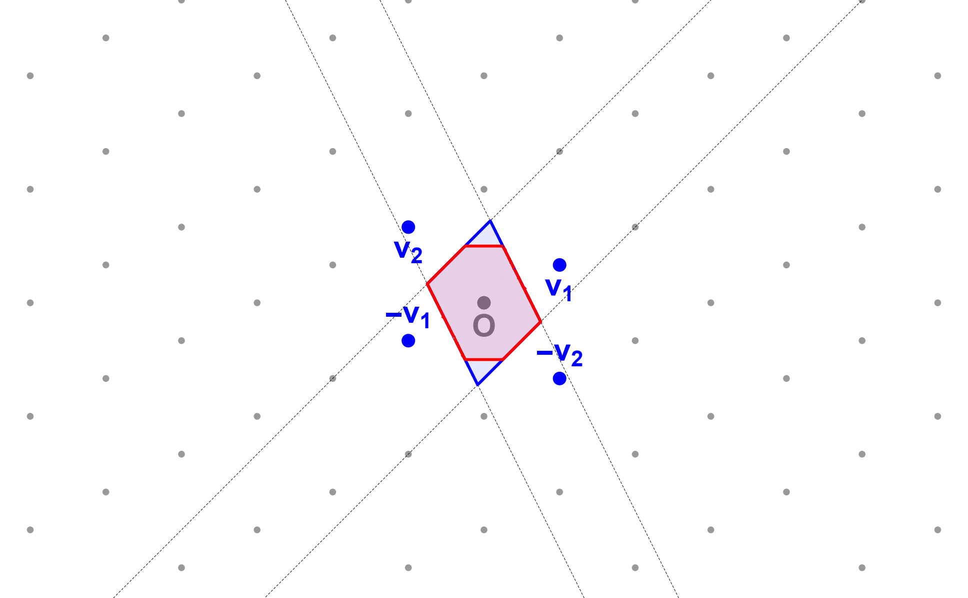
Sieving for CVPP

Relation with the Voronoi cell



Sieving for CVPP

Relation with the Voronoi cell



Sieving for CVPP

Overview

Sieving for CVPP

Overview

- Blue region: **Gauss cell** $\mathscr{G}$

Sieving for CVPP

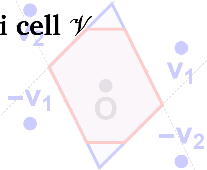
Overview

- Blue region: **Gauss cell** $\mathscr{G}$
  - Defined by $2^{0.21n+o(n)}$ short lattice vectors
  - Volume: $\mathrm{Vol}(\mathscr{G}) = 2^{O(n)} \cdot \det(\mathscr{L})$
  - Reductions always land in $\mathscr{G}$

Sieving for CVPP

Overview

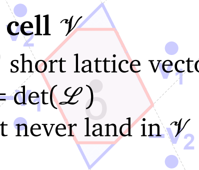
- Blue region: **Gauss cell** $\mathscr{G}$
  - Defined by $2^{0.21n+o(n)}$ short lattice vectors
  - Volume: $\mathrm{Vol}(\mathscr{G}) = 2^{O(n)} \cdot \det(\mathscr{L})$
  - Reductions always land in $\mathscr{G}$
- Red region: **Voronoi cell** $\mathscr{V}$



Sieving for CVPP

Overview

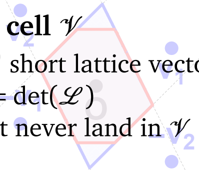
- Blue region: **Gauss cell** $\mathscr{G}$
  - Defined by $2^{0.21n+o(n)}$ short lattice vectors
  - Volume: $\mathrm{Vol}(\mathscr{G}) = 2^{O(n)} \cdot \det(\mathscr{L})$
  - Reductions always land in $\mathscr{G}$
- Red region: **Voronoi cell** $\mathscr{V}$
  - Defined by $2^{n+o(n)}$ short lattice vectors
  - Volume: $\mathrm{Vol}(\mathscr{V}) = \det(\mathscr{L})$
  - Reductions almost never land in $\mathscr{V}$



Sieving for CVPP

Overview

- Blue region: **Gauss cell** $\mathscr{G}$
  - Defined by $2^{0.21n+o(n)}$ short lattice vectors
  - Volume: $\mathrm{Vol}(\mathscr{G}) = 2^{O(n)} \cdot \det(\mathscr{L})$
  - Reductions always land in $\mathscr{G}$
- Red region: **Voronoi cell** $\mathscr{V}$
  - Defined by $2^{n+o(n)}$ short lattice vectors
  - Volume: $\mathrm{Vol}(\mathscr{V}) = \det(\mathscr{L})$
  - Reductions almost never land in $\mathscr{V}$
- Problems:



Sieving for CVPP

Overview

- Blue region: **Gauss cell** $\mathscr{G}$
  - Defined by $2^{0.21n+o(n)}$ short lattice vectors
  - Volume: $\mathrm{Vol}(\mathscr{G}) = 2^{O(n)} \cdot \det(\mathscr{L})$
  - Reductions always land in $\mathscr{G}$
- Red region: **Voronoi cell** $\mathscr{V}$
  - Defined by $2^{n+o(n)}$ short lattice vectors
  - Volume: $\mathrm{Vol}(\mathscr{V}) = \det(\mathscr{L})$
  - Reductions almost never land in $\mathscr{V}$
- Problems:
  - Exponentially small success probability $\mathrm{Vol}(\mathscr{V})/\mathrm{Vol}(\mathscr{G})$

Sieving for CVPP

Overview

- Blue region: **Gauss cell** $\mathscr{G}$
  - Defined by $2^{0.21n+o(n)}$ short lattice vectors
  - Volume: $\mathrm{Vol}(\mathscr{G}) = 2^{O(n)} \cdot \det(\mathscr{L})$
  - Reductions always land in $\mathscr{G}$
- Red region: **Voronoi cell** $\mathscr{V}$
  - Defined by $2^{n+o(n)}$ short lattice vectors
  - Volume: $\mathrm{Vol}(\mathscr{V}) = \det(\mathscr{L})$
  - Reductions almost never land in $\mathscr{V}$
- Problems:
  - Exponentially small success probability $\mathrm{Vol}(\mathscr{V})/\mathrm{Vol}(\mathscr{G})$
  - Probability only over randomness of targets

Sieving for CVPP

Solving the problems

- Idea 1: **Larger lists, weaker reductions**

Sieving for CVPP

Solving the problems

- Idea 1: **Larger lists, weaker reductions**
  - Problem: Exponentially small success probability

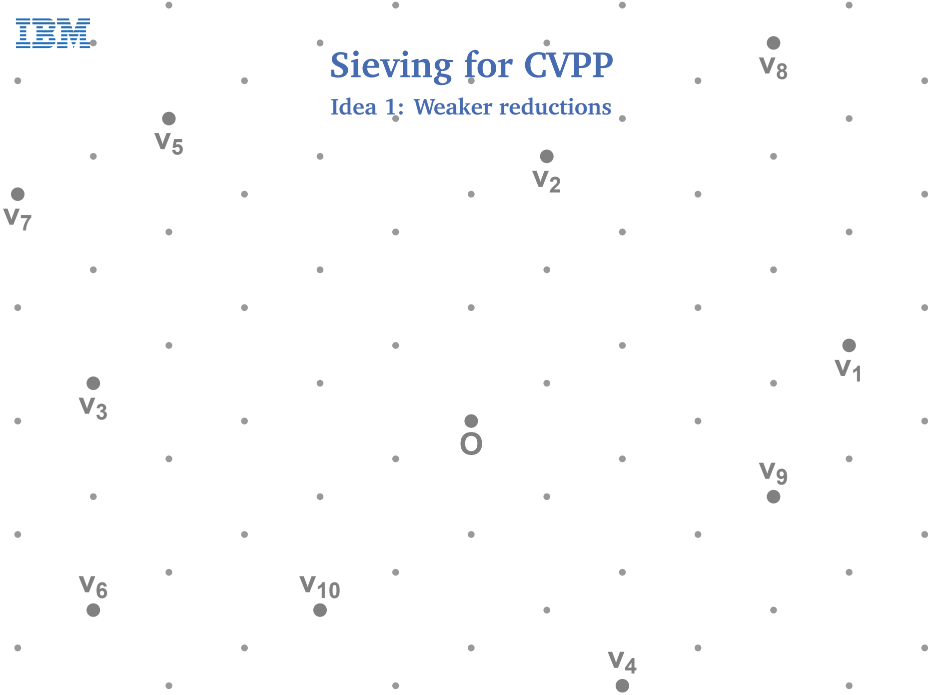
Sieving for CVPP

Solving the problems

- Idea 1: **Larger lists, weaker reductions**
  - Problem: Exponentially small success probability
  - To guarantee $\mathrm{Vol}(\mathscr{G}) \approx \mathrm{Vol}(\mathscr{V})$, need $2^{n/2+o(n)}$ vectors
  - Preprocessing: reduce $\boldsymbol{v}_1$ with $\boldsymbol{v}_2$ iff $\|\boldsymbol{v}_1 - \boldsymbol{v}_2\| \ll \|\boldsymbol{v}_1\|$

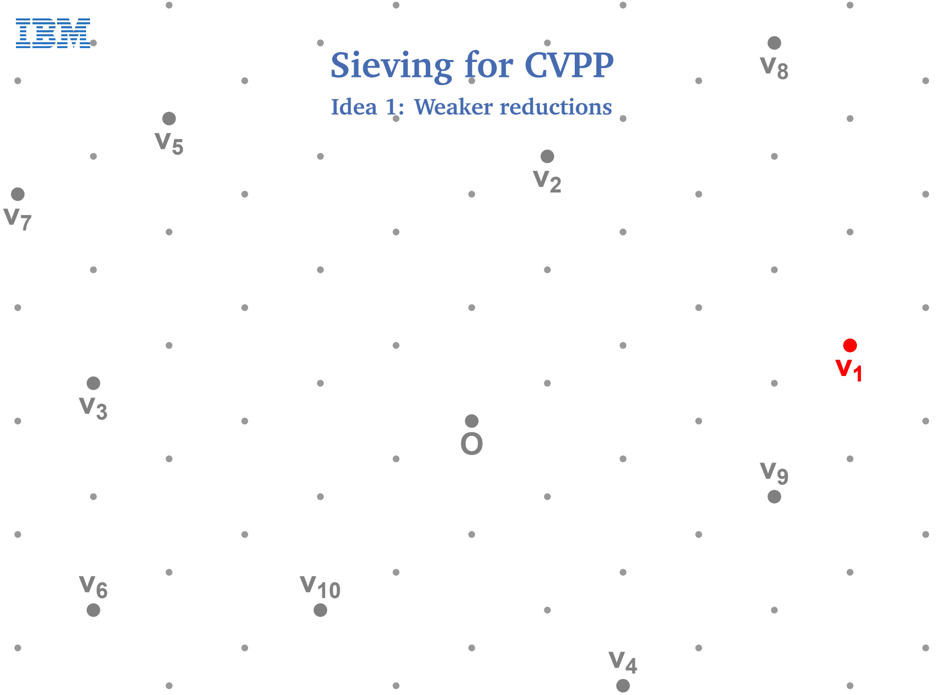
Sieving for CVPP

Idea 1: Weaker reductions



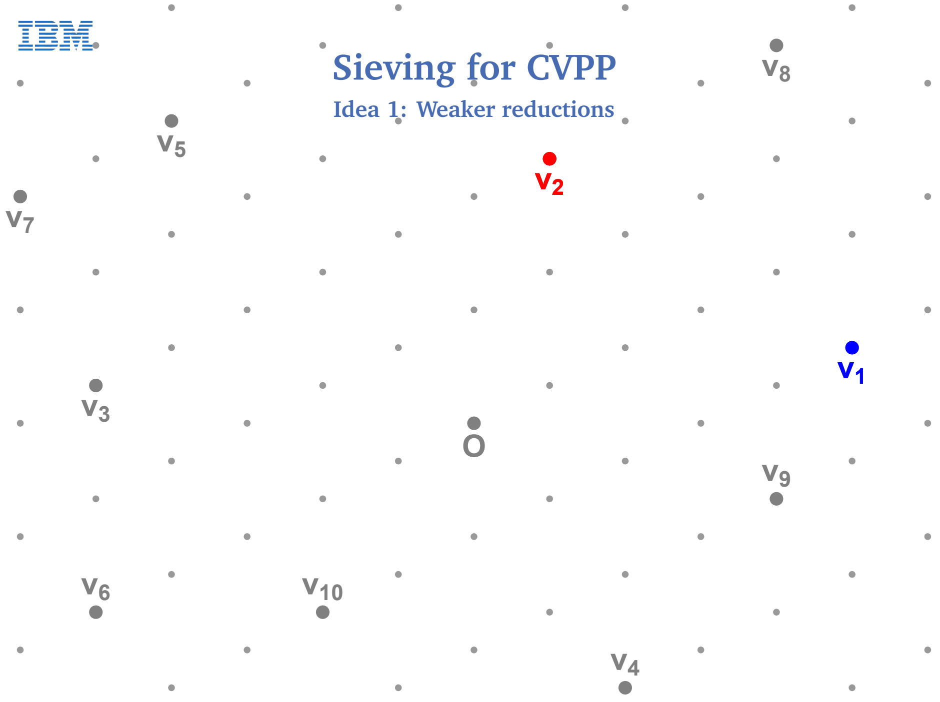
Sieving for CVPP

Idea 1: Weaker reductions



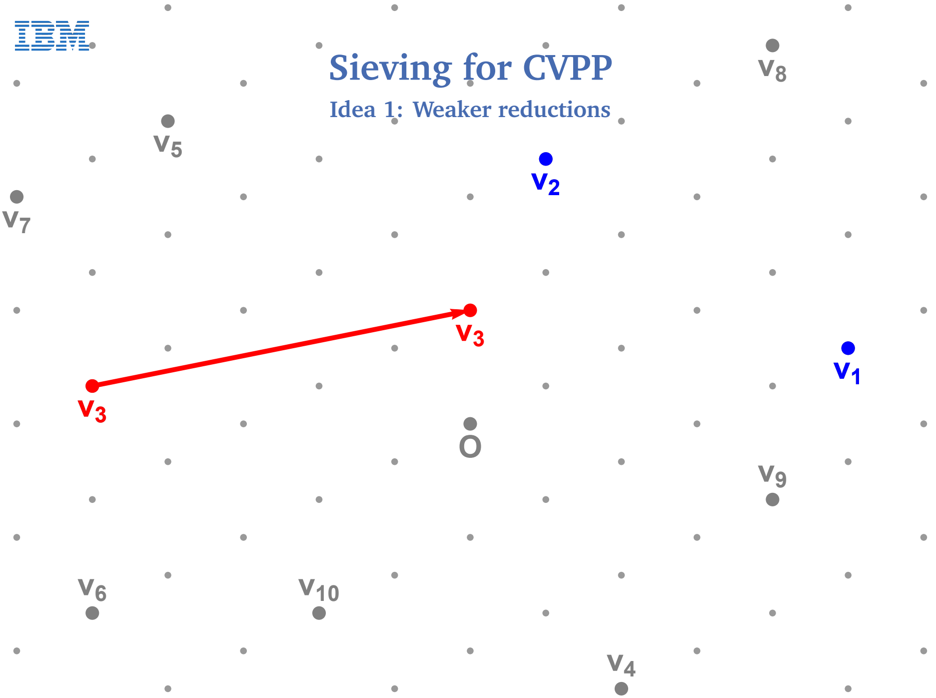
Sieving for CVPP

Idea 1: Weaker reductions



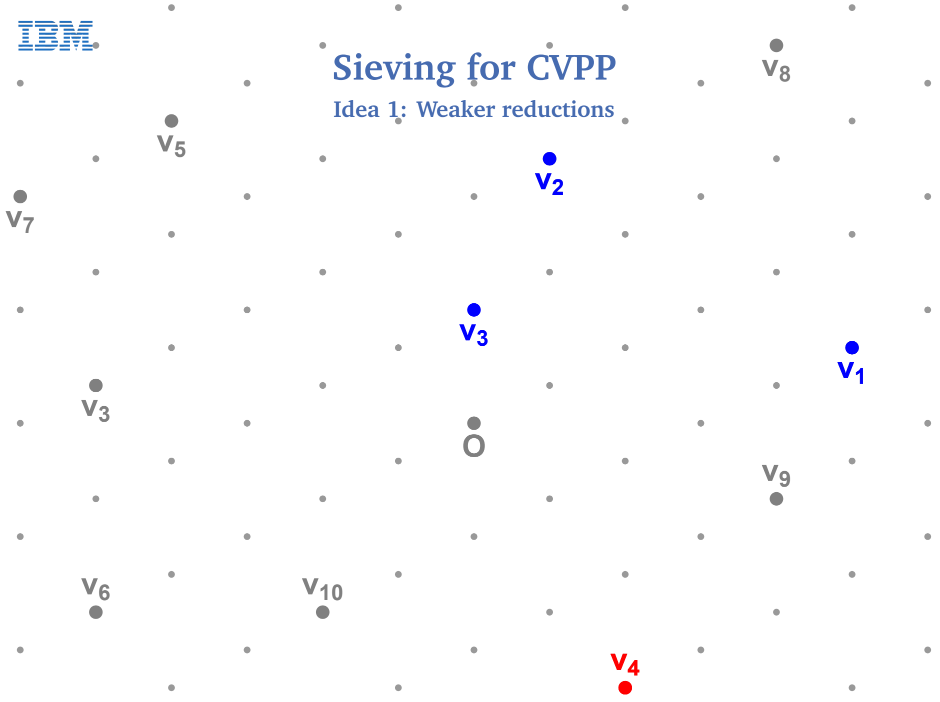
Sieving for CVPP

Idea 1: Weaker reductions



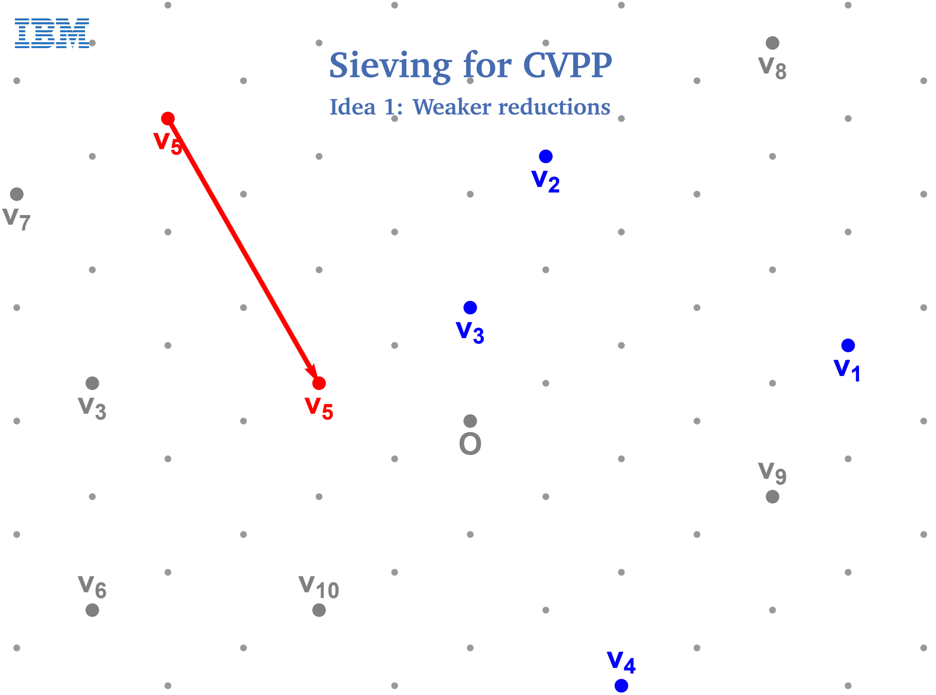
Sieving for CVPP

Idea 1: Weaker reductions



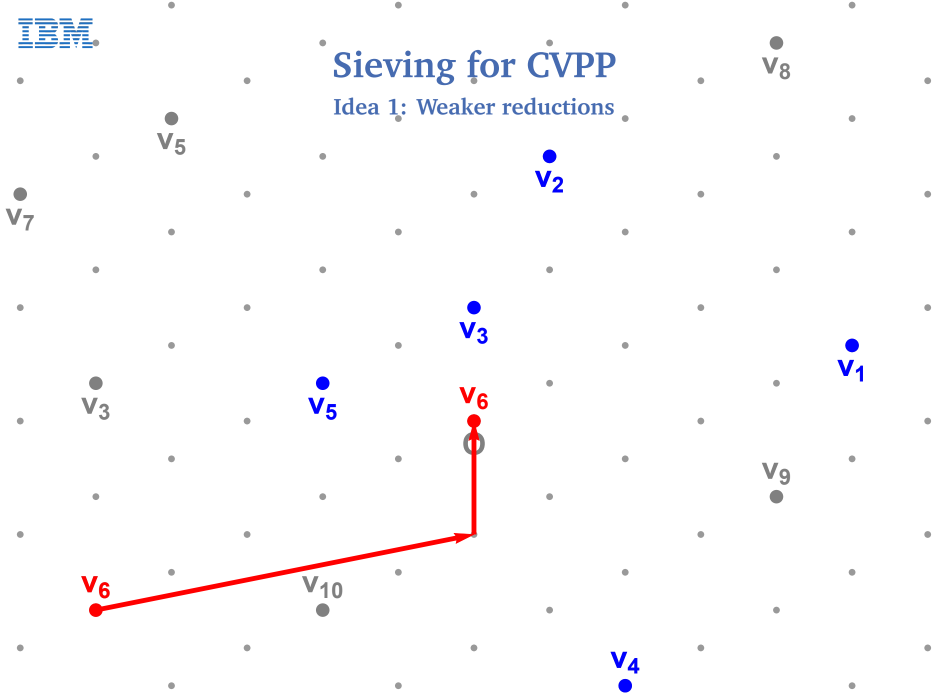
Sieving for CVPP

Idea 1: Weaker reductions



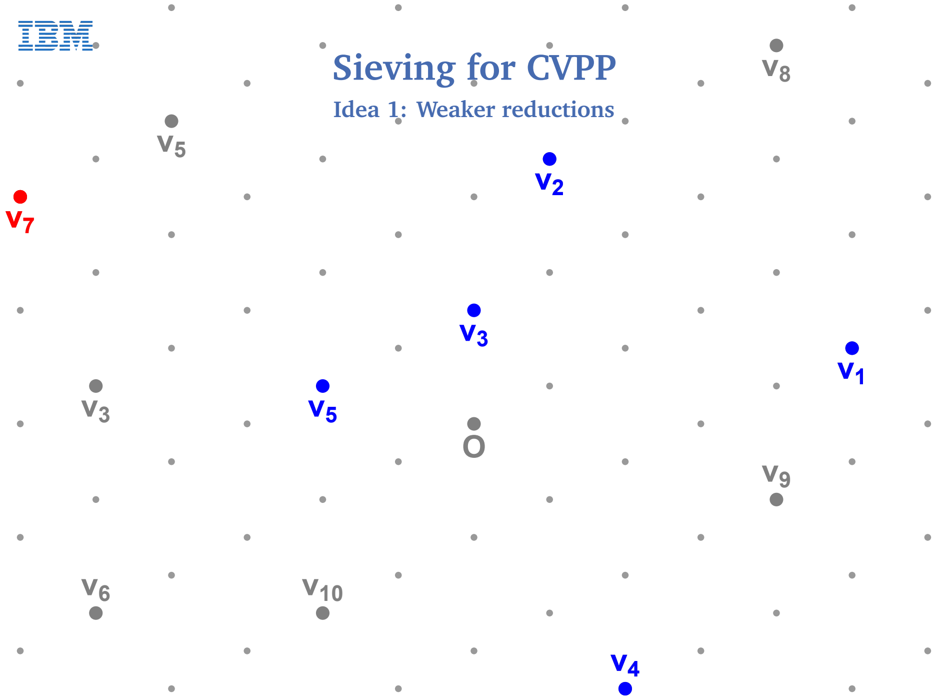
Sieving for CVPP

Idea 1: Weaker reductions



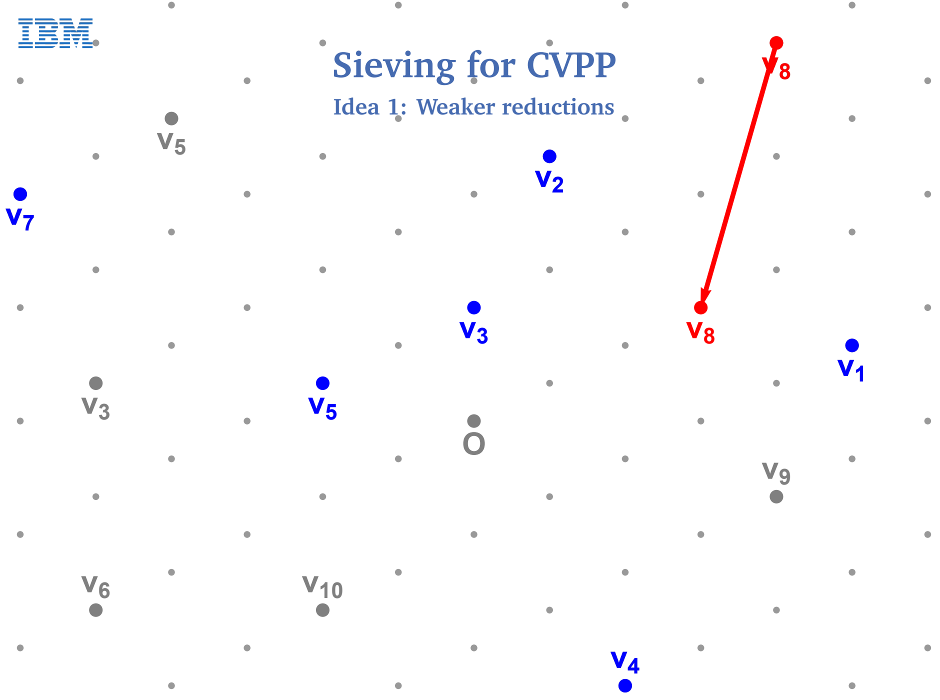
Sieving for CVPP

Idea 1: Weaker reductions



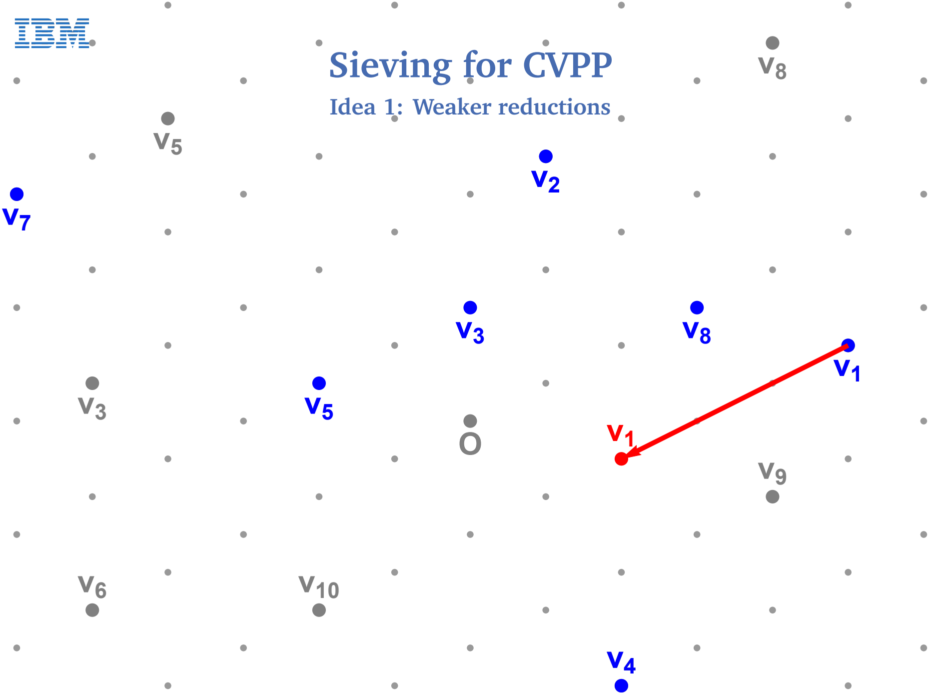
Sieving for CVPP

Idea 1: Weaker reductions



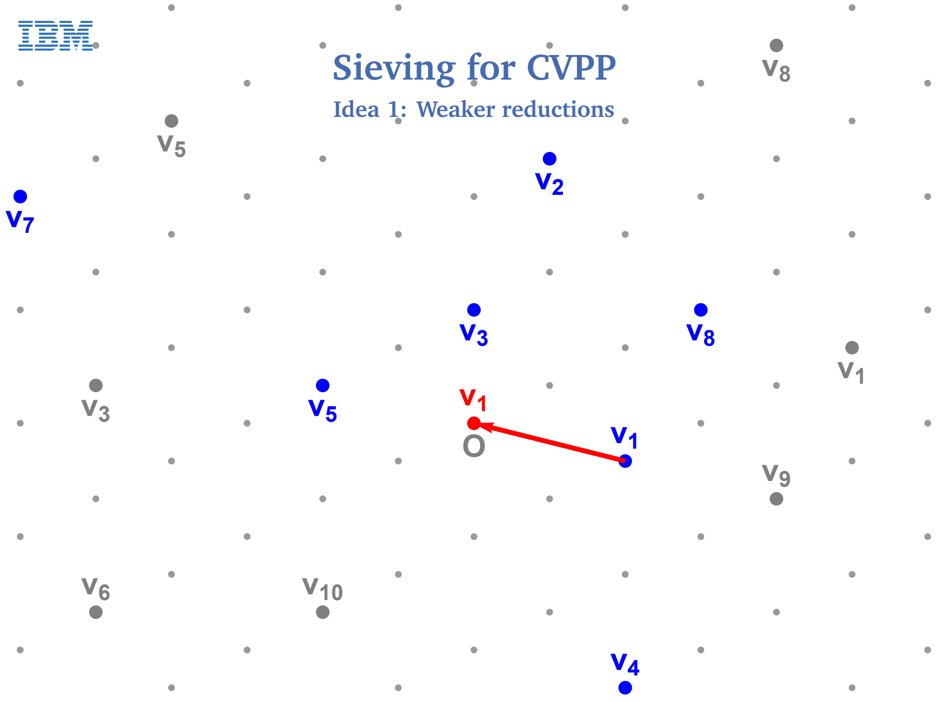
Sieving for CVPP

Idea 1: Weaker reductions



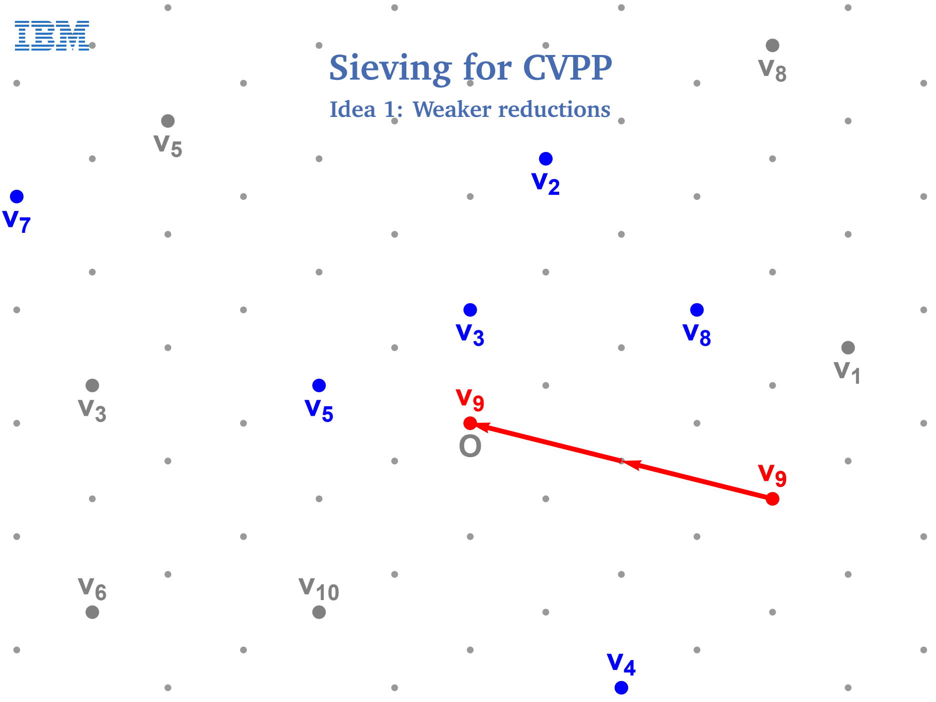
Sieving for CVPP

Idea 1: Weaker reductions



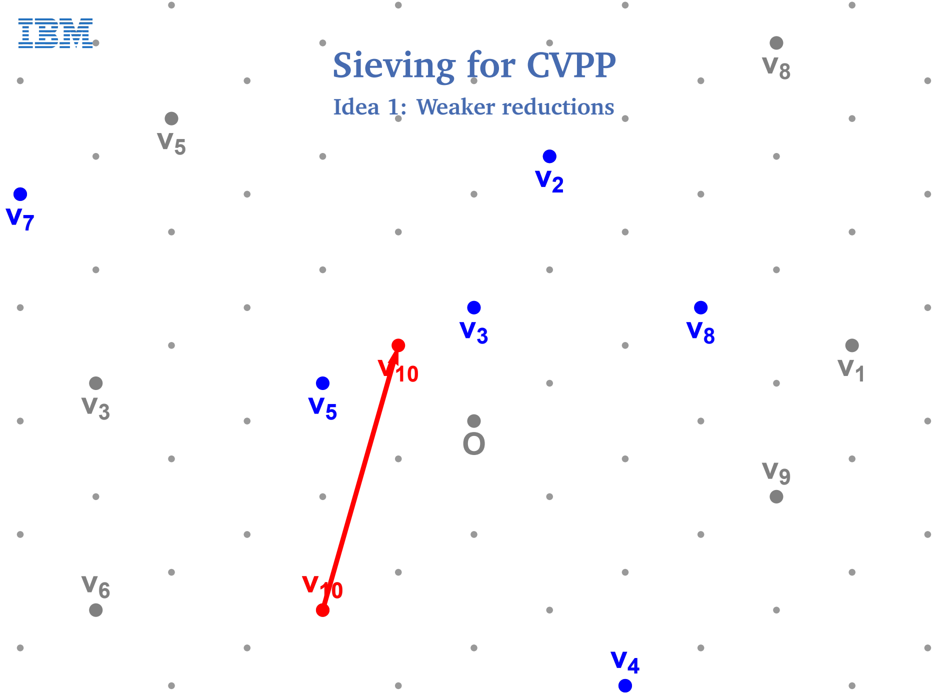
Sieving for CVPP

Idea 1: Weaker reductions



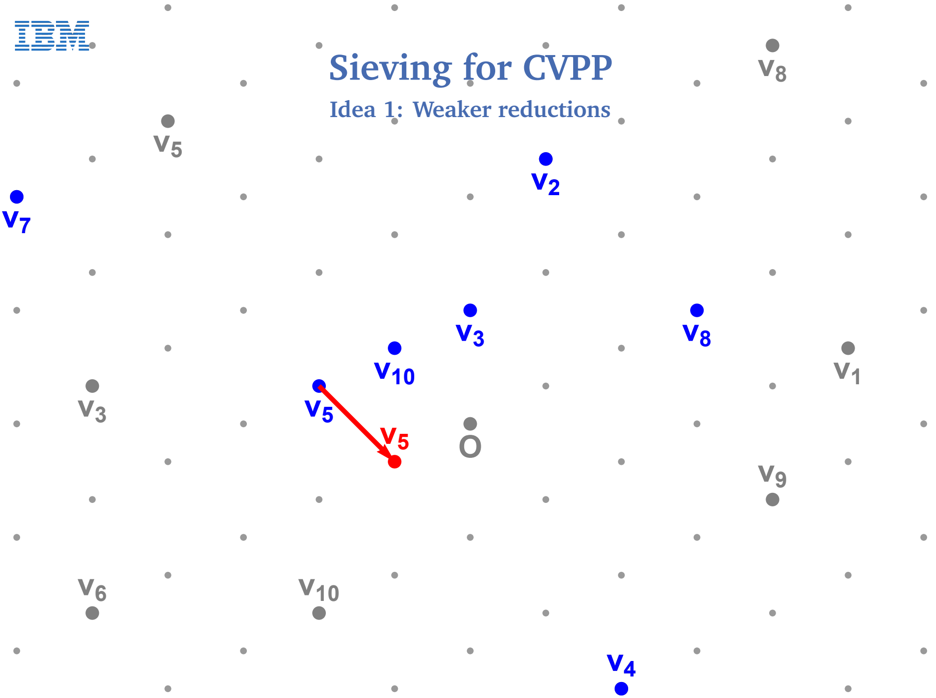
Sieving for CVPP

Idea 1: Weaker reductions



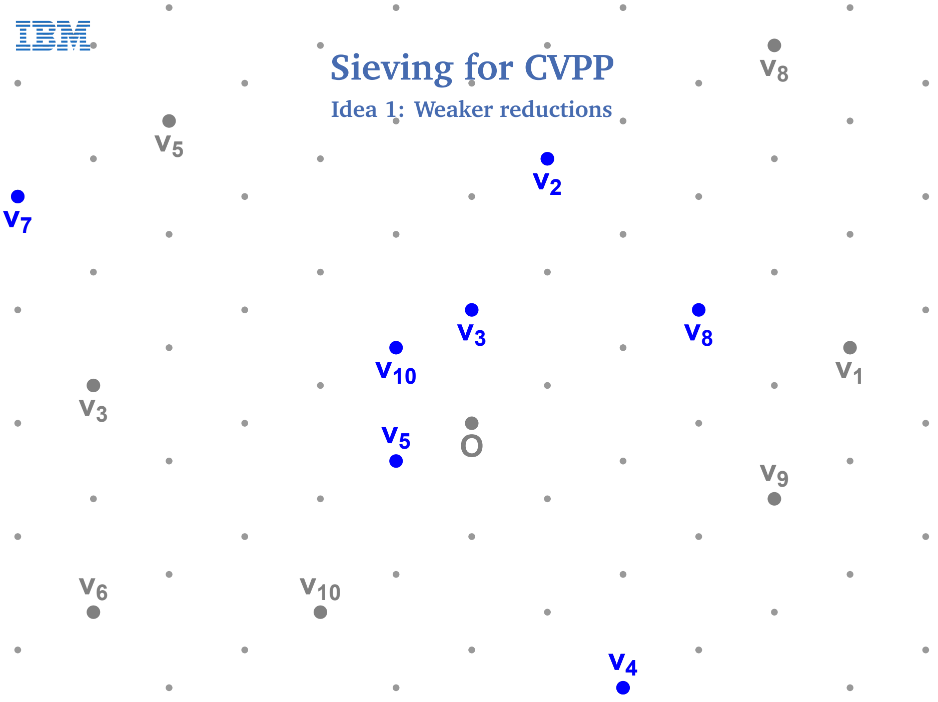
Sieving for CVPP

Idea 1: Weaker reductions



Sieving for CVPP

Idea 1: Weaker reductions



Sieving for CVPP

Solving the problems

- Idea 1: **Larger lists, weaker reductions**
  - Problem: Exponentially small success probability
  - To guarantee $\mathrm{Vol}(\mathscr{G}) \approx \mathrm{Vol}(\mathscr{V})$, need $2^{n/2+o(n)}$ vectors
  - Preprocessing: reduce $\boldsymbol{v}_1$ with $\boldsymbol{v}_2$ iff $\|\boldsymbol{v}_1 - \boldsymbol{v}_2\| \ll \|\boldsymbol{v}_1\|$

Sieving for CVPP

Solving the problems

- Idea 1: **Larger lists, weaker reductions**
  - Problem: Exponentially small success probability
  - To guarantee $\mathrm{Vol}(\mathscr{G}) \approx \mathrm{Vol}(\mathscr{V})$, need $2^{n/2+o(n)}$ vectors
  - Preprocessing: reduce $\boldsymbol{v}_1$ with $\boldsymbol{v}_2$ iff $\|\boldsymbol{v}_1 - \boldsymbol{v}_2\| \ll \|\boldsymbol{v}_1\|$
- Idea 2: **Rerandomizations**

Sieving for CVPP

Solving the problems

- Idea 1: **Larger lists, weaker reductions**
  - Problem: Exponentially small success probability
  - To guarantee $\mathrm{Vol}(\mathcal{G}) \approx \mathrm{Vol}(\mathcal{V})$, need $2^{n/2+o(n)}$ vectors
  - Preprocessing: reduce $\boldsymbol{v}_1$ with $\boldsymbol{v}_2$ iff $\|\boldsymbol{v}_1 - \boldsymbol{v}_2\| \ll \|\boldsymbol{v}_1\|$
- Idea 2: **Rerandomizations**
  - Problem: Probability only over randomness of targets

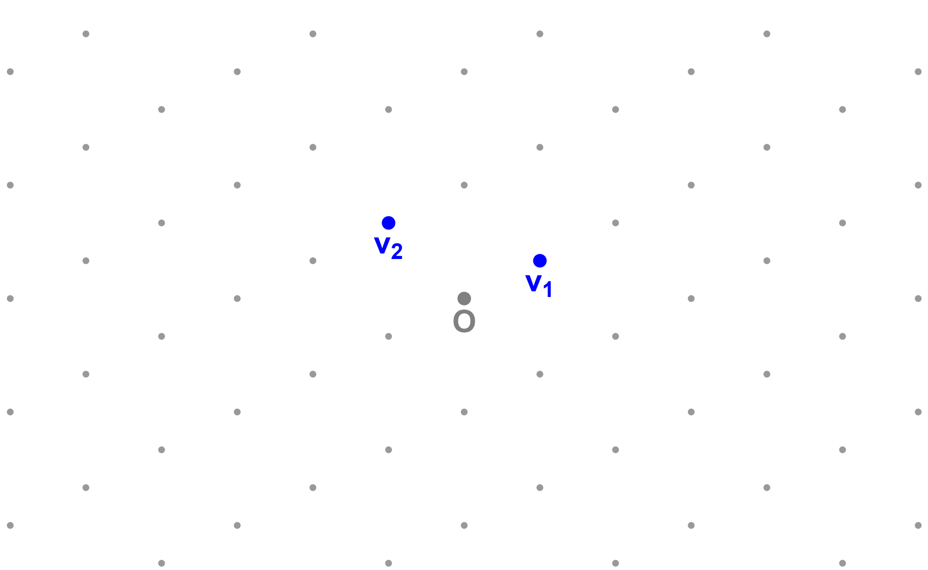
Sieving for CVPP

Solving the problems

- Idea 1: **Larger lists, weaker reductions**
  - Problem: Exponentially small success probability
  - To guarantee $\mathrm{Vol}(\mathscr{G}) \approx \mathrm{Vol}(\mathscr{V})$, need $2^{n/2+o(n)}$ vectors
  - Preprocessing: reduce $\boldsymbol{v}_1$ with $\boldsymbol{v}_2$ iff $\|\boldsymbol{v}_1 - \boldsymbol{v}_2\| \ll \|\boldsymbol{v}_1\|$
- Idea 2: **Rerandomizations**
  - Problem: Probability only over randomness of targets
  - Randomize target $\boldsymbol{t}$ before reducing ($\boldsymbol{t}' \in_R \boldsymbol{t} + \mathscr{L}$)
  - Randomness now over algorithm, independently of target

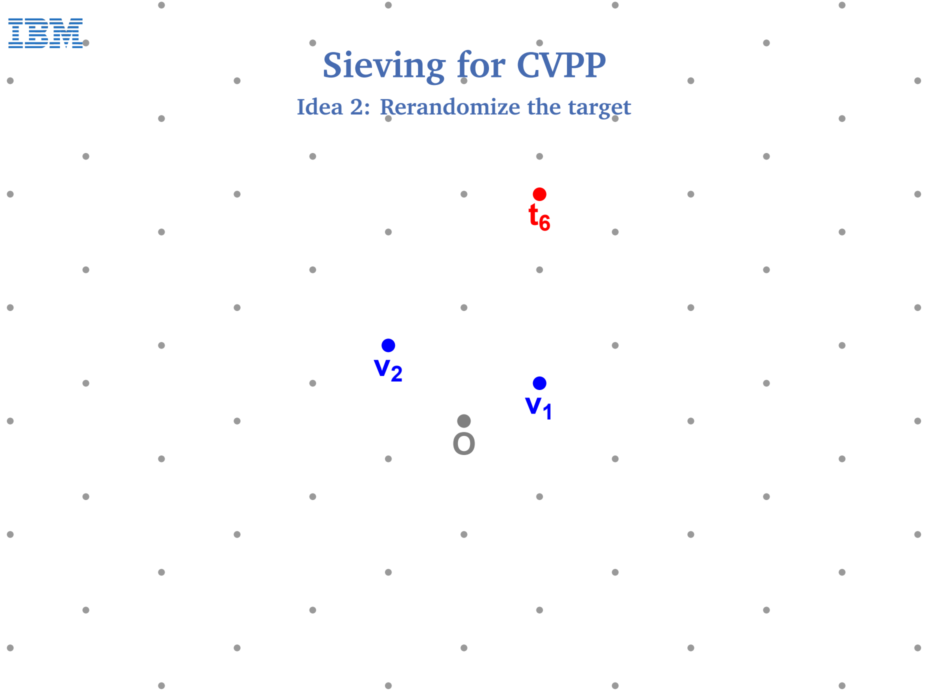
Sieving for CVPP

Idea 2: Rerandomize the target



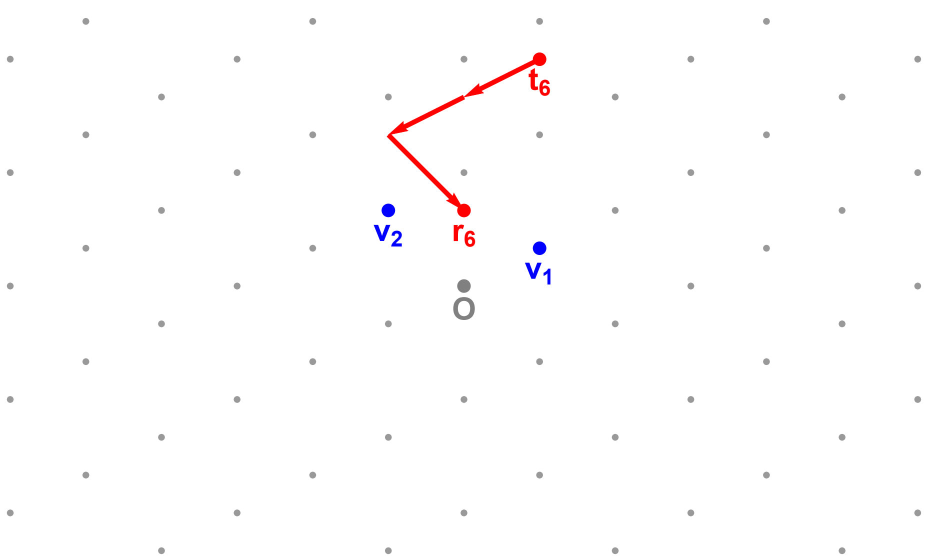
Sieving for CVPP

Idea 2: Rerandomize the target



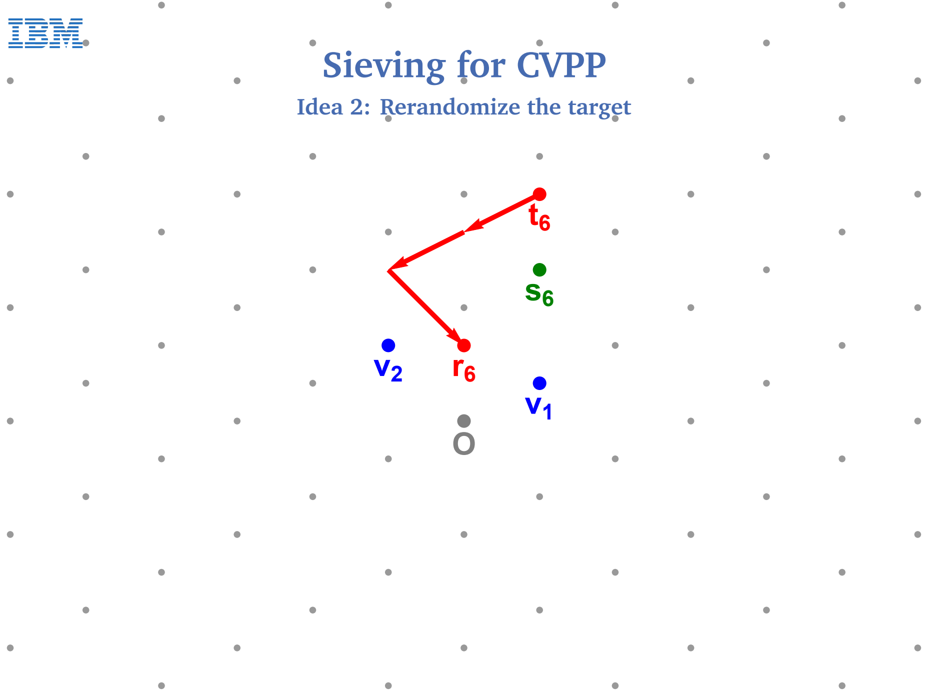
Sieving for CVPP

Idea 2: Rerandomize the target



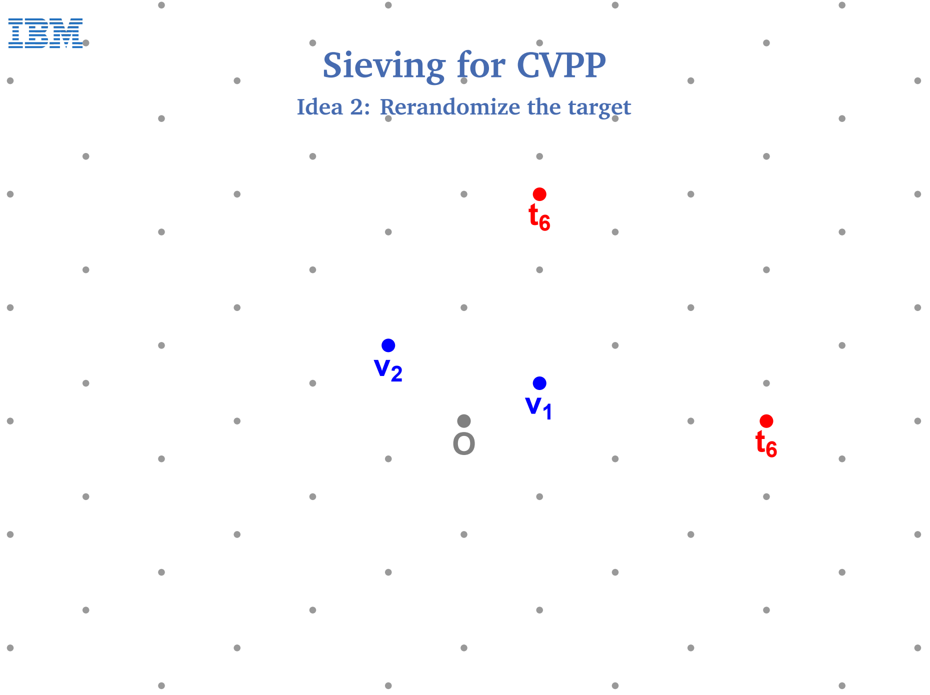
Sieving for CVPP

Idea 2: Rerandomize the target



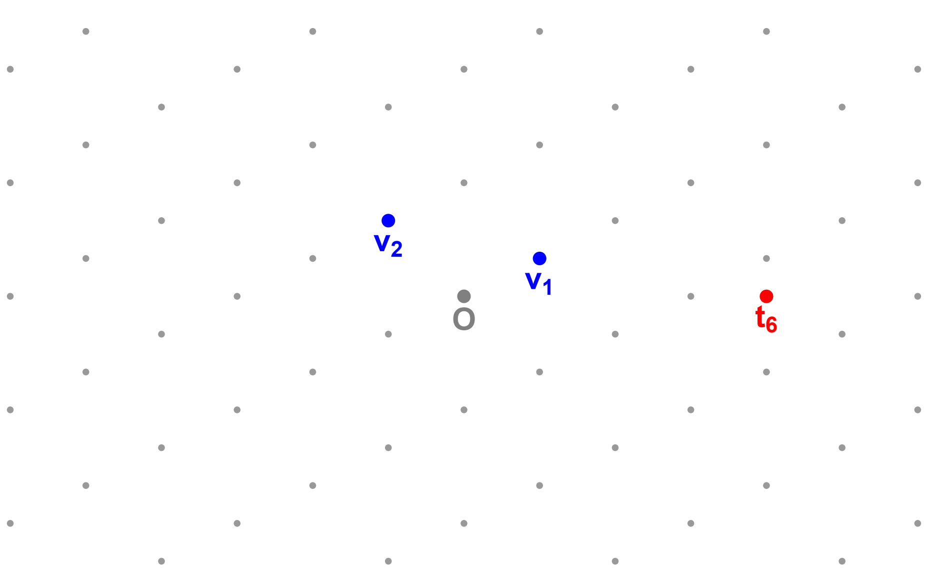
Sieving for CVPP

Idea 2: Rerandomize the target



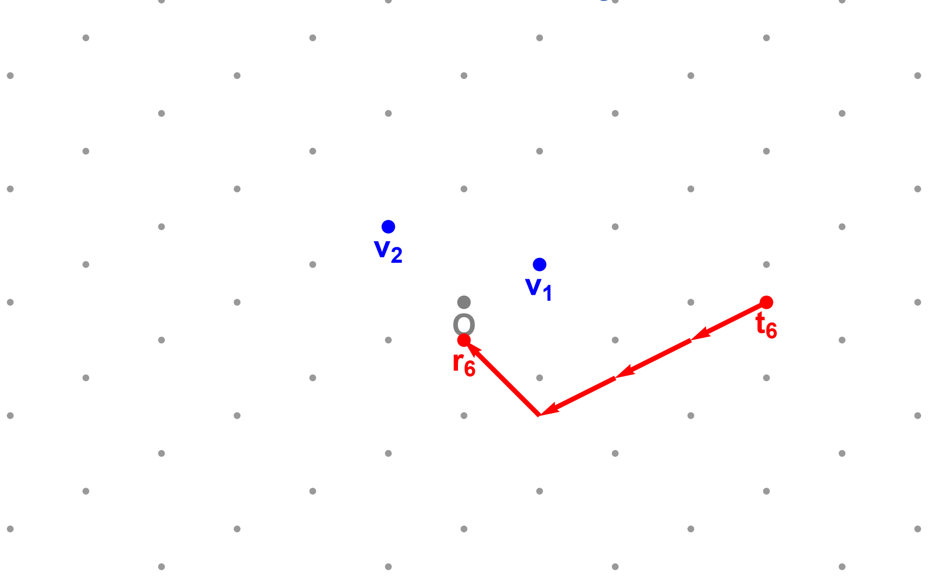
Sieving for CVPP

Idea 2: Rerandomize the target



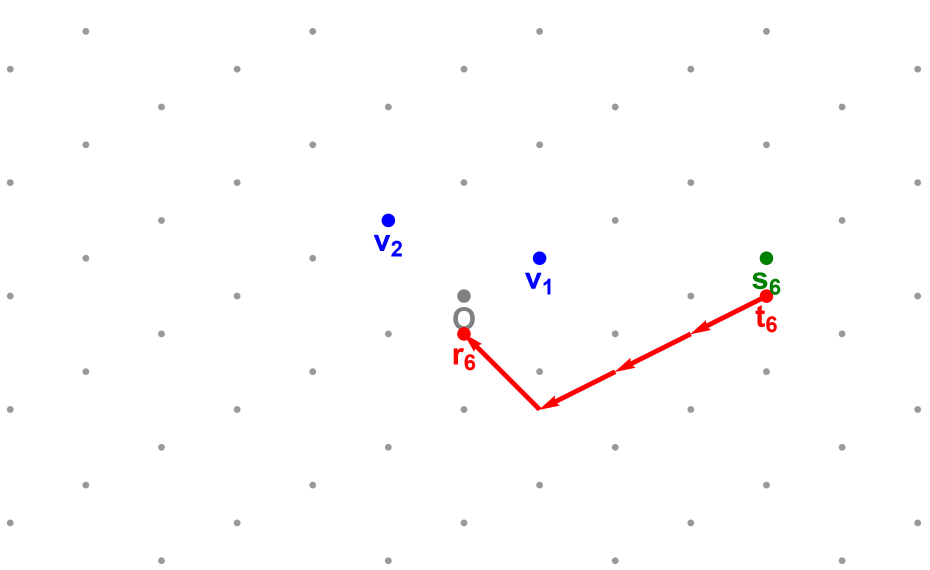
Sieving for CVPP

Idea 2: Rerandomize the target



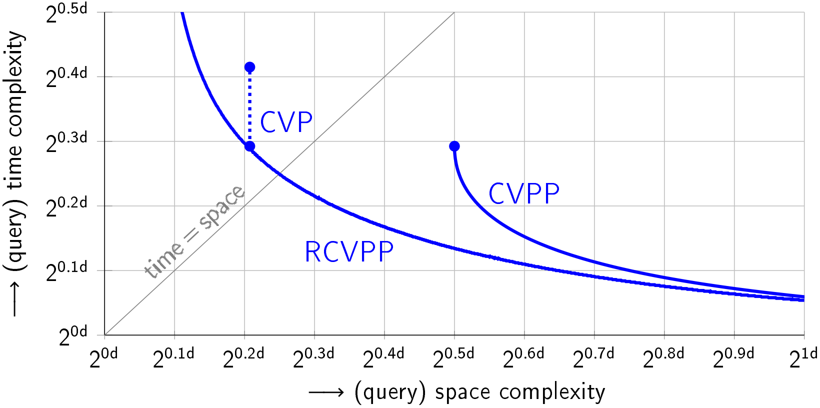
Sieving for CVPP

Idea 2: Rerandomize the target



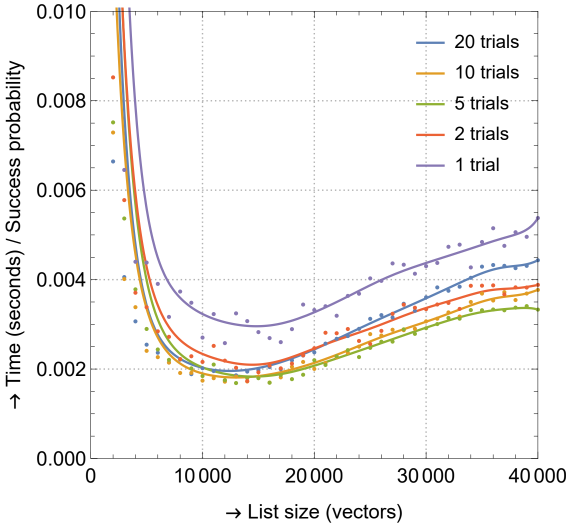
Sieving for CVPP

Trade-offs



Sieving for CVPP

Preliminary experiments ($n = 50$, HashSieve)



Conclusion

- Sieving for CVP same complexity as SVP

Conclusion

- Sieving for CVP same complexity as SVP
- Sieving for CVPP much easier than SVP

Conclusion

- Sieving for CVP same complexity as SVP
- Sieving for CVPP much easier than SVP
  - Preliminary experiments: 2000× faster in dimension 50

Conclusion

- Sieving for CVP same complexity as SVP
- Sieving for CVPP much easier than SVP
  - Preliminary experiments: 2000× faster in dimension 50
  - Competitive with enumeration for CVP(?)

Conclusion

- Sieving for CVP same complexity as SVP
- Sieving for CVPP much easier than SVP
  - Preliminary experiments: 2000× faster in dimension 50
  - Competitive with enumeration for CVP(?)
- Better complexities for approximate CVP and BDD

Conclusion

- Sieving for CVP same complexity as SVP
- Sieving for CVPP much easier than SVP
  - Preliminary experiments: 2000× faster in dimension 50
  - Competitive with enumeration for CVP(?)
- Better complexities for approximate CVP and BDD
- Open problem: hybrid enumeration with sieving

Conclusion

- Sieving for CVP same complexity as SVP
- Sieving for CVPP much easier than SVP
  - Preliminary experiments: 2000× faster in dimension 50
  - Competitive with enumeration for CVP(?)
- Better complexities for approximate CVP and BDD
- Open problem: hybrid enumeration with sieving
  - Bottom part of enumeration tree corresponds to batch-CVP

Conclusion

- Sieving for CVP same complexity as SVP
- Sieving for CVPP much easier than SVP
  - Preliminary experiments: 2000× faster in dimension 50
  - Competitive with enumeration for CVP(?)
- Better complexities for approximate CVP and BDD
- Open problem: hybrid enumeration with sieving
  - Bottom part of enumeration tree corresponds to batch-CVP
  - An efficient CVPP algorithm would speed up enumeration

Conclusion

- Sieving for CVP same complexity as SVP
- Sieving for CVPP much easier than SVP
  - Preliminary experiments: $2000\times$ faster in dimension 50
  - Competitive with enumeration for CVP(?)
- Better complexities for approximate CVP and BDD
- Open problem: hybrid enumeration with sieving
  - Bottom part of enumeration tree corresponds to batch-CVP
  - An efficient CVPP algorithm would speed up enumeration
  - CVPP in lower dimension $\implies$ no memory issues

Conclusion

- Sieving for CVP same complexity as SVP
- Sieving for CVPP much easier than SVP
  - Preliminary experiments: 2000× faster in dimension 50
  - Competitive with enumeration for CVP(?)
- Better complexities for approximate CVP and BDD
- Open problem: hybrid enumeration with sieving
  - Bottom part of enumeration tree corresponds to batch-CVP
  - An efficient CVPP algorithm would speed up enumeration
  - CVPP in lower dimension $\implies$ no memory issues
  - Randomized CVPP $\implies$ embarrassingly parallel

Questions?